ekinex
CONTROL YOUR LIVING SPACE

Manuale amministratore

Videocitofono con riconoscimento facciale
DICO EK-5DP-VI

Sommario

Versione	Modifiche	Data	Autore	Verifica
1.0	Prima versione	26/09/2023	G. Schiochet	C. Baldini
1.1	Aggiornamento modifiche al testo	17/11/2023	G. Schiochet	C. Baldini
1.2	Corretti riferimenti Delégo App	22/11/2023	G. Schiochet	C. Baldini
1.3	Aggiunto riferimento a relè di sicurezza EK-SR1-VI	01/12/2023	G. Schiochet	C. Baldini
1.4	Aggiornamento copertina con nuovo rendering	02/07/2024	G. Schiochet	I. Panero
2.0	Aggiornamento alla versione FW 216.43.100.27	12/07/2024	G. Schiochet	C. Baldini
2.1	Aggiornamento alla versione FW 216.43.100.31	25/07/2024	G. Schiochet	I. Panero

1. Scopo del documento

Grazie per aver scelto il dispositivo Ekinex EK-5DP-VI “DICO”.

Questo manuale è rivolto agli amministratori che necessitano di configurare correttamente il videocitofono. Il presente manuale è applicabile alla versione 216.43.0.18 e successive e fornisce tutte le configurazioni per le funzioni del dispositivo EK-5DP-VI “DICO”. Visitare il sito www.ekinex.com o contattare il supporto tecnico al seguente indirizzo e-mail: support@ekinex.com per qualsiasi ulteriore informazione o per richiedere l’ultima versione firmware.

2. Panoramica del prodotto

Il dispositivo Ekinex EK-5DP-VI “DICO” è un videocitofono IP con touch screen, con firmware sviluppato su sistema Linux. Integra comunicazioni audio e video, controllo accessi e videosorveglianza. Il dispositivo offre funzionalità personalizzabili attraverso il suo sistema avanzato Ekinex Delégo e la tecnologia di comunicazione basata sull'intelligenza artificiale, adattandosi alle tue preferenze operative. Questa soluzione completa garantisce un controllo olistico sugli ingressi e sui dintorni degli edifici, fornendo maggiore sicurezza attraverso vari metodi di accesso come accesso con smart card, NFC, app mobile, codice QR, codice PIN, ideale per edifici residenziali, uffici e complessi.

3. Specifiche del prodotto

Display	5'' IPS
Touch Screen	√
Risoluzione	1280 x 720 pixel
Fotocamera	2M pixel dual-lens, WDR
Uscite relè	1
Ingressi allarme	1
Lettore RF card	13,56MHz
Porta Ethernet	RJ45, 10/100Mbps adattativa 802.3af Power-over-Ethernet
Collegamento Wiegand	√
Riconoscimento facciale	√
RS485	√
PoE	√
Luminosità	500cd/m^2
RAM	1GB
ROM	8GB
Grado di protezione IP	IP65
Montaggio a parete	√

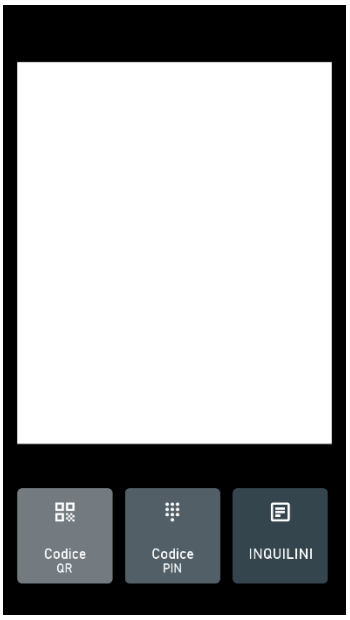
Montaggio ad incasso	√
Potenza POE in stand-by	5,5W
Potenza max. POE	9,8W
Consumo alimentatore in stand-by	5,5W
Consumo max. alimentatore	10W

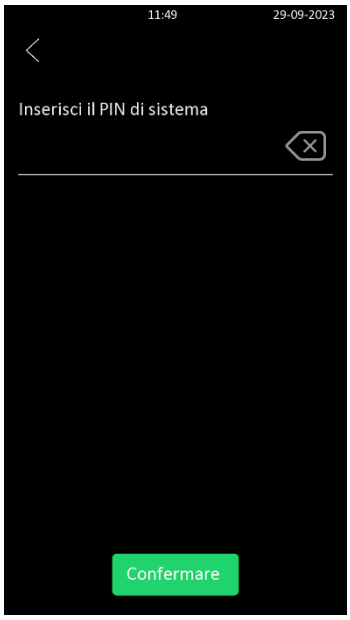
4. Accesso al dispositivo

È possibile accedere alle impostazioni di sistema del videocitofono DICO direttamente sul dispositivo o dall'interfaccia web del dispositivo.

4.1 Accesso alle impostazioni sul dispositivo

Per accedere alle impostazioni sul dispositivo, occorre esercitare una pressione prolungata sulla schermata iniziale per circa cinque secondi, quindi inserire il codice PIN predefinito **admin** e premere *Confermare*.



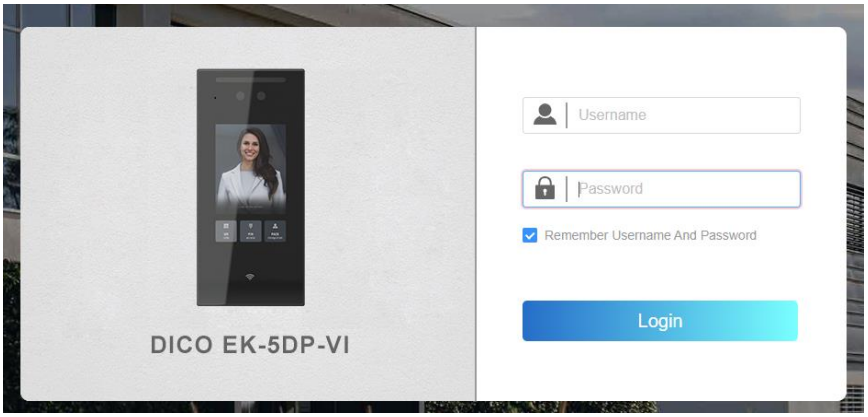


4.2 Accesso alle impostazioni dall'interfaccia web

Per cercare l'indirizzo IP del dispositivo sulla stessa LAN è inoltre possibile utilizzare un comune strumento di scansione IP.

Quindi inserire l'indirizzo IP del dispositivo in un browser web per accedere all'interfaccia web del dispositivo, nella quale sarà possibile configurare e regolare i parametri, ecc.

Utilizzare l'indirizzo IP per accedere al browser web tramite nome utente e password **admin** e **admin**.



