Jednostka VTO (Wersja 4.3)

Instrukcja obsługi

V1.0.1

Zalecenia dotyczące cyberbezpieczeństwa

Obowiązkowe działania na rzecz bezpieczeństwa cybernetycznego

1. Zmieniaj hasła i używaj silnych haseł:
Głównym powodem hakowania systemów są słabe lub domyślne hasła. Zaleca się natychmiastową zmianę domyślnych haseł i, gdy tylko jest to możliwe, wybranie silnego hasła. Silne hasło powinno składać się z co najmniej 8 znaków i kombinacji znaków specjalnych, cyfr oraz wielkich i małych liter.

2. Aktualizacja oprogramowania
Zgodnie ze standardową procedurą zalecamy aktualizowanie oprogramowania wewnętrznego rejestratora NVR, DVR i kamery IP, aby zapewnić, że system posiada najnowszą wersję oprogramowania wraz z najnowszymi zmianami i poprawkami dotyczącymi bezpieczeństwa.

Zalecenia dodatkowe mające na celu poprawę bezpieczeństwa w sieci

1. Regularnie zmieniaj hasła
Regularnie zmieniaj dane uwierzytelniające na swoich urządzeniach, aby mieć pewność, że dostęp do systemu mają tylko autoryzowani użytkownicy.

2. Zmień domyślne porty HTTP i TCP:
● Zmieniaj domyślne porty HTTP i TCP dla systemów. Są to dwa porty używane do komunikacji i zdalnego wyświetlania kanałów wideo.
● Porty te można zmienić na dowolny zestaw liczb od 1025 do 65535. Unikanie korzystania z domyślnych portów zmniejsza ryzyko, że osoby z zewnątrz będą mogły odgadnąć, z których portów korzystasz.

3. Włącz HTTPS / SSL:
Skonfiguruj certyfikat SSL, aby włączyć protokół HTTPS. Spowoduje to zaszyfrowanie całej komunikacji między urządzeniami a rejestratorem.

4. Włącz filtr IP:
Włączenie filtru IP zablokuje dostęp do systemu wszystkim, oprócz tych z określonymi adresami IP.

5. Zmień hasło ONVIF:
W przypadku starszego firmware'u kamery IP, hasło ONVIF nie zmienia się po zmianie danych logowania. Należy albo zaktualizować oprogramowanie kamery do najnowszej wersji, albo ręcznie zmienić hasło ONVIF.

6. Przekaż tylko potrzebne porty:

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

7. Wyłącz automatyczne logowanie w systemie SmartPSS:
Osoby używające SmartPSS do przeglądania swojego systemu oraz na komputerze używanym przez wiele osób powinny wyłączyć automatyczne logowanie. Dodaje to warstwę bezpieczeństwa, ograniczającą dostępu do systemu użytkownikom bez odpowiednich uprawnień.

8. Użyj innej nazwy użytkownika i innego hasła dla SmartPSS:
W przypadku naruszenia bezpieczeństwa twojego konta w mediach społecznościowych, banku, e-maila, itp. należy uniknąć sytuacji, gdy ktoś wejdzie w posiadanie haseł i zaloguje się nimi do systemu nadzoru wideo. Użycie innej nazwy użytkownika i hasła w systemie bezpieczeństwa utrudni innym odgadnięcie danych logowania do twojego systemu.

9. Ogranicz funkcje kont gości:
Jeśli system jest skonfigurowany dla wielu użytkowników, upewnij się, że każdy użytkownik ma prawa tylko do tych funkcji, których musi używać do wykonywania swojej pracy.

10. UPnP:
● UPnP automatycznie spróbuje przekierować porty w routerze lub modemie. Zwykle byłoby to wskazane. Jeśli jednak system automatycznie przekieruje porty i pozostawione zostaną domyślne dane logowania, do sytemu mogą zalogować się niepożądani użytkownicy.
● Jeśli ręcznie przekierowałeś porty HTTP i TCP w routerze / modemie, funkcja ta powinna niezależnie zostać wyłączona. Wyłączenie funkcji UPnP jest zalecane, gdy nie jest ona wykorzystywana w rzeczywistych aplikacjach.

11. SNMP:
Wyłącz SNMP, jeśli go nie używasz. Jeśli używasz SNMP, powinieneś robić to tylko tymczasowo, wyłącznie w celach śledzenia i testowania.

12. Multicast:
Funkcja Multicast służy do współdzielenia strumieni wideo pomiędzy dwoma rejestratorami. Obecnie nie są znane żadne problemy związane z Multicastem, ale jeśli nie korzystasz z tej funkcji, jej wyłączenie może zwiększyć bezpieczeństwo sieci.

13. Sprawdź Dziennik:
Jeśli podejrzewasz, że ktoś uzyskał nieautoryzowany dostęp do twojego systemu, możesz sprawdzić dziennik systemu. Dziennik systemu pokaże, które adresy IP zostały użyte do zalogowania się do systemu i co zostało udostępnione.

14. Fizycznie zablokuj urządzenie:

W optymalnym scenariuszu należy całkowicie zapobiec nieautoryzowanemu fizycznemu dostępowi do systemu. Najlepszym sposobem na osiągnięcie tego jest zainstalowanie rejestratora w skrytce, zamykanej szafie serwerowej lub w pomieszczeniu zmaykanym na klucz.

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

16. Odizoluj NVR i sieć kamer IP
Sieć, w której znajduje się NVR i kamera IP, nie powinna być tą samą siecią co publiczna sieć komputerowa. Zapobiegnie to dostępowi osób odwiedzających lub niepożądanych do tej samej sieci, której do prawidłowego funkcjonowania wymaga system bezpieczeństwa.

Przedmowa

Informacje ogólne

Niniejsza instrukcja przedstawia działanie interfejsu internetowego.

Wskazówki dotyczące bezpieczeństwa użytkowania

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

Hasła ostrzegawcze	Znaczenie
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

L.p.	Wersja	Wersja poprawki	Data udostępnienia
1	V1.0.0	Pierwsze wydanie	Wrzesień 2018

Informacja o ochronie prywatności

Jako użytkownik urządzenia lub administrator danych możesz gromadzić dane osobowe innych osób, takie jak wizerunek, odciski palców, numer rejestracyjny samochodu, adres e-mail, numer telefonu, GPS, itd. W celu ochrony uzasadnionych praw i interesów innych osób należy przestrzegać lokalnych przepisów i regulacji w zakresie ochrony prywatności stosując środki wykonawcze obejmujące między innymi: zapewnienie widocznej informacji w celu poinformowania osoby, której dane dotyczą, o istnieniu obszaru nadzoru oraz zapewnienie odpowiedniego kontaktu.

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 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 czytnika lub spróbować otworzyć plik za pomocą innego oprogramowania.
- 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

Poniższy opis jest właściwym sposobem korzystania z urządzenia. Przed użyciem należy dokładnie przeczytać instrukcję, aby uniknąć niebezpieczeństwa i utraty mienia. Należy ściśle przestrzegać niniejszej instrukcji podczas korzystania z urządzenia i zachować ją po przeczytaniu.

Wymagania eksploatacyjne

Nie należy umieszczać i instalować urządzenia w miejscu narażonym na bezpośrednie działanie promieni słonecznych lub w pobliżu urządzenia wytwarzającego ciepło.

Nie instalować urządzenia w wilgotnym, zakurzonym lub ciepłym miejscu.

Zachować poziomą instalację lub zainstalować w stabilnym miejscu i nie dopuść do upadku.

Chronić urządzenie przed zalaniem lub wylaniem się na nie płynu; nie należy umieszczać na urządzeniu niczego wypełnionego płynami, aby nie dopuścić do przedostania się płynów do urządzenia.

Proszę zainstalować urządzenie w dobrze wentylowanym miejscu, nie zasłaniać jego otworu wentylacyjnego.

Urządzenie należy podłączać do prądu zgodnego ze znamionowym zakresem wejściowym i wyjściowym.

Nie demontować urządzenia samodzielnie.

Proszę transportować, używać i przechowywać urządzenie w dozwolonym zakresie wilgotności i temperatury.

Zapotrzebowanie na moc

Należy stosować przewody elektryczne (przewody zasilające) zalecane w danym kraju i tylko zgodne ze specyfikacją znamionową!

Należy użyć zasilacza, który spełnia wymagania SELV (bezpieczeństwo bardzo niskiego napięcia) i zasilać napięciem znamionowym zgodnym z ograniczonym źródłem zasilania zgodnie z IEC60950-1.

Szczegółowe wymagania dotyczące zasilania można znaleźć na etykietach urządzeń.

Łącznik urządzenia jest urządzeniem rozłączającym. Podczas normalnego użytkowania należy zachować kąt ułatwiający obsługę.

Spis treści

1 Inicjalizacja

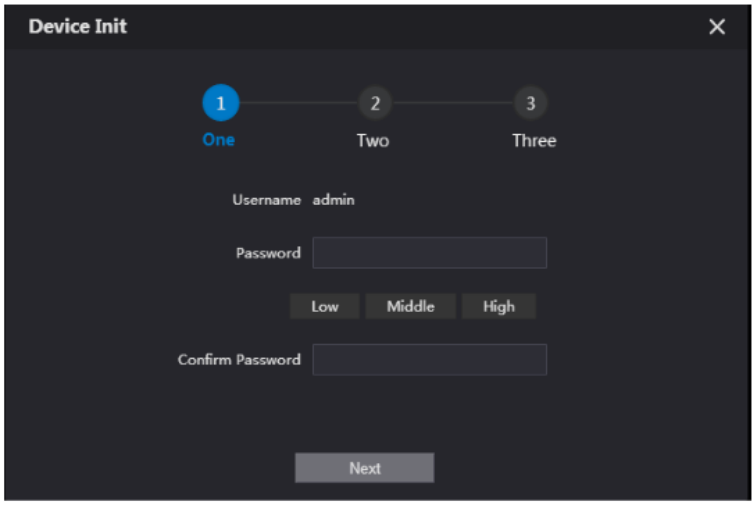
Przy pierwszym logowaniu lub po zresetowaniu VTO należy zainicjować interfejs internetowy. Domyślny adres IP VTO to 192.168.1.110. Upewnij się, że komputer znajduje się w tym samym segmencie sieci co VTO.

Krok 1 Podłącz VTO do źródła zasilania, a następnie uruchom go.

Krok 2 Otwórz przeglądarkę internetową w komputerze PC, następnie wprowadź domyślny adres IP VTO w pasku adresu, a następnie naciśnij przycisk Enter.

Zostanie wyświetlony interfejs **Device Init** . Patrz Rysunek 1-1.

Rys. 1-1 Inicjalizacja urządzenia



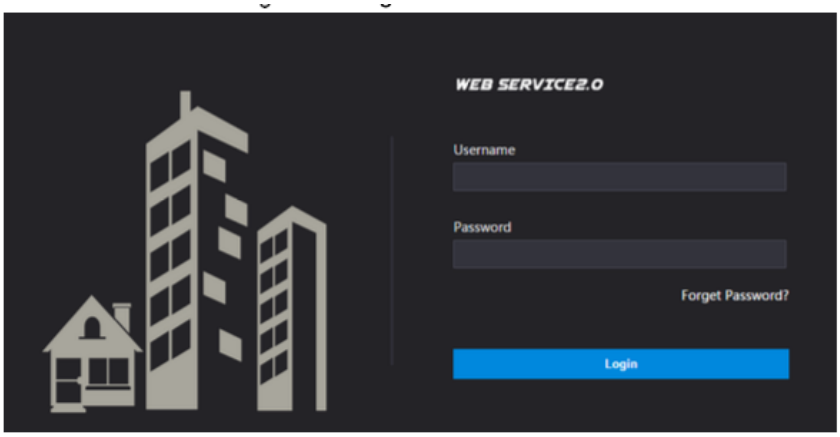
Krok 3 Wprowadź i potwierdź hasło, a następnie kliknij Next. Zostanie wyświetlony interfejs ustawień e-mail.

Krok 4 Zaznacz pole wyboru **Email**, a następnie wpisz swój adres e-mail. Ten adres e-mail posłuży do zresetowania hasła. Zaleca się uzupełnienie tego pola.

Krok 5 Kliknij **Dalej**. Inicjalizacja powiodła się.

Krok 6 Kliknij OK.

Zostanie wyświetlony interfejs logowania. Patrz Rysunek 1-2.



Rysunek 1-2 Interfejs logowania

2 Interfejs logowania

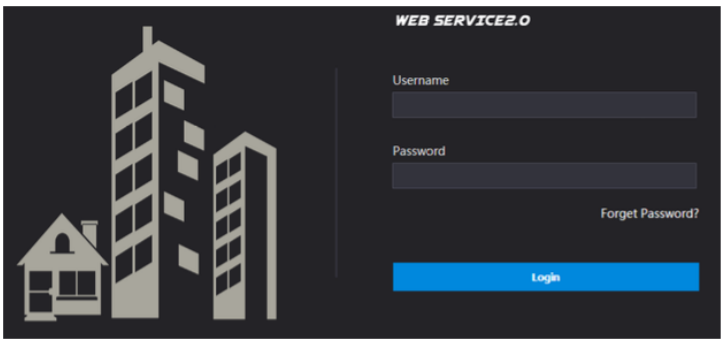
Logowanie

Przed zalogowaniem upewnij się, że komputer znajduje się w tej samej sieci co VTO.

Krok 1 Otwórz przeglądarkę internetową w komputerze, następnie wpisz adres IP VTO w pasku adresu, a następnie naciśnij Enter.

Zostanie wyświetlony interfejs logowania. Patrz Rysunek 2-1.

