MyEye

Video Recorder 16

Smart Video Recording up to 16 cameras

PL - Instrukcje i ostrzeżenia dotyczące instalacji i użytkowania

Nice

SPIS TREŚCI

1 WSTĘP

1.1 - Ogólne

Niniejsza skrócona instrukcja obsługi (zwana dalej „Przewodnikiem") przedstawia funkcje, montaż i obsługę urządzenia.

1.2 - Instrukcje bezpieczeństwa

W przewodniku mogą pojawić się następujące skategoryzowane zwroty ostrzegawcze o określonym znaczeniu.

Sygnały ostrzegawcze	Znaczenie
Ostrzeżenie	Wskazuje średnie lub niskie potencjalne zagrożenie, które może spowodować lekkie lub umiarkowane obrażenia, jeśli się go nie uniknie.
Uwaga	Wskazuje na potencjalne ryzyko, które może skutkować uszkodzeniem mienia, utratą danych, niższą wydajnością lub nieprzewidywalnymi rezultatami, jeśli się go nie uniknie.
Adnotacja	Zapewnia dodatkowe informacje jako podkreślenie i uzupełnienie tekstu.

1.3 - Informacja o ochronie prywatności

Jako użytkownik urządzenia lub administrator danych możesz gromadzić dane osobowe innych osób, takie jak twarze, odciski palców, numery rejestracyjne samochodów, adresy e-mail, numery telefonów, dane GPS itd. Musisz postępować zgodnie z lokalnymi przepisami i regulacjami dotyczącymi ochrony prywatności, aby chronić uzasadnione prawa i interesy innych osób, wdrażając środki, w tym między innymi: zapewnianie wyraźnej i widocznej identyfikacji w celu poinformowania osoby, której dane dotyczą, o istnieniu obszaru monitorowania i zapewnienie odpowiedniego kontaktu.

1.4 - Informacje o tym przewodniku

- Przewodnik służy wyłącznie jako odniesienie. W przypadku niezgodności między Przewodnikiem a rzeczywistym produktem, pierwszeństwo ma rzeczywisty produkt.
- Nie ponosimy odpowiedzialności za jakiekolwiek straty spowodowane operacjami niezgodnymi z Przewodnikiem.
- Przewodnik będzie aktualizowany zgodnie z najnowszymi przepisami ustawowymi i wykonawczymi pokrewnych regionów. Aby uzyskać szczegółowe informacje, zobacz kod QR lub naszą oficjalną stronę internetową. W przypadku rozbieżności między papierowym Podręcznikiem Użytkownika a wersją elektroniczną, pierwszeństwo ma wersja elektroniczna.
- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez uprzedniego pisemnego powiadomienia. Aktualizacje produktu mogą powodować pewne różnice między rzeczywistym produktem a Przewodnikiem. Prosimy o kontakt z działem obsługi klienta w celu uzyskania najnowszego programu i dodatkowej dokumentacji.
- Nadal mogą występować odchylenia w danych technicznych, opisach funkcji i operacji lub błędy w druku. W przypadku jakichkolwiek wątpliwości lub sporów zapoznaj się z naszym ostatecznym wyjaśnieniem.
- Wszystkie znaki towarowe, zastrzeżone znaki towarowe i nazwy firm w Przewodniku są własnością ich właścicieli.
- Odwiedź naszą stronę internetową i skontaktuj się z dostawcą lub obsługą klienta, jeśli wystąpią jakiekolwiek problemy podczas korzystania z urządzenia.
- W przypadku jakichkolwiek wątpliwości lub kontrowersji prosimy o zapoznanie się z naszym ostatecznym wyjaśnieniem.

2 ZAGROZENIA I OSTRZEZENIA

2.1 - Bezpieczeństwo elektryczne

- Wszystkie opisane tutaj montaże i operacje, powinny być zgodne z lokalnymi zasadami bezpieczeństwa elektrycznego.
- Używaj zasilacza spełniającego wymagania SELV (bezpieczne bardzo niskie napięcie) i zasilaj napięciem znamionowym zgodnym z wymaganiami dotyczącymi ograniczonego źródła zasilania w normie IEC60950-1. Szczegółowe wymagania dotyczące zasilania można znaleźć na etykietach urządzeń.
- Przed uruchomieniem urządzenia upewnij się, że urządzenie zasilające jest sprawne.
- Łatwo dostępne urządzenie odłączające powinno być włączone do okablowania instalacji budynku.
- Uważaj, aby kabel zasilający nie został przydeptany lub przygnieciony, w szczególności wtyczka, gniazdko elektryczne i złącze wystające z urządzenia.

2.2 - Środowisko

- Nie wystawiaj urządzenia na działanie silnego skupionego światła, takiego jak światło lampy lub światło słoneczne; w przeciwnym razie może to spowodować nadmierną jasność lub jasne plamy obrazu, które nie są wadą urządzenia i mogą wpłynąć na jego żywotność CMOS (Komplementarny półprzewodnik tlenku metalu).
- Nie umieszczaj urządzenia w wilgotnym lub zakurzonym otoczeniu, w bardzo wysokich lub niskich temperaturach, w miejscach o silnym promieniowaniu elektromagnetycznym lub niestabilnym oświetleniu.
- Trzymaj urządzenie z dala od cieczy, aby uniknąć uszkodzenia elementów wewnętrznych.
- Chroń wnętrze urządzenia przed deszczem lub wilgocią, aby uniknąć pożaru lub wyładowań atmosferycznych.
- Utrzymuj dobrą wentylację, aby uniknąć gromadzenia się ciepła.
- Transportuj, używaj i przechowuj urządzenie w zakresie dopuszczalnej wilgotności i temperatury.
- Ciężkie naprężenia, gwałtowne wibracje lub bryzgi wody są niedozwolone podczas transportu, przechowywania i instalacji.
- Na czas transportu zapakuj urządzenie w standardowe opakowanie fabryczne lub równoważny materiał.
- Zamontuj urządzenie w miejscu, do którego dostęp mają tylko profesjonalni pracownicy, posiadający odpowiednią wiedzę na temat zabezpieczeń i ostrzeżeń. Przypadkowe obrażenia mogą przytrafić się nieprofesjonalistom, którzy wejdą w obszar montażu, gdy urządzenie działa normalnie.

