Kamera sieciowa

Podręcznik użytkownika

UD09209B-A

Podręcznik użytkownika

Opis Podręcznika

Niniejszy Podręcznik dotyczy kamery sieciowej.

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

Podczas korzystania z niniejszego Podręcznika użytkownika należy uwzględniać zalecenia specjalistów.

Znaki towarowe

Zastrzeżenie prawne

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

W PRZYPADKU PRODUKTU Z DOSTĘPEM DO INTERNETU UŻYTKOWNIK KORZYSTA Z PRODUKTU NA WŁASNE RYZYKO. FIRMA HIKVISION NIE PONOSI ODPOWIEDZIALNOŚCI ZA NIEPRAWIDŁOWE FUNKCJONOWANIE PRODUKTU, NIEAUTORYZOWANE UJAWNIENIE 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.

Uwaga:

Jeżeli kamera nie synchronizuje czasu lokalnego z czasem sieciowym, należy ręcznie skonfigurować czas kamery. Należy ustanowić połączenie z kamerą i wyświetlić ustawienia czasu w oknie ustawień systemowych.

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.

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

	
Ostrzeżenia Należy przestrzegać tych środków ostrożności w celu uniknięcia poważnych obrażeń ciała lub śmierci.	**Uwagi** Należy przestrzegać tych środków ostrożności w celu uniknięcia potencjalnych obrażeń ciała lub szkód materialnych.

 **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. (Nasza firma nie ponosi żadnej odpowiedzialności za problemy spowodowane przez prace naprawcze lub konserwacyjne przeprowadzone przez nieautoryzowany serwis).

 **Uwagi:**

- Przed użyciem kamery należy upewnić się, że napięcie sieci elektrycznej jest odpowiednie.
- Należy chronić kamerę przed upadkiem lub udarem mechanicznym.
- Nie wolno dotykać modułów czujników palcami. Jeżeli konieczne jest oczyszczenie kamery, należy przetrzeć ją czystą ściereczką z niewielką ilością etanolu. Jeżeli kamera nie będzie używana przez dłuższy czas, należy zamocować na obiektywie kołpak chroniący czujnik przed kurzem i pyłem.
- Nie wolno kierować obiektywu kamery na źródło 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 wolno umieszczać kamery w lokalizacjach, w których występują bardzo wysokie lub niskie temperatury (zakres temperatur podano w specyfikacjach produktu), kurz, pył lub wilgoć, ani narażać jej na silne promieniowanie elektromagnetyczne.
- Aby zapobiec akumulacji ciepła, należy zapewnić prawidłową wentylację urządzenia.
- Należy chronić kamerę przed wodą i innymi cieczami.
- Przed transportem należy umieścić kamerę w oryginalnym opakowaniu lub użyć odpowiednich materiałów do pakowania. Można też użyć takiej samej tektury do pakowania.
- Nieprawidłowe użycie lub wymiana baterii może spowodować wybuch. Należy stosować rodzaj baterii zgodny z zaleceniami producenta.

Uwagi:

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

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

Spis treści

0505051080316

Rozdział 1 Wymagania systemowe

System operacyjny

Microsoft Windows XP SP1 lub nowszy

Procesor

2,0 GHz lub nowszy

Pamięć RAM

1 GB lub więcej

Komunikat na ekranie

Rozdzielczość 1024 x 768 lub większa

Przeglądarka internetowa

Internet Explorer w wersji 8.0 lub wyższej, Apple Safari w wersji 5.0.2 lub wyższej, Mozilla Firefox w wersji 30.0 lub wyższej i Google Chrome w wersji 31.0 lub wyższej.

Uwaga:

W przypadku programu Google Chrome w wersji 45 lub wyższej albo programu Mozilla Firefox w wersji 52 lub wyższej bez dodatków typu plug-in funkcje **Picture** i **Playback** są ukryte.

Aby korzystać z tych funkcji przy użyciu przeglądarki internetowej, należy zainstalować jej najniższą wersję lub zastąpić ją programem Internet Explorer w wersji 8.0 lub wyższej.

Rozdział 2 Połączenie sieciowe

Uwaga:

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

Zanim rozpoczniesz:

- Jeżeli chcesz konfigurować kamerę internetową przy użyciu sieci lokalnej (LAN, Local Area Network), zobacz *sekcję 2.1* ***Konfigurowanie kamery przy użyciu sieci LAN****.*
- Jeżeli chcesz konfigurować kamerę sieciową przy użyciu sieci rozległej (WAN, Wide Area Network), zobacz *sekcję 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.

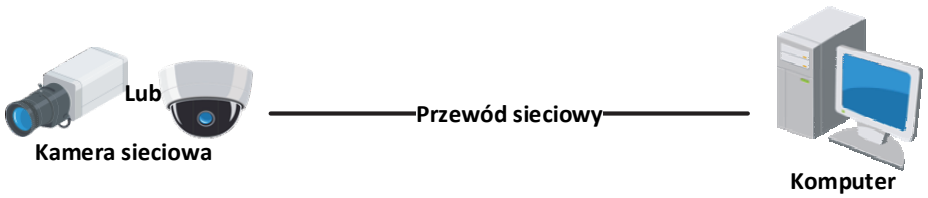
Uwaga: Aby uzyskać szczegółowe wprowadzenie do obsługi aplikacji SADP, należy zapoznać się z załącznikiem 1.

2.1.1 Połączenie przewodowe za pośrednictwem sieci LAN

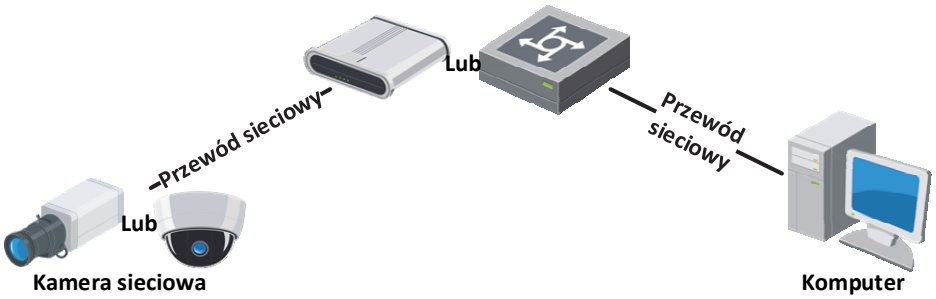
Na poniższych rysunkach przedstawiono dwie metody przewodowego połączenia kamery sieciowej z komputerem:

Cel:

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



Rysunek 2–1 Połączenie bezpośrednie



Rysunek 2–2 Połączenie przy użyciu przełącznika lub routera

2.1.2 Aktywacja kamery

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

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

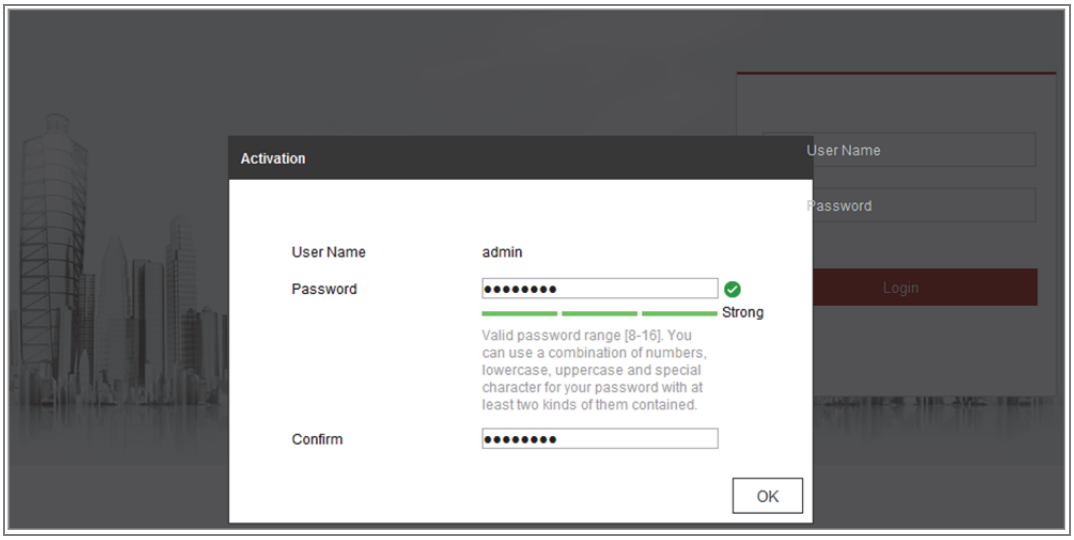
❖ Aktywacja za pośrednictwem przeglądarki internetowej

Kroki:

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

Uwagi:

- Domyślny adres IP kamery to 192.168.1.64.
- Komputer i kamera powinny należeć do tej samej podsieci.
- Obsługa protokołu DHCP w kamerze jest domyślnie włączona, dlatego należy wyszukać adres IP przy użyciu oprogramowania SADP.



Rysunek 2–3 Aktywacja przy użyciu przeglądarki internetowej

3. Utwórz hasło i wprowadź je w odpowiednim polu.

   Hasło nie powinno zawierać ciągu nazwy użytkownika.

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

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

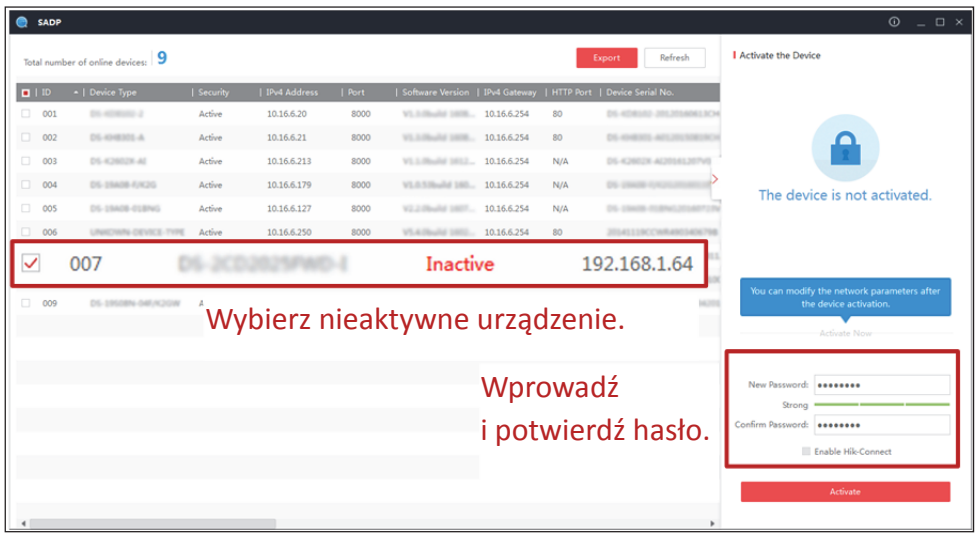
❖ Aktywacja za pośrednictwem aplikacji SADP

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

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

Kroki:

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



Rysunek 2–4 Oprogramowanie SADP

Uwaga:

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

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

   Hasło nie powinno zawierać ciągu nazwy użytkownika.

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

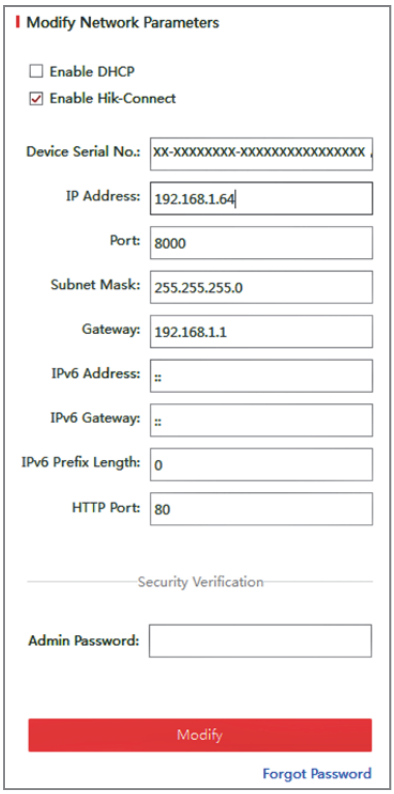
Uwaga:

Podczas aktywacji można włączyć usługę Hik-Connect dla urządzenia.

4. Kliknij przycisk Activate, aby rozpocząć aktywację.

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

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



Rysunek 2–5 Zmiana adresu IP

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

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

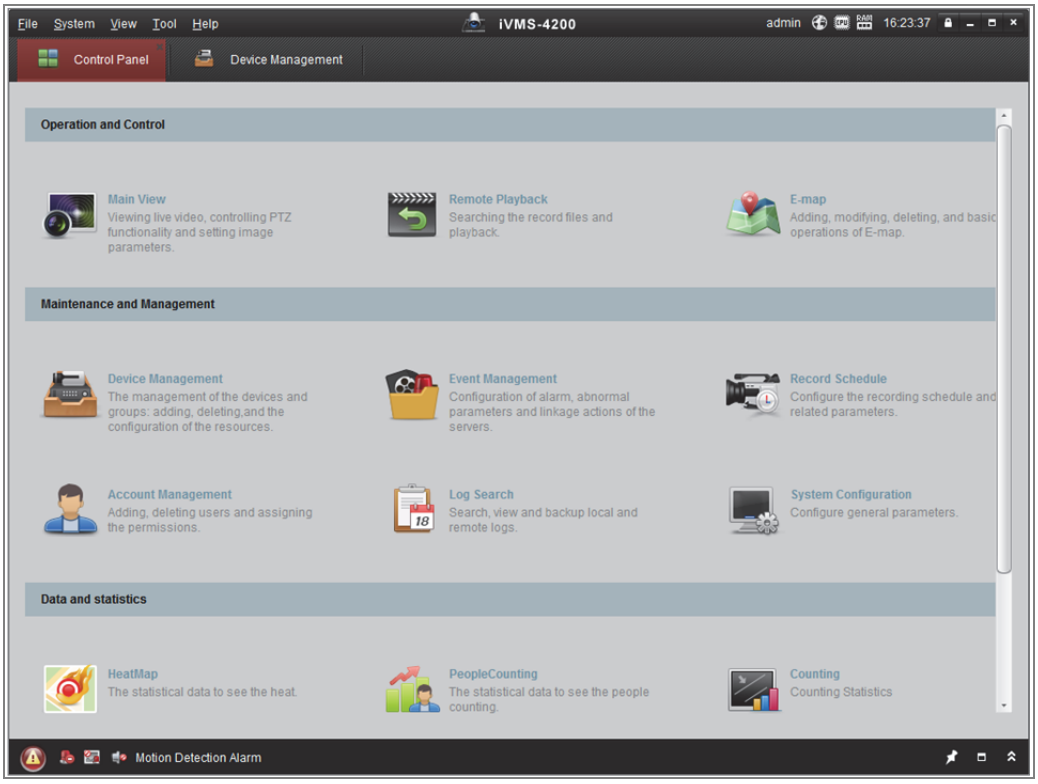
❖ Aktywacja za pośrednictwem oprogramowania do zarządzania urządzeniami wideo

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

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

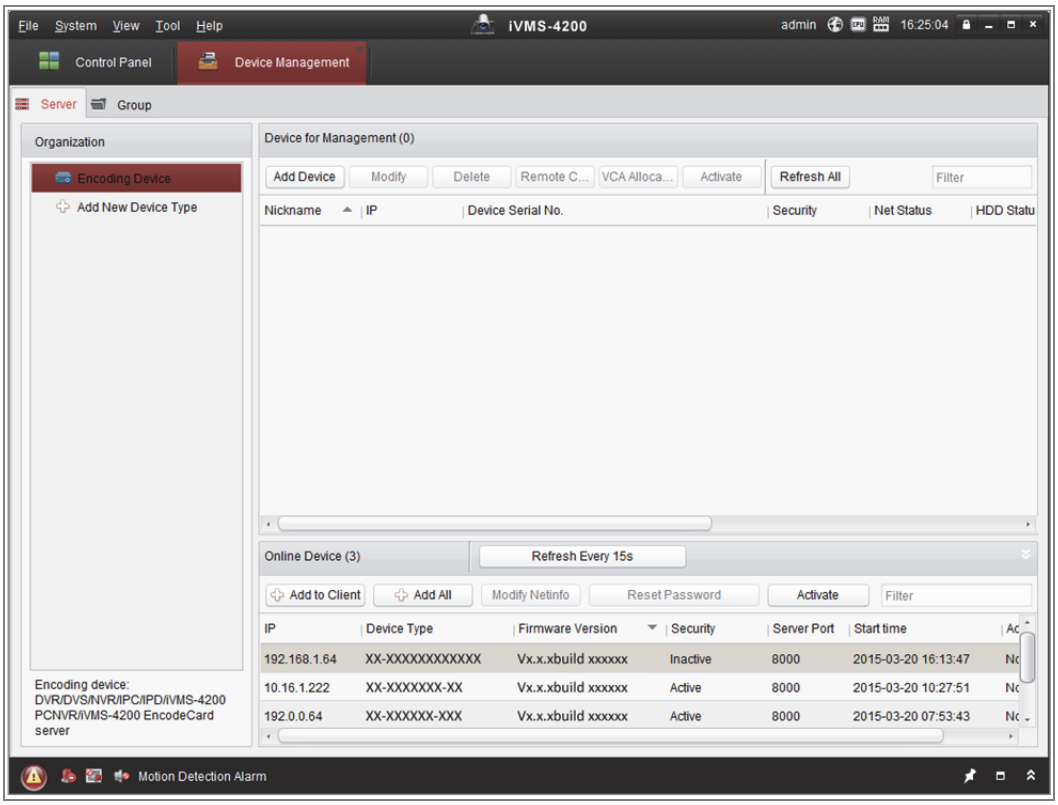
Kroki:

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



Rysunek 2–6 Panel sterowania

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

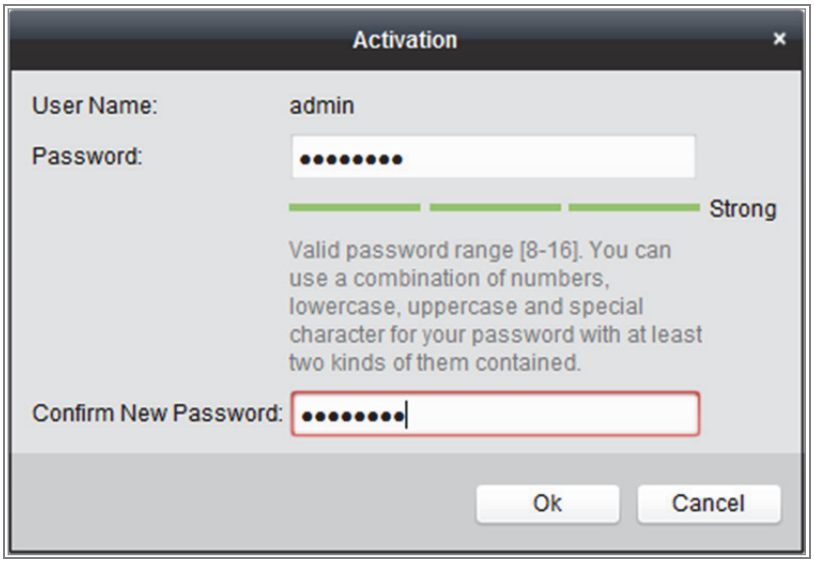


Rysunek 2–7 Zarządzanie urządzeniami

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

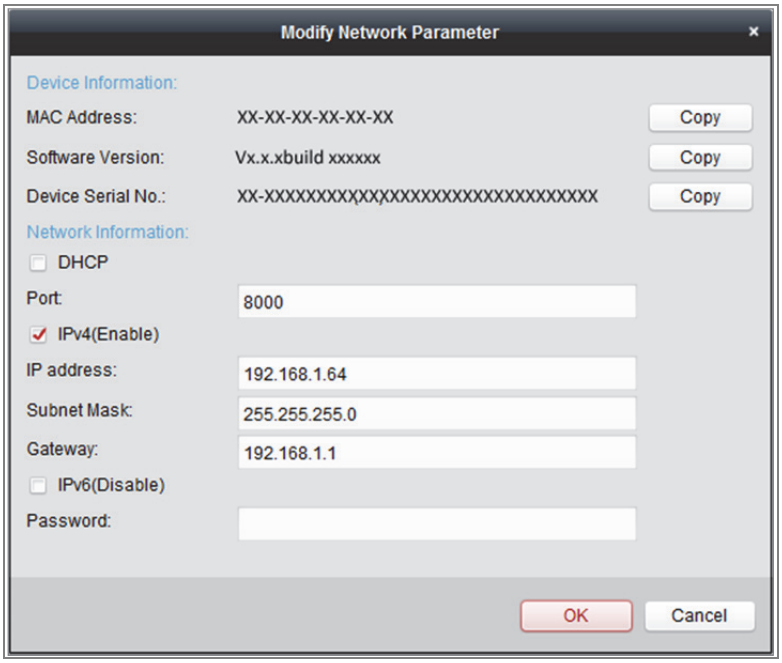
   Hasło nie powinno zawierać ciągu nazwy użytkownika.

Zalecane jest stosowanie silnego hasła —ZDECYDOWANIE ZALECAMY UTWORZENIE SILNEGO WŁASNEGO HASŁA (MINIMUM 8 ZNAKÓW Z UWZGLĘDNIENIEM PRZYNAJMNIEJ TRZECH Z NASTĘPUJĄCYCH KATEGORII: WIELKICH LITER, 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 okno Modyfikowanie parametrów sieciowych, przedstawione na rysunku poniżej.



Rysunek 2–9 Modyfikowanie parametrów sieciowych

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

2.1.3 (Opcjonalnie) Ustawianie pytania zabezpieczającego

Pytanie zabezpieczające umożliwia resetowanie hasła administratora, jeżeli administrator nie pamięta hasła.

Administrator może wprowadzić ustawienia pytania zabezpieczającego w oknie podręcznym podczas aktywacji kamery. Administrator może też skonfigurować tę funkcję w oknie **Zarządzanie użytkownikami**.

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 Połączenie przy użyciu statycznego adresu IP

Zanim rozpoczniesz:

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

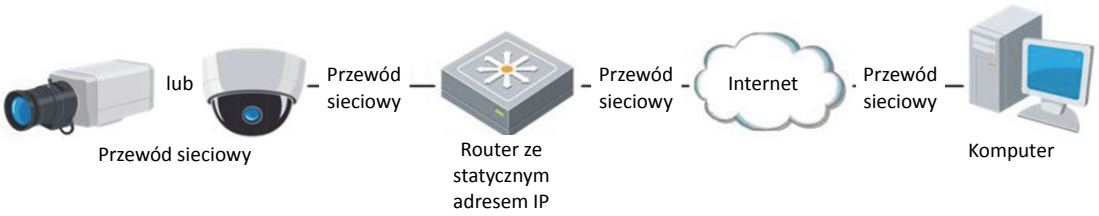
- **Połączenie kamery sieciowej przy użyciu routera**

Kroki:

1. Podłącz kamerę sieciową do routera.
2. Wprowadź adres IP sieci LAN, maskę podsieci i bramę. Aby uzyskać więcej informacji na temat konfiguracji adresu IP kamery sieciowej, zobacz sekcję 2.1.2.
3. Zapisz statyczny adres IP w ustawieniach routera.
4. Ustaw mapowanie portów, np. portów 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 przy użyciu routera ze statycznym adresem IP

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

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

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

2.2.2 Połączenie przy użyciu dynamicznego adresu IP

Zanim rozpoczniesz:

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

- **Połączenie kamery sieciowej przy użyciu routera**

Kroki:

1. Podłącz kamerę sieciową do routera.
2. Przypisz w kamerze adres IP sieci LAN, maskę podsieci i bramę. Aby uzyskać więcej informacji na temat konfiguracji adresu IP kamery sieciowej, zobacz sekcję 2.1.2.

3. W ustawieniach protokołu PPPoE routera wprowadź nazwę użytkownika, hasło i potwierdź hasło.
4. Ustaw mapowanie portów. Na przykład porty 80, 8000 i 554. Procedura mapowania portów może się różnić w zależności od modelu routera. Aby uzyskać pomoc w kwestii mapowania portów, należy skontaktować się z producentem routera.

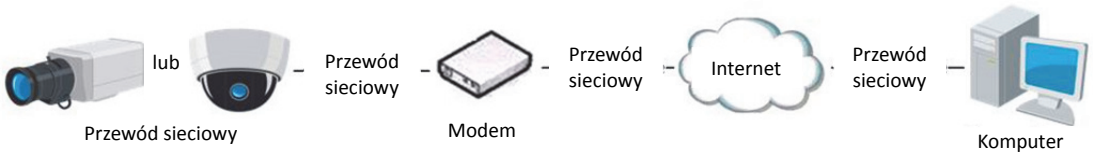
Uwaga: Aby uzyskać szczegółowe informacje na temat mapowania portów, należy zapoznać się z załącznikiem 2.

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

- **Połączenie kamery sieciowej przy użyciu modemu**

Cel:

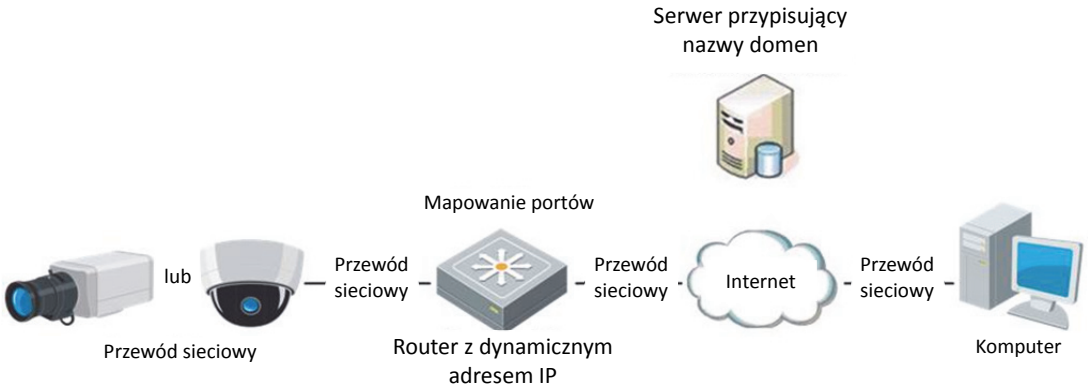
Ta kamera obsługuje automatyczne połączenia telefoniczne przy użyciu protokołu PPPoE. Kamera uzyskuje publiczny adres IP przy użyciu telefonicznego połączenia ADSL po podłączeniu jej do modemu. Należy skonfigurować parametry protokołu PPPoE kamery sieciowej. Aby uzyskać więcej informacji na temat konfiguracji, zobacz *sekcję 7.1.3* ***Konfigurowanie ustawień protokołu PPPoE.***



Rysunek 2–12 Dostęp do kamery z dynamicznym adresem IP

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

♦ Uzyskiwanie normalnej nazwy domeny



Rysunek 2–13 Uzyskiwanie normalnej nazwy domeny

Kroki:

1. Zastosuj nazwę domeny otrzymaną od dostawcy nazwy domeny.
2. Skonfiguruj ustawienia w oknie **Ustawienia systemu DDNS** kamery sieciowej. Aby uzyskać więcej informacji na temat konfiguracji, zobacz *sekcję 7.1.2* ***Konfigurowanie ustawień usługi DDNS***.
3. Uzyskaj dostęp do kamery przy użyciu zastosowanej nazwy domeny.

Rozdział 3 Dostęp do kamery sieciowej

3.1 Uzyskiwanie dostępu za pośrednictwem przeglądarki internetowej

Uwaga:

W przypadku niektórych modeli kamer protokół HTTPS jest domyślnie włączony, a kamera automatycznie tworzy niepodpisany certyfikat. Gdy kamera jest używana po raz pierwszy, przeglądarka internetowa powiadamia o problemie z certyfikatem. Aby anulować powiadamianie, należy zainstalować w kamerze podpisany certyfikat. Aby uzyskać więcej informacji na temat tej procedury, zobacz *7.2.6 Ustawienia protokołu HTTPS.*

Kroki:

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

   Uwaga:

   Domyślny adres IP to 192.168.1.64. Użytkownik powinien zmienić adres IP na adres w podsieci, w której znajduje się jego komputer.
3. Wprowadź nazwę użytkownika oraz hasło i kliknij przycisk **Login**.

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

   Uwaga:

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

Rysunek 3–1 Okno logowania

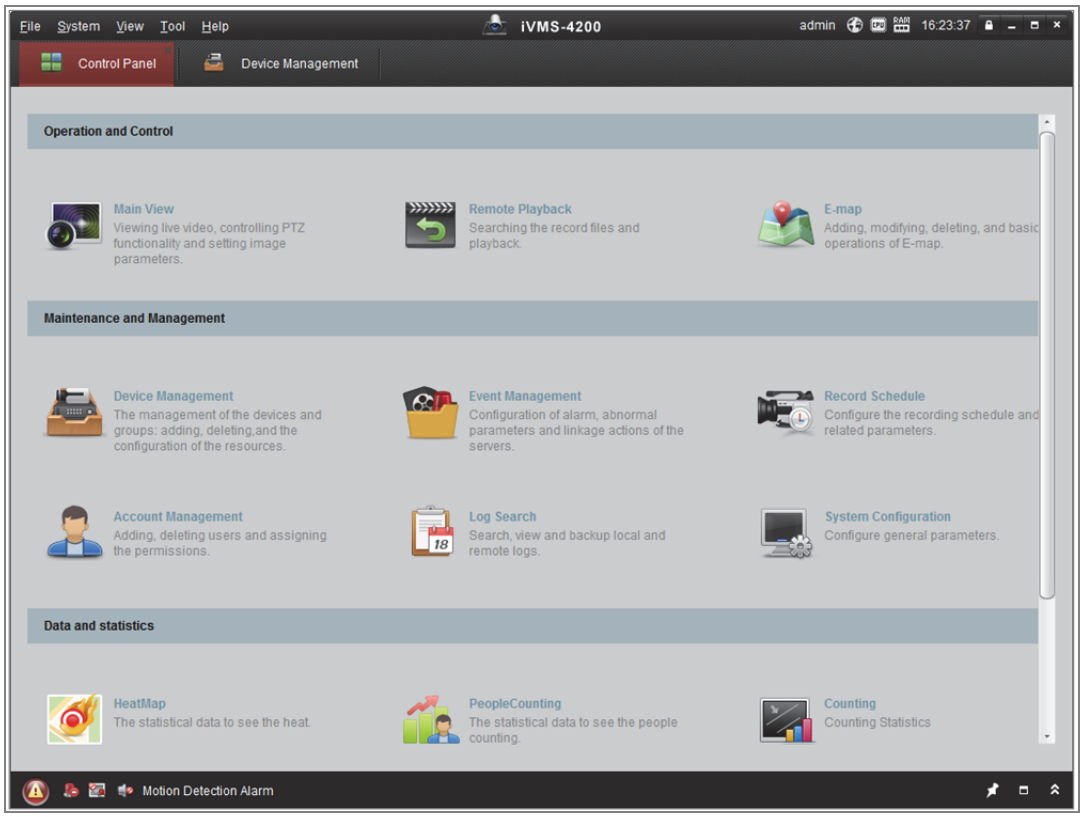
4. Kliknij przycisk **Login**.
5. (Opcjonalnie) Przed wyświetleniem podglądu na żywo i skorzystaniem z kamery zainstaluj dodatek typu plug-in. Postępuj zgodnie z monitami instalacyjnymi, aby zainstalować dodatek typu plug-in.

   Uwaga:

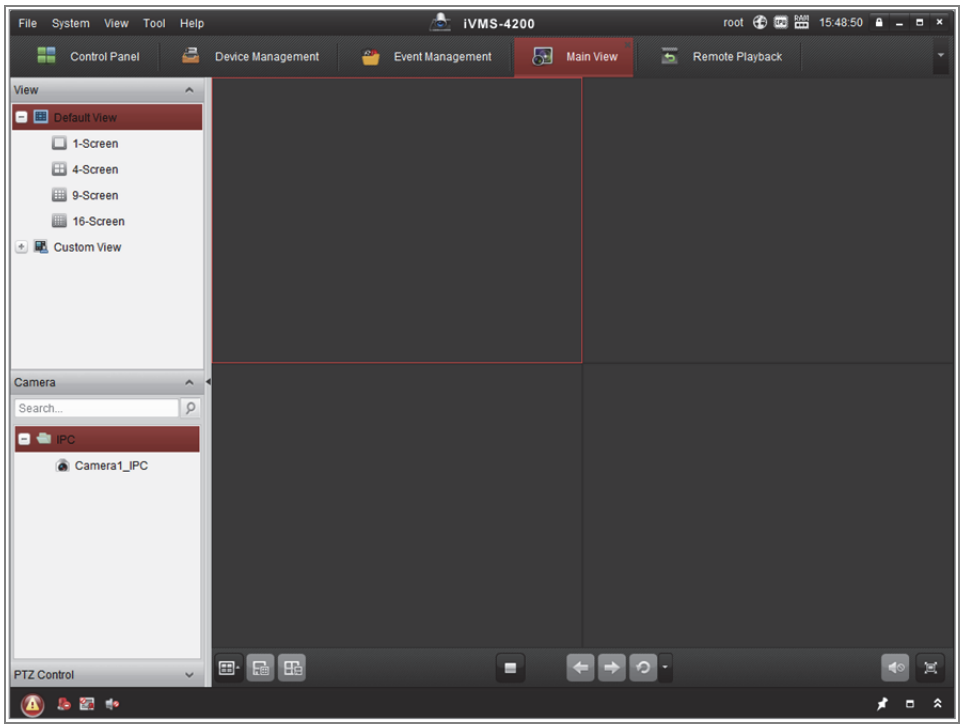
   W przypadku programu Google Chrome w wersji 45 lub wyższej albo programu Mozilla Firefox w wersji 52 lub wyższej bez dodatków typu plug-in instalacja nie jest wymagana. Funkcje **Picture** i **Playback** są jednak ukryte. Aby korzystać z tych funkcji przy użyciu przeglądarki internetowej, należy zainstalować jej najniższą wersję lub zastąpić ją programem Internet Explorer w wersji 8.0 lub wyższej.

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 3–2 Panel sterowania iVMS-4200



Rysunek 3–3 Widok główny oprogramowania iVMS-4200

Rozdział 4 Ustawienia Wi-Fi

Cel:

Korzystając z sieci bezprzewodowej, można ustanowić połączenie z siecią bez użycia kabla. Takie rozwiązanie jest bardzo praktyczne w przypadku monitoringu.

Uwaga: Ten Rozdział dotyczy tylko kamer z wbudowanym modułem Wi-Fi.

4.1 Konfigurowanie połączenia Wi-Fi w trybach zarządzania i ad-hoc

Cel:

Obsługiwane są dwa tryby połączenia. Należy wybrać tryb i wykonać kroki związane z konfigurowaniem sieci Wi-Fi.

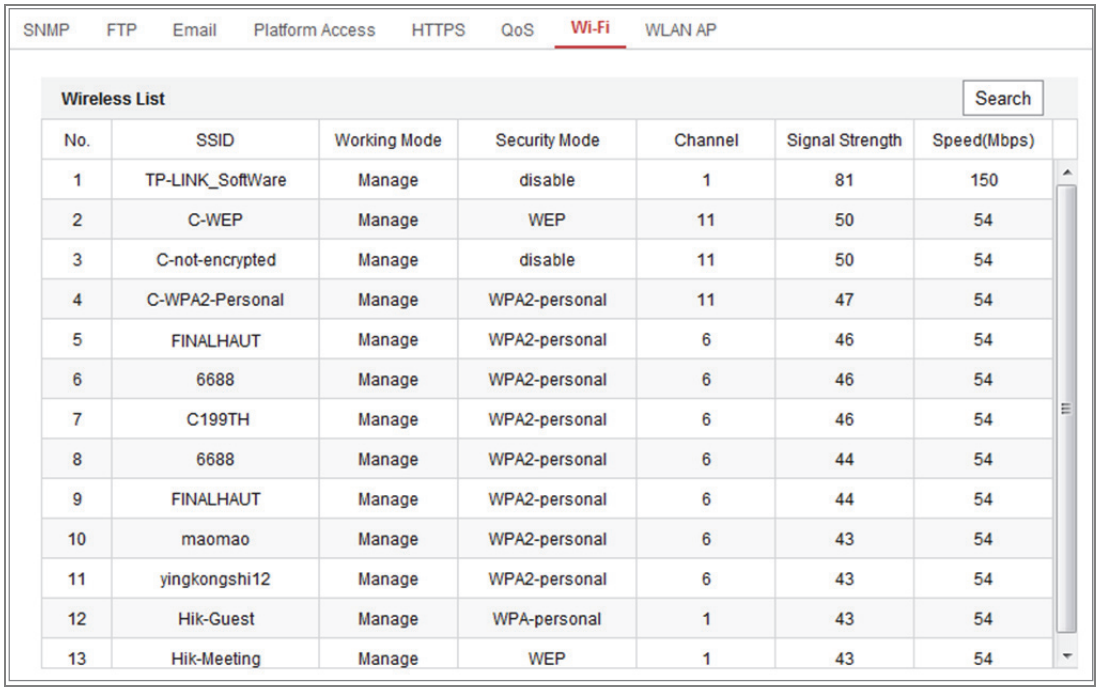
Połączenie bezprzewodowe w trybie zarządzania

Kroki:

1. Wyświetl okno konfiguracji Wi-Fi.

   Configuration > Network > Advanced Settings > Wi-Fi

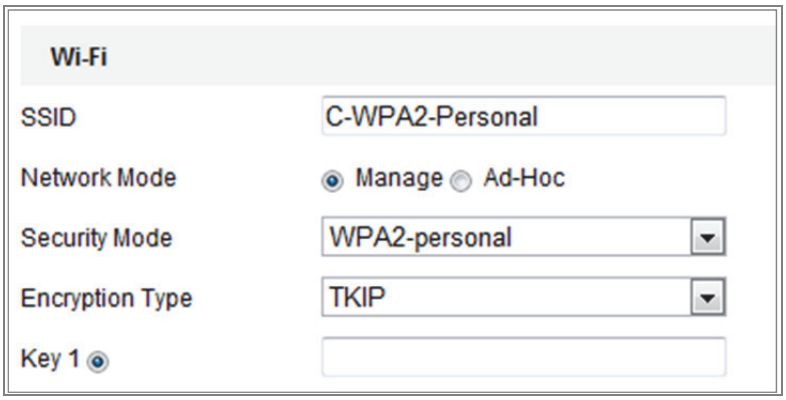
2. Kliknij przycisk **Search**, aby wyszukać połączenia online sieci bezprzewodowej.



No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
1	TP-LINK_SoftWare	Manage	disable	1	81	150
2	C-WEP	Manage	WEP	11	50	54
3	C-not-encrypted	Manage	disable	11	50	54
4	C-WPA2-Personal	Manage	WPA2-personal	11	47	54
5	FINALHAUT	Manage	WPA2-personal	6	46	54
6	6688	Manage	WPA2-personal	6	46	54
7	C199TH	Manage	WPA2-personal	6	46	54
8	6688	Manage	WPA2-personal	6	44	54
9	FINALHAUT	Manage	WPA2-personal	6	44	54
10	maomao	Manage	WPA2-personal	6	43	54
11	yingkongshi12	Manage	WPA2-personal	6	43	54
12	Hik-Guest	Manage	WPA-personal	1	43	54
13	Hik-Meeting	Manage	WEP	1	43	54

Rysunek 4–1 Lista Wi-Fi

3. Kliknij, aby wybrać połączenie bezprzewodowe na liście.



Rysunek 4–2 Tryb zarządzania w ustawieniach Wi-Fi

4. Zaznacz opcję *Manage* w sekcji *Network mode*. Ustawienie *Security mode* sieci zostanie wyświetlone automatycznie po wybraniu sieci bezprzewodowej i nie powinno być zmieniane ręcznie.

Uwaga: Te parametry są takie same, jak parametry routera.

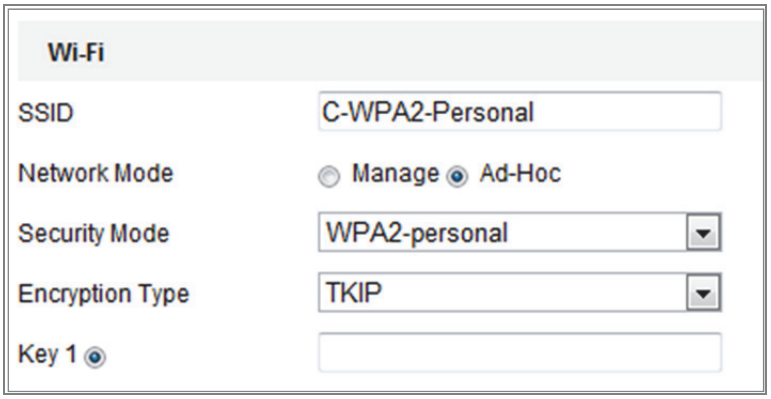
5. Wprowadź hasło połączenia z siecią bezprzewodową. Hasło powinno być takie samo, jak hasło połączenia sieci bezprzewodowej ustawione na routerze.

Połączenie bezprzewodowe w trybie ad-hoc

Jeżeli zostanie wybrany tryb Ad-hoc, ustanawianie połączenia z kamerą bezprzewodową za pośrednictwem routera nie jest konieczne. Scenariusz jest taki sam, jak w przypadku bezpośredniego połączenia kamery z komputerem przy użyciu kabla sieciowego.

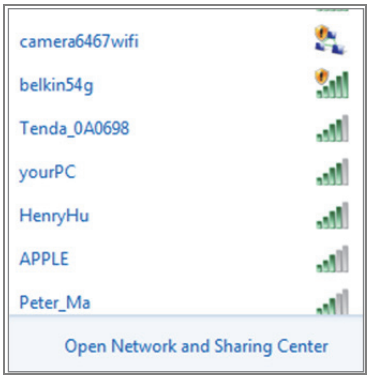
Kroki:

1. Wybierz tryb Ad-hoc.



Rysunek 4–3 Ustawienia Wi-Fi trybu ad-hoc

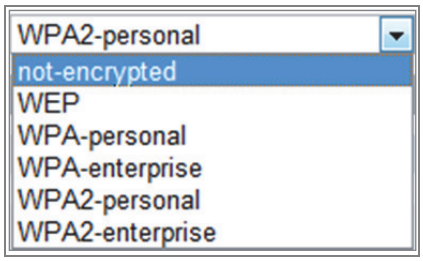
2. Dostosuj identyfikator SSID kamery.
3. Wybierz ustawienie Tryb zabezpieczenia połączenia bezprzewodowego.
4. Włącz funkcję połączeń bezprzewodowych dla komputera.
5. Po stronie komputera wyszukaj sieć, aby wyświetlić identyfikator SSID kamery na liście.



Rysunek 4–4 Punkt połączenia ad-hoc

6. Wybierz identyfikator SSID i ustanów połączenie.

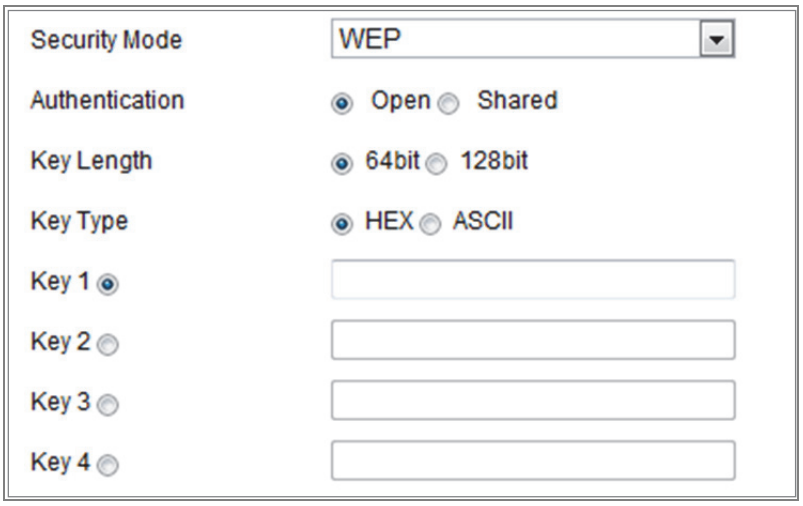
Opis trybu zabezpieczeń:



Rysunek 4–5 Tryb zabezpieczeń

Można wybrać dla opcji Security Mode ustawienia Not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal lub WPA2-enterprise.