Nota

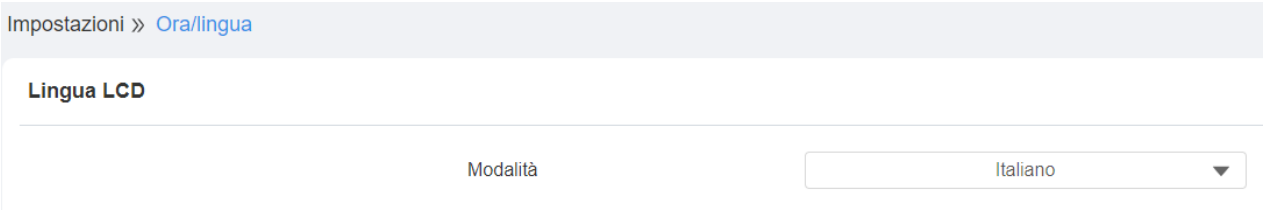
- Il browser Google Chrome è fortemente consigliato.
- Il nome utente e la password iniziali sono **admin / admin** (minuscolo) e si prega di fare attenzione in quanto l'interfaccia fa distinzione tra maiuscole e minuscole.

5. Impostazioni della lingua e della data/ora

5.1 Impostazione della lingua

È possibile selezionare la lingua del dispositivo e personalizzare il testo dell'interfaccia, inclusi i nomi di configurazione e la visualizzazione del testo sul dispositivo e sull'interfaccia web.

Per selezionare la lingua del dispositivo dall'interfaccia web, andare su **Impostazioni > Ora/Lingua > lingua LCD.**



Per personalizzare i nomi di configurazione e il testo visualizzato sul dispositivo, è necessario esportare e modificare il file .json prima di caricarlo sul dispositivo.

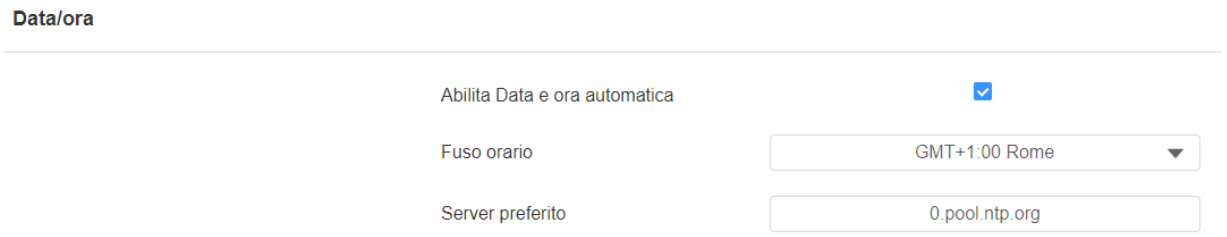
Questa operazione si può effettuare dall'interfaccia web al seguente link: **Impostazioni > Ora/Lingua > Caricamento Dizionario Lingue**

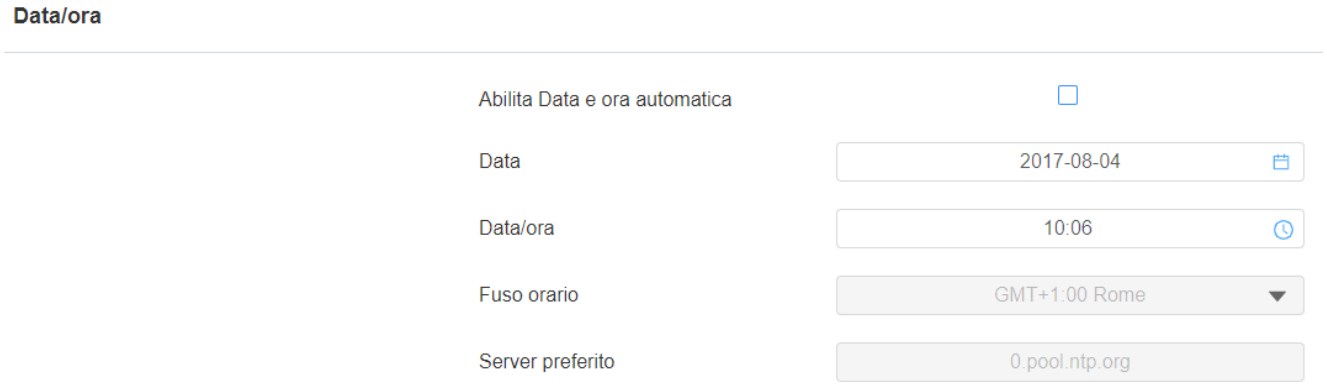
5.2 Impostazioni data/ora

L'impostazione di data e ora sull'interfaccia web può essere effettuata al seguente link:

Impostazioni > Ora/Lingua > Data/ora

Ciò consente all'utente di impostare l'ora e la data manualmente o aggiungendo un indirizzo del server NTP, per sincronizzare automaticamente l'ora e la data. Non appena viene selezionato il fuso orario, il dispositivo notificherà automaticamente il proprio fuso orario al server NTP in modo che questo possa sincronizzare l'impostazione del fuso orario nel dispositivo.





Impostazione parametri:

- **Abilita Data e ora automatica:** abilitarlo se si desidera che la data e l'ora del dispositivo vengano impostate e sincronizzate automaticamente con il fuso orario predefinito e il server NTP (**Network Time Protocol**).
- **Fuso orario:** selezionare il fuso orario specifico della zona in cui viene utilizzato il dispositivo e premere il tasto *Invia* per la conferma. Il fuso orario predefinito è GMT+0.00.
- **Server preferito**: inserire l'indirizzo del server utilizzato per la sincronizzazione di data/ora.

Nota

- Quando la casella di controllo non è selezionata, i parametri relativi al server NTP non possono essere modificati.

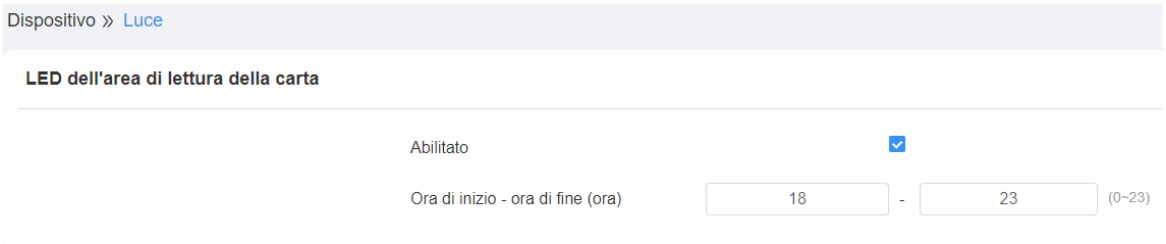
5.3 Impostazioni illuminazione

5.3.1 Configurazione impostazioni per il LED del lettore Card

Dall'interfaccia web è possibile abilitare o disabilitare l'illuminazione LED nell'area del lettore Card, in base alle esigenze dell'utente.

Analogamente, se non si desidera che la luce LED del lettore Card rimanga accesa, è anche possibile impostare l'intervallo di tempo durante il quale la luce LED può essere disattivata per ridurre il consumo di energia elettrica.