2.3 - Obsługa i codzienna konserwacja

- Nie dotykaj elementu rozpraszającego ciepło urządzenia, aby uniknąć oparzeń.
- Ostrożnie postępuj zgodnie z instrukcjami zawartymi w przewodniku podczas demontażu urządzenia; nieprofesjonalny demontaż może spowodować wyciek wody lub niską jakość obrazu. Skontaktuj się z serwisem posprzedażowym w celu wymiany środka osuszającego, jeśli po rozpakowaniu na soczewce pojawi się skroplona mgła lub gdy środek osuszający zmieni kolor na zielony (nie wszystkie modele są wyposażone w środek pochłaniający wilgoć).
- Zaleca się stosowanie urządzenia razem z odgromnikiem w celu poprawy efektu ochrony odgromowej.
- Zaleca się podłączenie otworu uziemiającego do uziemienia w celu zwiększenia niezawodności urządzenia.
- Nie dotykaj bezpośrednio czujnika obrazu (CMOS). Kurz i brud można usunąć dmuchawą lub delikatnie przetrzeć obiektyw miękką ściereczką zwilżoną alkoholem.
- Obudowę urządzenia można czyścić miękką, suchą ściereczką, której po zwilżeniu łagodnym detergentem można również użyć do usunięcia uporczywych plam. Aby uniknąć możliwego uszkodzenia powierzchni obudowy urządzenia, co mogłoby spowodować spadek wydajności, nie należy używać lotnych rozpuszczalników, takich jak alkohol, benzen, rozcieńczalnik ani silnych i ściernych detergentów.
- Osłona kopułkowa jest elementem optycznym, nie dotykaj ani nie wycieraj osłony rękoma bezpośrednio podczas montażu lub obsługi. Aby usunąć kurz, tłuszcz lub odciski palców, przetrzyj delikatnie zwilżoną bezolejową bawełną z dodatkiem dietylu lub zwilżoną miękką ściereczką. Do usunięcia kurzu można również użyć dmuchawy.

Ostrzeżenie

- Wzmocnij ochronę sieci, danych urządzenia i danych osobowych, stosując środki, które obejmują między innymi stosowanie silnego hasła, regularne modyfikowanie hasła, aktualizację oprogramowania urządzenia do najnowszej wersji oraz ustawienie prywatnej sieci komputerowej. W przypadku niektórych urządzeń ze starymi wersjami oprogramowania, hasło ONVIF nie zostanie automatycznie zmodyfikowane wraz ze zmianą hasła systemowego i konieczna będzie aktualizacja oprogramowania lub ręczna aktualizacja hasła ONVIF.
- Używaj standardowych komponentów lub akcesoriów dostarczonych przez producenta i upewnij się, że urządzenie jest instalowane i konserwowane przez profesjonalnych inżynierów.
- Powierzchnia przetwornika obrazu nie powinna być narażona na promieniowanie wiązki laserowej, w środowisku, w którym używane jest urządzenie wykorzystujące wiązkę laserową.
- Nie należy zasilać urządzenia dwoma lub więcej źródłami zasilania. Chyba, że podano inaczej. Niezastosowanie się do tej instrukcji może spowodować uszkodzenie urządzenia.

3 INSTALACJA

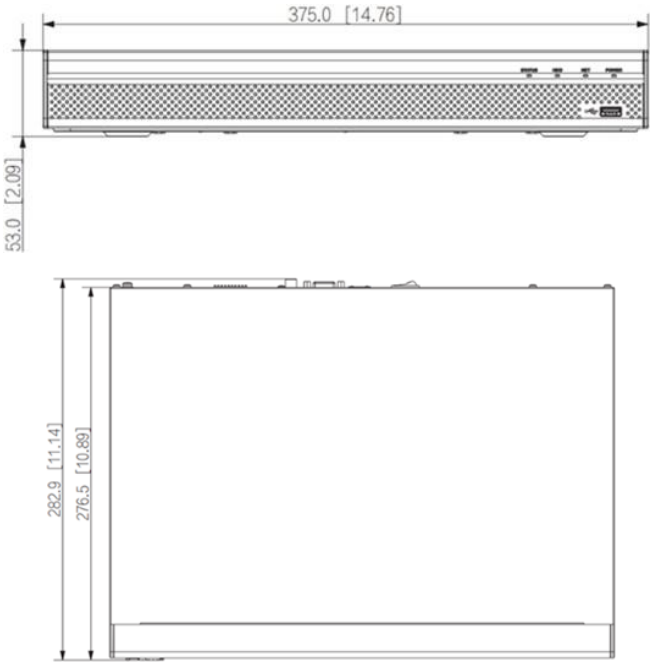
Uwaga

Wszystkie opisane tutaj czynności instalacyjne i operacyjne powinny być zgodne z lokalnymi przepisami bezpieczeństwa elektrycznego. Urządzenie nie jest przystosowane do montażu na ścianie panelem przednim skierowanym w dół.

- Poniższe ilustracje służą wyłącznie jako odniesienie. Obowiązują one dla rzeczywistego produktu.

3.1 - Wymiary

Poniższe rysunki służą wyłącznie jako odniesienie, a rzeczywisty produkt ma pierwszeństwo.

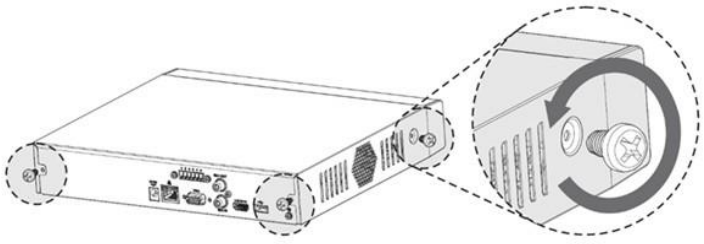


Ilustracja 3-1 Wymiary (jednostka: mm[cale])

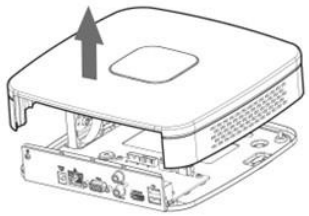
3.2 - Instalacja dysku twardego

Przed otwarciem pokrywy w celu wymiany dysku twardego należy wyłączyć NVR i odłączyć przewód zasilający.
Podczas pierwszej instalacji należy sprawdzić, czy dysk twardy został zainstalowany. Zaleca się użycie dysku twardego klasy korporacyjnej lub klasy surveillance poziomu. Nie zaleca się używania dysków twardych do komputerów PC.

