HILTRON
security

Unità VTH

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

V1.0.0

Prefazione

Generale

Questo documento introduce principalmente la struttura, l'installazione e la messa in servizio del prodotto.

Istruzioni di sicurezza

Nel manuale potrebbero apparire le seguenti parole di segnalazione classificate con un significato definito.

Avvertenze	Significato
 **PERICOLO**	Indica un rischio potenziale elevato che, se non evitato, provocherà la morte o lesioni gravi.
 **AVVERTIMENTO**	Indica un rischio potenziale medio o basso che, se non evitato, potrebbe causare lesioni lievi o moderate.
 **ATTENZIONE**	Indica un potenziale rischio che, se non evitato, potrebbe causare danni alla proprietà, perdita di dati, prestazioni inferiori o imprevedibilità risultato.
 CONSIGLI	Fornisce metodi per aiutarti a risolvere un problema o farti risparmiare tempo.
 **NOTA**	Fornisce ulteriori informazioni come l'enfasi e il supplemento al testo.

Cronologia delle revisioni

Versione	Contenuto di revisione	Data di rilascio
V1.0.0	Prima uscita.	Settembre 2020

A proposito del manuale

- Il manuale è solo di riferimento. Se c'è incoerenza tra il manuale e l'effettivo prodotto, prevale il prodotto reale.

- Non siamo responsabili per eventuali perdite causate da operazioni non conformi al manuale. - Il manuale verrebbe aggiornato in base alle ultime leggi e normative delle giurisdizioni correlate.

- Tutti i design e il software sono soggetti a modifiche senza preavviso scritto. Gli aggiornamenti del prodotto potrebbero causare alcune differenze tra il prodotto reale e il manuale. Si prega di contattare il servizio clienti per il programma più recente e la documentazione supplementare.
- Potrebbero esserci ancora deviazioni nei dati tecnici, nelle funzioni e nella descrizione delle operazioni o errori di Stampa. In caso di dubbi o controversie, ci riserviamo il diritto di una spiegazione finale.

- Aggiorna il software del lettore o prova un altro software di lettura tradizionale se il manuale (in PDF formato) non può essere aperto.
- In caso di incertezza o controversia, ci riserviamo il diritto di una spiegazione finale.

Importanti misure di salvaguardia e avvertenze

La seguente descrizione è il metodo di applicazione corretto del dispositivo. Si prega di leggere il manuale accuratamente prima dell'uso, al fine di prevenire pericoli e perdite di cose. Rispettare rigorosamente il manuale durante l'applicazione e conservarlo correttamente dopo la lettura.

Requisiti operativi

- Non esporre il dispositivo alla luce solare diretta oa fonti di calore.
- Non installare il dispositivo in un'area umida o polverosa.
- Installare il dispositivo orizzontalmente in luoghi stabili per evitare che cada.
- Non gocciolare o spruzzare liquidi sul dispositivo; non mettere sul dispositivo oggetti pieni di liquidi.
- Installare il dispositivo in luoghi ben ventilati e non ostruire la sua apertura di ventilazione.
- Utilizzare il dispositivo solo entro l'intervallo di ingresso e uscita nominale.
- Non smontare il dispositivo da soli.
- Il dispositivo deve essere utilizzato con cavi di rete schermati.

Requisiti di alimentazione

- Utilizzare i cavi di alimentazione consigliati nella regione in base alle specifiche nominali.
- Utilizzare un alimentatore che soddisfi i requisiti SELV (safety extra low voltage) e fornire un'alimentazione con tensione nominale conforme a Limited Power Source in IEC60950-1. Per i requisiti di alimentazione specifici, fare riferimento alle etichette del dispositivo.
- L'accoppiatore dell'apparecchio è un dispositivo di disconnessione. Durante il normale utilizzo, mantenere un angolo che faciliti il funzionamento.

Aggiornamento dispositivo

Non interrompere l'alimentazione durante l'aggiornamento del dispositivo. L'alimentazione può essere interrotta solo dopo che il dispositivo ha completato l'aggiornamento e si è riavviato.

Sommario

1 Struttura

1.1 Pannello frontale

Diversi modelli di dispositivi possono avere diverse dimensioni del pannello frontale e tipi di chiavi, ma chiavi o gli indicatori con lo stesso nome o icona hanno la stessa funzione.

Tabella 1-1 Descrizione del pannello frontale

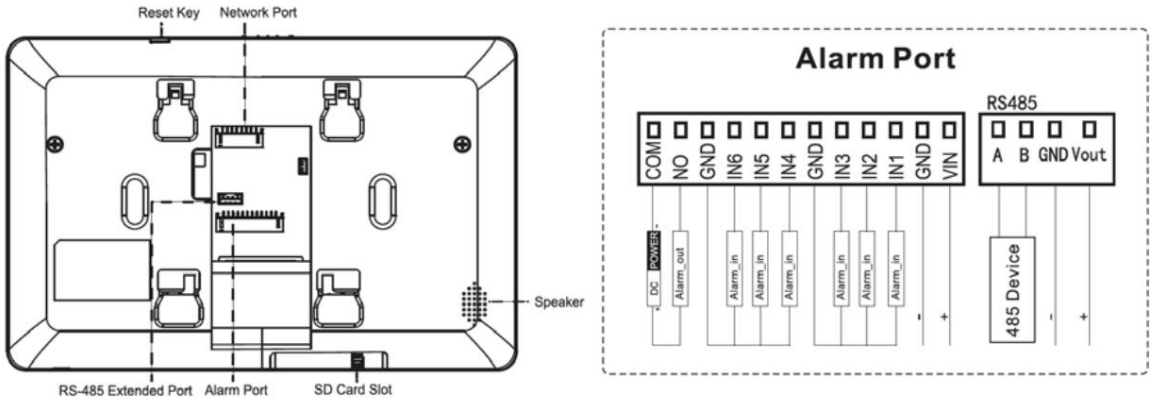
Icona	Nome	Descrizione
	sos	Chiamata d'emergenza.
	Menù	Vai al menu principale.
	Chiamata	• Rispondi alla chiamata. • Durante la chiamata, premere per riagganciare su. • Durante il monitoraggio, premere per parlare con l'unità VTO, villa VTO, stazione di recinzione e verifica VTO. • Durante la conversazione, premere per uscire dalla conversazione.
	Tenere sotto controllo	• In modalità standby, premere per monitorare il VTO principale. • Durante il monitoraggio, premere per uscire dal monitoraggio.
	Sbloccare	Quando si chiama, si parla, si monitora e si parla con VTO, premere per sbloccare il VTO corrispondente.
	Messaggio	Se è acceso, ci sono non letti messaggi.
	Potenza	Se è verde, lo è l'alimentatore normale.
Rete	Rete	• Se è acceso, la comunicazione con VTO è normale. • Se è spento, non puoi parlare all'OMC.
DND	DND	Se diventa verde, la funzione DND è abilitata.  Fare riferimento al manuale utente per Impostazioni DND eseguendo la scansione di Codice QR sulla copertina.

1.2 Porta del pannello posteriore

1.2.1 Serie VIS7PIW

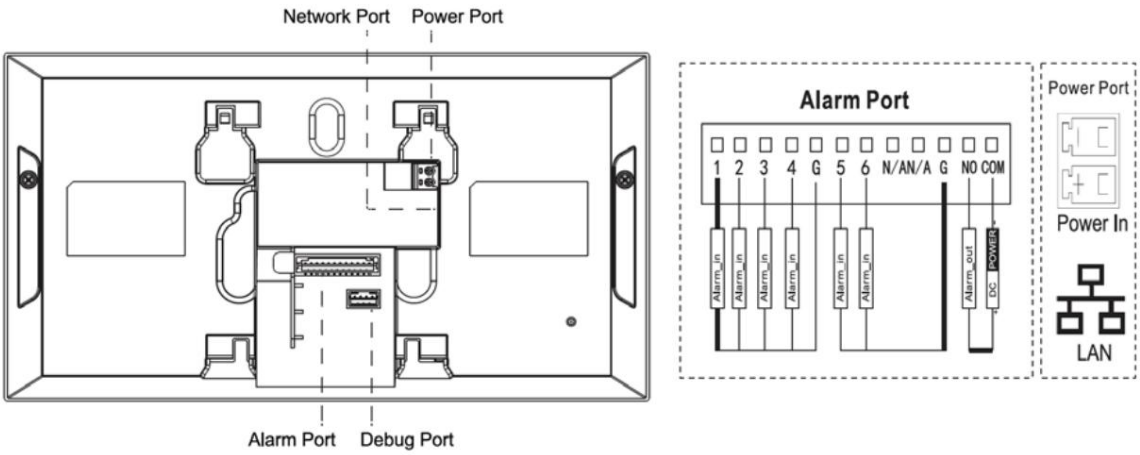
Le posizioni delle porte sul pannello posteriore possono differire. Prendi VTH5221 come esempio.