Per configurare tali impostazioni dall'interfaccia web, fare riferimento al link **Dispositivo > Luce > LED dell'area di lettura della carta**



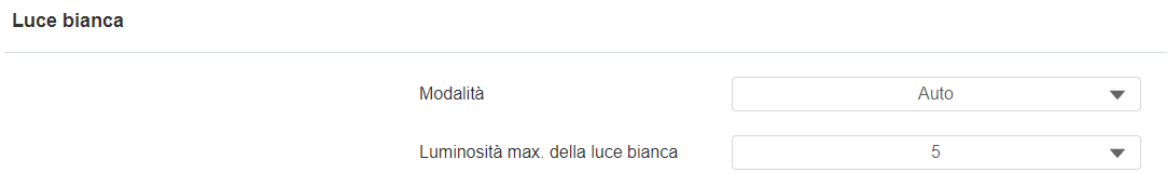
Impostazione parametri:

- **Ora di inizio – ora di fine:** inserire l'intervallo di tempo durante il quale l'illuminazione a LED è attiva.

  Ad es. se l'intervallo di tempo è dalle 18:00 alle 22:00, significa che la luce LED rimarrà accesa durante l'intervallo di tempo dalle 18:00 alle 22:00 nell'arco della giornata (24 ore).

5.3.2 Configurazione impostazioni per il LED luce bianca

Il LED a luce bianca viene utilizzato per rafforzare l'illuminazione per il riconoscimento facciale e per l'accesso al codice QR in un ambiente buio. Per configurare la funzione dall'interfaccia web, andare su **Dispositivo > Luce > Luce bianca**



Impostazione parametri:

- **Modalità**: selezionando **Auto**, la luce bianca si accenderà automaticamente per il riconoscimento del volto e la scansione del codice QR per l'apertura della porta. Se si seleziona **Off**, la luce bianca verrà disattivata.
- **Luminosità max. della luce bianca**: imposta la luminosità della luce bianca in un intervallo di valori da 1 a 5. Il valore predefinito della luce bianca è 3; maggiore è il valore, maggiore sarà la luminosità.

Nota

- Il LED IR deve essere attivato prima della funzione luce bianca se si utilizza il riconoscimento facciale, tuttavia, non è necessario che il LED IR sia attivato per la funzione luce bianca se si utilizza la scansione del codice QR.

5.4 Configurazione del display

Il videocitofono DICO consente di usufruire di una varietà di schermate per arricchire l'esperienza visiva e operativa dell'utente, attraverso l'impostazione personalizzata in base alle proprie preferenze.

5.4.1 Configurazione Screensaver

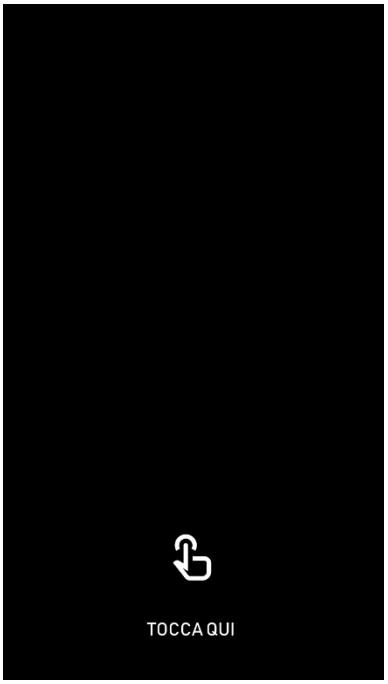
La funzione di Screensaver serve principalmente per la protezione del display. È possibile far sì che il dispositivo entri in stato di inattività per un periodo di tempo predefinito quando non viene eseguita alcuna operazione sul dispositivo o quando non viene rilevato nessuno in avvicinamento.

Per impostare la configurazione dall'interfaccia web, selezionare **Dispositivo > LCD > Visualizzazione standby.**

Impostazione parametri:

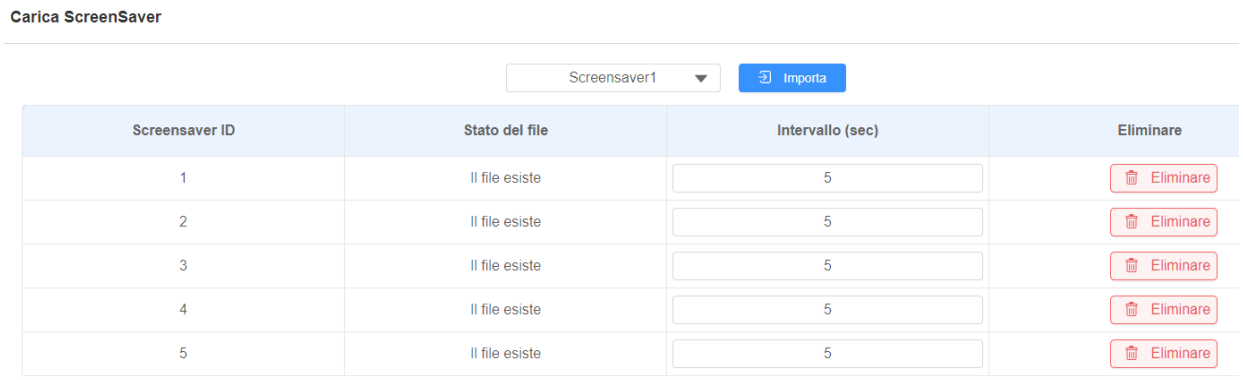
- **Modalità screensaver**: consente di abilitare o disabilitare la funzione screensaver.
- **Durata screensaver**: imposta la durata prevista del salvaschermo prima dello spegnimento del display del dispositivo. Questo timer è impostabile nell'intervallo da 5 secondi a 2 ore.
- **Sleep:** imposta il tempo di inizio del salvaschermo da 2 secondi a 30 minuti dall'ultima attività. Ad esempio, se si seleziona il tempo di inizio su 5 minuti, il salvaschermo si avvierà se non viene eseguita alcuna operazione sul dispositivo o se nessuno si avvicina in un intervallo di cinque minuti.
- **Modalità riattivazione**: consente di selezionare la modalità di riattivazione dello schermo. Scegliendo la modalità **Auto**, lo schermo si riattiverà quando qualcuno si avvicina senza che venga toccato; se si seleziona la modalità **Manuale**, sarà necessario toccare il display per riattivarlo; se invece si

seleziona la modalità **Icona Tocca qui**, dopo aver toccato il display si dovrà successivamente cliccare sull'icona "Tocca qui" (visibile sul display nella posizione centrale in basso) per la riattivazione.



5.4.2 Caricamento Screensaver

È possibile caricare le immagini da utilizzare come salvaschermo sul dispositivo, a partire dall'interfaccia web al link **Dispositivo > LCD > Carica Screensaver**. È consentito caricare un massimo di 5 immagini e ciascuna immagine verrà visualizzata a rotazione in base all'ordine dell'ID con una durata di tempo (Intervallo) impostata.