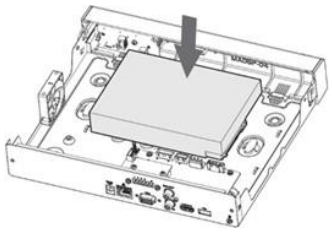
1. Odkręć śruby mocujące pokrywę obudowy (w tym dwie śruby na tylnym panelu i dwie śruby na lewym i prawym panelu).



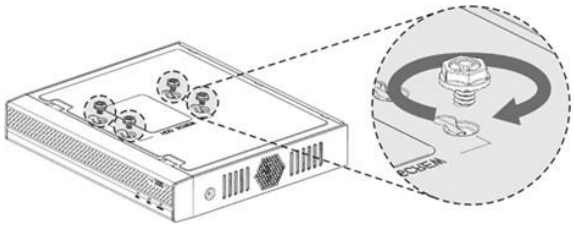
2. Zdejmij pokrywę zgodnie z kierunkiem wskazywanym przez poniższą strzałkę.



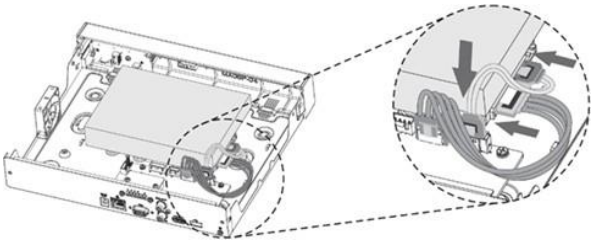
3. Dopasuj cztery otwory na płycie bazowej, aby umieścić dysk twardy.



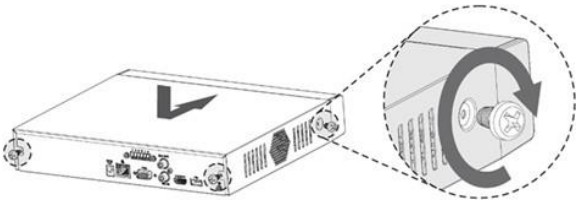
4. Odwróć urządzenie do góry nogami, dopasuj śruby do otworów na dysku twardym, a następnie przykręć je. Dysk twardy jest przymocowany do płyty bazowej



5. Podłącz kabel danych dysku twardego i kabel zasilania do urządzenia.

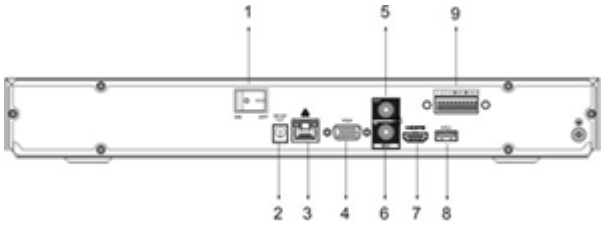


6. Załóż pokrywę i dokręć cztery śruby na płycie bazowej, aby zakończyć instalację.



3.3 - Podłączenie

- Poniższe rysunki służą wyłącznie jako odniesienie. Obowiązuje rzeczywisty produkt.
- Należy dokładnie sprawdzić ikony na tylnym panelu i odnieść się do rzeczywistego produktu w celu uzyskania szczegółowych informacji.
- Jeśli ikona to (DC12V), należy podłączyć zasilanie DC 12V. Jeśli ikona to (DC48V), należy podłączyć zasilanie DC 48V.



1	Przełącznik zasilania	2	Porty PoE
3	Port sieciowy	4	Wejście zasilania
5	Wyjście mikrofonu	6	Port VGA
7	Port HDMI	8	Port HDMI
9	Wejście/wyjście alarmowe		

4 KONFIGURACJA

4.1 - Uruchamianie

Przed uruchomieniem upewnij się, że

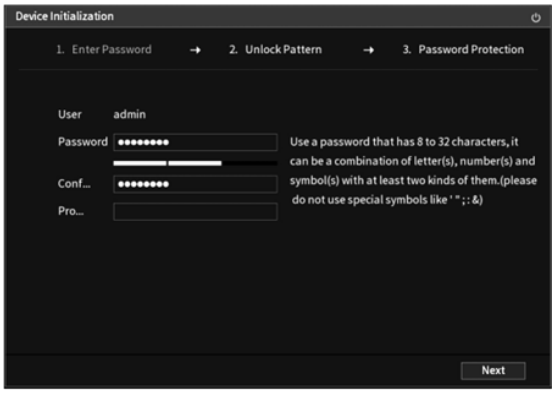
- Znamionowe napięcie wejściowe odpowiada wymaganiom zasilania NVR (Sieciowe Rejestratory Video).
- Podłączenie przewodu zasilającego jest gotowe.
- W celu zapewnienia bezpieczeństwa urządzenia należy najpierw podłączyć NVR do zasilacza, a następnie do gniazda zasilania.
- Zawsze używaj stabilnego prądu. Zaleca się stosowanie zasilacza UPS jako źródła zasilania.
- Urządzenia niektórych serii nie mają przycisku włączania i wyłączania zasilania. Urządzenie można uruchomić po podłączeniu zasilania.

Podłącz urządzenie do monitora lub telewizora za pomocą kabla HDMI, podłącz je do gniazda zasilania, a następnie naciśnij przycisk zasilania, aby uruchomić urządzenie.

4.2 - Inicjalizacja urządzenia

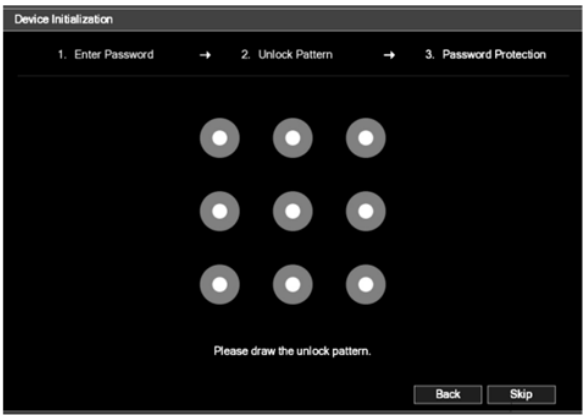
Podczas pierwszego uruchomienia należy skonfigurować informacje o haśle dla administratora (domyślnie). Aby zagwarantować bezpieczeństwo urządzenia, hasło logowania administratora powinno być odpowiednio ukryte i regularnie modyfikowane.