Rysunek 2-1 Interfejs logowania



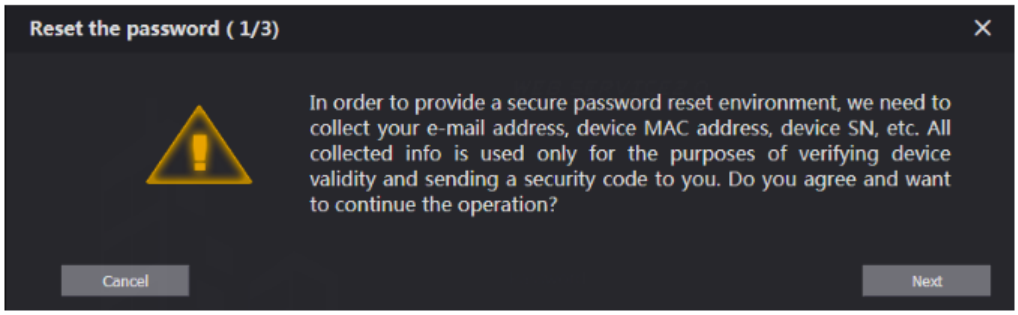
Wpisz „admin” jako nazwę użytkownika, następnie hasło ustawione podczas inicjalizacji, a następnie kliknij **Login**.

Resetowanie hasła

Krok 1 W interfejcie logowania (Rysunek 2 -1) Kliknij **Forgot Password?.**

Zostanie wyświetlone okno dialogowe **Reset the password (1/3)**. Patrz Rysunek 2-2.

Rysunek 2-2 Resetowanie hasła (1/3)



Krok 2 Kliknij **Dalej**.

Zostanie wyświetlone okno dialogowe **Reset the password (2/3)**. Patrz Rysunek 2-3.

Rys. 2-3 Resetowanie hasła (2/3)

Zeskanuj kod QR, aby otrzymać mail z kodem bezpieczeństwa, a następnie wprowadź otrzymany kod bezpieczeństwa.

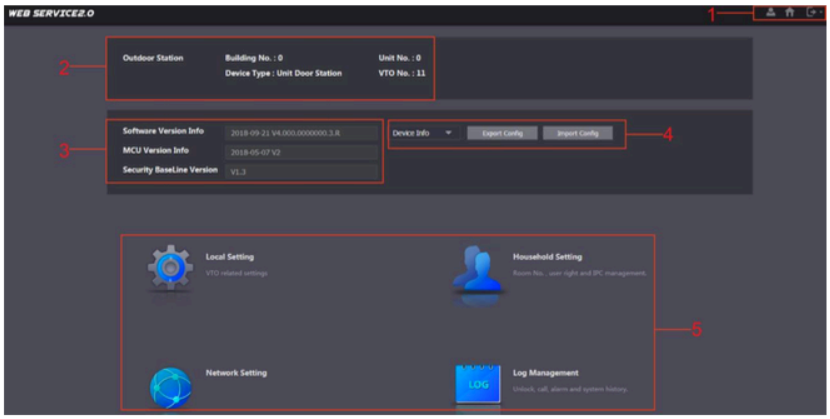
- Jeśli podczas inicjalizacji nie skonfigurowano poczty e-mail, należy skontaktować się z dostawcą lub działem obsługi klienta w celu uzyskania pomocy.
- Aby ponownie uzyskać kod zabezpieczający, odśwież kod QR.
- Użyj kodu zabezpieczającego w ciągu 24 godzin po otrzymaniu. W przeciwnym razie kod wygaśnie.
- Jeśli niepoprawny kod bezpieczeństwa zostanie wprowadzony 5 razy z rzędu, konto zostanie zablokowane na 5 minut.

Kliknij przycisk **Next**, a następnie wyświetlone zostanie okno dialogowe **Reset the password (3/3)** . Ustaw i potwierdź nowe hasło zgodnie z instrukcją, a następnie kliknij **OK**.

3 Interfejs główny

Zaloguj się do interfejsu internetowego VTO, aby wyświetlić interfejs główny. Patrz Rysunek 3-1.

Rysunek 3-1 Interfejs główny



Wprowadzenie do głównego interfejsu, patrz Tab.3 -1.

Tabela 3-1 Wprowadzenie do interfejsu głównego

L.p.	Funkcja	Opis
1	Funkcje ogólne	Poniższe przyciski wyświetlane są przez cały czas Kliknij  , aby zmienić hasło i adres e-mail. Kliknij,  aby przejść do głównego interfejsu. Kliknij  , aby się wylogować, zrestartować VTO lub przywrócić VTO do ustawień fabrycznych.
2	Informacje o VTO	Można wyświetlić ogólne informacje o VTO, w tym numer budynku, numer urządzenia, typ urządzenia i numer VTO.
3	Informacje o systemie	Można przejrzeć wersję oprogramowania, wersję MCU i wersję zabezpieczeń.
4	Konfigurator	Wybierz opcję **Device Info** lub **User Info**, a następnie możesz wyeksportować konfigurację VTO lub informacje o użytkowniku do komputera lub zaimportować je z niego.
5	Obszar	Kliknij przyciski, aby przejść do odpowiedniego menu.

4 Ustawienie lokalne

W niniejszym rozdziale przedstawiono sposób konfiguracji typu VTO, numeru VTO, wideo i audio, hasła dostępu, czasu systemowego i funkcji bezpieczeństwa.

Ogólne operacje:

- Po przeprowadzeniu każdej konfiguracji należy kliknąć przycisk **Confirm**, aby zapisać, i kliknąć przycisk **Refresh**, aby wyświetlić ostatnią zmianę.
- Jeśli klikniesz przycisk **Default**, wszystkie konfiguracje na bieżącej stronie zostaną przywrócone do wartości domyślnych; aby zapisać należy kliknąć przycisk **Confirm**.

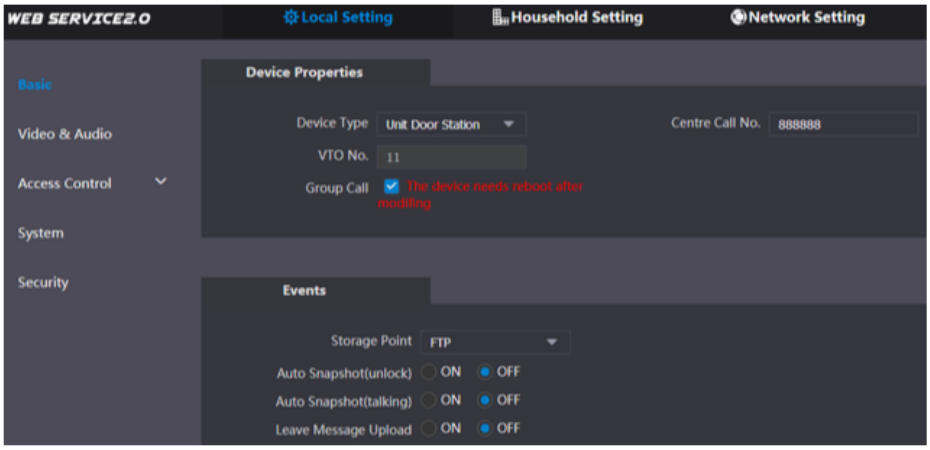
Informacje podstawowe

W tym rozdziale przedstawiono konfigurację typu urządzenia VTO, numeru VTO oraz automatycznej pamięci masowej.

Krok 1 W interfejsie głównym (rysunek 3-1), wybierz **Local Setting > Basic.**

Zostanie wyświetlony interfejs **Basic**. Patrz Rysunek 4-1.

Rysunek 4-1 Informacje podstawowe



Krok 2 Konfiguracja parametrów - szczegółowy opis patrz Tabela 2 -1.

Tabela 4-1 Opis parametrów podstawowych

Parametr	Opis
Typ urządzenia	Możesz wybrać Unit Door Station lub Fence Station. • **Unit Door Station**: Zwykle jednostka jest instalowana wewnątrz osiedla z określonym numerem budynku lub lokalu. • **Fence Station**: Zwykle instaluje się je przy bramie wjazdowej. Aby zadzwonić do konkretnego lokalu, należy wprowadzić numer budynku, numer jednostki i numer lokalu. Nie można zostawić wiadomości ani przejrzeć wpisu do listy kontaktów na stacji ogrodzeniowej. Numer budynku i numer lokalu dostępne są tylko gdy inne serwery pracują jako serwer SIP. Patrz "6.4 Serwer SIP".

Parametr	Opis
	• Stacja ogrodzeniowa jest zwykle używana, gdy inne serwery pracują jako Serwer SIP
Numer telefonu do centrum	Skonfiguruj numer centrum zarządzania by umożliwić dzwonienie do centrum zarządzania za pomocą każdego VTO lub VTH znajdującego się w sieci. Domyślny numer to 888888.
Numer VTO.	Numer VTO może być użyty do rozróżnienia każdego VTO i jest zazwyczaj skonfigurowany zgodnie z numerem urządzenia lub budynku. Do serwera SIP można dodawać urządzenia VTO za pomocą ich numerów. Jeśli VTO nie działa jako serwer SIP, wówczas można zmienić jego numer VTO (zaloguj się na stronie internetowej VTO, a następnie możesz zmienić numer).
Rozmowy grupowe	Zaznaczyć pole wyboru, aby włączyć tę funkcję, a w przypadku połączenia z głównym VTH, urządzenia dodatkowe VTH również odbierze połączenie.
Miejsce przechowywania	Można wybrać tylko **FTP** - wszystkie kadry zostaną automatycznie zapisane na serwerze FTP. • Auto Snapshot (unlock) Aby włączyć tę funkcję, należy wybrać opcję **ON** (Wł.), po czym system wykonuje zdjęcie za każdym razem, gdy drzwi zostaną odblokowane. • Auto Snapshot (talking) Wybierz opcję **ON**, aby włączyć tę funkcję, a następnie system będzie wykonywał zdjęcia za każdym razem, gdy użytkownik VTH odbierze połączenie z VTO. • Leave Message Upload Wybierz opcję **ON**, aby włączyć tę funkcję, a następnie system automatycznie wyśle wiadomości od gości na serwer FTP. • Najpierw należy włączyć funkcję FTP. Patrz "6.2 FTP". • Jeśli w głównym VTH znajduje się karta SD, pozostałe komunikaty zostaną domyślnie zapisane na karcie SD. • Aby odbierać komunikaty, należy ustawić wartość czasu komunikatów VTO na więcej niż 0. Patrz instrukcja obsługi VTH.

Krok 3 Kliknij **Confirm**, aby zapisać.

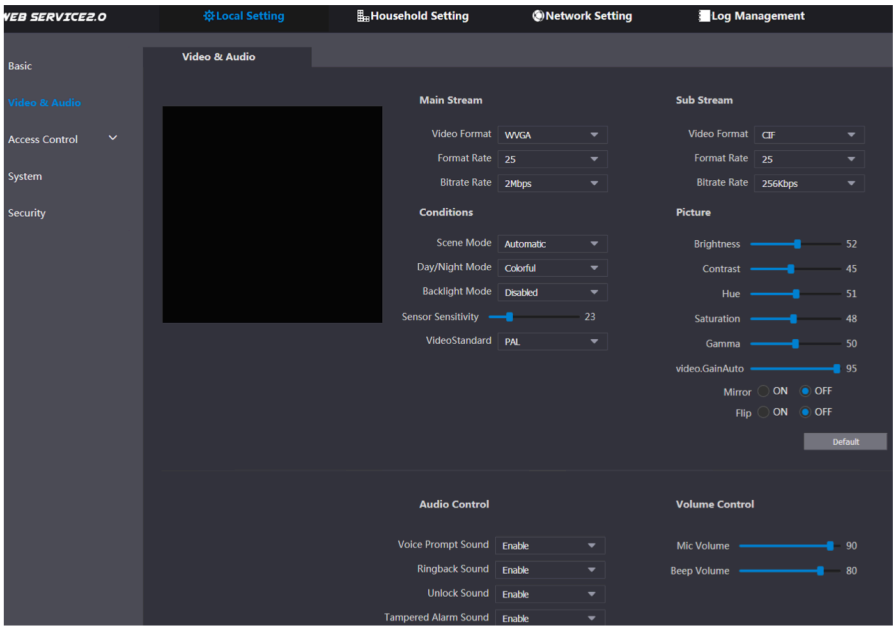
4.2 Obraz wideo i dźwięk

W tej sekcji przedstawiono sposób konfigurowania formatu i jakości obrazu wideo rejestrowanego przez VTO oraz ustawienia sterowania dźwiękiem.

Krok 1 W interfejsie głównym (rysunek 3-1), wybierz **Local Setting > Video & Audio.**

Zostanie wyświetlony interfejs **Video & Audio.** Patrz Rysunek 4-2.