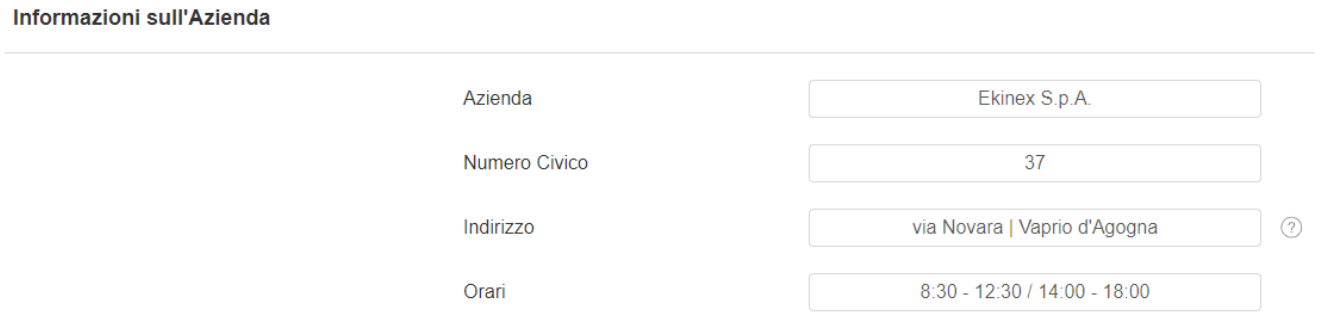


Nota

- Le immagini caricate devono essere in formato JPG o PNG con una dimensione massima di 2M pixel.
- Le immagini salvate in precedenza con uno specifico ID verranno sovrascritte quando si verifica il caricamento successivo di immagini con lo stesso ID.

5.4.3 Configurare la visualizzazione delle informazioni sull'azienda

È possibile configurare le informazioni aziendali per la pagina di benvenuto da interfaccia web, selezionando **Dispositivo > LCD > Informazioni sull'Azienda**.



Impostazione parametri:

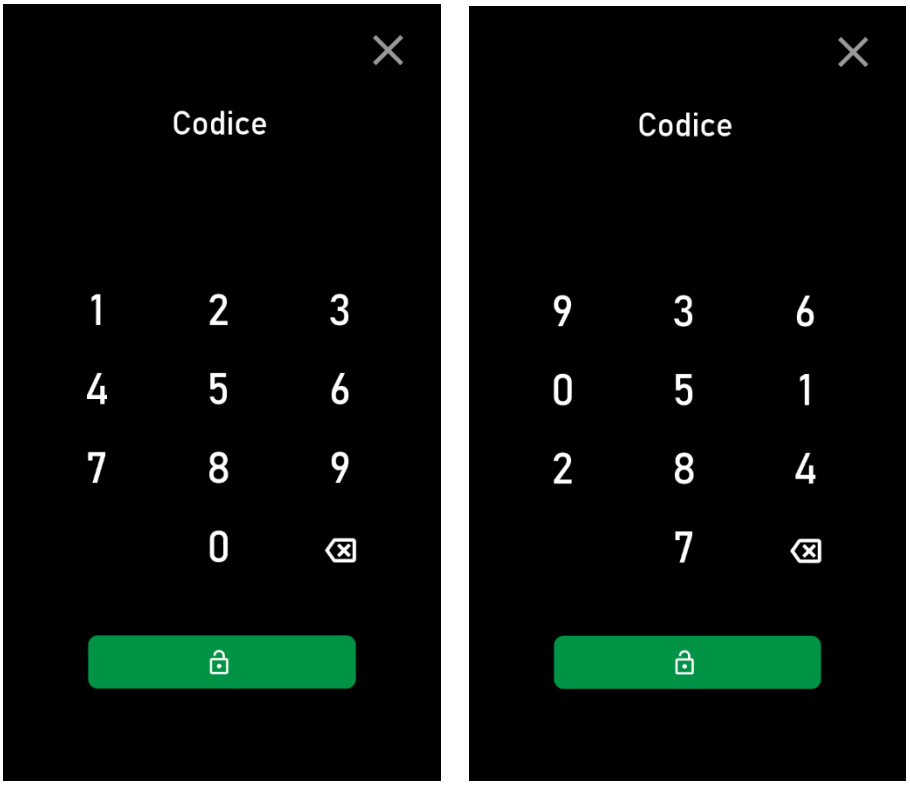
- **Azienda**: consente di inserire il nominativo dell'azienda.
- **Numero civico**: il numero civico dell'indirizzo, fino a 5 cifre;
- **Indirizzo**: può essere configurato su due righe, usando il carattere "|" per separarle;
- **Orari**: per insierire eventuali orari di apertura dell'azienda.

5.4.4 Configurare la modalità di visualizzazione della tastiera PIN

È possibile selezionare due tipi di modalità di visualizzazione della tastiera per l'inserimento del PIN; modalità **Normale** e **Casuale**. Sull'interfaccia web, questo può essere configurato in **Dispositivo > LCD > Modalità tastiera PIN**

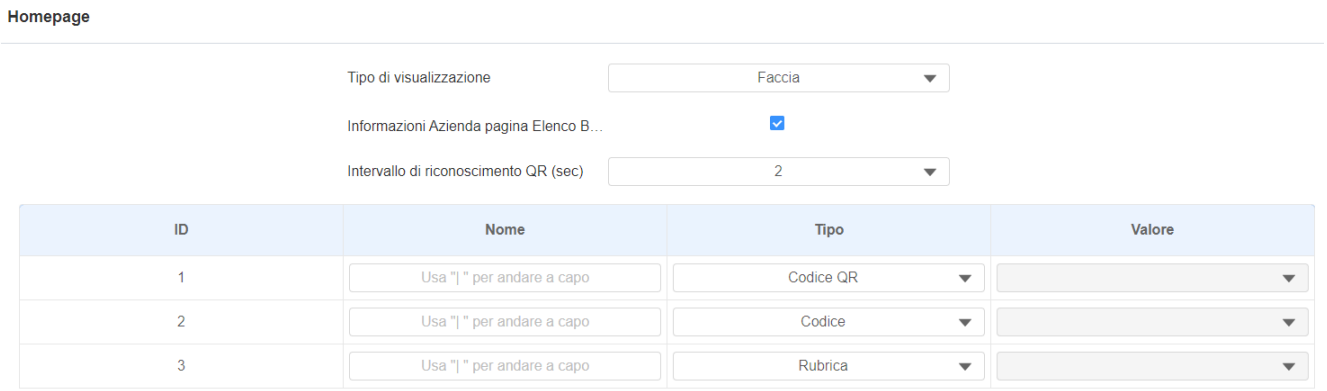
Impostazione parametri:

- **Normale**: la sequenza dei numeri è ordinata da 0 a 9;
- **Casuale**: i numeri sono riportati in modo causale: questo consente di aumentare la sicurezza, in quanto non c'è corrispondena trai numeri e le evenuali impionte digitali lasciate dall'utente autorizzato.