1. Włącz urządzenie. Zostanie wyświetlony interfejs inicjalizacji urządzenia
2. Ustaw lokalizację, język i standard wideo. Z listy rozwijanej wybierz region, język i standard wideo zgodnie z potrzebami.
3. Przeczytaj Umowę licencyjną oprogramowania i wybierz opcję "Przeczytałem i akceptuję wszystkie warunki".
4. Wybierz strefę czasową i skonfiguruj czas systemowy.
5. Skonfiguruj informacje o haśle dla administratora. Szczegółowe informacje znajdują się w poniższej tabeli



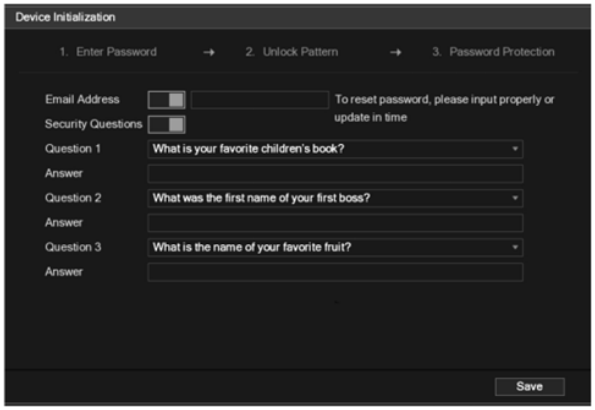
Parametr	Opis
Użytkownik	Domyślnie użytkownikiem jest admin.
Hasło	W polu Hasło wprowadź hasło administratora. Nowe hasło może zawierać od 8 do 32 znaków. Znaki muszą zawierać co najmniej dwa rodzaje cyfr, liter i znaków specjalnych (z wyłączeniem"'", """, ";", ":" i "&").
Potwierdź hasło	
Pytanie pomocnicze	W polu Prompt Question wprowadź informacje, które pomogą przypomnieć hasło.

6. Za pomocą myszy narysuj wzór odblokowania, a następnie narysuj go ponownie w celu potwierdzenia.



- Wzór, który chcesz ustawić, musi przecinać co najmniej cztery punkty.
- Jeśli nie chcesz konfigurować wzoru odblokowania, kliknij Pomiń.
- Po skonfigurowaniu wzoru odblokowania będzie on używany jako domyślna metoda uwierzytelniania. Jeśli pominiesz tę opcję ustawień, wprowadź hasło logowania.

7. Zastosować zarezerwowany adres e-mail i pytania zabezpieczające do NVR.

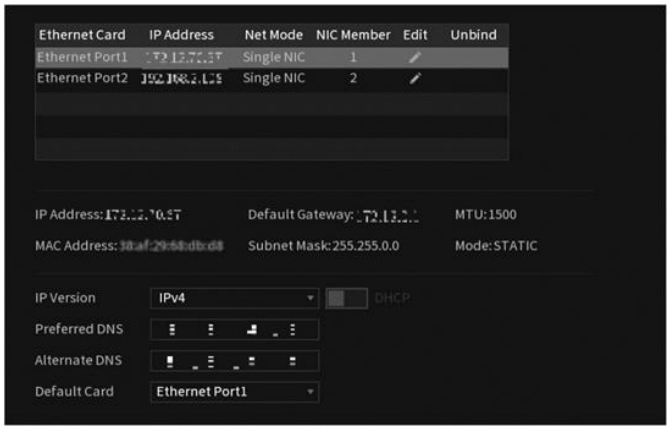


- Włącz pole wyboru Email address (Adres e-mail) i wprowadź adres e-mail.
- Zaznacz pole wyboru Enable Security Questions, a następnie wprowadź odpowiedzi na te pytania.
- Po skonfigurowaniu, jeśli zapomnisz hasła dla użytkownika admin, możesz zresetować hasło za pomocą zarezerwowanego adresu e-mail lub pytań zabezpieczających.
- Jeśli nie chcesz konfigurować ustawień, wyłącz funkcje adresu e-mail i pytań zabezpieczających w interfejsie.

8. Kliknij OK, aby zakończyć inicjalizację.

4.3 - Konfiguracja sieci

1. Wybierz Menu główne > Sieć > TCP/IP. Wyświetlony zostanie interfejs TCP/IP. Kliknij aby zmodyfikować adres IP zgodnie z aktualnym adresem domowym ustawieniami sieci domowej (domyślny adres IP to 192.168.1.108)



Parameter	Opis
Wersja IP	Z listy Wersja IP można wybrać IPv4 lub IPv6. Obie wersje są obsługiwane na potrzeby dostępu.
Adres MAC	Wyświetla adres MAC urządzenia NVR.
DHCP	Włącz funkcję DHCP. Adres IP, maska podsieci i brama domyślna nie są dostępne do konfiguracji po włączeniu DHCP. • Jeśli funkcja DHCP działa, uzyskane informacje będą wyświetlane w polach IP Address (Adres IP), Subnet Mask (Maska podsieci) i Default Gateway (Brama domyślna). W przeciwnym razie wszystkie wartości będą wskazywać 0.0.0.0. • Jeśli połączenie PPPoE powiedzie się, adres IP, maska podsieci, brama domyślna i DHCP nie będą dostępne do konfiguracji.
Adres IP **Maska podsieci** **Brama domyślna**	Wprowadź adres IP i skonfiguruj odpowiednią maskę podsieci i bramę domyślną. UWAGA Adres IP i brama domyślna muszą znajdować się w tym samym segmencie sieci
Preferowany DNS	Wprowadź adres IP DNS
Alternatywny DNS	Wprowadź adres IP alternatywnego DNS
MTU	Wprowadź wartość dla karty sieciowej. Wartość mieści się w zakresie od 1280 do 1500 bajtów. Wartością domyślną jest 1500. Sugerowane wartości MTU są następujące 1500: Największa wartość pakietu informacji Ethernet. Ta wartość jest zwykle wybierana, jeśli nie ma połączenia PPPoE lub VPN, a także jest wartością domyślną niektórych routerów, kart sieciowych i przełączników. 1492: Zoptymalizowana wartość dla PPPoE. 1468: Zoptymalizowana wartość dla DHCP. 1450: Zoptymalizowana wartość dla VPN.
Test	Kliknij Test, aby sprawdzić, czy wprowadzony adres IP i brama współpracują ze sobą.

