HILTRON
security

Unità VTO

Manuale d'uso

Hiltron Land S.r.l.
Strada provinciale di Caserta, 218 - 80144 Napoli
Tel: (+39)081 185 39 000 Fax: (+39)081 185 39 016
www.hiltronsecurity.net

V4.03

Introduzione

Generale

Questo manuale descrive il funzionamento dell'interfaccia web.

Istruzioni di sicurezza

All’interno del manuale possono comparire i seguenti indicatori di pericolo, il cui significato è definito qui sotto.

Indicatori di pericolo	Significato
 ATTENZIONE	Indica un rischio potenziale che, se non evitato, può causare danni materiali, perdite di dati, riduzione delle prestazioni o altre conseguenze imprevedibili.
 CONSIGLI	Spiegano metodi utili per risolvere un problema o per aiutarvi a risparmiare tempo.
 NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Cronologia delle revisioni

N.	Versione	Contenuto della revisione	Data di rilascio
1	V1.0.0	Prima versione.	Settembre 2018

Indicazioni sul manuale

- Questo manuale serve solo come riferimento. In caso di discrepanza fra il manuale e il prodotto, quest’ultimo prevarrà.
- Non ci riteniamo responsabili per eventuali perdite causate da un utilizzo non conforme a quanto esposto nel manuale.
- Il manuale verrà aggiornato in base alle leggi e ai regolamenti più recenti delle relative giurisdizioni. Per informazioni dettagliate, fare riferimento al manuale cartaceo, al CD-ROM, al codice QR o al nostro sito web ufficiale. In caso di incongruenze tra il manuale cartaceo e la versione elettronica, quest’ultima prevarrà.
- Grafiche e software sono soggetti a modifica senza preavviso. Gli aggiornamenti del prodotto possono generare delle differenze tra il prodotto effettivo e le informazioni contenute nel manuale. Contattare il servizio di assistenza per le procedure più recenti e la documentazione supplementare.
- Potrebbero inoltre esserci delle differenze nei dati tecnici, nelle descrizioni di funzioni e operazioni, o errori di stampa. In caso di dubbi o vertenze, ci riserviamo il diritto di interpretazione finale.

- Se non è possibile aprire il manuale in formato PDF, aggiornare il programma per la lettura dei file PDF o provarne un altro.
- Tutti i marchi commerciali, i marchi registrati e i nomi di società presenti nel manuale sono di proprietà dei rispettivi titolari.
- In caso di problemi nell'utilizzo del dispositivo, consigliamo di visitare il nostro sito web, contattare il fornitore o il servizio clienti.
- In caso di dubbi o controversie, ci riserviamo il diritto di interpretazione finale.

Norme di sicurezza e avvertenze importanti

Quanto segue indica il metodo di applicazione corretto del dispositivo. Leggere attentamente il manuale prima dell'uso, per evitare pericoli e danni alle proprietà. Attenersi scrupolosamente alle prescrizioni del manuale durante l'applicazione e conservarlo dopo la lettura.

Requisiti operativi

- Non collocare e installare il dispositivo in una zona esposta alla luce solare diretta o in prossimità di dispositivi che generano calore.
- Non installare il dispositivo in zone umide, polverose o esposte a fuliggine.
- Mantenere il dispositivo in orizzontale e installarlo in luoghi stabili per evitare che cada.
- Non versare liquidi sul dispositivo; non posizionare oggetti contenenti liquidi sul dispositivo per evitare che i liquidi penetrino all'interno.
- Installare il dispositivo in luoghi ben areati; non bloccarne le fessure di ventilazione.
- Utilizzare il dispositivo solo entro gli intervalli di ingresso e uscita nominali.
- Non smontare il dispositivo in modo arbitrario.
- Il dispositivo deve essere utilizzato con cavi di rete schermati.

Requisiti di alimentazione

- Il prodotto dovrà utilizzare cavi elettrici (cavi di alimentazione) del tipo previsto nella regione di utilizzo del dispositivo.
- Utilizzare una fonte di alimentazione che rispetti i requisiti dei sistemi SELV (bassissima tensione di sicurezza) e fornisca corrente con tensione conforme alle fonti di alimentazione limitata descritte nello standard IEC60950-1. Per i requisiti di alimentazione specifici, fare riferimento alle etichette del dispositivo.
- Questo dispositivo utilizza un accoppiatore come dispositivo di spegnimento. Durante l'utilizzo, mantenere un'angolazione che faciliti l'utilizzo.
- Non interrompere l'alimentazione elettrica durante l'aggiornamento del dispositivo.

Indice

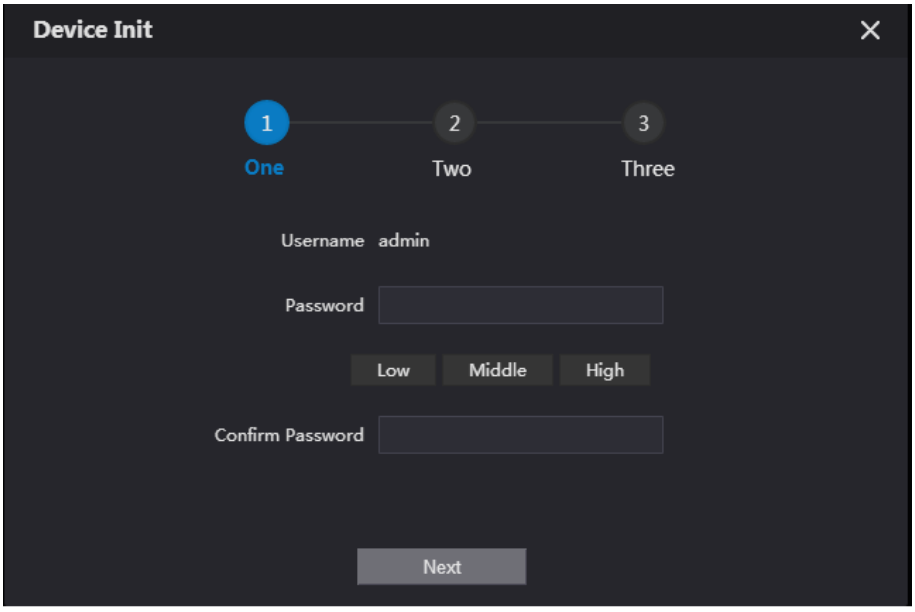
1 Inizializzazione

Al primo accesso o dopo la reimpostazione del VTO, occorre inizializzare l'interfaccia web. L'indirizzo IP predefinito del VTO è 192.168.1.110 e il PC connesso al sistema deve trovarsi nello stesso segmento di rete del VTO.

Fase 1: Collegare il VTO all'alimentazione elettrica, quindi eseguire l'avvio del sistema.

Fase 2: Aprire un browser internet sul PC, quindi inserire l'indirizzo IP predefinito del VTO nella barra degli indirizzi e premere Invio (Enter).

Figura 1-1 Inizializzazione del dispositivo



Fase 3: Accedere e confermare la password, quindi fare clic su **Avanti** (Next).

Il sistema mostra l'interfaccia di impostazione e-mail.

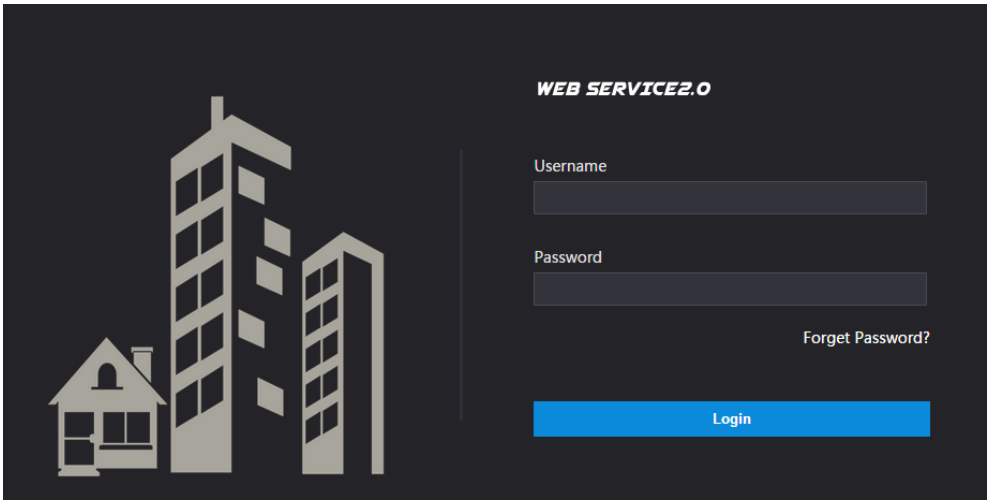
Fase 4: Selezionare la casella di controllo **Email** ed inserire il proprio indirizzo di posta elettronica. Questo indirizzo e-mail sarà usato per reimpostare la password, per cui si consiglia di procedere alla sua definizione.

Fase 5: Fare clic su "**Avanti**" (Next). L'inizializzazione è andata a buon fine.

Fase 6: Fare clic su **OK**.

Il sistema mostra l'interfaccia di Accesso (Login). Osservare la Figura 1-2.

Figura 1-2 Interfaccia di accesso



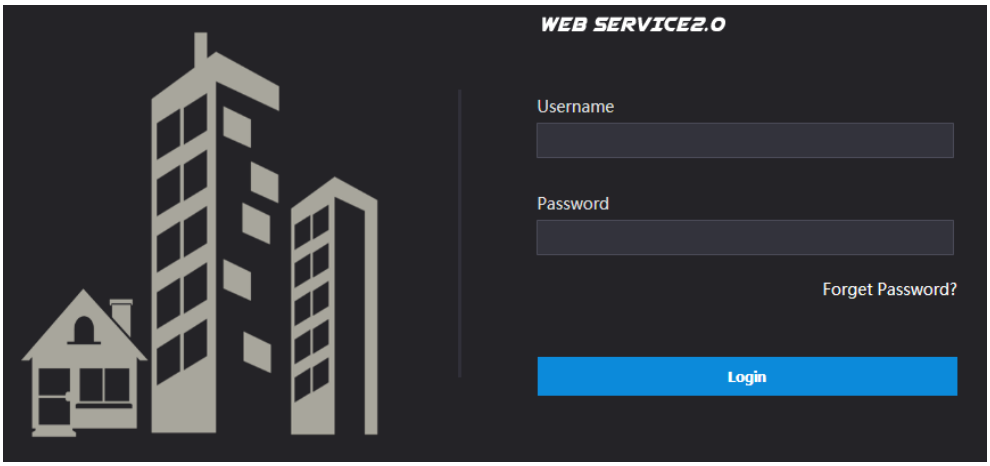
2 Interfaccia di accesso

2.1 Accesso

Prima di accedere, verificare che il PC si trovi nello stesso segmento di rete del VTO.

Fase 1: Aprire un browser internet sul PC, quindi inserire l'indirizzo IP del VTO nella barra degli indirizzi e premere Invio (Enter).

Figura 2-1 Interfaccia di accesso

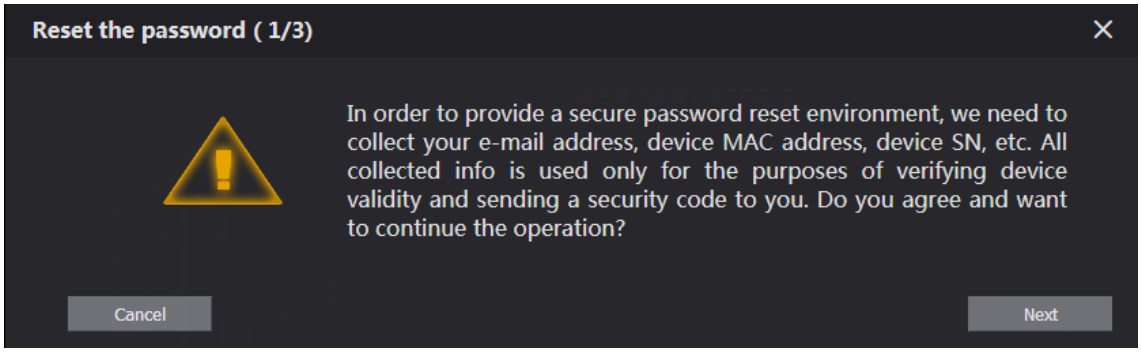


Fase 2: Il nome utente da inserire è "admin", mentre la password è quella definita durante l'inizializzazione. Quindi fare clic su **Accesso** (Login).

2.2 Reimpostazione della password

Fase 1: Sull'interfaccia di accesso (Figura 2-1), fare clic su **Password dimenticata?** (Forgot Password?).

Figura 2-2 Reimpostazione della password (1/3)



Fase 2: Fare clic su "**Avanti**" (Next).

Figura 2-3 Reimpostazione della password (2/3)

Fase 3: Effettuare la scansione del codice QR per ricevere il codice di sicurezza nella propria casella di posta e poi immettere il codice di sicurezza nella casella di input.

- In caso di mancata configurazione dell'e-mail durante l'inizializzazione, contattare il fornitore del servizio al cliente per assistenza.
- Per ottenere di nuovo il codice di sicurezza, aggiornare l'interfaccia del codice QR.
- Utilizzare il codice di sicurezza entro 24 ore dalla ricezione. Trascorso questo intervallo di tempo, non sarà più valido.
- Dopo aver inserito per 5 volte di fila un codice di sicurezza errato, l'account in uso sarà bloccato per 5 minuti.

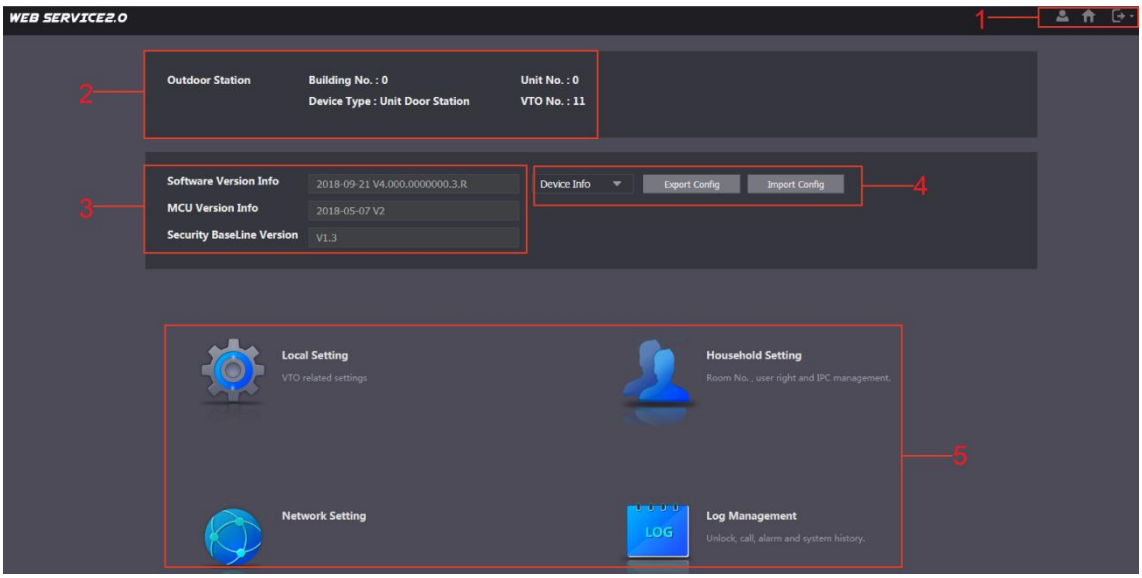
Fase 4: Facendo clic su **Avanti** (Next), il sistema mostra la casella di dialogo **Reimposta password (3/3)** (Reset the password (3/3).