Obraz wideo i dźwięk



Krok 2 Po skonfigurowaniu parametrów ustawienia zaczną natychmiast obowiązywać. Patrz tabela 4-2

Tabela 4-2 Opis parametrów wideo

Parametr		**Opis**
Główny strumień	Video Format	Wybierz rozdzielczość wideo spośród **720P**, **WVGA** i **D1**.
	Format Rate	Skonfiguruj liczbę klatek na sekundę. Można wybrać od **1** do **25** klatek w standardzie **PAL** i od **1** do **30** w standardzie **NTSC**. Im większa jest wartość, tym płynniejszy będzie obraz wideo.
	Bitrate Rate	Skonfiguruj ilość danych przesyłanych w ciągu 1 sekundy. Możesz dostosować do potrzeb. Im większa jest ta wartość, tym lepsza będzie jakość obrazu.
Sub Stream (podstrumień)	Video Format	Wybierz rozdzielczość wideo spośród **CIF**, **WVGA**, **QVGA i D1**.
	Format Rate	Skonfiguruj liczbę klatek na sekundę. Można wybrać od **1** do **25** klatek w standardzie **PAL** i od **1** do **30** w standardzie **NTSC**. Im większa jest wartość, tym płynniejszy będzie obraz wideo.
	Bitrate Rate	Skonfiguruj ilość danych przesyłanych w ciągu 1 sekundy. Możesz dostosować do potrzeb. Im większa jest ta wartość, tym lepsza będzie jakość obrazu.
Warunki	Scene Mode (tryb sceny)	Dostosuj obraz, aby dopasować go do różnych scenariuszy. Do wyboru są następujące opcje: **Automatyczna**, **Słoneczna**, **Nocna** i **Wyłączona**. Domyślnie jest on **automatyczny**.
	Day/Night Mode (tryb dzienny/nocny)	Można wybrać tryb **automatyczny**, **kolorowy** lub **czarno-biały**.
	BackLight Mode	Można wybrać jeden z następujących trybów: • **Disabled**: brak podświetlenia. • **Backlight**: kamera uzyskuje wyraźniejszy obraz ciemnych obszarów podczas nagrywania pod światło.

Parametr		Opis
		• **Wide dynamic**: system przyciemnia jasne obszary i kompensuje ciemne obszary, aby zapewnić lepszy obraz. • **Inhibition**: system ogranicza jasne obszary i zmniejsza efekt halo, aby przyciemnić ogólną jasność.
	Sensor Sensitivity	Dostosuj wartość, a im większa jest wartość, tym łatwiej uruchomi się czujnik.
	Video Standard	Wybierz **PAL** lub **NTSC** w zależności od urządzenia wyświetlającego.
Picture (obraz)	Brightness	Zmienia wartość, aby dostosować jasność obrazu. Im większa jest wartość, tym jaśniejszy będzie obraz, a im mniejsza wartość tym ciemniejszy obraz. Obraz może być zamglony, jeśli podano zbyt dużą wartość.
	Contrast	Zmienia kontrast obrazu. Im większa wartość, tym większy będzie kontrast między jasnymi i ciemnymi obszarami i odwrotnie. Jeśli wartość jest zbyt duża, ciemny obszar będzie za ciemny a jasny obszar może być prześwietlony. Obraz może być zamglony, jeśli wartość jest zbyt mała.
	Hue	Sprawia, że kolor jest głębszy lub jaśniejszy. Zaleca się domyślną wartość, którą ustala czujnik światła.
	Saturation (nasycenie)	Sprawia, że kolor jest głębszy lub jaśniejszy. Im większa wartość, tym głębszy kolor, a im niższa, tym jaśniejszy. Wartość nasycenia nie zmienia jasności obrazu.
	Gamma	Zmienia jasność obrazu i poprawia jego zakres dynamiczny w sposób nieliniowy. Im większa jest wartość, tym jaśniejszy będzie obraz, a im mniejsza wartość tym ciemniejszy obraz.
	Video.GainAuto (wzmocnienie)	Wzmocnij sygnał wideo, aby zwiększyć jasność obrazu. Jeśli wartość jest zbyt duża, w obrazie pojawi się więcej szumów.
	Mirror (odbicie)	Wybierz ustawienie **On**, aby obrócić obraz w lewo i prawo.
	Flip (odwrócenie)	Wybierz ustawienie **On**, aby obrócić obraz do góry nogami.
Audio Control	Aby włączyć lub wyłączyć dźwięk, wybierz opcję **Enable** or **Disabled**.	
Volume Control (głośność)	Mic Volume (głośność	Dostosuj wartość, a im większa jest wartość, tym głośniejsze ustawienie mikrofonu w VTO.
	Beep Volume (dźwięk	Dostosuj wartość, a im większa jest wartość, tym głośniejsze ustawienie dźwięku systemu.

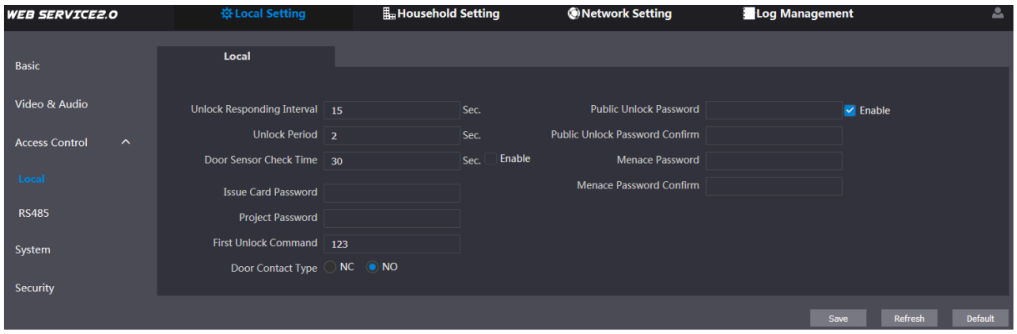
4.3 Kontrola dostępu

W niniejszym rozdziale przedstawiono sposób konfigurowania zamka, w tym czas reakcji na odblokowanie, polecenie otwarcia drzwi, hasła do wydania karty, wymuszenia hasła i protokołu sterowania windą.

4.3.1 Interfejs Lokalny

Krok 1 W głównym interfejsie (rysunek 3-1), wybierz **Local Setting > Access Control > Local.**
Wyświetli się interfejs **lokalny**. Patrz Rysunek 4-3.

Rys 4-3 Lokalny



Konfiguracja parametrów - szczegółowy opis patrz Tabela 4-3.

Tabela 4-3 Opis parametrów kontroli dostępu

Parametr	Opis
Unlock Responding Interval (czas pomiędzy odblokowaniem)	Odstęp czasowy do ponownego odblokowania po poprzednim otwarciu, mierzony w sekundach.
Unlock Period (czas odblokowania)	Czas, przez jaki zamek pozostaje otwarty po odblokowaniu, mierzony w sekundach.
Door Sensor Check Time (czas sprawdzenia czujnika drzwi)	Jeśli zainstalowano czujnik drzwi, można skonfigurować czas, a jeśli czas odblokowania przekracza czas **czujnika drzwi**, uruchomiony zostanie alarm czujnika drzwi i powiadomione zostanie centrum zarządzania. • Wybierz **Enable**, aby drzwi nie zostały zablokowane dopóki czujniki drzwi nie zetknie się ze sobą. • Jeśli nie zaznaczysz opcji **Enable**, drzwi będą nadal zablokowane po upłynięciu **okresu odblokowania**.
Wydaj hasło do karty	To hasło może być użyte do wydania nowej karty. ● To hasło jest tylko dla administratorów lub inżynierów. ● Domyślnie jest to 888888.
Hasło do projektu	Można go użyć do przejścia do interfejsu inżynierskiego, a domyślnie jest to 888888. Hasło do projektu jest tylko dla administratorów lub inżynierów.
First Unlock Command (polecenie pierwszego odblokowania)	Możesz podłączyć telefon innej firmy, na przykład telefon SIP, do VTO, i użyć go do zdalnego otwarcia drzwi.
Door Contact Type (typ [illegible])	Wybierz **NC** lub **NO** odpowiadający zamkowi, którego używasz.
Public Unlock Password (publiczne hasło odblokowania)	Zaznacz pole wyboru **Enable**, skonfiguruj publiczne hasło do odblokowania, a następnie wszyscy mieszkańcy będą w stanie otworzyć drzwi za pomocą ustalonego hasła.
Public Unlock Password Confirm (zatwierdzenie publicznego hasła)	

Parametr	Opis
Menace Password	W każdej z tych dwóch sytuacji można użyć specjalnego hasła, gdy gdy użytkownik zostaje zmuszony do wprowadzenia kodu otwarcia drzwi. • Domyślnie, niebezpieczne hasło to to samo hasło co hasło publiczne, tylko zapisane od tyłu. • Można skonfigurować dowolny numer w zależności od potrzeb. Po użyciu wymuszonego hasła: • W przypadku korzystania z VTO jako serwera SIP, pojawi się wpis alarmowy w **Log Management > Alarm.** • W przypadku korzystania z platformy jako serwera SIP, można podłączyć urządzenie, które zostanie powiadomione o zarejestrowanym alarmie.
Menace Password Confirm	

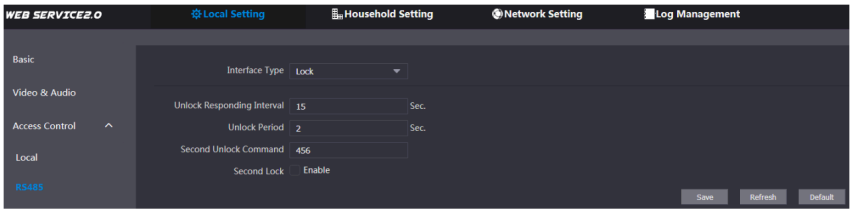
Krok 3 Kliknij Save.

4.3.2 RS485

W niniejszym rozdziale przedstawiono konfigurację kontroli dostępu urządzeń RS-485, w tym blokady i sterowania windami.

Krok 1 W głównym interfejsie (rysunek 3-1), wybierz **Local Setting > Access Control > RS485.** Wyświetli się interfejs **RS485** . Patrz Rysunek 4-4.

Rys. 4-4 RS485



Krok 2 Skonfiguruj parametry, a na liście **Interface Type** możesz wybrać **Lock** lub **Lift Control**. Szczegółowy opis patrz Tabela 4-4.

Tabela 4-4 Opis parametrów kontroli dostępu RS-485

Parametr		Opis
Blokada	Unlock Responding Interval (czas pomiędzy odblokowaniem)	Odstęp czasowy do ponownego odblokowania po poprzednim otwarciu, mierzony w sekundach.
Lock	Unlock Period (czas odblokowania)	Czas, przez jaki zamek pozostaje otwarty po odblokowaniu, mierzony w sekundach.
Blokada	Second Unlock Command (polecenie drugiego	Możesz podłączyć telefon innej firmy, na przykład telefon SIP, do VTO, i użyć go do zdalnego otwarcia drzwi.
Lock	Second Lock	Do urządzenia RS-485 można podłączyć jedne dodatkowe drzwi. • Jeśli zaznaczysz pole wyboru **Enable**, wówczas drugi zamek zostanie domyślnie otwarty po naciśnięciu przycisku odblokowania, przeciągnięciu karty dostępu lub użyciu hasła odblokowującego. • Jeśli nie zaznaczysz pola wyboru **Enable**, wówczas pierwszy zamek zostanie domyślnie otwarty po naciśnięciu przycisku odblokowania, przeciągnięciu karty dostępu lub użyciu hasła odblokowującego.
Lift Control	Lift Control Protocol	Wybierz protokół zgodnie z potrzebą, aby włączyć funkcję kontroli wind. Teraz możesz skonfigurować piętra, na których ma zatrzymywać się winda.

Parametr		Opis
	Baud Rate	Wprowadź szybkość transmisji wymaganego urządzenia RS-485 firmy zewnętrznej.
	Data Bit	Elementy te służą do debugowania portów szeregowych.
	Check Bit	
	Stop Bit	

Krok 3 Kliknij Save.

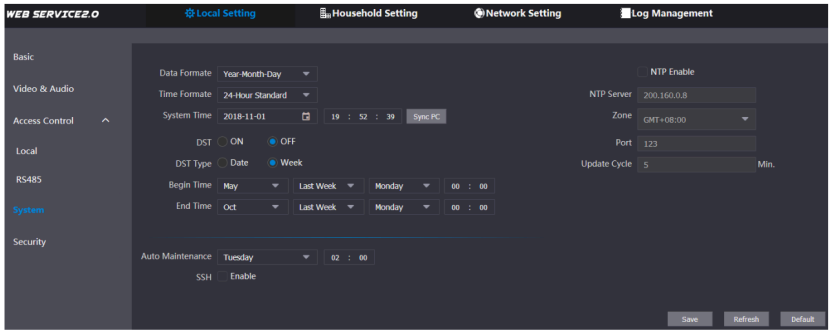
4.4 System

Niniejszy rozdział opisuje sposób konfiguracji formatu daty, czasu oraz serwera NTP.

W interfejsie głównym (rysunek 3-1), wybierz **Local Setting > System.**

Wyświetli się interfejs **systemowy**. Patrz Rysunek 4-5.

Rys. 4-5 System



Krok 2 Konfiguracja parametrów - szczegółowy opis patrz Tabela 4-5.

Tabela 4-5 Opis parametrów systemowych

Parametr	Opis
Date format (format daty)	Można wybrać rok-miesiąc-dzień, miesiąc-miesiąc-rok, oraz dzień-miesiąc-rok.
Time format (format czasu)	Skonfiguruj format czasu na **12-godzinny** lub **24-godzinny**.
System time (Czas systemowy)	Skonfiguruj datę, czas i strefę czasową systemu VTO. ⚠ Nie należy samodzielnie zmieniać czasu systemowego; może to spowodować problemy podczas wyszukiwania plików i publikowanie zdjęć lub powiadomień. Przed zmiana czasu systemowego, wyłącz nagrywanie wideo lub automatyczne zrzuty.
Sync PC	Kliknąć, aby zsynchronizować czas systemowy VTO z czasem systemowym komputera.
DST	Wybierz opcję **ON**, aby włączyć funkcję DST.
DST Type	Wybierz opcję **Date**, aby zdefiniować konkretną datę dla DST, lub wybierz dla
Begin time	Skonfiguruj czas początkowy i końcowy dla DST.
End Time)	Skonfiguruj czas początkowy i końcowy dla DST.
NTP Enable	Zaznaczyć pole wyboru, aby włączyć synchronizację NTP.

