Terminal do rozpoznawania twarzy

Instrukcja skrócona

V1.0.0

Przedmowa

Informacje ogólne

Niniejsza instrukcja przedstawia instalację i podstawowe funkcje terminala do rozpoznawania twarzy (zwanego dalej "terminalem").

Wskazówki dotyczące bezpieczeństwa użytkowania

W Podręczniku mogą pojawić się następujące skategoryzowane słowa o zdefiniowanym znaczeniu.

Hasła ostrzegawcze	Znaczenie
NIEBEZPIECZEŃSTWO	Wskazuje na wysokie potencjalne zagrożenie, które może prowadzić do śmierci lub ciężkich obrażeń ciała.
OSTRZEŻENIE	Oznacza średnie lub niskie potencjalne zagrożenie, które może powodować lekkie lub średnie obrażenia ciała.
UWAGA	Wskazuje na potencjalne zagrożenie, które może powodować straty rzeczowe, utratę danych, obniżenie wydajności lub nieprzewidziane skutki.
PORADY	Zapewnia porady, które pomogą Ci rozwiązać problem lub zaoszczędzić czas.
UWAGA	Zapewnia dodatkowe informacje w formie uzupełnienia do tekstu.

Historia zmian

Wersja	Wersja poprawki	Czas wydania
V1.0.0	Pierwsze wydanie	Lipiec 2020 r.

O podręczniku

- Podręcznik ma charakter wyłącznie informacyjny. W przypadku niezgodności między podręcznikiem a rzeczywistym produktem, pierwszeństwo ma produkt rzeczywisty.
- Nie ponosimy odpowiedzialności za jakiekolwiek straty spowodowane działaniami niezgodnymi z instrukcją.
- Podręcznik będzie aktualizowany zgodnie z najnowszymi przepisami prawa i regulacjami obowiązującymi w danym regionie. Szczegółowe informacje można znaleźć w papierowej instrukcji obsługi, na płycie CD-ROM, w kodzie QR lub na naszej oficjalnej stronie internetowej. W przypadku braku spójności między wersją papierową a elektroniczną, pierwszeństwo ma wersja elektroniczna.
- Wszystkie projekty i oprogramowanie mogą ulec zmianie bez uprzedniego pisemnego powiadomienia. Aktualizacje produktu mogą skutkować wystąpieniem pewnych różnic między rzeczywistym produktem a podręcznikiem. Prosimy o kontakt z działem obsługi klienta w celu uzyskania najnowszych oprogramowania i dodatkowej dokumentacji.
- Mimo tego mogą wystąpić różnice w danych technicznych, opisach funkcji i działania lub błędy w druku. W przypadku jakichkolwiek wątpliwości lub pytań, prosimy o zapoznanie się z naszym wyjaśnieniem.

- Jeśli nie można otworzyć Podręcznika (w formacie PDF), należy zaktualizować oprogramowanie do obsługi plikówtego typu lub spróbować otworzyć plik za pomocą innego programu.
- Wszystkie znaki towarowe, zarejestrowane znaki towarowe i nazwy firm wymienione w podręczniku są własnością ich prawowitych właścicieli.
- W przypadku wystąpienia jakichkolwiek problemów podczas korzystania z urządzenia należy odwiedzić naszą stronę internetową, skontaktować się z dostawcą lub działem obsługi klienta.
- W przypadku jakichkolwiek wątpliwości lub pytań, prosimy o zapoznanie się z naszym wyjaśnieniem.

Ważne informacje o zabezpieczeniach i ostrzeżeniach

W niniejszym rozdziale opisano prawidłową obsługę terminala dostępu, zapobieganie zagrożeniom i zapobieganie uszkodzeniom mienia. Przed rozpoczęciem korzystania z terminala należy dokładnie zapoznać się z treścią niniejszej instrukcji, przestrzegać jej podczas użytkowania oraz zachować ją do wykorzystania w przyszłości.

Wymagania eksploatacyjne

- Nie należy umieszczać ani instalować terminala w miejscu wystawionym na działanie promieni słonecznych lub w pobliżu źródła ciepła.
- Chronić terminal przed wilgocią, kurzem i sadzą.
- Aby zapobiec upadkowi, terminal powinien być zainstalowany poziomo w stabilnym miejscu.
- Należy unikać zalania i rozpryskania cieczy na terminal oraz należy dopilnować, aby na terminalu nie znajdowały się żadne przedmioty wypełnione cieczą, które mogłyby doprowadzić do zalania terminala.
- Zamontować terminal w dobrze wentylowanym miejscu i nie blokować przepływu powietrza do terminala.
- Zasilać terminal prądem o znamionowym zakresie mocy wejściowej i wyjściowej.
- Nie należy rozmontowywać terminala.
- W przypadku terminala z funkcją pomiaru temperatury ciała:
  - ◇ Terminal z funkcją pomiaru temperatury ciała należy zainstalować wewnątrz pomieszczenia w bezwietrznym środowisku i utrzymywać temperaturę otoczenia na poziomie od 15°C do 32°C.
  - ◇ Po włączeniu zasilania należy podgrzewać terminal z funkcją pomiaru temperatury ciała przez ponad 20 minut, aby umożliwić osiągnięcie przez niego równowagi termicznej.

Bezpieczeństwo elektryczne

- Niewłaściwe użycie baterii może spowodować pożar, wybuch lub zapłon.
- Baterię należy wymienić na taki sam model.
- Należy używać kabli zasilających zalecanych w danym regionie i zgodnych ze specyfikacją mocy znamionowej.
- Należy używać zasilacza dostarczonego wraz z terminalem; w przeciwnym razie może to spowodować obrażenia osób i uszkodzenie urządzenia.
- Źródło zasilania powinno być zgodne z wymogami normy dotczącej obwodu o napięciu znamionowym bardzo niskim (SELV), a zasilanie napięciem znamionowym powinno być zgodne z wymogami dotyczącymi źródła zasilania z własnym ograniczeniem zgodnie z normą IEC60950-1. Należy pamiętać, że wymagania dotyczące zasilania podane są na tabliczce znamionowej urządzenia.
- Podłączyć urządzenie (konstrukcja typu I) do gniazda zasilania z uziemieniem ochronnym.
- Łącznik urządzenia jest urządzeniem rozłączającym. Korzystać z łącznika pod kątem w celu łatwiejszej obsługi.