Fase 5: Impostare e confermare la nuova password secondo le istruzioni, poi fare clic su **OK**.

3 Interfaccia principale

Accedendo all'interfaccia web del VTO, il sistema mostra l'interfaccia principale. Osservare la Figura 3-1.

Figura 3-1 Interfaccia principale



Consultare Tabella 3-1 per la presentazione dell'interfaccia principale.

Tabella 3-1 Introduzione all'interfaccia principale

N.	Funzione	Descrizione
1	Funzioni generali	Questi pulsanti sono sempre visualizzati • Fare clic su per modificare la password e l'indirizzo e-mail. • Fare clic su per accedere all'interfaccia principale. • Fare clic su per uscire dalla sessione, riavviare il VTO o ripristinare le impostazioni di fabbrica del VTO.
2	Informazioni VTO	È possibile visualizzare le informazioni generali del VTO, quali n. edificio, n. unità, tipo di dispositivo e n. VTO.
3	Informazioni di sistema	È possibile visualizzare la versione software, la versione MCU e la versione base del sistema di sicurezza.
4	Gestione configurazione	Selezionare **Informazioni dispositivo** (Device Info) o **Informazioni utente** (User Info) per esportare/ importare la configurazione del VTO o le informazioni utente al/dal PC.
5	Area funzionale	Fare clic sul pulsante per accedere al menu corrispondente.

4 Impostazioni locali

Questo capitolo descrive la configurazione di parametri quali tipo e numero VTO, video e audio, password di accesso, orario di sistema e funzioni di sicurezza.

Operazioni generali:

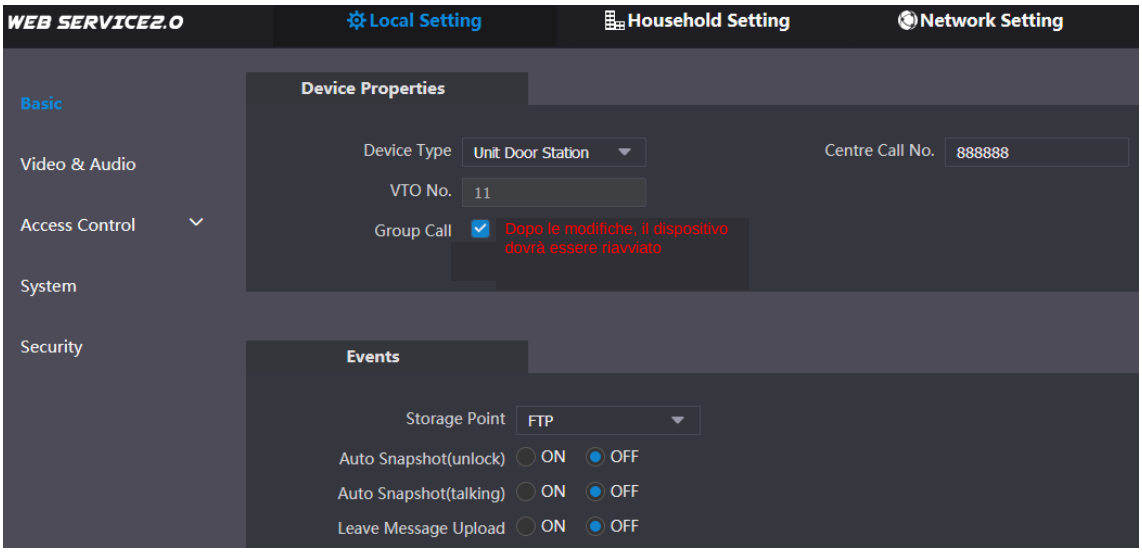
- Dopo la configurazione dei parametri, fare clic su **Conferma** (Confirm) per salvare e poi fare clic su **Aggiorna** (Refresh) per visualizzarne i valori più recenti.
- Facendo clic su **Impostazioni predefinite** (Default), tutti i parametri nella pagina corrente saranno ripristinati ai valori predefiniti, poi occorre fare clic su **Conferma** (Confirm) per salvare.

4.1 Impostazioni di base

Questa sezione descrive la configurazione di parametri di base quali tipo di dispositivo VTO, numero VTO e archiviazione automatica.

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Imp. Base** (Local Setting > Basic).

Figura 4-1 Impostazioni di base



Fase 2: Configura i parametri. Per ulteriori informazioni, consultare la sezione Tabella 4-1.

Tabella 4-1 Descrizione dei parametri di base

Parametro	Descrizione
Tipo di dispositivo	È possibile selezionare Stazione porta unità o Stazione perimetrale. ● **Stazione porta unità:** Di solito installata all'interno di impianti comunitari con uno specifico numero di edificio o di unità residenziale. ● **Stazione perimetrale:** Di solito installata all'ingresso di impianti comunitari, per cui occorre inserire il numero di edificio, il numero di unità e il numero di stanza per chiamare una stanza specifica. Le stazioni perimetrali non permettono l'invio di messaggi o la visualizzazione dei contatti.

Parametro	Descrizione
	 ● Il numero di edificio e quello di unità residenziale sono disponibili solo quando altri server fungono da server SIP. Fare riferimento alla sezione 6.4 Server SIP. ● La stazione perimetrale di solito è usata quando altri server fungono da server SIP.
N. centro di controllo.	Configurando il numero del centro di gestione, sarà possibile chiamare il centro da ogni dispositivo VTO o VTH nella rete. Il numero predefinito è 888888.
N. VTO	Il numero di VTO può essere utilizzato per distinguere ciascun dispositivo VTO e di solito è definito in base al numero di edificio o di unità. I dispositivi VTO possono essere aggiunti al server SIP con i propri numeri.  Se un VTO non funge da server SIP, il suo numero di VTO può essere modificato (a questo scopo accedere alla pagina web del VTO e poi effettuare la modifica).
Chiamate di gruppo	Selezionando la casella di controllo per abilitare questa funzione, quando si chiama un VTH master, anche i dispositivi VTH degli interni riceveranno la chiamata.
Posizione di archiviazione	È possibile selezionare solo **FTP** per fare in modo che tutte le istantanee siano salvate automaticamente nel server FTP. ● Istantanee automatiche (sblocco) Selezionando **ATTIVA** (ON) per abilitare questa funzione, il sistema scatta delle istantanee ogni volta che la porta è sbloccata. ● Istantanee automatiche (conversazione) Selezionando **ATTIVA** (ON) per abilitare questa funzione, il sistema scatta delle istantanee ogni volta che un utente VTH risponde a una chiamata dal VTO. ● Consentire caricamento messaggi Selezionando **ATTIVA** (ON) per abilitare questa funzione, il sistema carica automaticamente i messaggi dei visitatori sul server FTP.  ● Prima è necessario abilitare la funzione FTP. Fare riferimento alla sezione 6.2 FTP. ● Se il VTH principale è dotato di scheda SD, i messaggi rimasti saranno salvati per impostazione predefinita nella scheda SD. ● Per ricevere messaggi, il parametro **Durata messaggi VTO** (VTO Message Time) deve essere impostato su un valore maggiore di 0. Consultare il manuale d'uso del VTH.

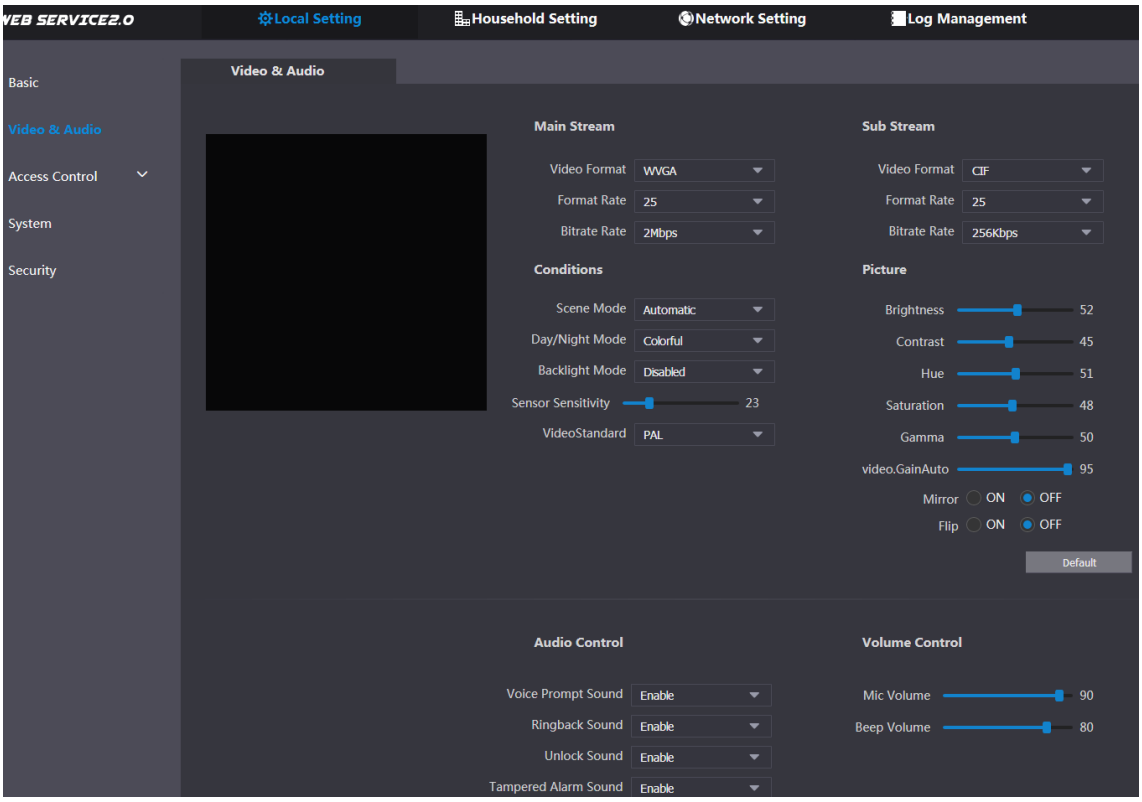
Fase 3: Fare clic su **Conferma** (Confirm) per salvare.

4.2 Video e audio

Questa sezione descrive la configurazione del formato e la qualità dei video registrati dal VTO e le impostazioni di controllo audio.

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Video e audio** (Local Setting > Video & Audio).

Figura 4-2 Video e audio



Fase 2: Configurando i parametri, essi avranno subito effetto. Osservare la Tabella 4-2.

Tabella 4-2 Descrizione dei parametri video

Parametro		Descrizione
Flusso principale	Formato video	Selezionare la risoluzione video tra **720P**, **WVGA** e **D1**.
	Velocità formato	Definisce il numero di fotogrammi per secondo. I valori ammessi vanno da **1** a **25** per l'opzione **PAL** e da **1** a **30** per l'opzione **NTSC**. Quanto più alto è il valore, tanto più scorrevole sarà il video.
	Velocità in bit	Definisce la quantità di dati trasmessi in 1 secondo. Si può definire il valore richiesto. Quanto più alto è il valore, tanto migliore sarà la qualità del video.
Flusso secondario	Formato video	Selezionare la risoluzione video tra **CIF**, **WVGA**, **QVGA** e **D1**.
	Velocità formato	Definisce il numero di fotogrammi per secondo. I valori ammessi vanno da **1** a **25** per l'opzione **PAL** e da **1** a **30** per l'opzione **NTSC**. Quanto più alto è il valore, tanto più scorrevole sarà il video.
	Velocità in bit	Definisce la quantità di dati trasmessi in 1 secondo. Si può definire il valore richiesto. Quanto più alto è il valore, tanto

Parametro		Descrizione
		migliore sarà la qualità del video.
Condizioni	Modalità scena	Permette di regolare il video per adattarlo a vari scenari. È possibile scegliere tra i valori **Automatico** (Automatic), **Assolato** (Sunny), **Notte** (Night) e **Disabilitato** (Disabled). Il valore predefinito è **Automatico** (Automatic).
	Modalità giorno/notte	È possibile scegliere tra le modalità **Automatico** (Automatic), **A colori** (Colorful) o **Bianco e nero** (Black White).
	Modalità retroilluminazione	Si possono selezionare le seguenti modalità: ● **Disabilitato**: Senza controluce. ● **Controluce:** La telecamera fornisce immagini più chiare di aree scure in caso di riprese di controluce. ● **Ampiezza dinamica:** Il sistema attenua le aree luminose e compensa quelle scure per garantire una chiarezza complessiva ottimale. ● **Inibizione:** Il sistema limita le aree luminose e riduce le dimensioni dell'alone per attenuare la luminosità complessiva.
	Sensibilità sensori	Regolazione del valore: quanto maggiore è il valore, tanto più facile sarà l'attivazione del sensore.
	Standard video	Selezionare **PAL** o **NTSC** in base al display del proprio dispositivo.
Immagine	Luminosità	Modifica il valore che regola la luminosità dell'immagine. Quanto maggiore è il valore, tanto più luminosa sarà l'immagine. Quanto minore è il valore, tanto più scura sarà l'immagine. L'immagine si sfoca facilmente quando si imposta un valore troppo elevato.
	Contrasto	Modifica livello di contrasto dell'immagine. Quanto maggiore è il valore, tanto maggiore sarà il contrasto tra aree chiare e scure dell'immagine. Con valori minori, avverrà il contrario. Se il valore impostato è troppo elevato, le aree scure diventeranno troppo scure e quelle chiare potranno facilmente diventare sovraesposte. L'immagine si sfoca facilmente quando si imposta un valore troppo basso.
	Tonalità	Rende il colore più profondo o più chiaro. Il valore predefinito è calcolato per il sensore luminoso ed è quello consigliato.
	Saturazione	Rende il colore più profondo o più chiaro. Quanto maggiore è il valore, tanto più intenso sarà il colore. Quanto minore è il valore, tanto più leggero sarà il colore. Il valore di saturazione non influenza la luminosità dell'immagine.
	Gamma	Modifica la luminosità dell'immagine e migliora l'intervallo dinamico in modo non lineare. Quanto maggiore è il valore, tanto più luminosa sarà l'immagine. Quanto minore è il valore, tanto più scura sarà l'immagine.
	Video.Guadagno	Amplifica il segnale video per aumentare la luminosità

Parametro		Descrizione
	automatico	dell'immagine. Se il valore è troppo elevato, le immagini avranno più disturbi.
	Specchio	Selezionando **Attiva** (On), l'immagine sarà visualizzata con i lati sinistro e destro invertiti.
	Capovolgimento	Selezionando **Attiva** (On), l'immagine sarà visualizzata capovolta.
Controlli audio	Selezionare **Abilita** (Enable) o **Disabilita** (Disabled) per attivare o disattivare ogni audio.	
Controlli del volume	Volume microfono	Regolazione del valore: quanto maggiore è il valore, tanto più elevato sarà il volume del microfono sul VTO.
	Volume bip	Regolazione del valore: quanto maggiore è il valore, tanto più elevato sarà il volume dei suoni di sistema.