4.4 - Dodawanie kamer IP

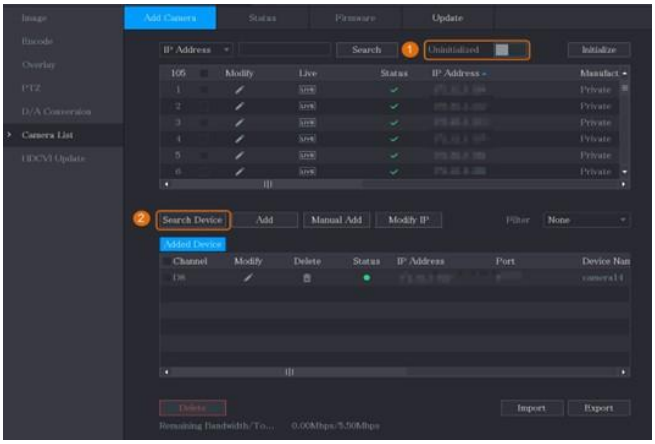
Kamerę IP można dodać na podstawie wyników wyszukiwania lub ręcznie wprowadzając informacje o adresie IP.

4.4.1 - Inicjalizacja kamer IP

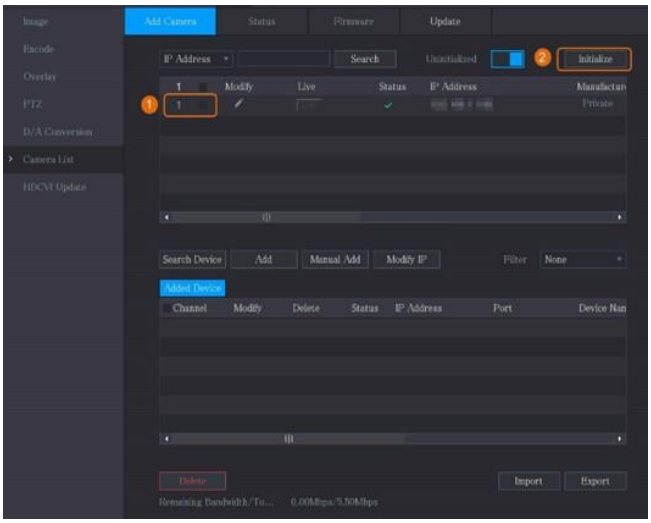
W tej części instrukcji przedstawiono sposób inicjowania nowych kamer lub kamer po przywróceniu ustawień fabrycznych.

- Po podłączeniu kamery do rejestratora NVR przez wbudowany port PoE, NVR automatycznie zainicjuje kamerę. Kamera domyślnie przyjmuje hasło i adres e-mail NVR.

1. Wybierz Menu główne > Kamera > Lista kamer > Dodaj kamerę.
2. Zaznacz pole wyboru Uninitialized, a następnie kliknij przycisk Search Device.



3. Wybierz kamerę, która ma zostać zainicjalizowana, a następnie kliknij przycisk inicjalizacji.



4. Zastosuj hasło i informacje e-mail do kamery IP

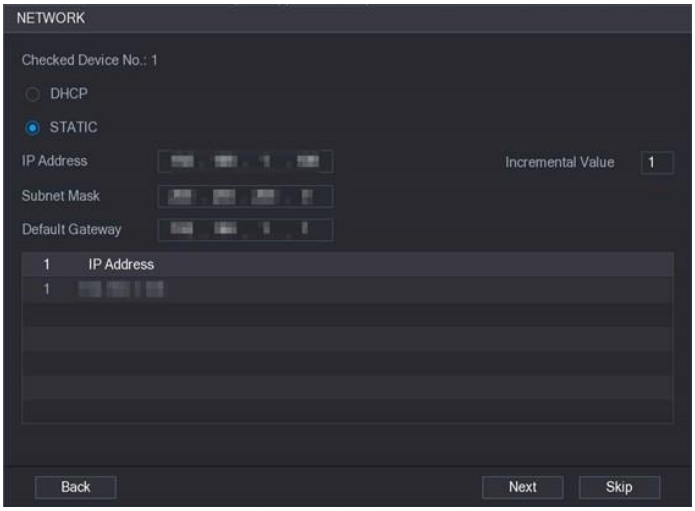
- Wybierz opcję "Using current device password and email info", aby pozostawić te same dane uwierzytelniające dla kamery, co w NVR.
- Usuń zaznaczenie opcji "Using current device password and email info", aby zdefiniować inne dane uwierzytelniające dla kamery.

5. Skonfiguruj adres IP kamery

- Wybierz DHCP, jeśli wdrożony jest serwer DHCP.
- Wybierz Statyczny (preferowany), a następnie wprowadź adres IP, maskę podsieci, bramę domyślną i wartość przyrostową.

