Riconoscimento facciale digitale
Postazione esterna

Guida rapida

V1.0.0

Introduzione

Generale

Questo manuale descrive la struttura, il processo di montaggio e la configurazione di base del dispositivo.

Modello

VTO7541G e VTO7521G

- VTO7541G: Dotato di funzioni di sblocco tramite volto, impronte digitali e schede.
- VTO7521G: Supporta solo lo sblocco tramite scheda.

Istruzioni di aggiornamento

Durante l'aggiornamento, tenere l'alimentazione attiva fino al termine del processo.

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.
NOTA	Fornisce informazioni aggiuntive che completano quelle riportate nel testo.

Cronologia delle revisioni

Versione	Contenuto della revisione	Data di rilascio
V1.0.0	Prima versione	Luglio 2019

Informativa sulla protezione della privacy

Gli utenti del dispositivo o gli analisti dei dati hanno la possibilità di raccogliere dati personali di terzi, quali volti, impronte digitali, numeri di targhe automobilistiche, indirizzi e-mail, numeri di telefono, dati GPS e simili. Gli utenti dei dispositivi devono rispettare norme e leggi locali di protezione della privacy per garantire il rispetto di diritti e interessi legittimi degli altri. A questo scopo, occorre adottare le seguenti misure, elencate a titolo esemplificativo e non esaustivo: Fornire segnali di identificazione chiari e ben visibili per informare i soggetti interessati dell'esistenza di un impianto di sorveglianza nell'area, fornendo i relativi contatti.

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 deve essere aggiornato sulla base delle più recenti leggi e normative in vigore nelle regioni interessate. Per informazioni dettagliate, consultare il manuale in formato cartaceo, CD-ROM o disponibile scansionando il codice QR o accedendo 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 incoerenze o incertezze, fare riferimento alla nostra spiegazione 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 durante l'utilizzo del dispositivo, è possibile consultare il nostro sito web o contattare il fornitore o il servizio di assistenza al cliente.
- In caso di incertezze o controversie, fare riferimento alla spiegazione 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 strettamente al 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 Panoramica

1.1 Introduzione

Il presente sistema digitale di riconoscimento facciale per esterni (nel seguito definito "VTO") può essere connesso a monitor interni (VTH), a postazioni master di videocitofoni (VTS) o a server di terzi per realizzare un impianto di videocitofoni.

I dispositivi VTO supportano funzioni di sblocco tramite volto, impronte digitali e schede. Il sistema supporta anche altre funzionalità, quali chiamate di emergenza, pubblicazione di informazioni e consultazione della cronologia.

1.2 Caratteristiche

- Chiamate audio/video: Dai VTO è possibile effettuare chiamate audio/video agli utenti con dispositivi VTS e VTH.
- Chiamate di gruppo: Da una singola unità VTO è possibile chiamare più utenti VTH allo stesso tempo.
- Video sorveglianza: Il sistema permette di monitorare aree adiacenti al VTO dal dispositivo VTH e dal centro di gestione.
- Chiamate di emergenza: Premere il tasto per chiamare il centro di controllo in caso di emergenza.
- Istantanee automatiche: È possibile scattare delle istantanee automaticamente quando il sistema è sbloccato o durante una chiamata e memorizzarle nell'FTP.
- Allarme: Il sistema supporta vari tipi di allarme, quali allarmi antimanomissione e di contatti porte. Dopo l'attivazione di un allarme, esso sarà segnalato al centro di gestione.
- Sblocco: sblocco tramite schede, impronte digitali, volti e da remoto.
- Pubblicazione di informazioni: Il dispositivo VTO è in grado di inviare messaggi a più dispositivi VTH.
- Visualizzazione cronologia: Il sistema permette di visualizzare le cronologie di chiamate, allarmi e delle procedure di sblocco.

2 Aspetto

Figura 2-1 Dimensioni (mm [pollici])