5.4.5 Configurazione della pagina iniziale

Si può modificare la visualizzazione della pagina iniziale configurando il nome delle schede (da 1 a 3 pulsanti) e la loro disposizione. Dall'interfaccia web del dispositivo, selezionare il percorso **Dispositivo > LCD > Homepage**



Impostazione parametri:

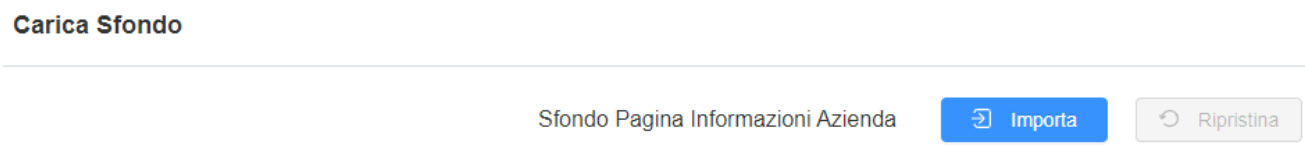
- **Tipo di visualizzazione**: impostabile tra quattro tipi di visualizzazione: **Informazioni sull'azienda**, **Faccia**, **Codice QR, Rubrica breve**. Scegliendo **Codice QR**, la fotocamera del videocitofono è disponibile per inquadrare un codice QR di accesso.

NOTA: scegliendo **Rubrica breve**, vengono visualizzati gli utenti per i quali è stato inserito un numero in Rubrica ed è stato selezionato *Tipo = Rubrica breve* nell'interfaccia web **Rubrica > utente > dettagli del contatto**

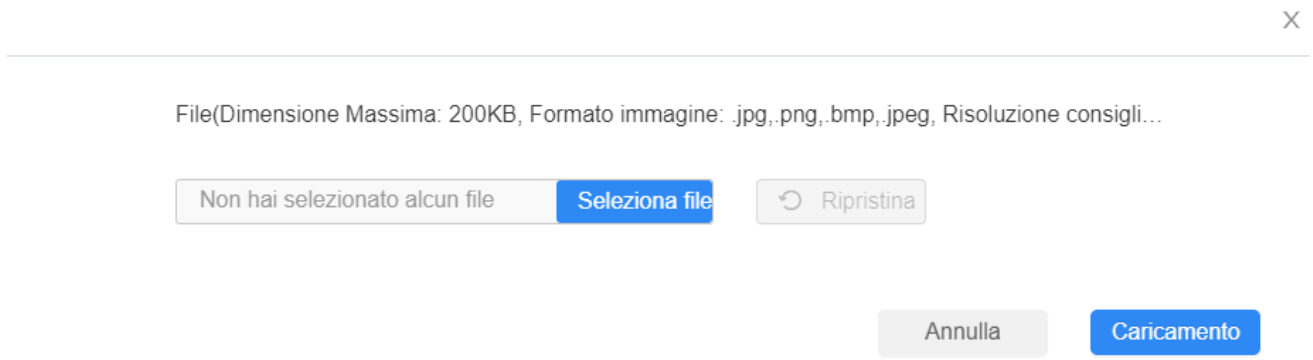
- **Informazioni Azienda pagina Elenco breve utenti**: permette di visualizzare le informazioni dell'azienda, anche scegliendo "Rubrica breve" come tipo di visualizzazione.
- **Intervallo di riconoscimento QR (sec)**: permette di impostare, in secondi, l'intervallo di tempo di riconoscimento tra due codici QR.
- **ID:** indentificativo del tasto
- **Nome**: inserire un nuovo nome per sostituire quello originale, senza cambiare l'attributo del tipo. E' possibile inserire fino a 2 righe, separate dal carattere "|".
- **Tipo**: seleziona il tipo di scheda corrispondente al numero di indice ID, che indica la posizione nella tabulazione. Ad esempio, se si desidera visualizzare la scheda *Chiamata rapida* nella posizione uno, è possibile modificare il tipo per l'indice ID 1 in *Chiamata rapida*. Allo stesso modo per la posizione di un'altra scheda.
- **Valore**: inserire il numero IP o SIP da collegare all'icona per la chiamata rapida. Il numero immesso verrà composto non appena si preme l'icona *Reception* nella schermata iniziale. Questo campo è valido solo per la chiamata rapida. È possibile inserire un massimo di cinque numeri di selezione rapida, tenendo presente che due numeri devono essere separati da ";". È inoltre possibile selezionare un gruppo di contatti da chiamare premendo l'icona *Reception*.

5.4.6 Configurare lo sfondo

È possibile caricare uno sfondo per la pagina Informazioni azienda, dall'interfaccia **Dispositivo > LCD > Carica sfondo**.



Cliccando su **Importa**, permette di selezionare un file immagine da utilizzare come sfondo. La dimensione massima consentità è di 200 kB, il formato può essere .jpg, .jpeg, .bmp, .png.



5.5 Configurazione volume e suoneria

La configurazione del volume e della suoneria nel videocitofono DICO permette di impostare il volume della chiamata (altoparlante), il volume del microfono e il volume delle notifiche (ad es., suono di porta aperta).

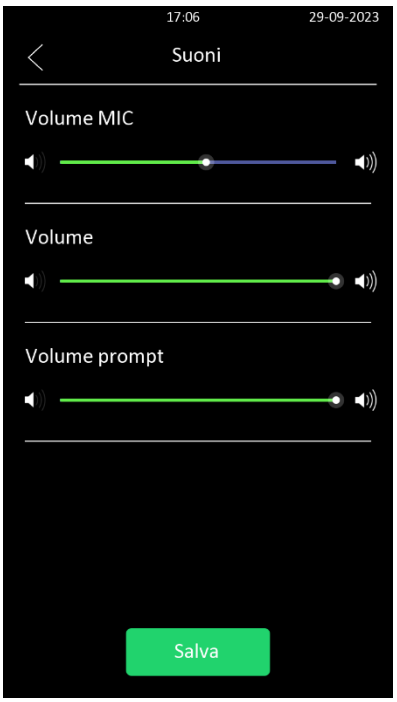
Inoltre, è consentito caricare il suono preferito, per arricchire l'esperienza utente personalizzata.

5.5.1 Configurazione del volume

È possibile configurare il volume del microfono, il volume dell'altoparlante e il volume dell'allarme antimanomissione (tamper) in base alle proprie esigenze di comunicazione audio/video basata su interfono. Inoltre è possibile impostare il volume dell'allarme tamper in caso di rimozione involontaria del citofono.

5.5.1.1 Configurazione del volume dal dispositivo

È possibile regolare il volume del microfono, il volume dell'altoparlante e il volume dei messaggi sul dispositivo. A partire dalla schermata delle impostazioni, premere su **Display e suoni > Suoni**.