Uwaga

- Ustaw wartość przyrostową, jeśli chcesz zmienić adresy IP wielu kamer jednocześnie. NVR będzie przyrostowo dodawać wartość do czwartej sekcji adresu IP po przydzieleniu adresu IP dla tych kamer

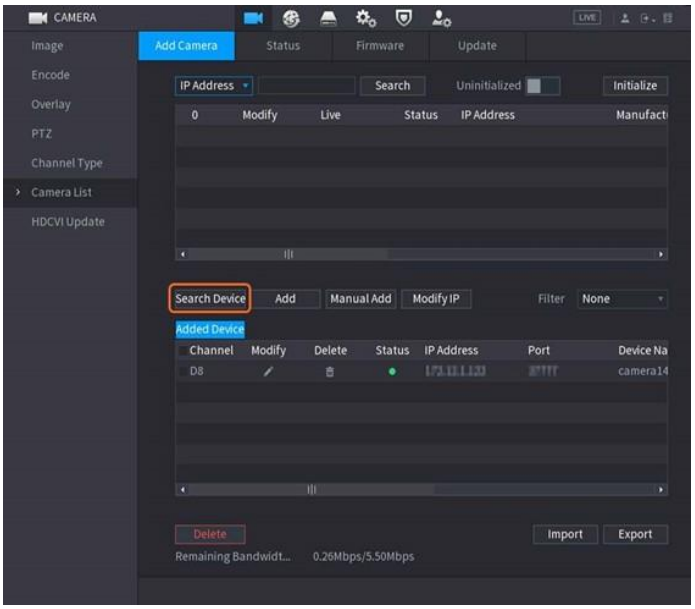


6. Kliknij przycisk Next (Dalej). Poczekaj 1-2 minuty na zakończenie procedury inicjalizacji. Kliknij przycisk Finished.

4.4.2 - Dodawanie kamer IP według wyników wyszukiwania

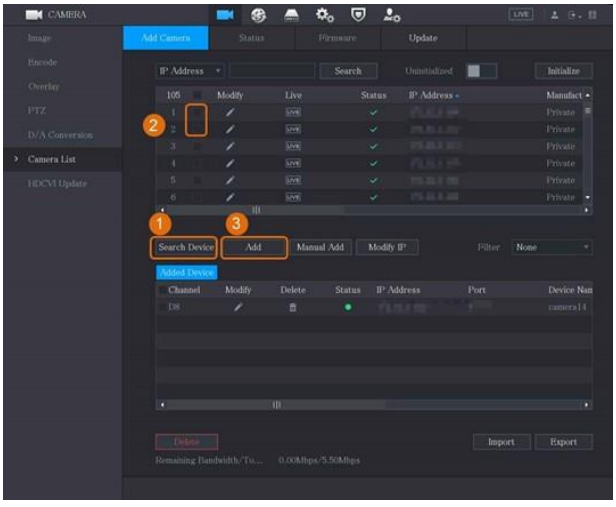
Upewnij się, że kamery, które chcesz dodać, zostały już zainicjowane i podłączone do właściwej sieci.

1. Wybierz Menu główne > Kamera > Lista kamer > Dodaj kamerę.
2. Kliknij przycisk Wyszukaj urządzenie.



3. Dodaj kamery IP:

- Dodaj przez dwukrotne kliknięcie: Kliknij dwukrotnie docelową kamerę, aby dodać ją do listy dodanych urządzeń
- Za pomocą tej metody można dodać tylko jedną kamerę naraz.
- Dodaj za pomocą pola wyboru: Zaznacz pole wyboru kamery docelowej, a następnie kliknij przycisk Dodaj, aby dodać ją do listy dodanych urządzeń.
- Można zaznaczyć więcej niż jedno pole wyboru i dodawać kamery partiami.



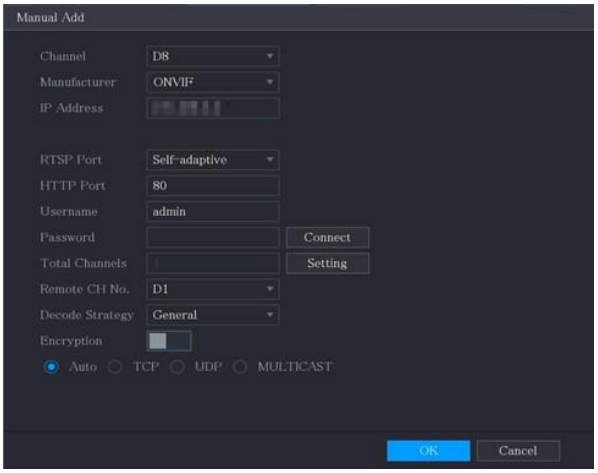
- Jeśli status dodanej kamery jest zielony, oznacza to, że kamera została prawidłowo dodana do NVR.
- Jeśli status dodanej kamery jest czerwony, oznacza to awarię połączenia między kamerą a NVR. Sprawdź parametry kamery, takie jak hasło, protokół i numer kanału, a następnie spróbuj dodać ją ponownie.

4.4.3 - Ręczne dodawanie kamer IP

Jednorazowo można dodać jedną kamerę IP według informacji IP.

Upewnij się, że kamery, które chcesz dodać, zostały już zainicjowane i podłączone do właściwej sieci.

1. Wybierz Menu główne > Kamera > Lista kamer > Dodaj kamerę.
2. Kliknij przycisk Manual Add.
3. W oknie dialogowym Manual Add skonfiguruj parametry.



Parametr	Opis
Kanał	Z listy rozwijanej Channel (Kanał) wybierz kanał, który ma być używany w urządzeniu NVR do podłączenia urządzenia zdalnego.
Producent	Z listy rozwijanej Manufacturer (Producent) wybierz producenta urządzenia zdalnego.
Adres IP	W polu IP Address wprowadź adres IP kamery IP. • Zmień wartość domyślną (192.168.0.0), z którą system nie może się połączyć.
Port RTSP	Wartość domyślna to 554. Wartość tę można zmienić w razie potrzeby.
Port HTTP	Domyślną wartością jest 80. Wartość tę można zmienić w razie potrzeby. • W przypadku wprowadzenia innej wartości, na przykład 70, należy wpisać 70 po adresie IP podczas logowania do NVR przez przeglądarkę.
Port TCP	Domyślną wartością jest 37777. Wartość tę można zmienić w razie potrzeby.
Nazwa użytkownika	Wprowadź nazwę użytkownika urządzenia zdalnego.
Hasło	Wprowadź hasło użytkownika urządzenia zdalnego.
Nr zdalnego CH.	Wprowadź numer kanału zdalnego urządzenia, które chcesz dodać.
Strategia dekodera	Z listy Decoder Strategy wybierz Default, Realtime lub Fluent, w zależności od potrzeb.
Typ protokołu	• Jeśli kamera IP jest dodawana przez protokół prywatny, wybierz TCP. • Jeśli kamera IP została dodana za pośrednictwem protokołu ONVIF, wybierz Auto, TCP, UDP lub MULTICAST. • Jeśli kamera IP została dodana przez innych producentów, wybierz TCP lub UDP.
Szyfrowanie	Jeśli kamera IP została dodana za pośrednictwem protokołu ONVIF, zaznaczenie pola wyboru Szyfrowanie zapewni ochronę szyfrowania przesyłanych danych. Aby korzystać z tej funkcji, funkcja HTTPS musi być włączona dla zdalnej kamery IP.