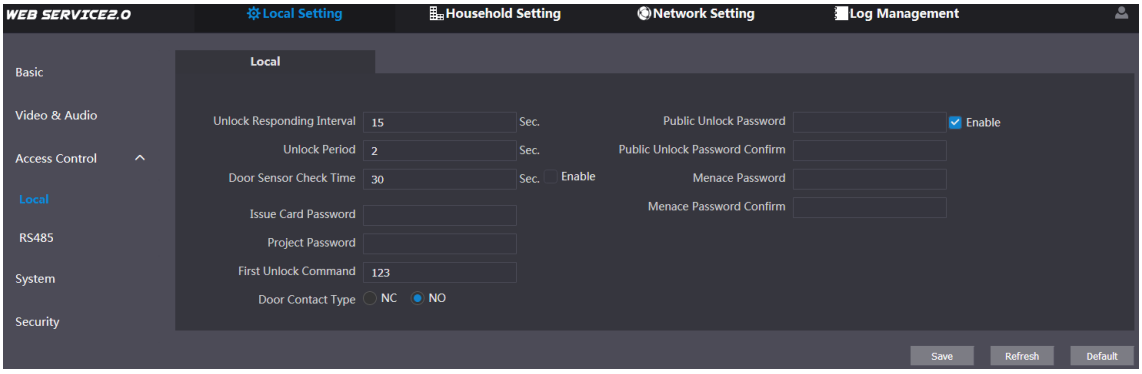
4.3 Controllo dell'accesso

Questa sezione descrive la configurazione dei sistemi di chiusura, comprendenti parametri quali intervallo di risposta sblocco, comandi di apertura porta, password di emissione scheda, password anticoercizione e protocollo di controllo ascensori.

4.3.1 Locale

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Controllo accessi > Locali** (Local Setting > Access Control > Local).

Figura 4-3 Locale



Fase 2: Configurare i parametri e consultare Tabella 4-3 per le descrizioni dettagliate.

Tabella 4-3 Descrizione dei parametri di controllo accessi locali

Parametro	Descrizione
Intervallo di risposta sblocco	Intervallo di tempo per poter sbloccare di nuovo dopo uno sblocco precedente, misurato in secondi.
Periodo di sblocco	Il tempo per cui la serratura resta aperta dopo lo sblocco, misurato in secondi.
Durata di controllo del sensore porta	Se il sensore porta è stato installato, è possibile configurare la durata. Quando il tempo di sblocco supera il valore della **Durata di controllo del sensore porta** (Door Sensor Check Time) definita, l'allarme del sensore porta sarà attivato e inviato al centro di gestione. ● Selezionando la casella di controllo **Abilita** (Enable), la porta

Parametro	Descrizione
	non sarà bloccata finché i sensori della porta non entrano in contatto tra di loro. ● Se la casella di controllo **Abilita** (Enable) non è selezionata, la porta sarà bloccata alla scadenza del **Periodo di sblocco** (Unlock Period).
Password di emissione scheda	Questa password può essere utilizzata per emettere nuove schede. ● La password può essere utilizzata solo da amministratori e tecnici. ● Il valore predefinito è 888888.
Password di progetto	Può essere usata per accedere all'interfaccia di progettazione; il suo valore predefinito è 888888. La password di progetto può essere utilizzata solo da amministratori e tecnici.
Comando di primo sblocco	È possibile collegare un telefono SIP di terzi al proprio VTO e usare il comando per aprire la porta da remoto.
Tipo di contatto porta	Selezionare **NC** o **NA** (NO) in base alla serratura in uso.
Password pubblica di sblocco	Selezionando la casella di controllo **Abilita** (Enable) e configurando la password pubblica di sblocco, tutti i residenti nell'unità coinvolta possono aprire la porta con questa password.
Conferma della password pubblica di sblocco	
Password antiminaccia	In caso di minacce alla sicurezza all'esterno della porta, sbloccando la porta tramite inserimento della password antiminaccia, il sistema invia una segnalazione di allarme al centro di gestione. ● Lapassword antiminaccia è l'inverso della password pubblica di sblocco. ● La password antiminaccia può essere modificata in base alle esigenze.
Conferma della password antiminaccia	Inserire di nuovo la password antiminaccia per confermarla.

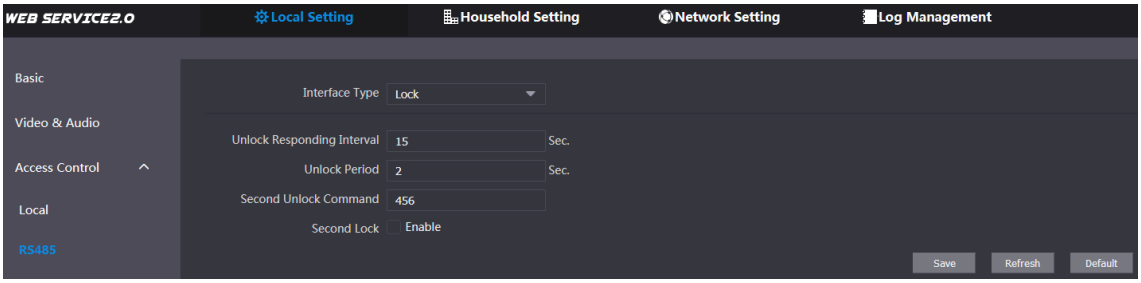
Fase 3: Fare clic su **Salva** (Save).

4.3.2 RS-485

Questa sezione descrive la configurazione dei dispositivi di controllo accessi RS-485, tra i quali quelli per il controllo di serrature e ascensori.

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Controllo accessi > RS485** (Local Setting > Access Control > RS485).

Figura 4-4 RS-485



Fase 2: È possibile configurare i parametri, selezionando tra quelli delle opzioni **Serratura** (Lock) o **Controllo ascensore** (Lift Control) nell'elenco **Tipo di interfaccia** (Interface Type). Per informazioni dettagliate, consultare la sezione Tabella 4-4.

Tabella 4-4 Descrizione parametri dei sistemi di controllo accessi RS-485

Parametro		**Descrizione**
Blocco	Intervallo di risposta sblocco	Intervallo di tempo per poter sbloccare di nuovo dopo uno sblocco precedente, misurato in secondi.
	Periodo di sblocco	Il tempo per cui la serratura resta aperta dopo lo sblocco, misurato in secondi.
	Comando di secondo sblocco	È possibile collegare un telefono SIP di terzi al proprio VTO e usare il comando per aprire la porta da remoto.
	Secondo blocco	È possibile collegare una o più porte ai dispositivi RS-485. ● Se la casella di controllo **Abilita** (Enable) è selezionata, premendo il pulsante di sblocco, passando la scheda di accesso o usando la password di sblocco, il sistema apre automaticamente il secondo blocco. ● Se la casella di controllo **Abilita** (Enable) non è selezionata, premendo il pulsante di sblocco, passando la scheda di accesso o usando la password di sblocco, il sistema apre automaticamente il primo blocco.
Controllo ascensori	Protocollo di controllo ascensori	Selezionando il protocollo richiesto per abilitare la funzione di controllo ascensori, è possibile definire i piani ai quali gli utenti possono fermarsi con l'ascensore.
	Velocità in baud	Immettere la velocità in baud del dispositivo RS-485 di terzi in uso.
	Bit di dati	Queste opzioni servono per il debugging della porta seriale.
	Bit di controllo	
	Bit di stop	

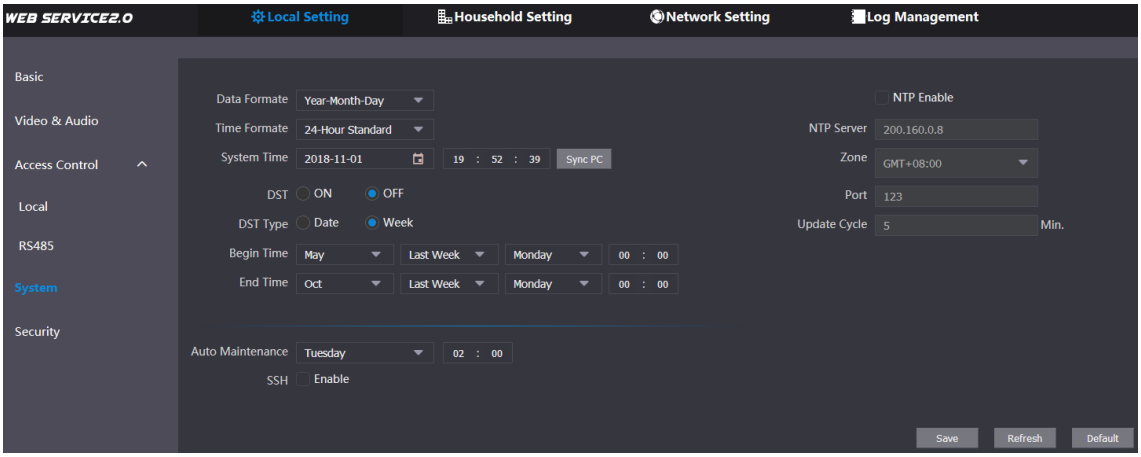
Fase 3: Fare clic su **Salva** (Save).

4.4 Sistema

Questo sezione descrive la configurazione del formato di data e orario e quella del server NTP.

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Sistema** (Local Setting > System).

Figura 4-5 Sistema



Fase 2: Configurare i parametri e consultare Tabella 4-5 per le descrizioni dettagliate.

Tabella 4-5 Descrizione dei parametri di sistema

Parametro	Descrizione
Formato data	I formati di data selezionabili sono Anno-Mese-Giorno, Mese-Giorno-Anno e Giorno-Mese-Anno.
Formato ora	Il formato orario può essere configurato, scegliendo tra **12 ore** (12-Hour) o **24 ore** (24-Hour).
Ora di sistema	Definire data, orario e fuso orario di sistema del VTO. Non modificare l'orario di sistema senza motivo; ciò potrebbe causare problemi alle funzioni di ricerca video e di pubblicazione di avvisi e istantanee. Prima di modificare l'orario di sistema, disattivare le funzioni di registrazione video e acquisizione automatica di istantanee.
Sincronizzazione PC	Fare clic qui per sincronizzare l'orario del sistema VTO e quello del PC.
Ora legale	Selezionare **ATTIVA** (ON) per abilitare la funzione ora legale.
Tipo ora legale	Selezionare **Data** per definire una data specifica o **Settimana** (Week) per definire la settimana di attivazione dell'ora legale.
Orario iniziale	Permette di definire l'orario iniziale e finale di validità dell'ora legale.
Data finale	
Abilitazione NTP	Selezionare la casella di controllo per attivare la funzione dell'orario NTP.
Server NTP	Inserire il nome di dominio del server NTP.
Zona	Il fuso orario dell'area corrente.
Porta	Il numero di porta del server NTP.
Aggiornamento	Indica la frequenza con cui l'orario del VTO si sincronizza con

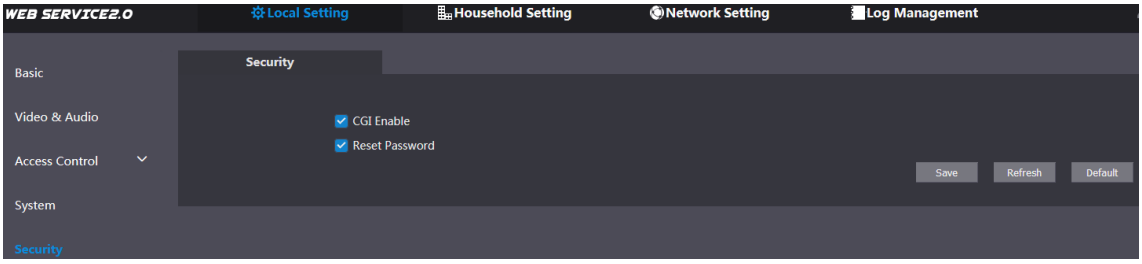
Parametro	Descrizione
ciclo	quello del server NTP; può essere al massimo di 30 minuti.
Manutenzione automatica	Selezionare data e ora di manutenzione automatica, che causerà il riavvio del VTO.
SSH	Selezionando la casella di controllo **Abilita** (Enable), sarà possibile connettere i dispositivi di debugging al VTO tramite protocollo SSH.

Fase 3: Fare clic su **Salva** (Save).

4.5 Sicurezza

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Sicurezza** (Local Setting > Security).

Figura 4-6 Sicurezza



Fase 2: Configurare i parametri e consultare Tabella 4-6 per le descrizioni dettagliate.

Tabella 4-6 Descrizione dei parametri di sicurezza

Parametro	Descrizione
Abilitazione CGI	Selezionando la casella di controllo per abilitare la funzione, sarà possibile usare il comando CGI.
Reimpostazione della password	Selezionando la casella di controllo per abilitare la funzione, sarà possibile reimpostare la password.

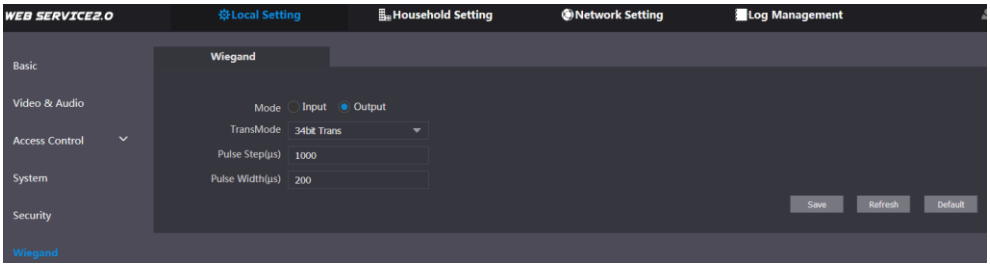
Fase 3: Fare clic su **Salva** (Save) per salvare.

4.6 Dispositivi Wiegand

Questa sezione descrive la configurazione dei parametri dei dispositivi Wiegand.

Fase 1: Sull'interfaccia principale (Figura 3-1), selezionare **Impostazioni Locali > Wiegand** (Local Setting > Wiegand).

Figura 4-7 Dispositivi Wiegand



Fase 2: Configura i parametri. Osservare la Tabella 4-7.

Tabella 4-7 Parametri Wiegand

Parametro	Descrizione
Modalità	Selezionare **Ingresso** (Input) o **Uscita** (Output) a seconda del tipo di

Parametro	Descrizione
	dispositivo Wiegand.
Modalità di trasmissione	Selezionare la velocità di trasmissione fra **34 bit**, **66 bit** e **26 bit**. Quanto più alto è il valore, tanto più veloce sarà la trasmissione.
Intervallo di impulso (µs)	Indica la frequenza del segnale Wiegand, il suo valore predefinito è 1000.
Ampiezza di impulso (µs)	Indica il valore massimo del segnale Wiegand, il suo valore predefinito è 200.

Fase 3: Fare clic su **Salva** (Save).

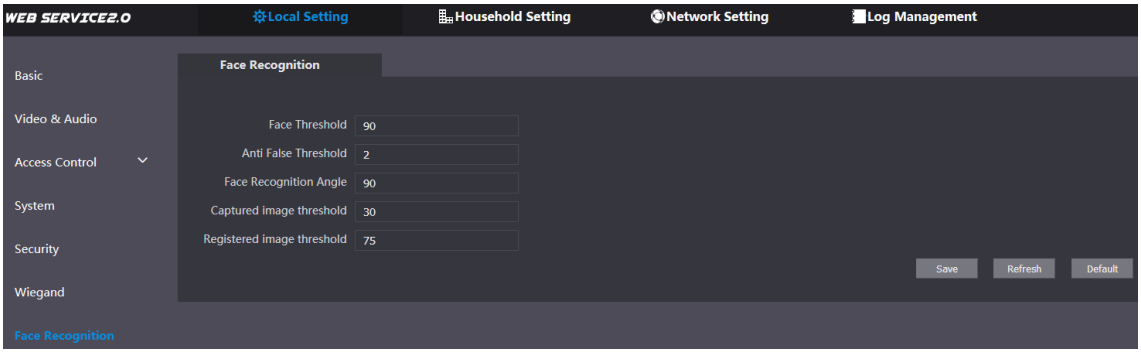
4.7 Riconoscimento facciale

Il riconoscimento facciale è disponibile su alcuni modelli selezionati.