Spis treści

1 Wymiary i elementy składowe

Figure 1-1 Wymiary i elementy składowe modelu X (mm [cale])

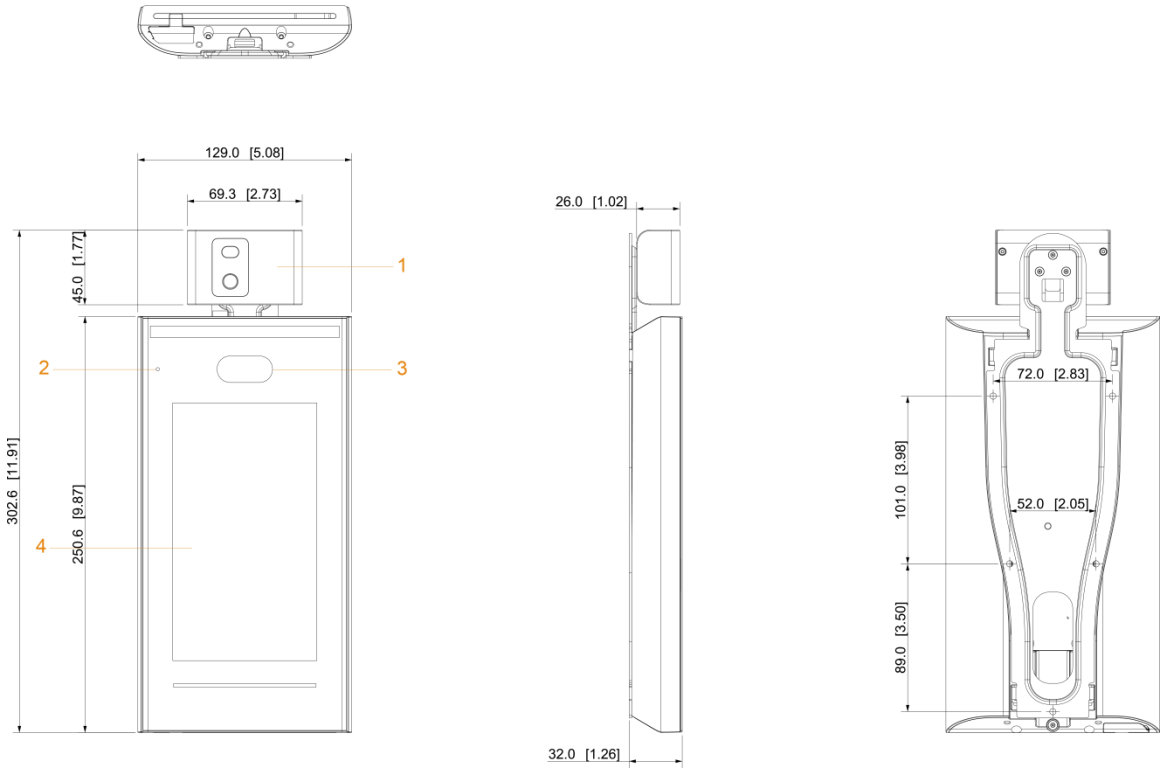


Table 1-1 Opis części składowych (1)

L.p.	Nazwa	L.p.	Nazwa
1	Terminal z funkcją pomiaru temperatury ciała	3	Podwójne kamery
2	Mikrofon	4	Wyświetlacz

Figure 1-2 Wymiary i elementy składowe modelu Y (mm [cale])

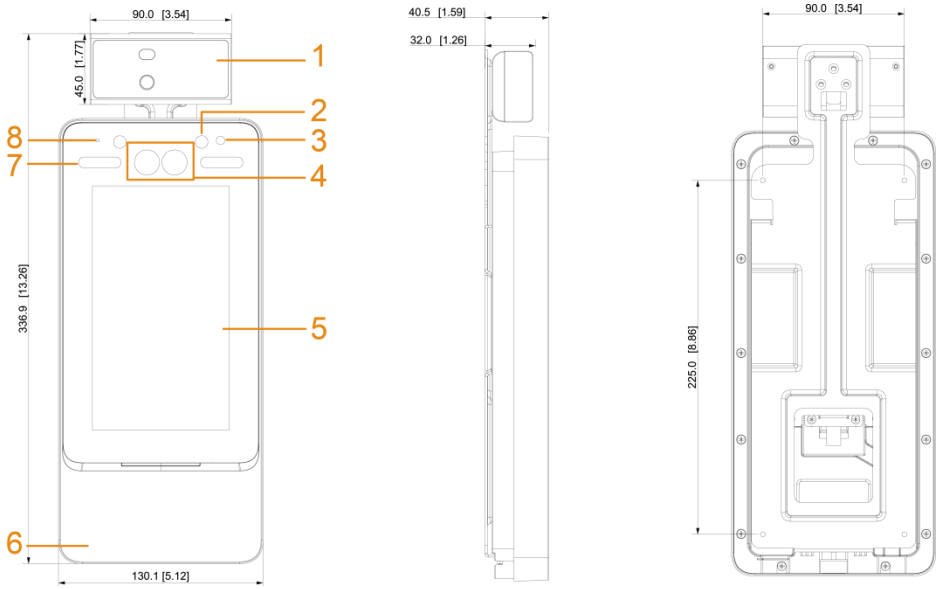


Table 1-2 Opis części składowych (2)

L.p.	Nazwa	L.p.	Nazwa
1	Terminal z funkcją pomiaru temperatury ciała	5	Wyświetlacz
2	Światło podczerwone	6	Obszar przeciągania karty
3	Fototranzystor	7	Oświetlacz LED w kolorze białym
4	Podwójne kamery	8	Mikrofon

2 Podłączenie i instalacja

2.1 Podłączenie przewodów

Połączenie kablowe modelu X i modelu Y jest takie samo. W niniejszym rozdziale, jako przykład, wykorzystano model X.

- Sprawdzić, czy moduł bezpieczeństwa kontroli dostępu jest włączony w menu **Function > Security Module.** Jeśli jest włączony, należy oddzielnie zakupić moduł bezpieczeństwa kontroli dostępu. Moduł bezpieczeństwa wymaga oddzielnego zasilania.
- Po uruchomieniu modułu bezpieczeństwa, przycisk wyjścia, sterowanie blokadą i połączenie przeciwpożarowe będą nieaktywne.