Figure 1-1 Pannello posteriore del VTH5221



1.2.7 VIS7NPIB/VIS7NPI

Figure 1-9



2 Installazione e messa in servizio

2.1 Installazione

⚠

- Non installare VTH in ambienti difficili con condensa, alte temperature, polvere, corrosivi sostanza e luce solare diretta.
- In caso di anomalia dopo l'accensione, scollegare il cavo di rete e interrompere immediatamente l'alimentazione. Accendere dopo la risoluzione dei problemi.
- L'installazione e il debug devono essere eseguiti da team di professionisti. Non smontare o riparare da soli in caso di guasto del dispositivo. Contatta il supporto tecnico.
- L'altezza del punto centrale del dispositivo deve essere di 1,4 m–1,6 m dal suolo.

2.1.1 Montaggio a parete

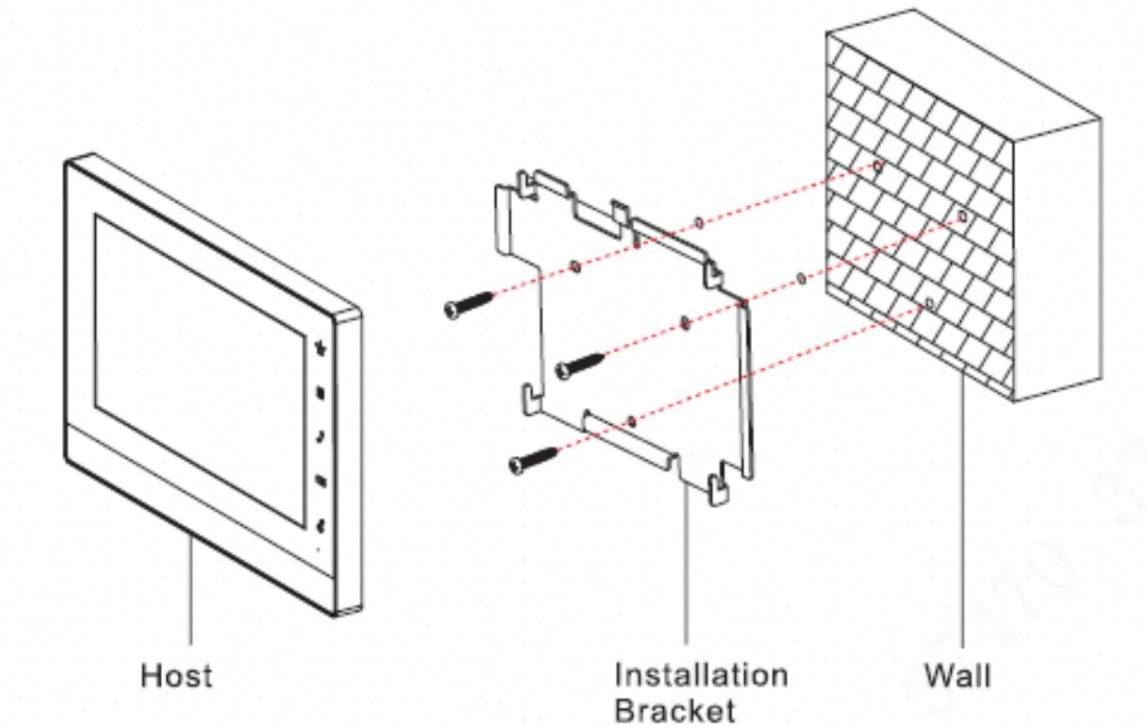
Installare direttamente il dispositivo con una staffa a parete, adatta a tutti i tipi di dispositivi. Prendi VTH1550CH come esempio.

Step 1 Praticare i fori nel muro in base alle posizioni dei fori della staffa di installazione.

Step 2 Fissare la staffa di installazione alla parete con viti.

Step 3 Mettere il dispositivo nella staffa di installazione dall'alto verso il basso.

Figure 2-1 Installazione a parete



2.1.2 Installazione con 86 Box

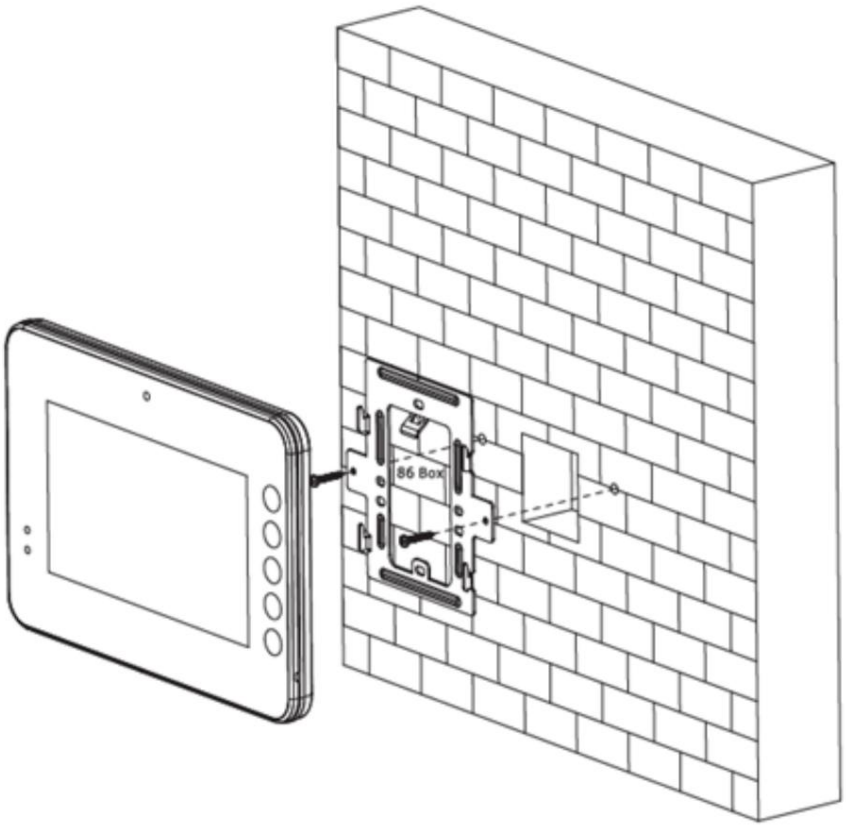
Installa il dispositivo con 86 box, adatto a tutti i tipi di dispositivi. Prendi VTH1560B/BW come un esempio.

Step 1 Incorpora la scatola 86 nel muro ad un'altezza adeguata.

Step 2 Fissare la staffa di installazione sulla scatola 86 con viti.

Step 3 Mettere il dispositivo nella staffa di installazione dall'alto verso il basso.

Figure 2-2 Installazione con scatola da 86



2.1.3 Installazione desktop con staffa

Installare il dispositivo con staffa sul desktop, che si applica solo al portatile VTH. Prendi VTH5221E-H come esempio.

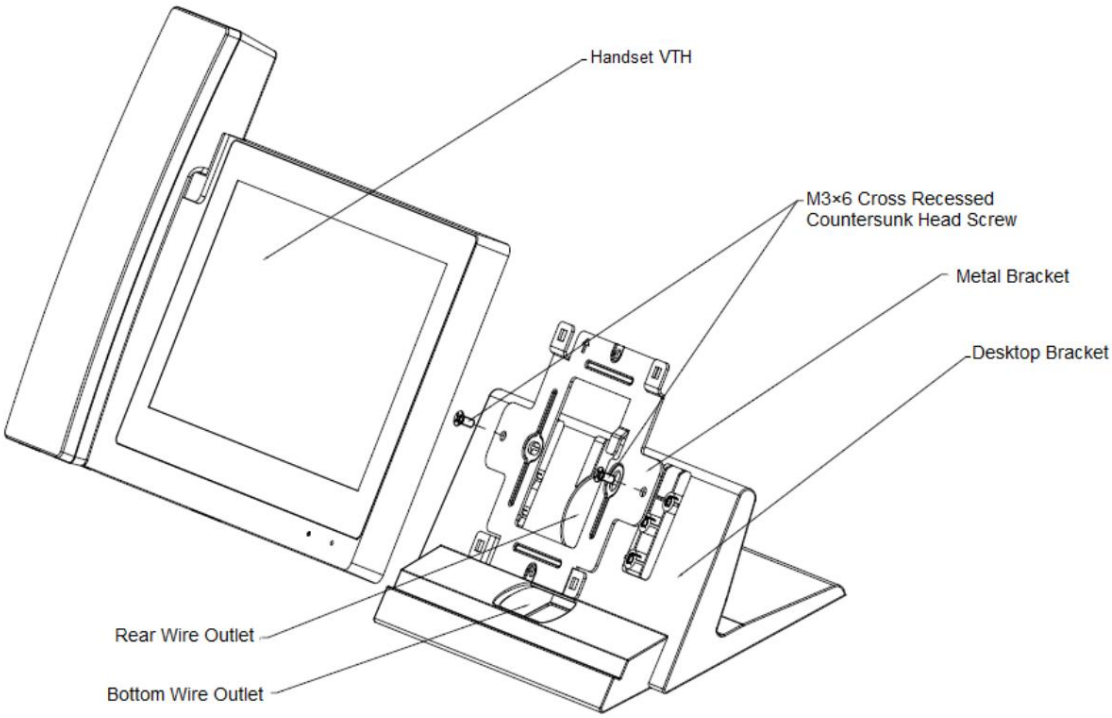
Step 1 Con due viti a testa svasata con intaglio a croce M3 × 6, serrare la staffa metallica sui due dadi superiori della staffa da tavolo.