Tryb WEP:



Rysunek 4–6 Tryb WEP

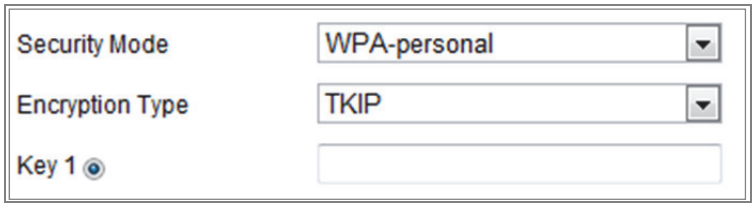
- Authentication — wybierz system uwierzytelniania przy użyciu klucza Open lub Shared, zależnie od metody używanej przez punkt dostępu. W przypadku niektórych punktów dostępu ta opcja jest niedostępna i prawdopodobnie używany jest system Open, zwany czasami uwierzytelnianiem SSID.
- Key length — długość klucza używanego do 64-bitowego lub 128-bitowego szyfrowania połączeń bezprzewodowych. Czasami może być wyświetlana długość klucza szyfrowania 40/64 i 104/128.
- Typ klucza — typy dostępnych kluczy są zależne od używanego punktu dostępu. Dostępne są następujące opcje:

  HEX — umożliwia ręczne wprowadzenie klucza w formacie szesnastkowym.

  ASCII — w przypadku tej metody wymagany jest ciąg pięciu znaków (tryb WEP 64-bitowy) i trzynastu znaków (tryb WEP 128-bitowy).

Tryb WPA-personal i WPA2-personal:

Wprowadź wymagany klucz wstępny dla punktu dostępu, który może być liczbą szesnastkową lub hasłem.

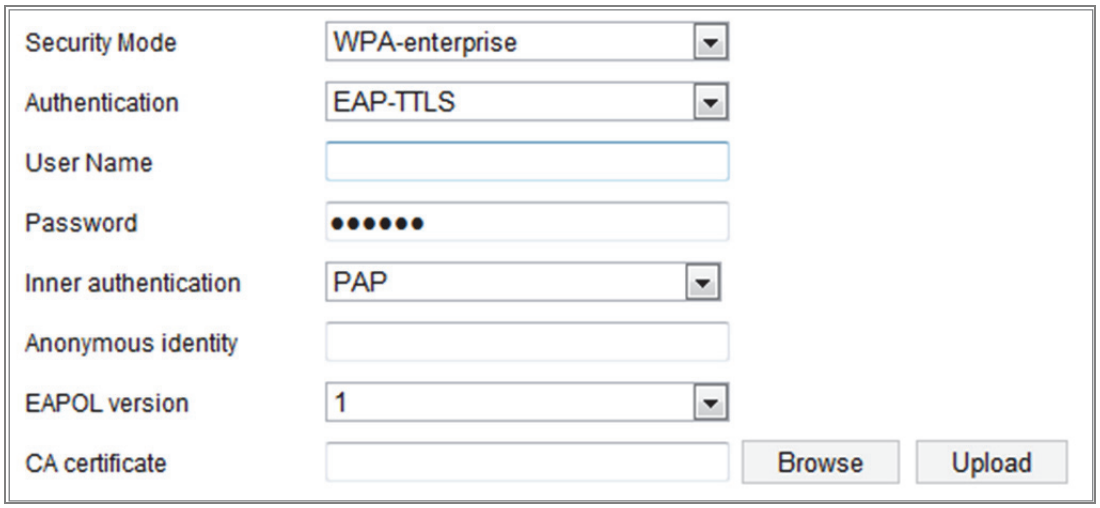


Rysunek 4–7 Tryb zabezpieczeń WPA-personal

Tryb WPA-enterprise i WPA2-enterprise:

Wybierz typ uwierzytelniania klient/serwer używany przez punkt dostępu (EAP-TTLS lub EAP-PEAP).

EAP-TLS



Rysunek 4–8 Uwierzytelnianie EAP-TLS

- Identity — wprowadź identyfikator użytkownika, który będzie wyświetlany w sieci.
- Private key password — wprowadź hasło dla swojego identyfikatora użytkownika.
- EAPOL version — wybierz wersję (1 lub 2) używaną w punkcie dostępu.
- CA Certificates — przekaż certyfikat urzędu certyfikacji (CA) wysyłany do punktu dostępu w celu uwierzytelnienia.

EAP-PEAP:

- User Name — wprowadź nazwę użytkownika wyświetlaną w sieci.
- Password — wprowadź hasło sieci.
- PEAP Version — wybierz wersję protokołu PEAP używanego w punkcie dostępu.
- Label — wybierz etykietę używaną przez punkt dostępu.
- EAPOL version — wybierz wersję (1 lub 2) używaną w punkcie dostępu.
- CA Certificates — przekaż certyfikat urzędu certyfikacji (CA) wysyłany do punktu dostępu w celu uwierzytelnienia.

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

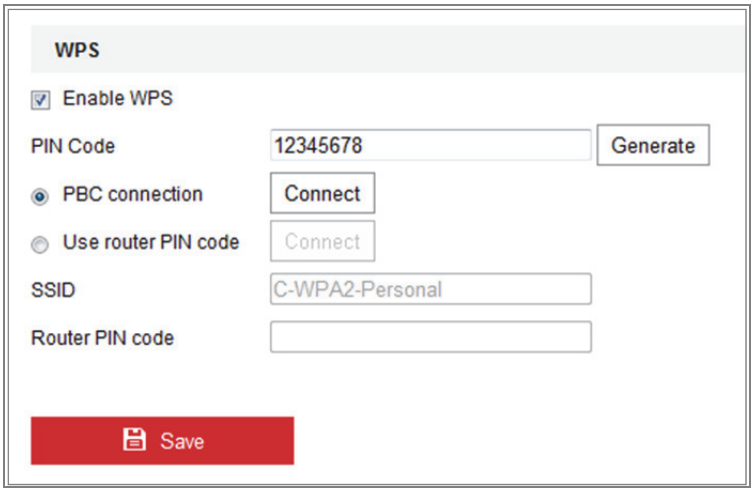
4.2 Łatwe ustanawianie połączenia Wi-Fi przy użyciu funkcji WPS

Cel:

Ustanawianie połączenia sieci bezprzewodowej jest złożonym procesem. Aby uniknąć złożonej konfiguracji połączenia bezprzewodowego, można włączyć funkcję WPS. Funkcja WPS (Wi-Fi Protected Setup) ułatwia konfigurację szyfrowanego połączenia urządzenia z routerem bezprzewodowym. Funkcja WPS ułatwia dodawanie nowych urządzeń do istniejącej sieci bez konieczności wprowadzania długich haseł. Dostępne są dwa tryby połączenia WPS: PBC i PIN.

Uwaga: Jeżeli funkcja WPS jest włączona, konfigurowanie parametrów, takich jak typ szyfrowania, i pamiętanie klucza połączenia bezprzewodowego nie jest konieczne.

Kroki:

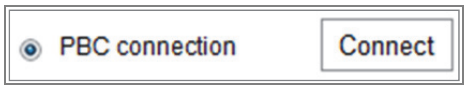


Rysunek 4–9 Ustawienia funkcji WPS Wi-Fi

Tryb *PBC*:

Skrót PBC oznacza konfigurację przycisków (Push-Button-Configuration), w której użytkownik po prostu naciska przycisk rzeczywisty lub wirtualny (taki jak przycisk Connect w oknie konfiguracji przeglądarki Internet Explorer) zarówno w punkcie dostępu (i witrynie rejestratora sieci), jak i w nowym bezprzewodowym urządzeniu klienckim.

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



Uwaga: Ten tryb musi być obsługiwany zarówno przez punkty dostępu, jak i łączące się z nimi urządzenia.

3. Sprawdź, czy router Wi-Fi jest wyposażony w przycisk WPS. Jeżeli tak, naciśnij ten przycisk. Wskaźnik obok przycisku zacznie migać, sygnalizując włączenie funkcji WPS routera. Aby uzyskać więcej informacji, skorzystaj z podręcznika użytkownika routera.
4. Naciśnij przycisk WPS, aby włączyć tę funkcję w kamerze.

Jeżeli kamera nie jest wyposażona w przycisk WPS, można też kliknąć przycisk wirtualny, aby włączyć funkcję PBC interfejsu internetowego.

5. Kliknij przycisk **Connect**.

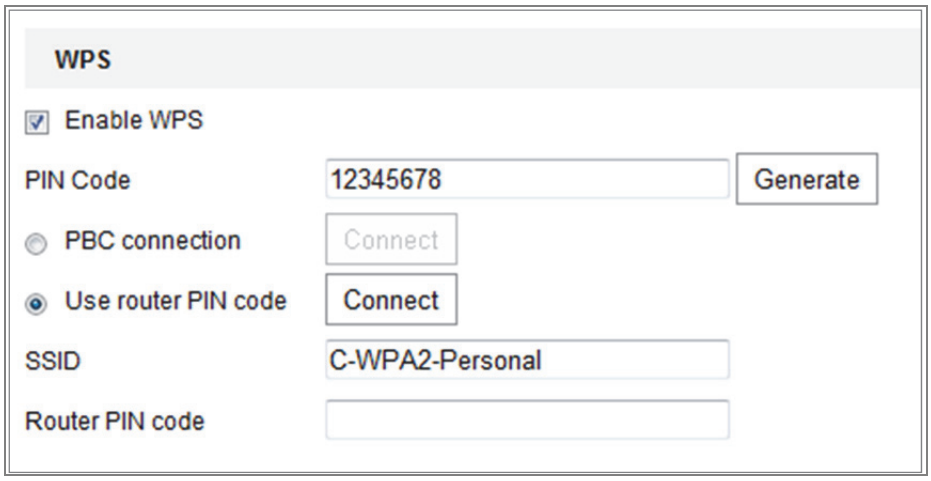
Gdy tryb PBC jest włączony zarówno w routerze, jak i kamerze, kamera jest łączona z siecią bezprzewodową automatycznie.

Tryb PIN:

W tym trybie wymagane jest odczytanie numeru identyfikacyjnego (PIN, Personal Identification Number) z etykiety lub wyświetlacza nowego urządzenia bezprzewodowego. Ten kod PIN należy następnie wprowadzić w celu ustanowienia połączenia z siecią (zazwyczaj punktem dostępu sieci).

Kroki:

1. Wybierz połączenie bezprzewodowe z listy. Identyfikator SSID zostanie wczytany automatycznie.
2. Wybierz opcję **Use route PIN code**.



Rysunek 4–10 Korzystanie z kodu PIN

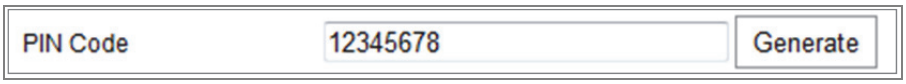
Jeżeli kod PIN jest generowany po stronie routera, należy wprowadzić kod PIN uzyskany z routera w polu **Router PIN code**.

3. Kliknij przycisk **Connect**.

Lub

Można wygenerować kod PIN po stronie kamery. Kod PIN wygasa po 120 sekundach.

1. Kliknij przycisk **Generate**.



2. Wprowadź kod w routerze. W przedstawionym przykładzie należy wprowadzić 48167581 w routerze.

4.3 Ustawienia własności adresu IP dla połączenia sieci bezprzewodowej

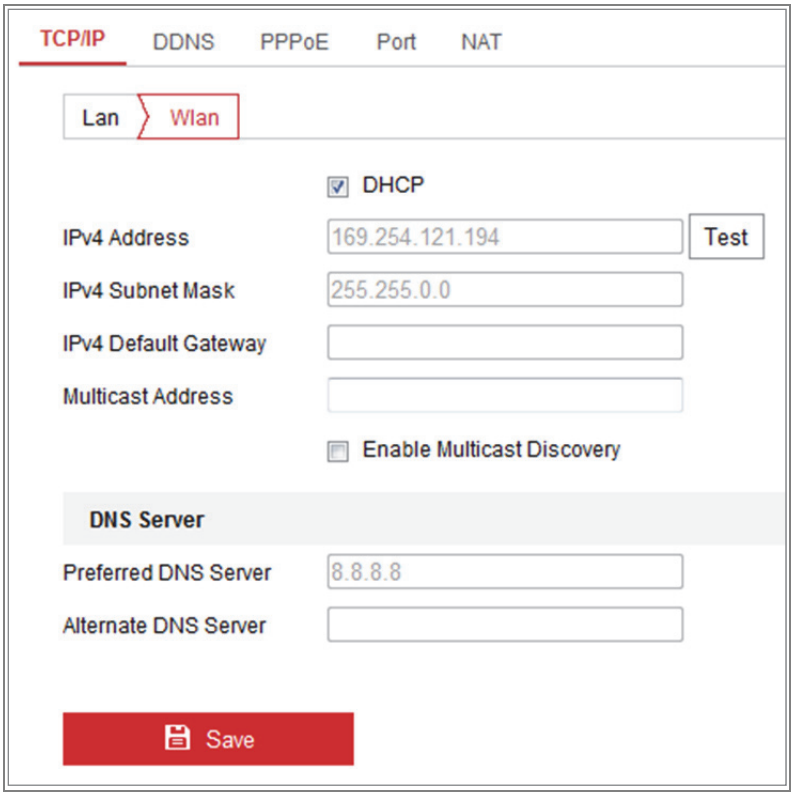
Domyślny adres IP karty sieci bezprzewodowej to 192.168.1.64. Podczas ustanawiania połączenia z siecią bezprzewodową można zmienić domyślny adres IP.

Kroki:

1. Wyświetl okno konfiguracji protokołu TCP/IP.

   Configuration > Network > Basic Settings > TCP/IP

2. Wybierz kartę Wlan.



Rysunek 4–11 Ustawianie parametrów sieci WLAN

3. Dostosuj adres IPv4, maskę podsieci IPv4 i bramę domyślną.

   Procedura konfiguracji jest taka sama, jak w przypadku sieci LAN.

   Jeżeli chcesz przypisać adres IP, możesz zaznaczyć pole wyboru, aby włączyć obsługę protokołu DHCP.

Rozdział 5 Widok na żywo

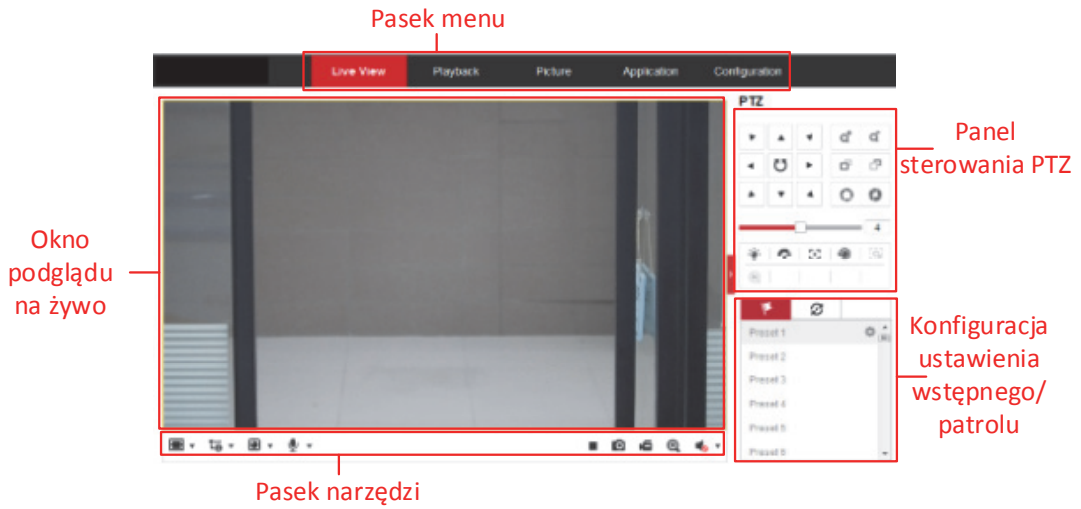
5.1 Interfejs podglądu na żywo

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 strony głównej.

Opis elementów interfejsu podglądu na żywo:



Rysunek 5–1 Strona podglądu na żywo

Pasek menu:

Kliknij poszczególne karty, aby wyświetlić strony Podgląd na żywo, Odtwarzanie, Zdjęcia, Aplikacja i Konfiguracja.

Okno podglądu na żywo:

Służy do wyświetlania obrazu podglądu na żywo.

Pasek narzędzi:

Korzystając z paska narzędzi, można dostosować rozmiar okna podglądu na żywo, typ strumienia i dodatki typu plug-in. Można wykonywać operacje na stronie podglądu

na żywo, takie jak uruchamianie/zatrzymywanie podglądu na żywo, wykonywanie zdjęć, nagrywanie, włączanie/wyłączanie dźwięku, dwukierunkowe przesyłanie sygnału audio lub włączanie/wyłączanie powiększenia cyfrowego.

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

Uwaga:

W przypadku programu Google Chrome w wersji 45 lub wyższej albo programu Mozilla Firefox w wersji 52 lub wyższej bez dodatków typu plug-in instalacja nie jest wymagana. Funkcje **Picture** i **Playback** są jednak ukryte. Aby korzystać z tych funkcji przy użyciu przeglądarki internetowej, należy zainstalować jej najniższą wersję lub zastąpić ją programem Internet Explorer w wersji 8.0 lub wyższej.

Sterowanie PTZ:

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

Ustawienia wstępne/patrole:

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

5.2 Uruchamianie podglądu na żywo

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

Rysunek 5–2 Pasek narzędzi podglądu na żywo

Tabela 5-1 Opis elementów paska narzędzi

Ikona	Opis
▶/■	Uruchamianie/zatrzymywanie podglądu na żywo.
4:3	Proporcje okna 4:3.
16:9	Proporcje okna 16:9.

Ikona	Opis
	Oryginalny rozmiar okna.
	Automatyczne dostosowanie rozmiaru okna.
, , itp.	Podgląd na żywo przy użyciu różnych strumieni wideo. Obsługiwane strumienie wideo są zależne od modelu kamery.
	Kliknij, aby wybrać wtyczkę innej firmy.
	Ręczne wykonanie zdjęcia.
/	Ręczne rozpoczynanie/kończenie nagrywania.
/	Włączanie dźwięku i dostosowanie głośności/wyciszanie dźwięku.
/	Włączanie/wyłączanie mikrofonu.
/	Włączanie/wyłączanie funkcji powiększenia cyfrowego.

Uwaga: Ikony są zależne od modelu kamery.

5.3 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 podglądu na żywo. Ścieżki zapisu wykonanych zdjęć i klipów można ustawić na stronie **Configuration > Local**. Aby skonfigurować zdalne zaplanowane nagrywanie, zobacz *sekcję 6.1*.

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

5.4 Sterowanie PTZ

Cel:

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

Uwaga: Sterowanie PTZ kamerą połączoną z siecią jest dostępne tylko w przypadku kamery obsługującej funkcję PTZ lub wyposażonej w moduł obracania/pochylania. Należy prawidłowo skonfigurować parametry PTZ na stronie ustawień RS485, korzystając z *sekcji 6.2.4* ***Konfigurowanie ustawień RS485***.

5.4.1 Panel sterowania PTZ

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

Użyj przycisków kierunkowych, aby sterować obrotem lub pochyleniem.

Rysunek 5–3 Panel sterowania PTZ

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

Uwagi:

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

Tabela 5-2 Opis panelu sterownia PTZ

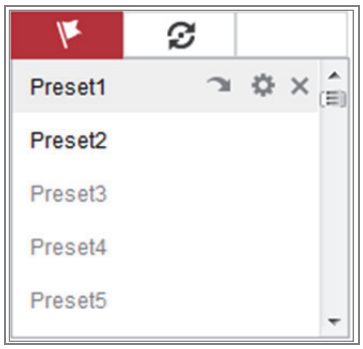
Ikona	Opis
	Powiększanie/pomniejszanie
	Wyostrzanie obiektów w bliży/dali
	Przysłona +/-
4	Regulacja prędkości PTZ
	Włączanie/wyłączanie oświetlenia
	Włączanie/wyłączanie wycieraczki
	Pomocnicza regulacja ostrości
	Inicjowanie obiektywu

	Regulacja prędkości obracania/pochylania
	Rozpoczęcie śledzenia ręcznego
	Uruchomienie funkcji Zoom 3D

5.4.2 Konfigurowanie/wywoływanie ustawienia wstępnego

- **Konfigurowanie ustawienia wstępnego**

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



Rysunek 5–4 Konfigurowanie ustawienia wstępnego

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

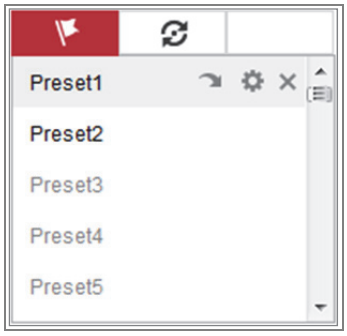
- **Wywoływanie ustawienia wstępnego:**

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

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

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

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



Rysunek 5–5 Wywoływanie ustawienia wstępnego

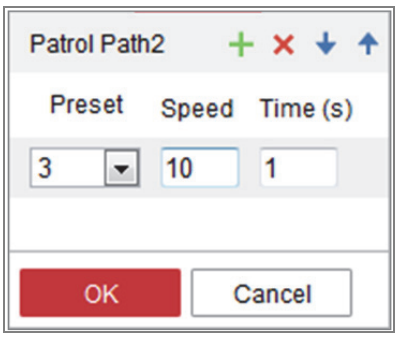
5.4.3 Konfigurowanie/wywoływanie patrolu

Uwaga:

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

Kroki:

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



Rysunek 5–6 Dodawanie ścieżki patrolu

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

Rozdział 6 Konfiguracja kamery sieciowej

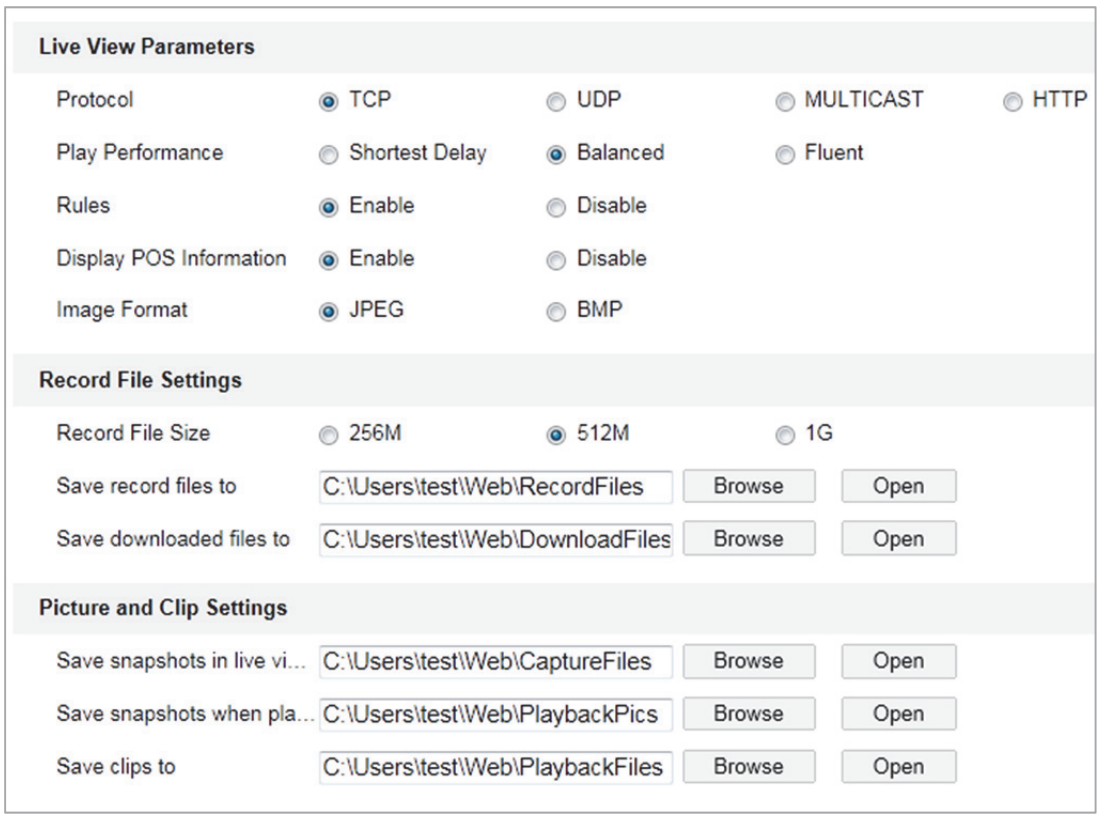
6.1 Konfigurowanie parametrów lokalnych

Cel:

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

Kroki:

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



Rysunek 6–1 Konfiguracja lokalna

2. Skonfiguruj następujące ustawienia:

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

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

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

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

    MULTICAST: Zalecane jest wybranie typu MCAST, jeżeli używana jest funkcja multiemisji (Multicast). Aby uzyskać więcej informacji na temat multiemisji, zobacz *sekcję 7.1.1* ***Konfigurowanie ustawień protokołu TCP/IP.***
  - **Play Performance:** Wybierz ustawienie odtwarzania Shortest Delay, Balanced lub Fluent.
  - **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.
  - **Display POS Information:** Po włączeniu tej funkcji informacje o wykrytym obiekcie są dynamicznie wyświetlane w pobliżu obiektu w podglądzie na żywo.

    Informacje są zależne od funkcji.

    Uwaga:

    Funkcja wyświetlania informacji o punkcie POS jest dostępna tylko w przypadku niektórych modeli kamer.
  - **Image Format:** wybierz format obrazu dla wykonywania zdjęć.
- **Record File Settings:** Ustaw ścieżkę zapisu nagranych plików wideo. To ustawienie dotyczy plików nagranych przy użyciu przeglądarki internetowej.

- **Record File Size:** Wybierz rozmiar pakietu ręcznie nagranych i pobranych plików wideo 256 MB, 512 MB lub 1 GB. Maksymalny rozmiar pliku nagrania będzie zgodny z wybranym ustawieniem.
- **Save record files to:** Ustaw ścieżkę zapisu ręcznie nagranych plików wideo.
- **Save downloaded files to:** ustaw ścieżkę zapisu pobranych plików wideo w trybie odtwarzania.

- **Picture and Clip Settings:** Ustaw ścieżkę zapisu zarejestrowanych zdjęć i przyciętych plików wideo. To ustawienie dotyczy zdjęć wykonanych przy użyciu przeglądarki internetowej.
  - **Save snapshots in live view to:** ustaw ścieżkę zapisu ręcznie wykonanych zdjęć w podglądzie na żywo.
  - **Save snapshots when playback to:** ustaw ścieżkę zapisu wykonanych zdjęć w trybie odtwarzania.
  - **Save clips to:** ustaw ścieżkę zapisu przyciętych plików wideo w trybie odtwarzania.

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

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

6.2 Konfigurowanie ustawień systemowych

Cel:

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

6.2.1 Konfigurowanie podstawowych informacji

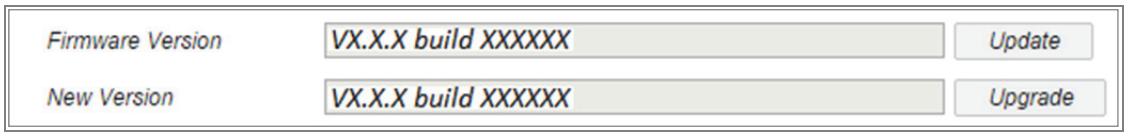
Przejdź do interfejsu informacji o urządzeniu, wybierając opcje: **Configuration > System > System Settings > Basic Information**.

W oknie **Basic Information** można edytować nazwę urządzenia i numer urządzenia.

Wyświetlane są inne informacje o kamerze sieciowej takie jak jej model, numer seryjny, wersja oprogramowania sprzętowego, wersja kodowania, liczba kanałów, liczba dysków twardych, numer wejścia alarmowego i numer wyjścia alarmowego. Informacje wyświetlane w tej części interfejsu nie mogą zostać zmienione. Stanowią one istotny punkt odniesienia podczas przyszłych zabiegów konserwacyjnych lub podczas modyfikacji urządzenia.

Uaktualnienie w trybie online

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



Rysunek 6–2 Uaktualnienie w trybie online

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

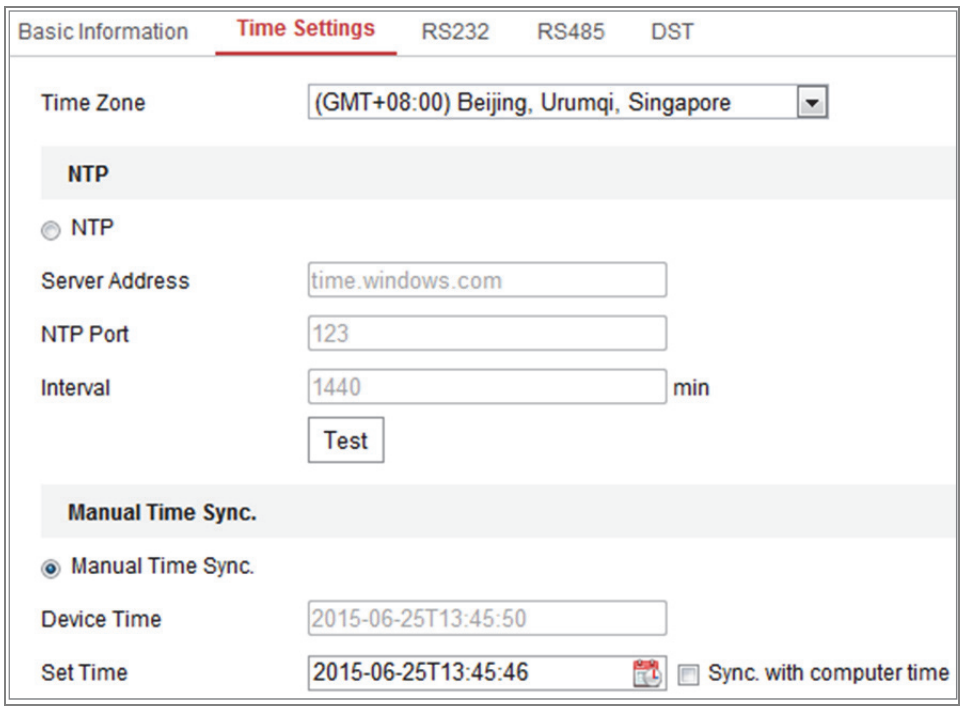
6.2.2 Konfigurowanie ustawień czasu

Cel:

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

Kroki:

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



Rysunek 6–3 Ustawienia czasu

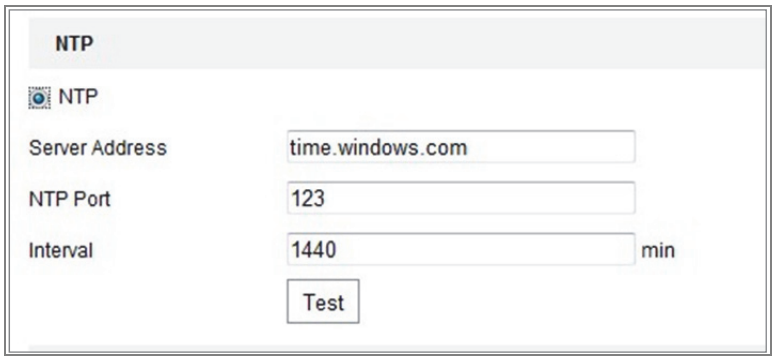
2. Wybierz strefę czasową w swojej lokalizacji z menu rozwijanego.
3. Skonfiguruj ustawienia protokołu NTP.
   (1) Kliknij, aby włączyć funkcję **NTP**.
   (2) Skonfiguruj następujące ustawienia:

   Server Address: adres IP serwera NTP.

   NTP Port: port serwera NTP.

   Interval: interwał czasowy między dwiema operacjami synchronizacji z serwerem NTP.

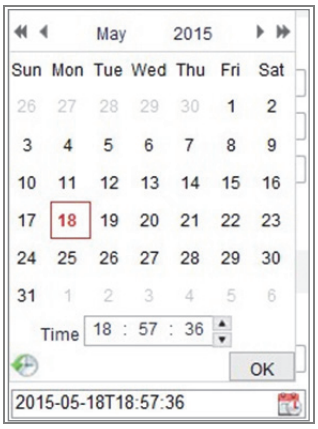
   (3) (Opcjonalnie) Można kliknąć przycisk **Test**, aby przetestować funkcję synchronizacji czasu z serwerem NTP.



Rysunek 6–4 Synchronizacja czasu z serwerem NTP

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

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



Rysunek 6–5 Ręczna synchronizacja czasu

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

6.2.3 Konfigurowanie ustawień RS232

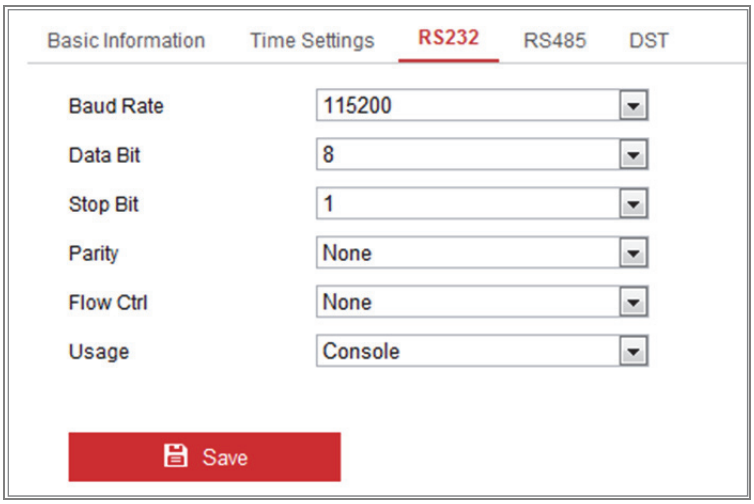
Dostępne są dwie metody korzystania z portu RS232:

- Konfiguracja parametrów: Podłącz komputer do kamery przy użyciu portu szeregowego. Parametry urządzenia można skonfigurować przy użyciu oprogramowania takiego jak HyperTerminal. Parametry portu szeregowego muszą być takie same, jak parametry portu szeregowego kamery.

- Kanał transparentny: Podłącz urządzenie szeregowe bezpośrednio do kamery. Urządzenie szeregowe będzie sterowane zdalnie przez komputer za pośrednictwem sieci.

Kroki:

1. Wyświetl okno Konfiguracja portu RS232: **Configuration > System > System Settings > RS232**.
2. Skonfiguruj szybkość transmisji bitów, bity danych, bit zatrzymania, parzystość, sterowanie przepływem i użycie.



Rysunek 6–6 Ustawienia RS232

Uwaga: Jeżeli konieczne jest podłączenie kamery przy użyciu portu RS232, parametry RS232 powinny być takie same, jak parametry skonfigurowane w tej sekcji.

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

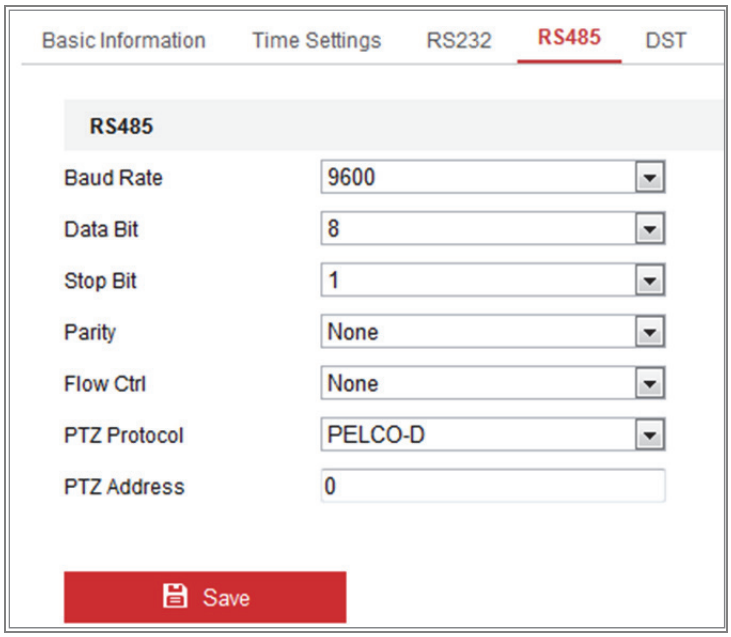
6.2.4 Konfigurowanie ustawień RS485

Cel:

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

Kroki:

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



Rysunek 6–7 Ustawienia RS-485

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

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

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

6.2.5 Konfigurowanie ustawień czasu letniego

Cel:

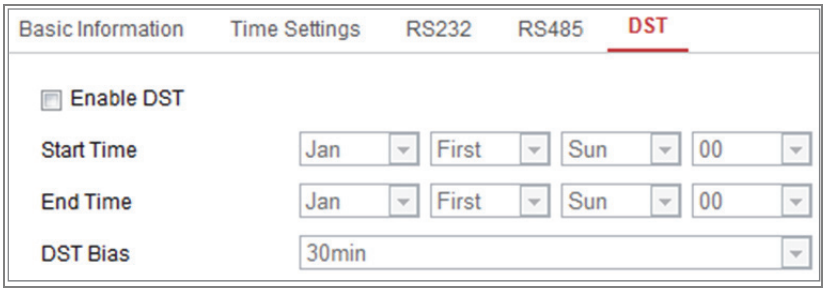
Czas letni (DST, Daylight Saving Time) umożliwia lepsze wykorzystanie naturalnego światła dziennego dzięki przesunięciu zegara o jedną godzinę do przodu w miesiącach letnich i do tyłu w okresie zimowym.

Należy skonfigurować czas letni zgodnie z wymaganiami.

Kroki:

1. Wyświetl okno konfiguracji czasu letniego.

   Configuration > System > System Settings > DST



Rysunek 6–8 Ustawienia czasu letniego (DST)

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

6.2.6 Konfigurowanie urządzeń zewnętrznych

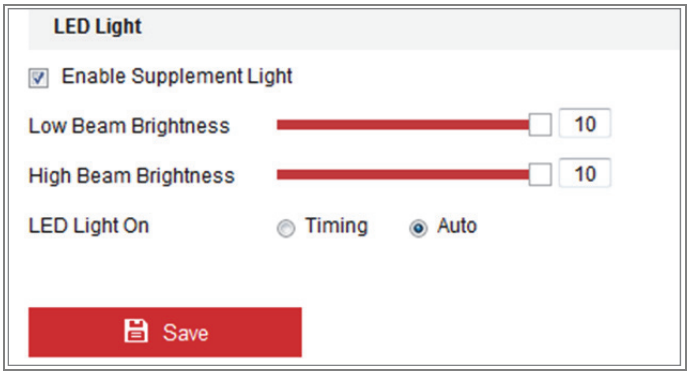
Cel:

Obsługiwanymi urządzeniami zewnętrznymi, takimi jak wycieraczka na obudowie lub oświetlenie LED, można sterować za pośrednictwem przeglądarki internetowej. Urządzenia zewnętrzne są zależne od modelu kamery.

Kroki:

1. Wyświetl okno konfiguracji Urządzenie zewnętrzne.

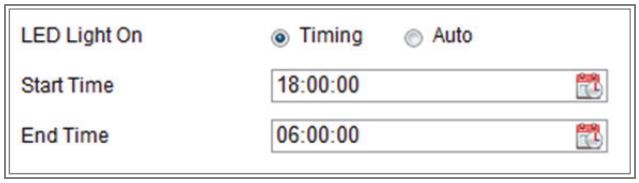
   Configuration > System > System Settings > External Device



Rysunek 6–9 Ustawienia urządzenia zewnętrznego

2. Zaznacz pole wyboru Enable Supplement Light, aby włączyć oświetlenie LED.
3. Przesuń suwak, aby dostosować ustawienia Low Beam Brightness i High Bean Brightness.
4. Wybierz tryb LED light. Dostępne są ustawienia Timing i Auto.

- **Timing:** Oświetlenie LED będzie włączane zgodnie z harmonogramem skonfigurowanym przez użytkownika. Należy skonfigurować ustawienia Czas Rozpoczęcia i Czas Zakończenia.



Rysunek 6–10 Konfigurowanie harmonogramu

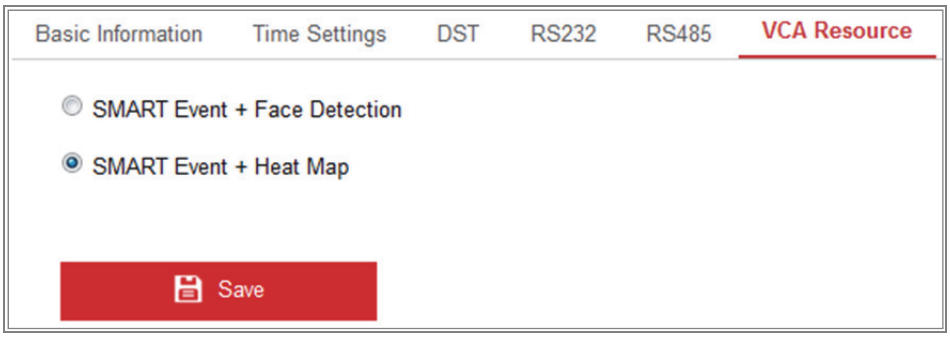
- **Auto:** oświetlenie LED będzie włączane zależnie od oświetlenia w otoczeniu.

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

6.2.7 Konfigurowanie zasobu VCA

Cel:

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



Rysunek 6–11 Konfiguracja zasobu VCA

Kroki:

1. Wyświetl okno konfiguracji Zasób VCA:

   Configuration > System > System Settings > VCA Resource

2. Wybierz żądaną kombinację VCA. Dostępna kombinacja VCA jest zależna od modelu kamery.
3. Kliknij przycisk „**Save**“, aby zapisać ustawienia. Ponowne uruchomienie jest wymagane po skonfigurowaniu funkcji Zasób VCA.

Uwagi:

- Kombinacje VCA wykluczają się wzajemnie. Aktywacja jednej z kombinacji powoduje ukrycie pozostałych kombinacji.
- Ta funkcja nie jest obsługiwana przez niektóre modele kamer.

6.2.8 Licencja na oprogramowanie open source

Można sprawdzić informacje dotyczące oprogramowania typu Open Source związanego z kamerą internetową, jeżeli jest to wymagane. Przejdź do **Configuration > System Settings > About**.

6.3 Konserwacja

6.3.1 Uaktualnienie i konserwacja

Cel:

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

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

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

  Uwagi:

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

- W przypadku kamer obsługujących łączność Wi-Fi, telefoniczną lub WLAN, akcja **Restore** nie powoduje przywrócenia domyślnych powiązanych ustawień wspomnianych funkcji.

- **Information Export**

  Device Parameters: kliknij, aby wyeksportować bieżący plik konfiguracji kamery. W przypadku tej operacji wymagane jest podanie hasła administratora.

  Dla eksportowanego pliku też można utworzyć hasło szyfrowania. Hasło szyfrowania jest wymagane w przypadku importowania tego pliku do innych kamer.