Questa sezione descrive la configurazione di parametri quali soglia di riconoscimento facciale, soglia di prevenzione di falsi positivi e angolo di riconoscimento facciale.

Fase 1: Selezionare la voce Impostazioni Locali > Riconoscimento facciale (Local Setting > Face Recognition).

Figura 4-8 Riconoscimento facciale



Fase 2: Permette di configurare i parametri di riconoscimento facciale.

Tabella 4-8 Descrizione dei parametri di riconoscimento facciale

Parametro	Descrizione
Soglia di riconoscimento facciale	Quanto maggiore è il valore, tanto maggiore sarà il livello di somiglianza richiesto tra il target e i dati del volto memorizzato per l'apertura della porta.
Soglia di prevenzione falsi positivi	Quanto maggiore è il valore, tanto minore è la probabilità che il sistema riconosca un target come volto umano, aumentando in tal modo l'accuratezza del riconoscimento.
Angolo di riconoscimento facciale	Quanto maggiore è il valore, tanto maggiore sarà l'angolazione di cui il target potrà ruotare la faccia durante il riconoscimento.
Soglia di acquisizione immagini	Indica la qualità delle immagini acquisite. Quanto maggiore è il valore, tanto migliore è la qualità dell'immagine.
Soglia di registrazione immagini	Indica la qualità richiesta per un'efficace registrazione delle immagini. Quanto maggiore è il valore, tanto migliore sarà la qualità richiesta.

Fase 3: Fare clic su **Salva** (Save).

5 Impostazioni domestiche

Questo capitolo si applica ai casi in cui il dispositivo VTO funge da server SIP (consultare 6.4 Server SIP) e descrive le procedure di aggiunta, modifica e rimozione di dispositivi VTO, VTH, VTS e IPC, oltre alle modalità di invio di messaggi dal server SIP agli altri dispositivi VTO e VTH. In caso di utilizzo di altri server SIP, consultare il relativo manuale per i dettagli di configurazione.

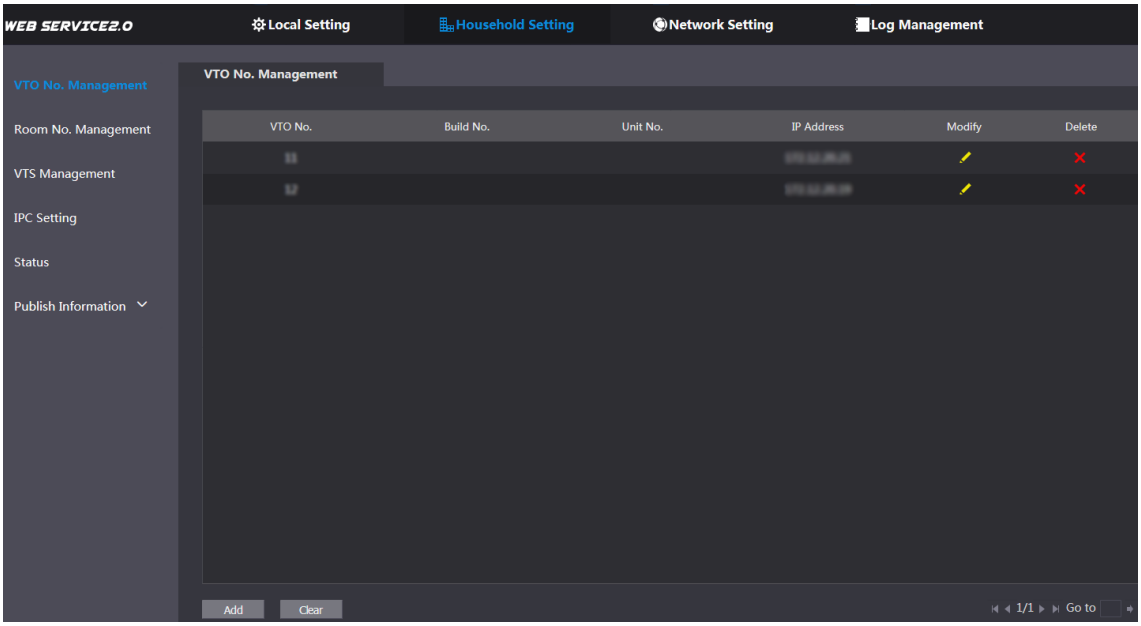
5.1 Gestione n. VTO

5.1.1 Aggiunta VTO

Aggiungendo dispositivi VTO a un server SIP, tutti i dispositivi VTO connessi allo stesso server SIP potranno effettuare chiamate audio e video tra loro.

Fase 1: Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Gestione n. VTO** (Household Setting > VTO No. Management).

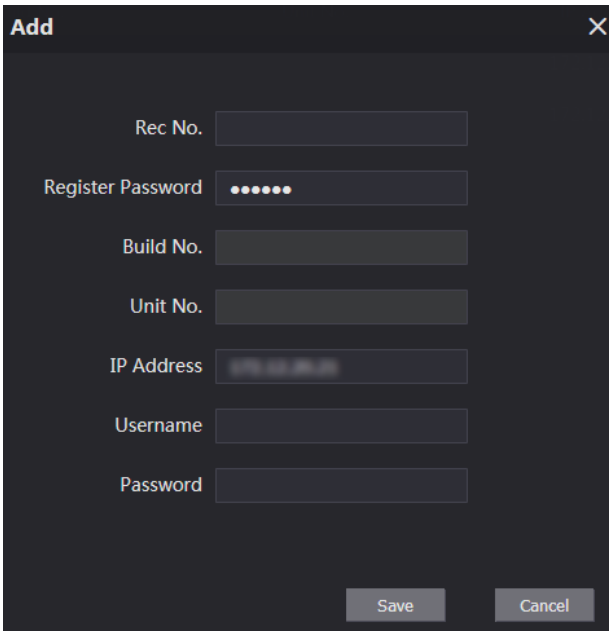
Figura 5-1 Gestione n. VTO



Fase 2: Fare clic su **Aggiungi** (Add).

Il sistema mostra l'interfaccia **Aggiunta** (Add). Osservare la Figura 5-2.

Figura 5-2 Aggiunta VTO



Fase 3: Configurare i parametri, assicurandosi anche di aggiungere il server SIP stesso. Osservare la Tabella 5-1.

Tabella 5-1 Aggiunta della configurazione VTO

Parametro	Descrizione
N. Rec	Il numero di VTO configurato per il VTO di destinazione. Consultare i dettagli in "Tabella 4-1."
Password di registrazione	Usare il valore predefinito.
N. edificio	Disponibile solo quando altri server fungono da server SIP.
N. unità	
Indirizzo IP	Indirizzo IP per il VTO di destinazione.
Nome utente	Nome utente e password per l'interfaccia web del VTO di destinazione.
Password	

Fase 4: Fare clic su **Salva** (Save).

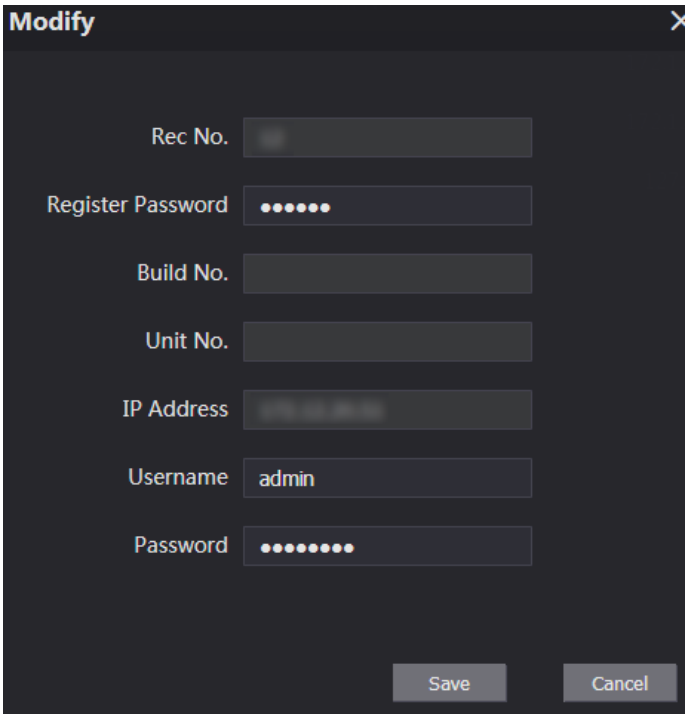
5.1.2 Modifica dei VTO

Il VTO attualmente in uso non può essere modificato o rimosso.

Fase 1: Sull'interfaccia di **Gestione n. VTO** (VTO No. Management) (Figura 5-1), fare clic su .

Il sistema mostra l'interfaccia **Modifica** (Modify). Osservare la Figura 5-3.

Figura 5-3 Modifica dei VTO



Fase 2: È possibile modificare **N. reg.** (Rec No.), **Nome utente** (Username) e **Password**. Consultare Tabella 5-1 per maggiori dettagli.
Fase 3: Fare clic su **Salva** (Save).

5.1.3 Rimozione dei VTO

Il VTO attualmente in uso non può essere modificato o rimosso.

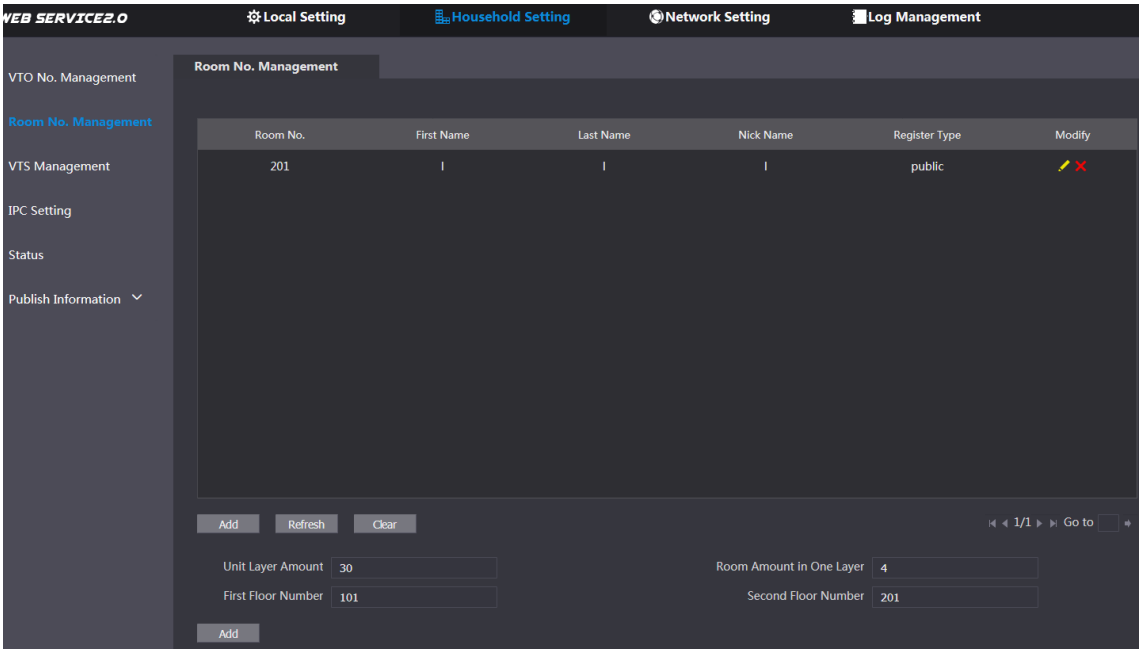
Sull'interfaccia di **Gestione N. VTO** (VTO No. Management) (Figura 5-1), fare clic su per rimuovere i VTO uno alla volta; oppure fare clic su **Cancella** (Clear) per rimuovere tutti i VTO.

5.2 Gestione n. stanza

5.2.1 Aggiunta del numero di stanza

È possibile aggiungere al server SIP il numero di stanza previsto, per poi configurare il numero di stanza sui dispositivi VTH per connetterli alla rete.
Fase 1: Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Gestione n. stanza** (Household Setting > Room No. Management).

Figura 5-4 Gestione n. stanza

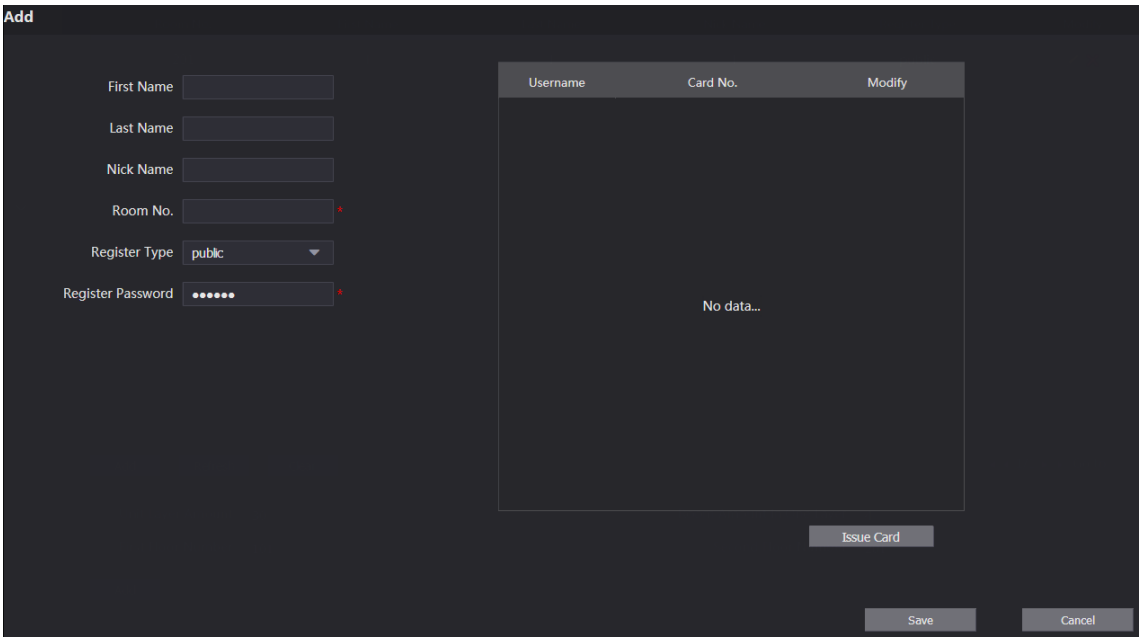


Fase 2: I numeri di stanza possono essere aggiunti singolarmente o in gruppi.

- Aggiunta di un numero di stanza singolo

1) Fare clic su **Aggiungi** (Add) nella posizione centrale in basso.

Figura 5-5 Aggiunta di un numero di stanza singolo



2) Configurare le informazioni delle stanze e per descrizioni dettagliate. Osservare la Tabella 5-2.

Tabella 5-2 Informazioni stanza

Parametro	Descrizione
Nome	Inserire le informazioni necessarie a distinguere le singole stanze.
Cognome	
Nome alternativo	
N. stanza	Numero di stanza previsto.

Parametro	Descrizione
Tipo di registrazione	Selezionare il valore **pubblico** (public), poiché **locale** (local) è riservato a usi futuri.
Password di registrazione	Usare il valore predefinito.

3) Fare clic su **Salva** (Save).

Il sistema mostra il numero di stanza aggiunto. Fare clic su per modificare le informazioni relative alla stanza; fare clic su per eliminare la stanza.