Parametr	Opis
NTP Server	Wprowadź nazwę domeny serwera NTP.
Zone	Strefa czasowa aktualnego obszaru.
Port	Numer portu serwera NTP.
Update cycle (cykl aktualizacji)	Przedział czasu, w którym VTO synchronizuje czas z serwerem NTP - nadłuższy wynosi 30 minut.
Auto Maintenance	Wybierz dzień i godzinę konserwacji automatycznej, po której VTO zrestartuje się.
SSH	Zaznaczyć **Enable**, aby podłączyć urządzenia do debuggowania do VTO za pomocą protokołu SSH.

Krok 3 Kliknij Save.

4.5 Bezpieczeństwo

Krok 1 W interfejsie głównym (rysunek 3-1), wybierz **Local Setting > Security.** Wyświetli się interfejs **bezpieczeństwa**. Patrz Rysunek 4-6.

Rysunek 4-6 Bezpieczeństwo

Krok 2 Konfiguracja parametrów - szczegółowy opis patrz Tabela 4-6.

Tabela 4-6 Opis parametrów bezpieczeństwa

Parametr	Opis
CGI Enable	Zaznaczyć pole wyboru, aby użyć polecenia CGI.
Reset Password	Zaznaczyć pole wyboru, aby zresetować hasło.

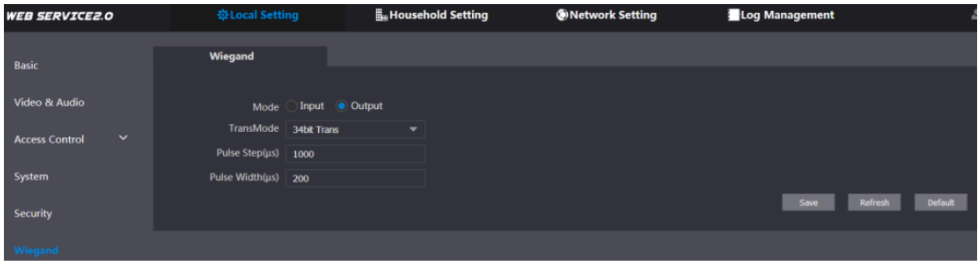
Krok 3 Kliknij **Save**, aby zapisać.

4.6 Wiegand

W poniższym rozdziale przedstawiono sposób konfiguracji parametrów urządzeń

Krok 1 Wiegand. W interfejsie głównym (rysunek 3-1), wybierz **Local Setting > Wiegand.** Wyświetli się interfejs **Wiegand**. Patrz Rysunek 4-7.

Rysunek 4-7 Wiegand



Krok 2 Skonfiguruj parametry. Patrz tabela 4-7

Tabela 4-7 Opis parametrów Wiegand

Parametr	Opis
Mode	Wybierz opcję **Input** lub **Output** w zależności od typu urządzenia Wiegand.
TransMode	Wybierz szybkość transmisji spośród **34 bit**ów, **66 bitów** i **26 bitów**. Im większa wartość, tym szybsza będzie transmisja.
Pulse Step (μs)	Częstotliwość sygnału Wiegand wynosi domyślnie 1000.
Pulse Width (μs)	Maksymalna wartość sygnału Wiegand wynosi domyślnie 200.

Krok 3 Kliknij Save.

4.7 Rozpoznawanie twarzy

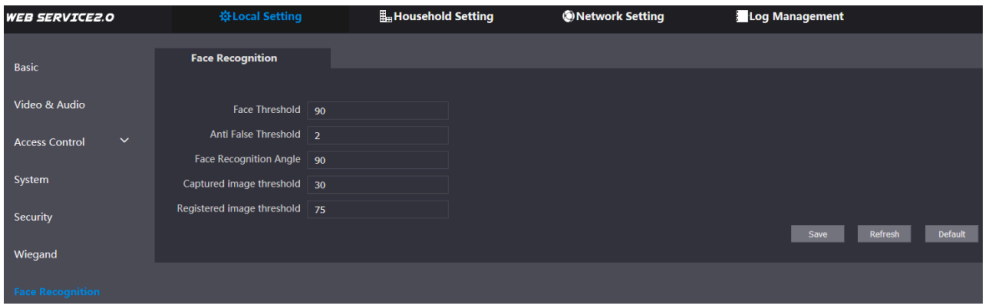
Rozpoznawanie twarzy dostępne jest w wybranych modelach.

W nieniejszym rozdziale przedstawiono sposób konfigurowania progu rozpoznawania twarzy, progu przeciwodblaskowego oraz kąta rozpoznawania twarzy.

Krok 1 Wybierz kolejno opcje **Local Setting > Face Recognition.**

Wyświetli się interfejs **Rozpoznawanie twarzy** . Patrz Rysunek 4-8.

Rysunek 4-8 Rozpoznawanie twarzy



Krok 2 Skonfiguruj parametry rozpoznawania twarzy. Patrz tabela 4-8

Tabela 4-8 Opis parametrów rozpoznawania twarzy

Parametr	Opis
Face Threshold	Im większa wartość, tym większe będzie wymagane podobieństwo twarzy do zapisanych danych, aby otworzyć drzwi.
Anti False Threshold	Im większa wartość, tym mniejsza szansa, że system rozpozna obiekt jako ludzką twarz, zwiększając tym dokładność rozpoznawania.
Face Recognition Angle	Im większa wartość, tym większy jest kąt, pod jakim można obrócić twarz podczas rozpoznawania.
Captured image threshold	Im wyższa wartość, tym lepsza jakość uchwyconych obrazów.
Registered image threshold	Im większa wartość, tym wyższa jest wymagana jakość obrazu by został on poprawnie zarejestrowany.

Krok 3 Kliknij Save.

5 Ustawienie dla gospodarstw domowych

Niniejszy rozdział opisuje sytuację, w której VTO działa jako serwer SIP (patrz 6.3), i omawia sposób dodawania, modyfikowania i usuwania urządzeń VTO, VTH, VTS i IPC oraz sposób wysyłania wiadomości z serwera SIP do innych urządzeń VTO i VTH. Jeśli używasz innych serwerów jako serwera SIP, zapoznaj się z odpowiednią instrukcją opisującą ich szczegółową konfigurację.

5.1 Zarządzanie numerem VTO

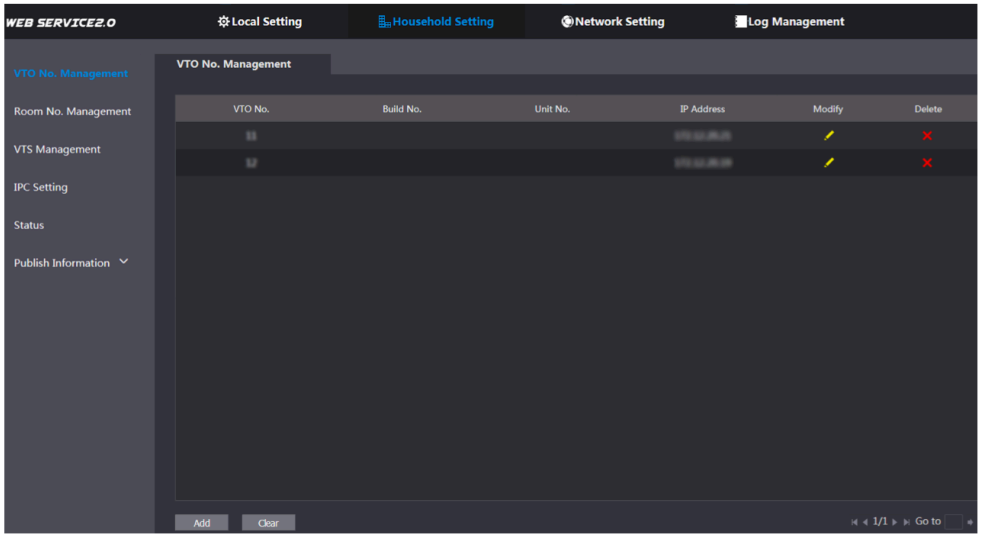
5.1.1 Dodawanie VTO

Do serwera SIP można dodać urządzenia VTO. Dodatkowo wszystkie urządzenia VTO podłączone do tego samego serwera SIP mogą między sobą nawiązywać połączenia wideo.

Krok 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz kolejno opcje **Household Setting > VTO. No. Management**.

Wyświetli się interfejs **zarządzania numerem VTO**. Patrz Rysunek 5-1.

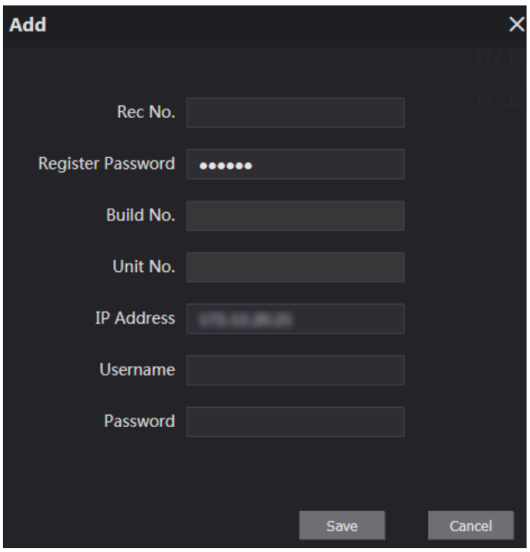
Zarządzanie numerem VTO



Krok 2 Kliknij na Add

Zostanie wyświetlony interfejs Dodawania. Patrz Rysunek 5-2.

Rysunek 5-2 Dodawanie VTO



Krok 3 Skonfiguruj parametry i upewnij się, że dodałeś również serwer SIP. Patrz tabela 5-1

Tabela 5-1 Dodaj konfigurację VTO

Parametr	Opis
Rec No.	Numer VTO, który został skonfigurowany dla docelowego VTO. Zobacz szczegóły w Tabeli 4. -1."
Register Password	Pozostaw wartość domyślną.
Build No.	Dostępne tylko wtedy, gdy inne serwery pracują jako serwer SIP.
Unit No.	
IP Address	Adres IP docelowego VTO.
Username	Nazwa użytkownika i hasło do interfejsu webowego docelowego VTO.
Password	

Krok 4 Kliknij Save.

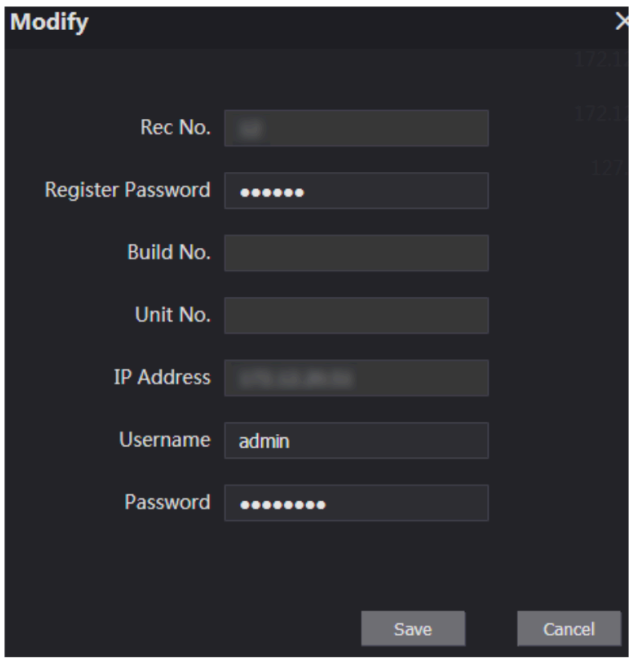
5.12 Zmiana informacji o VTO

Nie można modyfikować lub usuwać obecnie używanego VTO.

Krok 1 W interfejsie **zarządzania numerem VTO** (Rysunek 5-1), kliknij przycisk .

Wyświetli się ekran wprowadzania **modyfikacji.** Patrz Rysunek 5-3.

Zmiana informacji o VTO



Krok 2 Możesz zmienić **numer rekordu, nazwę użytkownika i hasło**. Szczegółowe informacje znajdują się w tabeli 5-1.

Krok3 Kliknij Save.

5.1.3 Usuwanie VTO

Nie można modyfikować lub usuwać obecnie używanego VTO.

W interfejsie **zarządzania numerem VTO** (Rysunek 5-1), kliknij , aby usunąć VTO jeden po drugim;

Kliknij przycisk **Clear**, aby usunąć wszystkie VTO.

5.2 Zarządzanie numerem lokalu

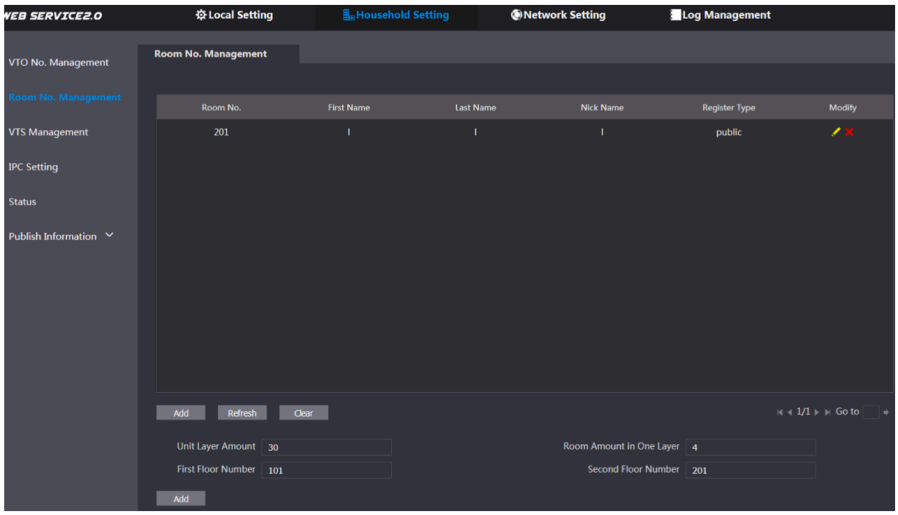
5.2.1 Dodanie numeru lokalu

Można dodać planowany numer lokalu do serwera SIP, a następnie skonfigurować numer lokalu na urządzeniach VTH, aby połączyć je z siecią.

Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz opcję **Household Setting > Room No. Management.**

Wyświetli się interfejs **zarządzania numerem lokalu**. Patrz Rysunek 5-4.

Rysunek 5-4 Zarządzanie numerem lokalu



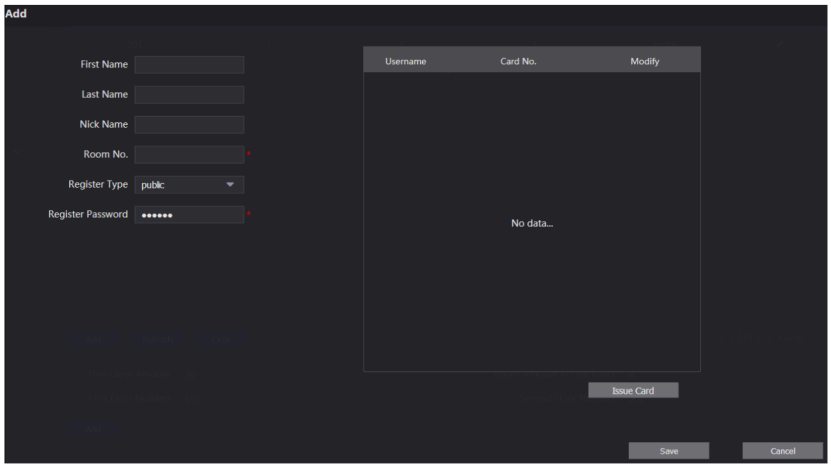
Krok 2 Możesz dodać pojedynczy numer lokalu lub przeprowadzić operację masowo.

- Dodaj pojedynczy numer lokalu

1) Kliknij przycisk **Add** na środku ekranu.

Zostanie wyświetlony interfejs Dodawania. Patrz Rysunek 5-5.

Rysunek 5-5 Dodaj pojedynczy numer lokalu



2) Skonfiguruj informacje o pomieszczeniu oraz dodaj szczegółowy opis. Patrz tabela 5-2

Tabela 5-2 Informacje o lokalach

Parametr	Opis
First Name	Wpisz informacje potrzebne do rozróżnienia każdego lokalu.
Last Name	
Nick Name	
Room No.	Numer zaplanowanego lokalu.
Register Type (typ rejestru)	Wybierz **publiczny**, **lokalny** jest zarezerwowany do wykorzystania w przyszłości.

Parametr	Opis
Register Password	Zachowaj wartość domyślną.

3) Kliknij przycisk **Save**.

Wyświetli się dodany numer lokalu. Kliknij **.** aby zmienić informacje o lokalu, i kliknij , aby usunąć lokal.

- Masowe dodawanie numerów lokali

1) Skonfiguruj **liczbę pięter**, **liczbę lokali na jednym piętrze**, numer **pierwszego** i **drugiego piętra** zgodnie z aktualnym stanem.

2) Kliknij przycisk **Add** na dole pozycji.

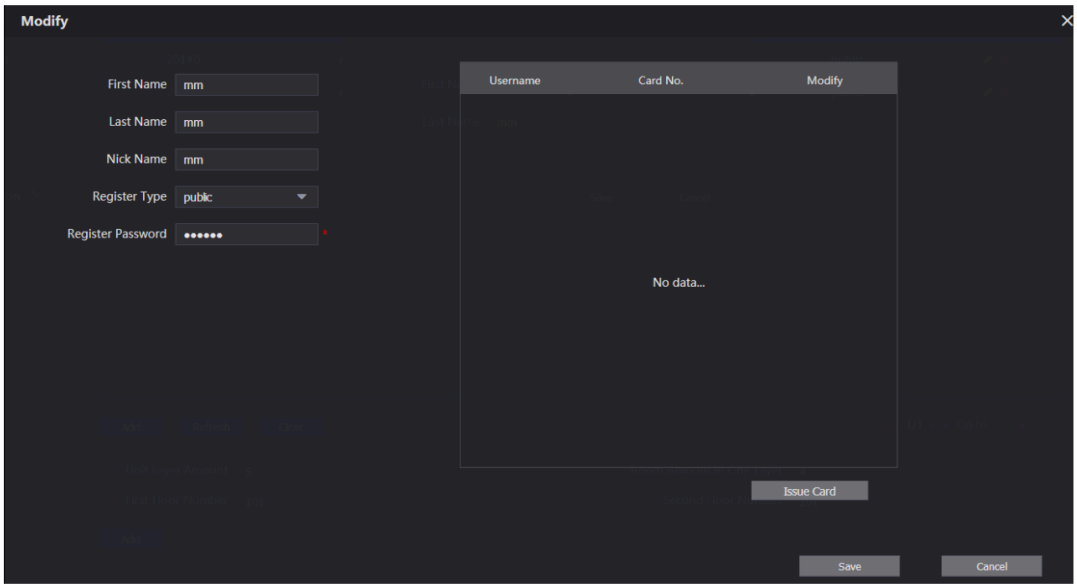
Wyświetlą się wszystkie dodane numery lokali. Kliknij przycisk **Refresh**, aby wyświetlić najnowszy stan lub kliknij przycisk **Clear**, aby usunąć wszystkie numery lokali.

5.2.2 Zmiana numeru lokalu

Krok 1 W interfejsie **zarządzania numerem lokalu** (Rysunek 5-4) kliknąć ..

Wyświetli się ekran wprowadzania **modyfikacji.** Patrz Rysunek 5-6.

Zmiana numeru lokalu



Krok 2 Możesz zmienić nazwy lokali. Szczegółowe informacje znajdują się w tabeli 5-2.

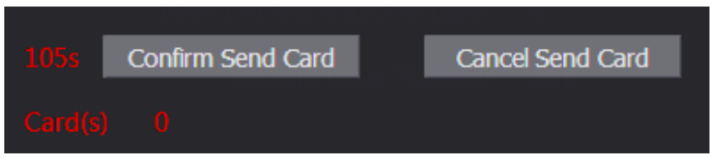
Krok 3 Kliknij Save.

5.2.3 Wydanie karty dostępu

Możesz wydać kartę do lokalu, a także ustawić ją jako kartę główną, lub ustawić status jako utracona.

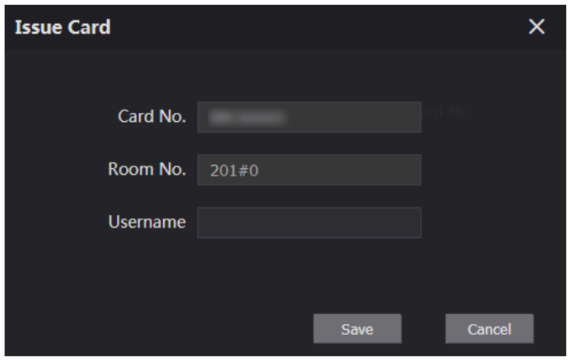
Krok 1 W interfejsie Zmiany numeru lokalu (Rysunek 5-6) kliknąć **Issue Card** (Wydaj kartę). Zostanie wyświetlone powiadomienie o odliczaniu. Patrz Rysunek 5-7.

Rysunek 5-7 Zawiadomienie o odliczaniu



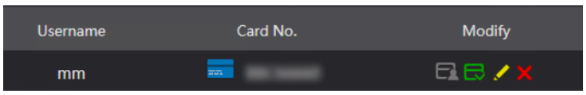
Krok 2 Przeciągnij kartę, która ma być uwierzytelniona przez VTO, a następnie wyświetli się okno dialogowe **Issue Card (Wydaj kartę**). Patrz Rysunek 5-8.

Wydanie karty



Krok 3 Wpisz imię i nazwisko, a następnie kliknij przycisk **Save**, po czym kliknij przycisk **Confirm Send Card** na powiadomieniu z odliczaniem (rysunek 5-7).
Zostanie wyświetlona wydana karta dostępu. Patrz 5-9

Rysunek 5-9. Wydana karta dostępu



Krok 4 Można skonfigurować kartę dostępu.

- Kliknij aby ustawić ją jako kartę główną, po czym ikona zmieni się na .
- Karta główna może być użyta w VTO do wydania karty dostępu do tego lokalu. Kliknij ponownie, aby wznowić.
- Kliknij aby zmienić jej stan na ‘utracona’. Ikona zmieni się w .. Karta w stanie utraconym nie może być użyta do otwarcia drzwi. Kliknij ponownie, aby wznowić.
- Kliknij aby zmienić nazwę użytkownika.
- Kliknij aby skasować kartę.

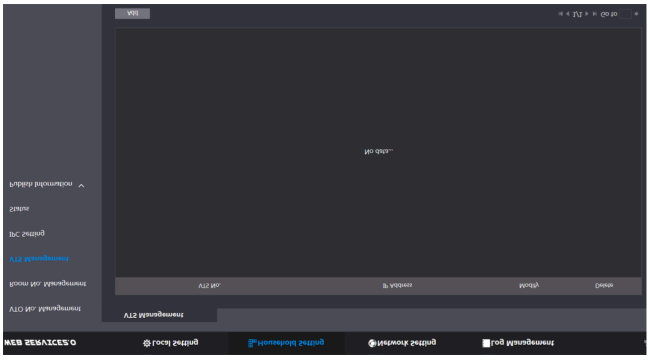
5.3 Zarządzanie VTS

Można dodać urządzenie VTS do serwera SIP, a VTS może służyć jako centrum zarządzania. Może zarządzać wszystkimi urządzeniami VTO i VTH w danej sieci, wykonywać lub odbierać z nich połączenia wideo oraz tworzyć podstawowe konfiguracje. Szczegółowe wprowadzenie znajduje się w odpowiednim podręczniku użytkownika.

Krok 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz kolejno opcje **Household Setting > VTS Management**

Zostanie wyświetlony interfejs **zarządzania VTS**. Patrz Rysunek 5-10.

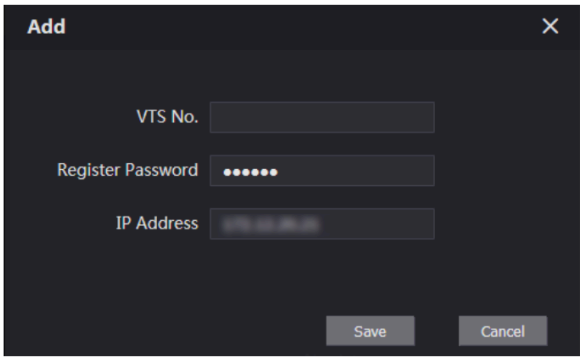
5.3 Zarządzanie VTS



Krok 2 Kliknij Add

Zostanie wyświetlony interfejs Dodawania. Patrz Rysunek 5-11.

Rysunek 5-11 Dodawanie VTO



Krok 3 W systemie VTS wybierz kolejno **Config > Advance Config,** a następnie wprowadź hasło (domyślnie 123456), a następnie wybierz **SIP Server, numer VTS** zostanie wyświetlony jako **nazwa użytkownika (**zazwyczaj jest to 888888XXX).

Krok 4 Skonfiguruj parametry - szczegółowy opis znajdziesz w tabeli 5-3.

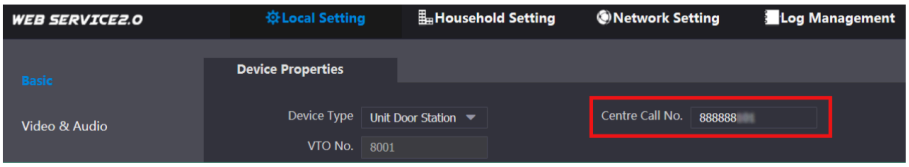
Tabela 5-3 Dodaj konfigurację VTO

Parametr	Opis
VTS No.	Numer VTO, który został skonfigurowany dla docelowego VTO.
Register Password	Pozostaw wartość domyślną.
IP Address	Adres IP docelowego VTS.

Krok 5 Kliknij przycisk Save, a następnie wyświetli się dodany VTS. Kliknij  w celu zmiany adresu IP, a następnie kliknij  , w celu usunięcia.

Krok 6 Wybierz kolejno opcje **Local Setting > Basic,** a następnie wpisz numer dodanego VTS w polu **Center Call No.** Teraz możesz połączyć się z VTS, naciskając przycisk centrum obsługi telefonicznej na VTO. Patrz Rysunek 5-12.

Rysunek 5-12 Numer telefonu do centrum



Krok 7 Kliknij przycisk **Confirm**.

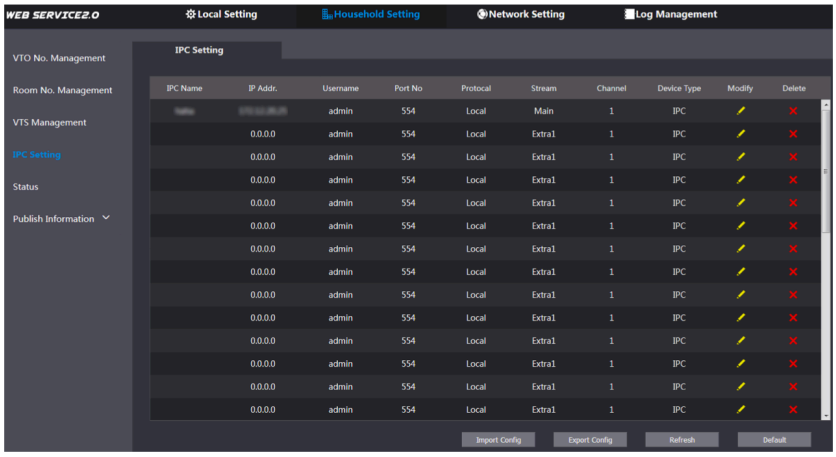
5.4 Ustawienia IPC

Do serwera SIP można dodać IPC, NVR, HCVR i XVR, wówczas wszystkie podłączone VTH mogą rejestrować obraz za pomocą dodanych kamer.