  Diagnose Information: kliknij, aby pobrać dziennik oraz informacje o systemie.

- **Import Config. File**

  Plik konfiguracji jest używany do zbiorczego konfigurowania kamer.

  Kroki:

  1. Kliknij przycisk **Browse**, aby wybrać zapisany plik konfiguracji.
  2. Kliknij przycisk **Import** i wprowadź hasło szyfrowania, aby rozpocząć importowanie pliku konfiguracji.

  Uwaga: Po zaimportowaniu pliku konfiguracyjnego należy ponownie uruchomić kamerę.

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

  Kroki:

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

     Oprogramowania: zlokalizuj dokładnie ścieżkę pliku uaktualnienia.

     Katalog Oprogramowania: wymagany jest tylko katalog, w którym znajduje się plik uaktualnienia.
  2. Kliknij przycisk **Browse**, aby wybrać lokalny plik uaktualnienia, a następnie kliknij przycisk **Upgrade** w celu rozpoczęcia zdalnego uaktualnienia.

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

6.3.2 Dziennik

Cel:

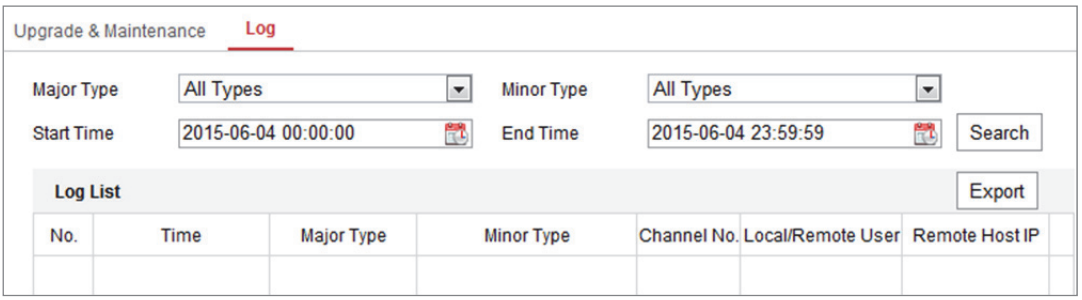
Operacje, alarmy, wyjątki i informacje dotyczące kamery można zapisywać w plikach rejestru. W razie potrzeby pliki rejestru można eksportować.

Zanim rozpoczniesz:

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

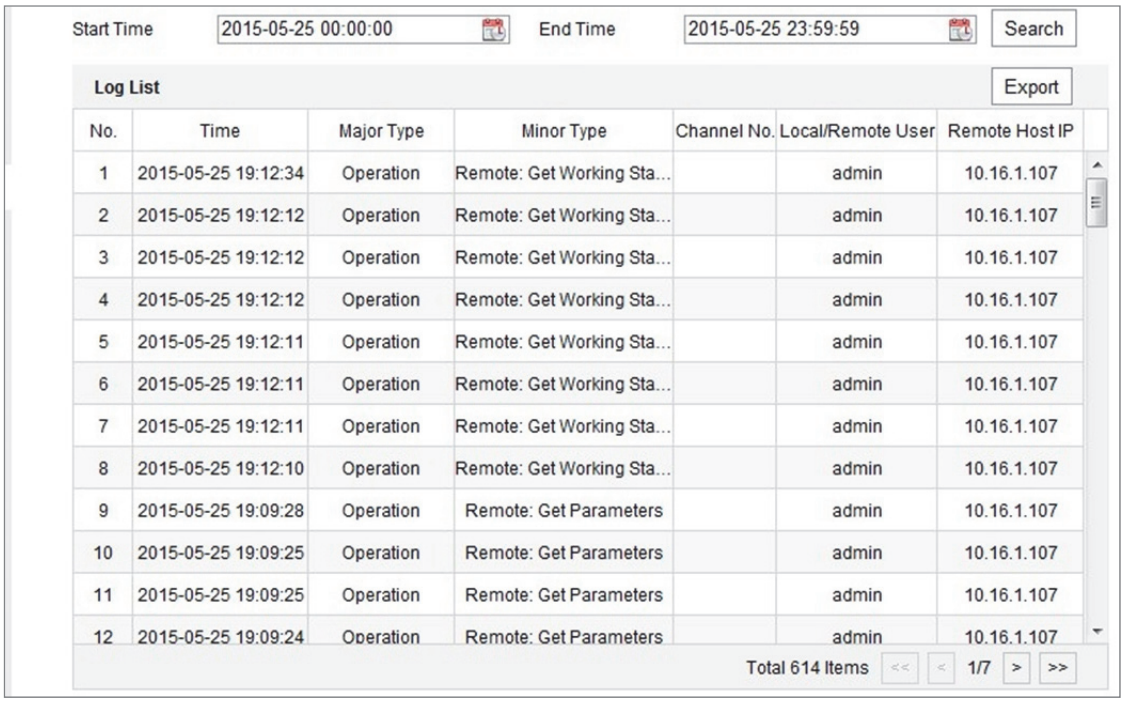
Kroki:

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



Rysunek 6–12 Okno wyszukiwania w dzienniku

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



Rysunek 6–13 Wyszukiwanie w dzienniku

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

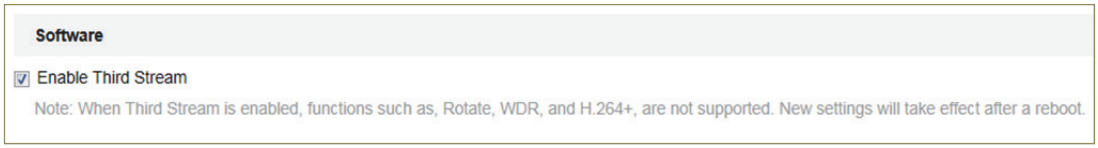
6.3.3 Usługa systemowa

Cel:

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

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

Third Stream: W przypadku niektórych modeli trzeci strumień jest domyślnie wyłączony. Zaznacz pole wyboru **Enable Third Stream**, aby włączyć tę funkcję.



Rysunek 6–14 Włączanie trzeciego strumienia

6.4 Ustawienia zabezpieczeń

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

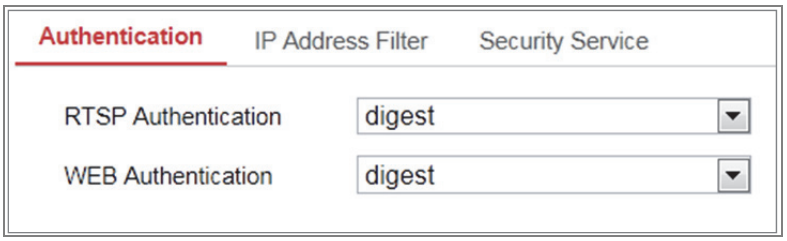
6.4.1 Uwierzytelniania

Cel:

Funkcja ta służy do ochrony danych strumienia podglądu na żywo.

Kroki:

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



Rysunek 6–15 Uwierzytelnianie

2. Ustaw metodę uwierzytelniania RTSP i WEB.

   Przestroga:

   Digest jest zalecaną metodą uwierzytelniania, zapewniającą lepszą ochronę danych. Należy pamiętać o ryzyku związanym z wybraniem metody uwierzytelniania Basic.

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

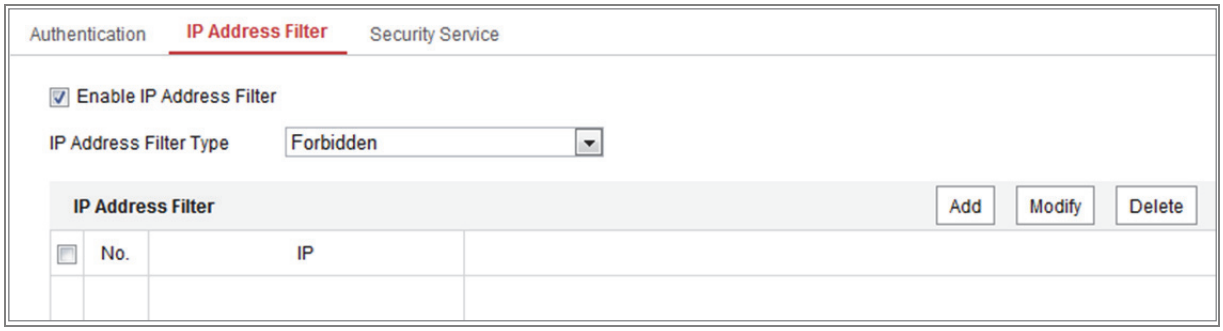
6.4.2 Filtr adresów IP

Cel:

Ta funkcja umożliwia kontrolę dostępu.

Kroki:

1. Wyświetl okno Filtr adresów IP: **Configuration > System > Security > IP Address Filter**



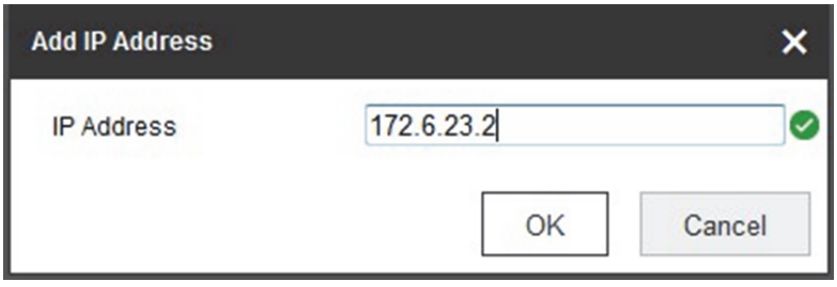
Rysunek 6–16 Filtr adresów IP

2. Zaznacz pole wyboru „**Enable IP Address Filter**“.
3. Wybierz filtr adresów IP z listy rozwijanej IP Address Filter. Dostępne są ustawienia **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 6–17 Dodawanie adresu IP

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

   - Modyfikowanie adresu IP

Kroki:

(1) Kliknij lewym przyciskiem myszy adres IP na liście filtrowania, a następnie kliknij przycisk „**Modify**“.

(2) Zmień adres IP znajdujący się w polu tekstowym.

Rysunek 6–18 Modyfikowanie adresu IP

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

- Usuń adres IP lub adresy IP.

  Wybierz adresy IP i kliknij przycisk **Delete**.

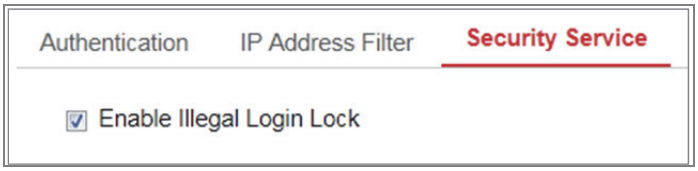
5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

6.4.3 Usługa zabezpieczeń

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

Kroki:

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



Rysunek 6–19 Usługa zabezpieczeń

2. Zaznacz pole wyboru **Enable Illegal Login Lock**.

   Illegal Login Lock: używane do ograniczania liczby kolejnych prób zalogowania użytkownika zakończonych niepowodzeniem. Próba zalogowania z adresu IP jest odrzucana, jeżeli administrator wprowadzi nieprawidłową nazwę użytkownika/hasło siedem razy (pięć razy w przypadku gościa/operatora).

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

6.5 Zarządzanie użytkownikami

6.5.1 Zarządzanie użytkownikami

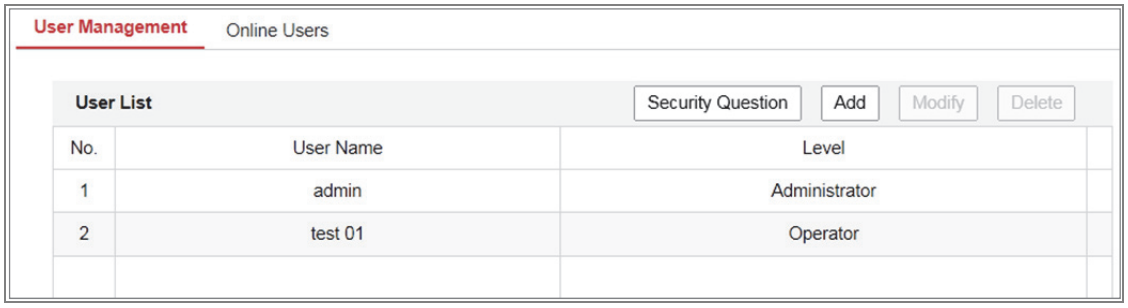
- **Jako administrator**

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

Przejdź do interfejsu zarządzania użytkownikami, wybierając opcje: **Configuration > System > User Management**

Uwaga:

Hasło administratora, jeżeli jest wymagane do dodawania i modyfikowania konta użytkownika.



Rysunek 6–20 Zarządzanie użytkownikami

- **Dodawanie użytkownika**

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

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

Kroki:

1. Kliknij przycisk **Add**, aby dodać użytkownika.

2. Wprowadź hasło administratora w polu **Admin Password** i nazwę użytkownika w polu **User Name**, wybierz poziom z listy **Level** i wprowadź hasło w polu **Password**.

   Uwagi:

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

Zalecane jest stosowanie silnego hasła — *Zdecydowanie zalecamy utworzenie silnego własnego hasła (minimum 8 znaków z uwzględnieniem przynajmniej trzech z następujących kategorii: wielkich liter, 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.*

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

- **Modyfikowanie użytkownika**

Kroki:

1. Kliknij lewym przyciskiem myszy, aby wybrać użytkownika z listy, i kliknij przycisk **Modify**.
2. Zmień ustawienia **User Name, Level** i **Password**.

Zalecane jest stosowanie silnego hasła —ZDECYDOWANIE ZALECAMY UTWORZENIE SILNEGO WŁASNEGO HASŁA (MINIMUM 8 ZNAKÓW Z UWZGLĘDNIENIEM PRZYNAJMNIEJ TRZECH Z NASTĘPUJĄCYCH KATEGORII: WIELKICH LITER, 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.

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

- **Usuwanie użytkownika**

Kroki:

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

- **Jako operator lub zwykły użytkownik**

  Operator lub zwykły użytkownik może modyfikować hasło. Aby wykonać tę akcję, należy podać stare hasło.

6.5.2 Pytanie zabezpieczające

Cel:

Pytanie zabezpieczające umożliwia resetowanie hasła administratora, jeżeli administrator nie pamięta hasła.

Ustawianie pytania zabezpieczającego:

Pytania zabezpieczające można ustawić podczas aktywacji kamery. Można też ustawić tę funkcję w oknie zarządzania użytkownikami.

Ustawienie pytania zabezpieczającego jest czyszczone podczas przywracania kamery (bez ustawienia domyślnego).

Kroki:

1. Wyświetl okno ustawień:

   Configuration > System > User Management > User Management
2. Kliknij przycisk **Security Question**.
3. Wprowadź poprawne hasło administratora.
4. Wybierz pytania i wprowadź odpowiedzi.
5. Kliknij przycisk **OK**, aby zapisać ustawienia.

Resetowanie hasła administratora:

Zanim rozpoczniesz:

Komputer używany do resetowania hasła i kamera powinny należeć do tej samego segmentu adresów IP tej samej sieci LAN.

Kroki:

1. Wyświetl okno logowania przy użyciu przeglądarki internetowej.
2. Kliknij przycisk **Forget Password**.
3. Odpowiedz na pytanie zabezpieczające.
4. Utwórz nowe hasło.

Uwaga:

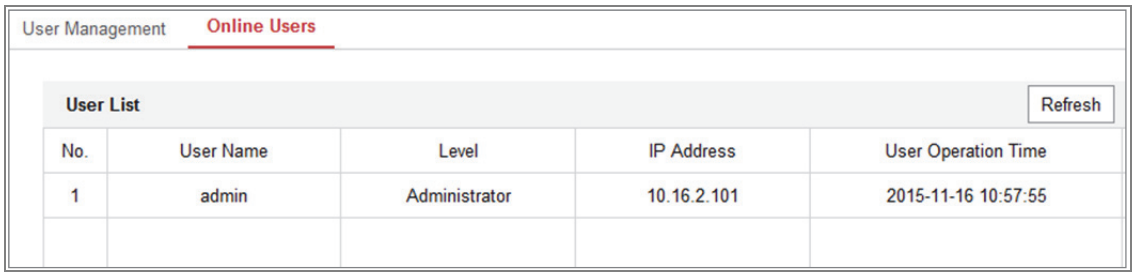
Adres IP użytkownika jest blokowany na 30 minut po siedmiu kolejnych próbach udzielenia odpowiedzi na pytania zabezpieczające, zakończonych niepowodzeniem.

6.5.3 Użytkownicy połączeni z urządzeniem

Cel:

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

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



Rysunek 6–21 Widok użytkowników w trybie online

Rozdział 7 Ustawienia sieciowe

Cel:

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

7.1 Konfigurowanie ustawień podstawowych

Cel:

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

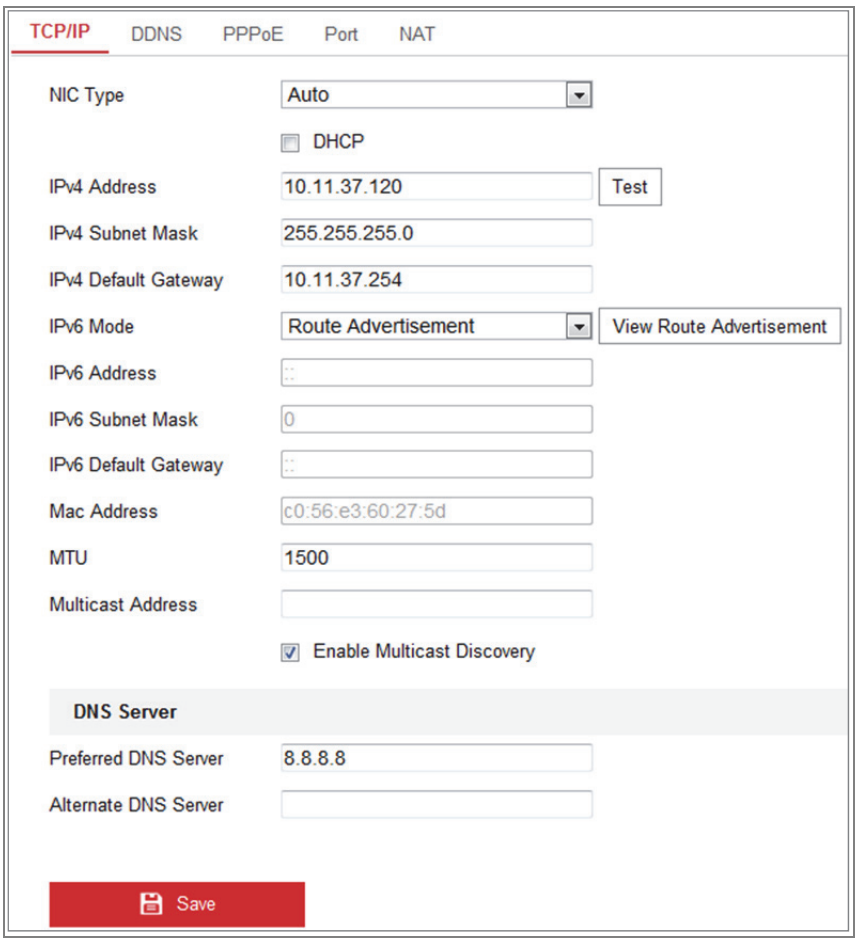
7.1.1 Konfigurowanie ustawień protokołu TCP/IP

Cel:

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

Kroki:

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



Rysunek 7–1 Ustawienia protokołu TCP/IP

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

Uwagi:

- Prawidłowy zakres wartości MTU to 1280–1500.
- W trybie multiemisji szybkoobrotowa kamera kopułkowa prześle strumień na adres grupy multiemisji, dzięki czemu wielu klientów może jednocześnie uzyskać dostęp do strumienia, przesyłając żądanie uzyskania kopii na adres

grupy multiemisji. Przed skorzystaniem z tej funkcji należy włączyć funkcję Multiemisja routera.

- Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

7.1.2 Konfigurowanie ustawień usługi DDNS

Cel:

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

Zanim rozpoczniesz:

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

Kroki:

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

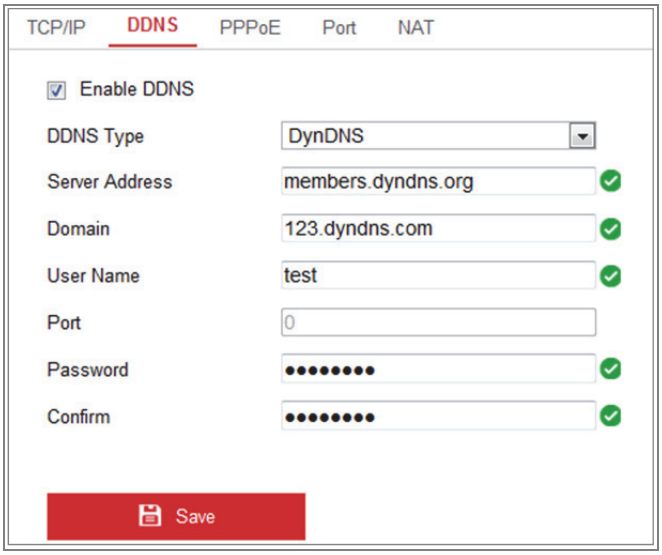
   Kroki:

   (1) Wprowadź adres serwera („**Server Address**“) usługi DynDNS (e.g. members.dyndns.org).

   (2) W polu tekstowym „**Domain**“ wprowadź nazwę domeny otrzymaną ze strony DynDNS.

   (3) Wprowadź nazwę użytkownika („**User Name**“) i hasło („**Password**“) zarejestrowane na stronie DynDNS.

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

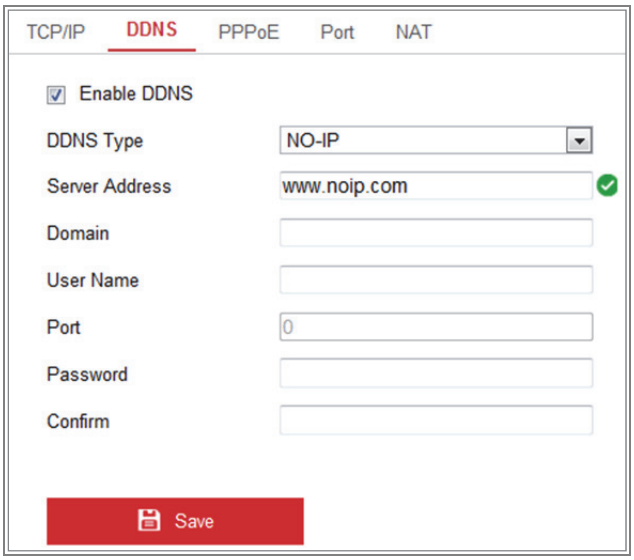


Rysunek 7–2 Ustawienia DynDNS

- NO-IP:

Kroki:

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



Rysunek 7–3 Ustawienia NO-IP DNS

(2) W polu Server Address wprowadź adres serwera www.noip.com

(3) Wprowadź zarejestrowaną nazwę w polu Nazwa domeny.

(4) Wprowadź informacje w polach Nazwa użytkownika i Hasło.

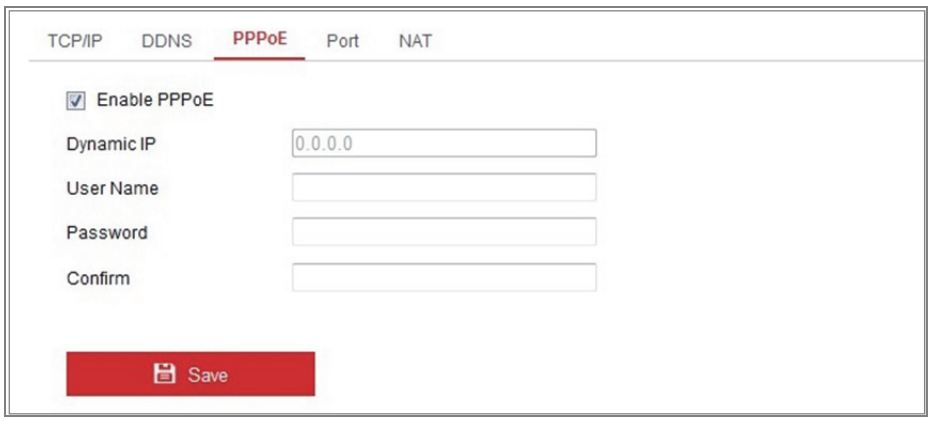
(5) Kliknij przycisk **Save**, aby wyświetlić kamerę z nazwą domeny.

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

7.1.3 Konfigurowanie ustawień protokołu PPPoE

Kroki:

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



Rysunek 7–4 Ustawienia funkcji PPPoE

2. Zaznacz pole wyboru „**Enable PPPoE**“, aby włączyć tę funkcję.
3. Wpisz nazwę użytkownika w polu **User Name** i hasło w polu **Password**, a następnie potwierdź hasło przy użyciu pola **Confirm**, aby uzyskać dostęp do funkcji PPPoE.

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

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

4. Kliknij przycisk **Save**, aby zapisać ustawienia i zamknąć okno.

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

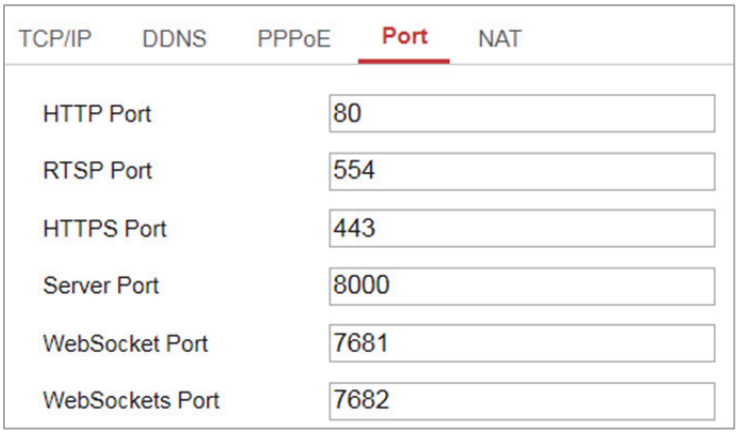
7.1.4 Konfigurowanie ustawień portów

Cel:

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

Kroki:

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



Rysunek 7–5 Ustawienia portów

2. Ustaw porty kamery.

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

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

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

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

   Uwaga:

   Gdy dostęp do kamery jest uzyskiwany przy użyciu oprogramowania klienckiego, a port serwera został zmieniony, należy wprowadzić poprawny numer portu serwera w oknie logowania, aby uzyskać dostęp do kamery.

WebSocket Port: Domyślny numer portu to 7681. Numer portu można zmienić na dowolną wartość z zakresu 1–65 535.

WebSockets Port: Domyślny numer portu serwera to 7682. Numer portu można zmienić na dowolną wartość z zakresu 1–65 535.

Uwaga:

W przypadku podglądu na żywo bez dodatków typu plug-in używane są protokoły WebSocket i WebSockets. Aby uzyskać więcej informacji, zobacz *7.2.11*.

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

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

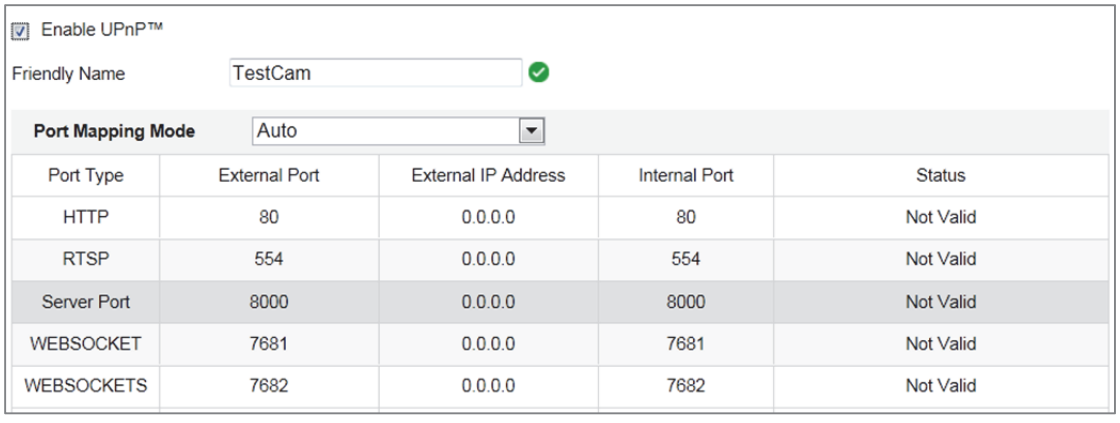
7.1.5 Konfigurowanie ustawień translacji adresów sieciowych (NAT)

Cel:

W oknie Translacja NAT można skonfigurować parametry funkcji UPnP™.

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

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



Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
WEBSOCKET	7681	0.0.0.0	7681	Not Valid
WEBSOCKETS	7682	0.0.0.0	7682	Not Valid

Rysunek 7–6 Ustawienia funkcji UPnP

Kroki:

1. Wyświetl ustawienia translacji NAT. **Configuration > Network > Basic Settings > NAT.**
2. Zaznacz pole wyboru „Enable UPnP™“ (Włącz UPnP™), aby włączyć funkcję UPnP.

   Uwaga:

   Kamera jest aktywna tylko po włączeniu funkcji UPnP™.
3. Wybierz przyjazną nazwę kamery lub użyj nazwy domyślnej.
4. Wybierz tryb mapowania portów. Dostępne są ustawienia Manual i Auto.

   Uwaga:

   Jeżeli zostanie wybrane ustawienie Auto, należy włączyć funkcję UPnP™ w routerze.

   Jeżeli zostanie wybrane ustawienie Manual, można dostosować wartość portu zewnętrznego i ręcznie skonfigurować ustawienia mapowania portów w routerze.
5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

7.2 Konfigurowanie ustawień zaawansowanych

Cel:

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

7.2.1 Konfigurowanie ustawień protokołu SNMP

Cel:

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

Zanim rozpoczniesz:

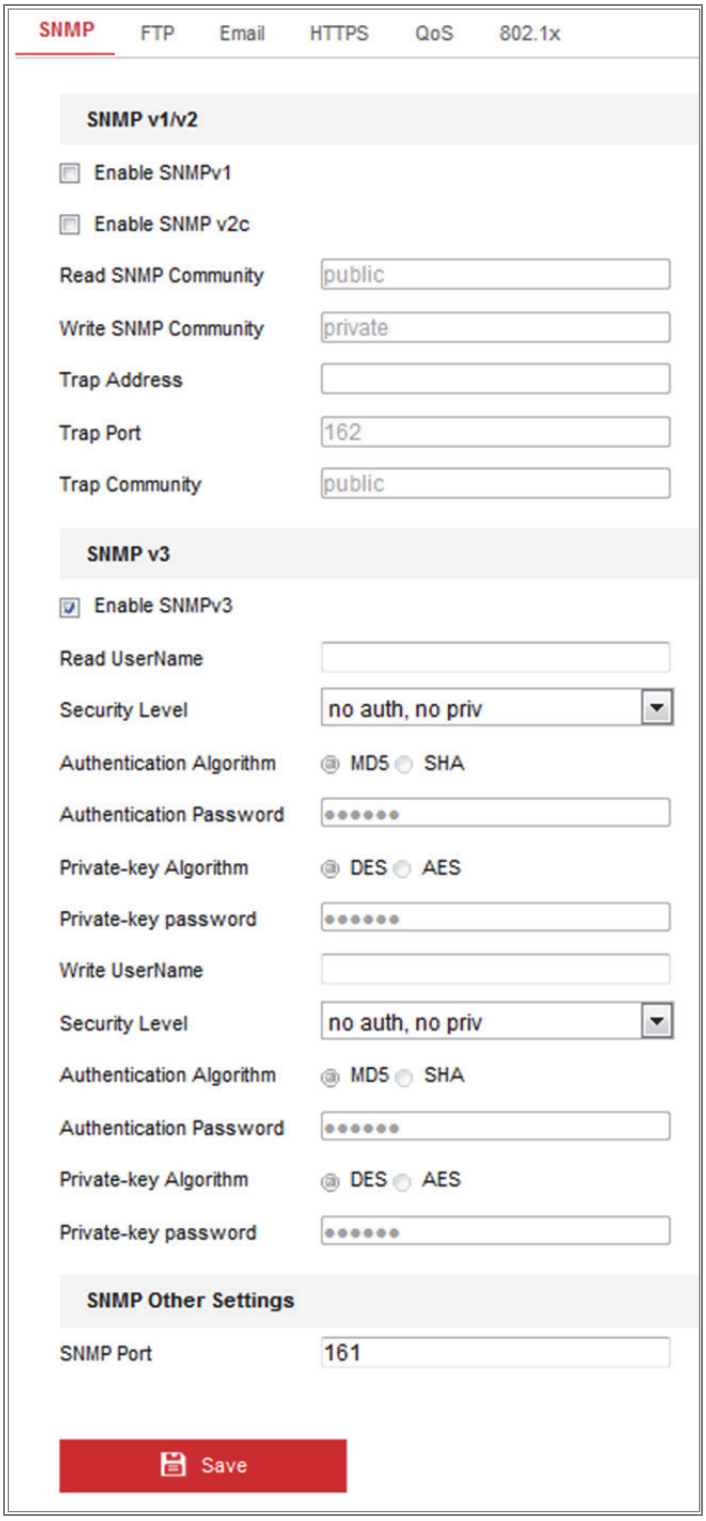
Przed skonfigurowaniem protokołu SNMP należy pobrać oprogramowanie SNMP i uzyskać informacje dotyczące kamery za pośrednictwem portu SNMP. Skonfigurowanie ustawienia Adres pułapki umożliwia kamerze wysłanie wiadomości dotyczących zdarzeń i wyjątków alarmowych do centrum monitoringu.

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

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

Kroki:

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



Rysunek 7–7 Ustawienia funkcji SNMP

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

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

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

Uwagi:

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

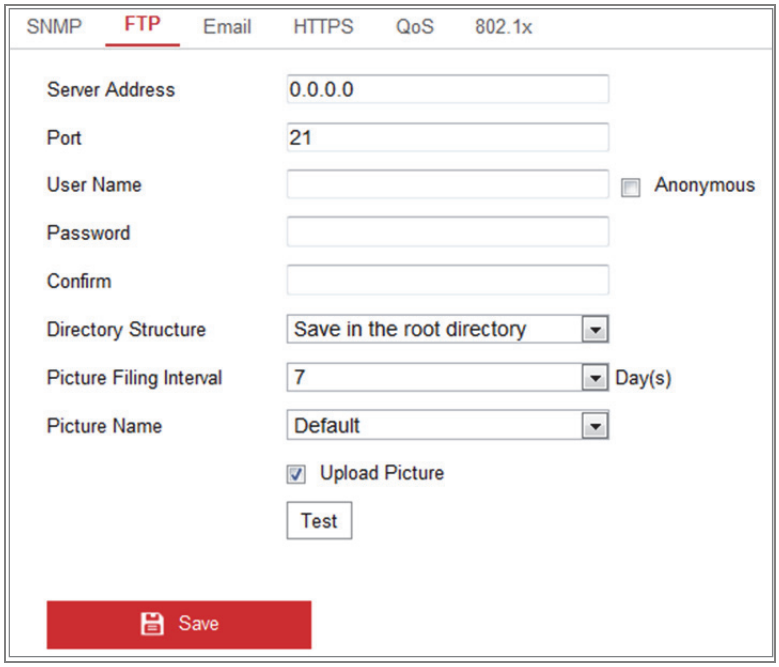
7.2.2 Konfigurowanie ustawień serwera FTP

Cel:

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

Kroki:

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



Rysunek 7–8 Ustawienia serwera FTP

2. Wprowadź adres i port serwera FTP.

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

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

4. Skonfiguruj strukturę katalogów i interwał zapisywania zdjęć.

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

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

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

adres IP_numer kanału_godzina wykonania zdjęcia_typ zdarzenia.jpg

(np. *10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg*).

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

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

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

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

   Uwaga: Dostęp anonimowy musi być obsługiwany przez serwer FTP.

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

7.2.3 Konfigurowanie ustawień wysyłania wiadomości e-mail

Cel:

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

Zanim rozpoczniesz:

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

Kroki:

1. Wyświetl okno Ustawienia protokołu TCP/IP (**Configuration > Network > Basic Settings > TCP/IP**), aby ustawić adres IPv4, maskę podsieci IPv4, bramę domyślną IPv4 i preferowany serwer DNS.

   Uwaga: Aby uzyskać więcej informacji, zobacz *sekcję 7.1.1* ***Konfigurowanie ustawień protokołu TCP/IP.***

2. Przejdź do interfejsu ustawień wysyłania wiadomości e-mail, wybierając opcje: **Configuration > Network > Advanced Settings > Email**.

3. Skonfiguruj następujące ustawienia:

   Sender: Imię nadawcy wiadomości e-mail.

   Sender’s Address: Adres e-mail nadawcy wiadomości.

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

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

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

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

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

Interval: odstęp czasowy między akcjami wysyłania załączonych zdjęć.

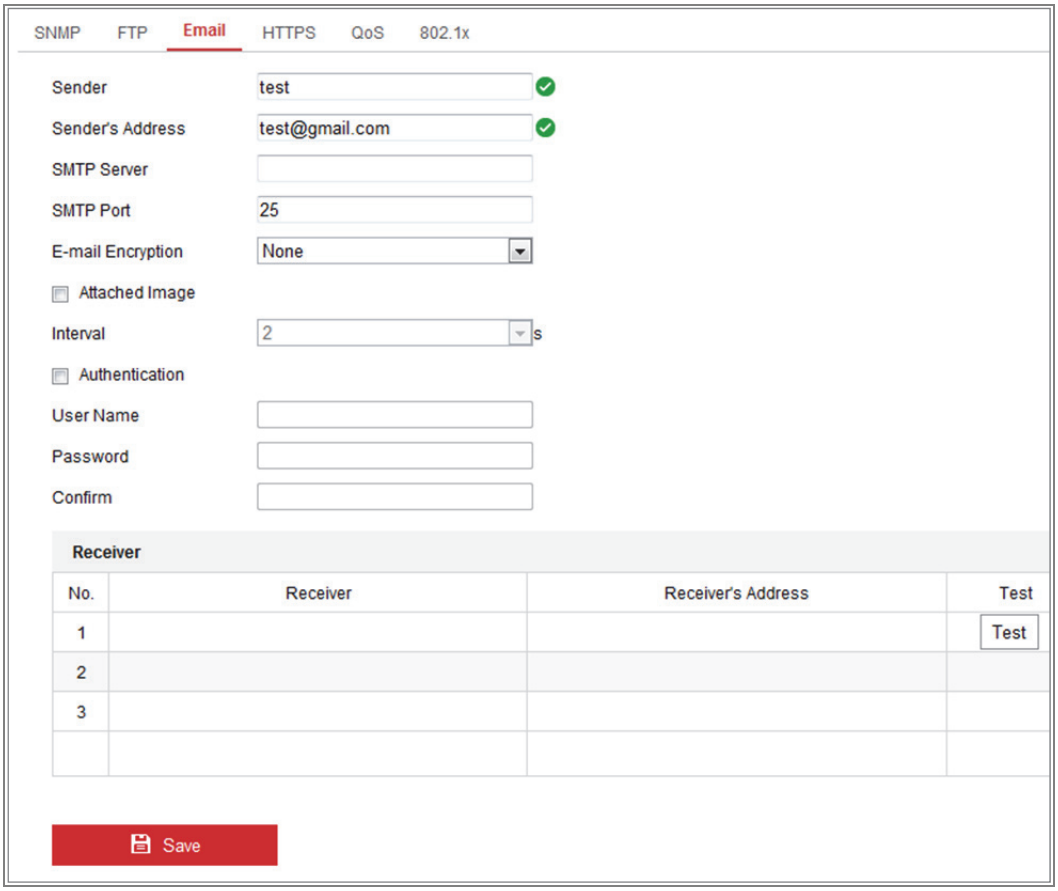
Authentication (opcjonalnie): jeżeli serwer e-mail wymaga uwierzytelnienia, zaznacz to pole wyboru, aby używać uwierzytelniania do logowania do tego serwera, i wprowadź nazwę użytkownika i hasło używane do logowania.

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

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

Receiver: Imię użytkownika, do którego przesyłane jest powiadomienie.

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



Rysunek 7–9 Ustawienia poczty e-mail

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

7.2.4 Dostęp do platformy

Cel:

Funkcja ta służy do zarządzania urządzeniami za pośrednictwem platformy.

Kroki:

1. Wyświetl ustawienia **Dostęp do platformy**: **Configuration > Network > Advanced Settings > Platform Access**

2. Zaznacz pole wyboru Enable, aby włączyć funkcję dostępu do urządzenia przy użyciu platformy.
3. Wybierz ustawienie Platform Access Mode.

   Uwaga: Aplikacja Hik-Connect jest przeznaczona dla urządzeń przenośnych. Korzystając z tej aplikacji, można wyświetlać widok na żywo obrazu z kamery, odbierać powiadomienia dotyczące alarmów itd.

Jeżeli ustawienie Platform Access Mode zostanie wybrane dla opcji Hik-Connect,

1) Kliknij i przeczytaj „Terms of Service” i „Privacy Policy” w oknie podręcznym.
2) Utwórz kod weryfikacyjny lub zmień ten kod dla kamery.

   Uwaga:

   - Kod weryfikacyjny jest wymagany podczas dodawania kamery do aplikacji Hik-Connect.
   - Aby uzyskać więcej informacji na temat aplikacji Hik-Connect, skorzystaj z Podręcznika użytkownika aplikacji Hik-Connect Mobile Client.

4. Można użyć domyślnego adresu serwera. Można też zaznaczyć pole wyboru Niestandardowy po prawej stronie i wprowadzić żądany adres serwera.
5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

7.2.5 Bezprzewodowe połączenie telefoniczne

Cel:

Strumień danych audio, wideo i zdjęć można przesyłać przy użyciu bezprzewodowej sieci 3G/4G.

Uwagi:

- Bezprzewodowe połączenia telefoniczne nie są obsługiwane przez niektóre modele kamer.
- Kamera obsługująca bezprzewodowe połączenia telefoniczne nie obsługuje protokołu PPPoE.

Kroki:

1. Kliknij kartę **Wireless Dial**, aby wyświetlić okno konfiguracji Bezprzewodowe połączenia telefoniczne: **Configuration > Network > Advanced Settings > Wireless Dial**
2. Zaznacz pole wyboru, aby włączyć ustawienia bezprzewodowych połączeń telefonicznych.
3. Skonfiguruj parametry połączeń telefonicznych.
    1) Wybierz tryb połączeń telefonicznych z listy rozwijanej. Dostępne są ustawienia Auto i Manual. Jeżeli wybrano ustawienie Auto, można skonfigurować harmonogram zabezpieczenia dla połączeń telefonicznych. Jeżeli wybrano ustawienie Manual, można skonfigurować czas przełączania do trybu offline i parametry ręcznego ustanawiania połączeń telefonicznych.
    2) Skonfiguruj numer dostępowy, nazwę użytkownika, hasło, punkt dostępu (APN), MTU i protokół weryfikacji. Można też pozostawić pola tych parametrów puste, aby po skonfigurowaniu innych parametrów urządzenie przyjęło domyślne ustawienia ustanawiania połączeń telefonicznych.
    3) Wybierz tryb sieci z listy rozwijanej. Dostępne są ustawienia Auto, 3G i 4G. Jeżeli zostanie wybrane ustawienie Auto, priorytet wyboru sieci jest następujący: 4G > 3G > Sieć przewodowa.