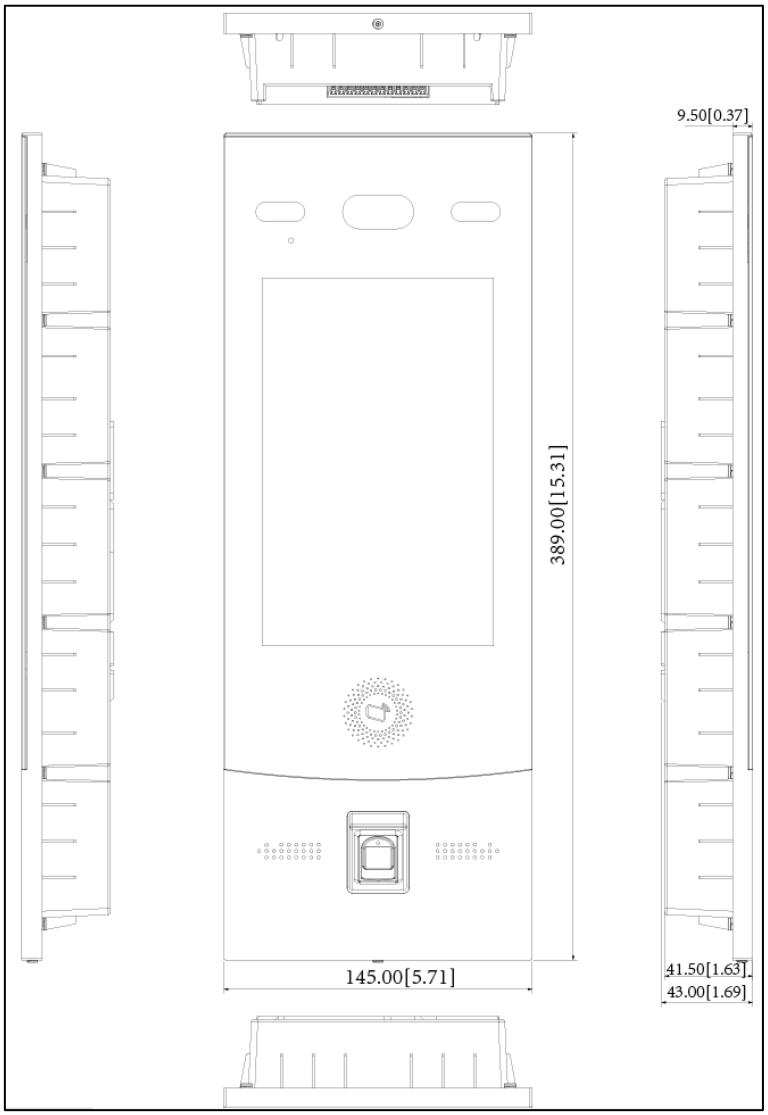


Figura 2-2 Componenti

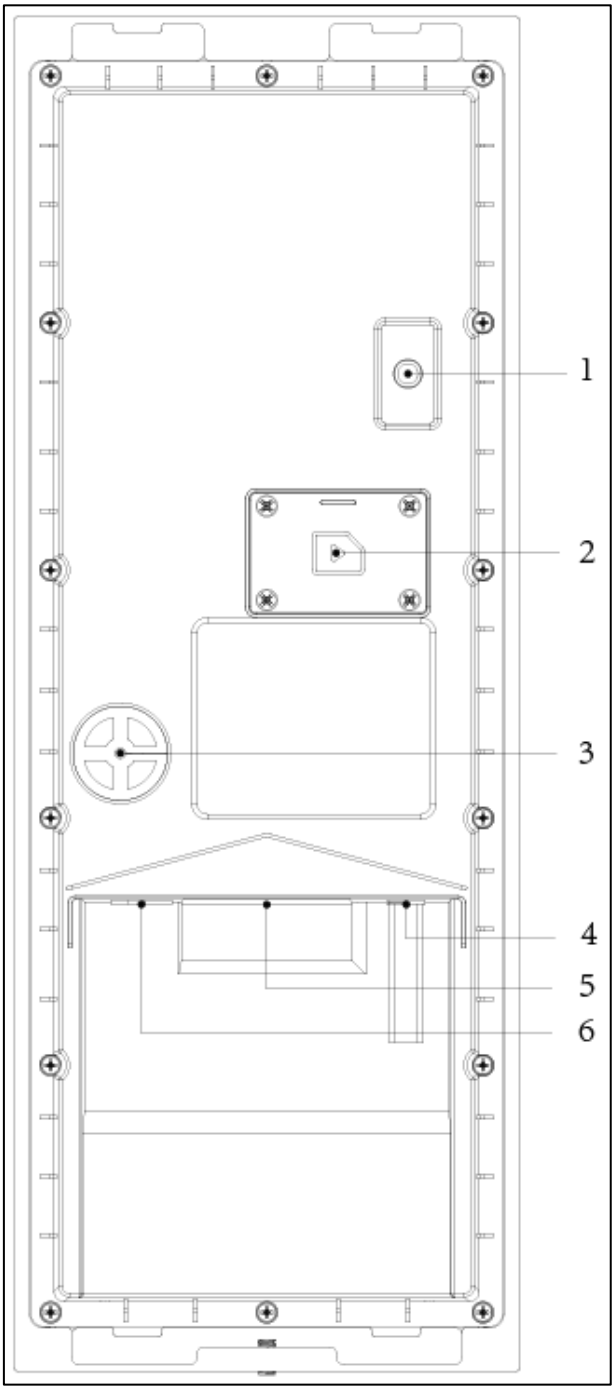


Tabella 2-1 Descrizione dei componenti

N.	Nome
1	Interruttore anti-manomissione
2	Copertura scheda SIM
3	Porta per antenna esterna 4G
4	Porta di alimentazione
5	Porte funzionali (ad esempio porte di ingresso e uscita allarmi, porte di serrature e interfacce Wiegand)
6	Porta Ethernet

3 Connessione cavi

Questa porta può essere usata per la connessione alle serrature delle porte e il metodo di connessione dipende dal tipo di serratura. Per informazioni dettagliate, consultare Figura 3-1 e Figura 3-2.

Figura 3-1 Connessione cavi (1)

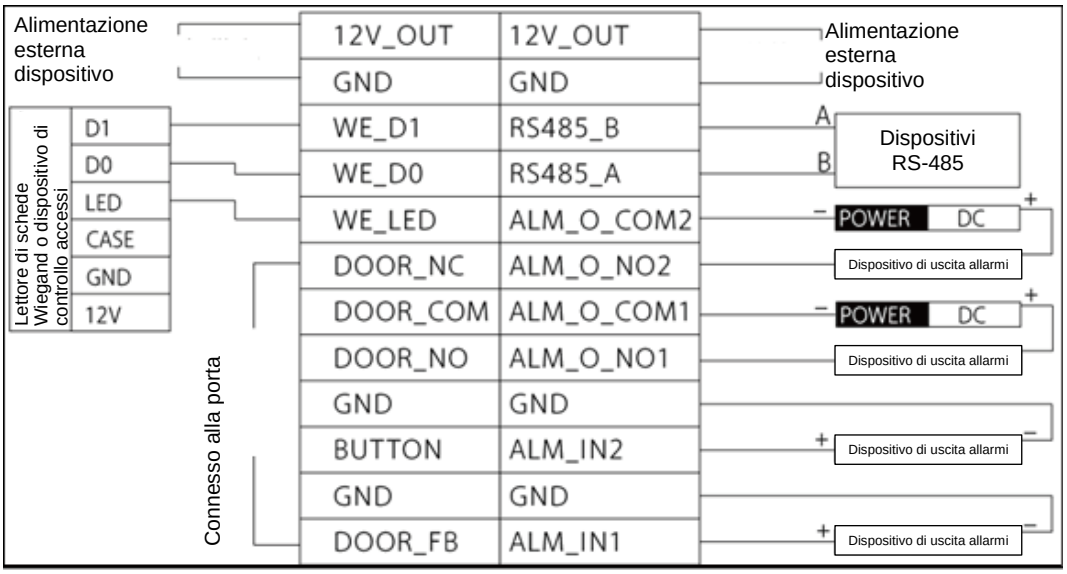
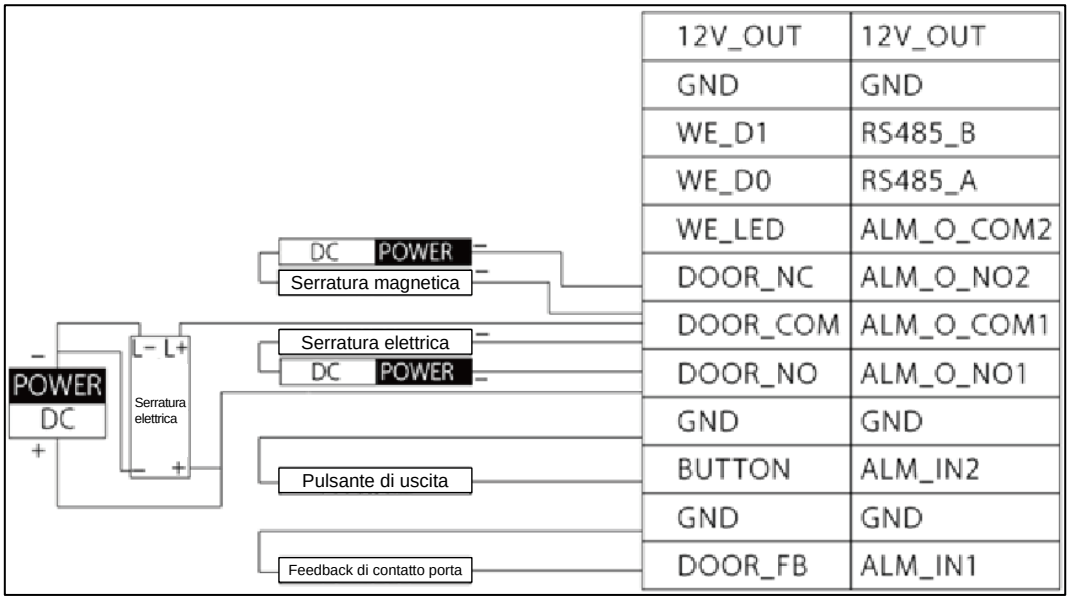


Figura 3-2 Connessione cavi (2)



4 Installazione

4.1 Requisiti di installazione

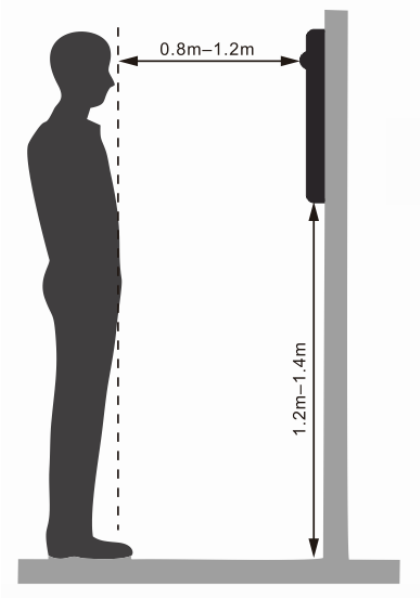
4.1.1 Note

- Non installare i dispositivi VTO in ambienti esposti a condensa, temperature elevate, grasso e polveri, agenti chimici corrosivi, luce solare diretta, o privi di copertura.
- L'installazione e la regolazione del dispositivo dovranno essere portati a termine da personale specializzato. Non provare a smontare da soli le unità VTO.

4.1.2 Linee guida

L'angolo di visualizzazione orizzontale dell'unità VTO può variare in base ai modelli. Cercare di posizionarsi quanto più vicino possibile al centro del dispositivo VTO. Consultare Figura 4-1 per la posizione di installazione.