Figure 2-1 Podłączenie przewodów

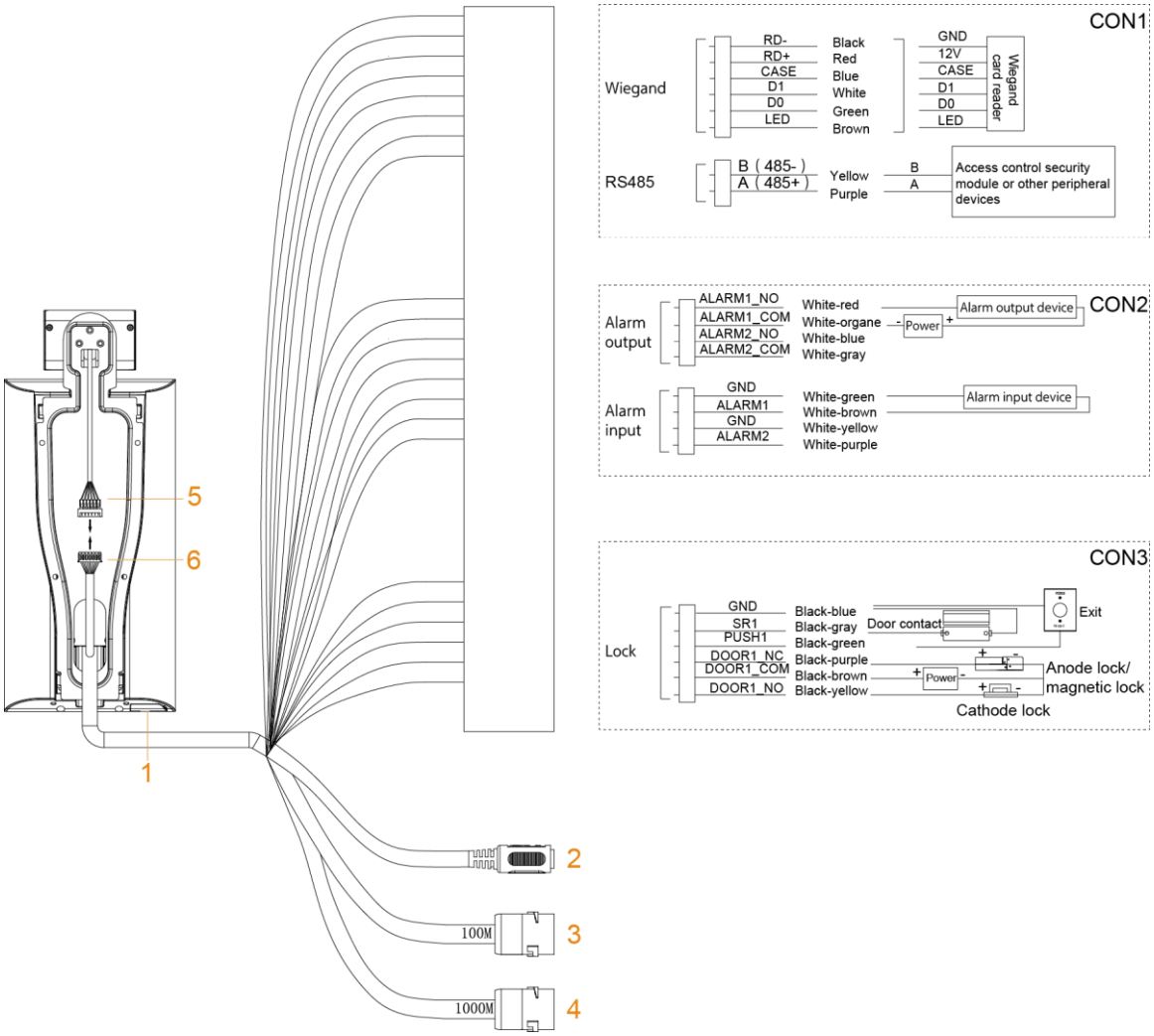


Table 2-1 Opis części składowych

L.p.	Nazwa
1	Port USB
2	Port zasilania
3	Port sieciowy 100M

L.p.	Nazwa
4	Port sieciowy 1000M (obsługiwany tylko przez 7-calowe terminale modelu X)
5, 6	Porty służące do podłączenia terminala z funkcją pomiaru temperatury ciała

2.2 Uwagi dotyczące instalacji

- Jeżeli w odległości 0,5 metra od terminala znajduje się źródło światła, minimalne natężenie oświetlenia nie powinno być mniejsze niż 100 Lux.
- Zaleca się, aby terminal był zainstalowany w pomieszczeniach, w odległości co najmniej 3 metrów od okien i drzwi oraz 2 metrów od źródeł światła.
- Unikać podświetlenia i bezpośredniego światła słonecznego.

Wymagania dotyczące oświetlenia otoczenia

Figure 2-2 Wymagania dotyczące oświetlenia otoczenia

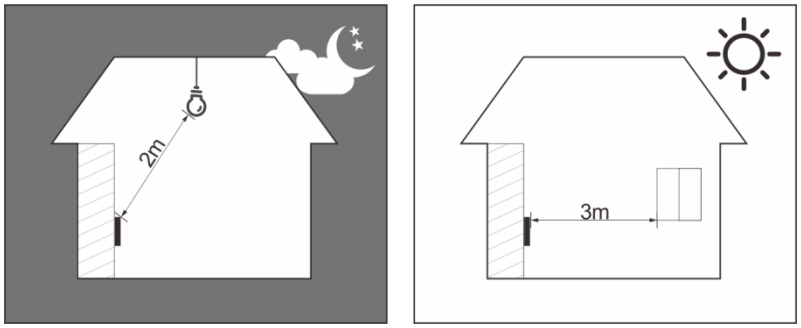
Wymagania dotyczące terminala z funkcją pomiaru temperatury ciała

- Zaleca się zainstalowanie terminala z funkcją pomiaru temperatury ciała w środowisku wewnętrznym bezwietrznym (stosunkowo odizolowanym od zewnątrz) i utrzymywanie temperatury otoczenia na poziomie od 15°C do 32°C.
- Po włączeniu zasilania należy podgrzewać terminal z funkcją pomiaru temperatury przez ponad 20 minut, aby umożliwić osiągnięcie przez nią równowagi termicznej.
- Jeśli nie da się zapewnić odpowiedniego środowiska wewnętrznego (w tym obszarów bezpośrednio zwróconych w stronę pomieszczeń wewnętrznych i zewnętrznych oraz drzwi zewnętrznych), należy ustanowić tymczasowe przejście ze stabilną temperaturą otoczenia w celu umożliwienia przeprowadzenia prawidłowego pomiaru temperatury.
- Czynniki takie jak światło słoneczne, wiatr, zimne powietrze oraz nawiew zimnego i ciepłego powietrza z klimatyzatora mogą łatwo wpływać na temperaturę powierzchni ludzkiego ciała oraz stan pracy terminala, co spowoduje różnice w temperaturze pomiędzy temperaturą mierzoną a rzeczywistą.
- Czynniki wpływające na pomiar temperatury
  - ◇ Wiatr: Wiatr wpływa na temperaturę czoła i na dokładność pomiaru temperatury.
  - ◇ Pocenie się: Pocenie się to naturalny proces chłodzenia organizmu i odprowadzenia ciepła. Kiedy ciało się poci, temperatura również spadnie.
  - ◇ Temperatura pomieszczenia: Jeśli temperatura w pomieszczeniu jest niska, temperatura powierzchni ludzkiego ciała obniży się. Jeśli temperatura w pomieszczeniu jest zbyt wysoka, osoba zacznie się pocić, co wpłynie na dokładność pomiaru temperatury.
  - ◇ Terminal z funkcją pomiaru temperatury ciała jest wrażliwy na fale świetlne o długości fali od 10um do 15um. Unikać używania urządzenia w słońcu, w pomieszczeniach ze świetlówkami,

przy wylotach klimatyzacji, ogrzewania, wylotach zimnego powietrza i w pobliżu szklanych powierzchni.