Step 2 Collega i fili.

Step 3 Far passare i cavi attraverso la presa nella parte posteriore o nella parte inferiore della staffa del desktop.

Step 4 Installare il ricevitore VTH nello slot nella parte superiore della staffa metallica.

Figure 2-3 Installazione desktop con staffe



2.2 Preparativi

Prima della messa in servizio, verificare se i seguenti lavori sono stati completati.

- Accendere il dispositivo solo dopo che non ci sono cortocircuiti o circuiti aperti.
- Pianifica IP e numero (funziona come numero di telefono) per ogni VTO e VTH.
- Confermare la posizione del server SIP.
- Scansiona il codice QR sulla copertina per i dettagli.
- Impostare le informazioni VTO e le informazioni VTH sull'interfaccia web per ogni VTO e impostare le informazioni VTH, le informazioni di rete e le informazioni VTO su ogni VTH.

2.2.1 Impostazioni VTO

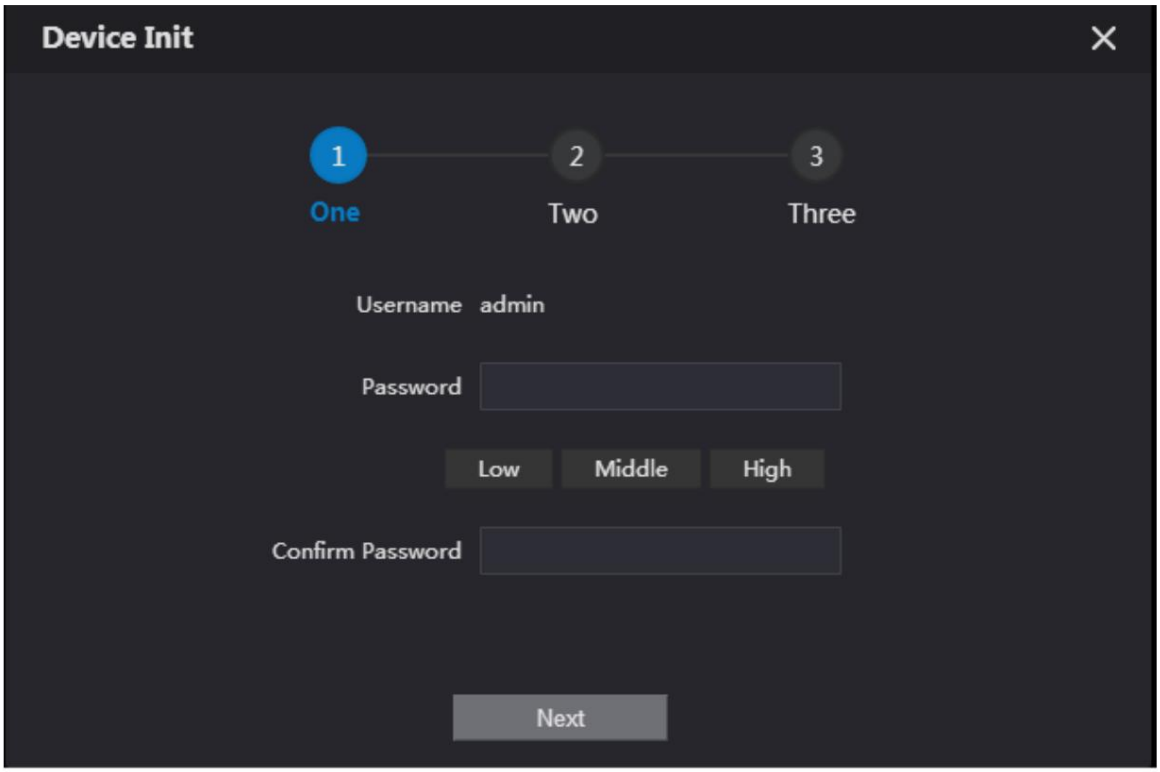
L'interfaccia VTO può differire per i diversi modelli e prevale l'interfaccia effettiva.

Per il primo utilizzo, inizializzare e modificare la password di accesso.

Assicurarsi che gli indirizzi IP predefiniti di PC e VTO si trovino nello stesso segmento di rete. Il predefinito L'indirizzo IP di VTO è 192.168.1.110.

Step 1 Accendi il dispositivo, quindi vai all'indirizzo IP predefinito di VTO nel browser.

Figure 2-4 Inizializzazione del dispositivo



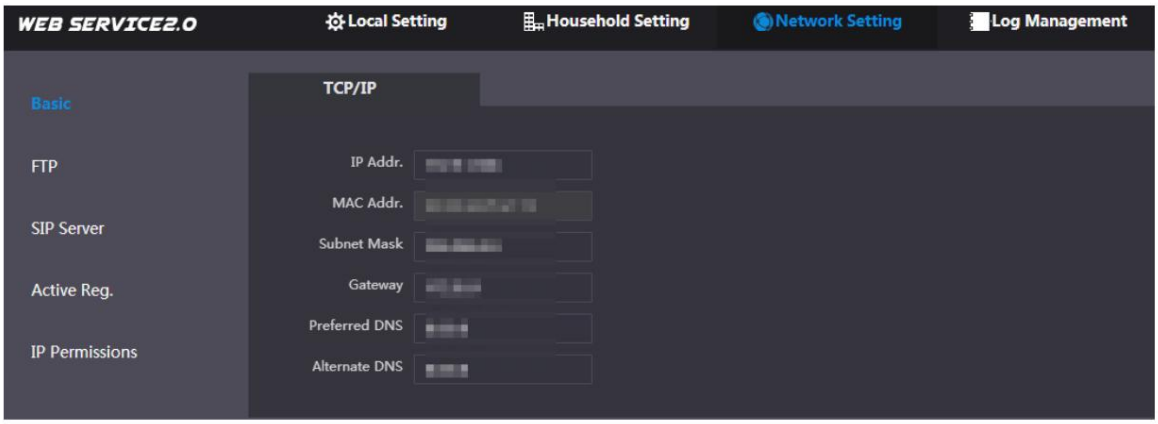
Step 2 Immettere la password e confermarla, quindi fare clic su **Avanti.** Seleziona E- **mail** e inserisci l'indirizzo e-mail per reimpostare la password.

Step 3 Immettere l'indirizzo predefinito nel browser per accedere all'interfaccia WEB.

Il nome utente predefinito è admin e la password è quella impostata in questo momento.

Step 4 Seleziona **Impostazioni di rete > Base.**

Figure 2-5 TCP/IP

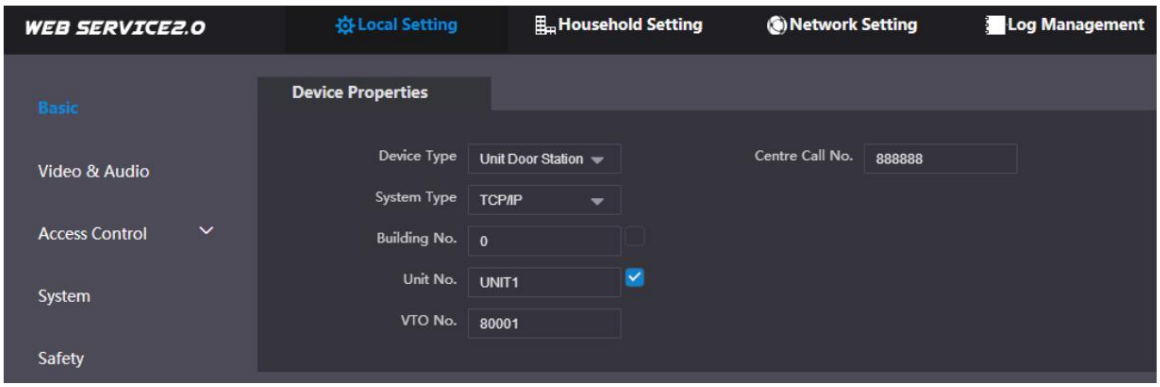


Step 5 Immettere l'indirizzo IP, la subnet mask e il gateway, quindi fare clic su **OK.**

Il VTO si riavvierà automaticamente e: **ÿ** Se il PC è nello stesso segmento di rete, l'interfaccia WEB passa all'interfaccia di login. **ÿ** Se il PC non è nello stesso segmento di rete, non è possibile accedere al nuovo indirizzo IP. Aggiungi PC allo stesso segmento di rete e riprovare.