4) Wprowadź czas przełączenia do trybu offline, jeżeli wybrano tryb Manual połączeń telefonicznych.
5) Wprowadź numer telefonu komórkowego w polu Numer UIM.
6) Kliknij przycisk Edit, aby skonfigurować harmonogram zabezpieczenia, jeżeli wybrano tryb Auto połączeń telefonicznych.
7) Kliknij przycisk „Save“, aby zapisać ustawienia.

4. Wyświetl stan łączności telefonicznej.
   1) Kliknij przycisk Refresh, aby wyświetlić informacje dotyczące stanu łączności telefonicznej, takie jak tryb czasu rzeczywistego, numer UIM lub siła sygnału.
   2) Jeżeli wybrano tryb Manual połączeń telefonicznych, można też ręcznie ustanawiać/rozłączać połączenie z siecią bezprzewodową.
5. Skonfiguruj listę numerów dozwolonych. Telefon komórkowy, którego numer jest uwzględniony na liście numerów dozwolonych, może odebrać wiadomość alarmową od urządzenia i ponownie uruchomić urządzenie przy użyciu usługi SMS.
   1) Zaznacz pole wyboru Enable SMS Alarm.
   2) Wybierz pozycję na liście numerów dozwolonych i kliknij przycisk Edit.
   3) Wprowadź numer telefonu komórkowego do umieszczenia na liście numerów dozwolonych, zaznacz pole wyboru Reboot via SMS, wybierz alarm do przesłania w wiadomości SMS i kliknij przycisk OK.

      Uwaga: Aby ponownie uruchomić urządzenie przy użyciu usługi SMS, należy wysłać do niego wiadomość „reboot”. Urządzenie prześle wiadomość „reboot success” po pomyślnym ponownym uruchomieniu.
   4) (Opcjonalnie) Można kliknąć przycisk Send Test SMS, aby wysłać wiadomość testową do telefonu komórkowego.
   5) Kliknij przycisk „Save“, aby zapisać ustawienia.

7.2.6 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.

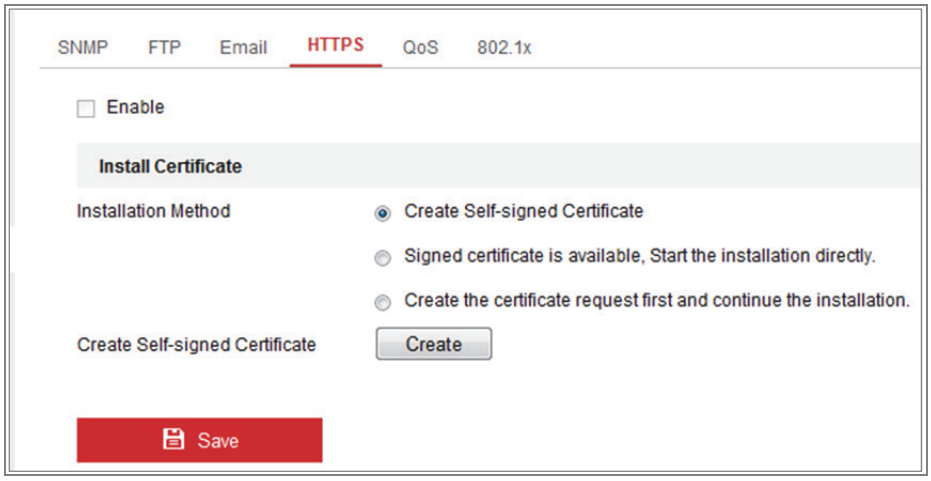
Jeżeli na przykład zostanie ustawiony numer portu 443 i adres IP 192.168.1.64, można uzyskać dostęp do urządzenia, wprowadzając adres https://192.168.1.64:443 w przeglądarce internetowej.

Uwaga:

- Jeżeli protokół HTTPS jest używany do uzyskiwania dostępu do kamery, należy włączyć opcję **WebSockets**, aby wyświetlać podgląd na żywo. Przejdź do **Configuration > Network > Advanced Settings > Network Service**.
- W przypadku niektórych modeli kamer funkcja HTTPS jest domyślnie włączona. Kamera automatycznie tworzy niepodpisany certyfikat. Gdy dostęp do kamery jest uzyskiwany przy użyciu protokołu HTTPS, przeglądarka internetowa powiadamia o problemie z certyfikatem. Należy zainstalować podpisany certyfikat w kamerze, aby anulować powiadamianie.

Kroki:

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



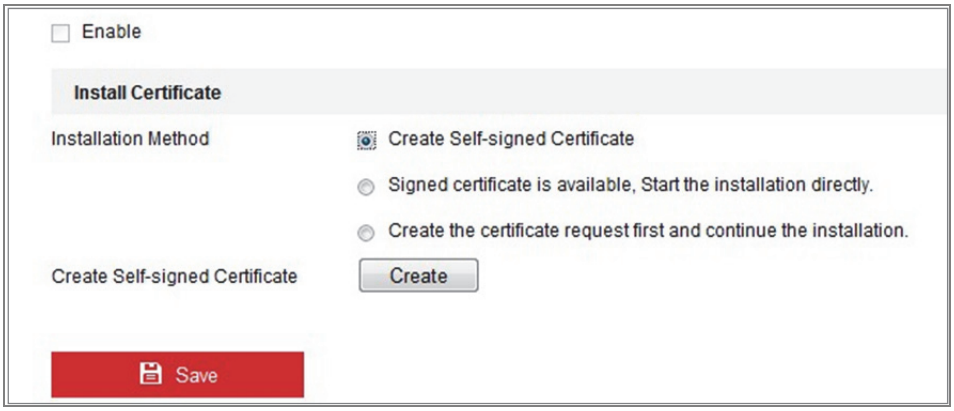
Rysunek 7–10 Konfiguracja funkcji HTTPS

3. Utwórz certyfikat z podpisem własnym lub autoryzowany certyfikat.

- Tworzenie certyfikatu z podpisem własnym

(1) Wybierz opcję **Create Self-signed Certificate** w sekcji Metoda instalacji.

(2) Kliknij przycisk **Create**, aby wyświetlić okno tworzenia.



Rysunek 7–11 Tworzenie certyfikatu z podpisem własnym

(3) Wprowadź nazwę kraju, nazwę/adres IP hosta, datę ważności i inne kraje.

(4) Kliknij przycisk **OK**, aby zapisać ustawienia.

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

- Tworzenie autoryzowanego certyfikatu

(1) Wybierz opcję **Create the certificate request first and continue the installation** w sekcji Metoda instalacji.

(2) Kliknij przycisk **Create**, aby utworzyć żądanie certyfikatu. Wpisz wymagane informacje w oknie podręcznym.

(3) Pobierz żądanie certyfikatu i prześlij je do zaufanego urzędu certyfikacji w celu uzyskania sygnatury.

(4) Po otrzymaniu prawidłowego sygnowanego certyfikatu zaimportuj go do urządzenia.

4. Po pomyślnym utworzeniu i zainstalowaniu certyfikatu dostępne będą informacje dotyczące certyfikatu.

Rysunek 7–12 Zainstalowany certyfikat

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

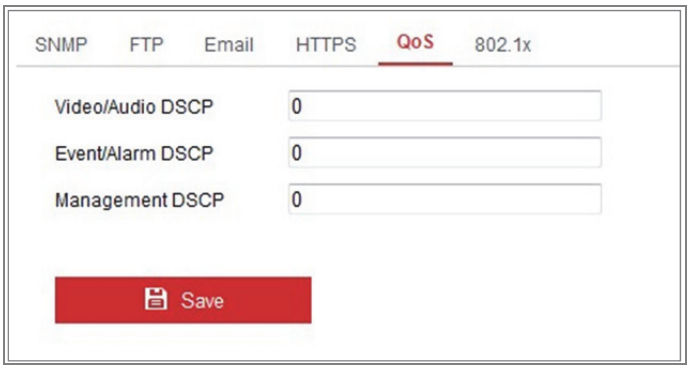
7.2.7 Konfigurowanie ustawień jakości usługi (QoS)

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 > Network > Advanced Settings > QoS**



Rysunek 7–13 Ustawienia jakości usługi (QoS)

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

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

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

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

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

7.2.8 Konfigurowanie ustawień standardu IEEE 802.1X

Cel:

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

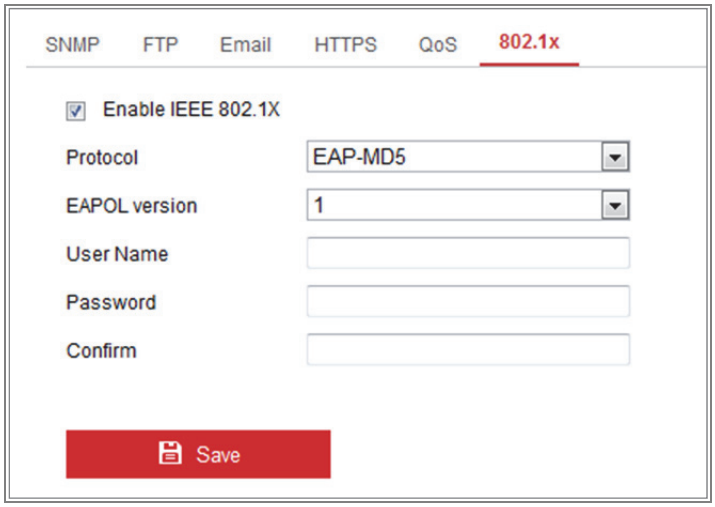
Zanim rozpoczniesz:

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

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

Kroki:

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



Rysunek 7–14 Ustawienia funkcji 802.1X

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

   Uwaga: Ustawienie **EAPOL version** musi być identyczne z odpowiednim ustawieniem routera lub przełącznika.
4. Wprowadź nazwę użytkownika i hasło, aby uzyskać dostęp do serwera.
5. Kliknij przycisk **Save**, aby ukończyć konfigurowanie ustawień.

Uwaga: Ustawienia zostaną uwzględnione po ponownym uruchomieniu.

7.2.9 Protokół integracji

Cel:

Jeżeli konieczne jest uzyskanie dostępu do kamery przy użyciu platformy innej firmy, można włączyć funkcję CGI. Jeżeli konieczne jest uzyskanie dostępu do urządzenia przy użyciu protokołu ONVIF, można skonfigurować użytkownika ONVIF w tym oknie. Aby uzyskać więcej informacji na temat reguł konfiguracji, skorzystaj z dokumentacji standardu ONVIF.

- **CGI**

  Zaznacz pole wyboru Enable Hikvision_CGI, a następnie wybierz uwierzytelnianie z listy rozwijanej.

  Uwaga: Digest jest zalecaną meodą uwierzytelniania.

- **ONVIF**

  Kroki:

  1. Zaznacz pole wyboru Enable ONVIF, aby włączyć tę funkcję.
  2. Dodaj użytkowników ONVIF. Można dodać maksymalnie 32 użytkowników. Ustaw nazwę użytkownika i hasło, a następnie je potwierdź. Można ustawić typ użytkownika Media user, Operator lub Administrator.

     Uwaga: Konto użytkownika ONVIF różni się od konta użytkownika kamery. Konto użytkownika ONVIF należy ustawić niezależnie.
  3. Zapisz ustawienia.

  Uwaga: Ustawienia użytkownika ONVIF są czyszczone po przywróceniu kamery.

7.2.10 Adaptacja przepustowości

Gdy ta funkcja jest włączone, płynność podglądu na żywo z kamery ma najwyższy priorytet. Kamera automatycznie dostosowuje parametry wideo i stosowana jest wstępnie zdefiniowana konfiguracja wideo. Ta funkcja zostanie włączona po ponownym uruchomieniu.

Uwaga: Adaptacja przepustowości jest dostępna tylko w przypadku niektórych modeli kamer.

7.2.11 Usługa sieciowa

Można kontrolować stan włączenia/wyłączenia (ON/OFF) funkcji określonego protokołu obsługiwanego przez kamerę.

Uwaga:

- Nieużywaną funkcję należy wyłączyć (OFF), aby zapewnić bezpieczeństwo.
- Ta funkcja jest obsługiwana tylko w przypadku niektórych modeli kamer.

W przypadku podglądu na żywo bez dodatków typu plug-in używany jest protokół **WebSocket** lub **WebSockets**.

Jeżeli dostęp do kamery jest uzyskiwany przy użyciu programu Google Chrome w wersji 45 lub wyższej albo programu Mozilla Firefox w wersji 52 lub wyższej, należy włączyć protokół WebSocket lub Websokets. W przeciwnym wypadku funkcje podglądu na żywo, wykonywania zdjęć i powiększenia cyfrowego będą niedostępne.

Jeżeli kamera używa protokolu HTTP, należy włączyć funkcję **WebSocket**.

Jeżeli kamera używa protokolu HTTPS, należy włączyć funkcję **WebSockets**.

Rozdział 8 Ustawienia wideo/audio

Cel:

Poniższe instrukcje dotyczą konfigurowania ustawień wideo, ustawień audio, ROI, wyświetlania informacji o strumieniu itp.

8.1 Konfigurowanie ustawień wideo

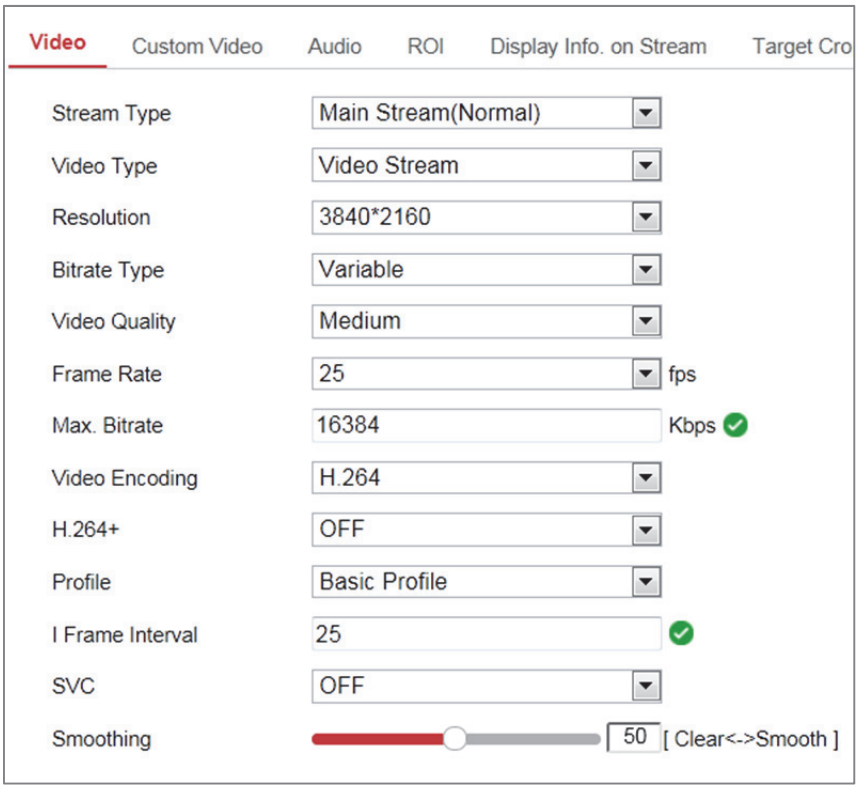
W przypadku niektórych modeli kamer można konfigurować parametry dostępnych strumieni wideo (na przykład strumienia głównego lub podstrumienia). Można też dostosować dodatkowe strumienie wideo, jeżeli będzie to konieczne.

- Na stronie **Wideo** skonfiguruj dostępne strumienie wideo.
- Na stronie **Custom Video** dodaj strumienie wideo.

8.1.1 Ustawienia wideo

Kroki:

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



Rysunek 8–1 Ustawienia wideo

2. Wybierz typ strumienia w polu Stream Type.

   Obsługiwane typy strumienia są wyświetlane na liście rozwijanej.

   Uwagi:

   - W przypadku niektórych modeli trzeci strumień **Third Stream** jest domyślnie wyłączony. Przejdź do **System > Maintenance > System Service > Software**, aby włączyć tę funkcję, jeżeli jest to wymagane.
   - Strumień główny jest zazwyczaj używany do nagrywania i wyświetlania podglądu na żywo przy odpowiedniej przepustowości, a podstrumienia można użyć do wyświetlania podglądu na żywo przy ograniczonej przepustowości.

3. Można dostosować następujące parametry dla wybranego typu strumienia.

   Video Type:

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

   Resolution:

   Wybierz rozdzielczość wyjścia wideo.

   Bitrate Type:

   Wybierz stałą lub zmienną transmisję danych.

   Video Quality:

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

   Frame Rate:

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

   Max. Bitrate:

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

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

Video Encoding:

Kamera obsługuje wiele typów kodowania, takich jak H.264, H.265, MJPEG lub MPEG4. Obsługiwany typ kodowania jest zależny od typu strumienia. Standard H.265 jest nową technologią kodowania. W porównaniu ze standardem H.264 umożliwia on zmniejszenie szybkości transmisji bitów przy tej samej rozdzielczości, liczbie klatek na sekundę i jakości obrazu.

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

H.264+ i H.265+:

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

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

Uwagi:

- Jeśli występują problemy ze zgodnością i obraz podgląd na żywo lub odtwarzania nie jest odpowiednio wyświetlany, wówczas należy zaktualizować odtwarzacz wideo do najnowszej wersji.
- Po włączeniu obsługi standardu H.264+/H.265+ parametry takie jak profil, interwał klatki I, jakość wideo i SVC są wyszarzone.
- Niektóre funkcje nie są dostępne po włączeniu obsługi standardu H.264+/H.265+. Okna związane z tymi funkcjami będą ukryte.
- Standardy H.264+/H.265+ umożliwiają automatyczne dostosowanie rozkładu szybkości transmisji bitów zgodnie z wymaganiami monitorowanej sceny w celu wykorzystania ustawionej maksymalnej szybkości transmisji bitów w perspektywie długoterminowej. Dostosowanie kamery do określonej monitorowanej sceny trwa co najmniej 24 godziny.

Max. Average Bitrate:

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

Profile:

Po wybraniu kodowania wideo H.264 lub H.265 można ustawić profil. Dostępne profile są zależne od modelu kamery.

I Frame Interval:

Ustaw parametr I Frame Interval w zakresie 1–400.

SVC:

Standard SVC (Scalable Video Coding) stanowi rozszerzenie standardu H.264/AVC i H.265. Wybierz pozycję przełącznika OFF lub ON, aby wyłączyć lub włączyć funkcję SVC. Po wybraniu ustawienia Auto urządzenie automatycznie wyodrębnia klatki z oryginalnego obrazu wideo, gdy przepustowość sieci jest niedostateczna.

Smoothing:

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

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

Uwaga:

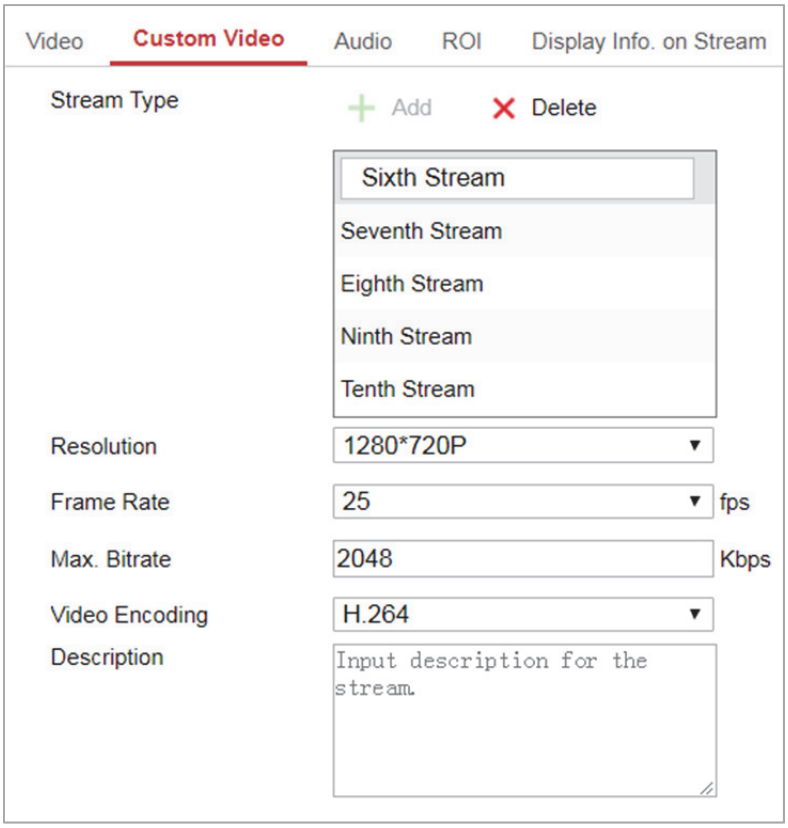
Parametry wideo są zależne od modelu kamery. Należy skorzystać z odpowiedniej strony wyświetlania funkcji kamery.

8.1.2 Wideo niestandardowe

Można skonfigurować pięć dodatkowych strumieni wideo, jeżeli jest to wymagane. Można wyświetlić podgląd na żywo niestandardowych strumieni wideo, ale nie można ich nagrywać ani odtwarzać.

Uwagi:

- Funkcja wideo niestandardowego musi być obsługiwana przez kamerę.
- Po przywróceniu kamery (nie przywróceniu ustawienia domyślnego) zachowywana jest liczba niestandardowych strumieni wideo oraz ich nazwy, ale powiązane parametry są przywracane.



Rysunek 8–2 Ustawienia wideo niestandardowego

Kroki:

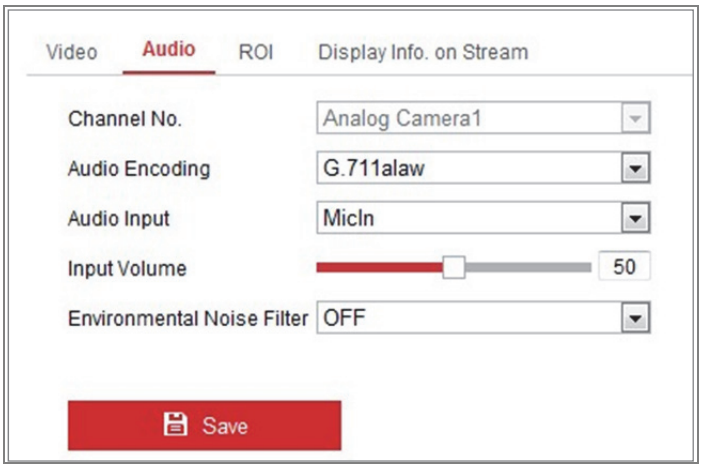
1. Kliknij przycisk , aby dodać strumień.
2. Zmień nazwę strumienia, jeżeli jest to konieczne.

   Uwaga: Nazwa strumienia może zawierać maksymalnie 32 litery i symbole (z wyjątkiem &, <, >, ' i ").
3. Dostosuj parametry strumienia (rozdzielczość, liczbę klatek na sekundę, maks. szybkość transmisji bitów, kodowanie wideo). Aby uzyskać więcej informacji na temat parametrów, zobacz *sekcję 8.1.1*.
4. (Opcjonalnie) Dodaj opis strumienia, jeżeli jest to konieczne.
5. (Opcjonalnie) Jeżeli strumień niestandardowy nie jest potrzebny, kliknij przycisk , aby go usunąć.
6. Zapisz ustawienia.

8.2 Konfigurowanie ustawień audio

Kroki:

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



Rysunek 8–3 Ustawienia audio

2. Skonfiguruj poniższe ustawienia.

   Uwaga: Ustawienia audio są zależne od modelu kamery.

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

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

   Input Volume: Regulacja w zakresie 0–100.

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

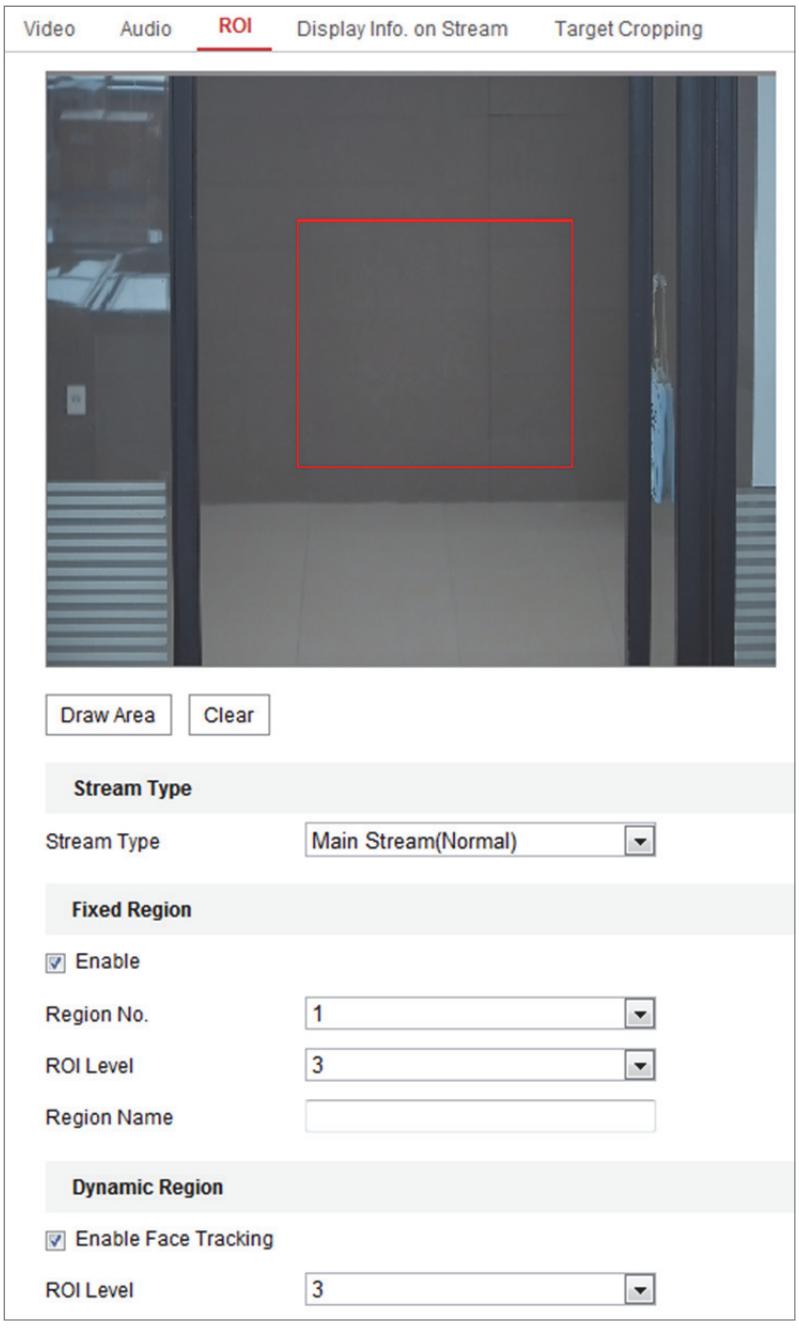
3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

8.3 Konfigurowanie kodowania ROI

Cel:

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

Uwaga: Funkcja ROI jest zależna od modelu kamery.



Rysunek 8–4 Ustawienia obszaru zainteresowania

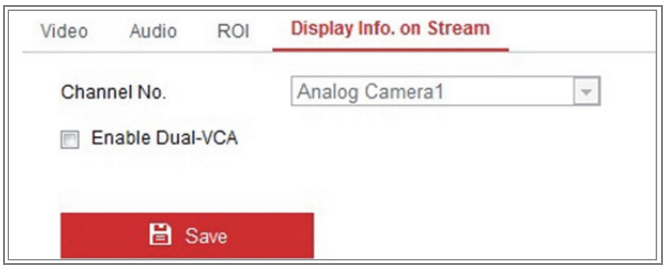
Kroki:

1. Przejdź do interfejsu ustawień kodowania obszaru zainteresowania (ROI), wybierając opcje: **Configuration > Video/Audio > ROI**.
2. Wybierz typ strumienia w polu Stream Type dla kodowania ROI.
3. Zaznacz pole wyboru **Enable** w obszarze Fixed Region.
4. Wybierz ustawienie **Fixed Region** ROI.
   (1) Wybierz pozycję Region No. z listy rozwijanej.
   (2) Zaznacz pole wyboru **Enable**, aby włączyć funkcję ROI dla wybranego obszaru.
   (3) Kliknij przycisk **Drawing**. Kliknij myszą i przeciągnij jej wskaźnik na ekranie, aby wyznaczyć czerwony prostokątny obszar ROI. Można kliknąć przycisk **Clear**, aby anulować wyznaczony obszar. Kliknij przycisk **Stop Drawing** po zakończeniu.
   (4) Wybierz ustawienie ROI level.
   (5) Wprowadź nazwę wybranego obszaru.
   (6) Kliknij przycisk **Save**, aby zapisać ustawienia ROI dla wybranego obszaru.
   (7) Powtórz kroki od (1) do (6), aby skonfigurować inne obszary.
5. Wybierz ustawienie **Dynamic Region** dla funkcji ROI.
   (1) Zaznacz pole wyboru, aby włączyć funkcję **Face Tracking**.
   Uwaga: Aby włączyć funkcję śledzenia twarzy, należy upewnić się, że funkcja detekcji twarzy jest obsługiwana i włączona.
   (2) Wybierz ustawienie ROI level.
6. Kliknij **Save**, aby zapisać ustawienia.

Uwaga: Poziom ROI oznacza poziom poprawy jakości obrazu. Im większa wartość, tym lepsza jakość obrazu.

8.4 Wyświetlanie informacji o strumieniu

Po zaznaczeniu pola wyboru **Enable Dual-VCA** informacje dotyczące obiektów (np. osoby lub pojazdu) będą oznaczane w strumieniu wideo. Następnie można skonfigurować reguły na podłączonym urządzeniu końcowym w celu wykrywania zdarzeń, takich jak przekroczenie linii lub wtargnięcie.



Rysunek 8–5 Wyświetlanie informacji o strumieniu

8.5 Konfigurowanie przycinania celu

Cel:

Można wyznaczyć obszar docelowy w podglądzie wideo na żywo, a następnie wyświetlać trzeci strumień w tym obszarze z określoną rozdzielczością i większą ilością szczegółów, jeżeli jest to wymagane.

Uwaga: Funkcja przycinania celu jest zależna od modelu kamery.

Kroki:

1. Wyświetl ustawienia **Target Cropping**.
2. Zaznacz pole wyboru **Enable Target Cropping**, aby włączyć tę funkcję.
3. Wybierz typ strumienia Third Stream.
4. Wybierz rozdzielczość przycinania wideo wyświetlanego w obszarze docelowym. Czerwony prostokąt w podglądzie wideo na żywo, reprezentujący obszar docelowy, można kliknąć i przeciągnąć w celu określenia położenia obszaru docelowego.
5. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

Rozdział 9 Ustawienia obrazu

Cel:

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

9.1 Konfigurowanie ustawień wyświetlania

Cel:

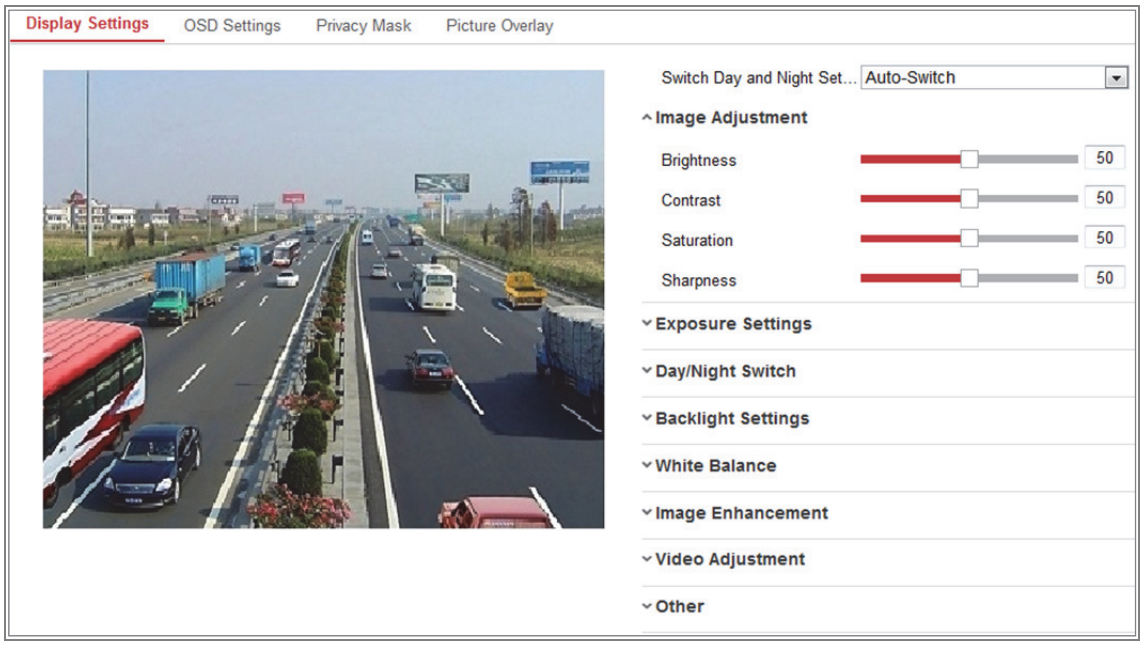
Konfigurowanie dostosowania obrazu, ustawień ekspozycji, przełącznika trybu dzień/noc, ustawienia oświetlenia, balansu bieli, poprawy jakości obrazu, dostosowania obrazu wideo i innych parametrów w ustawieniach wyświetlania.

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

9.1.1 Automatyczny przełącznik trybu dzień/noc

Kroki:

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



Rysunek 9–1 Ustawienia wyświetlania automatycznego przełącznika trybu dzień/noc

2. Skonfiguruj parametry obrazu z kamery.

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

- **Image Adjustment**

  Brightness oznacza jasność obrazu w zakresie 1–100.

  Contrast oznacza kontrast obrazu w zakresie 1–100.

  Saturation oznacza nasycenie kolorów obrazu w zakresie 1–100.

  Sharpness oznacza kontrast krawędzi obiektów w obrazie w zakresie 1–100.

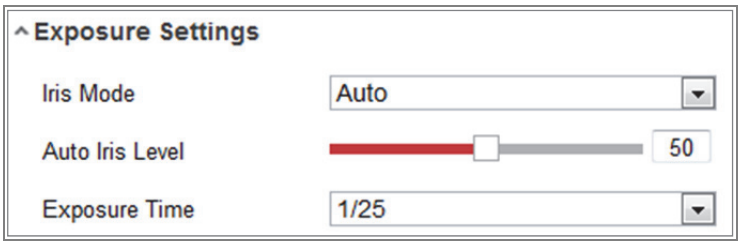
- **Exposure Settings**

  Jeżeli kamera jest wyposażona w stały obiektyw, dostępne jest tylko ustawienie **Manual** i nie można konfigurować trybu przysłony.

  Po wybraniu ustawienia **Auto** można ustawić automatyczny poziom przysłony w zakresie 0–100.

  Ustawienie **Exposure Time** określa czas otwarcia migawki elektronicznej w zakresie od 1 do 1/100 000 sek. Dostosuj ustawienie zgodnie z oświetleniem w otoczeniu.

Ustawienie **Gain** obrazu można również ręcznie konfigurować w zakresie 0–100. Im większa wartość, tym jaśniejszy obraz, ale również większe wzmocnienie zakłóceń szumowych.



Rysunek 9–2 Ustawienia ekspozycji

- **Focus**

W przypadku kamer z obiektywami zmiennoogniskowymi można ustawić tryb regulacji ostrości Auto, Manual lub Semi-auto.

Auto: Ostrość kamery jest regulowana automatycznie zgodnie ze scenariuszem monitorowania.

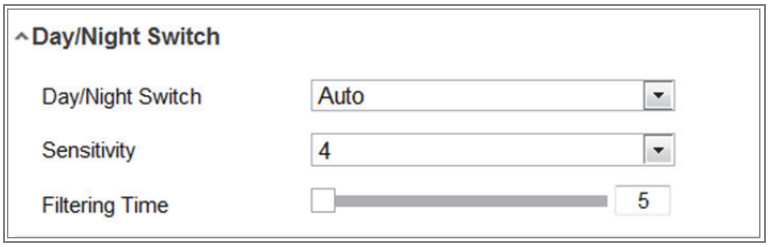
Manual: Można sterować obiektywem, ręcznie regulując ustawienia powiększenia, ostrości, inicjowania obiektywu lub wyostrzania dodatkowego.

Semi-Auto: Kamera automatycznie reguluje ostrość, gdy użytkownik zmieni parametry powiększenia.

- **Day/Night Switch**

Wybierz tryb Day/Night Switch zgodnie z wymaganiami dotyczącymi monitoringu.

Dostępne są ustawienia Day, Night, Auto, Scheduled-Switch i Triggered by alarm input przełącznika trybu dzień/noc.



Rysunek 9–3 Przełącznik trybu dzień/noc

Day: kamera pozostaje w trybie dziennym.

Night: kamera pozostaje w trybie nocnym.

Auto: kamera jest przełączana do trybu dziennego lub nocnego zgodnie z oświetleniem. Czułość można dostosować w zakresie 0–7. Im wyższa wartość, tym mniejsza zmiana oświetlenia powoduje przełączenie trybu. Ustawienie **Filtering Time** określa interwał czasowy między przełączaniem trybu dzień/noc. Można ustawić wartość 5–120 sek.

Scheduled-Switch: Ustaw godzinę rozpoczęcia i godzinę zakończenia, aby określić czas trwania trybu dzień/noc.

Triggered by alarm input: Przełącznik jest wyzwalany przez wejście alarmowe. Można ustawić tryb Day lub Night dla wyzwalania.

Smart Supplement Light: Dostępne są tryby ON, Auto i Manual oświetlenia pomocniczego.

Po wybraniu ustawienia **Auto** oświetlenie pomocnicze jest regulowane zależnie od oświetlenia w otoczeniu. Jeżeli na przykład bieżąca scena jest dostatecznie oświetlona, moc dodatkowego oświetlenia jest automatycznie zmniejszana, a jeżeli scena jest niedostatecznie oświetlona, moc dodatkowego oświetlenia jest zwiększana.

Po wybraniu ustawienia **Manual** można dostosować pomocnicze oświetlenie, zmieniając odległość. Jeżeli na przykład obiekt znajduje się w pobliżu kamery, moc dodatkowego oświetlenia jest zmniejszana, a w przypadku oddalonego obiektu moc dodatkowego oświetlenia jest zwiększana.

- **Backlight Settings**

BLC Area: Jeśli obiektyw kamery zostanie nakierowany na obiekt, którego tło jest silnie oświetlone, obraz obiektu będzie zbyt ciemny i niewyraźny. Ustawienie BLC umożliwia kompensację oświetlenia przedniej strony obiektu i zapewnia jego wyraźny obraz. Dostępne są ustawienia OFF, Up, Down, Left, Right, Center, Auto i Custom.

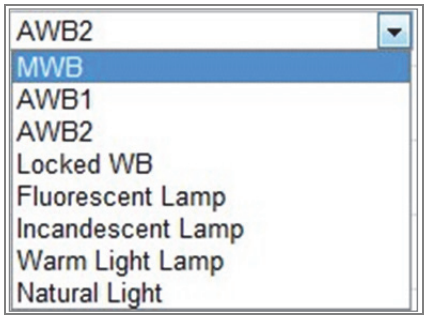
Uwaga: Jeżeli zostanie wybrany tryb Custom BLC, można wyznaczyć czerwony prostokąt w podglądzie na żywo, reprezentujący obszar BLC.

WDR: Szeroki zakres dynamiki można wykorzystać w przypadku wysokiego kontrastu w jasnych i ciemnych obszarach sceny.

HLC: Funkcji Korekcja intensywnego oświetlenia można użyć, gdy na scenie znajdują się źródła silnego światła wpływającego na jakość obrazu.

- **White Balance**

Balans bieli jest funkcją renderowania białego koloru przez kamerę, umożliwiającą dostosowanie tempeatury barwowej zgodnie z otoczeniem.



Rysunek 9–4 Balans bieli

- **Image Enhancement**

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

Defog Mode: Można włączyć funkcję usuwania mgły, gdy obraz jest niewyraźny z powodu mglistej pogody. Ta funkcja podkreśla szczegóły w celu uzyskania wyraźnego obrazu.

EIS (elektryczny stabilizator obrazu): Elektryczny stabilizator obrazu ogranicza niekorzystny wpływ wibracji na obraz wideo.

Grey Scale: Można wybrać zakres skali szarości 0–255 lub 16–235.

- **Video Adjustment**

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

Rotate: Aby optymalnie wykorzystać współczynnik proporcji obrazu 16:9, można włączyć funkcję obracania, gdy kamera jest używana do monitorowania sceny o małej szerokości.

Podczas instalowania należy obrócić kamerę o 90 stopni lub obrócić trzyosiowy obiektyw o 90 stopni i włączyć tryb obracania, aby uzyskać normalny widok sceny o współczynniku proporcji 9:16, zignorować zbędne informacje, takie jak obraz ściany, i uzyskać bardziej użyteczne informacje dotyczące sceny.

Scene Mode: Wybierz ustawienie sceny Indoor lub Outdoor zgodnie z rzeczywistym otoczeniem.

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

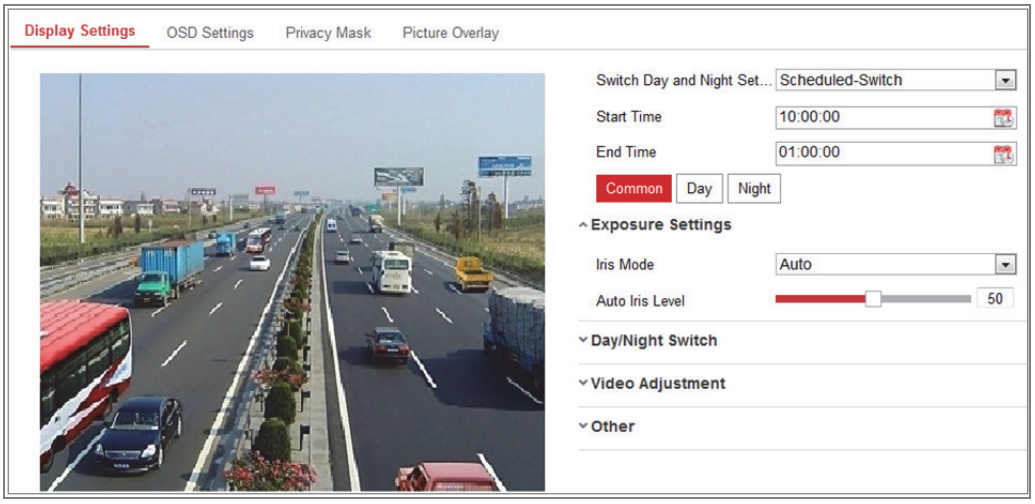
Lens Distortion Correction: W przypadku kamer z obiektywem sterowanym zdalnie obraz może być częściowo zniekształcony. Włącz tę funkcję, aby skorygować zniekształcenie.

- **Inne ustawienia**

  Niektóre modele kamer są wyposażone w wyjście CVBS, SDI lub HDMI. Wybierz ustawienie ON lub OFF lokalnego wyjścia zgodnie z wyposażeniem urządzenia.

9.1.2 Przełączanie trybu dzień/noc według harmonogramu

Korzystając z okna Przełączanie trybu dzień/noc według harmonogramu, można skonfigurować oddzielnie dla dnia i nocy parametry kamery gwarantujące jakość obrazu przy różnym oświetleniu.