Figura 4-1 Posizione di installazione



4.2 Installazione VTO

4.2.1 Installazione a parete

Figura 4-2 Installazione a parete

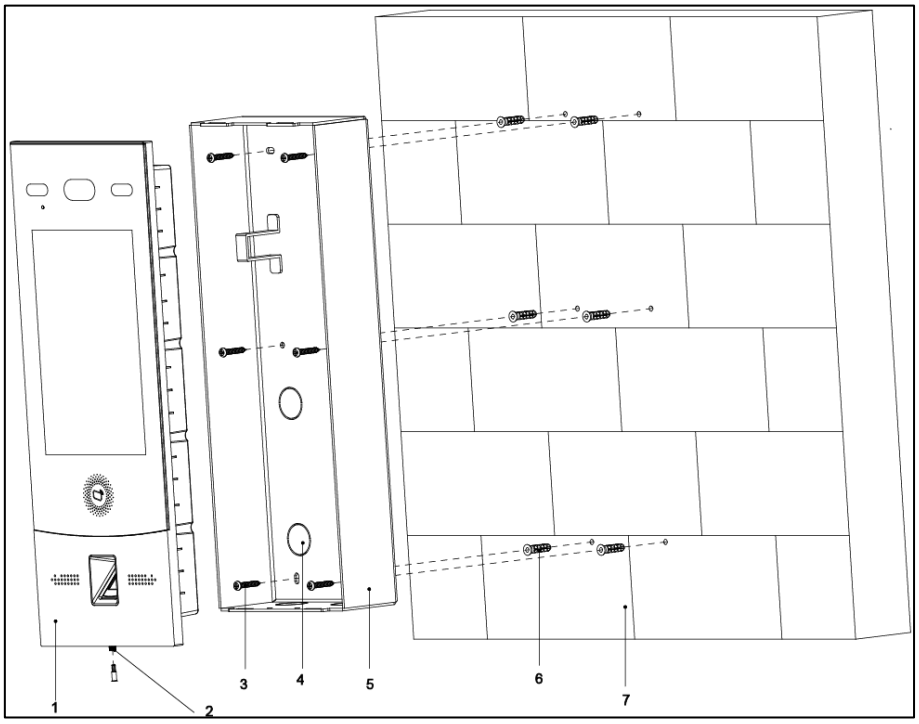


Tabella 4-1 Elenco di articoli

N.	Elemento	N.	Elemento	N.	Elemento	N.	Elemento
1	VTO	2	Vite di bloccaggio	3	viti 4 x 25	7	Parete
4	Ingresso cavo	5	Scatola di montaggio	6	Tassello di plastica	–	–

Fase 1: Praticare sulla parete dei fori in corrispondenza alla posizione dei fori sulla scatola di montaggio, quindi applicare i tasselli nei fori delle viti.

Fase 2: Fissare la scatola di montaggio alla parete con le viti ST 4.2 x 25.

Fase 3: Applicare del sigillante negli eventuali spazi vuoti tra la scatola di montaggio e la parete.

Fase 4: Connettere i cavi. Consultare i dettagli in "3 Connessione cavi."

Fase 5: Fissare il dispositivo VTO alla scatola di montaggio con le viti M4 x 30.

Fase 6: Stringere le viti di fissaggio nella parte inferiore del VTO per completare l'installazione.

4.2.2 Installazione a incasso

Figura 4-3 Installazione a incasso

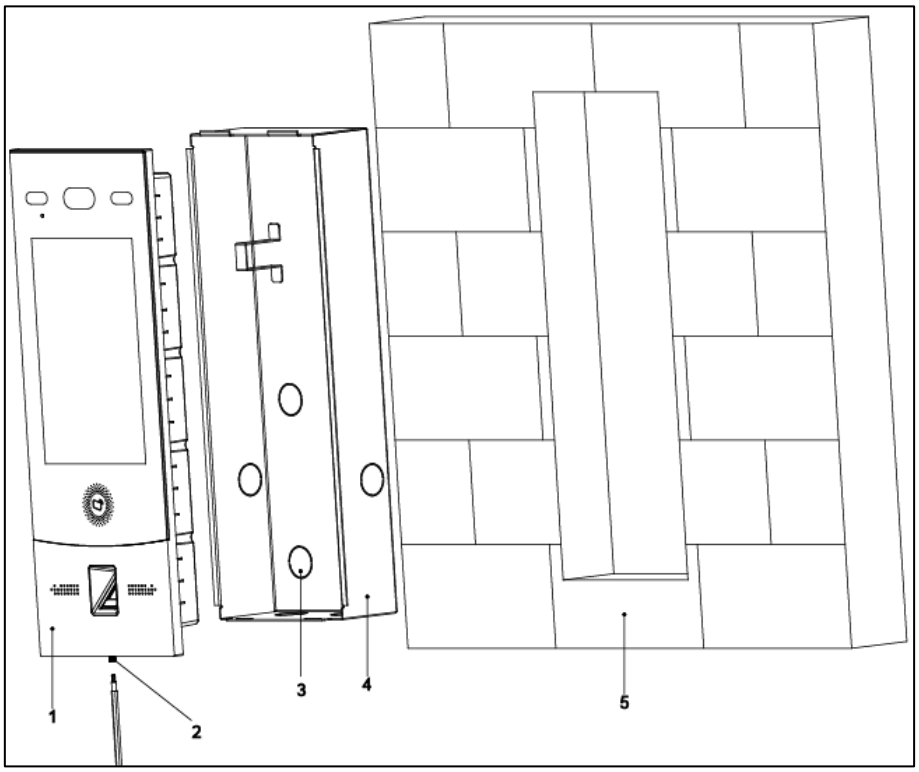


Tabella 4-2 Elenco di articoli

N.	Elemento	N.	Elemento	N.	Elemento
1	VTO	2	Vite di bloccaggio	3	Ingresso cavo
4	Scatola di montaggio	5	Parete	–	–

Fase 1: Ritagliare un'apertura delle dimensioni della scatola di montaggio sulla parete e quindi applicarvi la scatola.

Fase 2: Applicare del sigillante negli eventuali spazi vuoti tra la scatola di montaggio e la parete.

Fase 3: Connettere i cavi. Consultare i dettagli in "3 Connessione cavi."

Fase 4: Rimuovere la vite di fissaggio nella parte inferiore dell'unità VTO.

Fase 5: Fissare il dispositivo VTO alla scatola di montaggio con le viti M4 x 40.

Fase 6: Stringere le viti di fissaggio nella parte inferiore del VTO per completare l'installazione.

5 Configurazione

Questo capitolo descrive le procedure di inizializzazione, connessione e configurazioni primarie per i dispositivi VTO e VTH, allo scopo di implementare le funzioni base del sistema, quali gestione dispositivi, chiamate e operazioni di monitoraggio. Per maggiori informazioni sulla configurazione del sistema, consultare il manuale d'uso.

5.1 Processo di configurazione

Prima di procedere alla configurazione, controllare tutti i dispositivi e verificare che non ci siano corto circuiti o circuiti aperti.

Fase 1: Pianificare elementi di configurazione quali gli indirizzi IP di tutti i dispositivi e i numeri di unità residenziali e stanze richiesti dall'impianto.

Fase 2: Configurare il dispositivo VTO. Fare riferimento alla sezione 5.3 Configurazione del VTO.

1) Inizializzare il VTO. Fare riferimento alla sezione 5.3.1 Inizializzazione.
2) Configurare il numero del VTO. Fare riferimento alla sezione 5.3.2 Configurazione del numero del VTO.
3) Configurare i parametri di rete del VTO. Fare riferimento alla sezione 5.3.3 Configurazione dei parametri di rete.
4) Configurare il server SIP. Fare riferimento alla sezione 5.3.4 Scelta dei server SIP.
5) Aggiungere i dispositivi VTO al server SIP. Fare riferimento alla sezione 5.3.5 Aggiunta di dispositivi VTO..
6) Aggiungere i numero delle stanze al server SIP. Fare riferimento alla sezione 5.3.6 Aggiunta del numero di stanza.