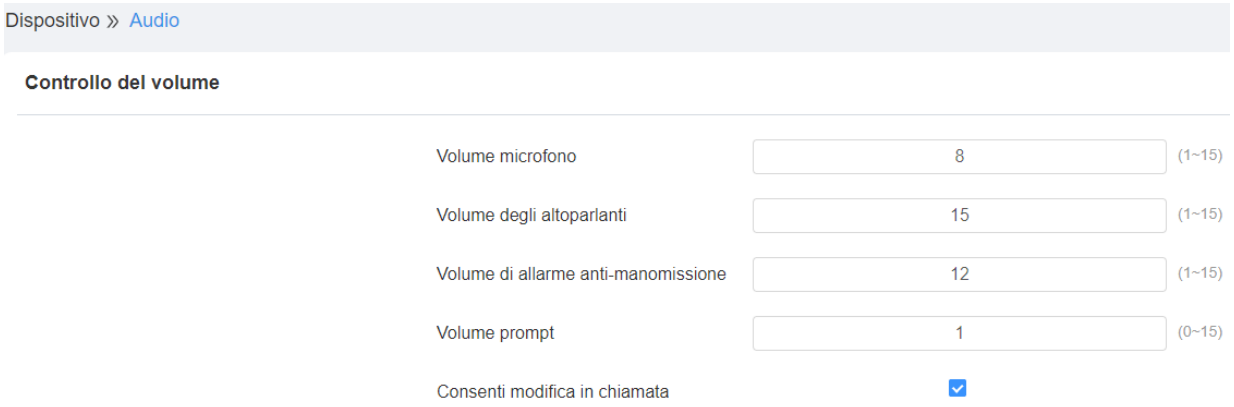


Impostazione parametri:

- **Volume MIC:** per regolare il volume del microfono.
- **Volume:** per regolare il volume dell'altoparlante interno.
- **Volume prompt:** per regolare il volume delle notifiche, che include vari tipi di suono di avviso per l'apertura o meno della porta, richiamata, suono di misurazione della temperatura (ove disponibile), ecc.

5.5.1.2 Configurazione del volume dall'interfaccia web

Nell'interfaccia Web è possibile impostare il volume dell'allarme tamper, il volume del microfono, il volume dell'altoparlante e il volume delle notifiche. Il percorso è **Dispositivo > Audio > Controllo del volume.**

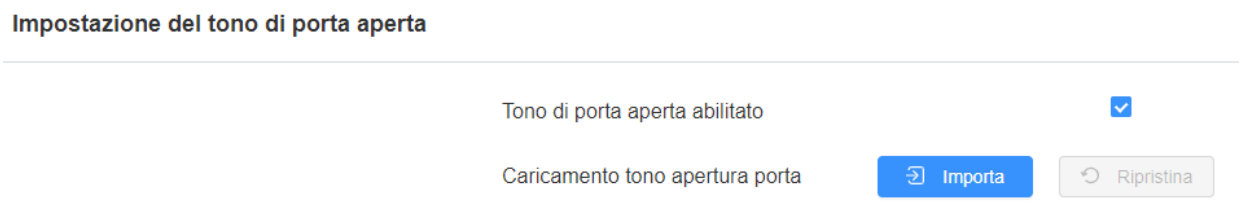


Impostazione parametri:

- **Volume microfono**: per regolare il volume del microfono.
- **Volume degli altoparlanti**: per regolare il volume dell'altoparlante interno.
- **Volume di allarme anti-manomissione**: per regolare il volume dell'allarme tamper.
- **Volume prompt:** per regolare il volume delle notifiche, che include vari tipi di suono di avviso per l'apertura o meno della porta, richiamata, suono di misurazione della temperatura (ove disponibile), ecc
- **Consenti modifica in chiamata:** per abilitare o disabilitare le modifiche durante una chiamata.

5.5.2 Caricamento del tono di apertura porta

È possibile caricare il segnale acustico di porta aperta tramite l'interfaccia web del dispositivo. Il percorso da seguire è **Dispositivo > Audio > Impostazione del tono di porta aperta.**

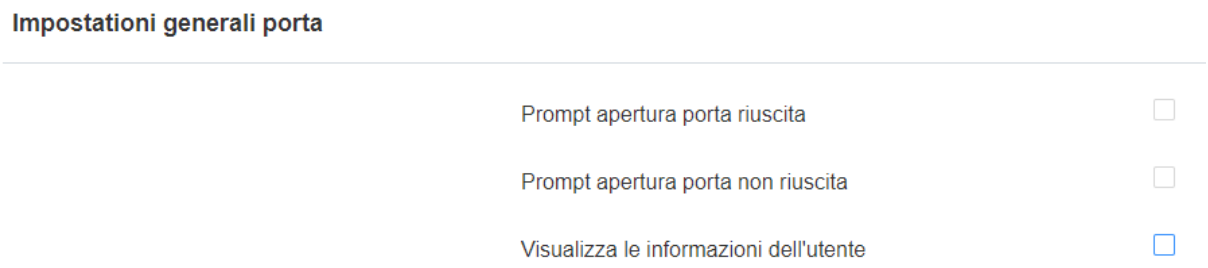


Nota

• Il file del segnale acustico di porta aperta deve essere in formato .wav e la dimensione del file deve essere inferiore a 200 KB.

5.5.3 Configurare il testo della richiesta di accesso alla porta

È possibile abilitare o disabilitare la visualizzazione della richiesta di accesso alla porta sulla schermata del terminale di controllo degli accessi in caso di mancata e riuscita apertura della porta. Questa impostazione è disponibile nell'interfaccia web al link **Controllo accessi > Relè > Impostazioni generali porta.**



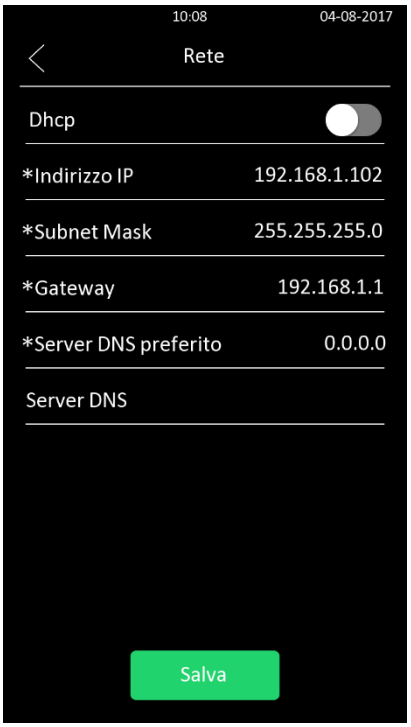
Impostazione parametri:

- **Prompt apertura porta riuscita:** selezionare la casella di controllo se si desidera visualizzare il messaggio di testo dopo l'apertura della porta avvenuta con successo.
- **Prompt apertura porta non riuscita:** selezionare la casella di controllo se si desidera visualizzare il messaggio di testo dopo il fallimento dell'apertura della porta.
- **Visualizza le informazioni dell'utente:** selezionare la casella di controllo se si desidera visualizzare le informazioni sull'utente rilevato.