Krok 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz kolejno opcje **Household Setting > IPC Setting**

Wyświetli się interfejs **ustawień IPC**. Patrz Rysunek 5-13.

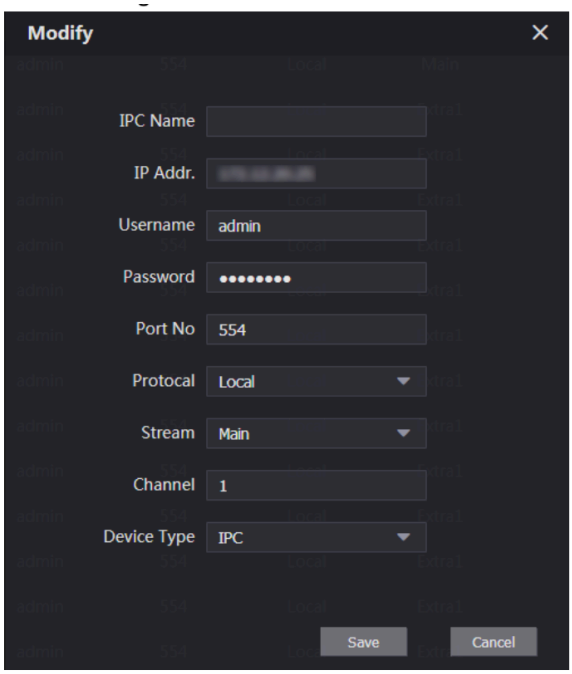
Rysunek 5-13 Ustawienia IPC



Krok 2 Całkowita liczba urządzeń, które można dodać jest stała. Można dodać wymagane urządzenie klikając  .

Wyświetli się ekran wprowadzania **zmian.** Patrz Rysunek 5-14.

Rysunek 5-14 Dodawanie IPC



Krok 3 Skonfiguruj parametry - szczegółowy opis znajdziesz w tabeli 5-4.

Tabela 5-4 Dodawanie konfiguracji IPC

Parametr	Opis
IPC Name	Wpisz nazwę dodawanego urządzenia.
IP Addr.	Adres IP urządzenia.
Username	Nazwa użytkownika i hasło do interfejsu webowego jednostki.
Password	
Port No.	Pozostaw wartość domyślną.
Protokół	Wybierz z **Local** lub **Onvif**.
Stream	Wybierz z **Main** lub **Extra1**; główny strumień ma lepszą jakość obrazu, ale także potrzebuje większej przepustowości.
Channel	Zdefiniuj kanał dla urządzenia.
Device Type	W zależności od potrzeb wybierz z **IPC**, **NVR**, **HCVR** i **XVR**.

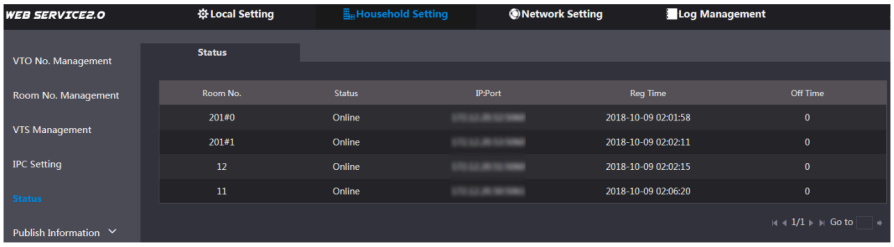
Krok 4 Kliknij przycisk Save, a następnie wyświetli się dodane urządzenie. Kliknij w celu zmiany adresu, a następnie kliknij , w celu usunięcia.
Można również kliknąć przycisk **Export Config**, aby wyeksportować bieżące urządzenia do lokalnego komputera PC, lub kliknąć przycisk **Import Config**, aby zaimportować istniejącą konfigurację.

5.5 Status

Można wyświetlić bieżący stan i adres IP wszystkich podłączonych urządzeń.

Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz kolejno opcje **Household Setting > Status.** Zostanie wyświetlony interfejs **stanu**. Patrz Rysunek 5-15.

Rysunek 5-15 Status



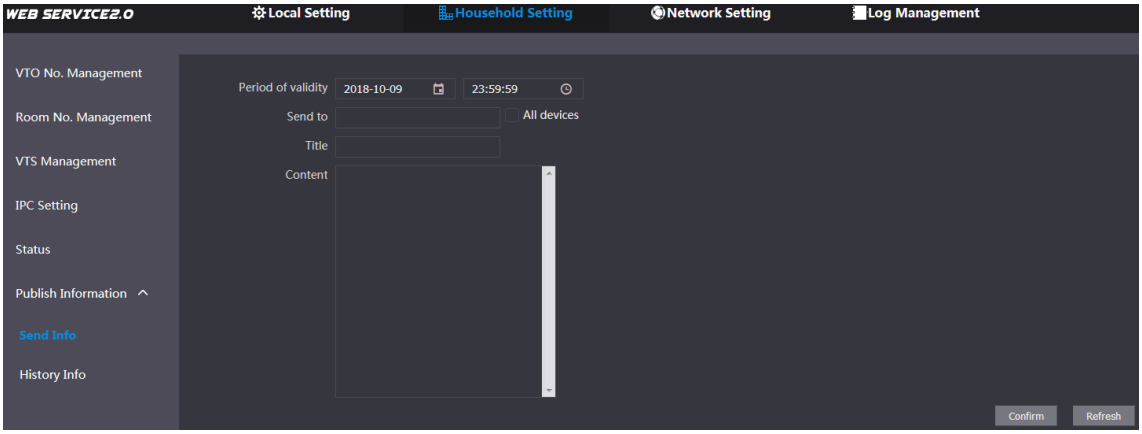
Można wysyłać wiadomości z serwera SIP do innych urządzeń VTH i przeglądać historię wysłanych wiadomości.

5.61 Wysyłanie informacji

Krok 1 Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz opcję **Household Setting > Publish Information > Send Info.**

Zostanie wyświetlony interfejs **Send Info**. Patrz Rysunek 5-16.

Rysunek 5-16 Wysyłanie informacji



Krok 2 Wprowadź numer docelowej jednostki VTO lub wybierz **All device**, aby wysłać wiadomość do wszystkich urządzeń w sieci.

- Jeśli chcesz wysłać informacje do więcej niż jednego VTH, należy oddzielić numery VTH średnikami. Na przykład, jeśli wprowadzisz 101; 102; 103 lub więcej, VTH o takich numerach otrzymają informacje od VTO.
- Period of validity (okres ważności) zarezerwowany jest do wykorzystania w przyszłości.

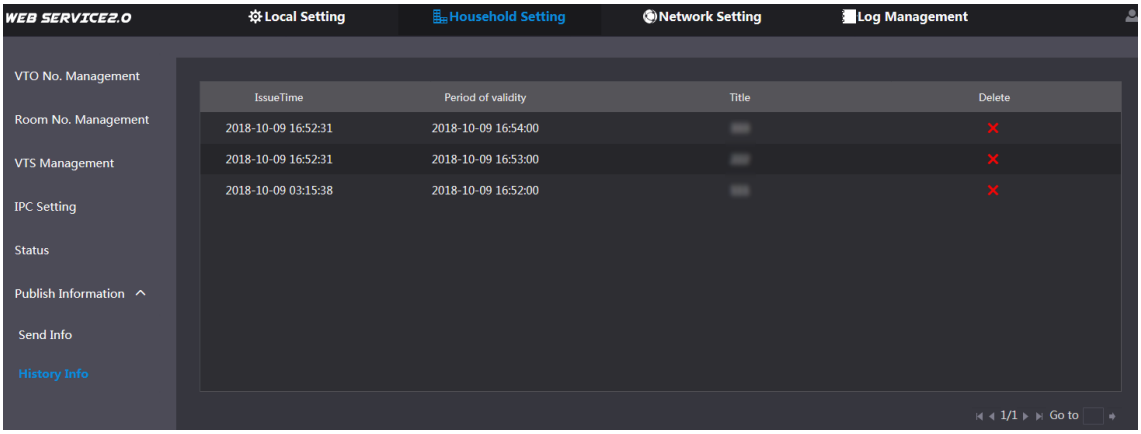
Krok 3 Kliknij przycisk **Confirm**.

5.6.2 Historia

Zaloguj się do interfejsu internetowego serwera SIP, a następnie wybierz opcję **Household Setting > Publish Information > Historia Info.**

Wyświetli się interfejs **informacji archiwalnych**. Patrz Rysunek 5-17.

Rysunek 5-17 Informacje archiwalne



Można przejrzeć czas i tytuł wysyłanych wiadomości.

5.7 Zarządzanie rozpoznanymi twarzami

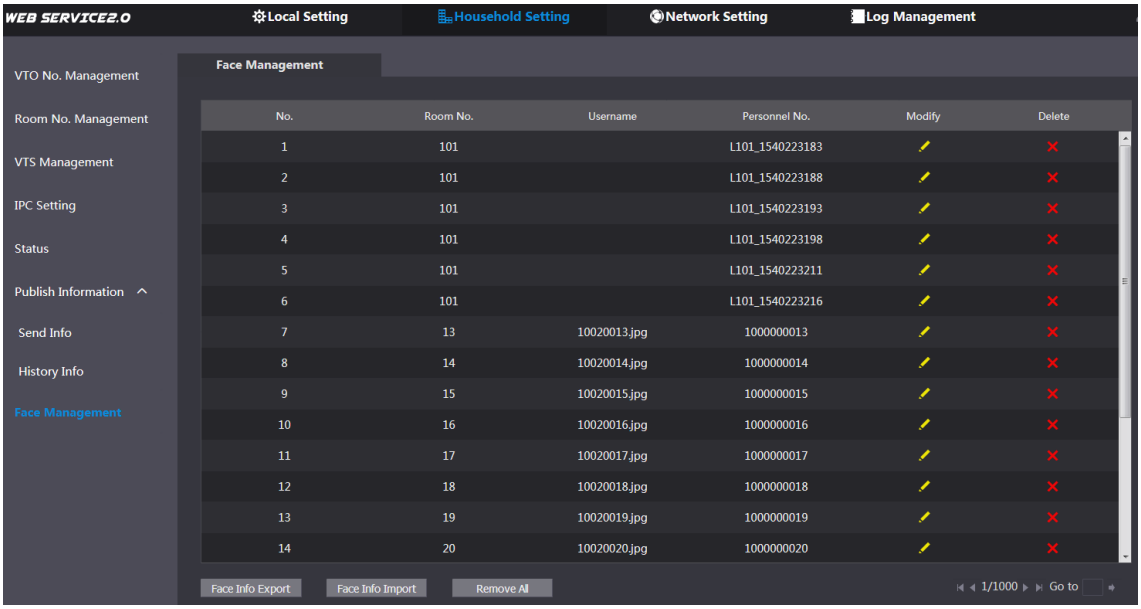
Możesz dodawać, usuwać, importować i eksportować dane twarzy.

- Rozpoznawanie twarzy dostępne jest w wybranych modelach.
- VTO może zapisać maksymalnie 10000 wizerunków twarzy.

Wybierz kolejno opcje **Household Setting > Face Managment.**

Zostanie wyświetlony interfejs **Face Management**. Patrz Rysunek 5-18.

Rysunek 5-18 Zarządzanie rozpoznanymi twarzami

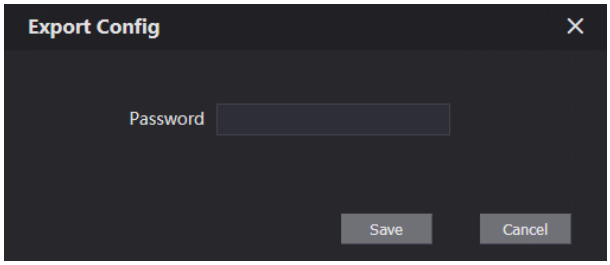


5.7.1 Eksportowanie danych o twarzy

Krok 1 Kliknij przycisk **Face Info Export**.

Wyświetli się interfejs **Export Config**. Patrz Rysunek 5-19.

Rysunek 5-19 Konfiguracja eksportu



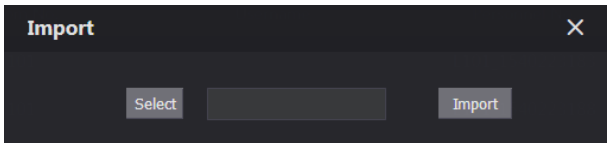
Krok 2 Wprowadź hasło dla interfejsu WWW, a następnie kliknij przycisk **Save**, aby wyeksportować dane twarzy.

5.7.2 Eksportowanie danych o twarzy

Krok 1 Kliknij **Face Info Import**.

Krok 2 Wprowadź hasło dla interfejsu WWW, a następnie kliknij przycisk **Save**. Zostanie wyświetlony interfejs importowania. Patrz Rysunek 5-20.

Rysunek 5-20 Importowanie



Krok 3 Kliknij przycisk **Select**, a następnie wybierz żądany plik.

Krok 4 Kliknij przycisk **Import**.

5.7.3 Usuwanie danych o twarzy

Kliknąć przycisk  , aby usunąć pojedyncze twarze.

Kliknij przycisk **Remove All**, aby usunąć wszystkie dane o twarzach.