Fase 3: Configurare il dispositivo VTH. Consultare il manuale d'uso del VTH.

Fase 4: Controllare la corretta configurazione. Fare riferimento alla sezione 6 Utilizzo del VTO.

5.2 VDPConfig

È possibile scaricare il software "VDPConfig" per eseguire l'inizializzazione dei dispositivi, la modifica degli indirizzi IP e l'aggiornamento di sistema per più dispositivi allo stesso tempo. Per maggiori informazioni, consultare il relativo manuale d'uso.

5.3 Configurazione del VTO

Collegare il dispositivo VTO al proprio PC con un cavo di rete, quindi al primo accesso creare una nuova password per l'interfaccia web.

5.3.1 Inizializzazione

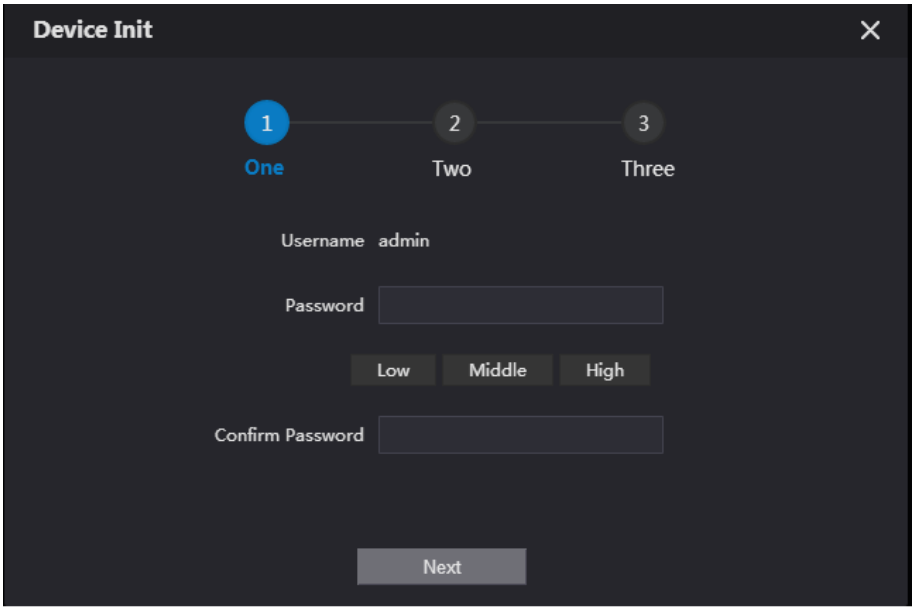
L'indirizzo IP predefinito del VTO è 192.168.1.110 e il PC connesso al sistema deve trovarsi nello stesso segmento di rete del VTO.

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

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

Il sistema mostra l'interfaccia **Inizializzazione dispositivi** (Device Init). Osservare la Figura 5-1.

Figura 5-1 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.

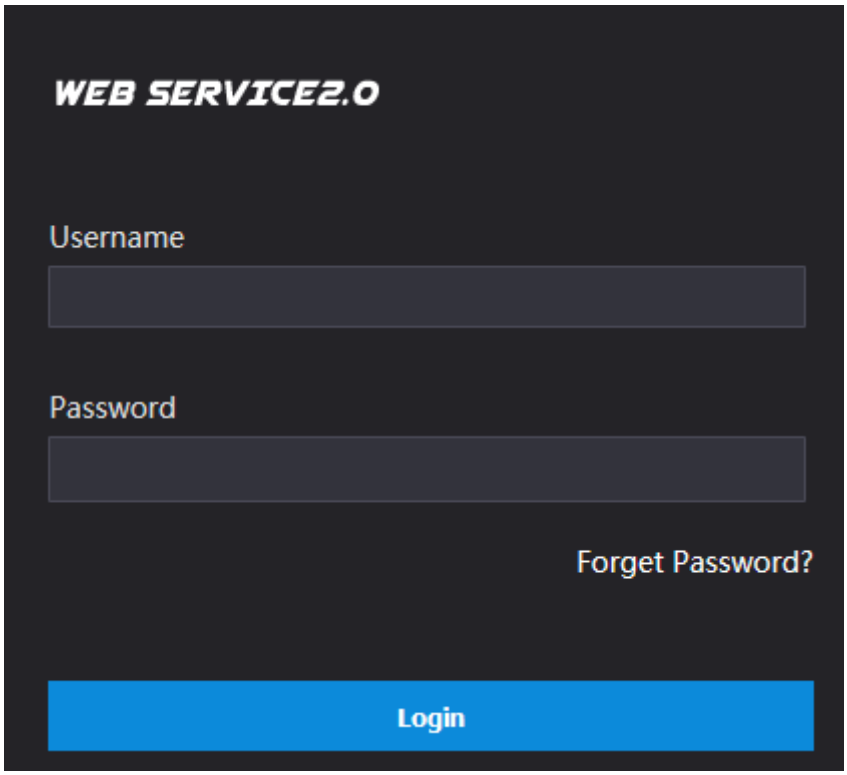
Fase 5: Fare clic su "**Avanti**" (Next).

L'inizializzazione è così terminata.

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

Il sistema mostra l'interfaccia di Accesso (Login). Osservare la Figura 5-2.

Figura 5-2 Interfaccia di accesso



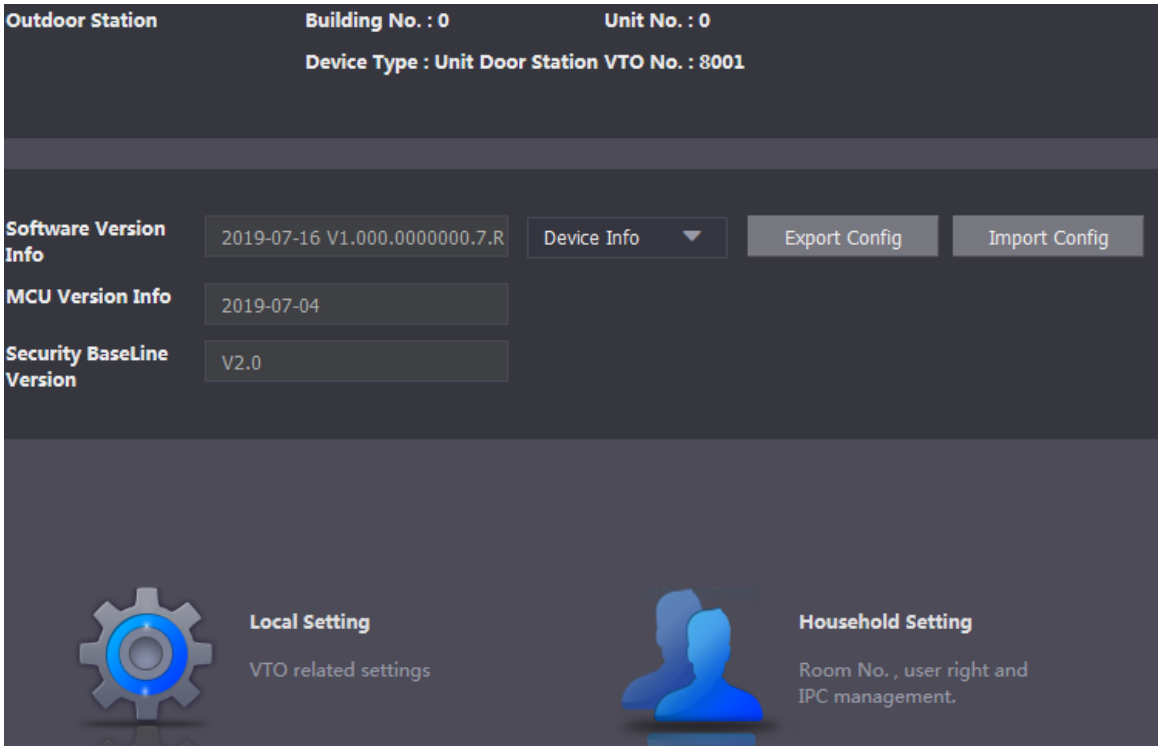
5.3.2 Configurazione del numero del VTO

Il numero di VTO può essere utilizzato per distinguere ciascuna unità VTO e di solito è definito in base al numero di edificio.