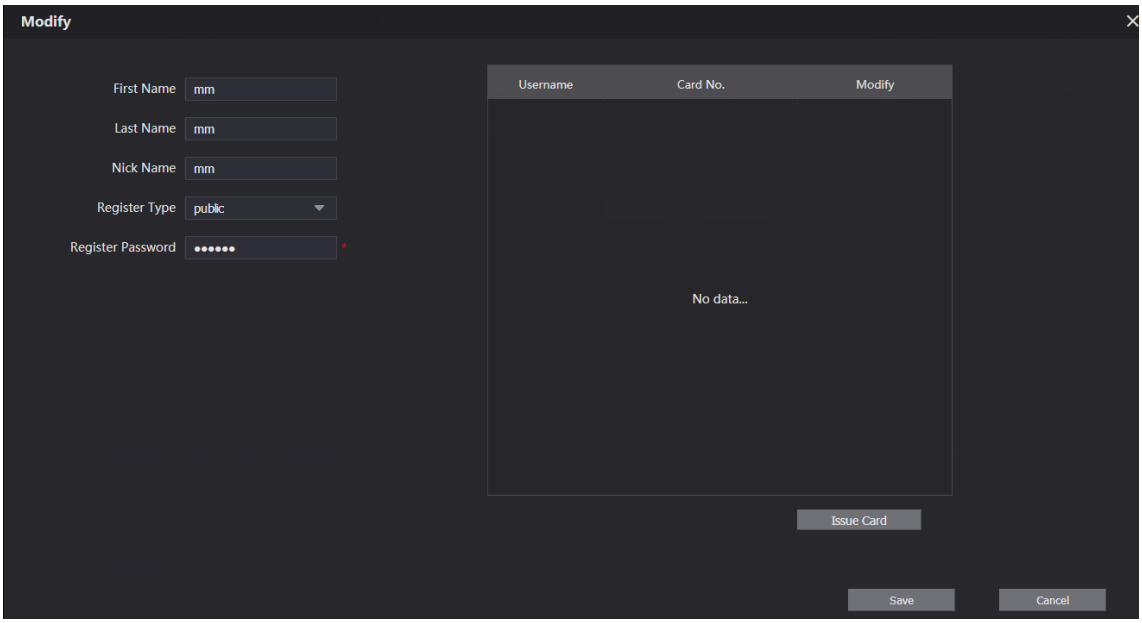
- Aggiunta di numeri di stanza in gruppo

1) Definire il **Numero di piani per unità residenziale** (Unit Layer Amount), **Numero di stanze in un piano** (Room Amount in One Layer), **Numero di primo** e **secondo piano** (First Floor Number, Second Floor Number) in base alle condizioni effettive.
2) Fare clic su **Aggiungi** (Add) nella posizione in basso.
   Il sistema mostra tutti i numeri di stanza aggiunti. Fai clic su **Aggiorna** (Refresh) per visualizzare lo stato aggiornato e fare clic su **Cancella** (Clear) per rimuovere i numeri di tutte le stanze.

5.2.2 Modifica del numero di stanza

Fase 1: Sull'interfaccia di **Gestione n. stanza** (Room No. Management) (Figura 5-4), fare clic su .

Figura 5-6 Modifica del numero di stanza



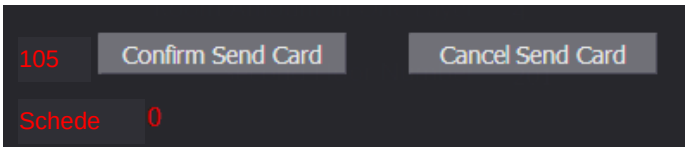
Fase 2: È possibile modificare i nomi delle stanze. Consultare Tabella 5-2 per maggiori dettagli.
Fase 3: Fare clic su **Salva** (Save).

5.2.3 Emissione di schede di accesso

È possibile emettere schede di accesso alle stanze, definendole come schede principali o marcandole come smarrite.

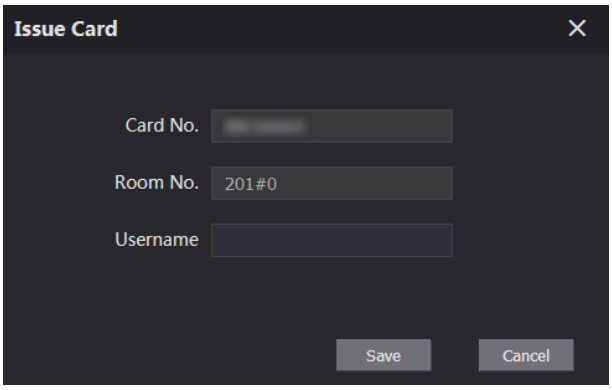
Fase 1: Nell'interfaccia di Modifica numero stanze (Modify room number) (Figura 5-6), fare clic su **Emissione schede** (Issue Card).

Figura 5-7 Avviso di conto alla rovescia



Fase 2: Passando la scheda che deve essere autorizzata sul VTO, il sistema mostra la casella di dialogo **Emissione schede** (Issue Card). Osservare la Figura 5-8.

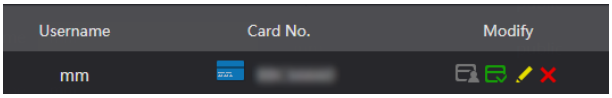
Figura 5-8 Emissione scheda



Fase 3: Inserire il nome richiesto, quindi fare clic su **Salva** (Save) e poi su **Conferma invio scheda** (Confirm Send Card) alla comparsa dell'avviso di conto alla rovescia (Figura 5-7).

Il sistema mostra la scheda di accesso emessa. Osservare la Figura 5-9.

Figura 5-9 Schede di accesso emesse



Fase 4: Le schede di accesso possono essere configurate.

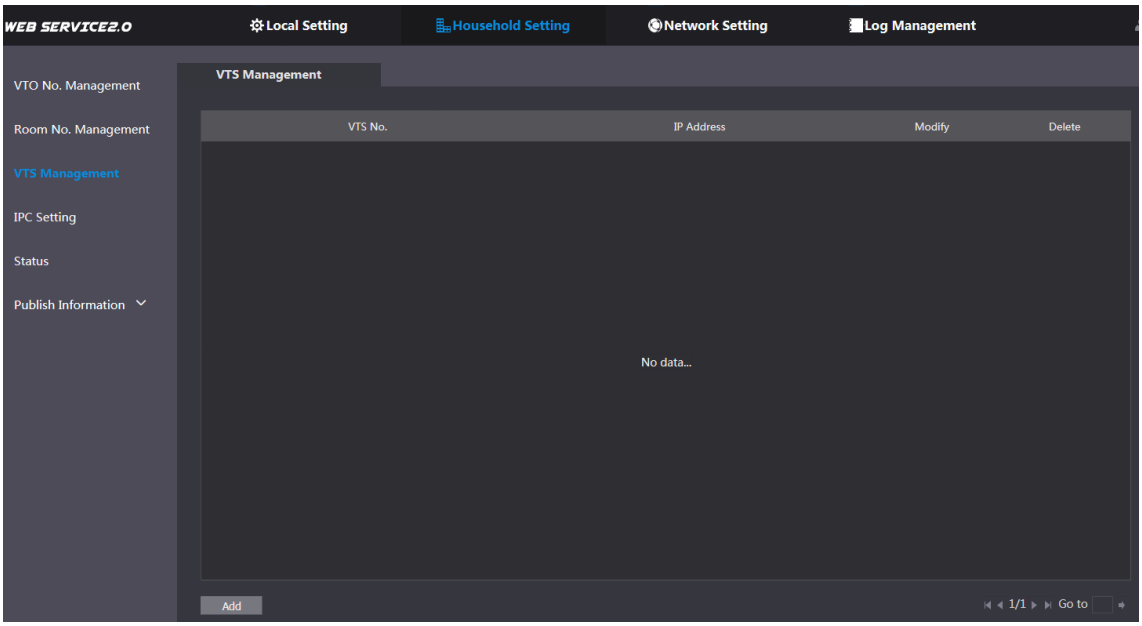
- Facendo clic su per definire una scheda come scheda principale, l'icona visualizzata diventa . La scheda principale può essere utilizzata per l'emissione di altre schede di accesso sul VTO. Fare di nuovo clic per riprendere.
- Facendo clic su per marcare una scheda come smarrita, l'icona visualizzata diventa . Le schede in stato smarrito non possono essere usate per l'apertura delle porte. Fare di nuovo clic per riprendere.
- Fare clic su per modificare il nome utente.
- Fare clic su per eliminare la scheda.

5.3 Gestione VTS

È possibile aggiungere al server SIP dei dispositivi VTS, che potranno essere utilizzati come centri di gestione. Permette di gestire tutti i dispositivi VTO e VTH in rete, fare e ricevere chiamate video tra di essi ed effettuare configurazioni di base. Per maggiori informazioni, consultare il relativo manuale d'uso.

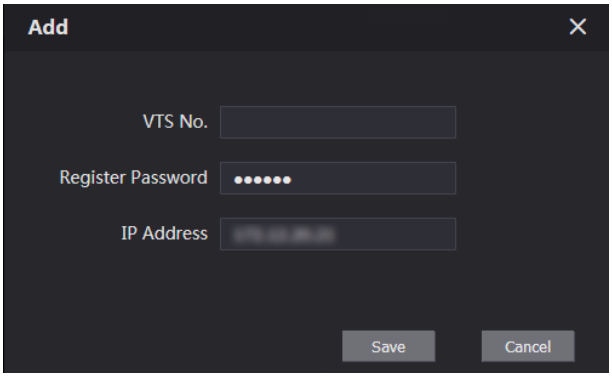
Fase 1: Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Gestione VTS** (Household Setting > VTS Management)

Figura 5-10 Gestione VTS



Fase 2: Fare clic su **Aggiungi** (Add).

Figura 5-11 Aggiunta di VTS



Fase 3: Selezionare sul VTS l'opzione **Configurazione > Configurazioni avanzate** (Config > Advance Config), poi immettere la password (valore predefinito 123456), quindi selezionare **Server SIP** (SIP Server). Il sistema mostra il **N. VTS** (VTS No.) come **Nome utente** (User Name) (di solito il valore è 888888XXX).

Fase 4: Configurare i parametri e consultare Tabella 5-3 per le descrizioni dettagliate.

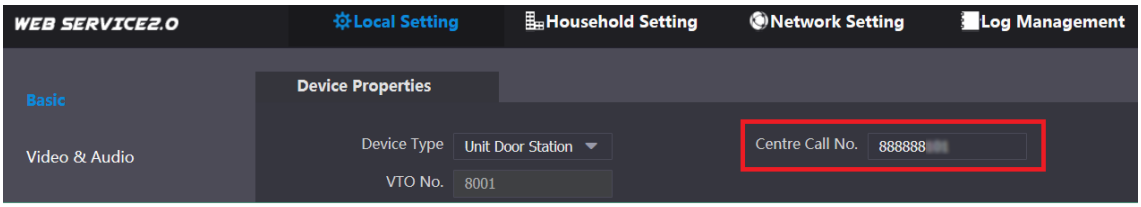
Tabella 5-3 Aggiunta della configurazione VTS

Parametro	Descrizione
N. VTS	Il numero di VTS configurato per il VTS di destinazione.
Password di registrazione	Usare il valore predefinito.
Indirizzo IP	Indirizzo IP per il VTS di destinazione.

Fase 5: Facendo clic su **Salva** (Save), il sistema mostra il VTS aggiunto. Fare clic su per modificare l'indirizzo IP; fare clic su per rimuoverlo.

Fase 6: Selezionare **Impostazioni Locali > Imp. base** (Local Setting > Basic), quindi inserire il numero del VTS aggiunto come **N. di chiamata centro** (Center Call No.). In tal modo, sarà possibile chiamare il VTS premendo il pulsante di chiamata centro sul VTO. Osservare la Figura 5-12.

Figura 5-12 N. di chiamata centro.



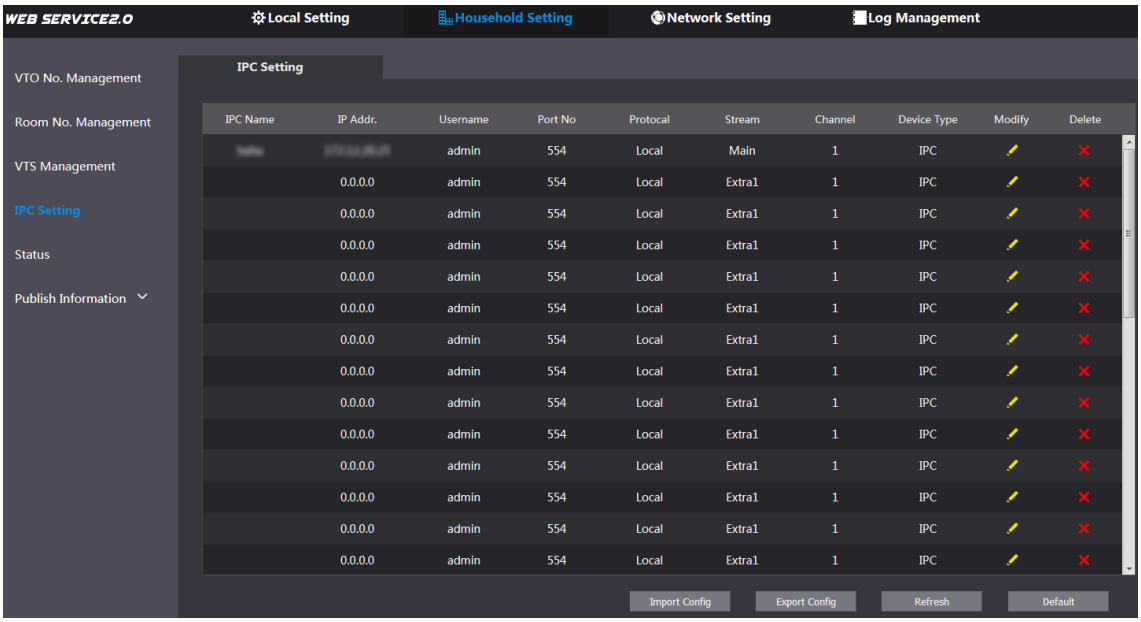
Fase 7: Fare clic su **Conferma** (Confirm).

5.4 Impostazioni IPC

È possibile aggiungere al server SIP dispositivi IPC, NVR, HCVR, XVR e poi tutti i VTH collegati potranno effettuare il monitoraggio con le telecamere aggiunte.

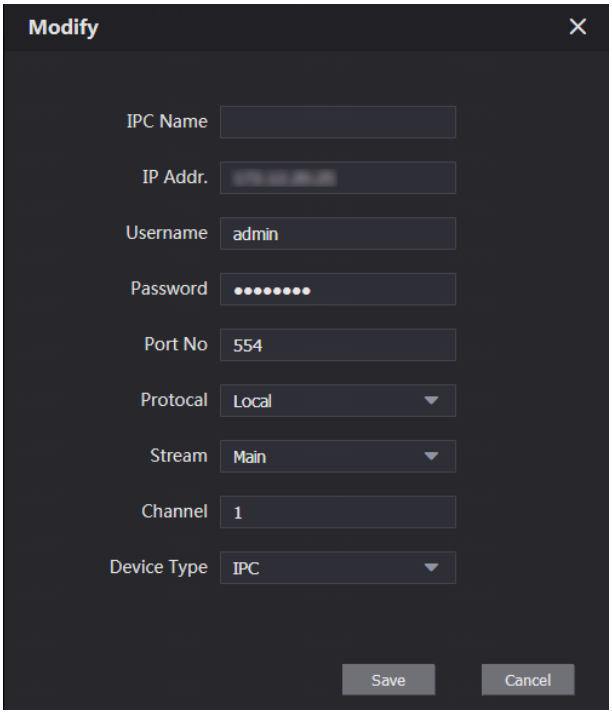
Fase 1: Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Impostazioni IPC** (Household Setting > IPC Setting)

Figura 5-13 Impostazioni IPC



Fase 2: La quantità totale di dispositivi che possono essere aggiunti è prefissata. È possibile fare clic su per aggiungere il dispositivo richiesto.