Rysunek 9–5 Konfiguracja przełączania trybu dzień/noc według harmonogramu

Kroki:

1. Kliknij ikonę kalendarza, aby wybrać godzinę rozpoczęcia i godzinę zakończenia przełączania.

   Uwagi:

   - Należy wybrać prawidłową godzinę rozpoczęcia i godzinę zakończenia dla trybu dziennego.
   - Przedział czasowy może rozpoczynać się i kończyć się w dwóch kolejnych dniach. Jeżeli na przykład zostanie ustawiona godzina rozpoczęcia 10:00 i godzina zakończenia 1:00, tryb dzienny rozpocznie się o godzinie 10:00 rano i zakończy się o godzinie 1:00 następnego dnia.

2. Kliknij kartę Common, aby skonfigurować typowe parametry dotyczące trybu dziennego i trybu nocnego.

   Uwaga: Aby uzyskać więcej informacji na temat poszczególnych parametrów, zobacz *sekcję 9.1.1 Automatyczny przełącznik trybu* dzień/*noc*.

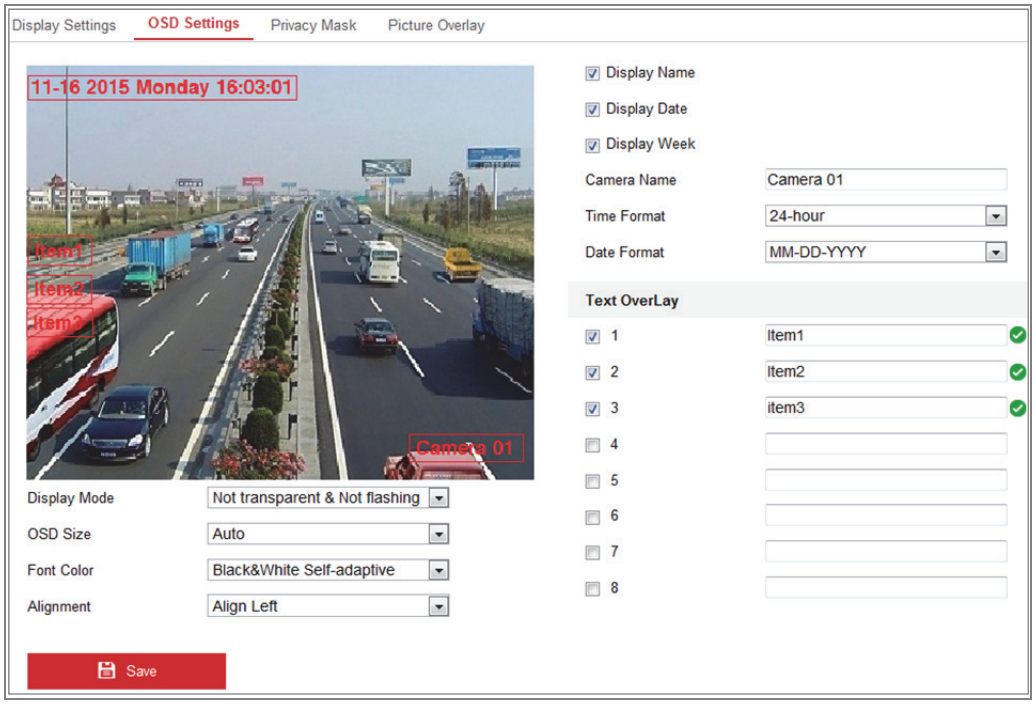
3. Kliknij kartę Day, aby skonfigurować parametry dotyczące trybu dziennego.
4. Kliknij kartę Night, aby skonfigurować parametry dotyczące trybu nocnego.

Uwaga: Ustawienia są zapisywane automatycznie, jeżeli jakikolwiek parametr zostanie zmieniony.

9.2 Konfigurowanie ustawień menu ekranowego

Cel:

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



Rysunek 9–6 Ustawienia OSD

Kroki:

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

(2) Wprowadź odpowiednie informacje w polu tekstowym.

Uwaga: Można skonfigurować maksymalnie osiem nakładek tekstowych.

7. Dostosuj położenie i wyrównanie ramek tekstowych.

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

   Uwaga: Wyrównanie można dostosować tylko w przypadku elementów Nakładka tekstowa.

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

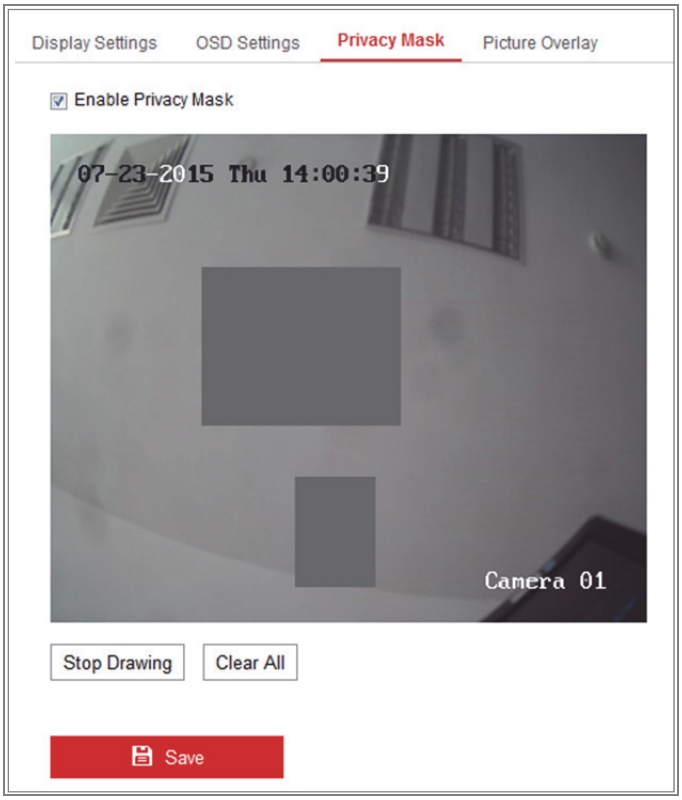
9.3 Konfigurowanie maski prywatności

Cel:

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

Kroki:

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



Rysunek 9–7 Ustawienia maski prywatności

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

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

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

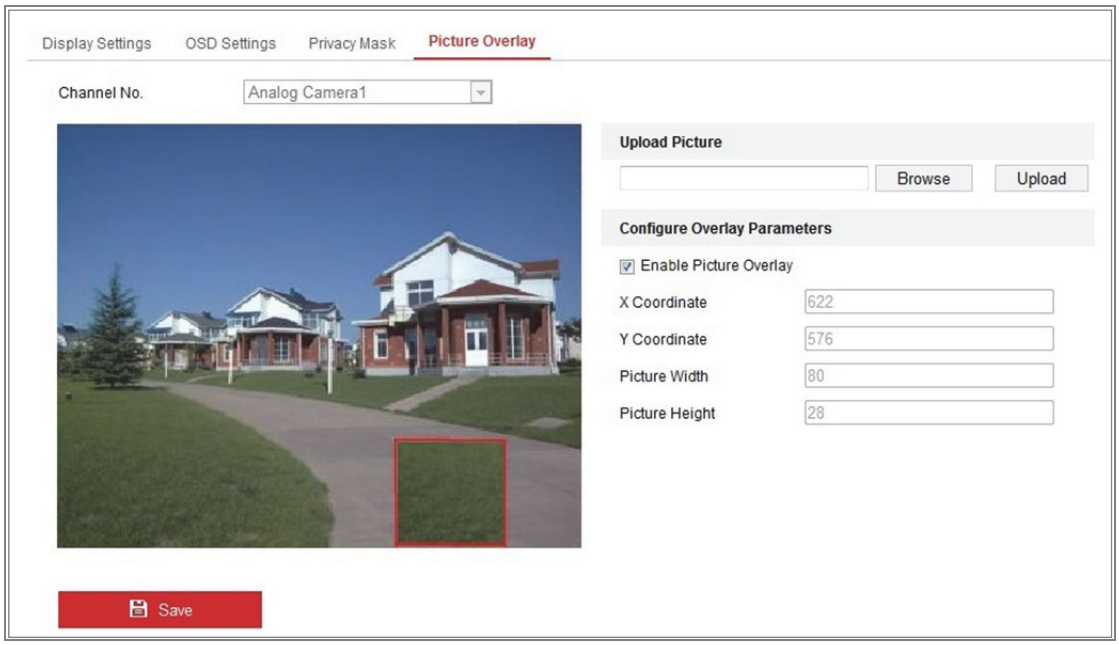
9.4 Konfigurowanie nakładania obrazu

Cel:

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

Kroki:

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



Rysunek 9–8 Nakładanie obrazu

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

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

Rozdział 10 Ustawienia zdarzeń

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

10.1 Zdarzenia podstawowe

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

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

10.1.1 Konfigurowanie detekcji ruchu

Cel:

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

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

- **Zwykła konfiguracja**

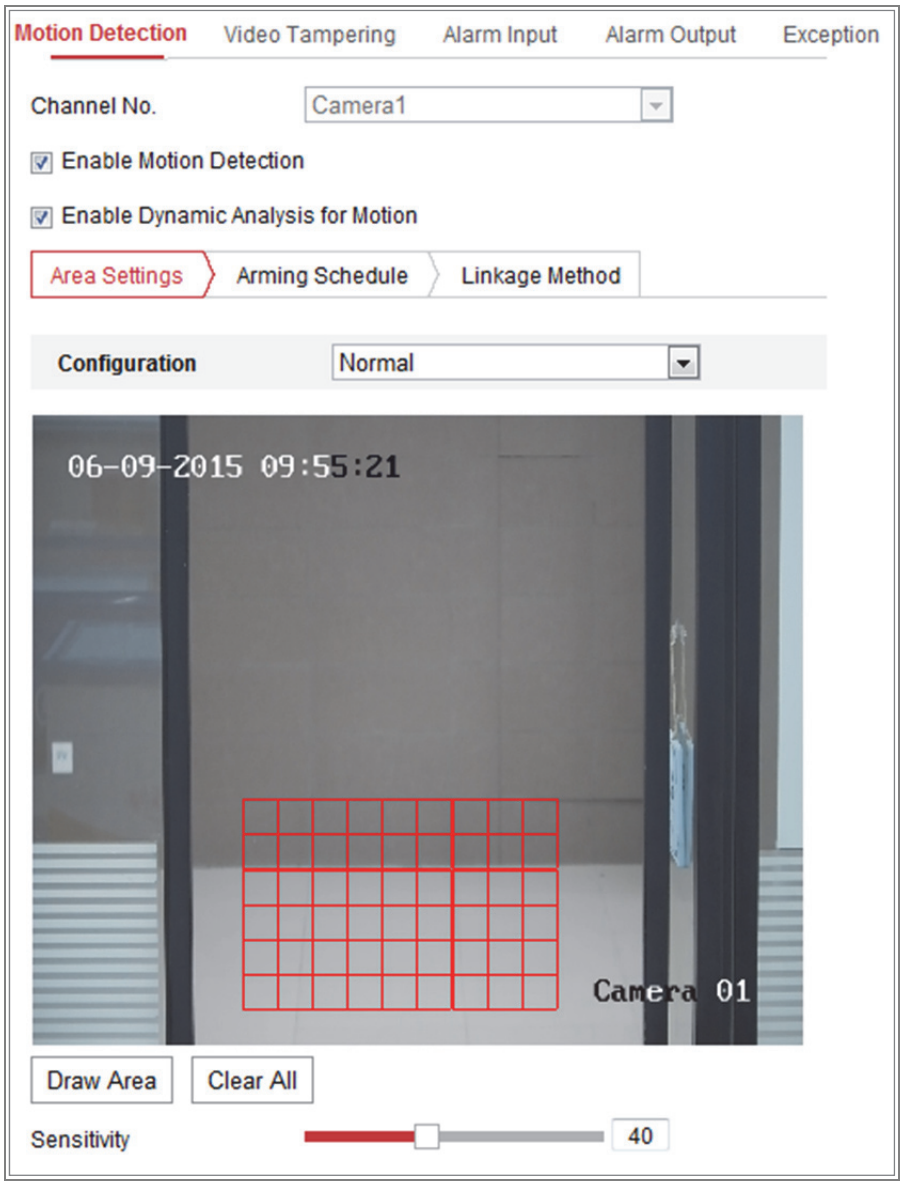
Po wybraniu zwykłej konfiguracji stosowany jest ten sam zestaw parametrów detekcji ruchu w ciągu dnia jak w nocy.

Zadania 1: Wyznaczanie obszaru detekcji ruchu

Kroki:

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

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



Rysunek 10–1 Włączanie detekcji ruchu

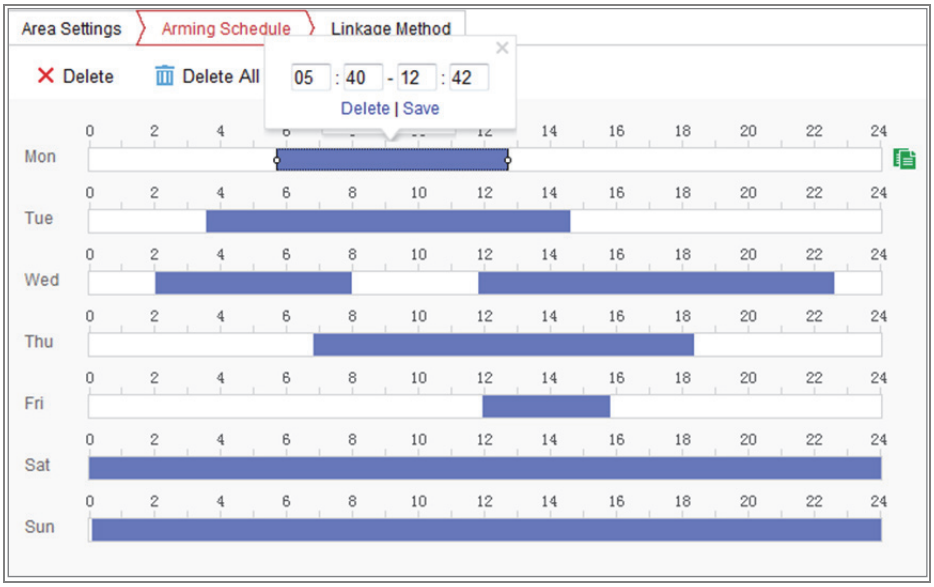
4. Kliknij przycisk **Draw Area**. Kliknij myszą i przeciągnij jej wskaźnik w podglądzie wideo na żywo, aby wyznaczyć obszar detekcji ruchu. Kliknij przycisk **Stop Drawing**, aby ukończyć wyznaczanie jednego obszaru.
5. (Opcjonalnie) Kliknij przycisk **Clear All**, aby usunąć wszystkie obszary.
6. (Opcjonalnie)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

Zadanie 2: Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu

Rysunek 10–2 Harmonogram uzbrajania

Kroki:

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



Rysunek 10–3 Harmonogram uzbrajania

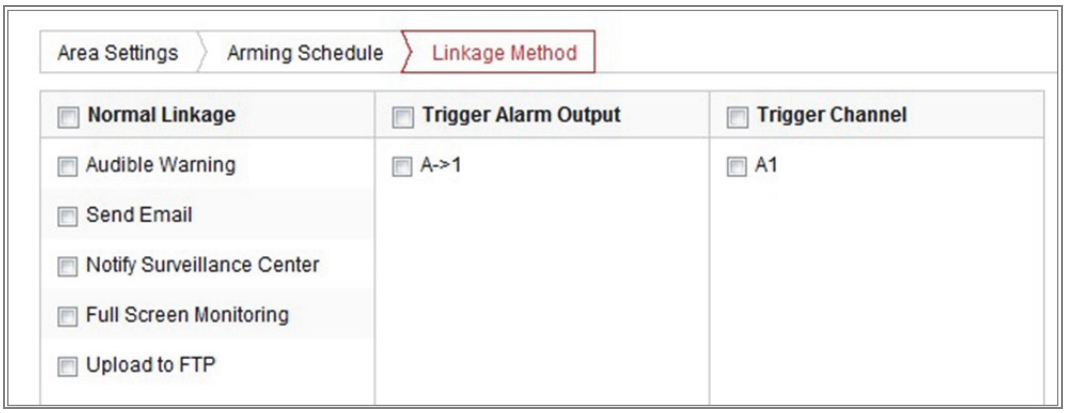
Uwaga: Po kliknięciu wybranego przedziału czasowego można go dostosować zgodnie z wymaganiami, przesuwając pasek czasu lub wprowadzając dokładną wartość.

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

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

Zadanie 3: Konfigurowanie działania powiązanego z detekcją ruchu

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



Rysunek 10–4 Działania powiązane

Uwaga: Powiązane działania są zależne od modelu kamery.

- **Audible Warning**

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

- **Notify Surveillance Center**

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

- **Send Email**

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

  Uwaga: Aby uzyskać więcej informacji na temat konfigurowania wysyłania wiadomości e-mail po wystąpieniu zdarzenia, zobacz *sekcję 7.2.3*.

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

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

  Uwagi:

  - Najpierw należy skonfigurować adres FTP i zdalny serwer FTP. Aby uzyskać więcej informacji, zobacz *sekcję 7.2.2* ***Konfigurowanie ustawień serwera FTP***.
  - Przejdź do **Configuration > Storage > Schedule Settings > Capture > Capture Parameters**, włącz funkcję wykonywania zdjęć wyzwalanego przez zdarzenia, a następnie ustaw interwał wykonywania zdjęć i liczbę zdjęć.

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

- **Trigger Channel**

  Wideo może być nagrywane po wykryciu ruchu. Aby móc skorzystać z tej funkcji, należy skonfigurować harmonogram nagrywania. Aby uzyskać więcej informacji, zobacz *sekcję 11.1*.

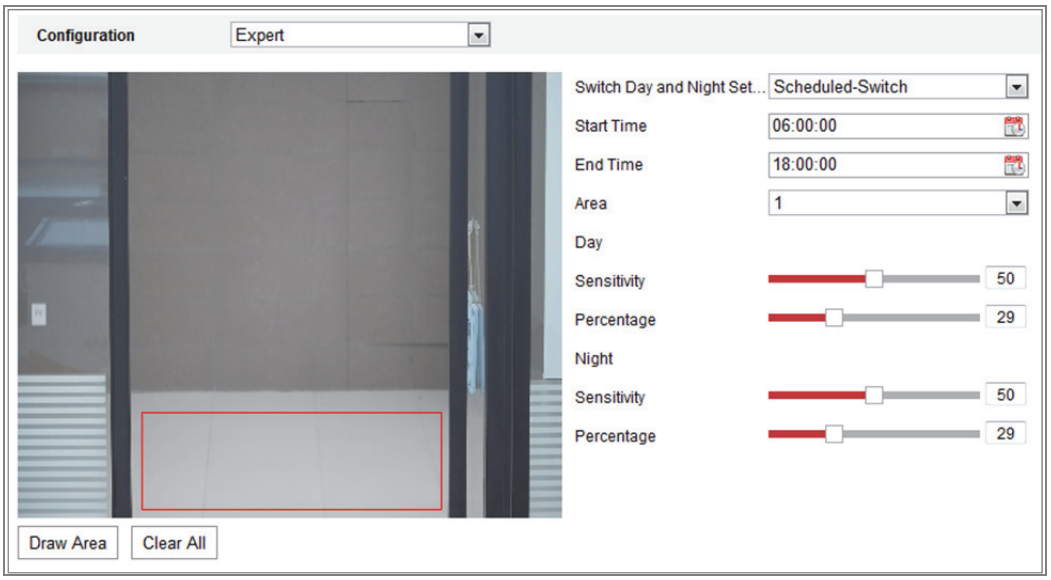
- **Trigger Alarm Output**

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

  Uwaga: Aby ustawić parametry związane z wyzwalaniem wyjścia alarmowego po wystąpieniu zdarzenia, zobacz *sekcję 10.1.4* ***Konfigurowanie wyjścia alarmu***.

Konfiguracja zaawansowana

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



Rysunek 10–5 Tryb zaawansowany detekcji ruchu

- Wyłączanie przełącznika trybu dzień/noc

Kroki:

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

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

- Automatyczny przełącznik trybu dzień/noc

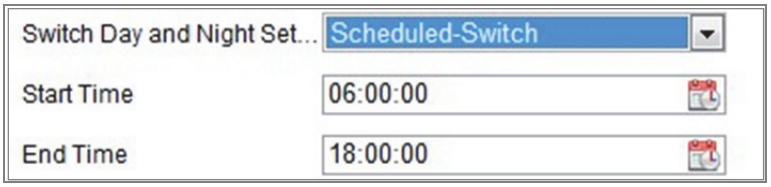
Kroki:

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

- Przełączanie trybu dzień/noc według harmonogramu

Kroki:

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



Rysunek 10–6 Przełączanie trybu dzień/noc według harmonogramu

3. Wybierz godzinę rozpoczęcia i godzinę zakończenia przełączania.

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

10.1.2 Konfigurowanie alarmu sabotażu sygnału wideo

Cel:

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

Obszarem detekcji dla tego alarmu jest cały ekran.

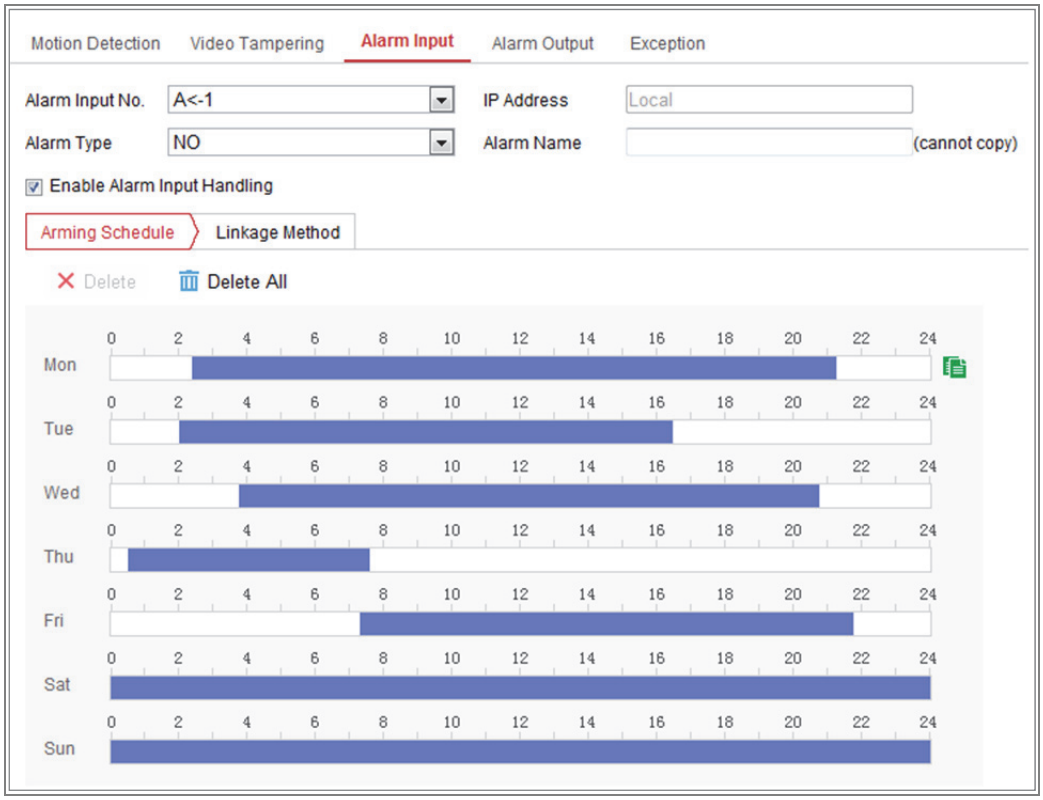
Kroki:

1. Wyświetl ustawienia detekcji sabotażu sygnału wideo (**Configuration > Event > Basic Event > Video Tampering.**).
2. Zaznacz pole wyboru **Enable Video Tampering**, aby włączyć funkcję detekcji sabotażu sygnału wideo.
3. Kliknij przycisk **Edit**, aby edytować harmonogram zabezpieczenia dla funkcji sabotażu sygnału wideo. Konfiguracja harmonogramu uzbrojenia przebiega tak samo, jak konfiguracja harmonogramu uzbrojenia dla detekcji ruchu. Zobacz ***Zadanie 2: Ustawianie harmonogramu uzbrajania dla funkcji detekcji ruchu*** w *sekcji 10.1.1.*
4. Zaznacz pole wyboru, aby wybrać powiązane działanie wykonywane po wykryciu sabotażu sygnału wideo. Zobacz ***Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu*** w *sekcji 10.1.1.*
5. Kliknij przycisk **Save**, aby zapisać ustawienia.

10.1.3 Konfigurowanie wejścia alarmu

Kroki:

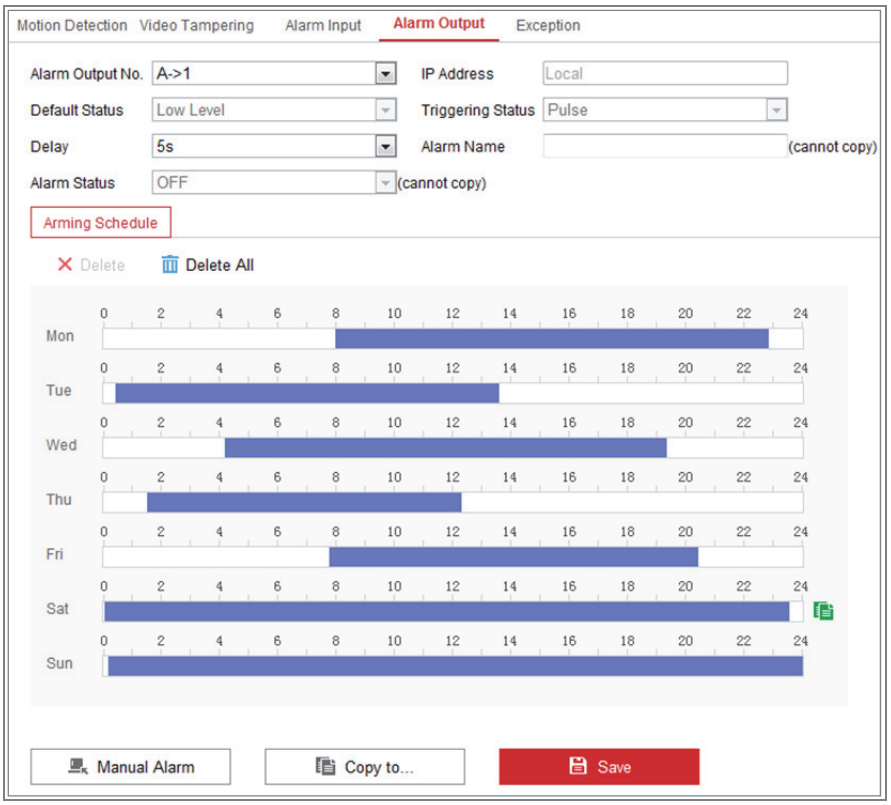
1. Przejdź do interfejsu ustawień wejścia alarmu, wybierając opcje: **Configuration > Event > Basic Event > Alarm Input**.
2. Wybierz numer wejścia alarmowego i typ alarmu. Dostępne typy alarmu to: NO (normalnie otwarty) i NC (normalnie zamknięty). Edytuj nazwę wejścia alarmowego (opcjonalnie).



Rysunek 10–7 Ustawienia wejścia alarmowego

3. Kliknij kartę **Arming Schedule**, aby ustawić harmonogram uzbrajania wejścia alarmowego. Zobacz ***Zadanie 2: Ustawianie harmonogramu uzbrajania dla funkcji detekcji ruchu*** w *sekcji 10.1.1.*
4. Kliknij przycisk **Linkage Method** i zaznacz pole wyboru, aby wybrać działanie powiązane z wejściem alarmowym. Zobacz ***Zadanie 3:*** *Ustawianie działania powiązanego z detekcją ruchu* w *sekcji 10.1.1.*
5. Ustawienia można skopiować i zastosować do innych wejść alarmu.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.1.4 Konfigurowanie wyjścia alarmu



Rysunek 10–8 Ustawienia wyjścia alarmowego

Kroki:

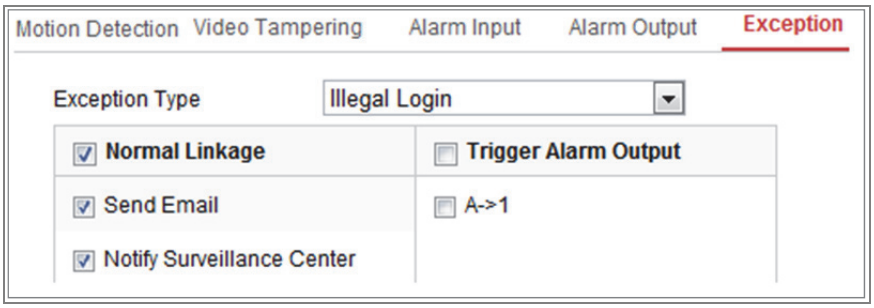
1. Przejdź do interfejsu ustawień wyjścia alarmu, wybierając opcje: **Configuration > Event > Basic Event > Alarm Output**.
2. Wybierz jeden kanał wyjścia alarmowego z listy rozwijanej **Alarm Output**. Można też skonfigurować nazwę wyjścia alarmowego (opcjonalnie).
3. W pozycji opóźnienia można wybrać jedną z wartości: 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min lub Manual. Czas opóźnienia to czas wstrzymania przesyłania sygnału alarmowego do wyjścia alarmu w momencie wystąpienia alarmu
4. Kliknij kartę **Arming Schedule**, aby wyświetlić okno Edycja harmonogramu. Konfiguracja harmonogramu czasowego przebiega tak samo, jak ustawianie harmonogramu uzbrajania dla detekcji ruchu. Zobacz ***Zadanie 2: Ustawianie harmonogramu uzbrajania dla funkcji detekcji ruchu*** w *sekcji 10.1.1.*
5. Ustawienia można skopiować i zastosować do innych wyjść alarmu.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.1.5 Obsługa zdarzeń nietypowych

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

Kroki:

1. Przejdź do interfejsu ustawień zdarzeń nietypowych, wybierając opcje: **Configuration > Event > Basic Event > Exception**.
2. Zaznacz pole wyboru, aby ustawić działania wykonywane w momencie wystąpienia alarmu zdarzenia nietypowego. Zobacz ***Zadanie 3:*** *Ustawianie działania powiązanego z detekcją ruchu* w *sekcji 10.1.1.*



Rysunek 10–9 Ustawienia wyjątków

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

10.1.6 Konfigurowanie innego alarmu

Uwaga: Niektóre kamery obsługują alarm bezprzewodowy, alarm pasywnej podczerwieni (PIR) lub alarm użytkownika.

- **Wireless Alarm**

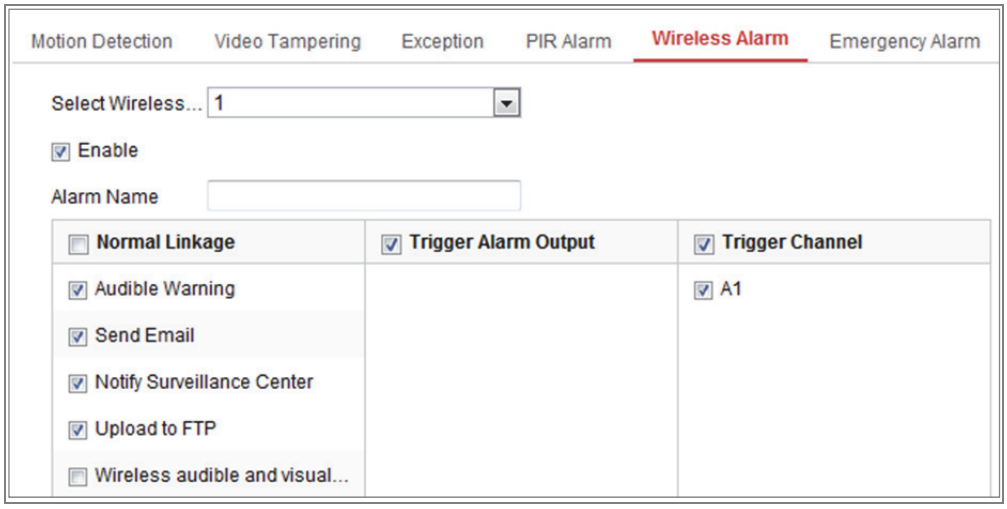
Cel:

Wysłanie bezprzewodowo do kamery sygnału alarmowego przez detektor, taki jak bezprzewodowy stycznik drzwiowy, powoduje wyzwolenie alarmu bezprzewodowego i ewentualne wykonanie serii działań.

Kroki:

1. Wyświetl okno Ustawienia alarmu bezprzewodowego:

   Configuration > Advanced Configuration > Basic Event > Wireless Alarm



Rysunek 10–10 Ustawianie alarmu bezprzewodowego

2. Wybierz numer alarmu bezprzewodowego.

   Obsługiwanych jest maksymalnie osiem kanałów wejścia zewnętrznego alarmu bezprzewodowego.

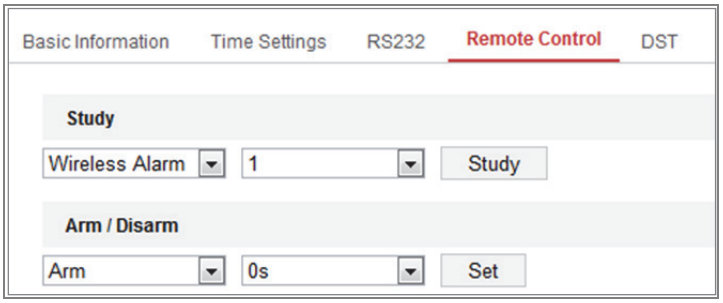
3. Zaznacz pole wyboru **Enable Wireless Alarm**, aby włączyć obsługę alarmu bezprzewodowego.

4. Wprowadź nazwę alarmu w polu tekstowym, zgodnie z wymaganiami.

5. Zaznacz pole wyboru, aby wybrać powiązane działania wykonywane po zgłoszeniu alarmu bezprzewodowego.

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

7. Umieść zewnętrzne urządzenie bezprzewodowe w pobliżu kamery i przejdź do **Configuration > System > System Settings > Remote Control**, aby zabezpieczyć kamerę i przetestować alarm bezprzewodowy.



Rysunek 10–11 Konfigurowanie alarmu bezprzewodowego

PIR Alarm

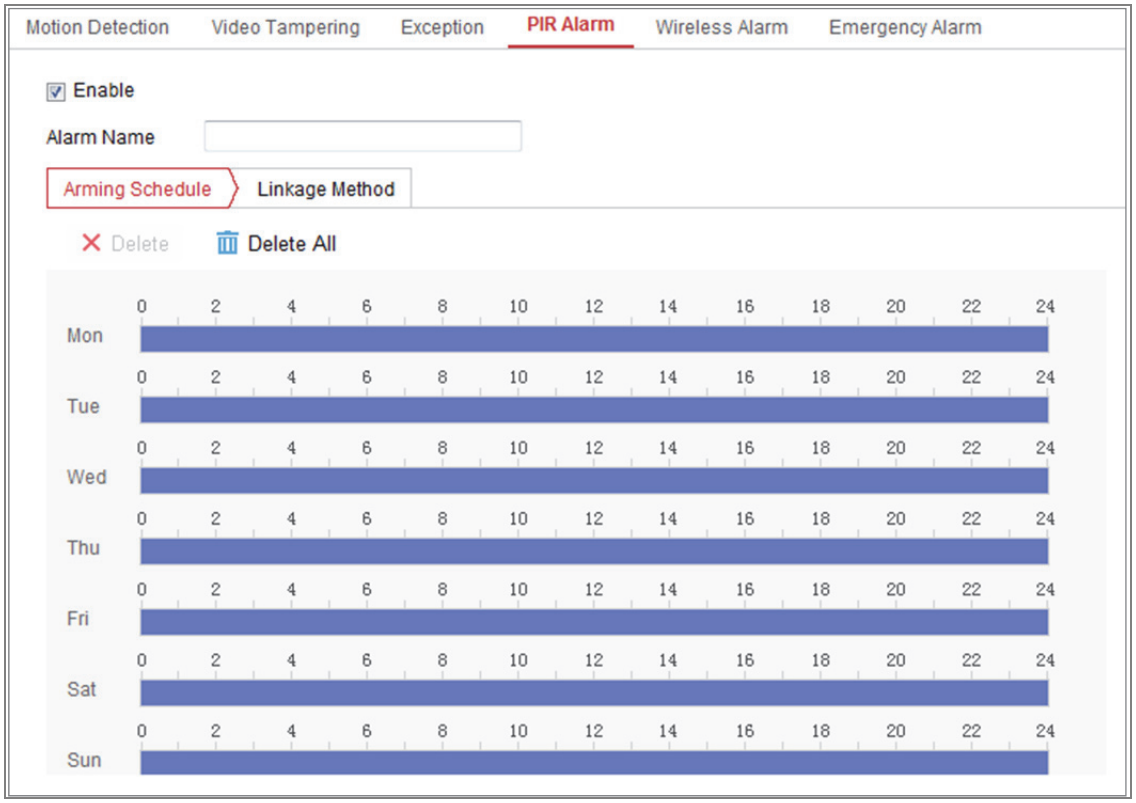
Cel:

Alarm czujnika pasywnej podczerwieni (PIR, Passive Infrared) jest wyzwalany, gdy intruz przemieszcza się w polu widzenia detektora. Można wykrywać energię cieplną rozpraszaną przez ciało ludzkie lub stałocieplne zwierzęta takie jak psy, koty itp.

Kroki:

1. Wyświetl okno Ustawienia alarmu pasywnej podczerwieni:

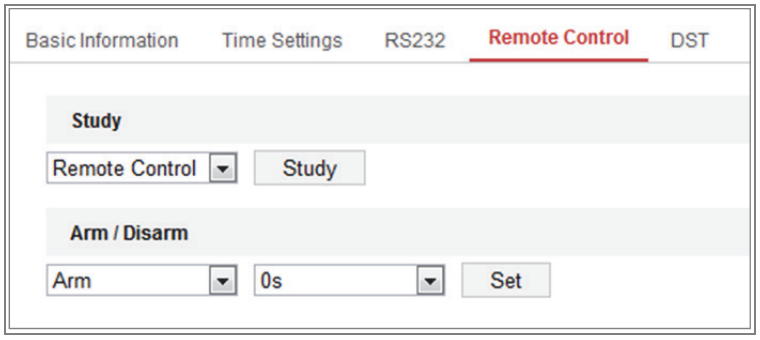
   Configuration > Advanced Configuration > Basic Event > PIR Alarm



Rysunek 10–12 Ustawianie alarmu pasywnego czujnika podczerwieni (PIR)

2. Zaznacz pole wyboru **Enable**, aby włączyć funkcję alarmu pasywnego czujnika podczerwieni (PIR).
3. Wprowadź nazwę alarmu w polu tekstowym, zgodnie z wymaganiami.
4. Zaznacz pole wyboru, aby wybrać powiązane działania wykonywane po zgłoszeniu alarmu pasywnej podczerwieni.
5. Kliknij przycisk **Edit**, aby skonfigurować harmonogram zabezpieczenia.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

7. Przejdź do **Configuration > Advanced Configuration > System > Remote Control**, aby zabezpieczyć kamerę.



Rysunek 10–13 Uzbrajanie alarmu pasywnego czujnika podczerwieni (PIR)

● Emergency Alarm

Cel:

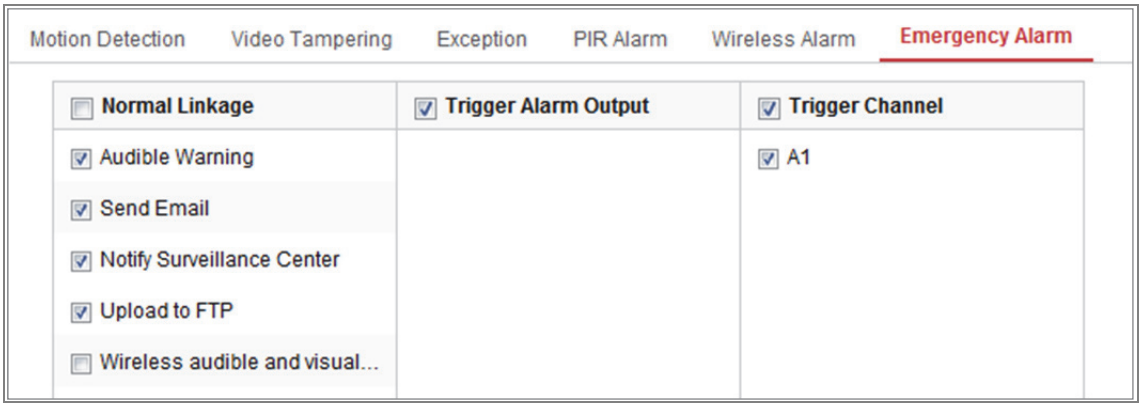
Można nacisnąć przycisk Zagrożenie na pilocie zdalnego sterowania, aby wyzwolić Alarm użytkownika w sytuacji zagrożenia.

Uwaga: Zdalne sterowanie jest wymagane do obsługi Alarmu użytkownika. Przejdź do **Configuration > System > System Settings > Remote Control**, aby przetestować zdalne sterowanie.

Kroki:

1. Wyświetl okno Ustawienia alarmu użytkownika:

   Configuration > Event > Basic Event > Emergency Alarm



Rysunek 10–14 Ustawianie alarmu użytkownika

2. Zaznacz pole wyboru, aby wybrać powiązane działania wykonywane po zgłoszeniu Alarmu użytkownika.
3. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.2 Zdarzenia inteligentne

Instrukcje podane w tej sekcji dotyczą konfigurowania zdarzeń inteligentnych, takich jak detekcja nietypowego dźwięku, detekcja braku ostrości, detekcja zmiany sceny, detekcja wtargnięcia i detekcja przekroczenia linii. Te zdarzenia mogą wyzwalać powiązane działania, takie jak Notify Surveillance Center, Send Email, Trigger Alarm Output, itp.

10.2.1 Konfigurowanie detekcji nietypowego dźwięku

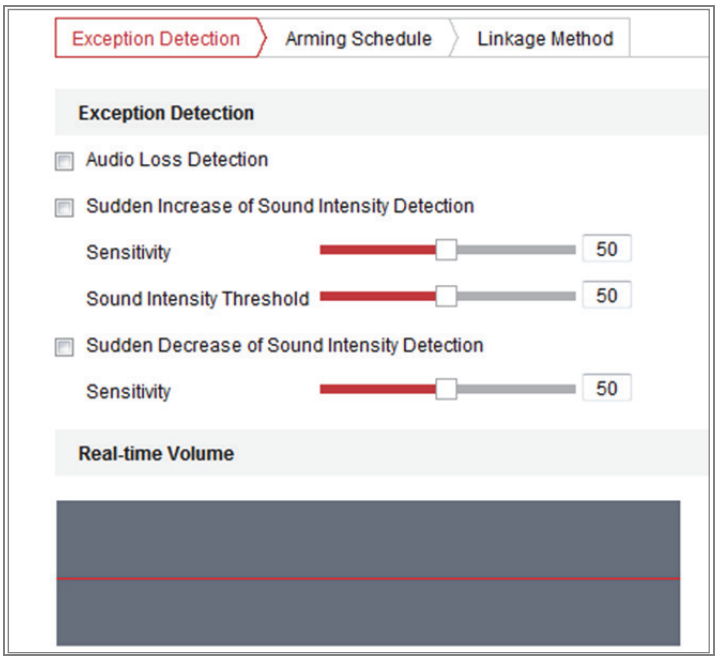
Cel:

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



Rysunek 10–15 Detekcja nietypowego sygnału audio

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:

   - Sensitivity: Zakres 1-100. Im niższa wartość, tym większa zmiana jest wymagana do wyzwolenia funkcji detekcji.
   - Sound Intensity Threshold: Zakres 1-100. To ustawienie umożliwia filtrowanie dźwięku w otoczeniu. Im większe natężenie dźwięku w otoczeniu, tym wyższa powinna być ta wartość. Można dostosować to ustawienie zgodnie z rzeczywistym otoczeniem.
   - W tym oknie jest wyświetlana głośność dźwięku w czasie rzeczywistym.
5. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Aby uzyskać szczegółowe instrukcje, zobacz **Zadanie 2 Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w *sekcji 10.1.1*.
6. Kliknij kartę **Linkage Method** i wybierz działania powiązane z detekcją nietypowego dźwięku, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie nagrywania w kanale i Wyzwolenie wyjścia alarmowego.
7. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.2.2 Konfigurowanie detekcji braku ostrości

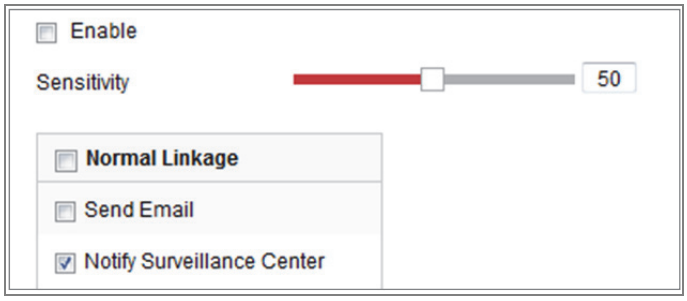
Cel:

Ta funkcja umożliwia detekcję rozmycia obrazu na skutek braku ostrości obiektywu i wykonanie określonych akcji po wyzwoleniu alarmu.