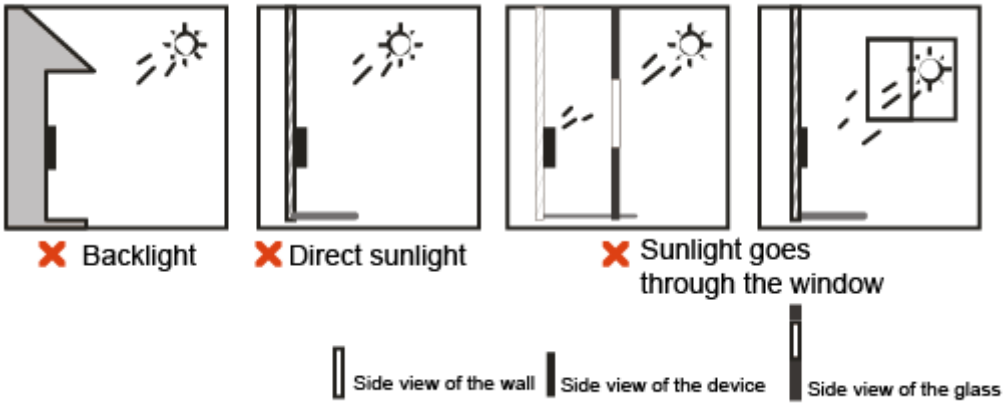
Miejsca zalecane

Figure 2-3 Miejsca zalecane



Miejsca niezalecane

Figure 2-4 Miejsca niezalecane



2.3 Montaż

Montaż modelu X i modelu Y przebiega tak samo. W niniejszym rozdziale, jako przykład, wykorzystano model X.

Należy sprawdzić, czy odległość między obiektywem a podłożem wynosi 1,4 metra.

Figure 2-5 Wysokość montażu

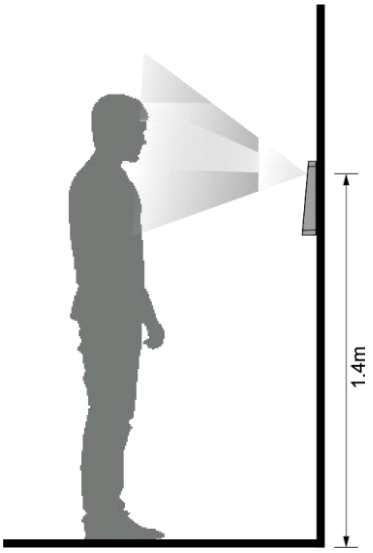
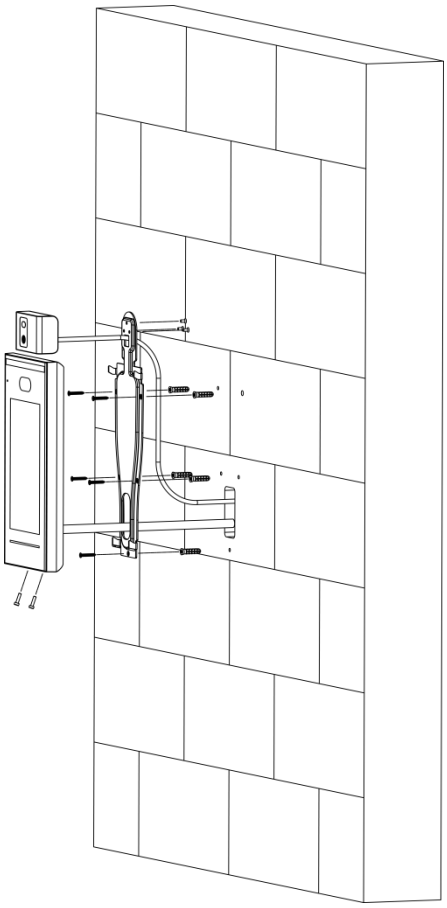


Figure 2-6 Schemat instalacji



Procedura montażu

Step 1 Przymocować czujnik temperatury do uchwytu za pomocą 3 śrub (wymagane tylko w przypadku regulatora dostępu z czujnikiem temperatury).

Step 2 Wywiercić sześć otworów (pięć otworów montażowych w uchwycie i jedno wejście kablowe) w ścianie zgodnie z otworami w uchwycie.

Step 3 Przymocować wspornik do ściany, instalując wkręty rozporowe w pięciu otworach montażowych wspornika.

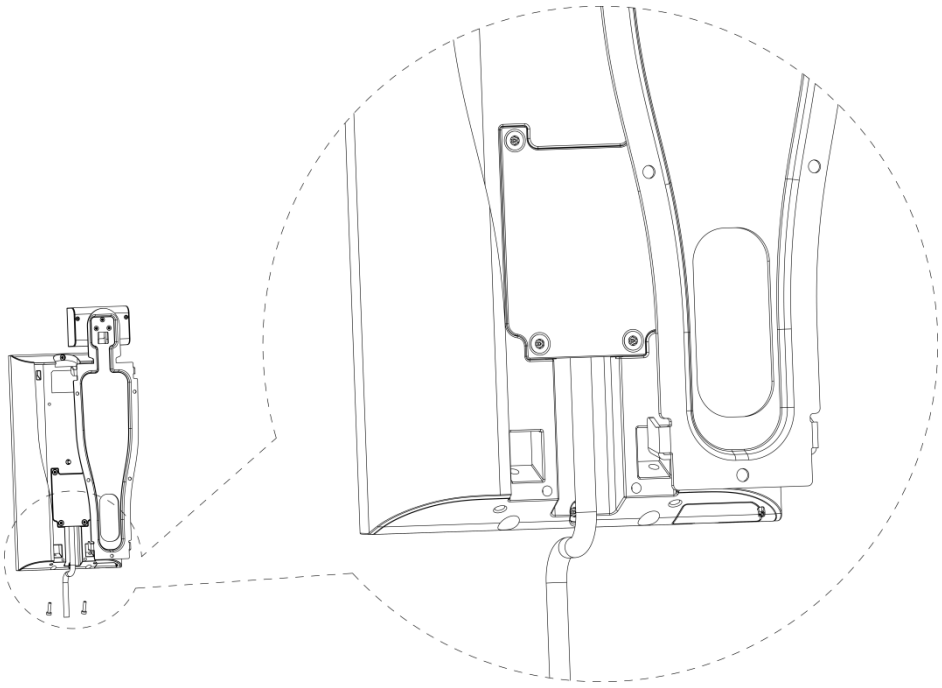
Step 4 Podłączyć kable do terminala. Patrz "2.1 Podłączenie przewodów."