Figura 5-14 Aggiungere l'IPC



Fase 3: Configurare i parametri e consultare Tabella 5-4 per le descrizioni dettagliate.

Tabella 5-4 Aggiunta della configurazione IPC

Parametro	Descrizione
Nome IPC	Inserire il nome del dispositivo richiesto.
Indirizzo IP.	Indirizzo IP del dispositivo.
Nome utente	Nome utente e password per l'interfaccia web del dispositivo.
Password	
N. di porta.	Usare il valore predefinito.
Protocollo	Selezionare **Locale** (Local) o **Onvif**.
Flusso	Selezionare **Principale** (Main) o **Extra1**. In tal modo il flusso principale avrà immagini di migliore qualità ma un maggior consumo di banda.
Canale	Definire un canale per il dispositivo.
Tipo di dispositivo	Selezionare **IPC**, **NVR**, **HCVR** o **XVR** in base alle esigenze.

Fase 4: Facendo clic su **Salva** (Save), il sistema mostra il dispositivo aggiunto. Fare clic su per modificarlo; fare clic su per rimuoverlo.

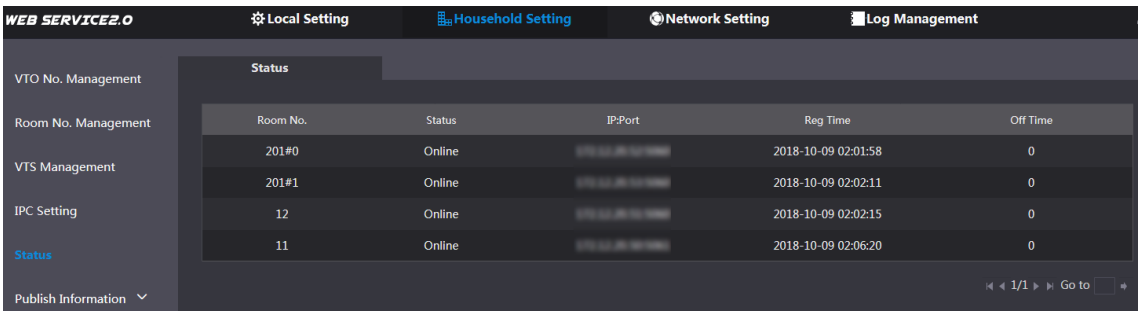
È anche possibile fare clic su **Esporta configurazione** (Export Config) per esportare i dispositivi correnti sul PC locale, oppure su **Importa configurazione** (Import Config) per importare una configurazione preesistente.

5.5 Stato

È possibile visualizzare lo stato operativo e l'indirizzo IP di tutti i dispositivi connessi.

Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Stato** (Household Setting > Status).

Figura 5-15 Stato



5.6 Pubblicazione di informazioni

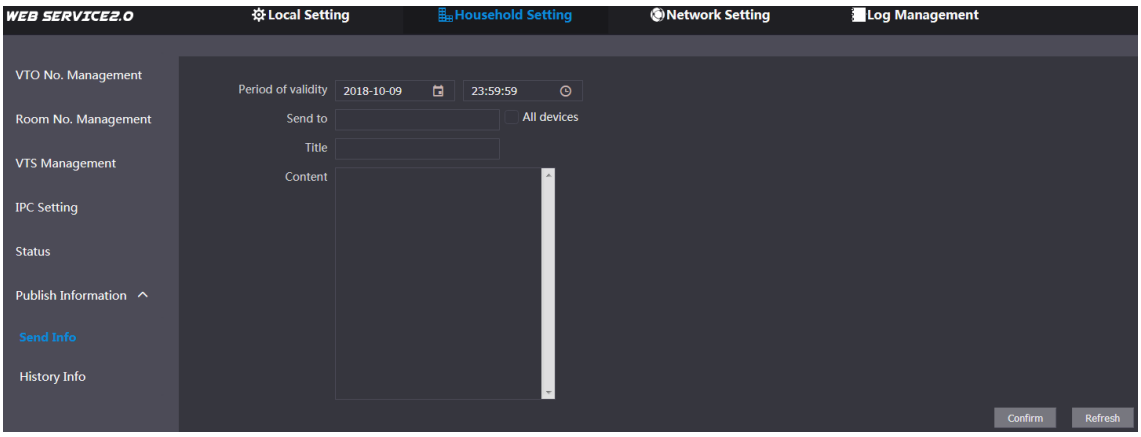
È possibile inviare messaggi dal server SIP agli altri dispositivi VTH e visualizzare la cronologia dei messaggi inviati.

5.6.1 Invio di informazioni

Fase 1: Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Pubblica informazioni > Invia Info** (Household Setting > Publish Information > Send Info).

Il sistema mostra l'interfaccia **Invia info** (Send Info). Osservare la Figura 5-16.

Figura 5-16 Invio di informazioni



Fase 2: Inserire il numero del VTO di destinazione oppure selezionare **Tutti i dispositivi** (All device) per inviare il messaggio a tutti i dispositivi in rete; seguirà l'invio del titolo e del contenuto del messaggio.

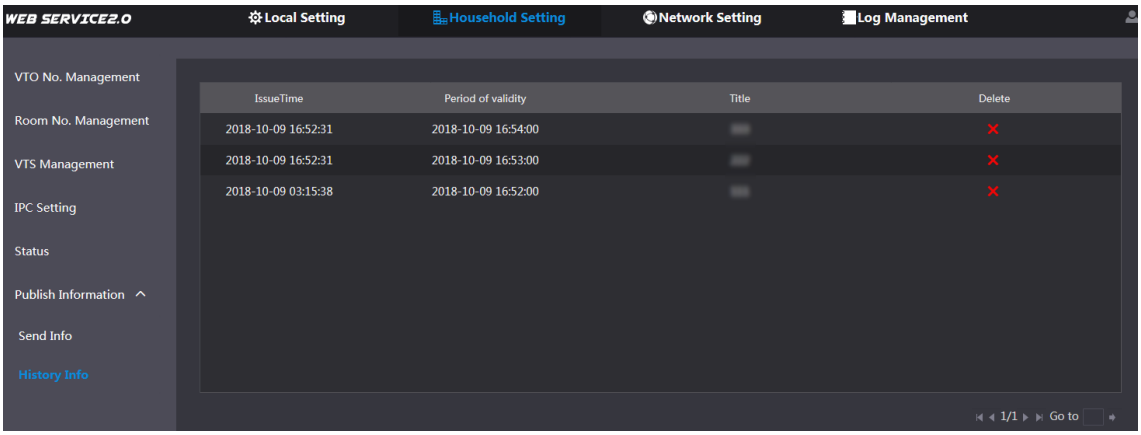
- Per inviare informazioni a più VTH, occorre elencare i numeri di VTH separati da punto e virgola. Ad esempio, immettendo 101; 102; 103 i VTH corrispondenti a questi numeri riceveranno le informazioni inviate dal VTO.
- Il parametro Periodo di validità è riservato a un uso futuro.

Fase 3: Fare clic su **Conferma** (Confirm).

5.6.2 Informazioni di cronologia

Accedere all'interfaccia web del server SIP, quindi selezionare **Impostazioni domestiche > Pubblica informazioni > Informazioni di cronologia** (Household Setting > Publish Information > History Info).

Figura 5-17 Informazioni di cronologia



Sarà possibile visualizzare l'orario e il titolo dei messaggi inviati.

5.7 Gestione dei dati facciali

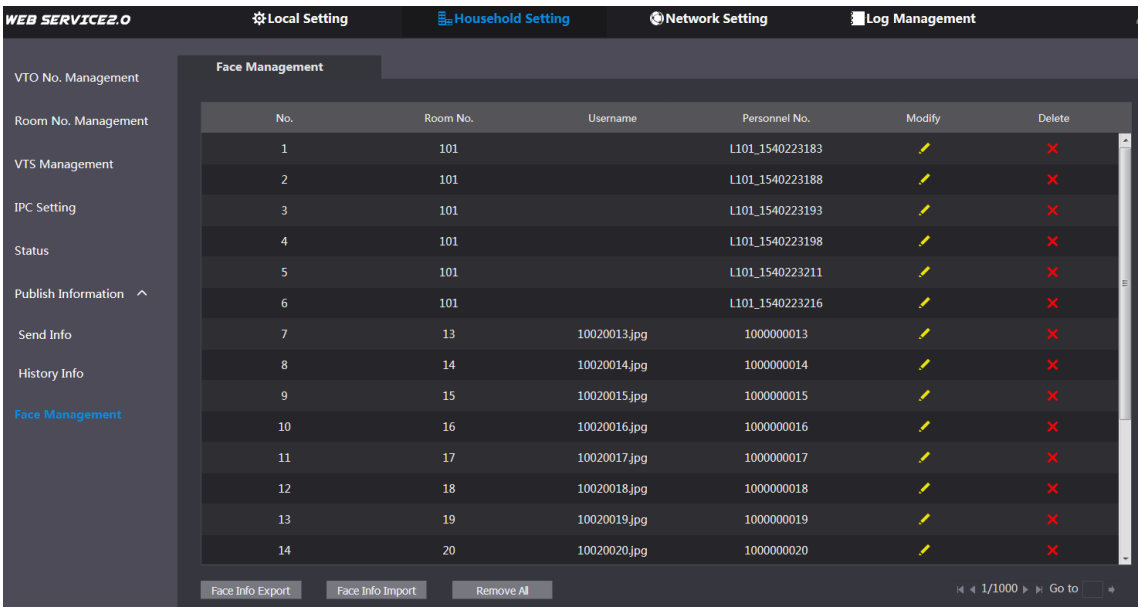
I datti facciali possono essere aggiunti, rimossi, importati ed esportati.

- Il riconoscimento facciale è disponibile su alcuni modelli selezionati.
- Il VTO può gestire al massimo i dati di 10.000 volti.

Selezionare **Impostazioni domestiche > Gestione volti** (Household Setting > Face Management).

Il sistema mostra l'interfaccia **Gestione Volti** (Face Management). Osservare la Figura 5-18.

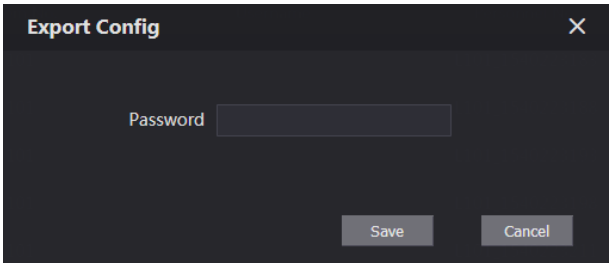
Figura 5-18 Gestione dei dati facciali



5.7.1 Esportazione dei dati facciali

Fase 1: Fare clic su **Esporta info facciali (**Face Info Export).

Figura 5-19 Esportazione configurazione



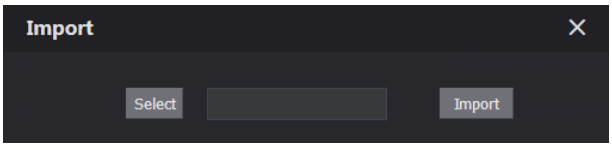
Fase 2: Inserire la password dell'interfaccia web, quindi fare clic su **Salva** (Save) per esportare i dati facciali.

5.7.2 Importazione dei dati facciali

Fase 1: Fare clic su Importa info facciali.

Fase 2: Inserire la password dell'interfaccia web, quindi fare clic su **Salva** (Save).

Figura 5-20 Importa



Fase 3: Fare clic su **Scegli** (Select) e selezionare il file richiesto.

Fase 4: Fare clic su **Importa** (Import).

5.7.3 Rimozione dei dati facciali

Fare clic su  per rimuovere i dati di un singolo volto.

Fare clic su **Rimuovi tutto** (Remove All) per rimuovere tutti i dati facciali.

6 Impostazioni di rete

Questo capitolo descrive la configurazione dei parametri di rete, quali indirizzo IP, FTP, server SIP, DDNS e UPnP.

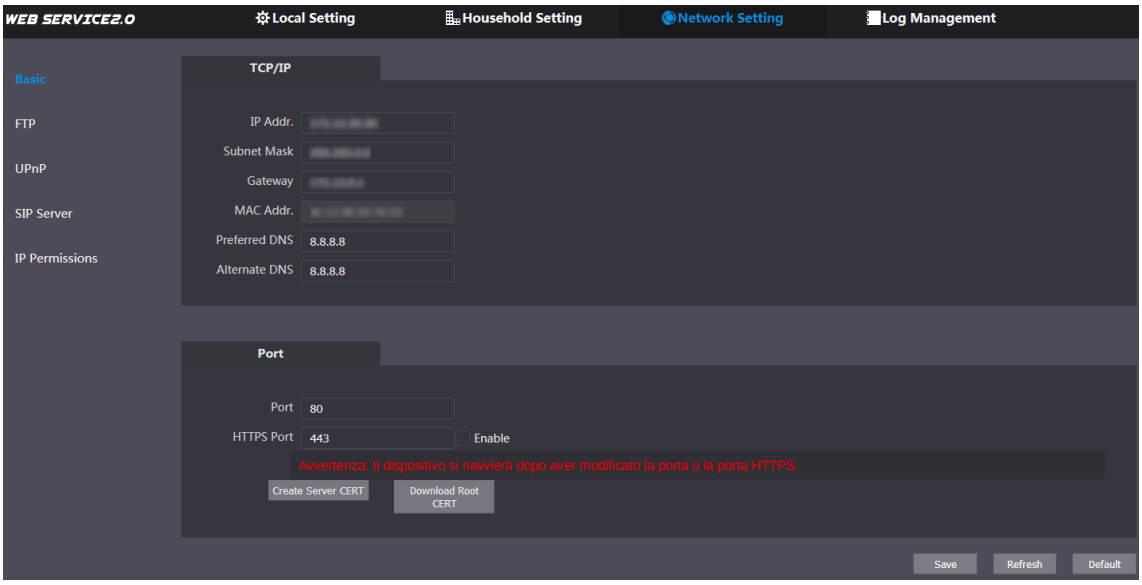
6.1 Impostazioni di base

6.1.1 TCP/IP

È possibile modificare l'indirizzo IP e il numero di porta del VTO.

Fase 1: Selezionare la **voce Impostazioni di Rete > Imp. base** (Network Setting > Basic).

Figura 6-1 Parametri TCP/IP e porte



Fase 2: Inserire i parametri di rete e il numero di porta previsti e quindi fare clic su **Salva** (Save).

Il VTO si riavvierà e per poter accedere di nuovo sarà necessario modificare anche l'indirizzo IP del PC in modo che esso di trovi nello stesso segmento di rete del VTO.