Uwaga: Funkcja detekcji braku ostrości jest zależna od modelu kamery.

Kroki:

1. Wyświetl ustawienia Detekcja braku ostrości (**Configuration > Event > Smart Event > Defocus Detection**).



Rysunek 10–16 Konfigurowanie detekcji braku ostrości

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak czułości detekcji do żądanego położenia. Wartość czułości można regulować w zakresie 1–100. Im wyższa wartość, tym mniejszy brak ostrości powoduje wyzwolenie alarmu.
4. Wybierz działania powiązane z detekcją braku ostrości, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail i Wyzwolenie wyjścia alarmowego.
5. Kliknij **Save**, aby zapisać ustawienia.

10.2.3 Konfigurowanie detekcji zmiany sceny

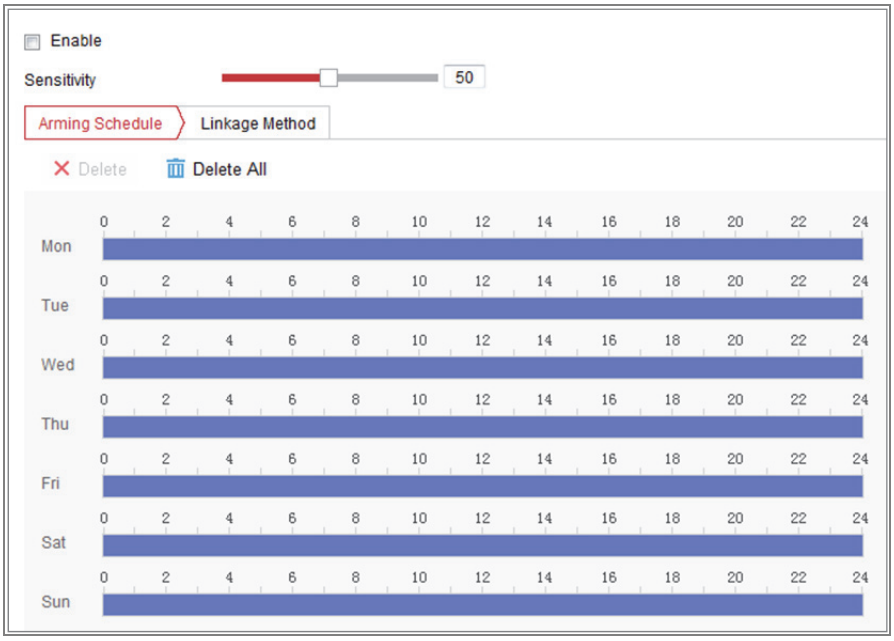
Cel:

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

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

Kroki:

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



Rysunek 10–17 Detekcja zmiany sceny

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Kliknij i przeciągnij suwak czułości detekcji do żądanego położenia. Wartość czułości można regulować w zakresie 1–100. Im wyższa wartość, tym mniejsza zmiana sceny powoduje wyzwolenie alarmu.
4. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Aby uzyskać szczegółowe instrukcje, zobacz *Zadanie 2* ***Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu*** w *sekcji 10.1.1*.
5. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane z detekcją zmiany sceny, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie kanału i Wyzwolenie wyjścia alarmowego.
6. Kliknij **Save**, aby zapisać ustawienia.

10.2.4 Konfigurowanie detekcji twarzy

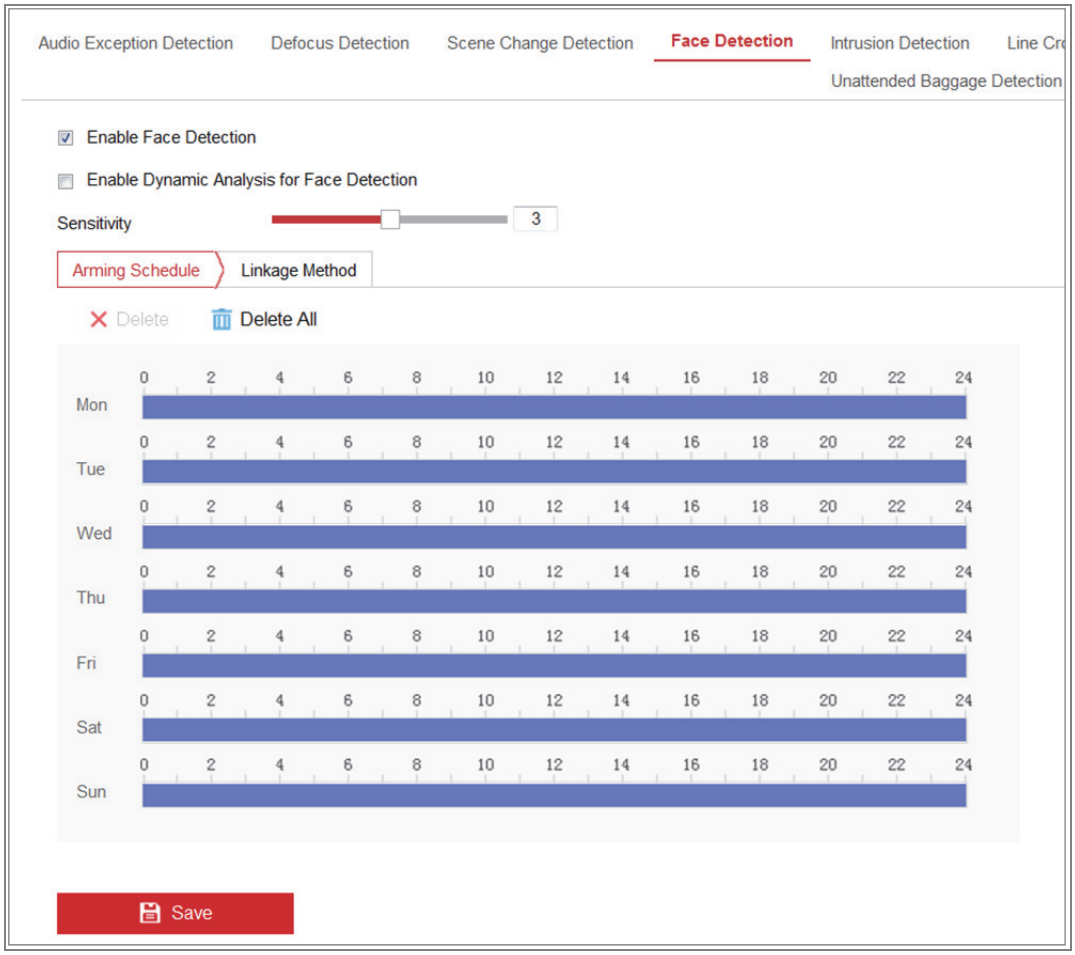
Cel:

Ta funkcja umożliwia detekcję twarzy na monitorowanej scenie i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Wyświetl ustawienia Detekcja twarzy **Configuration > Event > Smart Event > Face Detection**.
2. Zaznacz pole wyboru **Enable Face Detection**, aby włączyć tę funkcję.
3. Po zaznaczeniu pola wyboru **Enable Dynamic Analysis for Face Detection** wykryta twarz będzie oznaczana zielonym prostokątem w podglądzie na żywo.

   Uwaga: Aby oznaczyć wykrytą twarz w podglądzie wideo na żywo, należy przejść do **Configuration > Local** w celu włączenia opcji **Rules**.
4. Kliknij i przeciągnij suwak czułości detekcji do żądanego położenia. Czułość można regulować w zakresie 1–5. Im wyższa wartość, tym większa efektywność detekcji twarzy.
5. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Aby uzyskać szczegółowe instrukcje, zobacz **Zadanie 2 Konfigurowanie harmonogramu zabezpieczenia dla funkcji detekcji ruchu** w *sekcji 10.1.1*.
6. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane z detekcją twarzy. Zobacz ***Zadanie 3: Ustawianie działania powiązanego wykonywanego po wykryciu ruchu*** w *sekcji 10.1.1*.



Rysunek 10–18 Detekcja twarzy

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

10.2.5 Konfigurowanie detekcji wtargnięcia

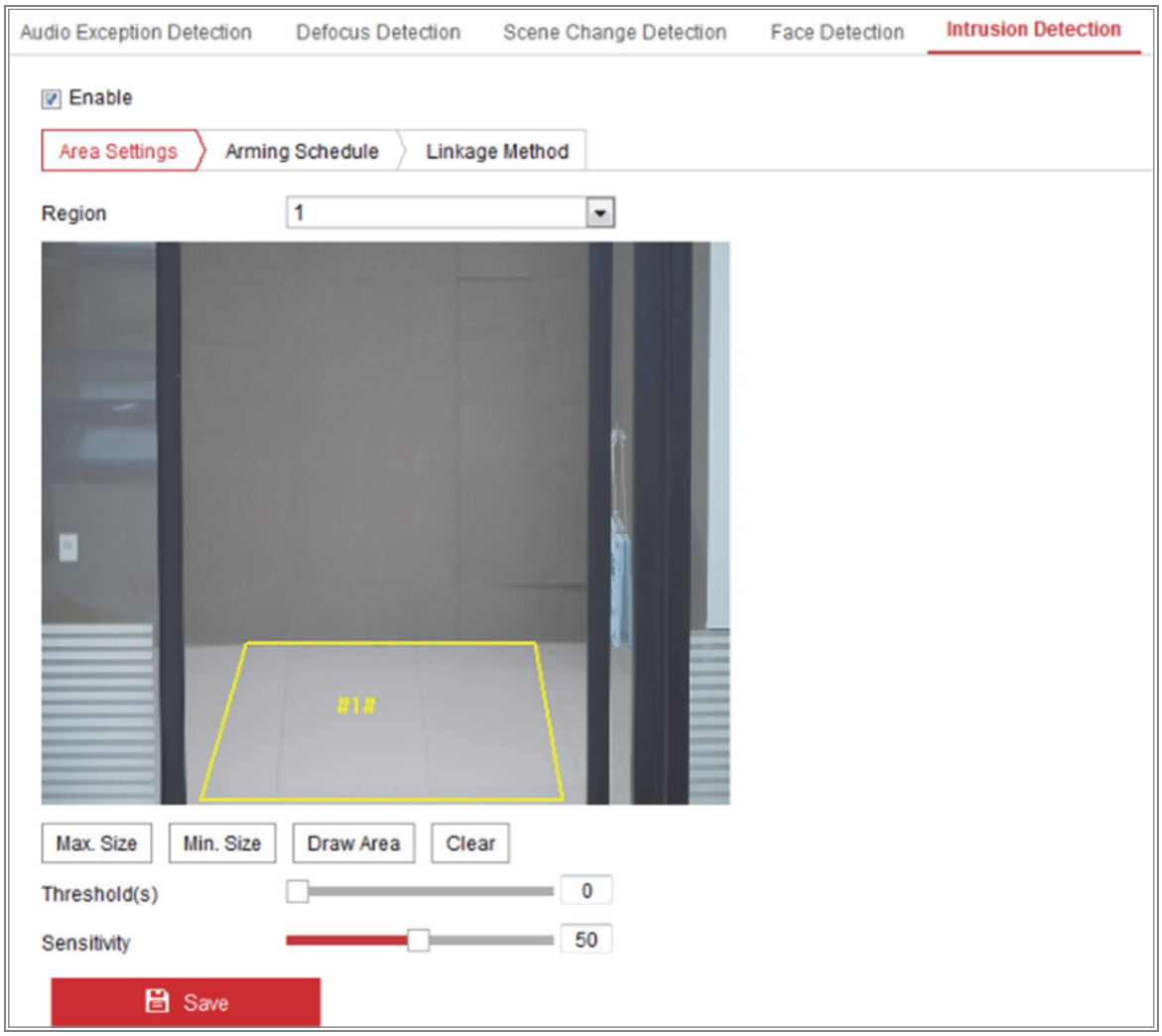
Cel:

Funkcja detekcji wtargnięcia umożliwia wykrywanie osób, pojazdów lub innych obiektów wkraczających do wstępnie wyznaczonej strefy wirtualnej lub przebywających bez uzasadnienia w tej strefie i wykonanie określonych akcji po wyzwoleniu alarmu.

Uwaga: Funkcja detekcji wtargnięcia jest zależna od modelu kamery.

Kroki:

1. Wyświetl ustawienia Detekcja wtargnięcia **Configuration > Event > Smart Event > Intrusion Detection**.



Rysunek 10–19 Detekcja wtargnięcia

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz numer obszaru z listy rozwijanej **Region**.

   Region: Wstępnie zdefiniowany obszar w podglądzie obrazu na żywo. Wykrycie obiektów, takich jak osoby lub pojazd, wchodzących lub wjeżdżających do wyznaczonego obszaru i przebywających w nim bezcelowo, będzie powodować wyzwolenie skonfigurowanego alarmu.
4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby rozpocząć wyznaczanie obszaru.
5. Zaznacz za pomocą lewego przycisku myszy cztery wierzchołki obszaru detekcji na podglądzie obrazu wideo na żywo, a następnie kliknij prawy przycisk myszy, aby zakończyć zaznaczanie.

6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

   Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

   Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.
7. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
8. Ustaw wartość progową czasu detekcji wtargnięcia.

   Wartość progowa: Wartość progowa czasu bezcelowego przebywania obiektu w wyznaczonym obszarze w zakresie 0–10 sek. Jeśli ustawiono wartość 0, wówczas alarm zostanie wyzwolony natychmiast po wtargnięciu obiektu do obszaru.
9. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Czułość jest określana procentowo jako część obiektu znajdująca się we wstępnie zdefiniowanym obszarze.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza część obiektu znajdującą się we wstępnie zdefiniowanym obszarze. S_T reprezentuje cały obiekt.

   Przykład: jeżeli zostanie ustawiona wartość 60, zdarzenie zostanie uznane za wtargnięcie, gdy co najmniej 40 procent obiektu znajdzie się w obszarze.

   Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele.

   Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.
10. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można skonfigurować do 4 obszarów. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane obszary.
11. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia.
12. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane z detekcją wtargnięcia, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie kanału i Wyzwolenie wyjścia alarmowego.
13. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.2.6 Konfigurowanie detekcji przekroczenia linii

Cel:

Funkcja detekcji przekroczenia linii umożliwia wykrywanie osób, pojazdu lub innych obiektów przekraczających wstępnie zdefiniowaną linię wirtualną i wykonanie określonych akcji po wyzwoleniu alarmu.

Uwaga: Funkcja detekcji przekroczenia linii jest zależna od modelu kamery.

Kroki:

1. Wyświetl ustawienia Detekcja przekroczenia linii (**Configuration > Event > Smart Event > Line Crossing Detection**).

Rysunek 10–20 Detekcja przekroczenia linii

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz linię z listy rozwijanej
4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby wyświetlić linię wirtualną w podglądzie wideo na żywo.
5. Przeciągnij linię do żądanego położenia w podglądzie wideo na żywo. Kliknij linię, a następnie kliknij i przeciągnij jeden z dwóch czerwonych kwadratów wyświetlonych na zakończeniach linii, aby określić jej kształt i długość.
6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

   Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

   Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.
7. Wybierz kierunek dla funkcji detekcji przekroczenia linii. Można wybrać kierunki A<->B, A->B i B->A.

   A<-> B: Gdy obiekt przekracza wyznaczoną linię w dowolnym kierunku, jest wykrywany i wyzwalane są alarmy.

   A-> B: Tylko obiekt przekraczający wyznaczoną linię ze strony A na stronę B może być wykryty.

   B-> A: Tylko obiekt przekraczający wyznaczoną linię ze strony B na stronę A może być wykryty.
8. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
9. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Procentowo określona część ciała osoby, która może znajdować się poza wstępnie zdefiniowaną linią.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza część obiektu przekraczającą wstępnie zdefiniowaną linię. S_T reprezentuje cały obiekt.

Przykład: jeżeli zostanie ustawiona wartość 60, przekroczenie linii nastąpi, gdy co najmniej 40 procent obiektu znajdzie się poza linią.

Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele.

Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.

10. Powtórz powyższe kroki, aby skonfigurować inne linie. Można ustawić maksymalnie cztery linie. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane linie.
11. Kliknij kartę **Arming Schedule**, aby ustawić harmonogram uzbrajania.
12. Wybierz działania powiązane z detekcją przekroczenia linii, takie jak Powiadomienie centrum monitoringu, Wysłanie wiadomości e-mail, Przekazanie do serwera FTP/karty pamięci/dysku NAS, Wyzwolenie kanału i Wyzwolenie wyjścia alarmowego.
13. Kliknij **Save**, aby zapisać ustawienia.

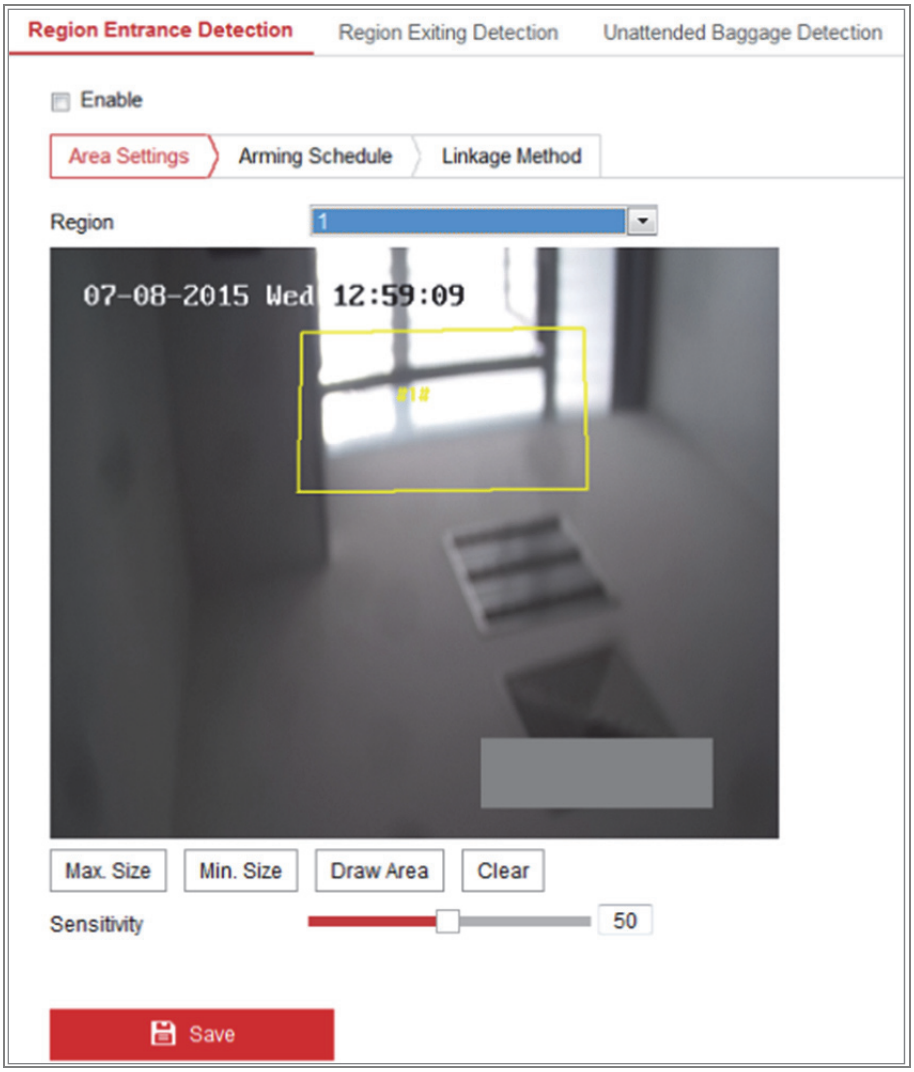
10.2.7 Konfigurowanie detekcji wejścia w obszar

Cel:

Funkcja detekcji wejścia w obszar umożliwia wykrywanie osób, pojazdów lub innych obiektów wkraczających do wstępnie wyznaczonej strefy z lokalizacji zewnętrznej i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Wyświetl ustawienia Detekcja wejścia w obszar **Configuration > Event > Smart Event > Region Entrance Detection**.



Rysunek 10–21 Detekcja wejścia w obszar

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz pozycję **Region** z listy rozwijanej ustawień detekcji.
4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby rozpocząć wyznaczanie obszaru.
5. Zaznacz za pomocą lewego przycisku myszy cztery wierzchołki obszaru detekcji na podglądzie obrazu wideo na żywo, a następnie kliknij prawy przycisk myszy, aby zakończyć zaznaczanie.
6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.

7. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
8. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Czułość jest określana procentowo jako część obiektu znajdująca się we wstępnie zdefiniowanym obszarze.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza część obiektu znajdującą się we wstępnie zdefiniowanym obszarze, a S_T oznacza całą powierzchnię obiektu.

   Przykład: jeżeli zostanie ustawiona wartość 60, zdarzenie zostanie uznane za wejście w obszar, gdy co najmniej 40 procent obiektu znajdzie się w obszarze.

   Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele.

   Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.
9. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można skonfigurować do 4 obszarów. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane obszary.
10. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia.
11. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane.
12. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

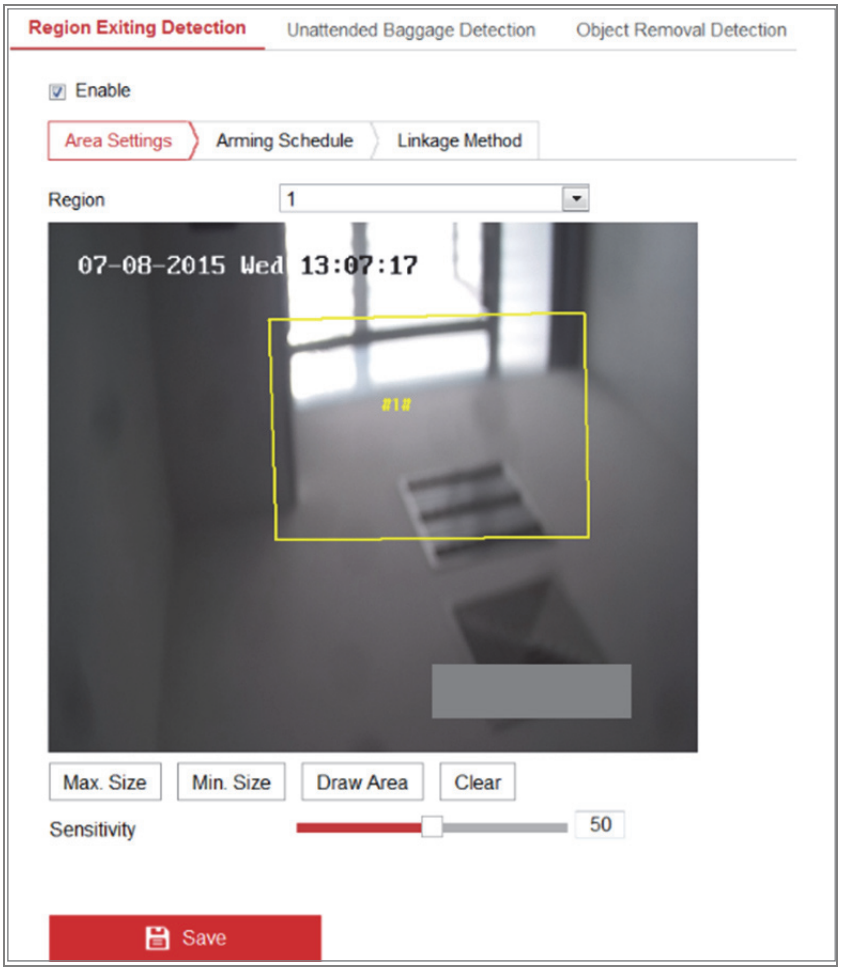
10.2.8 Konfigurowanie detekcji opuszczenia obszaru

Cel:

Funkcja detekcji opuszczenia obszaru umożliwia wykrywanie osób, pojazdów lub innych obiektów opuszczających wstępnie wyznaczoną strefę wirtualną i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Wyświetl ustawienia Detekcja wyjścia z obszaru (**Configuration > Event > Smart Event > Region Exiting Detection**).



Rysunek 10–22 Detekcja wyjścia z obszaru

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz pozycję **Region** z listy rozwijanej ustawień detekcji.
4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby rozpocząć wyznaczanie obszaru.
5. Zaznacz za pomocą lewego przycisku myszy cztery wierzchołki obszaru detekcji na podglądzie obrazu wideo na żywo, a następnie kliknij prawy przycisk myszy, aby zakończyć zaznaczanie.

6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

   Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

   Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.
7. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
8. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Czułość jest określana procentowo jako część obiektu znajdująca się poza wstępnie zdefiniowanym obszarem.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza część obiektu znajdującą się poza wstępnie zdefiniowanym obszarem. S_T reprezentuje cały obiekt.

   Przykład: jeżeli zostanie ustawiona wartość 60, zdarzenie zostanie uznane za wyjście z obszaru, gdy co najmniej 40 procent obiektu znajdzie się poza obszarem.

   Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele. Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.
9. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można skonfigurować do 4 obszarów. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane obszary.
10. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia.
11. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane.
12. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

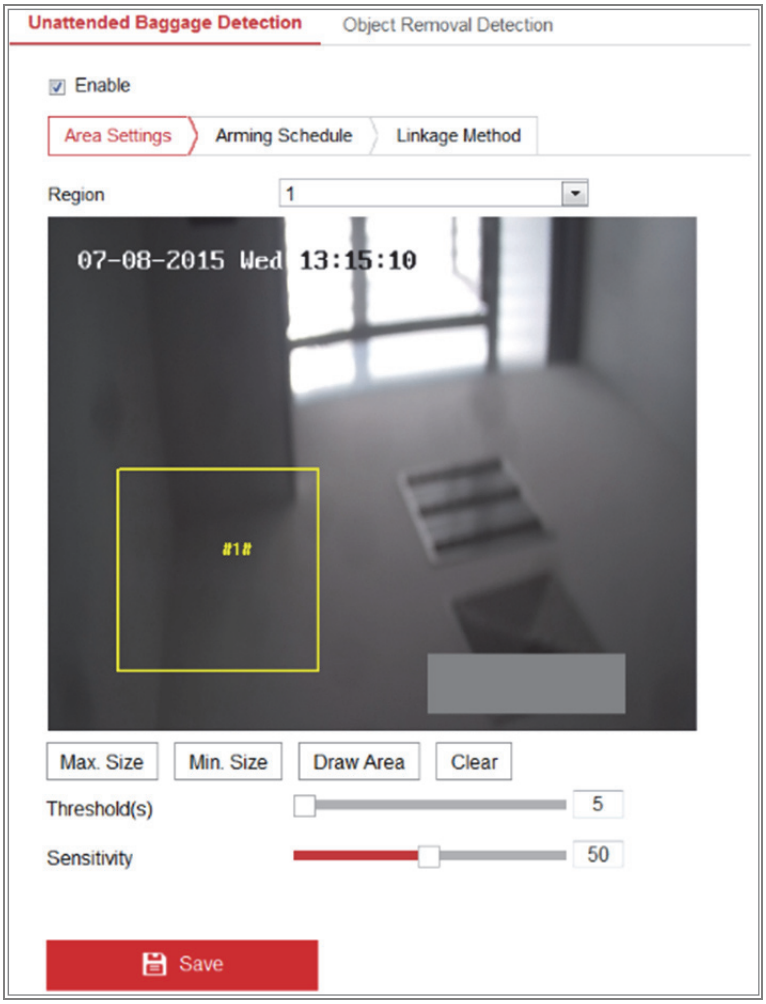
10.2.9 Konfigurowanie detekcji bagażu pozostawionego bez nadzoru

Cel:

Funkcja detekcji bagażu pozostawionego bez nadzoru umożliwia wykrycie porzuconych we wstępnie wyznaczonej strefie obiektów takich jak bagaż, torebka, niebezpieczne materiały itp. i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Wyświetl ustawienia Detekcja bagażu pozostawionego bez nadzoru **Configuration > Event > Smart Event > Unattended Baggage Detection**.



Rysunek 10–23 Detekcja bagażu pozostawionego bez nadzoru

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz pozycję **Region** z listy rozwijanej ustawień detekcji.

4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby rozpocząć wyznaczanie obszaru.
5. Zaznacz za pomocą lewego przycisku myszy cztery wierzchołki obszaru detekcji na podglądzie obrazu wideo na żywo, a następnie kliknij prawy przycisk myszy, aby zakończyć zaznaczanie.
6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

   Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

   Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.
7. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
8. Ustaw wartość progową czasu i czułość detekcji bagażu pozostawionego bez nadzoru.

   Threshold: Wartość progowa czasu pozostawania obiektów w wyznaczonym obszarze w zakresie 5–100 sek. Po ustawieniu wartości 10 alarm jest wyzwalany, jeżeli obiekt zostanie pozostawiony w obszarze przez 10 sekund.
9. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Czułość jest określana procentowo jako część obiektu znajdująca się we wstępnie zdefiniowanym obszarze.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza docelową część obiektu znajdującą się we wstępnie zdefiniowanym obszarze. S_T reprezentuje cały obiekt.

   Przykład: jeżeli zostanie ustawiona wartość 60, obiekt docelowy jest uznawany za bagaż pozostawiony bez nadzoru, gdy 40 procent obiektu znajdzie się w wyznaczonym obszarze.

   Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele.

   Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.

10. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można skonfigurować do 4 obszarów. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane obszary.
11. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia.
12. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane.
13. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.2.10 Konfigurowanie detekcji usunięcia obiektu

Cel:

Ta funkcja umożliwia detekcję usunięcia z wstępnie wyznaczonej strefy obiektów, takich jak elementy wyposażenia, i wykonanie określonych akcji po wyzwoleniu alarmu.

Kroki:

1. Wyświetl ustawienia Detekcja usunięcia obiektu **Configuration > Event > Smart Event > Object Removal Detection**.

Rysunek 10–24 Detekcja usunięcia obiektu

2. Zaznacz pole wyboru **Enable**, aby włączyć tę funkcję.
3. Wybierz pozycję **Region** z listy rozwijanej ustawień detekcji.
4. Kliknij kartę **Area Settings** i kliknij przycisk **Draw Area**, aby rozpocząć wyznaczanie obszaru.
5. Zaznacz za pomocą lewego przycisku myszy cztery wierzchołki obszaru detekcji na podglądzie obrazu wideo na żywo, a następnie kliknij prawy przycisk myszy, aby zakończyć zaznaczanie.
6. Skonfiguruj ustawienia Rozmiar maks. i Rozmiar min. dla wykrywanych obiektów. Obiekty mniejsze lub większe niż rozmiar docelowy nie będą powodować wyzwolenia alarmu.

   Max. Size: Maksymalny rozmiar obiektu. Obiekty o większym rozmiarze nie będą powodować wyzwolenia alarmu.

   Min. Size: Minimalny rozmiar obiektu. Obiekty o mniejszym rozmiarze nie będą powodować wyzwolenia alarmu.
7. Kliknij przycisk **Stop Drawing** po wyznaczeniu obszaru.
8. Ustaw wartość progową czasu detekcji usunięcia obiektu.

   Threshold: Wartość progowa czasu usunięcia obiektów z wyznaczonego obszaru w zakresie 5–100 sek. Po ustawieniu wartości 10 alarm jest wyzwalany, jeżeli obiekt zostanie usunięty z obszaru na 10 sekund.
9. Przeciągnij suwak, aby ustawić wartość czułości.

   Sensitivity: Zakres 1-100. Czułość jest określana procentowo jako część obiektu znajdująca się poza wstępnie zdefiniowanym obszarem.

   Czułość = $100 – S_1/S_T*100$

   S_1 oznacza docelową część obiektu znajdującą się poza wstępnie zdefiniowanym obszarem. S_T reprezentuje cały obiekt.

   Przykład: jeżeli zostanie ustawiona wartość 60, obiekt docelowy jest uznawany za usunięty, gdy 40 procent obiektu znajdzie się poza wyznaczonym obszarem.

   Uwaga: **Czułość** detekcji jest obsługiwana tylko przez niektóre modele.

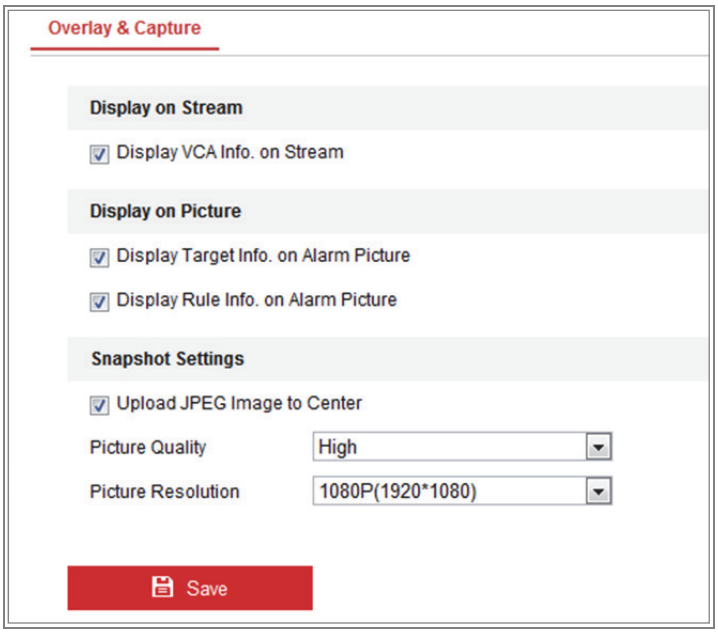
   Aby uzyskać więcej informacji, sprawdź elementy wyświetlanego okna.

10. Powtórz powyższe kroki, aby skonfigurować inne obszary. Można skonfigurować do 4 obszarów. Można kliknąć przycisk **Clear**, aby usunąć wszystkie wstępnie zdefiniowane obszary.
11. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia.
12. Kliknij kartę **Linkage Method**, aby wybrać działania powiązane.
13. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

10.3 Konfiguracja VCA

10.3.1 Analiza zachowań

Analiza zachowania umożliwia detekcję serii podejrzanych zachowań i wykonanie powiązanych działań po wyzwoleniu alarmu.



Rysunek 10–25 Analiza zachowań

❖ **Nakładka i wykonywanie zdjęć**

Informacje mogą być wyświetlane na zdjęciach i strumieniu.

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

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

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

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

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

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

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

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

❖ **Kalibracja 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.

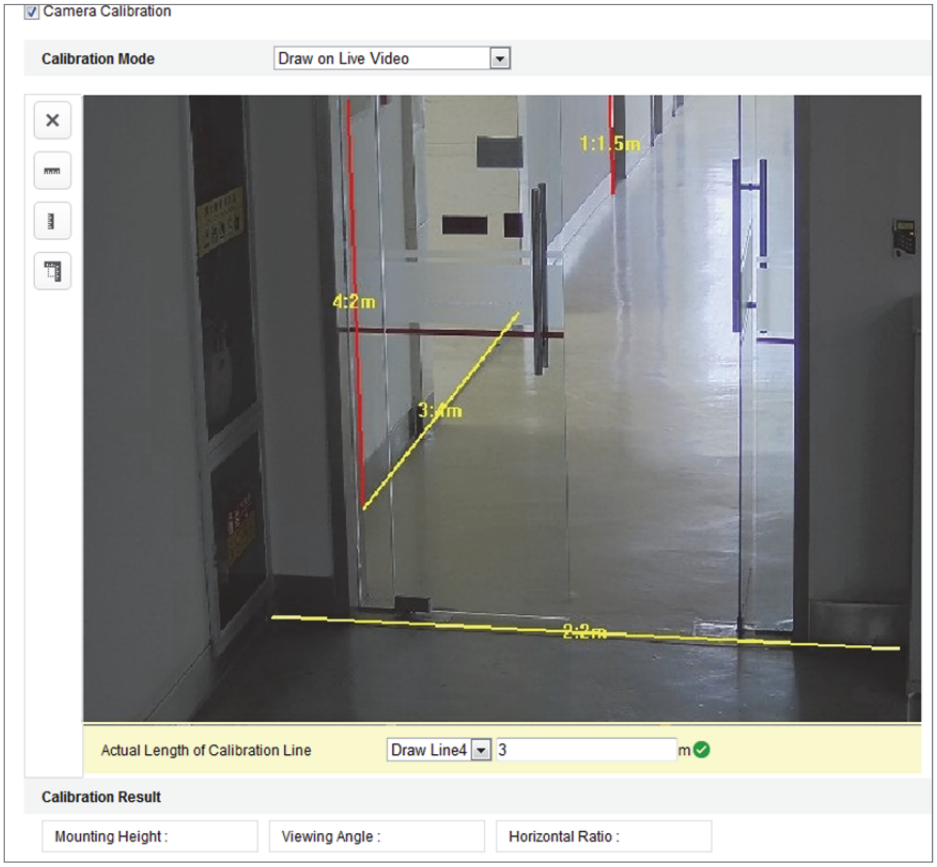
Kroki:

1. Zaznacz pole wyboru **Camera Calibration**, aby włączyć tę funkcję.
2. Wybierz ustawienie trybu kalibracji 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 **Draw Verification Line (Horizontal) / (Vertical)**, aby wyznaczyć poziomą/pionową linię weryfikacyjną w podglądzie na żywo, i wprowadź rzeczywistą długość w polu Real Length. Korzystając z wyznaczonych linii referencyjnych i ich rzeczywistej długości, kamera może analizować inne obiekty w podglądzie na żywo.
3. Kliknij przycisk Horizontal Verify  / Vertical Verify  , aby wyznaczyć linię poziomą/pionową w podglądzie na żywo, i kliknij przycisk **Start Verifying**  w celu obliczenia długości linii. Porównaj obliczoną długość linii z rzeczywistą długością, aby zweryfikować skonfigurowane informacje kalibracyjne.

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



Rysunek 10–26 Wyznaczanie linii w podglądzie na żywo

4. Można kliknąć przycisk , aby usunąć wyznaczone linie.
5. Kliknij przycisk „Save“, aby zapisać ustawienia.

❖ **Chroniony obszar**

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

Kroki:

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

Uwagi:

- Obsługiwany jest wielokątny obszar o maksymalnie dziesięciu bokach.

- Aby usunąć wyznaczone obszary, należy kliknąć przycisk .
- Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć obszarów chronionych.

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

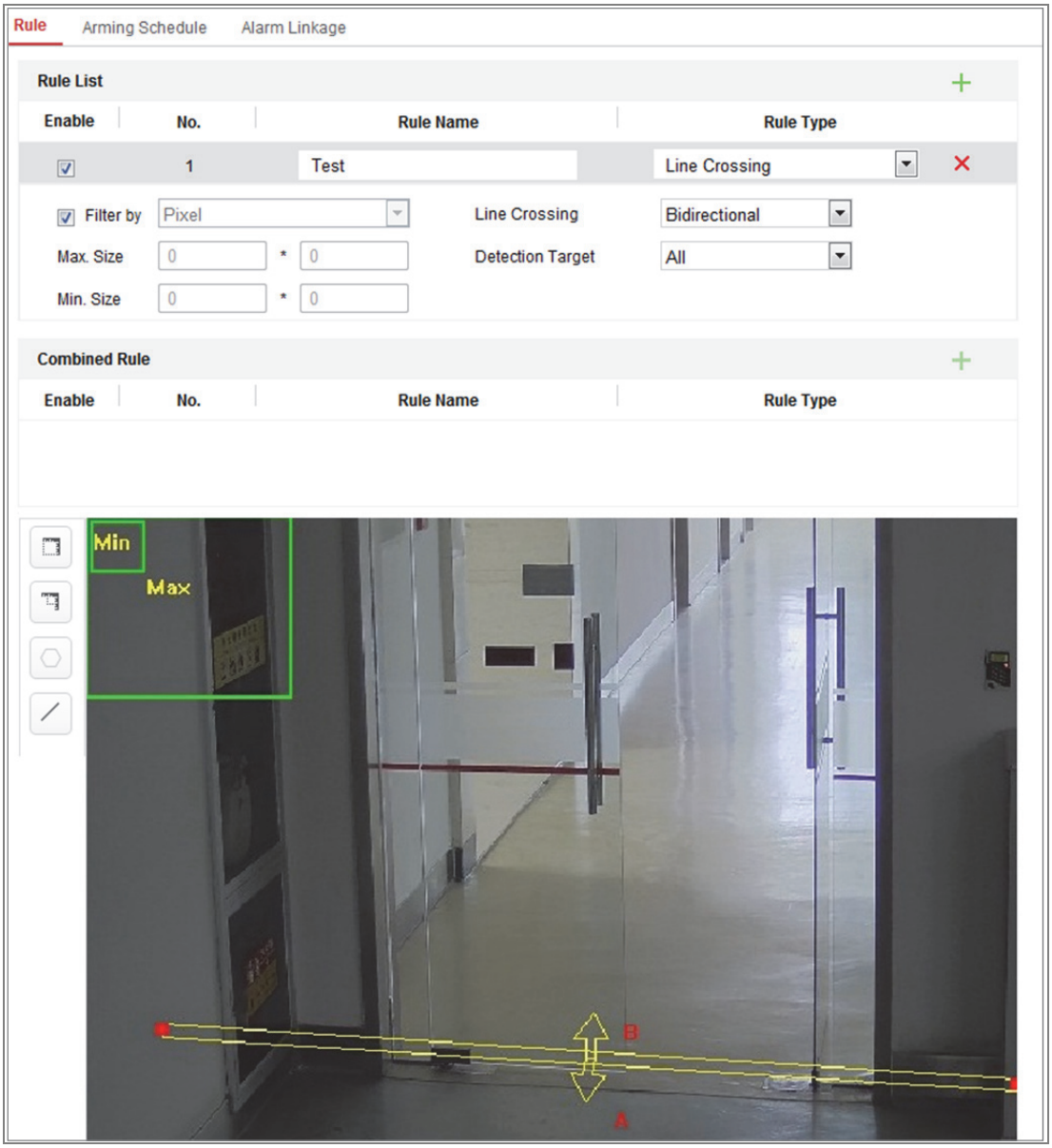
❖ **Reguła**

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

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

Kroki:

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



Rysunek 10–27 Konfigurowanie reguły

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.