Step 6 Accedere nuovamente all'interfaccia WEB e selezionare **Impostazioni locali > Base.**

Figure 2-6 Proprietà del dispositivo



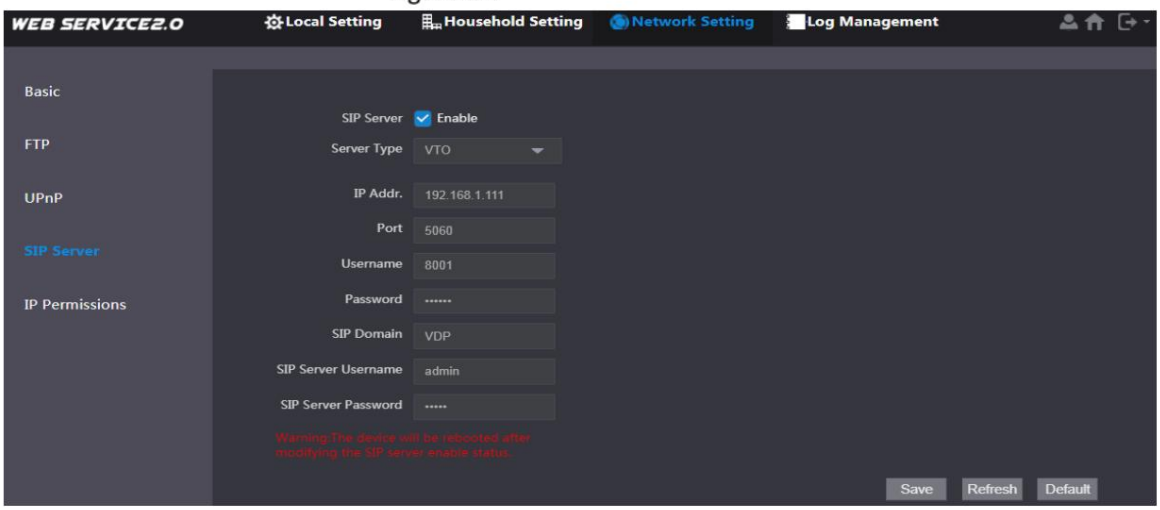
1) Selezionare **Tipo di sistema** come TCP/IP.

2) Fare clic su **OK.**

3) Riavviare il dispositivo manualmente o attendere il riavvio automatico.

Step 7 Accedere all'interfaccia WEB, quindi selezionare **Impostazioni di rete > Server SIP.**

Figure 2-7 Server SIP (1)



1) Seleziona il tipo di server.

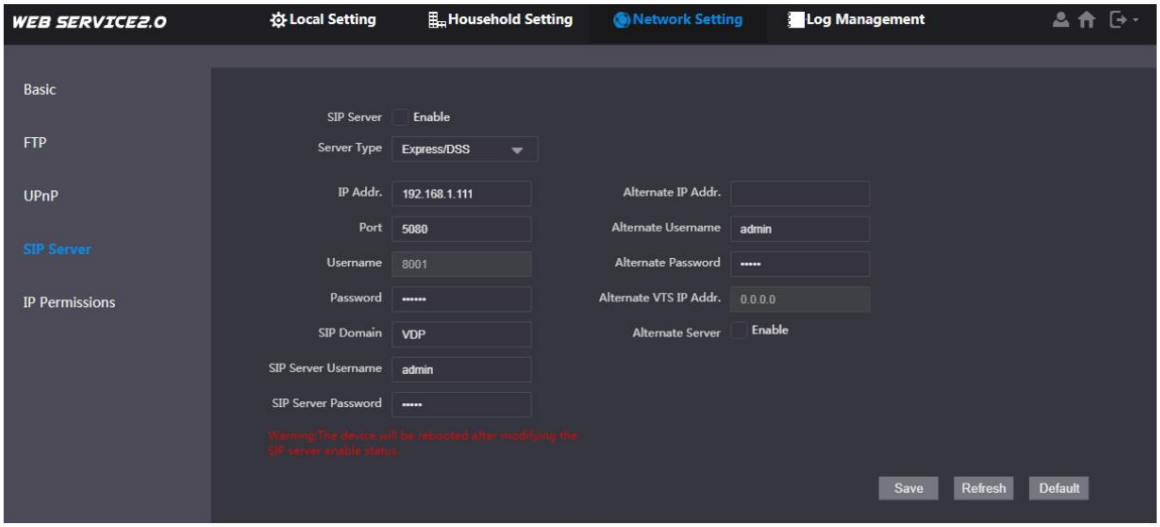
- Quando VTO funziona come server SIP, selezionare **Tipo di server** come **VTO.** Si applica a uno edificio o unità.
- Quando la piattaforma (Express/DSS) funziona come server SIP, selezionare **Tipo di server** come **Express/DSS.** Si applica a più edifici o unità.

2) Impostare il numero VTO e fare clic su **Salva.**

- Quando la piattaforma funziona come server SIP, abilitare **Support Building** e **Support Unità** secondo necessità e configurazione di conseguenza.
- Dopo che VTO è stato impostato come server SIP, la funzione di chiamata di gruppo apparirà sull'interfaccia. Abilitalo secondo necessità.

Step 8 Selezionare **Impostazioni di rete > Server SIP.**

Figure 2-8 Server SIP (2)



- L'attuale VTO funziona come server SIP.

  Abilita **il server SIP** e fai clic su **Salva.** Il VTO si riavvierà automaticamente.

ÿ Un altro VTO o piattaforma funziona come server SIP.

  Configura i parametri e fai clic su **Salva.** Il VTO si riavvierà automaticamente.

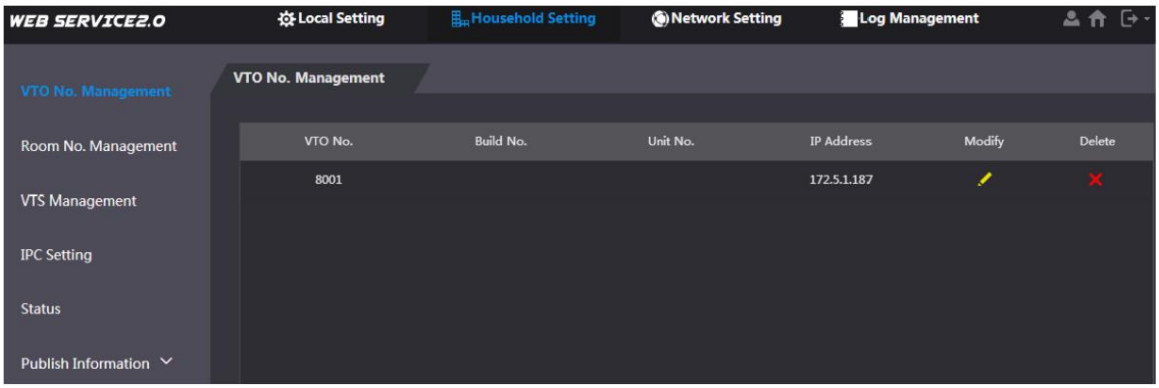
Tabella 2-1 Descrizione del parametro

Parametro	Descrizione
Indirizzo IP	Indirizzo IP del server SIP.
Porta	● 5060 per impostazione predefinita quando un altro VTO funziona come server SIP. ● 5080 per impostazione predefinita quando la piattaforma funziona come server SIP.
Nome utente/Password	Mantieni il valore predefinito.
Dominio SIP	● Immettere VDP quando un altro VTO funziona come server SIP. ● Mantieni vuoto o usa il valore predefinito quando la piattaforma funziona come SIP server.
Login Username/Password	Nome utente e password per accedere al server SIP.

- Le impostazioni VTO sono state completate quando la piattaforma o un altro VTO funziona come SIP server.
- Se l'attuale VTO funziona come server SIP, eseguire i passaggi 9 e 10.

Step 9 (Facoltativo) Accedere all'interfaccia WEB, quindi selezionare **Impostazioni famiglia > N. VTO. Gestione.**

Figure 2-9 OMC n. gestione



Fare clic su **Aggiungi,** configurare i parametri e fare clic su **OK.** Ripetere questo passaggio per aggiungere altri VTO.

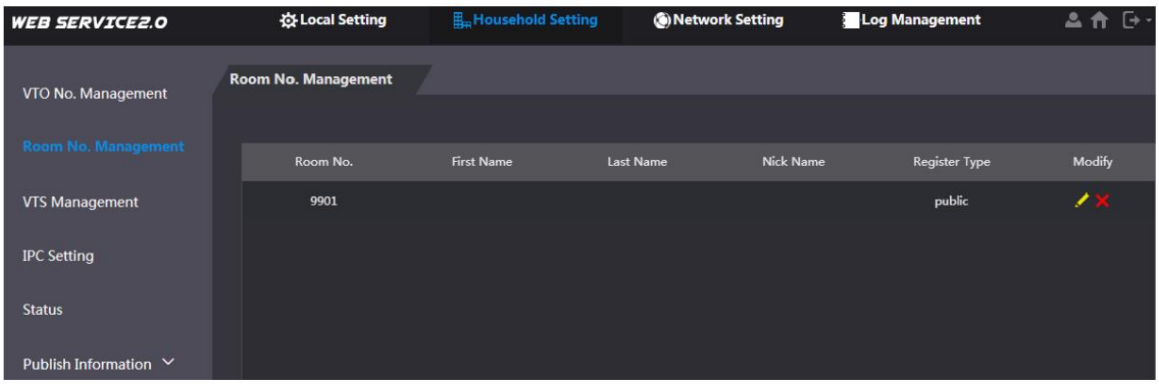
Tabella 2-2 Gestione n. VTO

Parametro	Descrizione
VTO n.	Numero VTO.
Costruisci n.	Numero dell'edificio in cui si trova VTO.
Unità n.	Numero di unità in cui si trova VTO.
Indirizzo IP	Indirizzo IP di VTO.