6.1.2 HTTPS

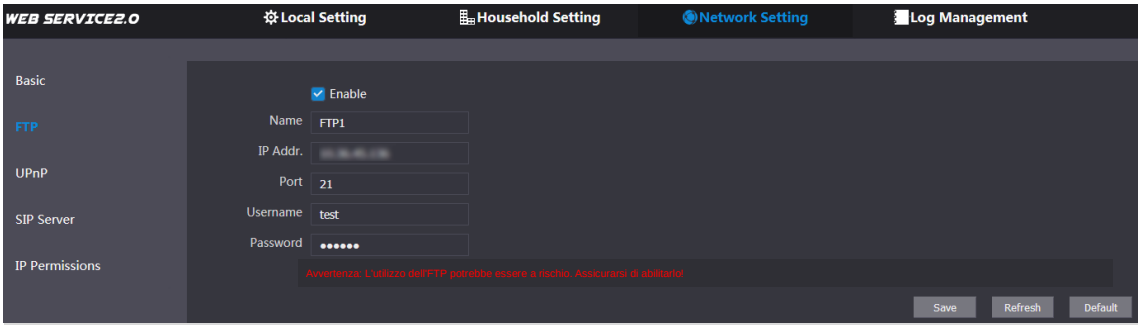
Selezionando la casella di controllo **Abilita** (Enable) della voce **Porta HTTPS** (HTTPS Port), il VTO si riavvierà. Dopo il riavvio, è possibile accedere al VTO inserendo "https:// Indirizzo IP VTO" nella barra degli indirizzi del browser.

6.2 FTP

Configurando il server FTP, sarà possibile salvare i video e le istantanee registrati sul server FTP.

Fase 1: Selezionare la **voce Impostazioni di Rete > FTP** (Network Setting > FTP).

Figura 6-2 FTP



Fase 2: Configura i parametri. Osservare la Tabella 6-1.

Tabella 6-1 Descrizione dei parametri FTP

Parametro	Descrizione
Abilita	Selezionare la casella di controllo per attivare la funzione FTP.
Nome	Inserire il nome del server FTP richiesto.
Indirizzo IP.	Indirizzo IP del server FTP.
Porta	Il valore predefinito è 21.
Nome utente	Nome utente e password del server FTP.
Password	

Fase 3: Fare clic su **Salva** (Save).

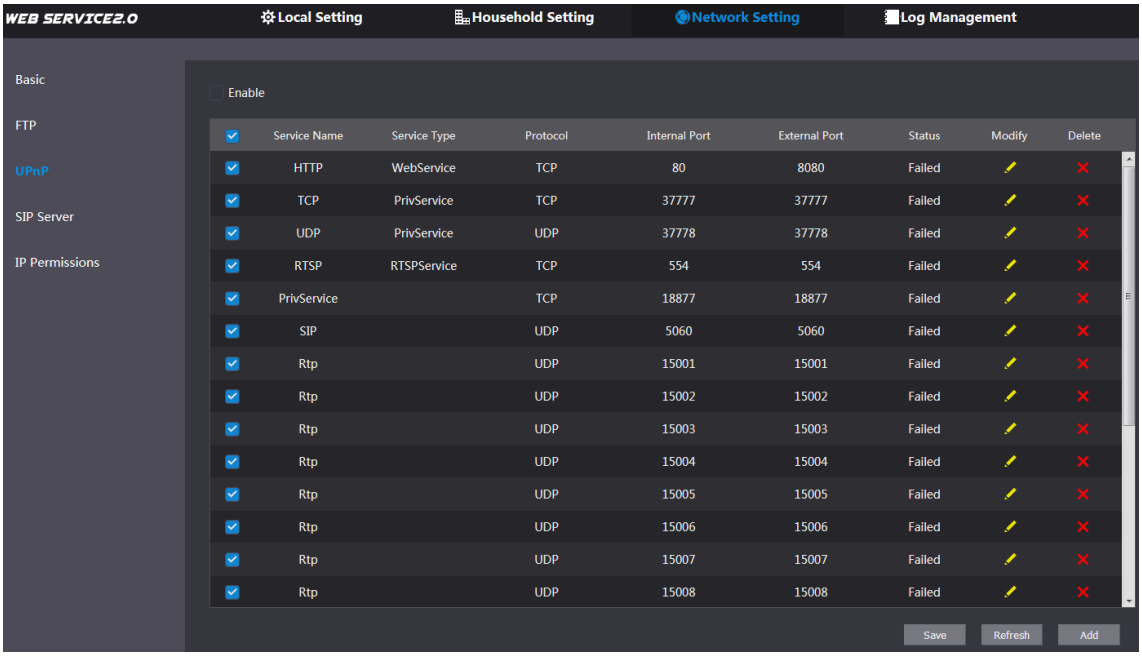
6.3 UPnP

Il protocollo Universal Plug and Play (UPnP) definisce le relazioni di mappatura delle porte tra le reti LAN e WAN. Questa funzione permette di avere accesso ai dispositivi della rete locale (LAN) tramite rete geografica (WAN).

- Questa funzione è disponibile solo quando il VTO funge da server SIP.
- La funzione è richiesta solo quando il VTO è connesso a un router dotato di funzione UPnP.

Fase 1: Selezionare la **voce Impostazioni di Rete > UPnP** (Network Setting > UPnP).

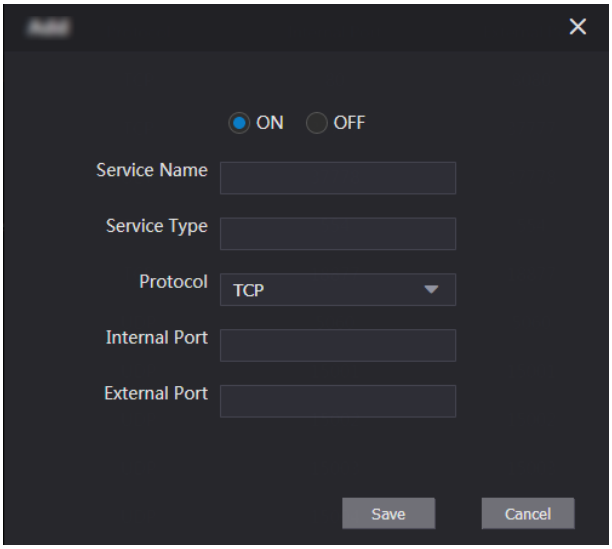
Figura 6-3 UPnP



Fase 2: Selezionare la casella di controllo **Abilita** (Enable) per attivare la funzione UPnP.

Fase 3: Alcune relazioni predefinite di mappatura porte sono state definite con impostazioni di fabbrica, che possono essere modificate facendo clic su . È anche possibile fare clic su **Aggiungi** (Add) per aggiungerne di nuove.

Figura 6-4 Modifica/Aggiunta UPnP



Fase 4: Configura i parametri. Osservare la Tabella 6-2.

Tabella 6-2 Descrizione dei parametri UPnP

Parametro	Descrizione
ATTIVA /DISATTIVA	Selezionare **ATTIVA** (ON) per abilitare questa relazione di mappatura.
Nome servizio	Nome del servizio.
Tipo di servizio	Permette di definire il tipo di servizio richiesto.
Protocollo	È possibile scegliere **TCP** o **UDP**. Per garantire la stabilità della trasmissione, si suggerisce di scegliere **TCP**.

Parametro	Descrizione	
Porta interna	Porta sul VTO in rete locale che si intende visitare.	 • Per evitare conflitti durante la mappatura di porte con il router, usare numeri di porta compresi tra 1024 e 5000, e non quelli tra 1 e 255 o tra 256 e 1023. • In caso di mappatura di più dispositivi su porte esterne, si consiglia di pianificarli in anticipo, per evitare che vari dispositivi possano essere mappati sulla stessa porta esterna. • Accertarsi che le porte da usare non siano già utilizzate né soggette a limitazioni. • Le porte esterne di TCP e UDP devono essere le stesse.
Porta esterna	Porta del router cui viene mappata la porta del VTO.	

Fase 5: Fare clic su **Salva** (Save).

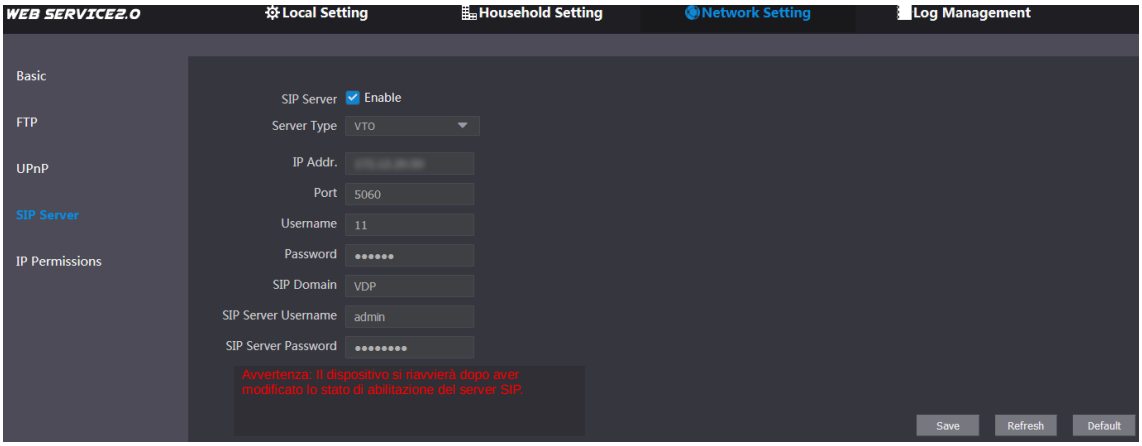
Aprire il browser web e inserire "http:// Indirizzo IP WAN: numero di porta esterna". In tal modo sarà possibile accedere al dispositivo connesso alla rete locale tramite la porta corrispondente.

6.4 Server SIP

Il server SIP permette la trasmissione in rete del protocollo di comunicazione interna, in modo che tutti i dispositivi VTO e VTH connessi allo stesso server SIP siano in grado di effettuare chiamate video tra di loro. I dispositivi VTO possono fungere da server SIP oppure si possono usare altri server allo scopo.

Fase 1: Selezionare la **voce Impostazioni di Rete > Server SIP** (Network Setting > SIP Server).

Figura 6-5 Server SIP



Fase 2: Selezionare il tipo di server richiesto.

- Se il VTO in uso funge da server SIP
  Selezionare la casella di controllo **Abilita** (Enable) della voce **Server SIP** (SIP Server) e poi fare clic su **Salva** (Save).

Il VTO si riavvierà e poi sarà possibile aggiungere dispositivi VTO e VTH al VTO in uso. Consultare i dettagli in "5 Impostazioni domestiche."

Se il VTO in uso non funge da server SIP, non selezionare la casella di controllo **Abilita** (Enable) per il **Server SIP** (SIP Server), altrimenti la connessione non riuscirà.

- Se altri VTO fungono da server SIP
  Selezionare **VTO** sull'elenco **Tipo server** (Server Type) e poi configurare i parametri. Osservare la Tabella 6-3.

Tabella 6-3 Configurazione del server SIP

Parametro	Descrizione
Indirizzo IP.	Indirizzo IP del VTO, che funge da server SIP.
Porta	5060
Nome utente	Usare il valore predefinito.
Password	
Dominio SIP	VDP
Nome utente del server SIP	Nome utente e password per l'interfaccia web del server SIP.
Password del server SIP	

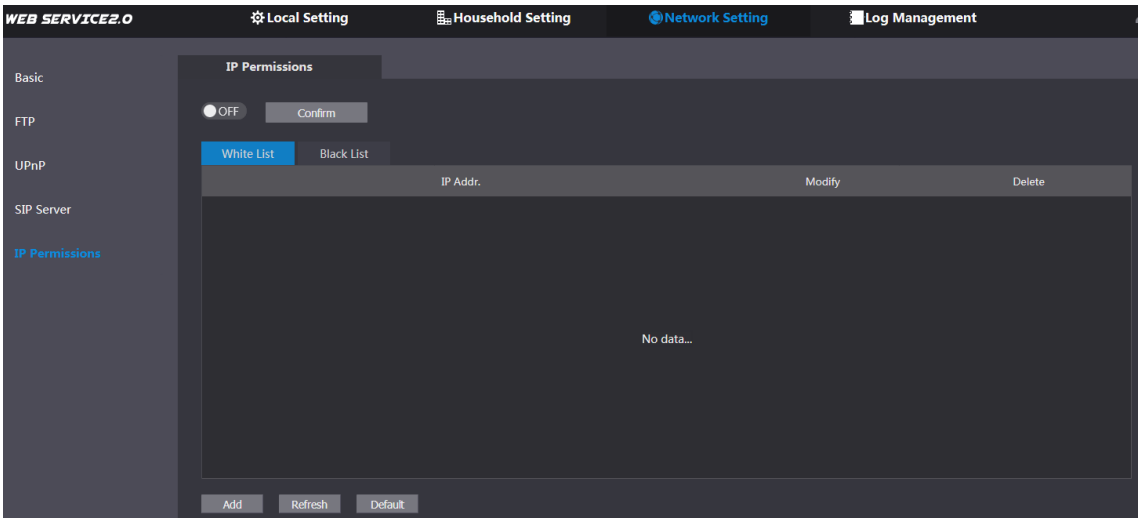
- Se altri server fungono da server SIP
  Selezionare il **Tipo server** (Server Type) richiesto e poi consultare il relativo manuale per i dettagli di configurazione.

6.5 Autorizzazioni IP

Per aumentare la sicurezza di rete e dei dati, occorre definire le autorizzazioni di accesso per i vari indirizzi IP.

Fase 1: Selezionare la voce Impostazioni di Rete > Autorizzazioni IP (Network Setting > IP Permissions).

Figura 6-6 Autorizzazioni IP

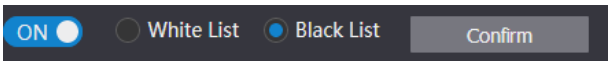


Fase 2: Fare clic su 

.

Il sistema mostra le opzioni **White List** e **Black List**. Osservare la Figura 6-7.

Figura 6-7 White List e Black List



È possibile utilizzare solo una delle due opzioni alla volta.

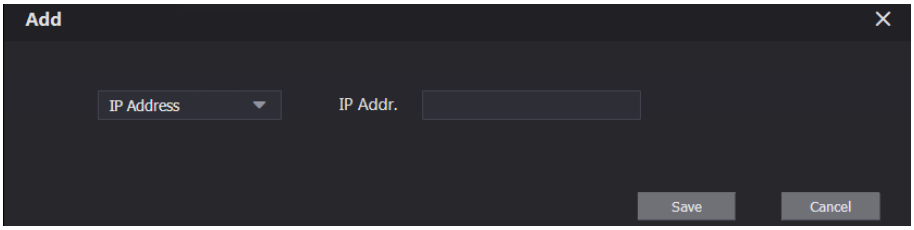
- **White list**: Solo gli indirizzi IP in elenco possono accedere al VTO.
- **Black list**: Nessuno degli indirizzi IP in elenco può accedere al VTO.

Fase 3: Selezionare White List o Black List.

- Per usare la black list, selezionare **Black List** e poi fare clic su **Conferma** (Confirm).
- Per usare la white list, selezionare **White List** e poi aggiungere gli indirizzi IP o le sezioni IP alla white list prima di fare clic su **Conferma** (Confirm).

Fase 4: Fare clic su **Aggiungi** (Add).

Figura 6-8 Aggiunta di indirizzi IP



Fase 5: È possibile selezionare e inserire singoli indirizzi IP o sezioni IP e poi fare clic su **Salva** (Save).