Detection Target: Wybierz ustawienie Human lub Vehicle jako cel detekcji.

Można też wybrać ustawienie All, aby wykrywać wszystkie obiekty jako cele.

Draw line/area: Aby korzystać z funkcji detekcji przekroczenia linii, należy wyznaczyć linię i wybrać kierunek przekroczenia (dwukierunkowo, A-do-B lub B-do-A). W przypadku innych zdarzeń, takich jak wtargnięcie, wejście w obszar lub opuszczenie obszaru, należy kliknąć lewym przyciskiem myszy podgląd wideo na żywo, aby wyznaczyć punkty końcowe obszaru, i kliknąć prawym przyciskiem myszy w celu zakończenia wyznaczania obszaru.

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

4. Zaznacz pole wyboru połączonej reguły, aby uwzględnić ją w analizie zachowań.
5. 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:

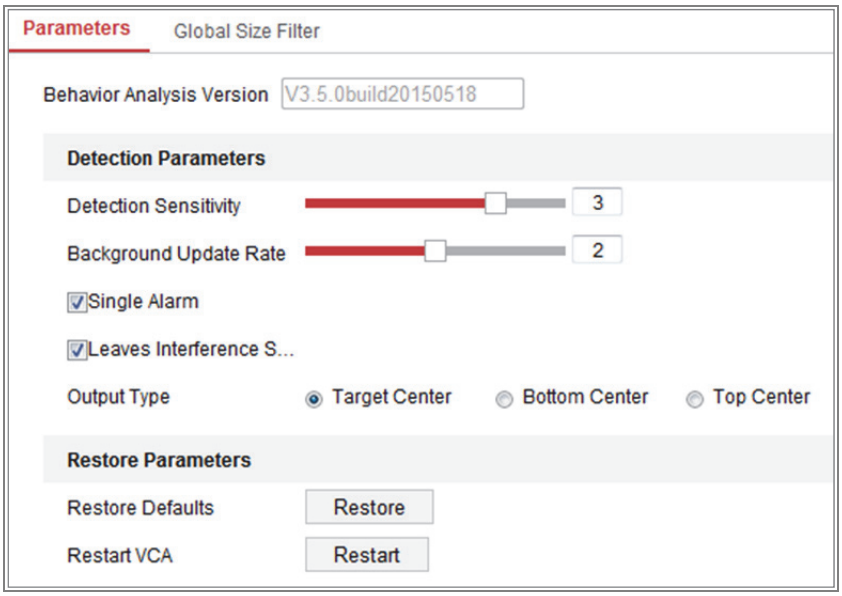
   - Jeśli w pozycji rule type wybierzesz opcję None, reguła będzie nieważna i nie będzie można skonfigurować analizy zachowania.
   - Można skonfigurować maksymalnie osiem pojedynczych reguł i dwie reguły połączone. W przypadku reguł połączonych obsługiwana jest detekcja przekroczenia linii, wtargnięcia, opuszczenia obszaru i wejścia w obszar.
6. Kliknij przycisk „**Save**“, aby zapisać ustawienia.
7. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia dla każdej reguły, i kliknij przycisk **Save** w celu zapisania ustawień.
8. Kliknij kartę **Linkage Method**, zaznacz pole wyboru odpowiedniego działania powiązanego dla poszczególnych reguł i kliknij przycisk **Save** w celu zapisania ustawień.

❖ **Konfiguracja zaawansowana**

Behavior Analysis Version: Wersja biblioteki algorytmów.

- **Parameter**

Skonfiguruj następujące parametry, aby szczegółowo określić konfigurację.



Rysunek 10–28 Konfiguracja zaawansowana

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

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

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 ustawienia: środek celu, dolna część celu i górna część celu. Przykład: 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 przeciwieństwie do lokalnego filtru rozmiarów w regule globalny filtr rozmiarów dotyczy wszystkich reguł.

  Kroki:

  1. Zaznacz pole wyboru **Global Size Filter**, aby włączyć tę funkcję.
  2. Wybierz ustawienie Actual Size lub Pixel opcji Filter Type.

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

  Uwagi:

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

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

  Uwagi:

  - Wyznaczony obszar zostanie skonwertowany na piksel przez algorytm tła.
  - Nie można skonfigurować globalnego filtru rozmiarów, jeżeli podgląd na żywo zostanie zatrzymany.
  - Długość/szerokość rozmiaru maksymalnego powinna być większa niż długość/szerokość rozmiaru minimalnego.

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

10.3.2 Wykonywanie zdjęć twarzy

Kamera może wykonać zdjęcie twarzy w skonfigurowanym obszarze i przekazać z tym zdjęciem informacje dotyczące wykrytej osoby, takie jak wiek i płeć.

❖ **Nakładka i wykonywanie zdjęć**

Informacje mogą być wyświetlane na zdjęciach i strumieniu.

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

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

Snapshot Setting: Wybierz jakość wykonanego zdjęcia. Dostępne są ustawienia Good, Better i Best.

Background Upload: Zaznacz pole wyboru przekazywania tła, jeżeli chcesz przekazać również zdjęcie tła.

❖ **Chroniony obszar**

Ta funkcja umożliwia wyznaczenie obszaru chronionego, w którym zdjęcia twarzy nie będą wykonywane. Obsługiwane są maksymalnie cztery obszary chronione.

Kroki:

1. Kliknij symbol sześciokąta  , aby wyznaczyć obszar chroniony, klikając punkty końcowe lewym przyciskiem myszy w podglądzie na żywo, i kliknij prawym przyciskiem w celu zakończenia wyznaczania obszaru.

Uwagi:

- Obsługiwany jest wielokątny obszar o 4–10 bokach.
- Aby usunąć wyznaczone obszary, należy kliknąć przycisk  .
- Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć obszarów chronionych.

Rysunek 10–29 Wyznaczanie obszaru chronionego

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

❖ **Reguła**

Kroki:

1. Zaznacz pole wyboru **Rule**, aby włączyć obsługę reguł wykonywania zdjęć twarzy.
2. Kliknij symbol prostokąta , aby wyznaczyć minimalną odległość źrenic. Odległość źrenic zostanie wyświetlona w polu poniżej podglądu na żywo. Minimalna odległość źrenic określa rozmiar prostokątnego obszaru między źrenicami i jest podstawowym parametrem identyfikowania celu przez kamerę.
3. Kliknij symbol sześciokąta , aby wyznaczyć obszar detekcji, w którym będą wykonywane zdjęcia twarzy. Wyznacz obszar, klikając punkty końcowe lewym przyciskiem myszy w podglądzie na żywo, i kliknij prawym przyciskiem w celu zakończenia wyznaczania obszaru.

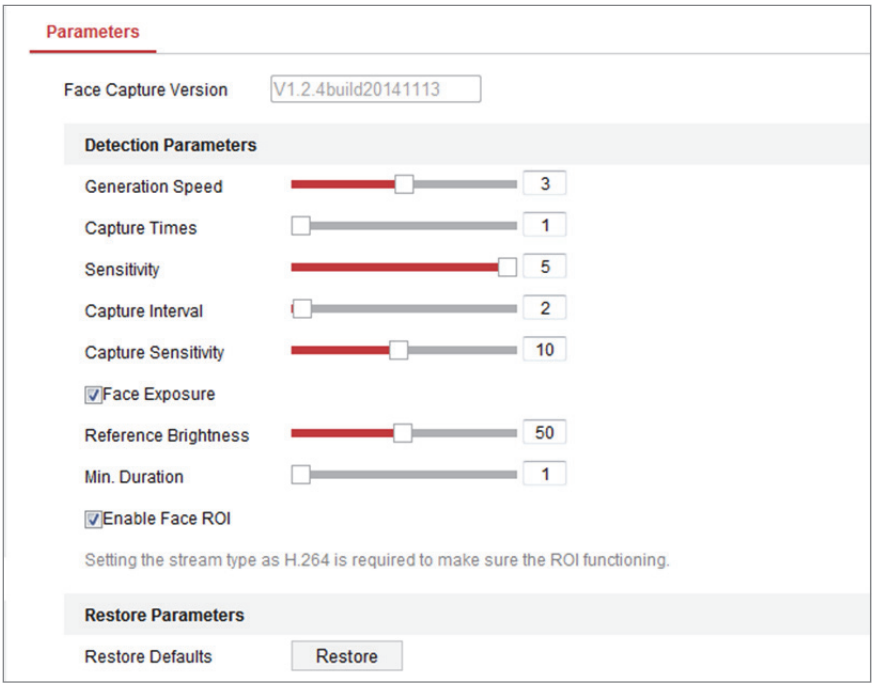
   Uwagi:

   - Obsługiwany jest wielokątny obszar o 4–10 bokach.
   - Jeżeli podgląd na żywo zostanie zatrzymany, nie można wyznaczyć konfigurowanego obszaru.
4. Kliknij przycisk „**Save**“, aby zapisać ustawienia.

❖ Konfiguracja zaawansowana

Face Capture Version: Wersja biblioteki algorytmów.

Należy skonfigurować następujące parametry zgodnie z rzeczywistym środowiskiem.



Rysunek 10–30 Zaawansowana konfiguracja wykonywania zdjęć twarzy

Parametry detekcji:

Generation Speed [1~5]: Szybkość identyfikowania celu. Im wyższa wartość, tym szybciej cel będzie rozpoznawany. Jeżeli zostanie ustawiona niska wartość, zdjęcie twarzy wykrytej wcześniej w skonfigurowanym obszarze nie zostanie wykonane. Umożliwia to ograniczenie wykrywania twarzy na grafice ściennej lub plakatach. Zalecana jest wartość domyślna 3.

Capture Times [1~10]: Liczba wykonywanych zdjęć twarzy wykrytej w skonfigurowanym obszarze. Domyślna wartość to 1.

Sensitivity [1~5]: Czułość identyfikacji celu. Im wyższa wartość, tym łatwiej twarz jest wykrywana, jednak liczba nieuzasadnionych alertów jest większa. Zalecana jest wartość domyślna 3.

Capture Interval [1–255 klatek]: Interwał ramek dla funkcji wykonywania zdjęć. Jeżeli zostanie ustawiona wartość domyślna 1, kamera wykonuje zdjęcie twarzy w każdej ramce.

Capture Sensitivity [0~20]: Wartość progowa dla uznania celu za twarz przez kamerę. Kamera będzie uznawać cel za twarz pod warunkiem, że liczba punktów wynikająca z algorytmu jest co najmniej równa tej wartości. Zalecana jest wartość domyślna 2.

Zaawansowane parametry wykonywania zdjęć twarzy:

Face Exposure: Zaznacz pole wyboru, aby włączyć funkcję ekspozycji twarzy.

Reference Brightness [0~100]: Referencyjna jasność twarzy w trybie ekspozycji twarzy. Jeżeli zostanie wykryta twarz, kamera dostosowuje jasność twarzy zgodnie z ustawioną wartością. Im wyższa wartość, tym większa jasność twarzy.

Minimum Duration [1–60 min]: Minimalny czas trwania ekspozycji twarzy w kamerze. Wartość domyślna to 1 minuta.

Uwaga: Jeżeli funkcja ekspozycji twarzy jest włączona, należy upewnić się, że funkcja WDR jest wyłączona i wybrano ręczną regulację przysłony.

Enable Face ROI: Twarz, której zdjęcie wykonuje kamera, jest regionem zainteresowania, w którym jakość obrazu jest wyższa.

Restore Default: Kliknij przycisk **Restore**, aby przywrócić fabryczne ustawienia domyślne wszystkich parametrów uwzględnionych w konfiguracji zaawansowanej.

10.3.3 Zliczanie osób

Cel:

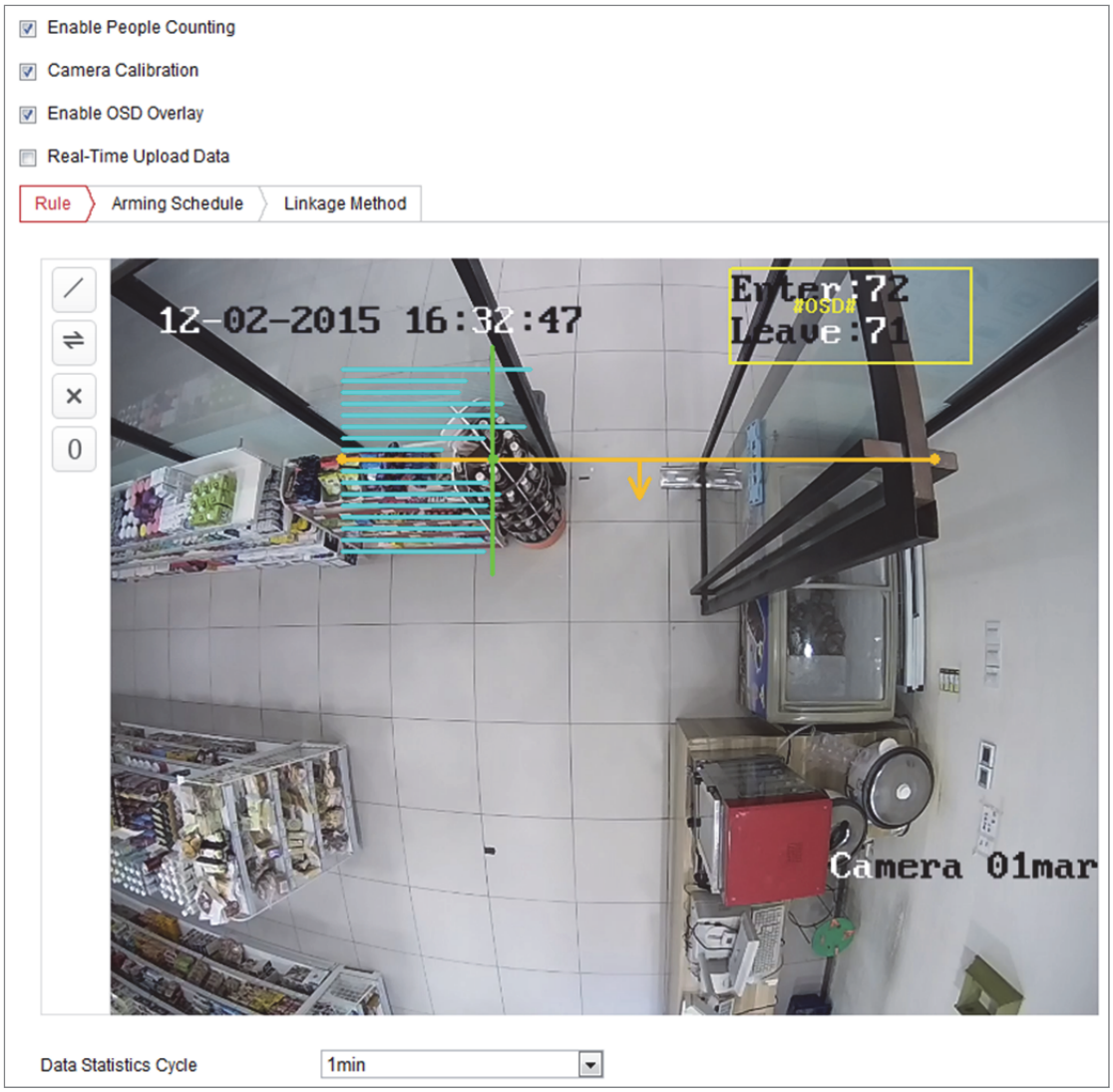
Ta funkcja umożliwia obliczenie liczby osób wchodzących w skonfigurowany obszar lub opuszczających ten obszar i jest powszechnie stosowana w wejściach lub wyjściach.

Uwagi:

Zalecane jest zainstalowanie kamery bezpośrednio ponad wejściem/wyjściem. Aby zapewnić lepszą dokładność zliczania, należy zainstalować kamerę poziomo.

Kroki:

1. Wyświetl okno Konfiguracja zliczania: **Configuration > People Counting**.



Rysunek 10–31 Konfiguracja zliczania osób

2. Zaznacz pole wyboru **Enable People Counting**, aby włączyć tę funkcję.
3. Wyznacz linię detekcji.

   Można wyznaczyć pomarańczową linię detekcji w podglądzie na żywo. Obiekty przekraczające tę linię w dowolnym kierunku będą wykrywane i zliczane.

   1) Kliknij przycisk po lewej stronie w podglądzie na żywo. Pomarańczowa linia zostanie wyświetlona na obrazie.
   2) Przeciągnij linię detekcji, aby dostosować jej położenie.
   3) Przeciągnij żółte punkty końcowe linii detekcji, aby dostosować jej długość.

      Uwaga:

      - Linię detekcji należy wyznaczyć bezpośrednio poniżej kamery, tak aby obejmowała całe wejście/wyjście.

- Nie wolno umieszczać linii w miejscu, w którym ludzie mogą pozostawać przez pewien czas.

4) Można kliknąć przycisk ✕, aby usunąć linię detekcji.
5) Można kliknąć przycisk ⇌, aby zmienić kierunek. Żółta strzałka wskazuje kierunek wejścia.

4. Zaznacz pole wyboru **Camera Calibration**, aby włączyć funkcję kalibracji kamery. W podglądzie obrazu na żywo wyświetlana jest zielona pionowa linia kalibracji i kilka niebieskich linii poziomych.

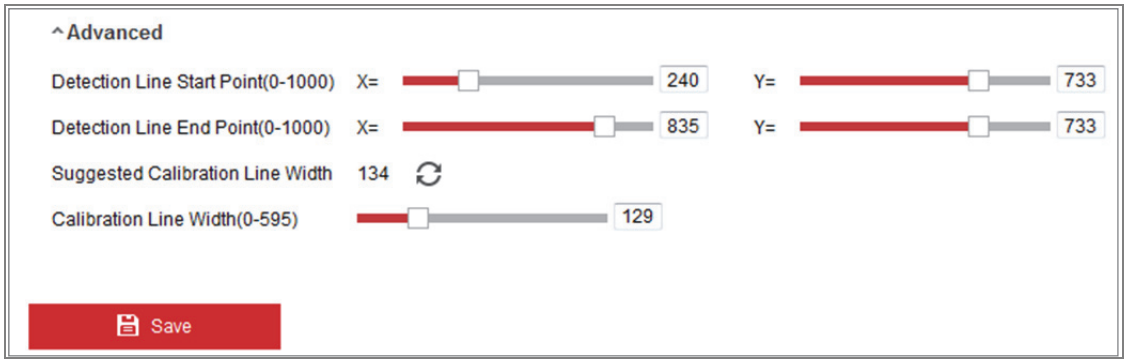
   Camera Calibration: Ustaw szerokość (zazwyczaj szerokość w ramionach) dla funkcji zliczania osób. Prawidłowo skonfigurowane parametry kalibracji zapewniają większą dokładność zliczania.

   Blue Horizontal Lines: Pojedyncza niebieska linia wskazuje szerokość detekcji (zazwyczaj szerokość w ramionach) przechodzącej osoby. Można wyświetlić maksymalnie osiem niebieskich linii po obu stronach linii detekcji. Te linie stanowią odniesienie dla ustawienia kalibracyjnego.

   Calibration Line (zielona linia pionowa): Odległość od lewego punktu końcowego do tej linii (szerokość linii kalibracyjnej) oznacza skonfigurowaną szerokość sylwetki osoby. Można przeciągnąć linię kalibracyjną, aby dostosować odległość zgodnie z rozmieszczeniem niebieskiej linii.

   Advanced: Można precyzyjnie dostosować rozmiar linii detekcji i linii kalibracyjnej.

   1) Przeciągnij wskaźniki lub wprowadź wartości w polach tekstowych, aby skonfigurować Punkt początkowy linii detekcji i Punkt końcowy linii detekcji.
   2) Kliknij przycisk ↻, aby odświeżyć proponowaną szerokość linii kalibracyjnej, obliczoną automatycznie przez system.
   3) Przeciągnij wskaźnik lub wprowadź wartość, aby ustawić szerokość linii kalibracyjnej. Można zaakceptować proponowaną wartość lub zmienić ją zgodnie z wymaganiami.



Rysunek 10–32 Zaawansowana konfiguracja zliczania osób

5. Konfigurowanie i wyświetlanie danych zliczania.
   1) Po zaznaczeniu pola wyboru **Enable OSD Overlay** liczba osób wchodzących i wychodzących będzie wyświetlana w podglądzie na żywo i aktualizowana w czasie rzeczywistym.
   2) Można przeciągnąć ramkę tekstu OSD, aby dostosować jej położenie zgodnie z wymaganiami.
   3) Jeżeli chcesz przekazywać dane zliczania w czasie rzeczywistym, zaznacz pole wyboru **Real-Time Upload Data**.
   4) Jeżeli chcesz ręcznie ustawić cykl zliczania, wybierz przedział czasowy z listy rozwijanej **Data Statistics Cycle**.
   5) Aby zresetować licznik, kliknij przycisk 0 po lewej stronie w podglądzie na żywo.
6. Kliknij kartę **Arming Schedule**, aby skonfigurować harmonogram zabezpieczenia. Zobacz *Zadanie 2: Ustawianie harmonogramu uzbrajania dla funkcji detekcji ruchu* w *sekcji 10.1.1*.
7. Kliknij kartę **Linkage Method**, aby wybrać działanie powiązane. Zobacz *Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu* w *sekcji 10.1.1*.
8. Kliknij **Save**, aby zapisać ustawienia.

Uwaga:

Statystyki zliczania osób są obliczane na karcie **Application**. Przejdź do sekcji **Application**, aby sprawdzić statystyki zliczania osób.

10.3.4 Zliczanie

Ta funkcja umożliwia obliczenie liczby osób wchodzących w skonfigurowany obszar lub opuszczających ten obszar i jest powszechnie stosowana w wejściach lub wyjściach.

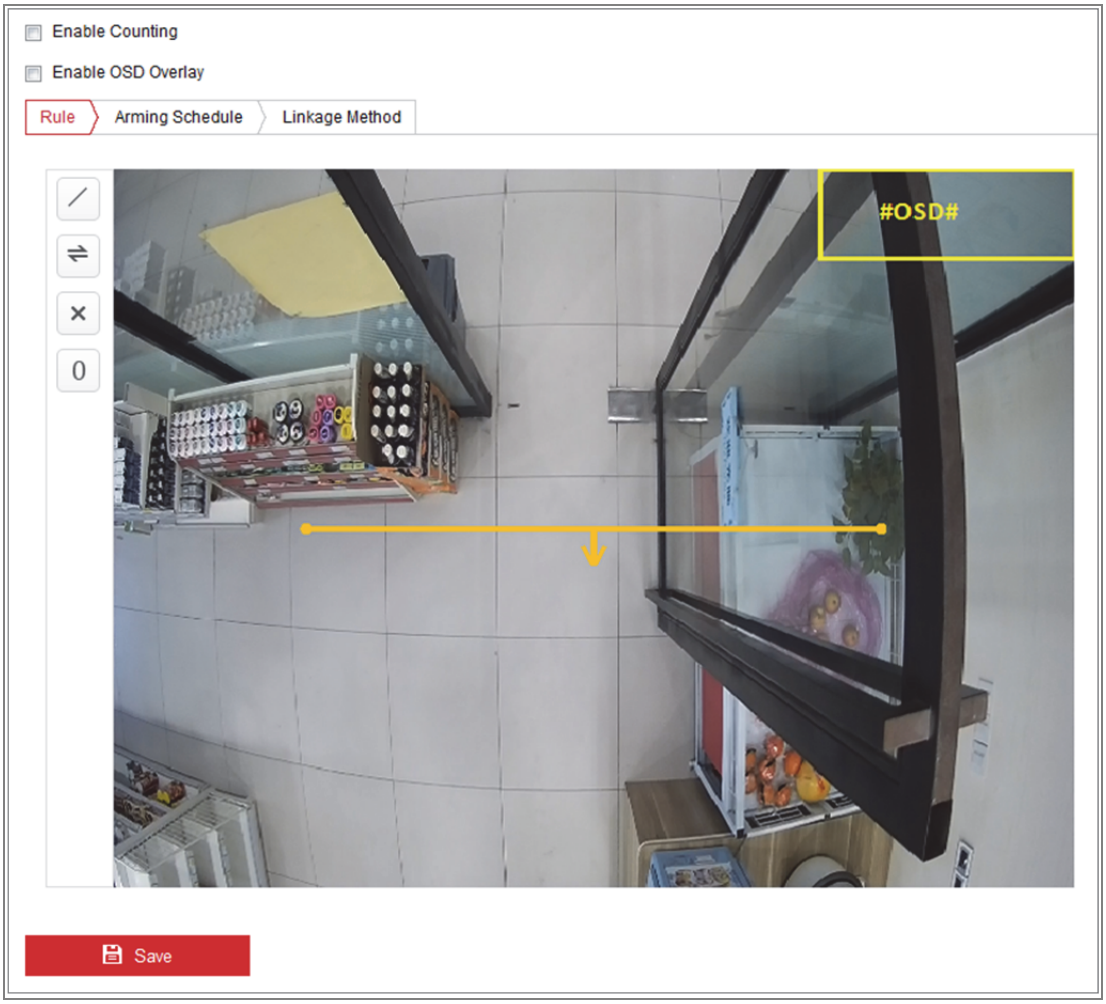
W przeciwieństwie do funkcji kamery iDS ta funkcja zliczania osób nie wymaga kalibracji kamery.

Uwagi:

Zalecane jest zainstalowanie kamery bezpośrednio ponad wejściem/wyjściem i upewnienie się, że jest ustawiona poziomo, ponieważ zapewnia to większą dokładność zliczania.

Kroki:

1. Wyświetl okno Konfiguracja zliczania: **Configuration > Counting**.



Rysunek 10–33 Konfiguracja zliczania

2. Zaznacz pole wyboru **Enable Counting**, aby włączyć tę funkcję.
3. Po zaznaczeniu pola wyboru **Enable OSD Overlay** liczba osób wchodzących i wychodzących będzie wyświetlana w podglądzie wideo na żywo i aktualizowana w czasie rzeczywistym.
4. Wyznacz linię detekcji.

   Można wyznaczyć pomarańczową linię detekcji w podglądzie na żywo. Obiekty przekraczające tę linię w dowolnym kierunku będą wykrywane i zliczane.

   1) Kliknij przycisk , aby wyznaczyć pomarańczową linię detekcji, która będzie wyświetlana na obrazie.

      Uwaga:

      - Linię detekcji należy wyznaczyć bezpośrednio poniżej kamery, tak aby obejmowała całe wejście/wyjście.
      - Wyznacz linię detekcji w lokalizacji, w której ludzie zazwyczaj nie pozostają przez pewien czas.

   2) Kliknij i przeciągnij linię detekcji, aby dostosować jej położenie.
   3) Kliknij i przeciągnij dwa punkty końcowe linii detekcji, aby dostosować jej długość.
   4) Kliknij przycisk , aby usunąć linię detekcji.
   5) Kliknij przycisk , aby zmienić kierunek.
5. Kliknij przycisk 0 , aby wyzerować liczbą wchodzących i wychodzących osób.
6. Kliknij kartę **Arming Schedule**, aby wyświetlić harmonogram zabezpieczenia, a następnie kliknij myszą i przeciągnij jej wskaźnik na pasku czasu w celu ustawienia godziny.
7. Kliknij kartę **Linkage Method**, aby wybrać działanie powiązane.
8. Kliknij **Save**, aby zapisać ustawienia.

Uwaga:

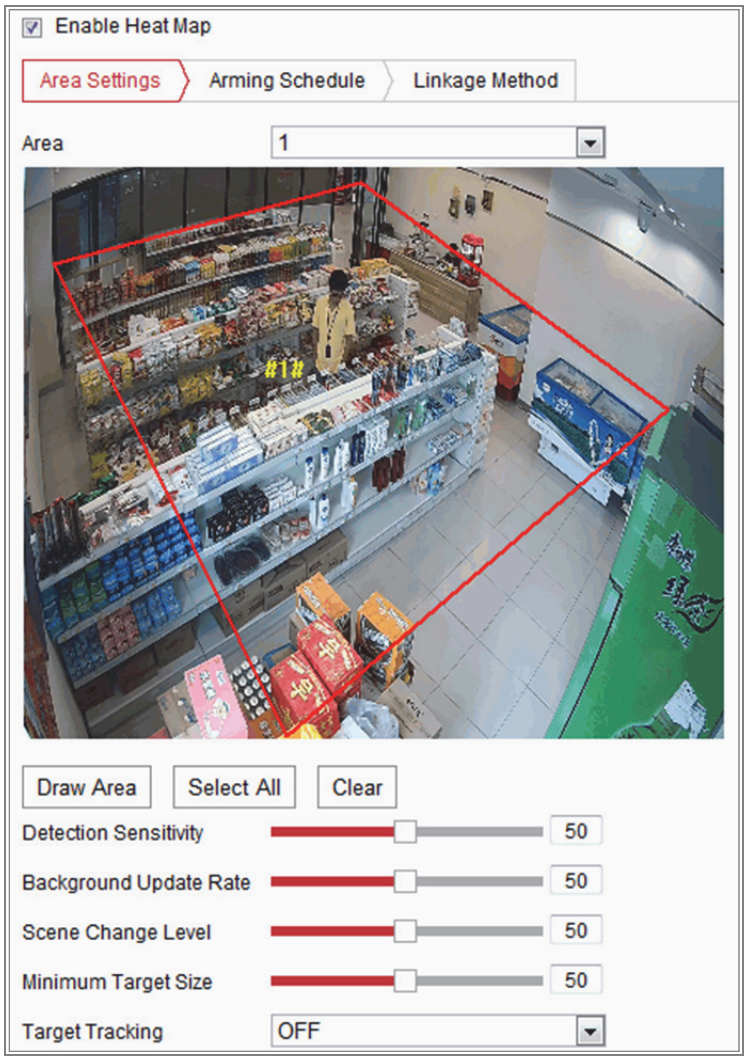
Statystyki zliczania są obliczane na karcie **Application**. Przejdź do sekcji **Application**, aby sprawdzić statystyki zliczania.

10.3.5 Kolorowa mapa danych

Kolorowa mapa danych przedstawia w formie graficznej dane wyróżnione kolorami. Funkcja kolorowej mapy danych kamery jest zazwyczaj używana do analizowania godzin odwiedzin i czasu przebywania klientów w wyznaczonym obszarze.

Kroki:

1. Wyświetl okno konfiguracji Kolorowa mapa danych: **Configuration > Heat Map**.



Rysunek 10–34 Konfiguracja mapy danych

2. Zaznacz pole wyboru **Enable Heat Map**, aby włączyć tę funkcję.
3. Przejdź do sekcji **Area Settings**, aby wyznaczyć obszar detekcji. Wyznacz obszar, klikając punkty końcowe lewym przyciskiem myszy w podglądzie na żywo, i kliknij prawym przyciskiem w celu zakończenia wyznaczania obszaru. Można skonfigurować maksymalnie osiem obszarów.

Uwaga: Można kliknąć przycisk **Select All**, aby wybrać całe okno podglądu na żywo jako skonfigurowany obszar. Można też kliknąć przycisk **Delete**, aby usunąć bieżący wyznaczony obszar.

4. Skonfiguruj parametry wyznaczonego obszaru.

   Detection Sensitivity [0~100]: Czułość identyfikacji celu przez kamerę. Nadmierna czułość może powodować zgłaszanie nieuzasadnionych alertów. Zalecane jest ustawienie domyślnej czułości 50.

   Background Update Rate [0~100]: Szybkość zastępowania poprzedniej sceny nową sceną. Przykład: osoby znajdujące się obok regału są zliczane podwójnie, jeżeli towary zostaną usunięte z regału i kamera uzna zmianę obrazu regału za nową scenę. Zalecana jest wartość domyślna 50.

   Scene Change Level [0~100]: Poziom szybkości reagowania kamery na dynamicznie zmieniające się otoczenie takie jak kołyszące się zasłony. Kamera może uznać kołyszące się zasłony za cel. Jeżeli ten poziom zostanie ustawiony prawidłowo, nie będą zgłaszane nieuzasadnione alerty. Poziom domyślny to 50.

   Minimum Target Size [0~100]: Rozmiar celu identyfikowanego przez kamerę. Można ustawić rozmiar celu zgodnie z rzeczywistym otoczeniem. Rozmiar domyślny to 50.

   Target Track: Wybierz ustawienie ON lub OFF, aby włączyć lub wyłączyć funkcję śledzenia celu.

5. Przejdź do karty **Arming Schedule**, a następnie przeciągnij wskaźnik myszy na pasku czasu, aby ustawić harmonogram uzbrajania.
6. Przejdź do karty **Linkage Method** i wybierz powiązane działanie, zaznaczając pole wyboru Notify Surveillance Center.
7. Kliknij **Save**, aby zapisać ustawienia.

Uwaga:

Statystyki kolorowej mapy danych są obliczane na karcie Aplikacja. Przejdź do sekcji Aplikacja, aby sprawdzić statystyki kolorowej mapy danych.

10.3.6 Ruch drogowy

Cel:

Dostępne są ustawienia Vehicle Detection i Mixed-traffic Detection monitorowania ruchu drogowego. W trybie Vehicle Detection można wykryć przejeżdżający pojazd i wykonywać zdjęcie jego tablicy rejestracyjnej. Mogą być również automatycznie rejestrowane informacje takie jak kolor i logo pojazdu. W trybie Mieszana detekcja ruchu drogowego można wykryć pieszego, pojazd silnikowy i pojazd niesilnikowy i wykonać jego zdjęcie (pieszy, pojazd niesilnikowy lub pojazd silnikowy bez tablicy rejestracyjnej) albo zdjęcie jego tablicy rejestracyjnej (pojazd silnikowy z tablicą rejestracyjną). Można wysłać sygnał alarmowy w celu powiadomienia centrum monitoringu i przekazać wykonane zdjęcie do serwera FTP.

Uwaga: Funkcja monitorowania ruchu drogowego jest zależna od modelu kamery.

- **Konfiguracja detekcji**

Kroki:

1. Wybierz rodzaj detekcji z listy. Dostępne są ustawienia Vehicle Detection i Mixed-traffic Detection.

   Uwaga: Aby aktywować nowe ustawienia podczas przełączania rodzaju detekcji ruchu drogowego, należy ponownie uruchomić urządzenie.
2. Zaznacz pole wyboru Enable, aby włączyć wybraną funkcję detekcji.
3. Wybierz numer pasa z odpowiedniej listy rozwijanej. Dostępne są cztery ścieżki do wyboru.
4. Kliknij i przeciągnij linię pasa do żądanego położenia lub kliknij i przeciągnij zakończenie linii, aby dostosować długość i kąt linii.
5. Dostosuj współczynnik powiększenia dla kamery, tak aby przybliżyć widok w czerwonej ramce. Można dostosować tylko położenie czerwonej ramki.

   Uwaga: Dla każdego pasa można wykonać zdjęcie tylko jednej tablicy rejestracyjnej w danej chwili.
6. Wybierz z listy rozwijanej Skrót nazwy województwa używany, gdy nie można rozpoznać tablicy rejestracyjnej.

7. Skonfiguruj harmonogram zabezpieczenia.
   1) Kliknij kartę Arming Schedule, aby wyświetlić harmonogram uzbrajania.
   2) Kliknij pasek czasu i przeciągnij wskaźnik myszy, aby wybrać przedział czasowy. Kliknij przycisk Delete lub Delete All, aby usunąć skonfigurowany harmonogram.
   3) Przesuń wskaźnik myszy do końca każdego dnia, aby wyświetlić okno dialogowe umożliwiające skopiowanie bieżących ustawień do innych dni.
   4) Kliknij przycisk „Save“, aby zapisać ustawienia.

   Uwaga: Przedziały nie mogą na siebie zachodzić. Dla każdego dnia można skonfigurować maksymalnie osiem przedziałów czasowych.
8. Skonfiguruj powiązane działanie. Dostępne są ustawienia Notify Surveillance Center i Upload to FTP/Memory Card/NAS.
   - **Notify Surveillance Center:** W chwili wystąpienia zdarzenia sygnał alarmowy lub nietypowy sygnał jest przesyłany do zdalnego oprogramowania do zarządzania monitoringiem.
   - **Upload to FTP/Memory Card/NAS:** W momencie wyzwolenia alarmu wykonywane jest zdjęcie, które jest następnie przesyłane na serwer FTP. Zdjęcie można zapisać na lokalnej karcie SD lub podłączonym dysku NAS.
9. Kliknij przycisk Save, aby aktywować ustawienia.

Rozdział 11 Ustawienia magazynowania nagrań i zdjęć

Zanim rozpoczniesz:

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

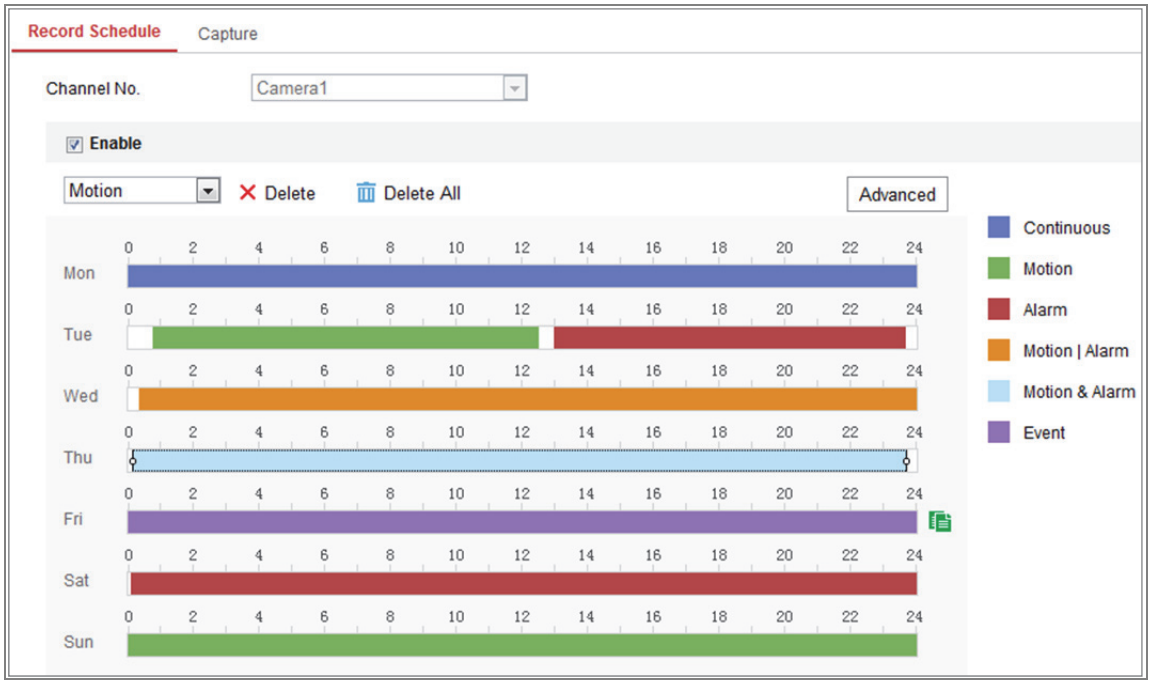
11.1 Konfigurowanie harmonogramu nagrywania

Cel:

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

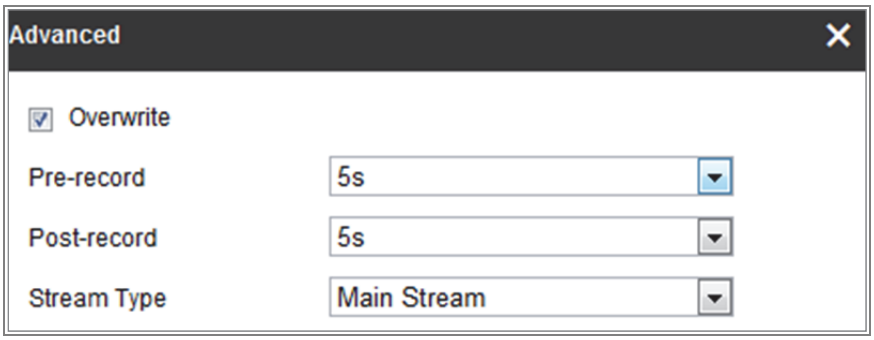
Kroki:

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



Rysunek 11–1 Harmonogram nagrywania

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



Rysunek 11–2 Parametry nagrywania

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

  Dostępne ustawienia nagrywania z wyprzedzeniem to No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s lub Not limited.
- Post-record: Funkcja ta służy do przedłużenia nagrywania po zdarzeniu lub po zakończeniu ustawionego za pomocą harmonogramu okresu nagrywania. Jeżeli na przykład alarm wyzwolił nagrywanie o godz. 11:00 i skonfigurowano czas nagrywania z opóźnieniem 5 sekund, kamera będzie nagrywać do godz. 11:00:05.

  Dostępne ustawienia nagrywania z opóźnieniem to 5s, 10s, 30s, 1 min, 2 min, 5 min lub 10 min.
- Stream Type: Wybierz typ strumienia do nagrywania.

Uwaga: Konfiguracje parametrów nagrywania są zależne od modelu kamery.

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

- **Nieprzerwane**

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

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

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

  Oprócz konfigurowania harmonogramu nagrywania należy ustawić obszar detekcji ruchu i zaznaczyć pole wyboru Trigger Channel w pozycji Linkage Method w oknie ustawień detekcji ruchu. Aby uzyskać więcej informacji, zobacz ***Zadanie 1: Ustawianie obszaru detekcji ruchu*** w *sekcji 10.1.1.*

- **Nagrywanie wyzwalane przez alarm**

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

  Aby korzystać z tej funkcji, oprócz harmonogramu nagrywania należy także ustawić parametr **Alarm Type** i zaznaczyć pole wyboru **Trigger Channel** na karcie **Linkage Method** w oknie **Ustawienia wejść alarmowych**. Aby uzyskać więcej informacji, zobacz *sekcję 10.1.3*.

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

  Jeżeli wybrano ustawienie **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 więcej informacji, zobacz *sekcje 10.1.1* i *10.1.3*.

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

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

  Aby móc skorzystać z tej funkcji, oprócz harmonogramu nagrywania należy także skonfigurować ustawienia w interfejsie **detekcji ruchu** i **ustawień wejścia alarmu**. Aby uzyskać więcej informacji, zobacz *sekcje 10.1.1* i *10.1.3*.