Figure 6-3

6 Ustawienia sieciowe

W niniejszym rozdziale przedstawiono sposób konfiguracji adresu IP, serwera FTP, SIP, DDNS i UPnP.

6.1 Informacje podstawowe

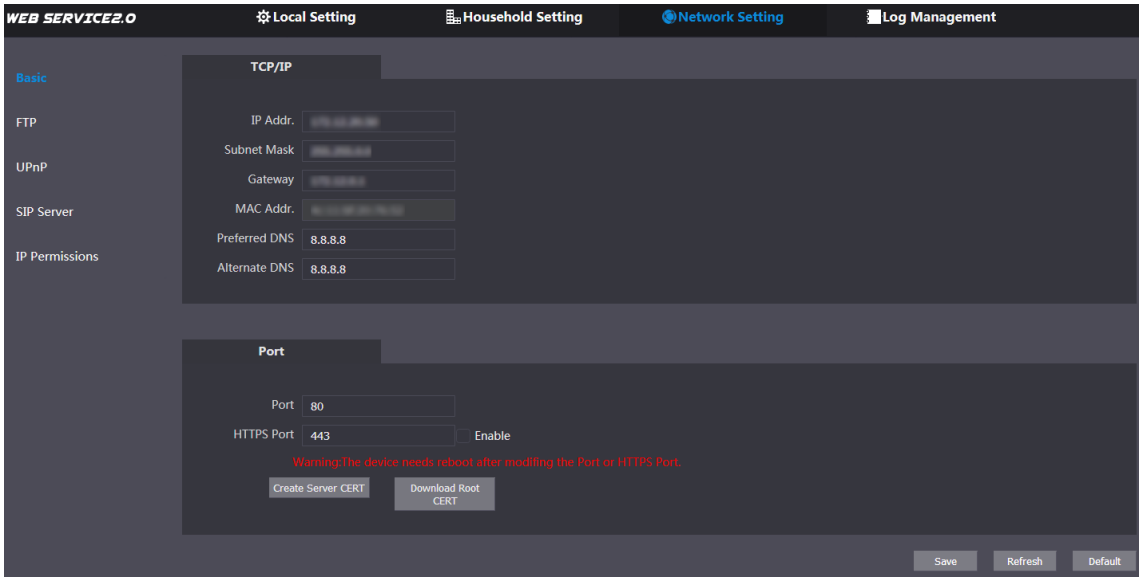
6.1.1 TCP/IP

Można zmienić adres IP i numer portu VTO.

Krok 1 Wybierz **Network Setting > Basic.**

Wyświetlane są informacje o TCP/IP oraz informacje o porcie. Patrz Rysunek 6-1.

Rysunek 6-1 TCP/IP i port



Krok 2 Wprowadź parametry sieci i numer portu, którego chcesz użyć, a następnie kliknij przycisk **Save**.

VTO uruchomi się ponownie. Aby ponownie się zalogować, należy zmienić adres IP komputera PC na należący do tego samego segmentu sieci co adres VTO.

6.1.2 HTTPS

Zaznaczyć pole wyboru **Enable** przy **HTTPS Port**. VTO uruchomi się ponownie. Po ponownym uruchomieniu można zalogować się do VTO wpisując "https://". adres IP VTO" w pasku adresu przeglądarki.

6.2 FTP

Skonfiguruj serwer FTP. Następnie możliwe będzie zapisanie nagranych filmów i zrzutów na serwerze FTP.

Krok 1 Wybierz **Network Setting > FTP.**

Wyświetli się interfejs **FTP**. Patrz Rysunek 6-2.

Skonfiguruj parametry. Patrz tabela 6-1

Rysunek 6-2 FTP

Krok 2 Konfigurowanie parametrów. Patrz tabela 6-1.

Tabela 6-1 Opis parametrów FTP

Parametr	Opis
Enable	Zaznaczyć pole wyboru, aby włączyć funkcję FTP.
Name	W razie potrzeby wpisz nazwę serwera FTP.
IP Addr.	Adres IP serwera FTP.
Port	Domyślnie jest to 21.
Username	Nazwa użytkownika i hasło serwera FTP.
Password	

Kliknij **Save**.

6.3 UPnP

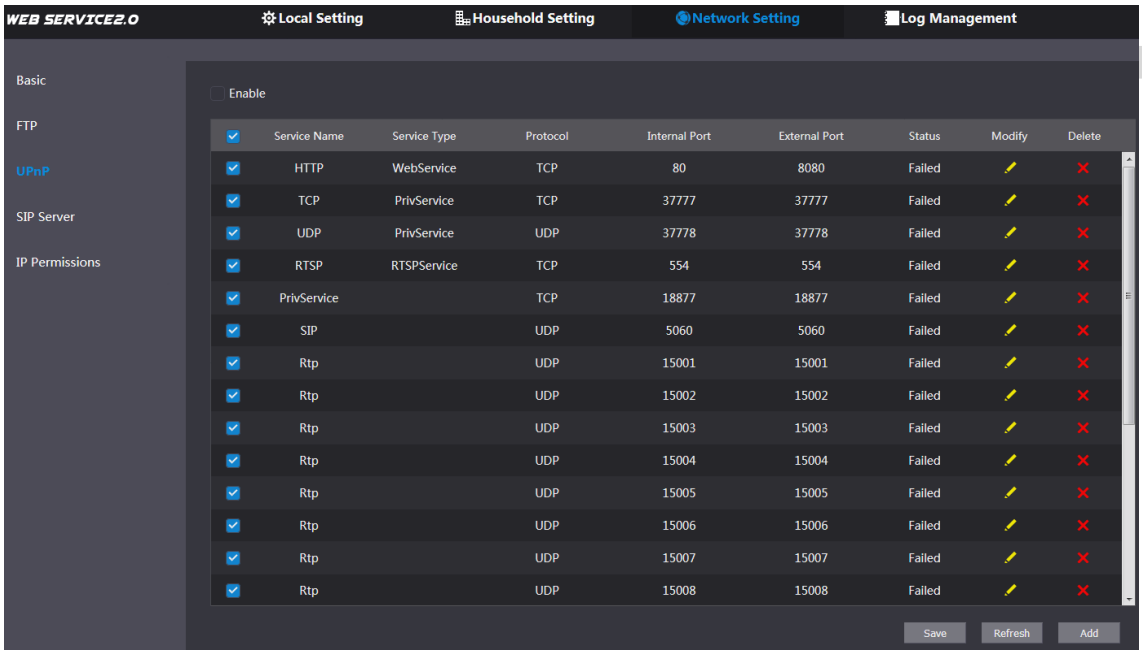
Universal Plug and Play to protokół, który określa relację pomiędzy portami w sieciach LAN i WAN. Funkcja ta umożliwia łączenie się z lokalnymi urządzeniami za pośrednictwem sieci.

- Funkcja ta działa tylko wtedy, gdy VTO pracuje jako serwer SIP.
- Funkcja ta jest potrzebna tylko wtedy, gdy VTO jest podłączone do routera z funkcją UPnP.

Krok 1 Wybierz **Network Setting > UPnP.**

Wyświetli się interfejs **UPnP** . Patrz Rysunek 6-3.

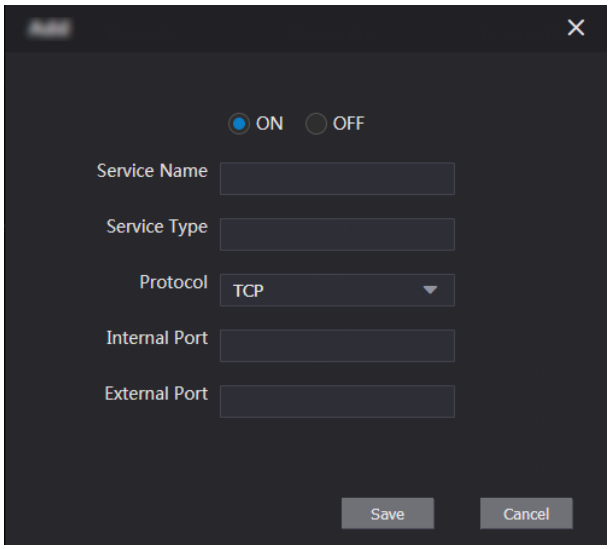
Rysunek 6-3 UPnP



Krok 2 Zaznaczyć pole wyboru **Enable**, aby włączyć funkcję UPnP.

Krok 3 Fabrycznie przygotowano kilka ustawień, które można zmienić. Możesz też kliknąć przycisk **Add**, aby dodać nowy. Wyświetli się interfejs **zmiany/dodawania**. Patrz Rysunek 6-4.

Rysunek 6-4 Zmiana/dodawanie UPnP



Krok 4 Konfigurowanie parametrów. Patrz tabela 6-2

Tabela 6-2 Opis parametrów UPnP

Parametr	Opis
ON/OFF	Wybierz opcję **ON**, aby włączyć relację mapowania.
Service Name	Nazwa usługi.
Service Type	Określ rodzaj usługi w zależności od potrzeb.
Protocol	Można wybrać **TCP** lub **UDP**. Dla stabilności transmisji, zaleca się użycie **TCP**.

Parametr	Opis	
Internal Port	Port w lokalnym VTO, z którym należy się połączyć.	● Aby uniknąć konfliktu, podczas mapowania portów z routerem staraj się używać numeru portu od 1024 do 5000, a nie od 1 do 255 i od 256 do 1023. ● W przypadku mapowania wielu urządzeń na porty zewnętrzne, operację należy zaplanować z wyprzedzeniem, aby uniknąć mapowania różnych urządzeń na ten sam port zewnętrzny. ● Sprawdź, czy porty, z których korzystasz nie są już używane lub ograniczone. ● Zewnętrzne porty TCP i UDP muszą być takie same.
External Port	Port na routerze, do którego mapowany jest port VTO.	

Krok 5 Kliknij **Save**.

Step 4 Otwórz przeglądarkę internetową na komputerze i wpisz "http://". adres WAN IP: external port number", a następnie połącz się z odpowiednim portem lokalnego urządzenia.

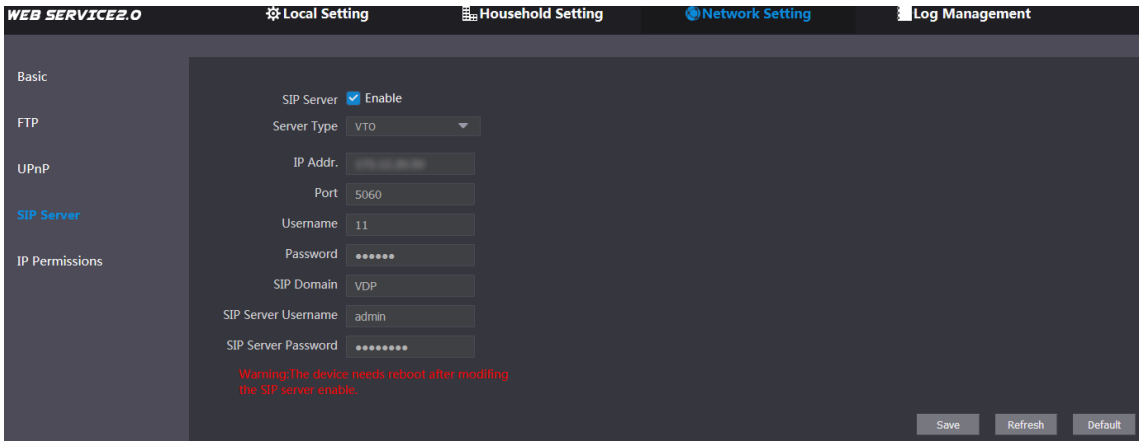
6.4 Serwer SIP

Serwer SIP jest wymagany w sieci do przesyłania protokołu interkomowego, dzięki czemu wszystkie urządzenia VTO i VTH podłączone do tego samego serwera SIP mogą nawiązywać między sobą połączenia wideo. Jako serwera SIP można użyć urządzenia VTO lub innych serwerów.

Krok 1 Wybierz opcję **Nettwork Setting > SIP Server.**

Wyświetli się interfejs **serwera SIP**. Patrz Rysunek 6-5.

Serwer SIP



Krok 2 Wybierz typ serwera, którego potrzebujesz.

- Jeśli VTO, z którym łączysz się, działa jako serwer SIP

  Zaznacz pole wyboru **Enable** przy **SIP server**, a następnie kliknij przycisk **Save**.

  VTO zostanie zrestartowane, a po ponownym uruchomieniu możesz dodać do niego urządzenia VTO i VTH. Zobacz szczegóły w Tabeli 6-5 Ustawienie dla gospodarstw domowych.

Jeśli VTO, z którym się łączysz nie działa jako serwer SIP, nie zaznaczaj pola wyboru **Enable** przy SIP Server, w przeciwnym razie połączenie zostanie przerwane.

- Jeśli inny VTO działa jako serwer SIP

Na liście **Server Type** wybierz **VTO**, a następnie skonfiguruj parametry. Patrz tabela 6-3

Tabela 6-3 Konfiguracja serwera SIP

Parametr	Opis
IP Addr.	Adres IP VTO, który działa jako serwer SIP.
Port	5060
Username	Zachowaj wartość domyślną.
Password	
SIP Domain	VDP
SIP Server Username	Nazwa użytkownika i hasło do interfejsu webowego serwera SIP.
SIP Server Password	

- Jeśli inne serwery działają jako serwer SIP

  Wybierz typ serwera w polu **Server Type**, a następnie zapoznaj się z odpowiednią instrukcją dotyczącą szczegółowej konfiguracji.