- È possibile modificare il numero di un VTO, quando esso non funge da server SIP.
- Il numero del VTO può contenere al massimo 5 cifre e deve essere diverso da quello di tutti i numeri di stanza.

Fase 1: Accedendo all'interfaccia web del VTO, il sistema mostra l'interfaccia principale. Osservare la Figura 5-3.

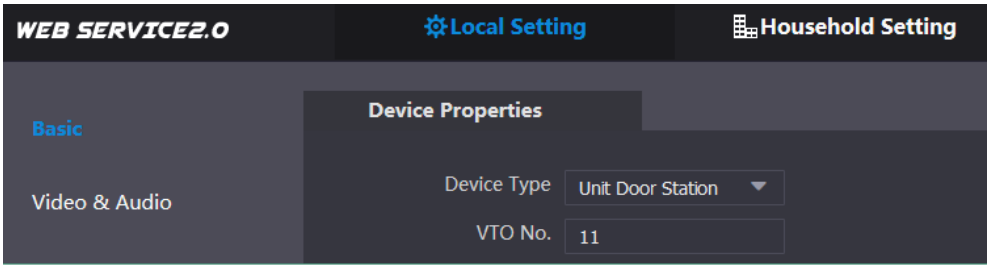
Figura 5-3 Interfaccia principale



Fase 2: Selezionare la voce Impostazioni Locali > Imp. base (Local Setting > Basic).

Il sistema mostra l'interfaccia **Proprietà dispositivi** (Device Properties). Osservare la Figura 5-4.

Figura 5-4 Proprietà dei dispositivi



Fase 3: Inserire nella casella di immissione **N. VTO**(VTO No.) il numero di VTO previsto per questo dispositivo e poi fare clic su **Conferma** (Confirm) per salvare l'impostazione.

5.3.3 Configurazione dei parametri di rete

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

Il sistema mostra le informazioni TCP/IP. Osservare la Figura 5-5.

Figura 5-5 Informazioni TCP/IP

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

Il sistema VTO si riavvia.

Assicurarsi che l'indirizzo IP del dispositivo VTO e del PC si trovino nello stesso segmento di rete.

5.3.4 Scelta dei server SIP

Il protocollo SIP (Session Initiation Protocol) gestisce le operazioni di segnalazione e controllo delle sessioni di comunicazione multimediale richieste per realizzare le chiamate audio e video. Un server SIP è un'applicazione che fornisce informazioni o istruzioni agli agenti utente.

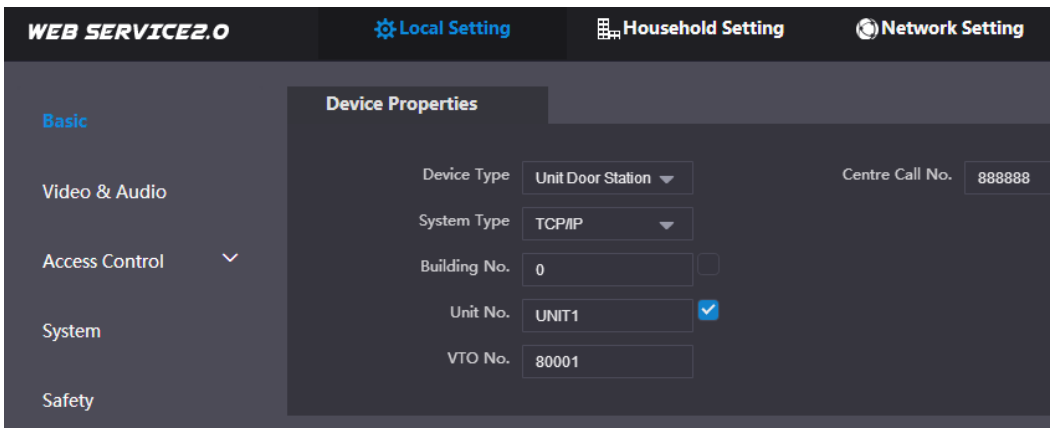
- Quando il dispositivo VTO in uso o altri fungono da server SIP, selezionare la voce **VTO** dall'elenco a discesa **Tipo server** (Server Type). Questa scelta si applica a uno scenario con un solo edificio.
- Quando la piattaforma (Express/DSS) funge da server SIP, selezionare la voce **Express/DSS** dall'elenco a discesa **Tipo server** (Server Type). Questa scelta si applica a uno scenario in cui ci sono più edifici o unità residenziali.

Fase 1: Accedere alla pagina web.

Fase 2: Nella pagina iniziale, selezionare **Impostazioni Locali > Imp. Base** (Local Setting > Basic).

Il sistema mostra l'interfaccia **Proprietà dispositivi** (Device Properties). Osservare la Figura 5-6.

Figura 5-6 Proprietà dei dispositivi



1) Selezionare la voce **TCP/IP** dall'elenco a discesa **Tipo sistema** (System Type).

Il tipo di sistema predefinito è quello analogico e va sostituito con quello TCP/IP. In caso contrario, la connessione del VTH non riuscirà.

2) Fare clic su **OK** per salvare le impostazioni.
3) Per rendere efficaci le impostazioni, riavviare il dispositivo manualmente o attendere il riavvio automatico.

Fase 3: Accedere di nuovo all'interfaccia web.

Fase 4: Selezionare la voce Impostazioni di **Rete > Server SIP** (Network Setting > SIP Server).

Il sistema mostra l'interfaccia **Server SIP** (SIP Server). Osservare la Figura 5-7.

Figura 5-7 Server SIP (1)

Fase 5: Selezionare un server SIP.

Unità VTO come server SIP

Fase 1: Selezionare la voce **Abilita** (Enable) dietro **Server SIP** (SIP Server).

Fase 2: Selezionare la voce **VTO** dall'elenco a discesa **Tipo Server** (Server Type).

Fase 3: Configurare i parametri (consultare Tabella 5-1per i dettagli).

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

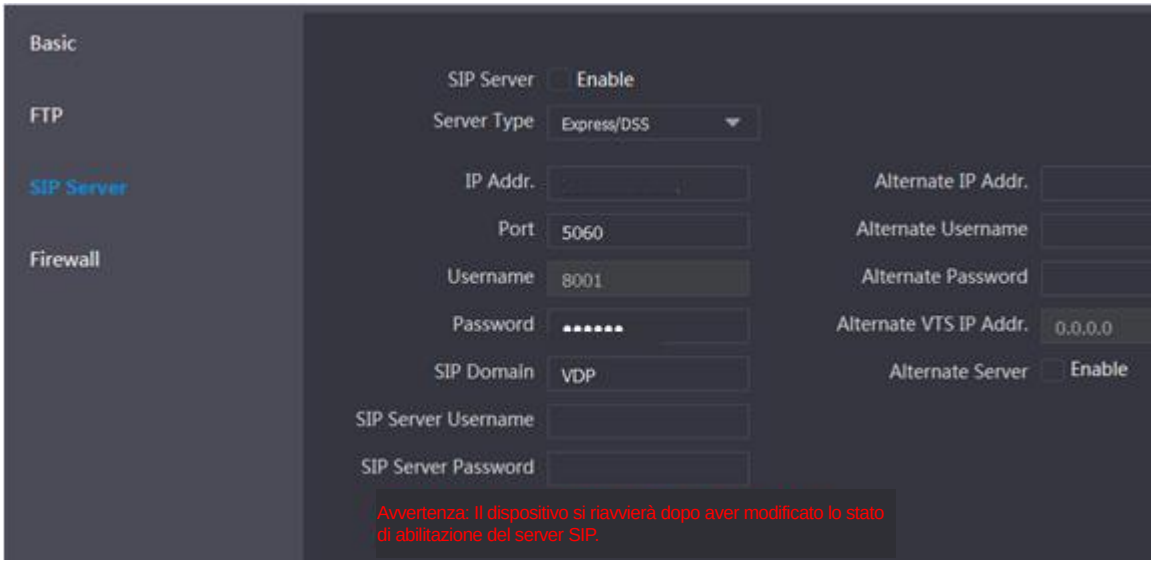
Il sistema VTO si riavvia automaticamente.