- **Nagrywanie wyzwalane po wystąpieniu zdarzeń**

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

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

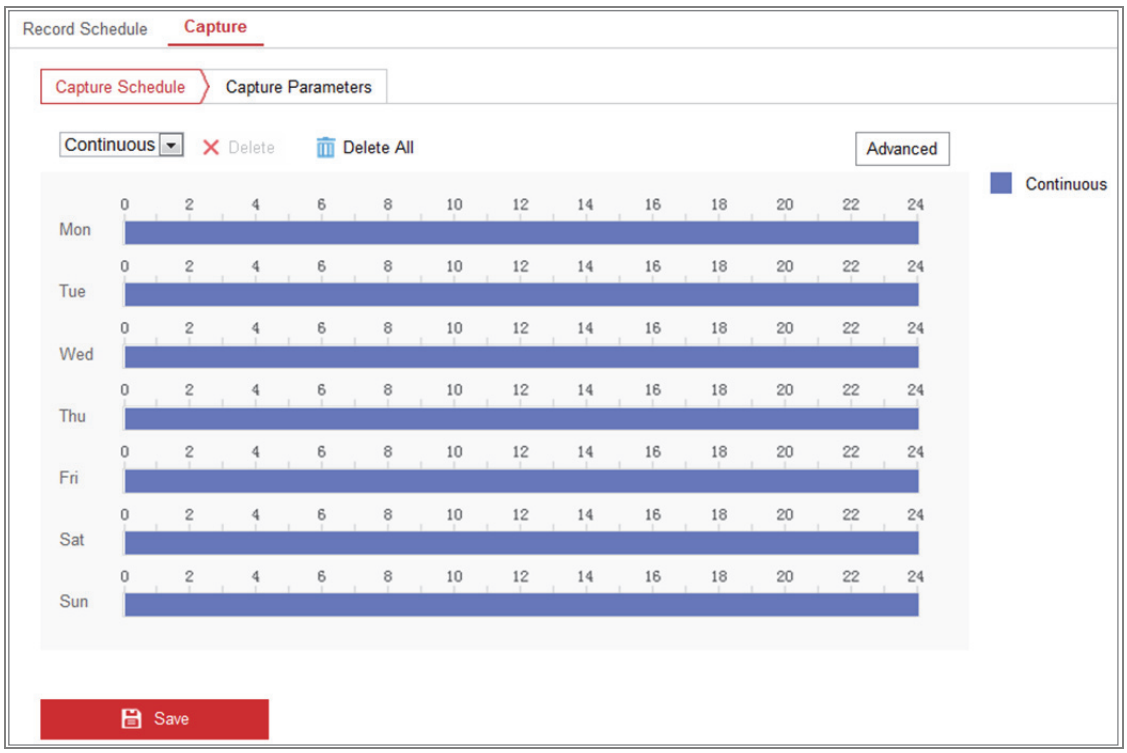
11.2 Konfigurowanie harmonogramu wykonywania zdjęć

Cel:

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

Kroki:

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

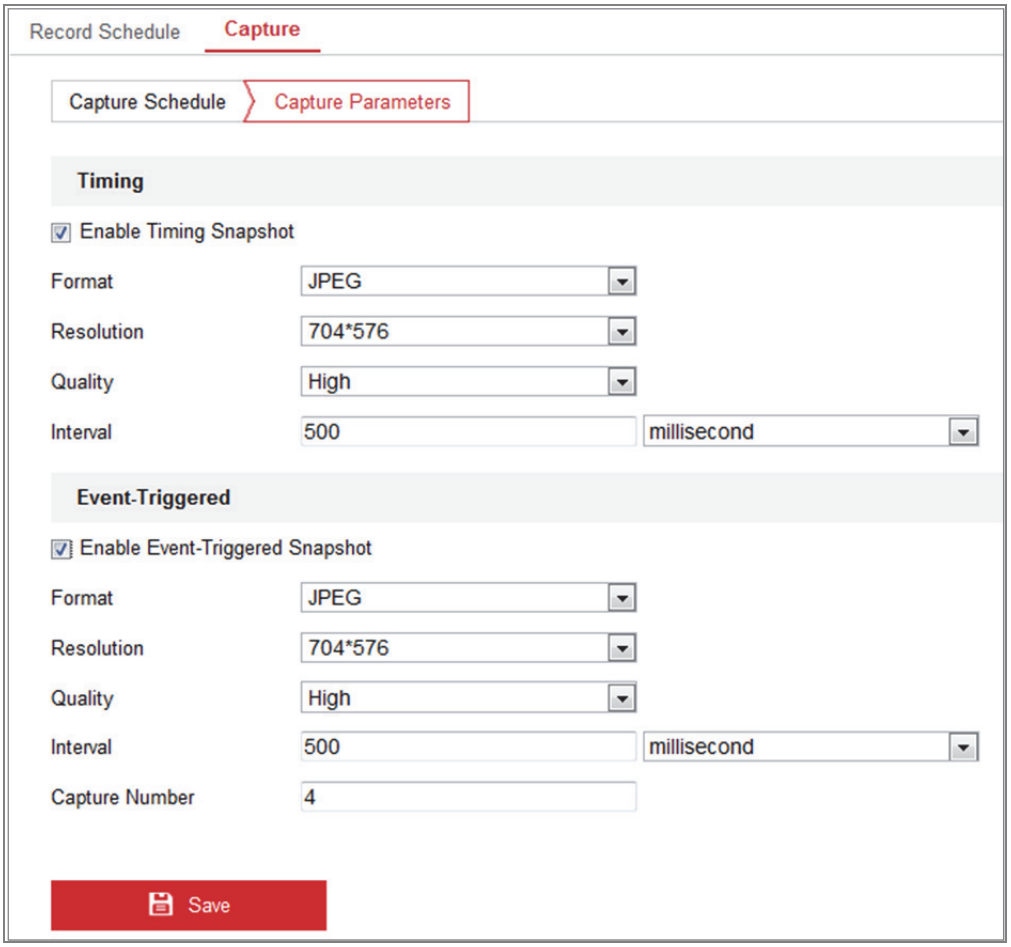


Rysunek 11–3 Konfiguracja wykonywania zdjęć

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

Rysunek 11–4 Zaawansowane ustawienia harmonogramu wykonywania zdjęć

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



Rysunek 11–5 Ustawianie parametrów wykonywania zdjęć

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

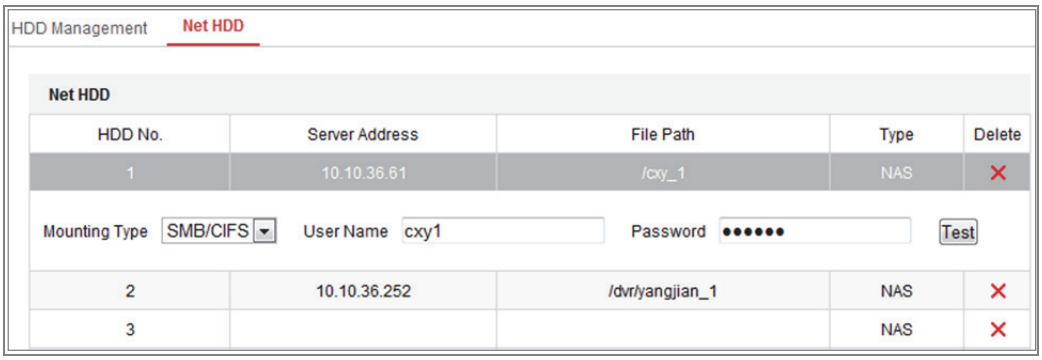
11.3 Konfigurowanie sieciowego dysku HDD

Zanim rozpoczniesz:

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

Kroki:

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



Rysunek 11–6 Dodawanie dysku sieciowego

(2) Wprowadź adres IP dysku sieciowego i ścieżkę plików.

(3) Wybierz typ protokołu udostępniania. Dostępne opcje to „NFS“ i „SMB/CIFS“. Jeżeli zostanie wybrane ustawienie SMB/CIFS, można skonfigurować nazwę użytkownika i hasło, aby zapewnić ochronę.

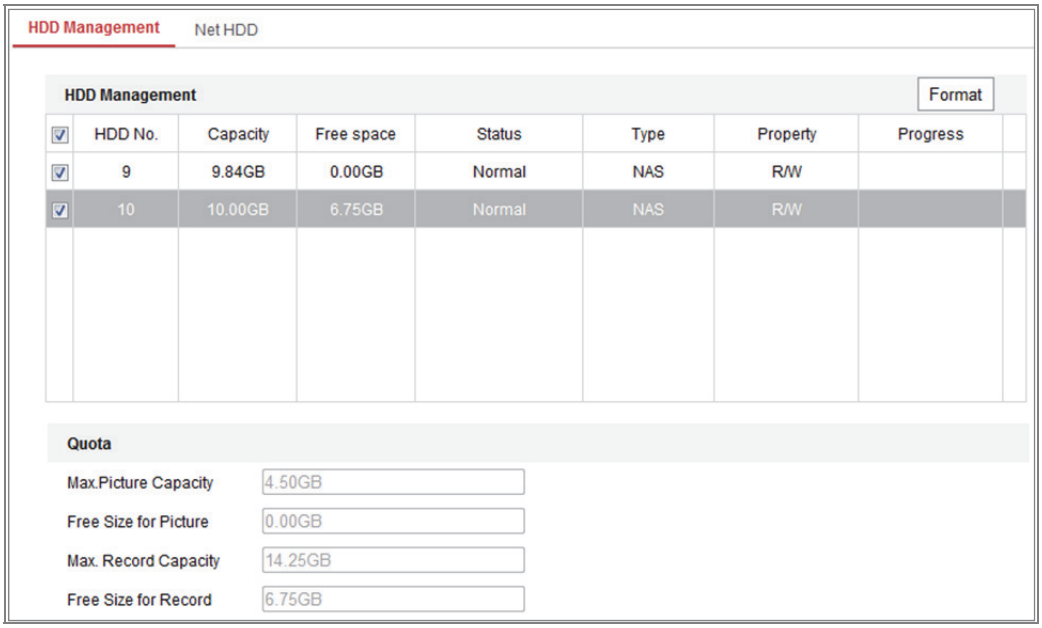
Uwaga: Aby uzyskać informacje o tworzeniu ścieżki zapisu plików, należy zapoznać się z *Instrukcją obsługi urządzeń magazynujących dołączonych do sieci (NAS)*.

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

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

2. Inicjowanie dodanego dysku sieciowego

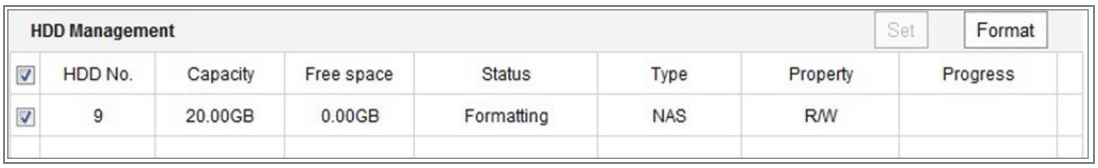
(1) Przejdź do interfejsu ustawień dysku HDD, wybierając opcje: **„Configuration“ > „Storage“ > „Storage Management“ > „HDD Management“**. W interfejsie tym wyświetlane są informacje o pojemności dysku, dostępnym wolnym miejscu, stanie, typie i właściwościach dysku.



Rysunek 11–7 Zarządzanie magazynem

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

Po zakończeniu inicjowania stan dysku zostanie zmieniony na **Normal**.

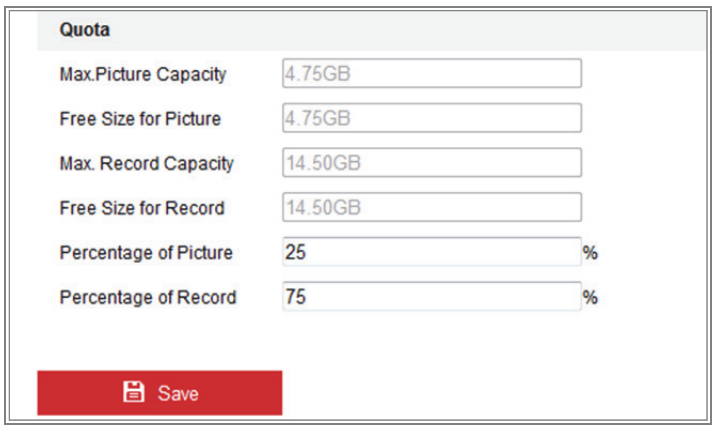


Rysunek 11–8 Wyświetlanie stanu dysku

3. Zdefiniuj przydział dla nagrywania i wykonywania zdjęć.

(1) Wprowadź procentową wartość przydziału magazynowania nagrań i zdjęć.

(2) Kliknij przycisk „**Save**“ i odśwież stronę przeglądarki, aby aktywować ustawienia.



Rysunek 11–9 Ustawienia przydziału

Uwaga:

Do kamery można przyłączyć do 8 dysków NAS.

11.4 Detekcja karty pamięci

Cel:

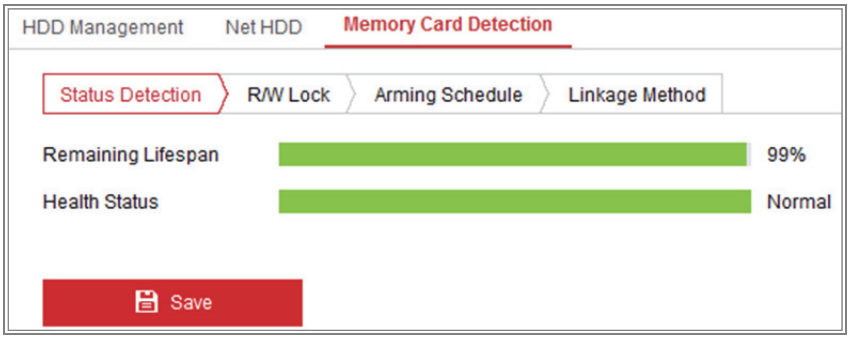
Funkcja detekcji karty pamięci umożliwia wyświetlanie informacji dotyczących stanu karty pamięci, blokowanie karty pamięci i powiadamianie o wykryciu usterki karty pamięci.

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

Kroki:

1. Wyświetl okno konfiguracji Detekcja karty pamięci:

   Configuration > Storage > Storage Management > Memory Card Detection



Rysunek 11–10 Detekcja karty pamięci

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

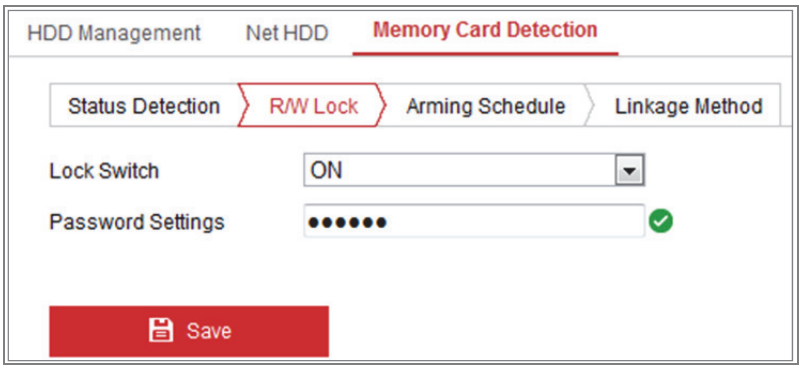
   Remaining Lifespan: Procentowo wyrażony pozostały czas przydatności do użytku. Czas przydatności karty do użytku jest zależny od czynników takich jak jej pojemność i szybkość transmisji bitów. Należy wymienić kartę pamięci, jeżeli zbliża się koniec okresu jej przydatności do użytku.

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

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

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

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



Rysunek 11–11 Ustawianie blokady odczytu/zapisu

- Dodanie blokady

(1) Wybierz z listy **Lock Switch** ustawienie ON.

(2) Wprowadź hasło.

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

- Odblokowanie

(1) Jeżeli kamera zablokuje zainstalowaną w niej kartę pamięci, odblokowanie następuje automatycznie, a użytkownicy nie muszą wykonywać żadnych czynności w celu odblokowania karty.

(2) Jeżeli karta pamięci (z blokadą) zostanie użyta w innej kamerze, można wyświetlić okno **HDD Management**, aby ręcznie odblokować kartę. Wybierz kartę pamięci i kliknij przycisk **Unlock** wyświetlany obok przycisku **Format**. Następnie wprowadź poprawne hasło, aby usunąć blokadę.

Uwagi:

- Kartę można odczytywać i zapisywać tylko po odblokowaniu.
- Jeżeli zostaną przywrócone ustawienia fabryczne kamery, która zablokowała kartę pamięci, można usunąć blokadę, korzystając z okna Zarządzanie dyskami twardymi.

- Usuwanie blokady

(1) Wybierz z listy **Lock Switch** ustawienie **OFF**.

(2) Wprowadź poprawne hasło w polu tekstowym **Password Settings**.

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

4. Skonfiguruj ustawienia **Arming Schedule** i **Linkage Method**, jeżeli chcesz otrzymać powiadomienie w przypadku zmiany stanu kondycji karty pamięci na stan inny niż „dobra”. Zobacz ***Zadanie 2: Ustawianie harmonogramu uzbrajania dla funkcji detekcji ruchu*** i ***Zadanie 3: Ustawianie działania powiązanego z detekcją ruchu*** w *sekcji 10.1.1.*
5. Kliknij przycisk **Save**, aby zapisać ustawienia.

11.5 Konfigurowanie Magazynowania uproszczonego

Cel:

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

Uwagi:

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

1. Wyświetl okno Magazynowanie uproszczone:

Configuration > Storage > Storage Management > Lite Storage

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

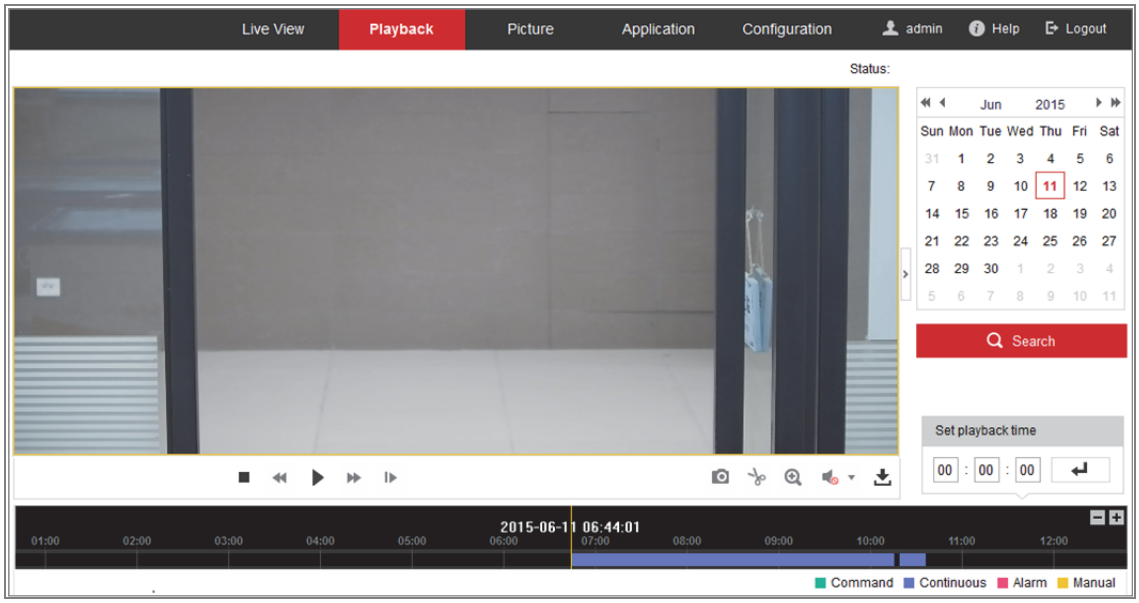
Rozdział 12 Odtwarzanie

Cel:

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

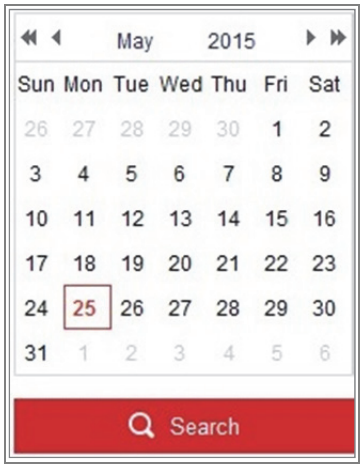
Kroki:

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



Rysunek 12–1 Okno odtwarzania

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



Rysunek 12–2 Wyszukiwanie plików wideo

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

Korzystając z paska narzędzi znajdującego się w dolnej części okna odtwarzania, można sterować procesem odtwarzania.

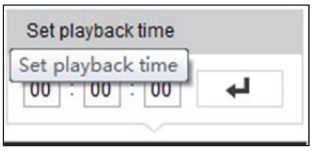
Rysunek 12–3 Pasek narzędzi odtwarzania

Tabela 12-1 Opis przycisków

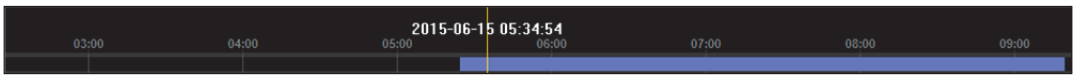
Przycisk	Opis	Przycisk	Opis
	Odtwarzanie		Rejestrowanie zdjęć
	Wstrzymanie	/	Rozpoczęcie/zakończenie przycinania plików wideo
	Zatrzymanie	/	Włączanie dźwięku i dostosowanie głośności/wyciszanie
	Zmniejszenie szybkości		Pobierz
	Zwiększenie szybkości		Odtwarzanie poklatkowe
/	Włączanie/wyłączanie cyfrowego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

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

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

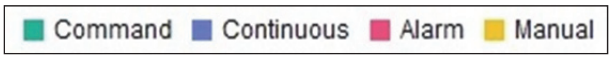


Rysunek 12–4 Ustawianie czasu odtwarzania



Rysunek 12–5 Pasek postępu

Typy wideo wyróżniono różnymi kolorami na pasku postępu.



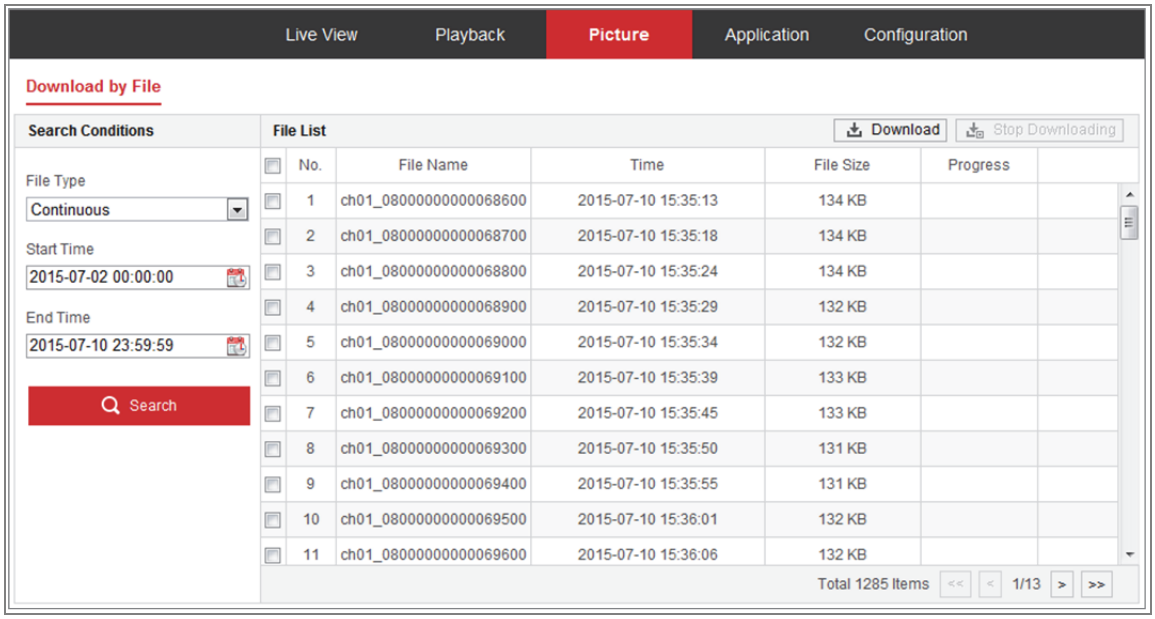
Rysunek 12–6 Typy wideo

Rozdział 13 Zdjęcia

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

Uwagi:

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



Rysunek 13–1 Wyszukiwanie zdjęć

Kroki:

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

Uwaga:

Za każdym razem można wyświetlić maksymalnie 4000 zdjęć.

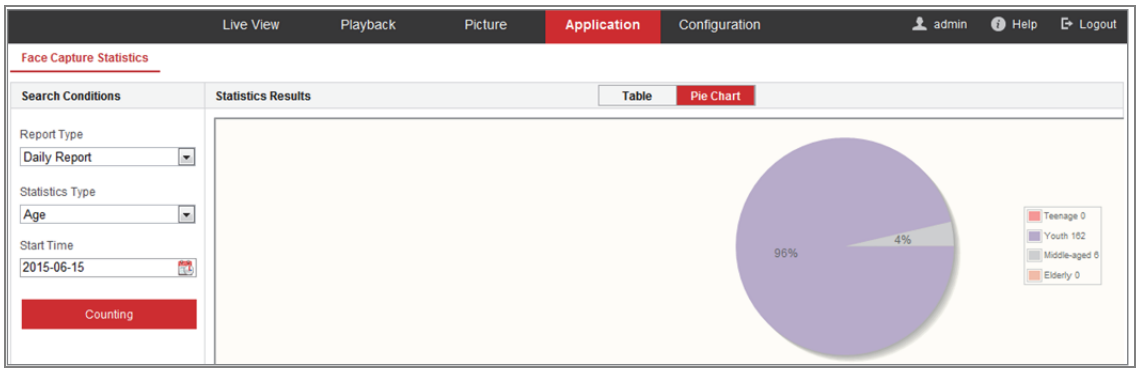
Rozdział 14 Aplikacja

Kliknij przycisk **Application**, aby wyświetlić okno zliczania statystycznego. Można wyszukiwać, wyświetlać i pobierać dane zliczania przechowywane w magazynie lokalnym lub sieciowym.

Uwaga: Funkcja Aplikacja jest zależna od modelu kamery.

14.1 Statystyki wykonywania zdjęć twarzy

Po włączeniu funkcji wykonywania zdjęć twarzy można wyświetlać i pobierać dane wykonanych zdjęć twarzy z karty aplikacji. Aby uzyskać bardziej zrozumiałe wyniki, można wyświetlić dane na różnych wykresach.



Rysunek 14–1 Okno aplikacji

Kroki:

1. Wybierz typ raportu. Dostępny jest raport dzienny, tygodniowy, miesięczny i roczny.
2. Wybierz typ statystyk.
3. Wybierz godzinę początkową i kliknij przycisk Counting.

   Wynik zliczania jest jest wyświetlany w obszarze wyników statystycznych. Kliknij przycisk Table lub Pie Chart, aby wyświetlić wynik w różnym formacie.

Uwaga: Jeżeli wyniki zliczania zostaną wyświetlone w tabeli, można wyeksportować dane do pliku programu Excel.

14.2 Statystyki zliczania osób

Po włączeniu funkcji zliczania osób można wyświetlać i pobierać dane zliczania osób z karty aplikacji. Aby uzyskać bardziej zrozumiałe wyniki, można wyświetlić dane na różnych wykresach.

Kroki:

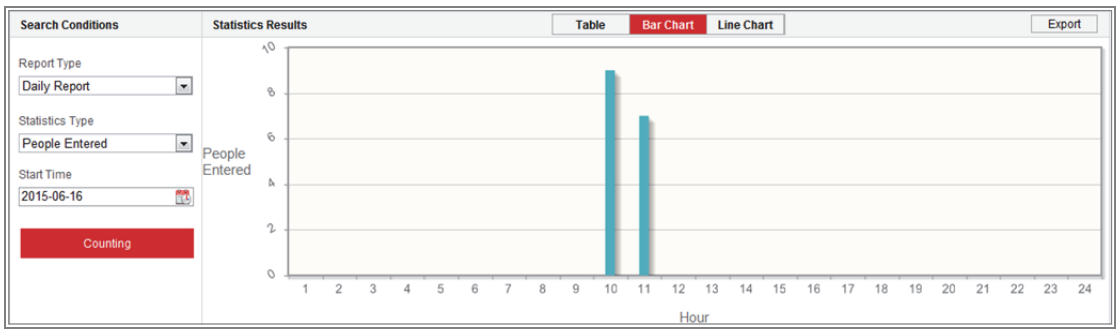
1. Wybierz typ raportu. Dostępny jest raport dzienny, tygodniowy, miesięczny i roczny.

   Uwaga: Raport dzienny umożliwia obliczenie danych dla wybranego dnia. Raport tygodniowy umożliwia wykonanie obliczeń dla tygodnia, do którego należy wybrana data. Raport miesięczny umożliwia wykonanie obliczeń dla miesiąca, do którego należy wybrana data. Raport roczny umożliwia wykonanie obliczeń dla roku, do którego należy wybrana data.

2. Wybierz typ statystyk. Dostępne są ustawienia People Entered i People Exited.
3. Wybierz godzinę początkową i kliknij przycisk Counting.

   Wynik zliczania jest jest wyświetlany w obszarze wyników statystycznych. Kliknij przycisk Table, Bar Chart lub Line Chart, aby wyświetlić wynik w różnym formacie.

   Uwaga: Jeżeli statystyki zostaną wyświetlone w tabeli, dostępny jest przycisk **Export** umożliwiający wyeksportowanie danych do pliku programu Excel.



Rysunek 14–2 Zliczanie osób

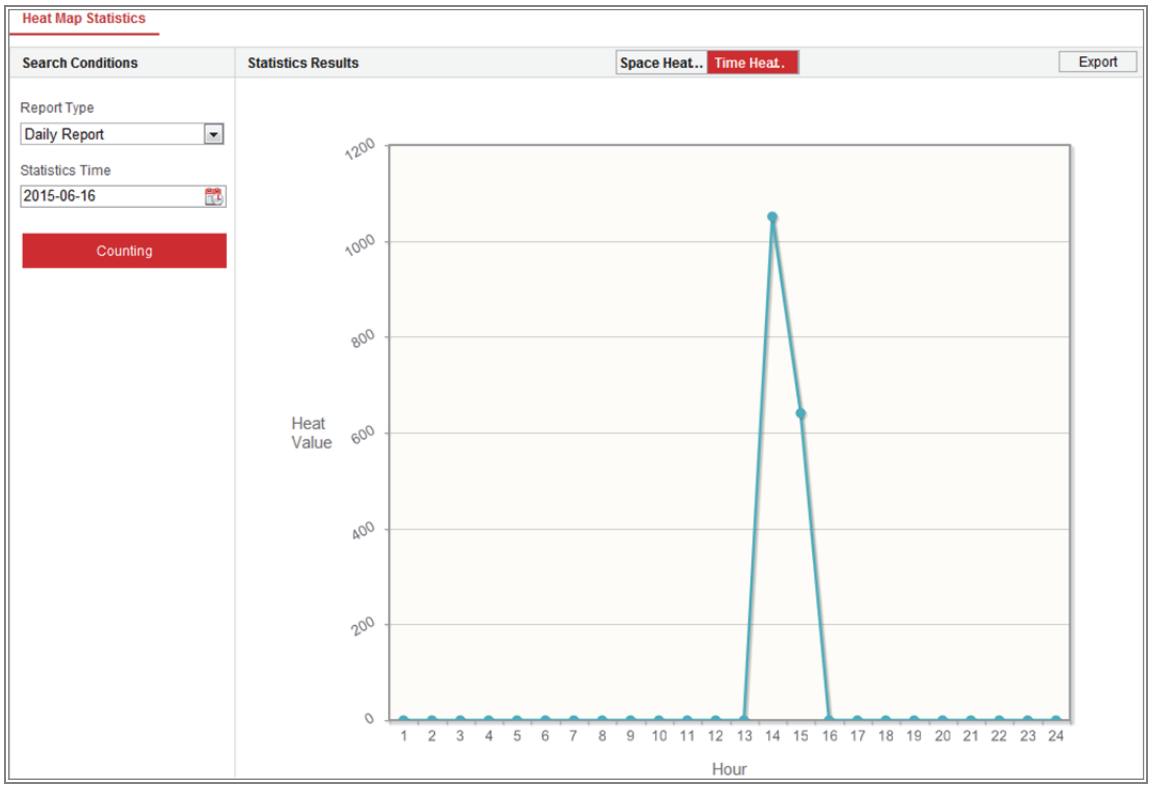
14.3 Statystki kolorowej mapy danych

Po włączeniu funkcji kolorowej mapy danych można wyświetlać i pobierać dane kolorowej mapy danych z karty aplikacji. Aby uzyskać bardziej zrozumiałe wyniki, można wyświetlić dane na różnych wykresach.

Kroki:

1. Wybierz typ raportu. Dostępny jest raport dzienny, tygodniowy, miesięczny i roczny.

   Uwaga: Raport dzienny umożliwia obliczenie danych dla wybranego dnia. Raport tygodniowy umożliwia wykonanie obliczeń dla tygodnia, do którego należy wybrana data. Raport miesięczny umożliwia wykonanie obliczeń dla miesiąca, do którego należy wybrana data. Raport roczny umożliwia wykonanie obliczeń dla roku, do którego należy wybrana data.
2. Wybierz godzinę początkową i kliknij przycisk **Counting**, aby wyświetlić mapę danych.
3. Wybierz ustawienie **Space Heat Map** lub **Time Heat Map**, aby wyświetlić wyniki. Jeżeli statystyki zostaną wyświetlone na mapie danych czasu, dostępny jest przycisk **Export** umożliwiający wyeksportowanie danych do pliku programu Excel.



Rysunek 14–3 Mapa danych czasu

Uwaga:

Po zakończeniu instalacji nie należy regulować obiektywu elektronicznego, ponieważ może to spowodować niedokładność danych.

14.4 Statystyki zliczania

Po włączeniu funkcji zliczania można wyświetlać i pobierać dane zliczania z karty aplikacji. Aby uzyskać bardziej zrozumiałe wyniki, można wyświetlić dane na różnych wykresach.

Kroki:

1. Wybierz typ raportu. Dostępny jest raport dzienny, tygodniowy, miesięczny i roczny.

   Uwaga: Raport dzienny umożliwia obliczenie danych dla wybranego dnia. Raport tygodniowy umożliwia wykonanie obliczeń dla tygodnia, do którego należy wybrana data. Raport miesięczny umożliwia wykonanie obliczeń dla miesiąca, do którego należy wybrana data. Raport roczny umożliwia wykonanie obliczeń dla roku, do którego należy wybrana data.

2. Wybierz typ statystyk. Dostępne są ustawienia People Entered i People Exited.
3. Wybierz godzinę początkową i kliknij przycisk **Counting**, aby wyświetlić mapę danych.
4. Wybierz przycisk **Table, Bar Chart** lub **Line Chart**, aby wyświetlić wyniki.
   Jeżeli statystyki zostaną wyświetlone w tabeli, dostępny jest przycisk **Export** umożliwiający wyeksportowanie danych do pliku programu Excel.

Aneks

Aneks 1 Wprowadzenie do oprogramowania SADP

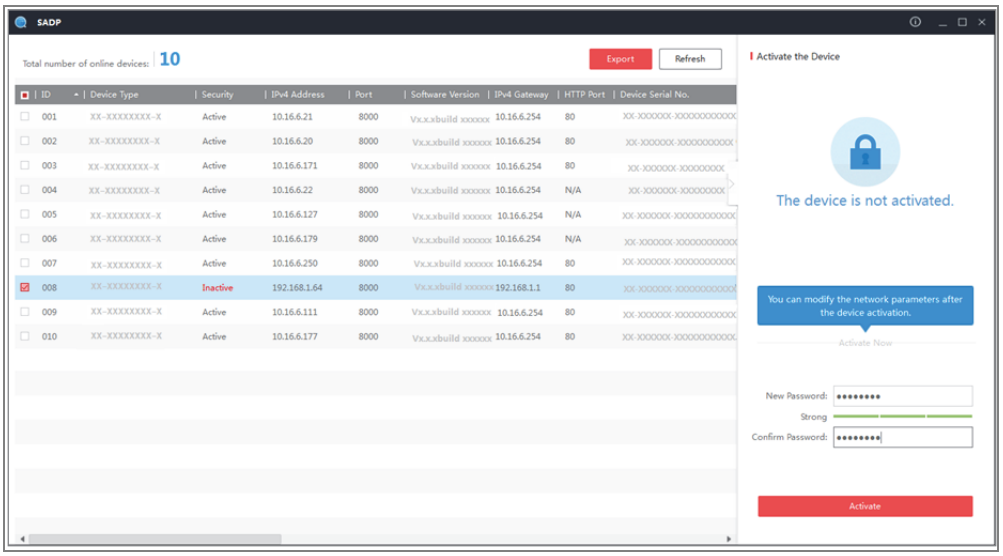
- **Opis oprogramowania SADP**

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

- **Wyszukiwanie aktywnych urządzeń połączonych z siecią**

♦ **Automatyczne wyszukiwanie urządzeń połączonych z siecią**

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



Rysunek A.1.1 Wyszukiwanie urządzeń połączonych z siecią

Uwaga:

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

♦ **Ręczne wyszukiwanie urządzeń połączonych z siecią**

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

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

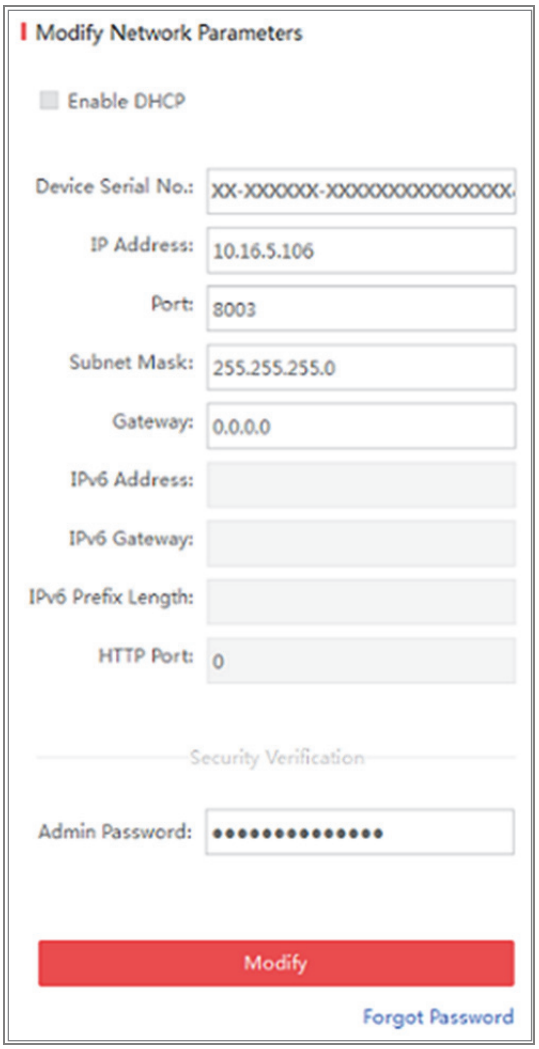
● Modyfikowanie parametrów sieciowych

Kroki:

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

- *Aby zapewnić ochronę prywatności i systemu przed zagrożeniami bezpieczeństwa, zdecydowanie zalecamy używanie silnych haseł dla wszystkich funkcji i urządzeń sieciowych. Należy wybrać własne hasło (co najmniej osiem znaków należących do co najmniej trzech z następujących kategorii: wielkie litery, małe litery, cyfry i znaki specjalne) w celu zapewnienia lepszej ochrony urządzenia.*

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



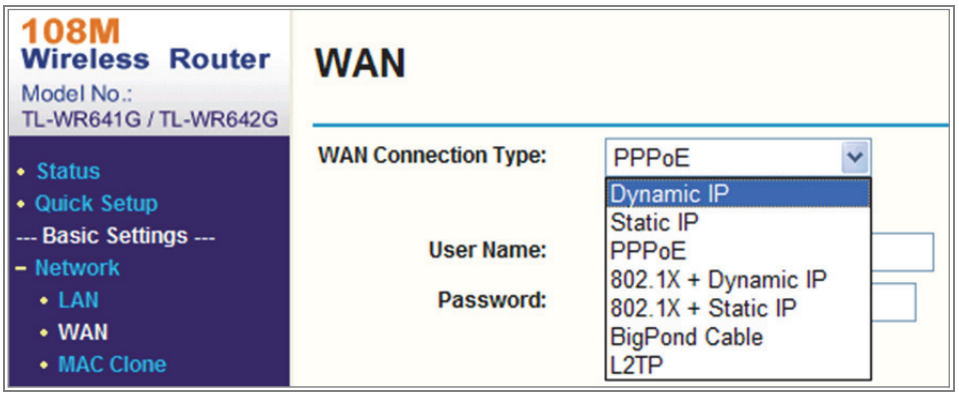
Rysunek A.1.2 Modyfikowanie parametrów sieciowych

Aneks 2 Mapowanie portów

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

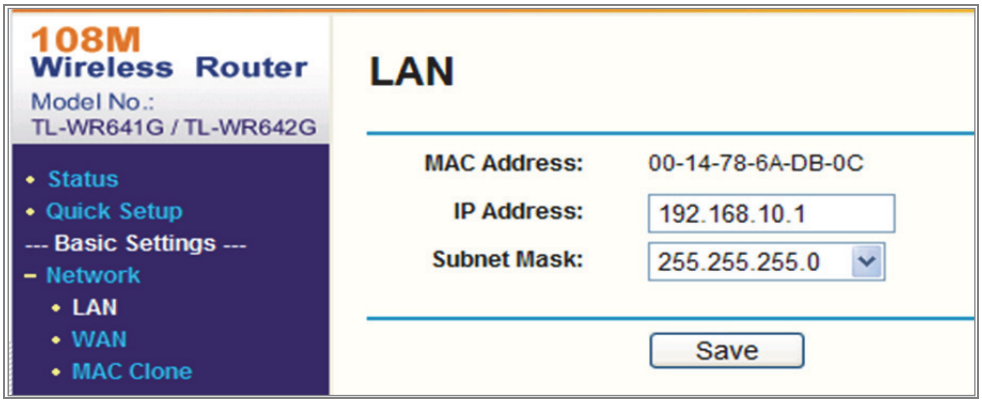
Kroki:

1. Wybierz parametr **WAN Connection Type**, jak przestawiono poniżej:



Rysunek A.2.1 Wybór typu połączenia sieci WAN

2. 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

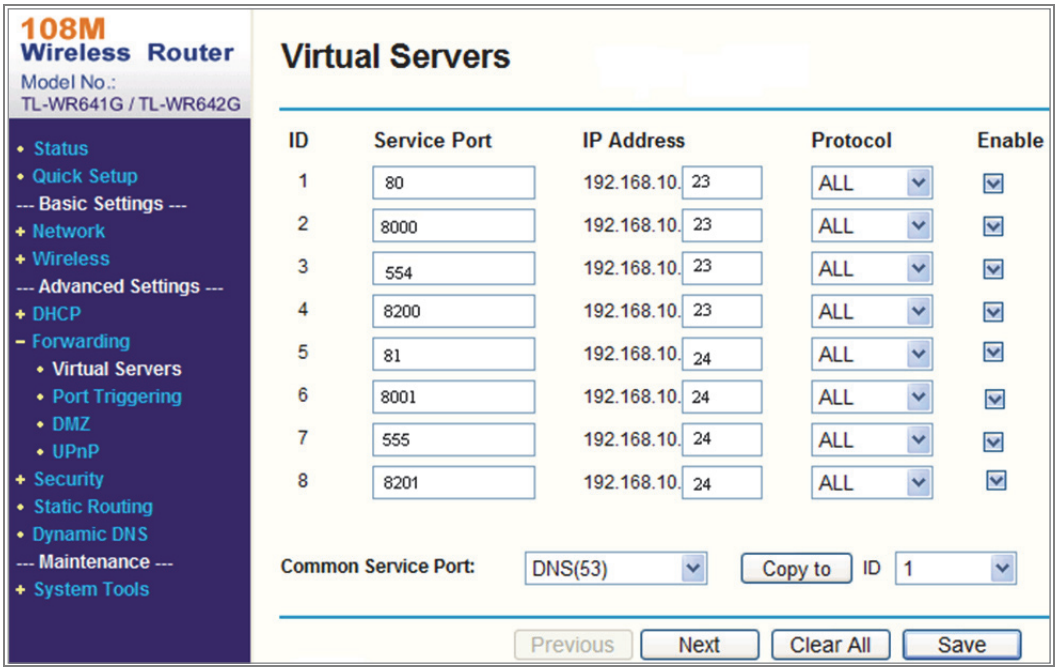
3. Ustaw mapowanie portu na serwerze wirtualnym **przekazywania**. Domyślnie kamera korzysta z portu 80, 8000 i 554. Można zmienić te wartości portów, korzystając z przeglądarki internetowej lub oprogramowania klienckiego.

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.



Rysunek A.2.3 Mapowanie portów

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


See Far, Go Further