Step 5 Zawiesić terminal na haku wspornikowym.

Step 6 Dokręcić śruby w dolnej części terminala.

Step 7 Nałożyć silikonowy uszczelniacz na gniazdo kabla terminala.

Figure 2-7 Nakładanie uszczelniacza silikonowego



3 Działanie systemu

3.1 Inicjalizacja

Przy pierwszym włączeniu terminala należy ustawić hasło administratora oraz e-mail; w przeciwnym razie nie będzie można użyć terminala.

Figure 3-1 Inicjalizacja

- Hasło administratora można zresetować za pomocą adresu e-mail, który został wprowadzony w momencie ustanawiania hasła.
- Hasło musi składać się z 8 do 32 znaków nieoznaczonych jako puste i zawierać co najmniej dwa rodzaje znaków: duże litery, małe litery, liczbę i znak specjalny (z wyjątkiem " " ; : &).
- W przypadku terminala bez ekranu dotykowego, inicjalizacja odbywa się za pośrednictwem interfejsu WWW. Szczegółowe informacje znajdują się w instrukcji obsługi.

3.2 Dodawanie nowych użytkowników

Nowych użytkowników można dodawać poprzez wprowadzanie identyfikatorów użytkowników, nazwisk, importowanie odcisków palców, obrazów twarzy, haseł i wybieranie poziomów użytkowników.

Poniższe rysunki mają charakter wyłącznie informacyjny i pierwszeństwo ma rzeczywisty interfejs.

Step 1 Wybrać **User > New User**.

Figure 3-2 Nowy użytkownik

Step 2 Skonfigurować parametry na interfejsie.

Table 3-1 Opis parametrów nowego użytkownika

Parametr	Opis
User ID	Wprowadzić identyfikatory użytkowników. Identyfikatory składają się z 32 znaków (w tym cyfr i liter), a każdy identyfikator jest niepowtarzalny.
Nazwa	Podać nazwy zawierające maksymalnie 32 znaki (w tym cyfry, symbole i litery).
Face	Upewnić się, że twarz jest wyśrodkowana w ramce do robienia zdjęć. Następnie zdjęcie zostanie automatycznie zrobione. Szczegółowe informacje na temat nagrywania obrazu twarzy, patrz „ Appendix 2 Uwagi dotyczące rejestrowania/porównania twarzy.”
Card	Można zarejestrować maksymalnie pięć kart dla każdego użytkownika. W interfejsie rejestracji karty wprowadzić numer karty lub przeciągnąć kartę, po czym informacje o karcie zostaną odczytane przez terminal. Funkcję Duress Card można włączyć w interfejsie rejestracji kart. Alarmy zostaną uruchomione, jeśli do otwarcia drzwi użyta zostanie karta sygnalizująca wymuszenie. Jeśli terminal nie posiada modułu odczytu kart, należy podłączyć urządzenie do peryferyjnych czytników kart.

Parametr	Opis
PWD	Hasło do otwierania drzwi. Maksymalna długość hasła wynosi 8 cyfr. Jeśli terminal nie posiada ekranu dotykowego, należy go podłączyć do peryferyjnego czytnika kart. Na czytniku kart znajdują się przyciski.
Level	Można wybrać poziom dostępu dla nowych użytkowników. Do wyboru są dwie opcje. ● User: Użytkownicy mają pozwolenie tylko na otwieranie drzwi. ● Admin: Administratorzy mogą otwierać drzwi, a także posiadać uprawnienia do konfiguracji parametrów. Zaleca się stworzenie więcej niż jednego konta administratora, aby w razie utraty hasła nie utracić dostępu.
Period	Czas, w którym użytkownik może otworzyć drzwi. Szczegółowe ustawienia przedziałów czasowych znajdują się w instrukcji obsługi.
Holiday Plan	Można ustawić plan urlopowy, w trakcie którego użytkownik może otwierać drzwi. Szczegółowe ustawienia planu urlopowego znajdują się w instrukcji obsługi.
Valid Date	Możesz ustawić okres obowiązywania uprawnień do otwierania drzwi dla użytkownika.
User Level	Istnieje sześć poziomów: ● General: Zwykli użytkownicy mogą normalnie otwierać drzwi. ● Blacklist: Gdy użytkownicy znajdujący się na czarnej liście otworzą drzwi, personel serwisowy zostanie o tym poinformowany. ● Guest: Goście mogą otwierać drzwi w określonych godzinach i dniach. Po upływie danego czasu lub okresu nie będą oni w stanie ponownie otworzyć drzwi. ● Patrol: Pracownicy ochrony mogą rejestrować swoją obecność, ale nie mają uprawnień do otwierania. ● VIP: Gdy użytkownik VIP otworzy drzwi, personel serwisowy zostanie o tym poinformowany. ● Special: Gdy osoby VIP odblokują drzwi, nastąpi 5 sekundowe opóźnienie przed ich zamknięciem.
Use Time	Dla użytkownika typu Gość, można ustawić maksymalne czasy, kiedy da się otworzyć drzwi.

Step 3 Dotknąć , aby zapisać konfigurację.