6. Impostazioni di rete

6.1 Impostazione della connessione di rete dal dispositivo

È possibile selezionare la modalità **DHCP** (Dynamic Host Configuration Protocol) o la connessione **IP statica**. Quando si seleziona la connessione IP statica, è necessario impostare manualmentel'indirizzo IP, la maschera di sottorete, il gateway predefinito e i server DNS.

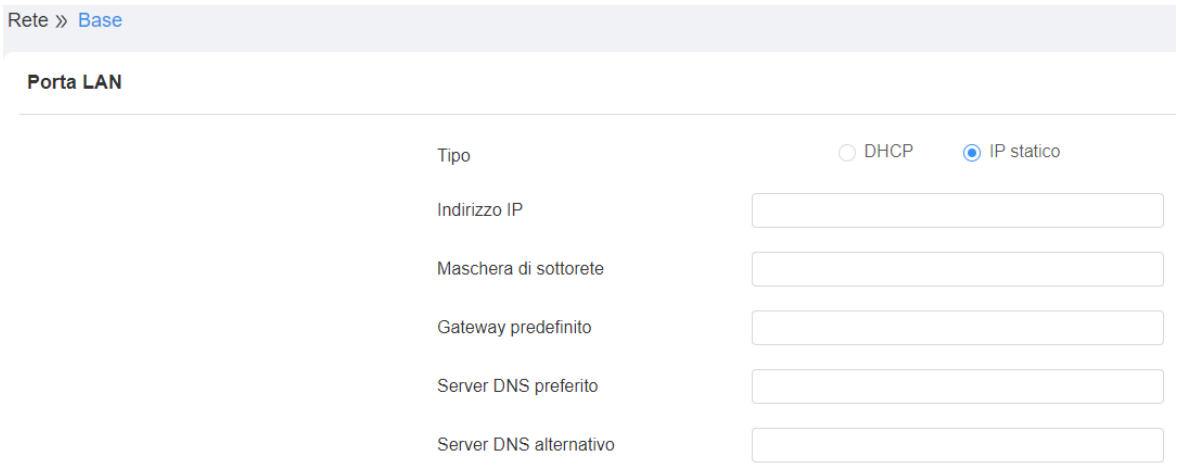


Impostazione parametri:

- **DHCP**: selezionare la modalità DHCP spostando l'interruttore a levetta verso destra. La modalità DHCP è la connessione di rete predefinita. Se la modalità DHCP è attivata, al citofono verranno assegnati automaticamente dal server DHCP l'indirizzo IP, la maschera di sottorete, il gateway predefinito e l'indirizzo del server DNS.
- **IP statico**: selezionare la modalità IP statico spostando l'interruttore a levetta verso sinistra. Quando è selezionata la modalità IP statico, l'indirizzo IP, la maschera di sottorete, il gateway predefinito e l'indirizzo del server DNS devono essere configurati manualmente in base al sistema di rete cui il dispositivo è connesso.
- **Indirizzo IP**: impostare l'indirizzo IP del dispositivo se è selezionata la modalità IP statico.
- **Subnet Mask**: impostare la subnet Mask in base al sistema di rete.
- **Gateway**: impostare l'indirizzo IP del gateway predefinito.

- **Server DNS preferito** e **alternativo**: impostare un server DNS (**Domain Name Server**) preferito e (facoltativamente) uno alternativo, in base all' ambiente di rete. Il server DNS preferito è l'indirizzo del server DNS primario mentre il server DNS alternativo è l'indirizzo del server secondario. Il videocitofono si collegherà al server alternativo quando il server DNS primario non è disponibile.

Per configurare la rete del dispositivo sull'interfaccia web, andare su **Rete > Base > Porta LAN.**



6.2 Distribuzione del dispositivo nella rete

Prima della configurazione, il videocitofono DICO deve essere distribuito nell'ambiente di rete in termini di posizione, modalità operativa, indirizzo e numeri di interno rispetto ad altri apparati per il controllo dei dispositivi e per comodità di gestione.

Per impostare la configurazione da interfaccia web, andare su **Rete > Avanzate > Impostazioni connessione**

Impostazione parametri:

- **Modalità server**: viene impostata automaticamente in base all'effettiva connessione del dispositivo con un server specifico nella rete come **ACMS**, **Cloud** e **Nessuno**. "**Nessuno**" è l'impostazione di fabbrica predefinita che indica che il dispositivo non è in alcun tipo di server, pertanto è possibile scegliere Ekinex Delégo in modalità rilevamento.
- **Modalità Discovery**: abilitare questa impostazione per attivare la modalità di rilevamento del dispositivo in modo che possa essere rilevato da altri dispositivi nella rete, oppure disabilitarla se si desidera nascondere il dispositivo per non essere scoperto da altri dispositivi.
- **Indirizzo del dispositivo**: specificare l'indirizzo del dispositivo inserendo le informazioni sulla posizione del dispositivo da sinistra a destra: Comunità, Unità, Scala, Piano, Stanza in sequenza.
- **Estensione del dispositivo**: inserire il numero di interno del dispositivo installato.
- **Posizione del dispositivo**: inserire la posizione in cui viene installato e utilizzato il dispositivo.

6.3 Impostazioni NAT

Network Address Translation (NAT) è il processo che viene utilizzato per mappare più indirizzi privati locali su indirizzi pubblici prima di trasferire le informazioni. Per facilitare la trasmissione dei dati tra il citofono ed il server SIP sarà necessario impostare il NAT.

Per impostare questi parametri dall'interfaccia web, andare su **Account > Avanzate > NAT**.

Impostazione parametri:

- **Messaggi UDP Keep Alive**: se abilitato, il dispositivo invierà il messaggio al server SIP in modo che il server SIP riconosca se il dispositivo è in stato online.
- **Intervallo di messaggi Alive UDP**: imposta l'intervallo di tempo per l'invio del messaggio in un intervallo da 5 a 60 secondi. Il valore predefinito è 30 secondi.
- **RPort abilitato**: abilita RPort quando il server SIP è in una rete WAN (Wide Area Network).

7. Configurazione chiamata intercomunicante

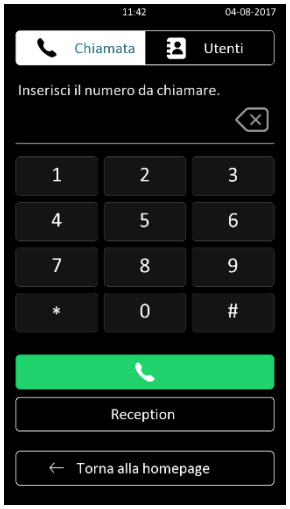
La chiamata intercomunicante nel dispositivo può essere configurata per consentire di eseguire una varietà di chiamate interfono personalizzate come chiamate IP e chiamate SIP per diversi scenari applicativi.