Piattaforma (Express/DSS) come server SIP

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

Il sistema mostra l'interfaccia **Server SIP** (SIP Server). Osservare la Figura 5-8.

Figura 5-8 Server SIP (2)



Fase 2: Selezionare la voce **Express/DSS** dall'elenco a discesa **Tipo Server** (Server Type).

Fase 3: Impostare i parametri come indicato in Tabella 5-1.

Tabella 5-1 Descrizione parametri del server SIP

Parametro	Descrizione
Indirizzo IP	Indirizzo IP del server SIP.
Porta	• Il valore predefinito è 5060 quando c'è un altro VTO che funge da server SIP. • Il valore predefinito è 5080 quando la piattaforma funge da server SIP.
Nome utente/password	Usare il valore predefinito.
Dominio SIP	• Dovrà essere VDP quando c'è un altro VTO che funge da server SIP. • Può essere vuoto o restare al valore predefinito quando la piattaforma funge da server SIP.
Nome utente e password di accesso	Nome utente e password per accedere al server SIP.
Indirizzo IP alternativo.	Indirizzo IP del server alternativo. Se l'opzione server alternativo è abilitata e la piattaforma Express o DSS funge da server SIP, ma non funziona normalmente, il dispositivo VTO fungerà da server SIP.
Nome utente alternativo	Nome utente e password per accedere al server alternativo.
Password alternativa	
Indirizzo IP del VTS alternativo.	Indirizzo IP per il VTS alternativo.
Server alternativo	Dopo aver inserito l'indirizzo IP, il nome utente, la password alternativi e l'indirizzo IP del VTS, occorre selezionare la casella di controllo **Abilita** (Enable) per attivare il server alternativo.

Fase 4: Fare clic su **OK** per salvare le impostazioni.

Il sistema VTO si riavvia automaticamente.

Quando la piattaforma funge da server SIP, se occorre definire il n. edificio e il n. unità residenziale, bisogna prima abilitare le opzioni **Supporto edifici** (Support Building) e **Supporto Unità** (Support Unit).

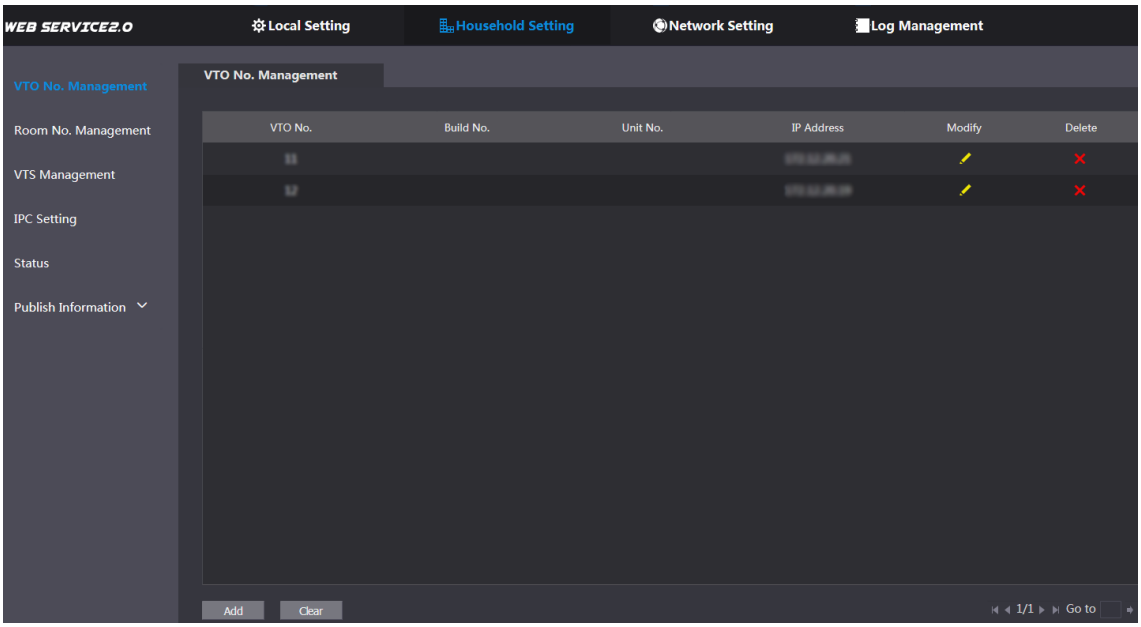
5.3.5 Aggiunta di dispositivi VTO.

Aggiungendo l'unità VTO al server SIP, tutti i citofoni connessi allo stesso server SIP potranno effettuare chiamate audio e video tra loro. La seguente sezione si applica al caso in cui il VTO funge da server SIP, per cui, se si utilizzano server SIP di altro tipo, occorre consultare il relativo manuale per i dettagli di configurazione.

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

Il sistema mostra l'interfaccia **Gestione n. VTO** (VTO No. Management). Osservare la Figura 5-9.

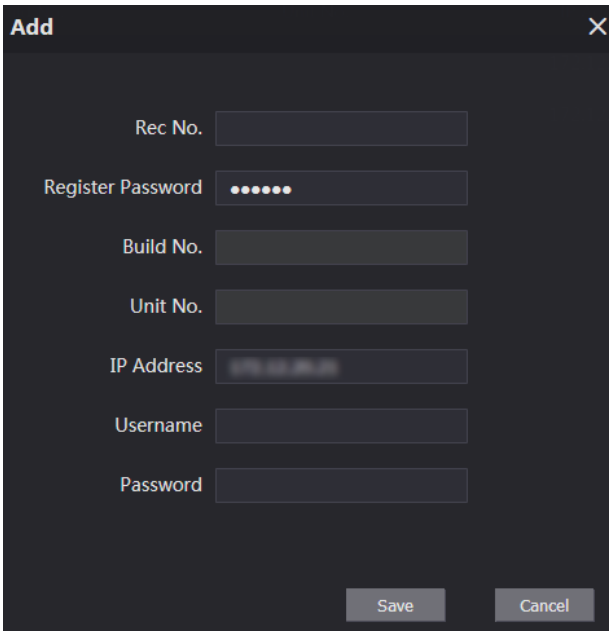
Figura 5-9 Gestione n. VTO



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

Il sistema mostra l'interfaccia **Aggiunta** (Add). Osservare la Figura 5-10.

Figura 5-10 Aggiunta VTO



Fase 3: Configurare i parametri, assicurandosi anche di aggiungere il server SIP stesso. Osservare la Tabella 5-2.

Tabella 5-2 Aggiunta della configurazione VTO

Parametro	Descrizione
N. Rec	Il numero di VTO configurato per il VTO di destinazione. Consultare i dettagli in "5.3.2 Configurazione del numero del VTO."
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).