4 Operacje internetowe

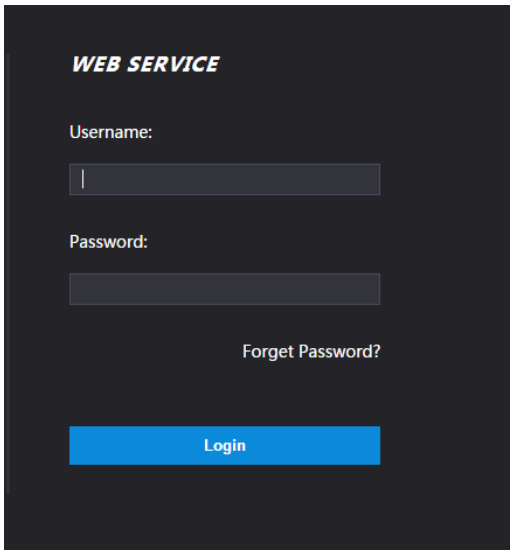
Terminal można konfigurować i obsługiwać za pomocą interfejsu webowego. Za pomocą interfejsu webowego można ustawić parametry, w tym parametry sieciowe, parametry wideo i parametry terminala; można również dostosowywać i aktualizować system. Szczegółowe informacje znajdują się w instrukcji obsługi. W niniejszym rozdziale opisano funkcję logowania.

Przed pierwszym logowaniem do interfejsu webowego należy ustawić hasło i adres e-mail. Ustawione hasło służy do logowania do interfejsu webowego, a adres e-mail do resetowania haseł.

Step 1 Otworzyć przeglądarkę internetową IE, wpisać adres IP (domyślnie 192.168.1.108) terminala w pasku adresu, a następnie nacisnąć klawisz Enter.

- Sprawdzić czy komputer używany do logowania się do interfejsu webowego znajduje się w tej samej sieci LAN co urządzenie.
- 7-calowy terminal w modelu X wyposażony jest w podwójne karty NIC. Domyślny adres IP dla portu sieciowego 1000M to 192.168.1.108, a dla portu sieciowego 100M to 192.168.2.108.

Figure 4-1 Logowanie



Step 2 Należy wprowadzić login i hasło.

- Domyślną nazwą użytkownika o uprawnieniach administratora jest admin, a hasłem logowania hasło ustawione w chwili inicjowania terminala. Należy regularnie zmieniać hasło administratora i przechowywać je w bezpiecznym miejscu.
- Aby przywrócić utracone hasło logowania administratora, należy kliknąć przycisk **Forget Password?** Patrz instrukcja obsługi.

Step 3 Kliknąć **Login**.

Wyświetli się strona główna interfejsu internetowego.

Appendix 1 Uwagi dotyczące pomiaru temperatury

- Po włączeniu zasilania należy podgrzewać terminal z funkcją pomiaru temperatury ciała przez ponad 20 minut, aby umożliwić osiągnięcie przez niego równowagi termicznej.
- Terminal z funkcją pomiaru temperatury ciała należy zainstalować wewnątrz pomieszczenia w bezwietrznym środowisku i utrzymywać temperaturę otoczenia na poziomie od 15°C do 32°C.
- Unikać bezpośredniego nasłonecznienia terminalu z funkcją pomiaru temperatury ciała.
- Należy unikać instalowania terminalu z funkcją pomiaru temperatury ciała naprzeciwko źródła światła i szyby.
- Terminal z funkcją pomiaru temperatury ciała należy trzymać z dala od źródeł wywołujących zakłócenia termiczne.
- Czynniki takie jak światło słoneczne, wiatr, zimne powietrze oraz nawiew zimnego i ciepłego powietrza z klimatyzatora wpływają na temperaturę powierzchni ludzkiego ciała, co spowoduje różnice w temperaturze pomiędzy temperaturą mierzoną a rzeczywistą.
- Pocenie się to naturalny proces chłodzenia organizmu i odprowadzenia ciepła, który powoduje również różnice w temperaturze pomiędzy temperaturą mierzoną a rzeczywistą.
- Należy regularnie (co 2 tygodnie) dokonywać przeglądu terminala z funkcją pomiaru temperatury ciała. Aby utrzymać powierzchnię czujnika temperatury i czujnika odległości w czystości, należy przecierać je miękką i niezakurzoną szmatką.

Appendix 2 Uwagi dotyczące rejestrowania/porównania twarzy

Przed rejestracją

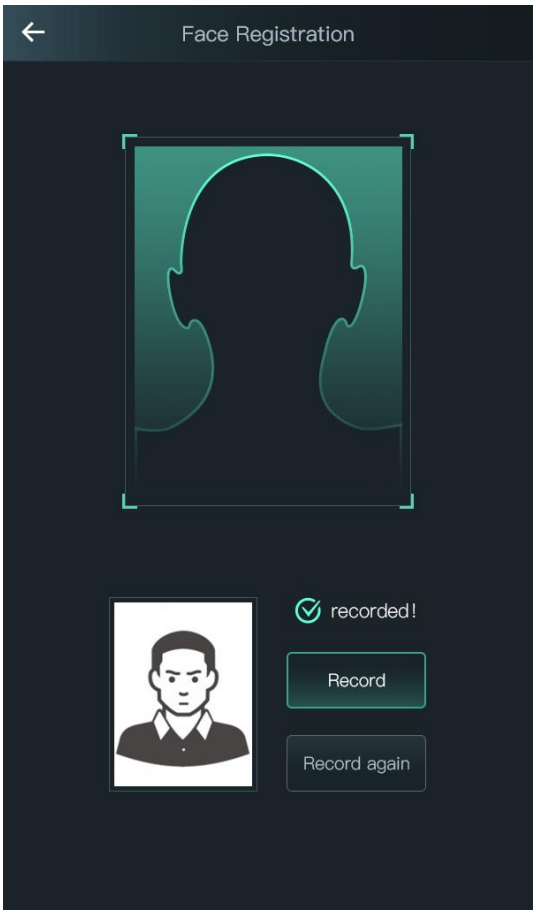
- Okulary, kapelusze i broda mogą wpływać na wydajność rozpoznawania twarzy.
- Nie zakrywać brwi podczas noszenia nakrycia głowy.
- Nie zmieniać zbytnio stylu zarostu przed użyciem urządzenia; w przeciwnym razie rozpoznawanie twarzy może się nie powieść.
- Utrzymywać twarz w czystości.
- Urządzenie należy instalować w odległości co najmniej dwóch metrów od źródła światła i co najmniej trzech metrów od okien lub drzwi; w przeciwnym razie podświetlenie i bezpośrednie światło słoneczne mogą wpływać na działanie urządzenia i rozpoznawanie twarzy.

Podczas rejestracji

Twarze można rejestrować za pomocą terminala lub platformy. Aby zarejestrować się na platformie, należy zapoznać się z instrukcją obsługi platformy.

Umieścić głowę po środku ramki zdjęcia. Twarz zostanie zarejestrowana automatycznie.