Step 10 (Facoltativo) Selezionare **Impostazione nucleo familiare > Gestione n. stanza.**

Aggiungi entrambi quando ci sono VTH master ed estensione.

Figure 2-10 Gestione della camera n



Fare clic su **Aggiungi,** configurare i parametri e fare clic su **OK.** Ripetere questo passaggio per aggiungere altri VTH.

Tabella 2-3 Gestione n. camera

Parametro	Descrizione
Stanza No.	Imposta il numero della stanza VTH. - Il numero della stanza VTH è composto da 1–6 numeri, lettere o loro combinazioni. Dovrebbe essere lo stesso con il numero di stanza configurato VTH. Vedere la Figura 2-15. ● Quando sono presenti VTH master ed estensioni, terminare il VTH master in cortocircuito no. con #0, ed estensione VTH breve n. con #1, #2 e #3, per ottenere la funzione di chiamata di gruppo. Ad esempio, se il master VTH è 101#0, le estensioni dovrebbero essere 101#1, 101#2...
Nome di battesimo	Imposta nome utente e nickname per ogni VTH.
Cognome	
Soprannome	
Tipo di registro	Segnalazione dell'uso interattivo nel sistema SIP. Mantieni il valore predefinito.

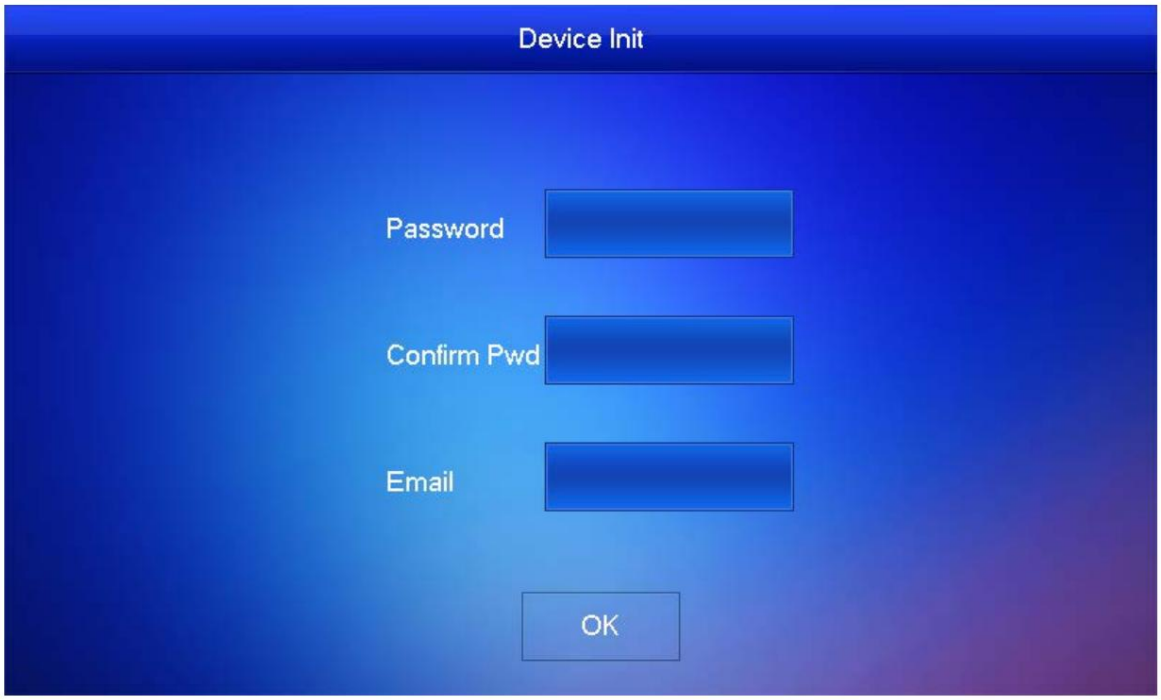
2.2.2 Impostazioni VTH

2.2.2.1 Inizializzazione

Per il primo utilizzo, imposta la password e associa l'indirizzo e-mail. La password viene utilizzata per accedere all'interfaccia di impostazione del progetto, mentre l'indirizzo e-mail viene utilizzato per recuperare la password quando la dimentichi.

Step 1 Accendi il dispositivo.

Figure 2-11 Imposta la password e associa l'indirizzo e-mail



Step 2 Immettere la password e confermarla, immettere l'e-mail e toccare **OK.**

Step 3 Tocca **Impostazioni** per più di 6 secondi, inserisci la password impostata in questo momento, quindi tocca **OK.**

Step 4 Tocca **Rete.**

Gli indirizzi IP di VTH e VTO dovrebbero trovarsi nello stesso segmento di rete. In caso contrario, VTH non può ottenere informazioni VTO dopo la configurazione.

Figure 2-12 Rete

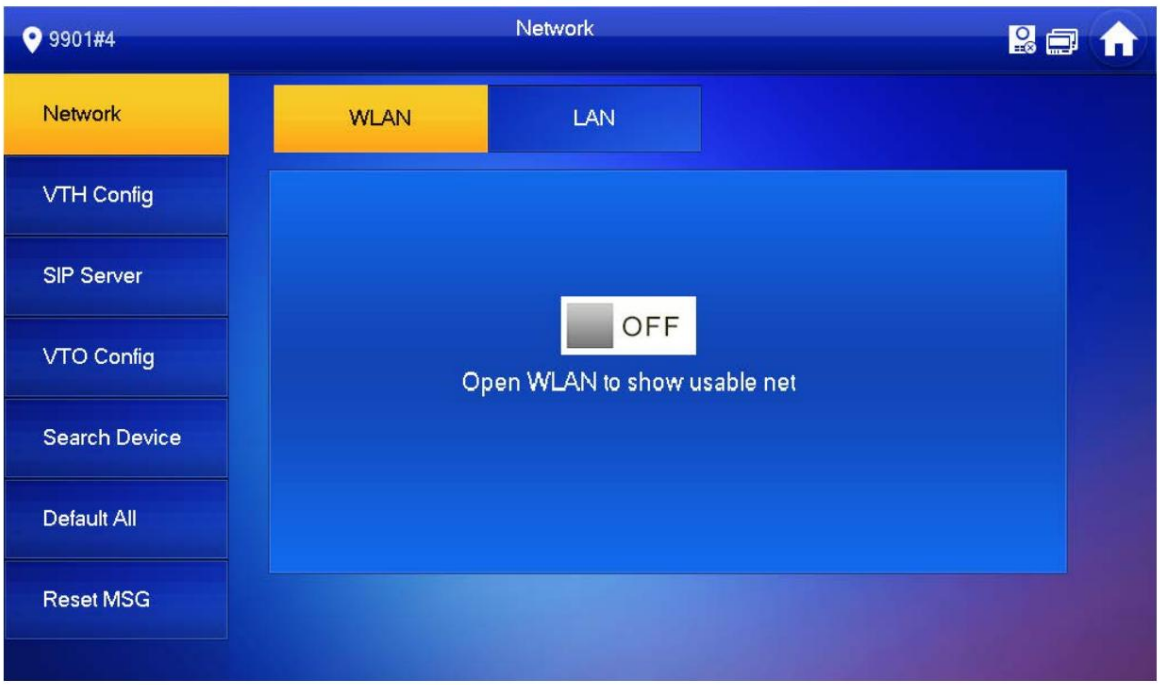
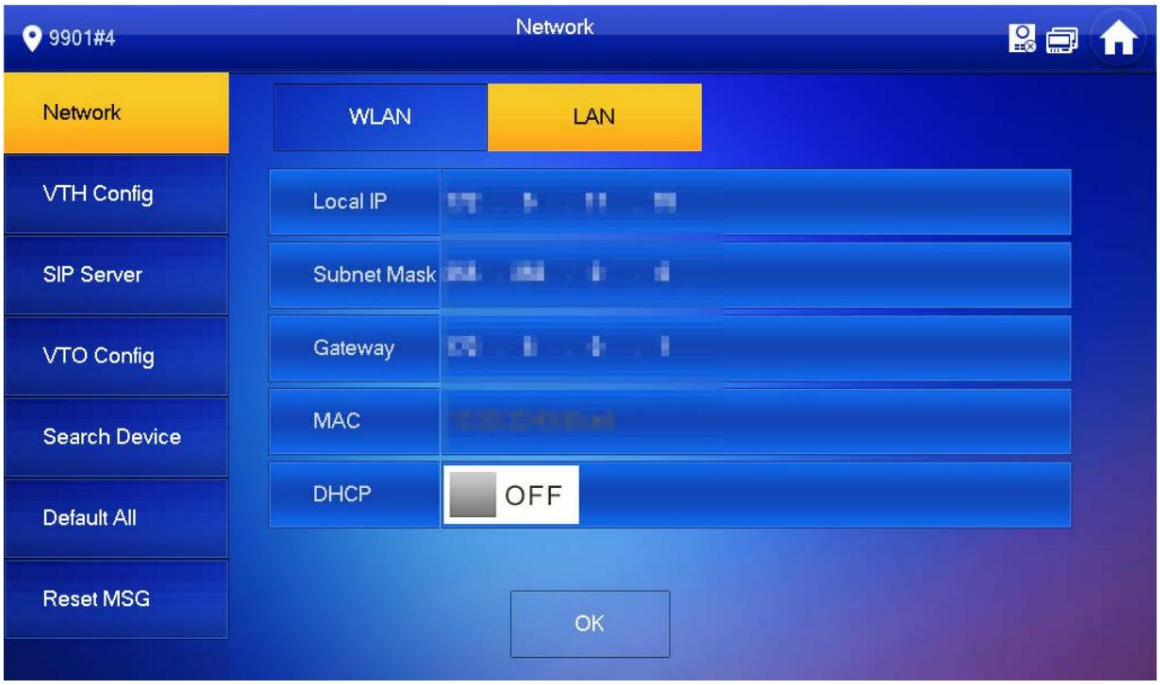