5.3.6 Aggiunta del numero di stanza

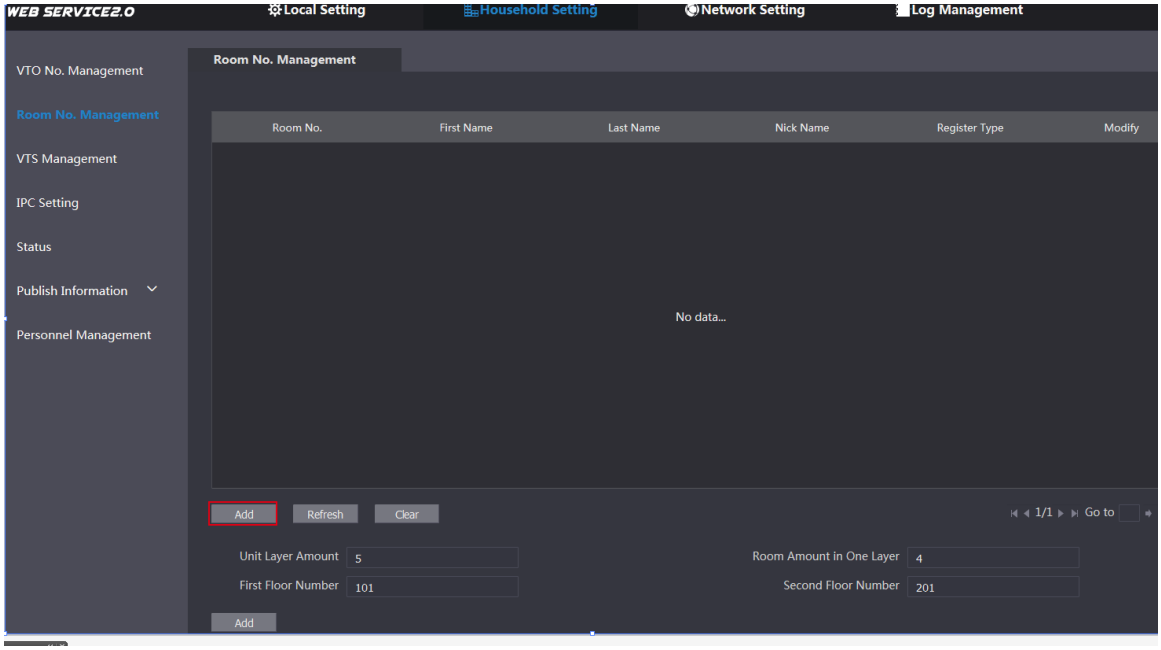
È possibile aggiungere al server SIP il numero di stanza previsto, per poi configurare il numero di stanza sui dispositivi VTH per connetterli alla rete. Nel seguito consideriamo il caso in cui il VTO funga da server SIP. Se l'utente fa uso di altri server SIP, consultare il manuale corrispondente per i dettagli.

Il numero di stanza può contenere al massimo 6 caratteri tra cifre e lettere o loro combinazioni e deve essere diverso dai numeri di tutti gli altri dispositivi VTO.

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

Il sistema mostra l'interfaccia **Gestione n. stanza** (Room No. Management). Osservare la Figura 5-11.

Figura 5-11 Gestione n. stanza

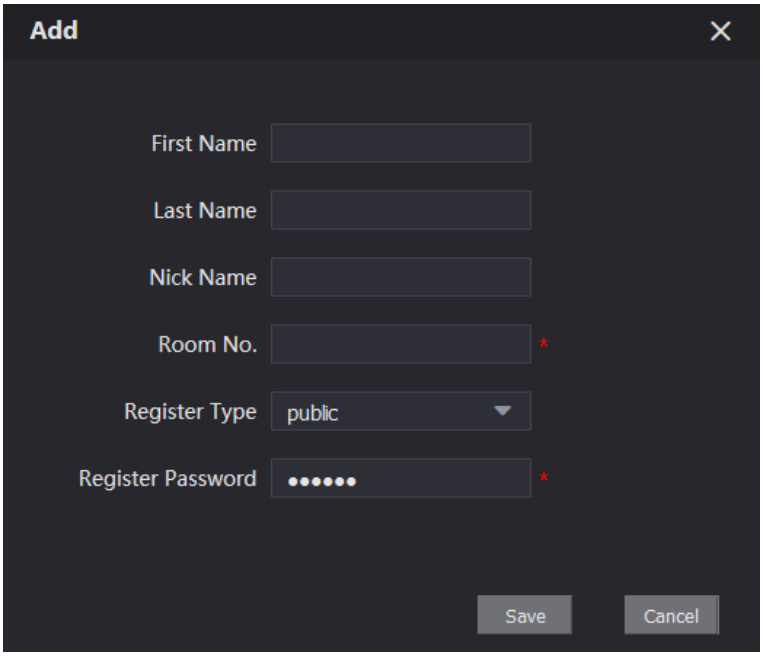


Fase 2: I numeri di stanza possono essere aggiunti singolarmente o in gruppi.

- Aggiunta di un numero di stanza singolo

1) Fare clic su **Aggiungi** (Add). Osservare la Figura 5-11.
   Il sistema mostra l'interfaccia **Aggiunta** (Add). Osservare la Figura 5-12.

Figura 5-12 Aggiunta di un numero di stanza singolo



2) Configurare le informazioni della stanza. Osservare la Tabella 5-3.

Tabella 5-3 Informazioni stanza

Parametro	Descrizione
Nome	Inserire le informazioni necessarie a distinguere le singole stanze.
Cognome	
Nome alternativo	

Parametro	Descrizione
N. stanza	Numero di stanza previsto. ● In caso di utilizzo di più dispositivi VTH, il numero di stanza corrispondente all'unità VTH master deve essere "numero stanza#0", mentre i numeri delle stanze corrispondenti ai VTH degli interni saranno "numero stanza#1", "numero stanza#2" ecc. ● È possibile avere un massimo di 10 dispositivi VTH di interni per ciascun VTH master.
Tipo di registrazione	Selezionare il valore **pubblico** (public), poiché **locale** (local) è riservato a usi futuri.
Password di registrazione	Usare il valore predefinito.

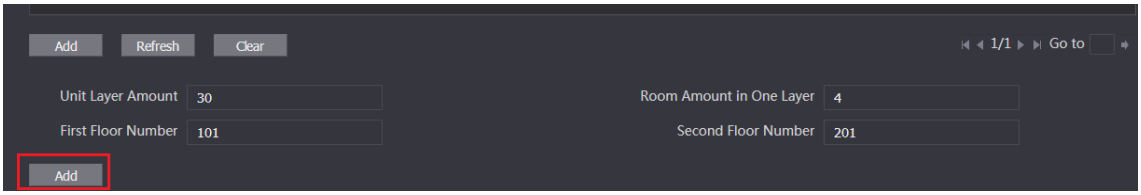
3) Fare clic su **Salva** (Save).

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) nell'angolo in basso a sinistra dell'interfaccia. Osservare la Figura 5-13.

Figura 5-13 Aggiunta in gruppo



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.

6 Utilizzo del VTO

6.1 Funzioni di chiamata

6.1.1 Chiamata con numero di stanza

Fase 1: In modalità standby, toccare  .

Il sistema mostra l'interfaccia di chiamata.

Fase 2: Inserire il numero di stanza e poi toccare **Chiama** (Call).

Si udrà un messaggio vocale che dice "Chiamata in corso, attendere (Calling now, please wait a moment)".

Fase 3: Per interrompere la chiamata in corso, toccare **Riaggancia** (Hangup).

6.1.2 Chiamata di contatti

Tutti i numeri di stanza aggiunti al server SIP sono mostrati tra i contatti del VTO.

Fase 1: In modalità standby, toccare **Rubrica** (PhoneBook) per visualizzare i contatti.

Fase 2: Selezionare il contatto da chiamare e toccare **Chiama** (Call).

6.2 Modalità progetto

La modalità progetto può essere utilizzata dagli amministratori di sistema per applicare configurazioni avanzate al VTO, quali emissione di schede di accesso, modifica degli indirizzi IP dei dispositivi e aggiunta di numeri di stanze.

6.2.1 Accesso alla modalità progetto

Toccare **Chiama** (Call) sull'interfaccia di standby, quindi immettere "*+password di progetto+#" per accedere alla modalità di progetto. La password di progetto predefinita è 888888; essa può essere modificata sull'unità VTO oppure sull'interfaccia web del VTO.

6.2.2 Modifica dell'indirizzo IP

Fase 1: In modalità progetto, selezionare **Configurazione IP** (IP Config).