Appendix Figure 2-1 Rejestracja

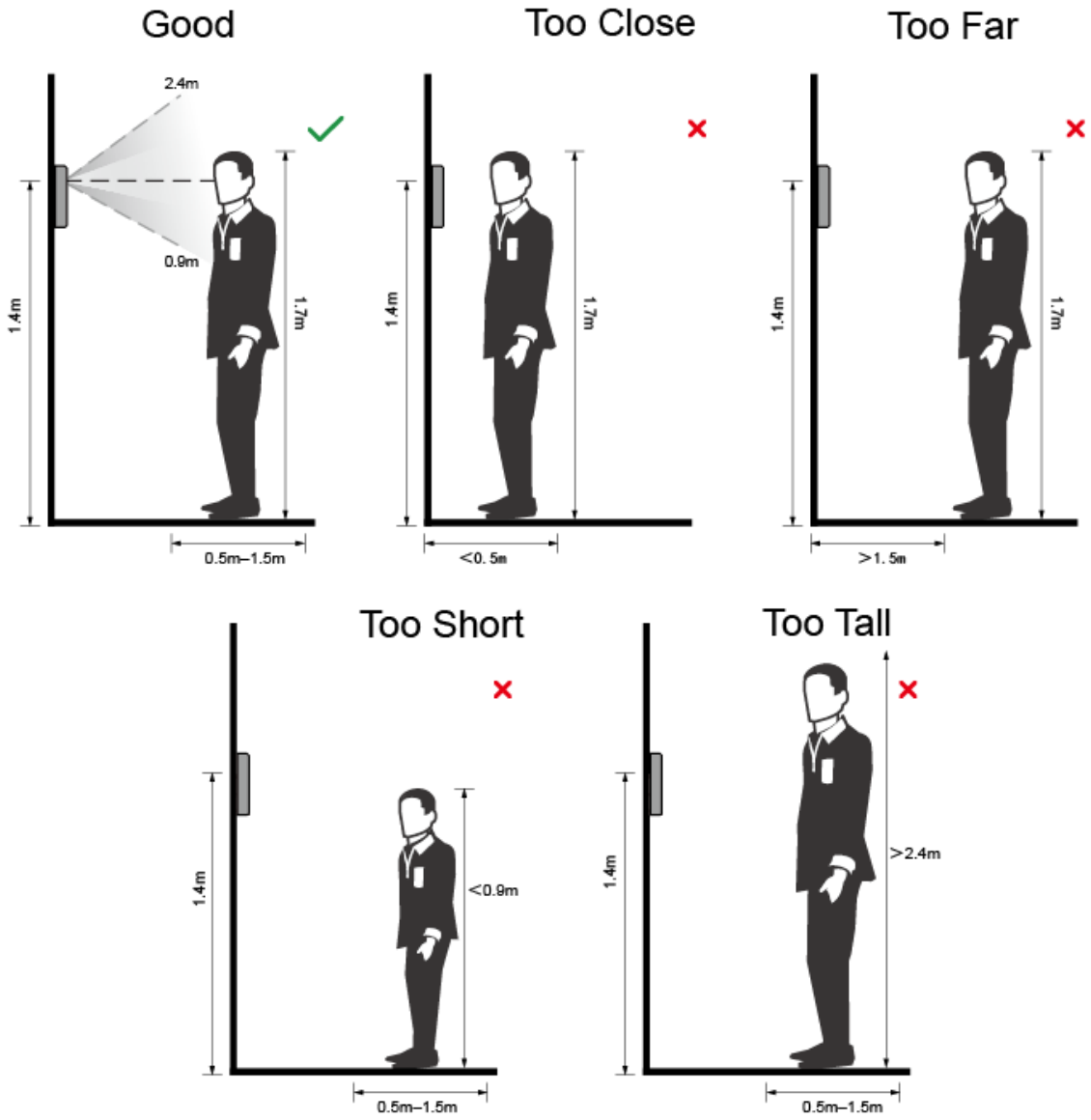


- Nie potrząsać głową ani ciałem, w przeciwnym razie rejestracja może się nie udać.
- Należy unikać jednoczesnego pojawiania się dwóch twarzy w kadrze.

Pozycja twarzy

Jeśli twarz nie znajduje się w odpowiedniej pozycji, może to mieć wpływ na efekt rozpoznawania.

Appendix Figure 2-2 Właściwa pozycja twarzy

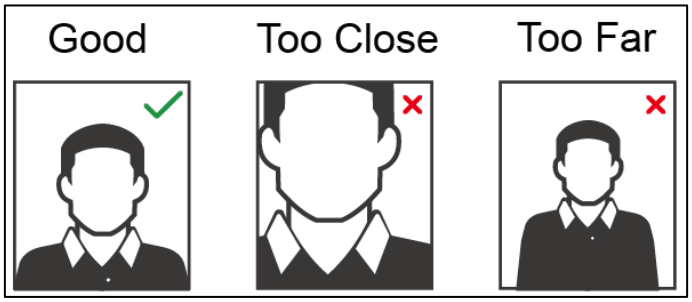


Wymagania dotyczące twarzy

- Należy sprawdzić czy twarz jest czysta, a czoło nie jest zakryte włosami.
- Nie należy nosić okularów, nakrycia głowy, gęstej brody ani innych ozdób twarzy, które wpływają na rejestrację obrazu twarzy.
- Należy skierować twarz w stronę środka kamery, trzymać otwarte oczy i zachować naturalny wyraz twarzy.
- Podczas rejestrowania lub rozpoznawania twarzy, nie należy trzymać twarzy zbyt blisko lub zbyt daleko od aparatu.

Appendix Figure 2-3 Pozycja głowy

Appendix Figure 2-4 Odległość twarzy



- W przypadku importowania obrazów twarzy za pośrednictwem platformy zarządzania, należy upewnić się, że rozdzielczość obrazu mieści się w zakresie 150 × 300-600 × 1200 pikseli, obraz na rozdzielczość większą niż 500 × 500 pikseli, rozmiar obrazu jest mniejszy niż 75 KB, oraz że nazwisko i identyfikator zgadzają się.
- Sprawdzić czy twarz nie zajmuje 2/3 całego obszaru obrazu, a współczynnik proporcji nie przekracza 1:2.

Appendix 3 Zalecenia dotyczące cyberbezpieczeństwa

Bezpieczeństwo cybernetyczne to coś więcej niż tylko modne słowo: to pojęcie, które odnosi się do każdego urządzenia podłączonego do Internetu. Monitoring IP nie jest odporny na zagrożenia cybernetyczne, ale przy zachowaniu podstawowych środków ostrożności i zabezpieczeniu sieci oraz urządzeń sieciowych można zmniejszyć podatność na ataki. Poniżej znajduje się kilka wskazówek i zaleceń, jak zapewnić większe bezpieczeństwo systemu.