4.5 - Konfigurowanie harmonogramu przechowywania nagrań wideo

Domyślnie wszystkie kamery nieprzerwanie nagrywają wideo przez 24 godziny na dobę. W razie potrzeby można zmodyfikować ustawienia.

1. Wybierz Menu główne > Pamięć > Harmonogram > Nagrywanie

2. Skonfiguruj parametry.

Parameter	Beschreibung
Kanał	Kliknij listę rozwijaną Kanał Z oraz wybierz kanał, aby zmienić ustawienia nagrywania wideo.
Zapis wstępny	W polu Pre-record ustaw czas przechwytywania dodatkowego wideo, które pojawia się przed zdarzeniem, aby zapewnić kontekst nagrania. Zakres wartości: 0 do 30 s.
Redundancja	Umożliwia użytkownikom ustawienie jednego z dysków twardych jako nadmiarowego dysku twardego w celu zapisywania nagranych plików na różnych dyskach twardych. W przypadku awarii dysku twardego można znaleźć kopię zapasową nagrania na nadmiarowym dysku twardym. • Wybierz Main Menu > STORAGE > Disk Manager, a następnie ustaw HDD jako redundantny HDD. • Wybierz kolejno Main Menu > STORAGE > Schedule > Record, a następnie zaznacz pole Redundancy. • Jeśli wybrany kanał nie nagrywa, funkcja nadmiarowości zacznie działać przy następnym nagrywaniu bez względu na to, czy pole wyboru zostanie zaznaczone, czy nie. • Jeśli wybrany kanał nagrywa, aktualnie nagrane pliki zostaną spakowane, a następnie rozpocznie się nagrywanie zgodnie z nowym harmonogramem. • Ta funkcja jest dostępna w wybranych modelach. • Nadmiarowy dysk twardy tworzy kopie zapasowe tylko nagranych filmów, ale nie migawek.
Typ zdarzenia	Zaznacz pole wyboru typu zdarzenia. Ogólne: Nagrywanie ogólne oznacza, że NVR nagrywa wszystkie filmy w określonym przedziale czasu. Nagrywanie ogólne jest oznaczone kolorem zielonym. Ruch: Nagrywanie ruchu oznacza, że NVR nagrywa wideo tylko wtedy, gdy zostanie wyzwolona detekcja ruchu. Nagrywanie ruchu jest reprezentowane przez żółty kolor. Alarm: Nagrywanie alarmowe oznacza, że NVR nagrywa wideo po wyzwoleniu alarmu. Nagrywanie alarmowe jest reprezentowane przez kolor czerwony. RCP: Nagrywanie M&A łączy w sobie nagrywanie ruchu i nagrywanie alarmowe. Urządzenie nagrywa wideo po wykryciu ruchu lub wyzwoleniu dowolnego alarmu. Nagrywanie M&A jest reprezentowane przez kolor pomarańczowy. Inteligentne: Inteligentne nagrywanie oznacza, że NVR nagrywa wideo po wyzwoleniu inteligentnej detekcji. Inteligentne nagrywanie jest oznaczone kolorem niebieskim. POS: Nagrywanie POS oznacza, że NVR nagrywa wideo, gdy urządzenie POS jest używane do dokonywania płatności. Nagrywanie POS jest reprezentowane przez kolor fioletowy. Inteligentne: Inteligentne nagrywanie oznacza, że NVR nagrywa wideo, gdy uruchomiona zostanie inteligentna detekcja. Inteligentne nagrywanie jest reprezentowane przez kolor niebieski. POS: Nagrywanie POS oznacza, że NVR nagrywa wideo, gdy urządzenie POS jest używane do dokonywania płatności. Nagrywanie POS jest reprezentowane przez kolor fioletowy.
Okres	Określa okres, w którym skonfigurowane ustawienie nagrywania jest aktywne. System aktywuje alarm tylko w zdefiniowanym okresie.
Kopiuj do	Kliknij Kopiuj, aby skopiować ustawienia do innych kanałów.

3. Ustaw harmonogram, rysując lub edytując

- Rysowanie: Naciśnij i przytrzymaj lewy przycisk myszy i przeciągnij myszą, aby narysować okres
- Edycja: Kliknij, aby skonfigurować okres, a następnie kliknij OK

4. Kliknij Zastosuj

- Skonfigurowany harmonogram zapisu może wejść w życie tylko wtedy, gdy funkcja automatycznego zapisu jest włączona.

4.6 - Logowanie do interfejsu internetowego

1. Otwórz przeglądarkę Internet Explorer, wprowadź adres IP urządzenia w pasku adresu i naciśnij Enter. Jeśli wyświetlony zostanie kreator konfiguracji, postępuj zgodnie z instrukcjami, aby dokończyć ustawienia.
2. Wprowadź nazwę użytkownika i hasło w polu logowania, a następnie kliknij Login.
3. W przypadku pierwszego logowania kliknij Click Here to Download Plugin, a następnie zainstaluj wtyczkę zgodnie z instrukcjami.
4. Wyświetlony zostanie główny interfejs.

5 ZALECENIA DOTYCZĄCE CYBERBEZPIECZENSTWA

Obowiązkowe działania na rzecz cyberbezpieczeństwa

A. Zmiana haseł i używanie silnych haseł:

Głównym powodem "włamań" do systemów jest posiadanie słabych lub domyślnych haseł. Zaleca się natychmiastową zmianę domyślnych haseł i wybieranie silnych haseł, gdy tylko jest to możliwe. Silne hasło powinno składać się z co najmniej 8 znaków i kombinacji znaków specjalnych, cyfr oraz wielkich i małych liter.