Fase 2: Inserire l'indirizzo IP richiesto.

Fase 3: Toccare **OK** per salvare il nuovo indirizzo IP, oppure toccare **Annulla** (Cancel) per annullare la modifica.

6.2.3 Registrazione dell'utente

Solo gli utenti registrati possono sbloccare le porte, per cui gli utenti devono registrarsi.

Fase 1: Sull'interfaccia Modalità Progetto (Project Mode), selezionare **Registrazione utenti** (User Registration).

Il sistema mostra l'interfaccia di **Registrazione utenti** (User Registration).

Fase 2: Toccare  .

Il sistema mostra l'interfaccia di inserimento informazioni utenti (enter user information).

Fase 3: Inserire n. di personale, n. di stanza e nome utente.

Fase 4: Toccare **OK** per salvare le informazioni inserite.

Fase 5: Toccare  per scattare una foto all'utente.

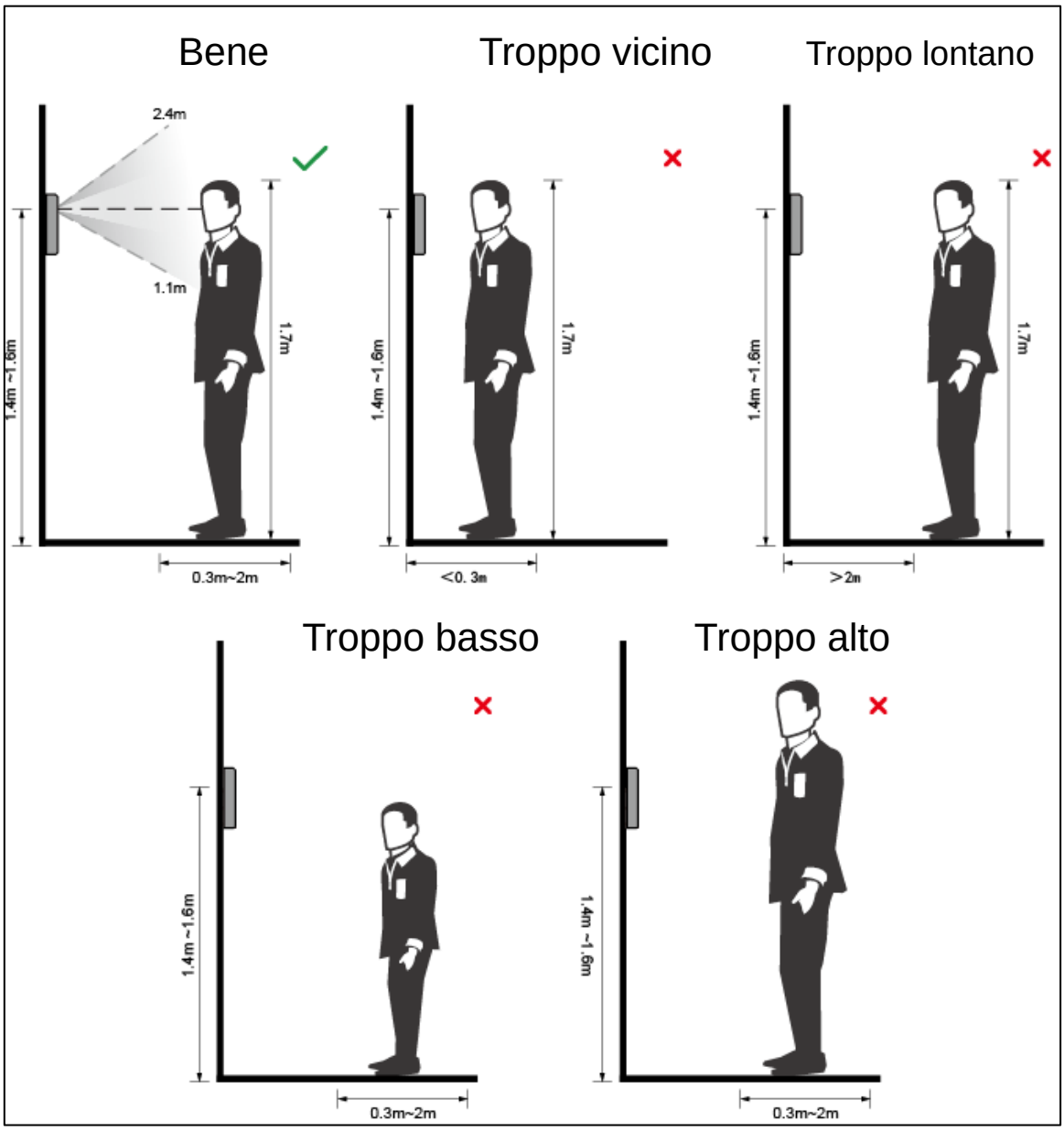
Fase 6: Toccare **OK** per salvare la foto, quindi il sistema passa all'interfaccia **Registrazione utente** (User Registration); oppure toccare **Annulla** (Cancel) per scattare una nuova foto.

Appendice 1 Note sulla registrazione dei volti

Posizione facciale

Se i volti non si trovano nella giusta posizione, il riconoscimento facciale potrebbe esserne compromesso.

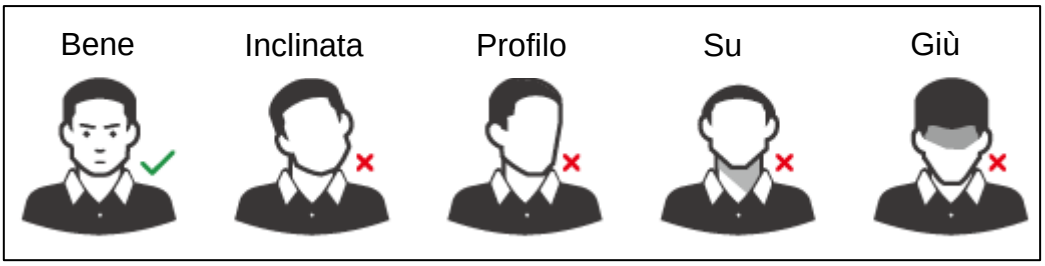
Appendice Figura 1-1 Corretta posizione facciale



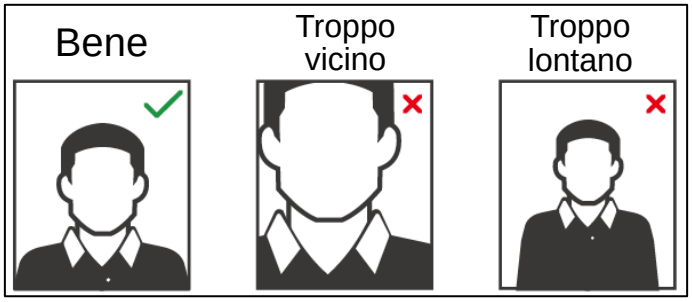
Requisiti sui volti

- Assicurarsi che il volto sia pulito, rivolto in avanti e non coperto dai capelli.
- Non indossare occhiali, cappelli, non portare la barba lunga, né altri accessori facciali che potrebbero compromettere la registrazione dell'immagine facciale.
- Sistemare il proprio volto in posizione centrale di fronte alla fotocamera, con gli occhi ben aperti e senza espressioni facciali particolari.
- Durante la registrazione o il riconoscimento facciale, non avvicinare o allontanare troppo il viso dalla fotocamera.

Appendice Figura 1-2 Posizione della testa



Appendice Figura 1-3 Distanza del volto



- Durante l'importazione di immagini facciali tramite la piattaforma di gestione, verificare che: la risoluzione dell'immagine sia compresa nell'intervallo 150×300–600×1200; i pixel dell'immagine siano più di 500x500; la dimensione dell'immagine sia minore di 100 Kb e il nome dell'immagine coincida con l'identificativo della persona.
- Verificare che il volto non superi i 2/3 dell'area dell'intera immagine e che le proporzioni non superino 1:2.

Appendice 2 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.