Figure 2-13 E



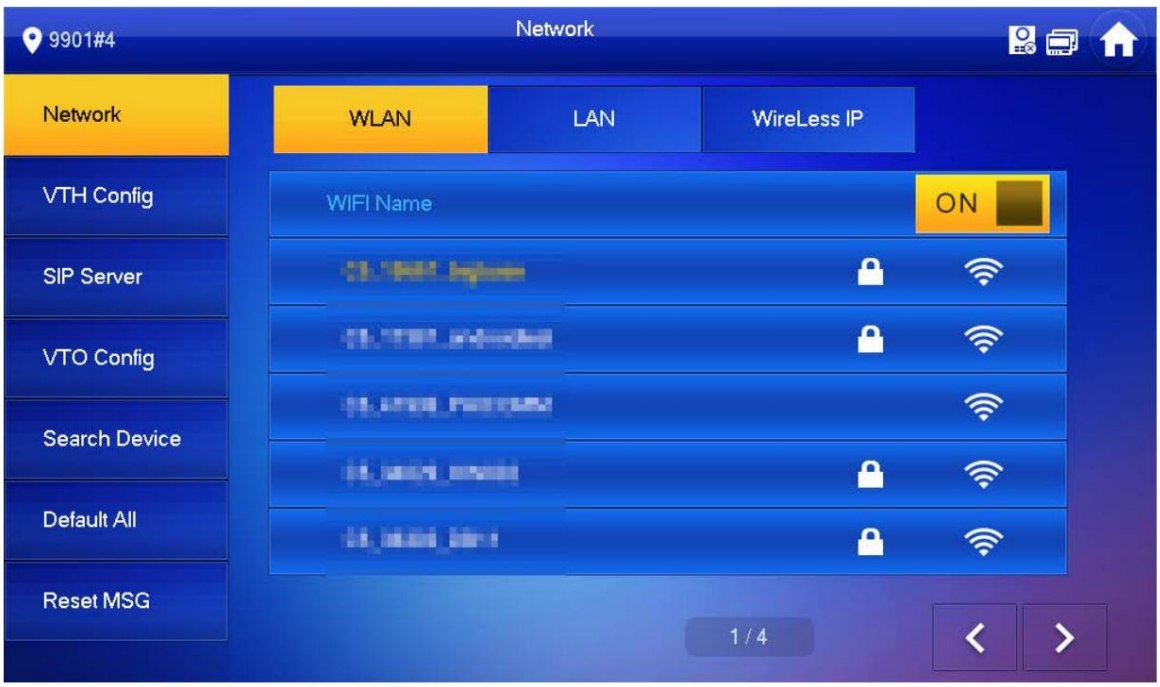
ÿ LAN

Tocca **Rete > LAN.** Immettere l'IP locale, la subnet mask e il gateway, quindi toccare **OK.** Oppure tocca OFF per abilitare la funzione DHCP per ottenere automaticamente le informazioni IP.

ÿ WLAN

1) Toccare **Rete > WLAN,** quindi toccare OFF .

Figure 2-14 WLAN



2) Prima di connetterti a una rete WIFI, esegui prima una delle seguenti operazioni.

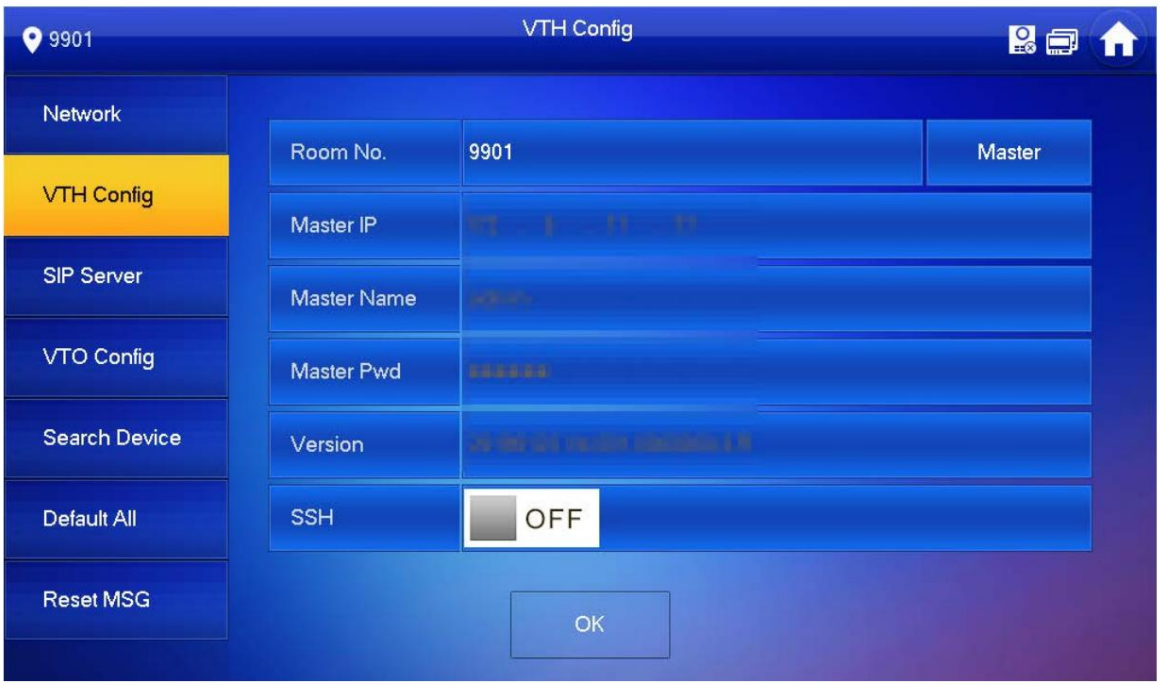
- Toccare **WireLessIP,** immettere IP locale, subnet mask e gateway, quindi toccare **OK.**
- Tocca **WireLessIP,** tocca OFF per abilitare la funzione DHCP per ottenere automaticamente le informazioni IP.

Per abilitare la funzione DHCP, utilizzare un router con funzione DHCP.

3) Collegarsi a una rete WIFI.

Step 5 Tocca **Configurazione VTH.**

Figure 2-15 Configurazione VTH



- Utilizzare come VTH master.

Immettere il numero della stanza (come 9901 o 101#0) e toccare **OK.**

Room No. dovrebbe essere uguale a VTH Short No., che viene impostato quando si aggiunge VTH sull'interfaccia web. In caso contrario, non riuscirà a connettersi a VTO.

Se è presente l'estensione VTH, la stanza n. dovrebbe terminare con #0. In caso contrario, non riuscirà a connettersi VTO.

- Utilizzare come estensione VTH.

1) Tocca **Master** e l'icona passa a **Extension.**

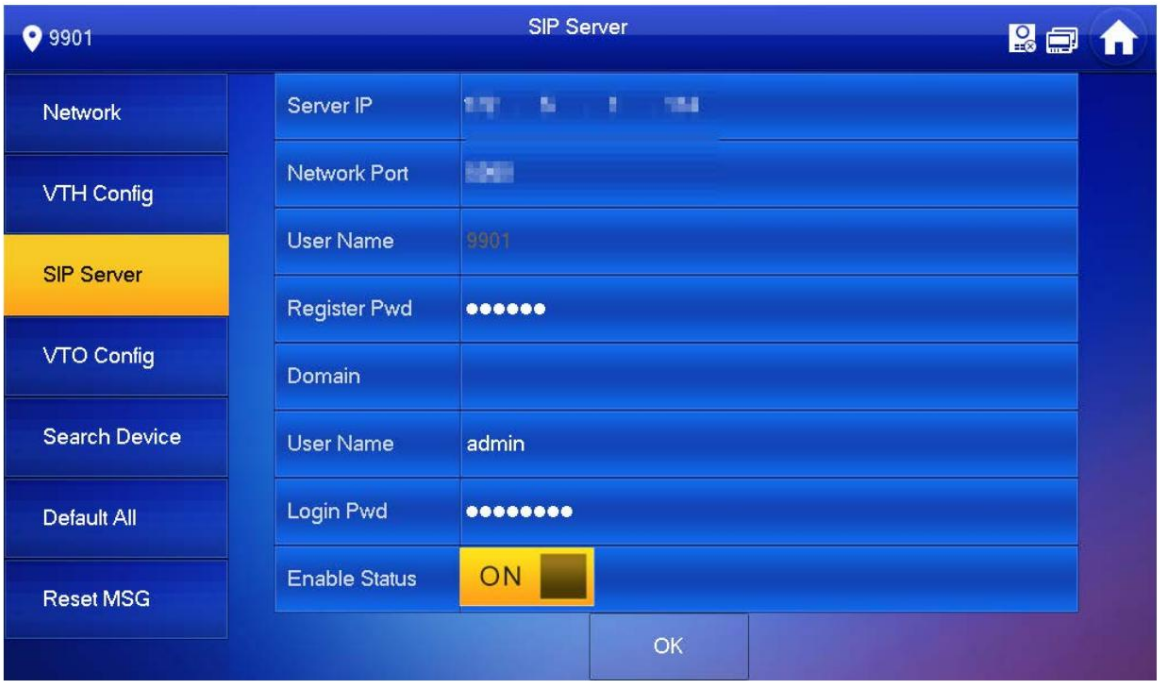
2) Immettere il numero della stanza (come 101#1) e l'indirizzo IP del master VTH.