B. Aktualizacja oprogramowania sprzętowego

Ponieważ jest to standardowa procedura w branży technologicznej, zalecamy aktualizowanie oprogramowania NVR i kamer IP, aby upewnić się, że system korzysta z najnowszych poprawek i poprawek bezpieczeństwa.

Rekomendacje "Nice to have" w celu poprawy bezpieczeństwa sieci

A. Regularna zmiana haseł
Regularnie zmieniaj poświadczenia do swoich urządzeń, aby upewnić się, że tylko autoryzowani użytkownicy mają dostęp do systemu.

B. Zmiana domyślnych portów HTTP i TCP:

- Zmień domyślne porty HTTP i TCP dla systemów. Są to dwa porty używane do komunikacji i zdalnego przeglądania kanałów wideo.
- Porty te można zmienić na dowolny zestaw numerów z zakresu 1025-65535. Unikanie domyślnych portów zmniejsza ryzyko, że osoby postronne będą w stanie odgadnąć, których portów używasz.

C. Szyfrowana transmisja audio i wideo

Jeśli zawartość danych audio i wideo jest bardzo ważna lub wrażliwa, zalecamy korzystanie z funkcji szyfrowanej transmisji, aby zmniejszyć ryzyko kradzieży danych audio i wideo podczas transmisji.

Przypomnienie: szyfrowana transmisja spowoduje pewną utratę wydajności transmisji.

D. Włącz filtr IP:

Włączenie filtra IP uniemożliwi dostęp do systemu wszystkim osobom, z wyjątkiem osób o określonych adresach IP.

E. Zmień hasło ONVIF:

W przypadku starszego oprogramowania sprzętowego kamery IP hasło ONVIF nie zmienia się po zmianie poświadczeń systemu. Konieczna będzie aktualizacja oprogramowania sprzętowego kamery do najnowszej wersji lub ręczna zmiana hasła ONVIF.

F. Włącz blokadę konta

Funkcja blokady konta jest domyślnie włączona i zalecamy pozostawienie tej funkcji włączonej, aby zagwarantować bezpieczeństwo konta. Jeśli atakujący spróbuje zalogować się przy użyciu niewłaściwego hasła kilka razy, odpowiednie konto i źródłowy adres IP zostaną zablokowane.

G. Przekazuj tylko potrzebne porty:

- Przekazuj tylko te porty HTTP i TCP, których potrzebujesz. Nie należy przekazywać do urządzenia szerokiego zakresu numerów. Nie DMZ adresu IP urządzenia.
- Nie trzeba przekierowywać żadnych portów dla poszczególnych kamer, jeśli wszystkie są podłączone do rejestratora na miejscu; potrzebny jest tylko NVR.

H. Ograniczenie funkcji kont gości:

Jeśli system jest skonfigurowany dla wielu użytkowników, upewnij się, że każdy użytkownik ma dostęp tylko do funkcji, których potrzebuje do wykonywania swojej pracy.

I. Wyłącz niepotrzebne usługi i wybierz bezpieczne tryby

Jeśli nie jest to konieczne, zaleca się wyłączenie niektórych usług, takich jak SNMP, SMTP, UPnP itp. w celu zmniejszenia ryzyka.

W razie potrzeby zaleca się korzystanie z bezpiecznych trybów, w tym między innymi z następujących usług:

- SNMP: Wybierz SNMP v3 i skonfiguruj silne hasła szyfrujące i hasła uwierzytelniające.
- SMTP: Wybierz TLS, aby uzyskać dostęp do serwera skrzynki pocztowej.
- FTP: Wybierz SFTP i skonfiguruj silne hasła.

- Hotspot AP: Wybierz tryb szyfrowania WPA2-PSK i ustaw silne hasła.

J. Bezpieczny audyt

Sprawdzanie użytkowników online: zalecamy regularne sprawdzanie użytkowników online, aby sprawdzić, czy NVR jest zalogowany bez autoryzacji.

Sprawdzanie dziennika urządzeń: Przeglądając dzienniki, można poznać adresy IP, które zostały użyte do zalogowania się do urządzeń i ich kluczowych operacji.

K. Dziennik sieciowy

Ze względu na ograniczoną pojemność pamięci urządzenia, przechowywany dziennik jest ograniczony. Jeśli konieczne jest zapisanie dziennika przez długi czas, zaleca się włączenie funkcji dziennika sieciowego, aby zapewnić synchronizację krytycznych dzienników z serwerem dziennika sieciowego w celu śledzenia.

L. Fizyczne zablokowanie urządzenia:

Najlepiej byłoby zapobiec nieautoryzowanemu fizycznemu dostępowi do systemu. Najlepszym sposobem na osiągnięcie tego celu jest zainstalowanie rejestratora w zamkniętej skrzynce, zamykanej szafie serwerowej lub w pomieszczeniu za zamkniętymi drzwiami.

M. Podłączanie kamer IP do portów PoE z tyłu jednostki NVR:

Kamery podłączone do portów PoE z tyłu NVR są odizolowane od świata zewnętrznego i nie można uzyskać do nich bezpośredniego dostępu.

N. Tworzenie bezpiecznego środowiska sieciowego

Aby lepiej zapewnić bezpieczeństwo sprzętu i zmniejszyć potencjalne zagrożenia cybernetyczne, zalecamy:

- Wyłączyć funkcję mapowania portów routera, aby uniknąć bezpośredniego dostępu do urządzeń intranetowych z sieci zewnętrznej.
- Sieć powinna być podzielona i odizolowana zgodnie z rzeczywistymi potrzebami sieci. Jeśli nie ma wymagań komunikacyjnych między dwiema podsieciami, sugeruje się użycie VLAN, sieci GAP i innych technologii do partycjonowania sieci, aby osiągnąć efekt izolacji sieci.
- Ustanowienie systemu uwierzytelniania dostępu 802.1x w celu zmniejszenia ryzyka nieautoryzowanego dostępu do sieci prywatnych.

O. Zaleca się włączenie zapory sieciowej lub funkcji listy blokowania i zezwalania, aby zmniejszyć ryzyko ataku na urządzenie.

6 DODATKOWE INFORMACJE

Aby uzyskać więcej informacji i pobrać wymagane oprogramowanie, odwiedź następującą stronę internetową:

IS0900A00_26-09-2023

Nice SpA
Oderzo TV Italia
info@niceforyou.com