Obowiązkowe działania, które należy podjąć w celu zapewnienia bezpieczeństwa sieci:

1. **Używanie silnych haseł**

   Proszę zapoznać się z poniższymi sugestiami dotyczącymi ustawiania haseł:

   - Hasło powinno składać się z co najmniej 8 znaków;
   - Zawierać co najmniej dwa rodzaje znaków, duże i małe litery, cyfry i symbole;
   - Nie zawierać nazwy konta lub nazwy konta w zapisanej od tyłu;
   - Nie należy używać znaków ciągłych, takich jak 123, abc, itp;
   - Nie należy używać nakładających się na siebie znaków, takich jak 111, aaa, itp;

2. **Aktualizacja oprogramowania firmware i oprogramowania klienckiego**

   - Aby zapewnić, że system posiada najnowszą wersję oprogramowania wraz z najnowszymi zmianami i poprawkami dotyczącymi bezpieczeństwa, zgodnie ze standardową procedurą, zalecamy aktualizowanie oprogramowania sprzętu (takiego jak NVR, DVR, kamery IP, itp.). Gdy urządzenie jest podłączone do sieci publicznej, zaleca się włączenie funkcji "auto-check for updates" w celu uzyskania aktualnych informacji o aktualizacjach oprogramowania sprzętowego udostępnionych przez producenta.
   - Sugerujemy pobranie i korzystanie z najnowszej wersji oprogramowania klienckiego.

Zalecenia dodatkowe mające na celu poprawę bezpieczeństwa w sieci

1. **Ochrona fizyczna**

   Sugerujemy zapewnienie fizycznej ochrony sprzętu, w szczególności urządzeń przechowujących dane. Aby ograniczyć fizyczny dostęp osobom nieuprawnionym, grożący uszkodzeniem sprzętu, nieuprawnionym podłączeniem urządzeń wymiennych (takich jak pamięć USB, port szeregowy), itp., należy, na przykład, umieścić sprzęt w szafie w specjalnym pomieszczeniu komputerowym oraz wdrożyć dobrze przemyślane uprawnienia kontroli dostępu oraz udostępniania kluczy.

2. **Regularnie zmieniaj hasła**

   Należy regularnie zmieniać hasła, aby zmniejszyć ryzyko ich odgadnięcia lub złamania.

3. **Ustawianie i aktualizacja haseł, resetowanie haseł**

   Urządzenie obsługuje funkcję resetowania hasła. Należy ustawić odpowiednie informacje pozwalające na resetowanie hasła, takie jak adres skrzynki pocztowej użytkownika i pytania służące do odzyskania hasła. Jeśli informacje ulegną zmianie, należy je odpowiednio wcześnie uaktualnić. Podczas ustawiania pytań zabezpieczających hasło, należy użyć pytań, których nie da się łatwo odgadnąć.

4. **Włączyć blokadę konta**

   Funkcja blokady konta jest domyślnie włączona i zalecamy jej utrzymanie w celu zagwarantowania bezpieczeństwa. Jeśli ktoś kilkakrotnie spróbuje zalogować się przy użyciu błędnego hasła, konto i adres źródłowy IP zostaną zablokowane.

5. **Zmiana domyślnych portów HTTP i innych**

Sugerujemy zmianę domyślnych portów HTTP i innych portów usług na dowolny zestaw numerów pomiędzy 1024~65535, zmniejszając ryzyko, że osoby z zewnątrz będą mogły odgadnąć wykorzystywane adresy portów.

6. **Włączyć HTTPS**

   Sugerujemy włączenie protokołu HTTPS, aby podczas przeglądania sieci korzystać z bezpiecznego kanału komunikacji.

7. **Włączyć Białą listę**

   Zalecamy włączenie funkcji białej listy, która zablokuje dostęp do systemu wszystkim, oprócz tych z określonymi adresami IP. W związku z tym należy dodać do białej listy adres IP komputera oraz adres IP towarzyszącego mu urządzenia.

8. **Wiązanie adresu MAC**

   Zalecamy, aby powiązać adres IP i MAC bramy z urządzeniem, zmniejszając tym samym ryzyko spoofingu ARP.

9. **Rozsądne przypisanie kont i uprawnień**

   Zgodnie z wymaganiami biznesowymi i zarządczymi, należy rozsądnie dodawać użytkowników i przydzielać im minimalny zestaw uprawnień.

10. **Wyłączyć zbędne usługi i wybrać bezpieczne tryby pracy**

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

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

    - SNMP: Wybrać SNMP v3 i ustawić silne hasła szyfrujące oraz hasła uwierzytelniające.
    - SMTP: Wybrać TLS, aby uzyskać dostęp do serwera skrzynek pocztowych.
    - FTP: Wybrać SFTP i ustawić silne hasła.
    - AP hotspot: Wybrać tryb szyfrowania WPA2-PSK i ustawić silne hasła.

11. **Transmisja kodowana audio i wideo**

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

    Przypomnienie: transmisja szyfrowana powodowuje pewną utratę wydajności.

12. **Bezpieczne audyty**

    - Sprawdzanie użytkowników online: sugerujemy regularne sprawdzanie użytkowników, aby sprawdzić, czy miały miejsce logowania bez upoważnienia.
    - Sprawdzanie dziennika: Przeglądając dzienniki, można poznać adresy IP, które były używane do logowania się do urządzeń oraz ich kluczowe operacje.

13. **Dziennik sieciowy**

    Ze względu na ograniczoną pamięć sprzętową, rozmiar dziennika jest ograniczony. W przypadku konieczności długotrwałego przechowywania dziennika, zaleca się włączenie funkcji dziennika sieciowego, co pozwoli na synchronizację najważniejszych rejestrów z sieciowym serwerem.

14. **Budowa bezpiecznego środowiska sieciowego**

    Aby zapewnić większe bezpieczeństwo i zmniejszyć potencjalne zagrożenia, zalecamy:

    - Wyłączyć funkcję mapowania portów w routerze, aby ograniczyć bezpośredni dostęp do urządzeń intranetowych z sieci zewnętrznej.
    - Sieć powinna być podzielona i odizolowana zgodnie z rzeczywistymi potrzebami sieci. Jeśli nie ma wymagań dotyczących komunikacji między dwoma podsieciami, zaleca się wykorzystanie VLAN, GAP i innych technologii w celu podziału i odizolowania sieci.

- Ustanowienie systemu uwierzytelniania dostępu 802.1x w celu zmniejszenia ryzyka nieautoryzowanego dostępu do sieci prywatnych.
- Zaleca się włączenie funkcji firewalla lub czarnej i białej listy, aby zmniejszyć ryzyko ataku na urządzenie.