Master name e password sono il nome utente e la password del master VTH. Il nome utente predefinito è **admin** e la password è quella impostata nel passaggio precedente.

3) Toccare **OK** per salvare le impostazioni.

Step 6 Tocca **Server SIP.**

Figure 2-16 server SIP



1) Configurare i parametri del **server SIP.**

Tabella 2-4 Server SIP

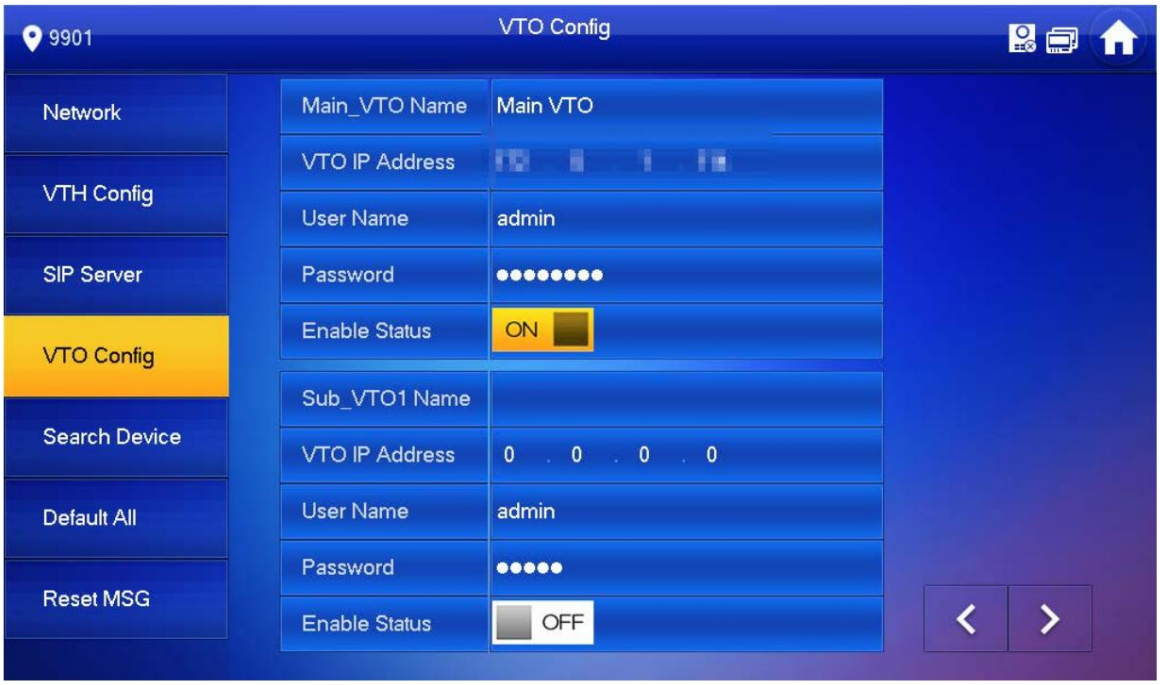
Parametro	Descrizione
IP del server	● Quando la piattaforma funziona come server SIP, l'IP del server è l'indirizzo IP della piattaforma. ● Quando VTO funziona come server SIP, l'IP del server è l'indirizzo IP del VTO.
Porta di rete	● Quando la piattaforma funziona come server SIP, la porta di rete è 5080. ● Quando VTO funziona come server SIP, la porta di rete è 5060.
Nome utente	Usa il valore predefinito.
Registra Pwd	
Dominio	● Dominio di registrazione del server SIP, che può essere vuoto. ● Immettere VDP quando VTO funziona come server SIP.
Nome utente	Nome utente e password di accesso al server SIP.
Accedi Pwd	

2) Impostare **Abilita stato** su 3) ON.

Toccare **OK.**

Step 7 Tocca **Configurazione VTO.**

Figure 2-17 Configurazione VTO



Step 8 Aggiungi VTO.

ÿ Aggiungi VTO principale.

1) Immettere il nome VTO principale, l'indirizzo IP VTO, nome utente e password.

2) Impostare **Abilita stato** su ON.

Il nome **utente** e la **password** devono corrispondere al nome utente e alla password di accesso dell'interfaccia WEB di VTO. In caso contrario, non riuscirà a connettersi.

ÿ Aggiungi sub VTO.

1) Immettere il nome del sub VTO, l'indirizzo IP del sub VTO, il nome utente e la password.

2) Impostare Abilita stato su ON.

Rubinetto / per voltare pagina e aggiungere altri sub VTO.

2.3 La messa in produzione

2.3.1 VTO Chiama VTH

Comporre la stanza VTH n. (come 101) a VTO per chiamare VTH. VTH si apre monitorando video e icone operative.

La figura seguente indica che la scheda SD è stata inserita nel VTH. Se la scheda SD non è inserita, le icone di registrazione e istantanea sono grigie.

Figure 2-18 Chiama VTH da VTO

2.3.2 VTH Monitora il VTO

VTH è in grado di monitorare VTO o IPC. Prendi VTO come esempio.

Selezionare **Monitor > Porta** e selezionare il VTO per accedere all'immagine di monitoraggio.

La figura seguente indica che la scheda SD è stata inserita nel VTH. Se la scheda SD non è inserita, le icone di registrazione e istantanea sono grigie.

Figure 2-19 Porta

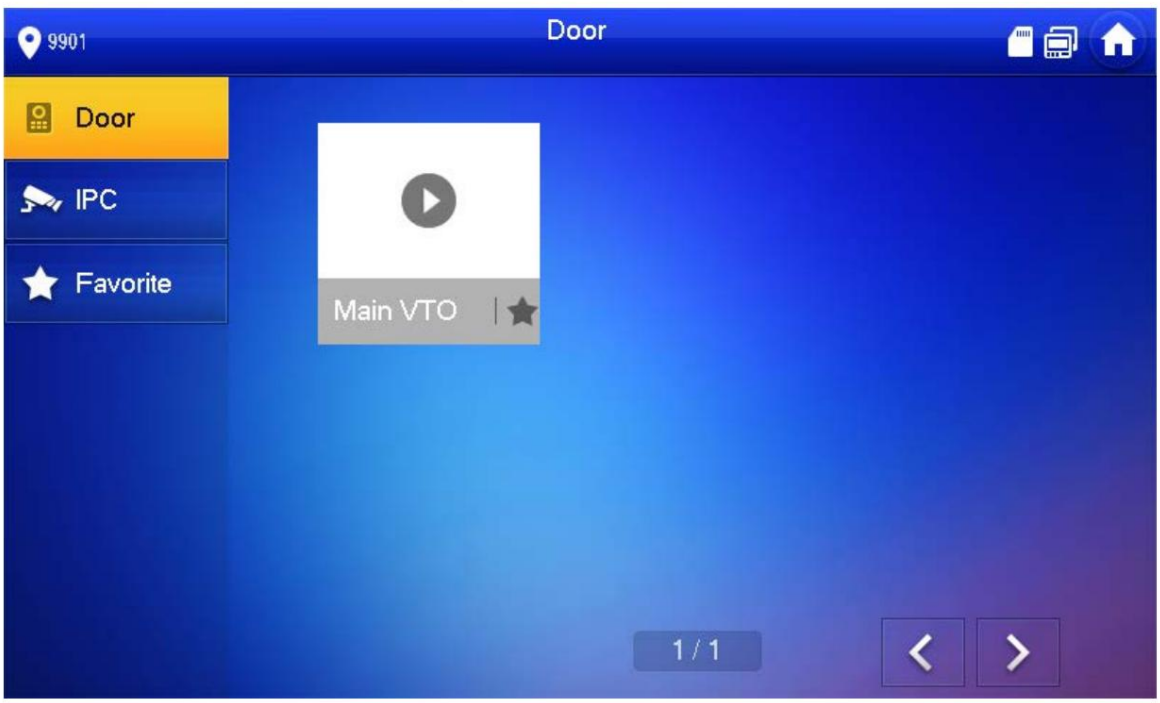
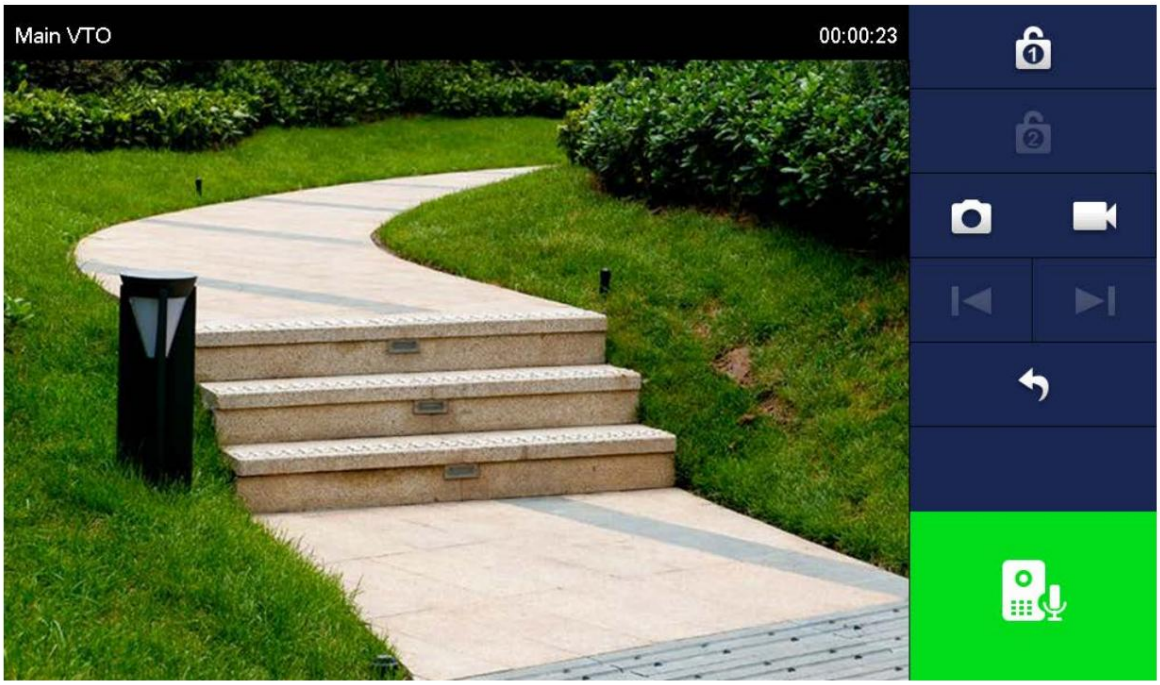