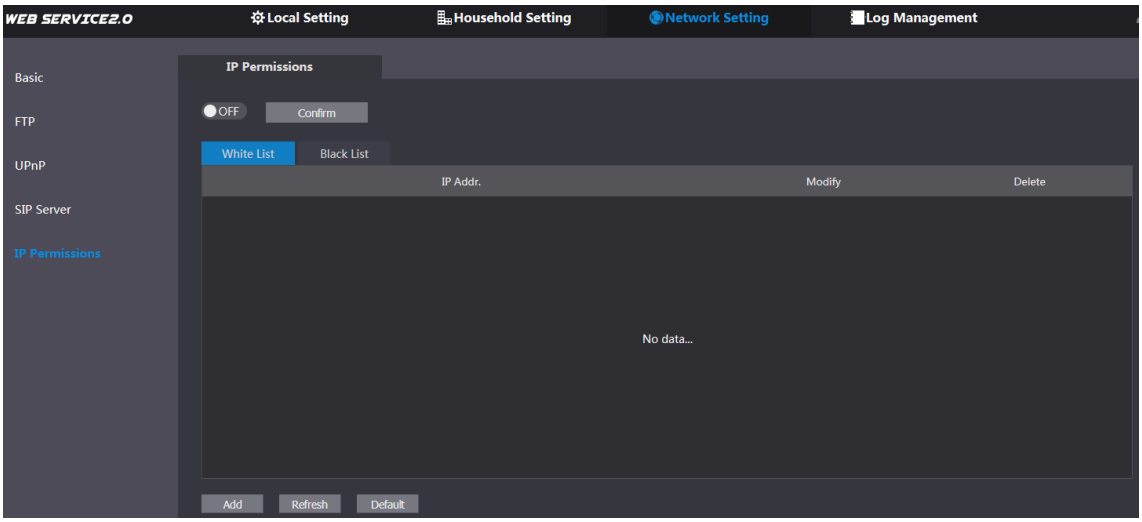
Uprawnienia IP

Aby zwiększyć bezpieczeństwo sieci i danych, należy skonfigurować uprawnienia dostępu dla różnych adresów IP.

Krok 1 Wybierz **Network Setting > IP Permissions.**

Wyświetli się interfejs **uprawnień IP**. Patrz Rysunek 6-6.

Rysunek 6-6 Uprawnienia IP

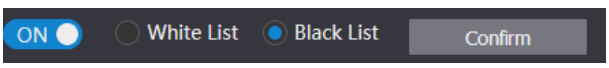


Krok 2 Kliknij 

.

Wyświetlą się opcje **White List i Black List (Biała lista** i **Czarna lista**). Patrz Rysunek 6-7.

Rysunek 6-7 Biała i czarna lista



Można używać tylko jednej listy w tym samym czasie.

- **White list**: tylko adresy IP znajdujące się na liście mogą zalogować się do VTO.
- **Black list**: wszystkie adresy IP znajdujące się na liście mają zakaz logowania się do VTO.

Krok 3 Wybierz opcję White List lub Black List.

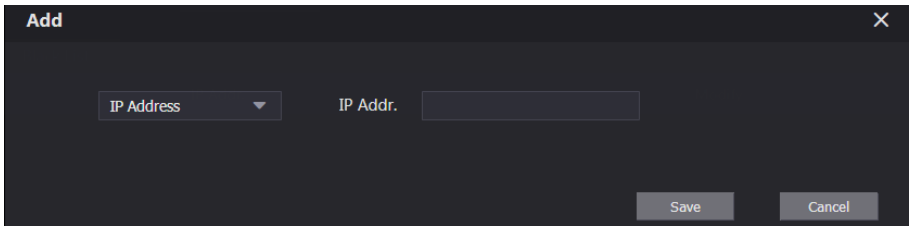
- Jeśli chcesz użyć czarnej listy, wybierz **Black List**, a następnie kliknij **Confirm**.

- Jeśli chcesz użyć białej listy, wybierz **White List**, a następnie przed kliknięciem **Confirm** dodaj adres IP lub sekcję IP do białej listy.

Krok 4 Kliknij **Add**

Zostanie wyświetlony interfejs Dodawania. Patrz Rysunek 6-8.

Rysunek 6-8 Dodawanie adresu IP



Krok 5 Możesz wybrać i wprowadzić pojedynczy adres IP lub sekcję IP, a następnie kliknąć przycisk **Save.**

7 Zarządzanie rejestrem

Można przeglądać historię połączeń, zapis alarmów, zapis odblokowań oraz różne rejestry systemowe.

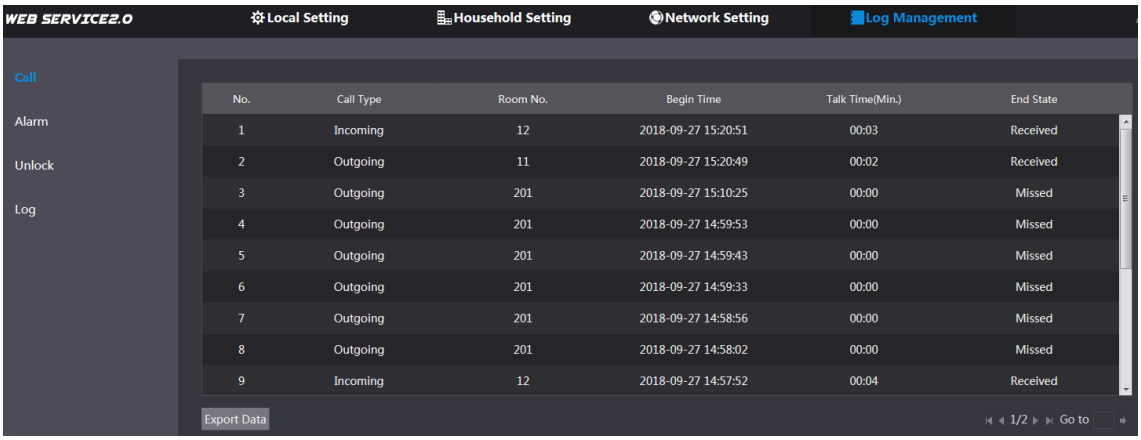
7.1 Połączenie

Można przejrzeć typ połączenia, numer lokalu, czas rozpoczęcia rozmowy, czas rozmów i stan końcowy.

Wybierz **Log Management > Call.**

Zostanie wyświetlony interfejs **połączenia**. Patrz Rysunek 7-1.

Rysunek 7-1 Połączenie



Kliknij przycisk **Export Data**, aby wyeksportować nagrania do komputera.

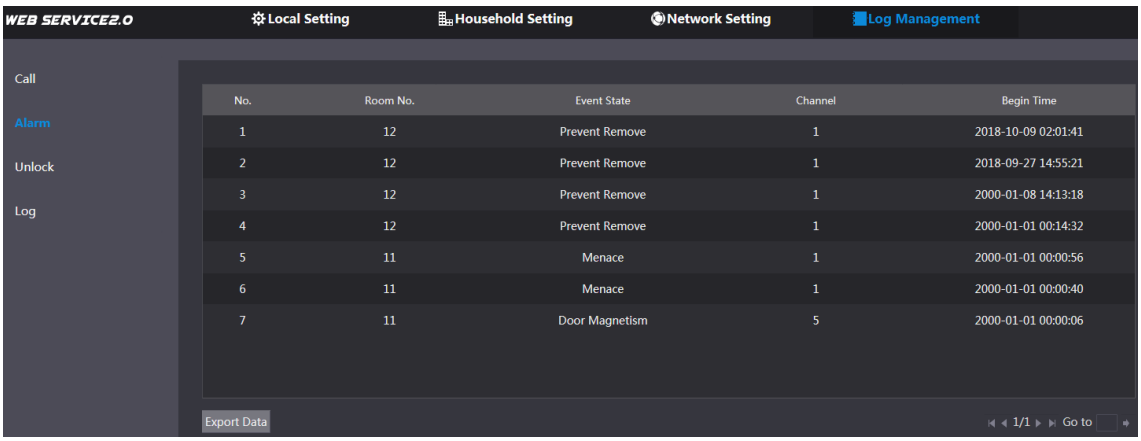
7.2 Alarm

Funkcja ta jest wyświetlana tylko wtedy, gdy VTO, z którym jesteś połączony działa jako serwer SIP. Wówczas możesz przeglądać zapis alarmów VTO i VTH oraz alarmy zarejestrowane po wpisaniu hasła pod przymusem.

Wybierz **Log Management > Alarm.**

Wyświetli się interfejs **alarmowy**. Patrz Rysunek 7-2.

Rysunek 7-2 Alarm



Kliknij przycisk **Export Data**, aby wyeksportować nagrania do komputera.

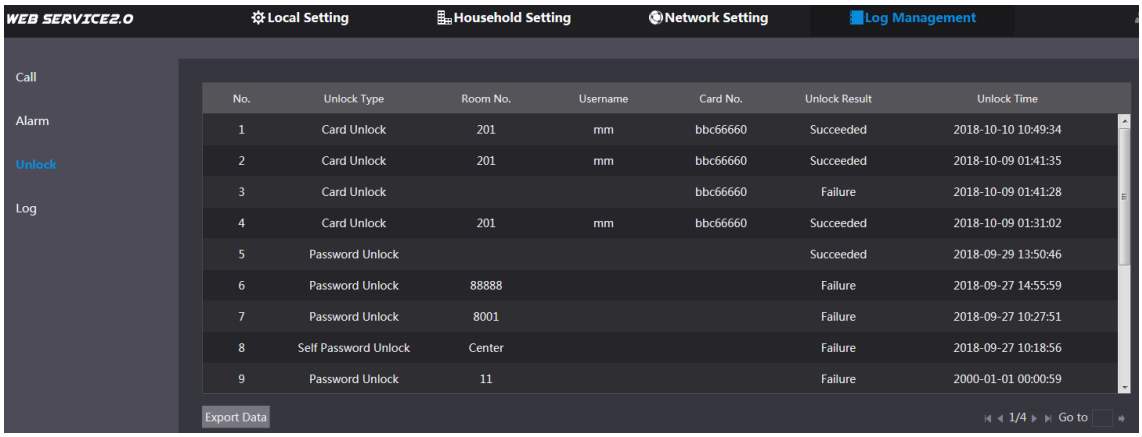
7.3 Odblokowanie

Możesz przeglądać różne zdarzenia takie jak odblokowanie, w tym odblokowanie karty dostępu, odblokowanie hasłem, odblokowanie zdalne i naciśnięcie przycisku odblokowania.

Wybierz opcję **Log Management > Unlock.**

Wyświetli się interfejs Odblokowania. Patrz Rysunek 7-3.

Rysunek 7-3 Odblokowanie



Kliknij przycisk **Export Data**, aby wyeksportować nagrania do komputera.

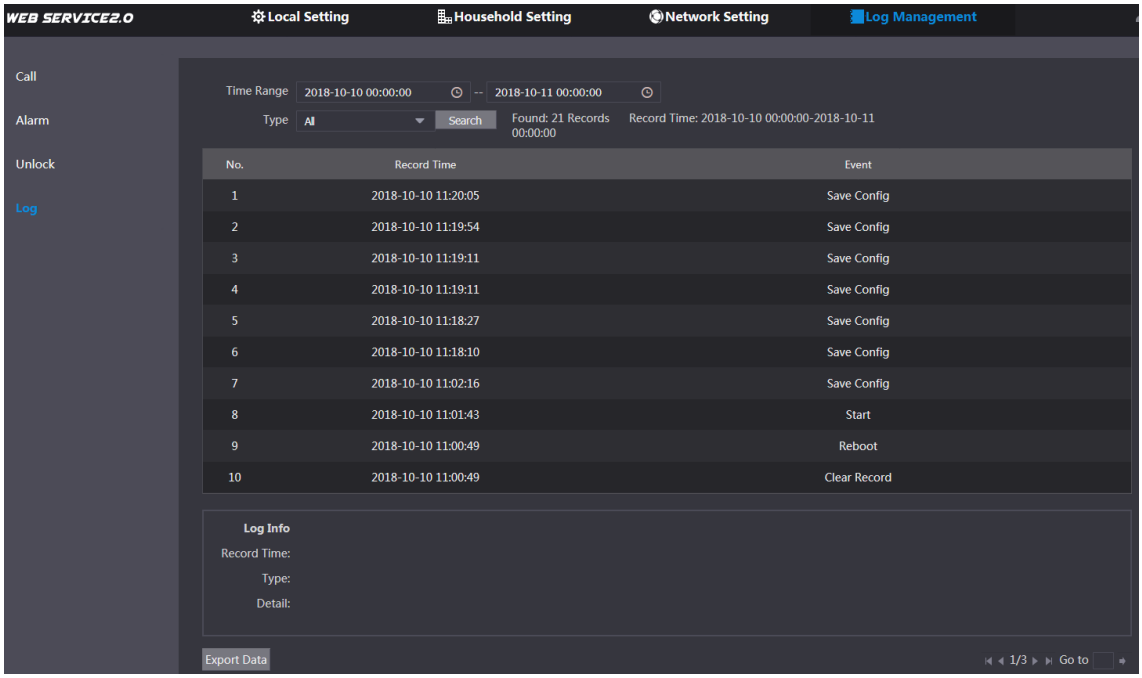
7.4 Dziennik

Można przeglądać dziennik, w tym dziennik systemu, nagrywania, konfiguracji, konta i zabezpieczeń.

Krok 1 Wybierz opcję **Log Management > Log.**

Wyświetli się interfejs Dziennik. Patrz Rysunek 7-4.

Rysunek 7-4 Dziennik



Skonfiguruj zakres czasowy, następnie wybierz rodzaj dziennika, z którego chcesz skorzystać, a następnie kliknij **Search**. Kliknij przycisk **Export Data**, aby wyeksportować nagrania do komputera.