7 Gestione registri

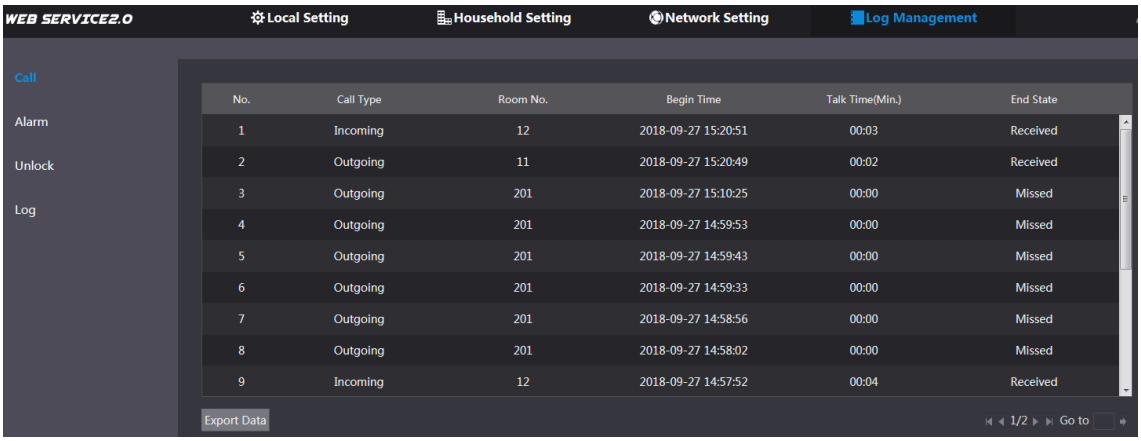
È possibile visualizzare le cronologie di chiamate, le registrazioni di allarmi e sblocchi e vari registri di sistema.

7.1 Chiamata

È possibile visualizzare il tipo di chiamata, il numero di stanza, l'orario iniziale, la durata di conversazione e lo stato finale.

Fase 1: Selezionare **Gestione registri > Chiamate** (Log Management > Call).

Figura 7-1 Chiamata



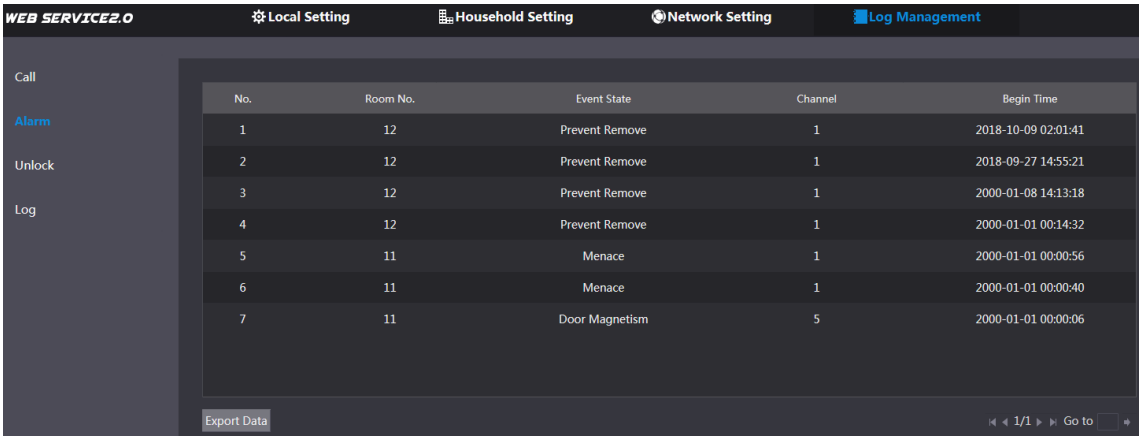
Fase 2: Fare clic su **Esporta dati** (Export Data) per esportare le registrazioni sul proprio PC.

7.2 Allarme

Questa funzione è visualizzata solo quando il VTO in uso funge da server SIP e permette di visualizzare le registrazioni di allarmi VTO e VTH e di allarmi anticoercizione.

Fase 1: Selezionare Gestione registri > Allarmi (Log Management > Alarm).

Figura 7-2 Allarme



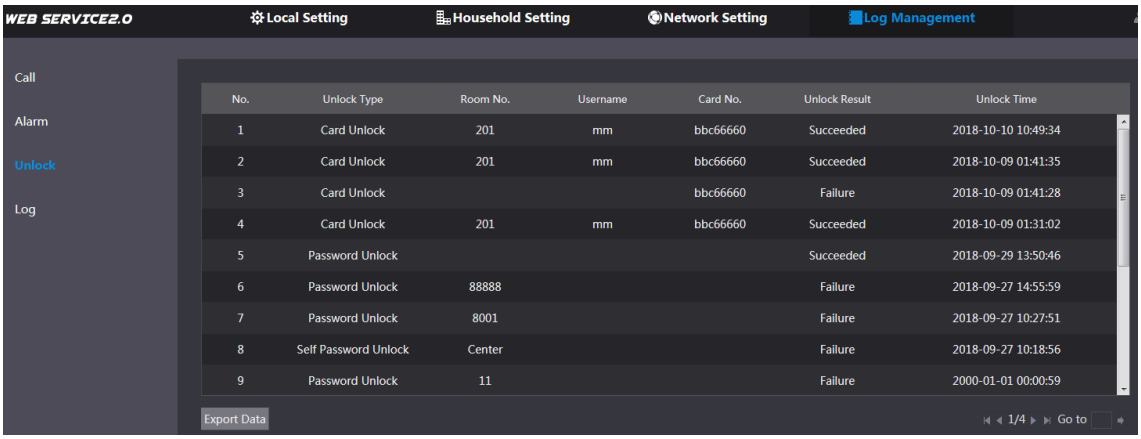
Fase 2: Fare clic su **Esporta dati** (Export Data) per esportare le registrazioni sul proprio PC.

7.3 Sblocco

È possibile visualizzare le registrazioni di sblocco, compresi quelli con scheda di accesso, password, sblocchi remoti e con pressione del pulsante.

Fase 1: Selezionare **Gestione registri > Sblocchi** (Log Management > Unlock).

Figura 7-3 Sblocco



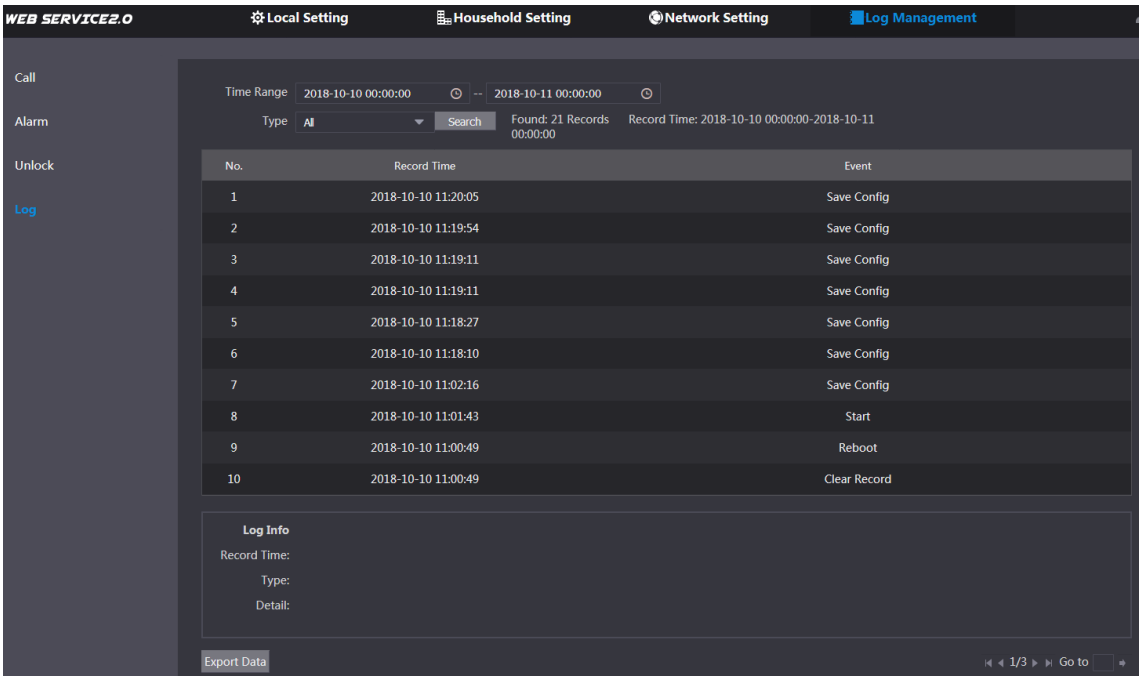
Fase 2: Fare clic su **Esporta dati** (Export Data) per esportare le registrazioni sul proprio PC.

7.4 Log

È possibile visualizzare vari registri di sistema, comprendenti informazioni di sistema, registrazioni, configurazioni, account e di sicurezza.

Fase 1: Selezionare **Gestione registri > Registri** (Log Management > Log).

Figura 7-4 Log



Fase 2: Configurare gli intervalli di tempo, selezionare i tipi di registri richiesti e poi fare clic su **Ricerca** (Search).

Fase 3: Fare clic su **Esporta dati** (Export Data) per esportare le registrazioni sul proprio PC.

Appendice 1 Suggerimenti in materia di sicurezza informatica

La sicurezza informatica non è solamente una parola di moda: è qualcosa che ha a che fare con tutti i dispositivi collegati a Internet. La sorveglianza video IP non è immune ai rischi informatici, ma adottare semplici misure di protezione e rafforzamento delle reti e dei dispositivi di rete rende questi ultimi meno suscettibili agli attacchi. Di seguito sono forniti alcuni consigli e raccomandazioni su come creare un sistema di sorveglianza più sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di rete di base dei dispositivi:

1. **Utilizzare password sicure**

   Seguire queste raccomandazioni quando si impostano le password:

   - la lunghezza non deve essere inferiore a 8 caratteri;
   - utilizzare almeno due tipi di caratteri diversi scelti fra lettere maiuscole e minuscole, numeri e simboli;
   - le password non devono contenere il nome dell'account o il nome dell'account al contrario;
   - non utilizzare caratteri in sequenza, come 123, abc ecc.;
   - non utilizzare caratteri ripetuti, come 111, aaa ecc.;

2. **Aggiornare il firmware e il software del client regolarmente**

   - Per assicurare che il sistema sia sempre protetto dalle patch e dagli aggiornamenti di sicurezza più recenti, è consigliabile mantenere aggiornati i firmware dei propri dispositivi (come NVR, DVR, telecamere IP ecc), come previsto dagli standard del settore tecnologico. Quando i dispositivi sono collegati a una rete pubblica, è consigliabile attivare la funzione Verifica automaticamente la presenza di aggiornamenti (auto-check for updates) per ottenere informazioni regolari sugli aggiornamenti del firmware rilasciati dai produttori.
   - È consigliabile scaricare e utilizzare l'ultima versione del software del client.

Raccomandazioni facoltative ma consigliate per migliorare la sicurezza di rete dei dispositivi:

1. **Protezione fisica**

   È consigliabile proteggere fisicamente le apparecchiature, specialmente i dispositivi di archiviazione. Ad esempio, posizionare le apparecchiature all'interno di un armadio in una stanza dei computer e implementare misure per il controllo degli accessi e la gestione delle chiavi adatte a evitare che il personale non autorizzato possa danneggiare l'hardware, collegare senza permesso dispositivi rimovibili (come chiavette USB e porte seriali) ecc.

2. **Modificare le password con regolarità**

   È consigliabile modificare le password regolarmente per ridurre il rischio che vengano scoperte o violate.

3. **Impostare e aggiornare tempestivamente le informazioni per il ripristino delle password**

   Il dispositivo supporta la funzione di ripristino della password. Configurare per tempo le informazioni relative al ripristino della password, compreso l'indirizzo e-mail dell'utente finale e le domande di sicurezza. Se le informazioni cambiano, modificarle tempestivamente. Quando si impostano le domande di sicurezza per il ripristino della password, è consigliabile non utilizzare domande le cui risposte possono essere facilmente indovinate.

4. **Attivare il blocco dell’account**

   La funzione di blocco dell’account è attiva per impostazione predefinita ed è consigliabile non disattivarla per garantire la sicurezza dell’account. Se un malintenzionato cerca di accedere ripetutamente con una password errata, l’account corrispondente e l’indirizzo IP utilizzato verranno bloccati.

5. **Modificare i valori predefiniti delle porte HTTP e relative agli altri servizi**

   Per ridurre il rischio che venga scoperto il numero di porta utilizzato, è consigliabile modificare i valori predefiniti delle porte HTTP e relative agli altri servizi scegliendo una qualsiasi combinazione di numeri compresa fra 1024 e 65535.

6. **Attivare il protocollo HTTPS**

   È consigliabile attivare il protocollo HTTPS, così da poter accedere al servizio web tramite un canale di comunicazione sicuro.

7. **Attivare la whitelist**

   È consigliabile attivare la whitelist per consentire l’accesso al sistema solo dagli indirizzi IP specificati. Pertanto, assicurarsi di aggiungere alla whitelist l’indirizzo IP del proprio computer e dei propri dispositivi.

8. **Associare l’indirizzo MAC**

   È consigliabile associare gli indirizzi IP e MAC del gateway alle apparecchiature per ridurre il rischio di spoofing ARP.

9. **Assegnare account e autorizzazioni in modo ragionevole**

   Aggiungere gli utenti con ragionevolezza e assegnare loro il minimo set di permessi in base alle esigenze lavorative e di gestione.

10. **Disattivare i servizi non necessari e scegliere modalità sicure**

    Per ridurre i rischi, è consigliabile disattivare servizi come SNMP, SMTP, UPnP ecc quando non sono necessari.

    Se sono necessari, è vivamente consigliato utilizzare le modalità sicure per i servizi che seguono (l’elenco non è esaustivo):

    - SNMP: scegliere SNMPv3 e impostare password crittografiche e di autenticazione sicure.
    - SMTP: scegliere TLS per accedere al server e-mail.
    - FTP: scegliere SFTP e impostare password sicure.
    - Hotspot AP: scegliere la crittografia WPA2-PSK e impostare password sicure.

11. **Utilizzare la trasmissione crittografata di audio e video**

    Se i contenuti audio e video sono molto importanti o sensibili, è consigliabili utilizzare la funzione di trasmissione crittografata per ridurre il rischio che i dati vengano rubati.

    Nota: la trasmissione crittografata rende la trasmissione meno efficiente.

12. **Verifiche di sicurezza**

    - Verifica degli utenti online: è consigliabile verificare regolarmente gli utenti online per vedere se qualcuno ha eseguito l’accesso al dispositivo senza autorizzazione.
    - Verifica dei registri delle apparecchiature: controllando i registri, è possibile conoscere gli indirizzi IP utilizzati per accedere ai propri dispositivi e alle operazioni chiave.

13. **Registro di rete**

    A causa della limitata capacità di archiviazione delle apparecchiature, il registro salvato è limitato. Se è necessario archiviare il registro per un tempo maggiore, è consigliabile attivare il registro di rete per assicurarsi che i registri critici siano sincronizzati con il server del registro di rete, garantendo una tracciatura efficiente.

14. Costruire un ambiente di rete sicuro

Per garantire la sicurezza delle apparecchiature e ridurre i rischi informatici potenziali, è consigliabile:

- disattivare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da una rete esterna;
- la rete deve essere suddivisa e isolata in base alle effettive esigenze di rete. in assenza di requisiti di comunicazione fra due sottoreti, è consigliabile utilizzare tecnologie come VLAN, GAP e altre per suddividere la rete e isolarla.
- Utilizzare il sistema di autenticazione degli accessi 802.1x per ridurre il rischio di accessi non autorizzati alle reti private.

Hiltron Land S.r.l.
Strada provinciale di Caserta, 218 - 80144 Napoli
Tel: (+39)081 185 39 000 Fax: (+39)081 185 39 016
www.hiltronsecurity.it