Figure 2-20 Video di monitoraggio



Appendix 1 Raccomandazioni sulla sicurezza informatica

La sicurezza informatica è più di una semplice parola d'ordine: è qualcosa che riguarda ogni dispositivo connesso a Internet. La videosorveglianza IP non è immune dai rischi informatici, ma l'adozione di misure di base per la protezione e il rafforzamento delle reti e delle apparecchiature in rete le renderà meno suscettibili agli attacchi. Di seguito sono riportati alcuni suggerimenti e consigli su come creare un sistema di sicurezza più sicuro.

Azioni obbligatorie da intraprendere per la sicurezza di base della rete del dispositivo:

1. Usa password complesse

Fare riferimento ai seguenti suggerimenti per impostare le password:

- La lunghezza non deve essere inferiore a 8 caratteri;
- Includere almeno due tipi di caratteri; i tipi di carattere includono maiuscole e minuscole lettere, numeri e simboli;
- Non contenere il nome dell'account o il nome dell'account in ordine inverso;
- Non utilizzare caratteri continui, come 123, abc, ecc.;
- Non utilizzare caratteri sovrapposti, come 111, aaa, ecc.;

2. Aggiorna il firmware e il software client in tempo

- Secondo la procedura standard in Tech-industry, si consiglia di mantenere aggiornato il firmware del dispositivo (come NVR, DVR, telecamera IP, ecc.) per garantire che il sistema sia dotato delle patch e correzioni di sicurezza più recenti. Quando il dispositivo è connesso alla rete pubblica, si consiglia di abilitare la funzione "verifica automatica aggiornamenti" per ottenere informazioni tempestive sugli aggiornamenti firmware rilasciati dal produttore.

- Si consiglia di scaricare e utilizzare l'ultima versione del software client.

Consigli "Piacere da avere" per migliorare la sicurezza della rete del tuo dispositivo:

1. Protezione fisica

Ti consigliamo di eseguire la protezione fisica del dispositivo, in particolare dei dispositivi di archiviazione. Ad esempio, posizionare il dispositivo in una sala computer speciale e in un armadio e implementare un'autorizzazione di controllo degli accessi e una gestione delle chiavi ben fatte per impedire a personale non autorizzato di eseguire contatti fisici come danni all'hardware, connessione non autorizzata di dispositivi rimovibili (come un disco flash USB , porta seriale), ecc.

2. Modificare le password regolarmente

Ti consigliamo di cambiare le password regolarmente per ridurre il rischio di essere indovinato o violato.

3. Impostare e aggiornare le password Reimpostare le informazioni

tempestivamente Il dispositivo supporta la funzione di reimpostazione della password. Si prega di impostare le informazioni correlate per la reimpostazione della password in tempo, inclusa la casella di posta dell'utente finale e le domande sulla protezione della password. Se le informazioni cambiano, si prega di modificarle in tempo. Quando si impostano domande di protezione con password, si consiglia di non utilizzare quelle facilmente intuibili.

4. Abilita il blocco dell'account

La funzione di blocco dell'account è abilitata per impostazione predefinita e ti consigliamo di mantenerla attiva per garantire la sicurezza dell'account. Se un utente malintenzionato tenta di accedere più volte con la password errata, l'account corrispondente e l'indirizzo IP di origine verranno bloccati.

5. Modifica HTTP predefinito e altre porte di servizio

Ti consigliamo di modificare le porte HTTP e di altro servizio predefinite in qualsiasi insieme di numeri compreso tra 1024 e 65535, riducendo il rischio che estranei possano indovinare quali porte stai utilizzando.

6. Abilita HTTPS

Ti consigliamo di abilitare HTTPS, in modo da visitare il servizio Web attraverso una comunicazione sicura canale.

7. Associazione dell'indirizzo MAC

Ti consigliamo di associare l'indirizzo IP e MAC del gateway al dispositivo, riducendo così il rischio di spoofing ARP.

8. Assegnare account e privilegi in modo ragionevole

In base ai requisiti aziendali e di gestione, aggiungere utenti ragionevolmente e assegnare loro un set minimo di autorizzazioni.

9. Disabilita i servizi non necessari e scegli le modalità sicure

Se non necessario, si consiglia di disattivare alcuni servizi come SNMP, SMTP, UPnP, ecc., per ridurre i rischi.

Se necessario, si consiglia vivamente di utilizzare le modalità sicure, inclusi, a titolo esemplificativo, i seguenti servizi:

- SNMP: scegli SNMP v3 e imposta password e autenticazione di crittografia avanzata Le password.
- SMTP: scegli TLS per accedere al server della casella di posta.
- FTP: scegli SFTP e imposta password complesse.
- Hotspot AP: scegli la modalità di crittografia WPA2-PSK e imposta password complesse.

10. Trasmissione crittografata audio e video

Se i contenuti dei tuoi dati audio e video sono molto importanti o sensibili, ti consigliamo di utilizzare la funzione di trasmissione crittografata, per ridurre il rischio di furto di dati audio e video durante la trasmissione.

Promemoria: la trasmissione crittografata causerà una perdita di efficienza di trasmissione.

11. Controllo sicuro

- Verifica utenti online: ti suggeriamo di controllare regolarmente gli utenti online per vedere se il dispositivo lo è effettuato l'accesso senza autorizzazione.
- Verifica registro dispositivo: visualizzando i registri, puoi conoscere gli indirizzi IP utilizzati per accedere ai tuoi dispositivi e le loro operazioni chiave.

12. Registro di rete

A causa della capacità di archiviazione limitata del dispositivo, il registro archiviato è limitato. Se è necessario salvare il registro per molto tempo, si consiglia di abilitare la funzione del registro di rete per garantire che i registri critici siano sincronizzati con il server del registro di rete per la traccia.

13. Costruire un ambiente di rete sicuro

Al fine di garantire al meglio la sicurezza del dispositivo e ridurre i potenziali rischi informatici, consigliamo:

- Disabilitare la funzione di mappatura delle porte del router per evitare l'accesso diretto ai dispositivi intranet da rete esterna.
- La rete deve essere partizionata e isolata in base alle effettive esigenze della rete. Se non ci sono requisiti di comunicazione tra due sottoreti, si suggerisce di utilizzare VLAN, GAP di rete e altre tecnologie per partizionare la rete, in modo da ottenere l'effetto di isolamento della rete.
- Stabilire il sistema di autenticazione dell'accesso 802.1x per ridurre il rischio di accesso non autorizzato alle reti private.
- Abilitare la funzione di filtraggio degli indirizzi IP/MAC per limitare la gamma di host autorizzati ad accedere al dispositivo.