7.1 Chiamata IP e configurazione della chiamata IP

Le chiamate IP possono essere effettuate direttamente dal dispositivo DICO inserendo il numero IP sul dispositivo. E' inoltre possibile disabilitare la chiamata IP diretta, in modo che non venga effettuata alcuna chiamata IP sul dispositivo.

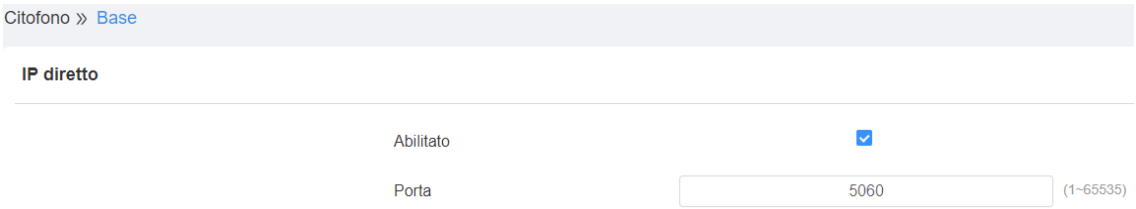
7.1.1 Effettuare chiamate IP

Per effettuare una chiamata IP diretta sul dispositivo, è possibile premere l'icona **Chiamata**, quindi inserire il numero IP o SIP e premere l'icona per chiamare.



7.1.2 Configurazione chiamate IP dall'interfaccia web

Per configurare le chiamate IP dall'interfaccia web, andare al seguente link: **Citofono > Base > IP diretto**



Impostazione parametri:

- **Abilitato**: per abilitare o disabilitare le chiamate IP dirette.

- **Porta** (IP diretta): la porta IP diretta è 5060 per impostazione predefinita, con l'intervallo di porte compreso tra 1 e 65535. Se si immettono valori compresi nell'intervallo ma diversi da 5060, è necessario verificare se il valore immesso è coerente con il valore corrispondente sul dispositivo con cui si desidera stabilire una connessione dati.

7.2 Chiamata SIP e configurazione chiamata SIP

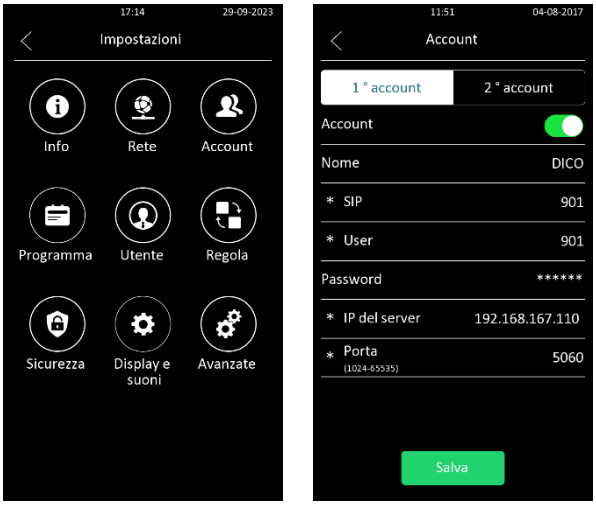
È possibile effettuare una chiamata SIP (**Session Initiation Protocol**) nello stesso modo in cui si effettuano le chiamate IP sul dispositivo. Tuttavia, i parametri delle chiamate SIP relativi all'account, al server e al tipo di trasporto devono essere configurati prima di poter effettuare chiamate di questo tipo sul dispositivo.

7.2.1 Registrazione account SIP

Il dispositivo DICO supporta due account SIP che possono essere tutti registrati in base alle proprie applicazioni. Ad esempio, si può passare da uno all'altro se uno qualsiasi degli account fallisce e diventa non valido. L'account SIP può essere configurato sul dispositivo e sull'interfaccia web del dispositivo.

7.2.1.1 Configurazione account SIP sul dispositivo

Nella schermata **Impostazioni** del dispositivo, selezionare **Account**.

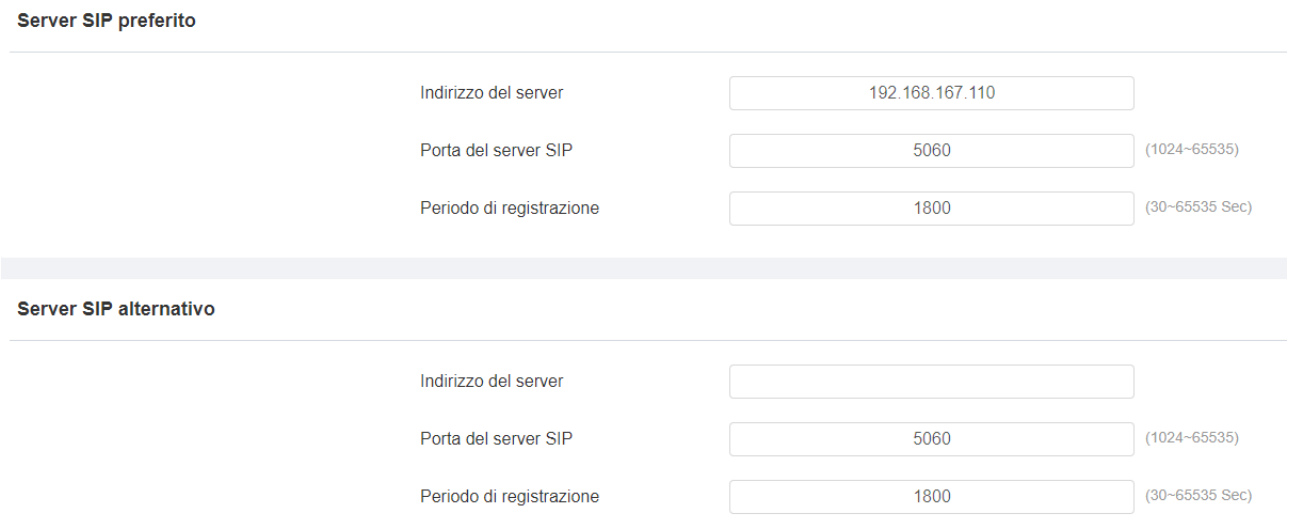


Impostazione parametri:

- **Account**: spostare l’interruttore a scorrimento verso destra per registrare l’account SIP.
- **Nome**: configura il nome, ad esempio l’identificativo da mostrare sul dispositivo chiamato.
- **SIP**: immettere il nome di registrazione dell'account SIP, da richiedere all’amministratore SIP.
- **User**: inserire il nome utente ottenuto dall'amministratore dell'account SIP.
- **Password**: inserire la password ottenuta dall'amministratore dell'account SIP.

7.2.2 Configurazione del server SIP da interfaccia web

È possibile configurare server SIP per i dispositivi, per effettuare sessioni di chiamata tramite server SIP tra apparati intercomunicanti. Per configurare un server SIP, è possibile accedere all'interfaccia web e selezionare **Account > Base > Server SIP preferito.**



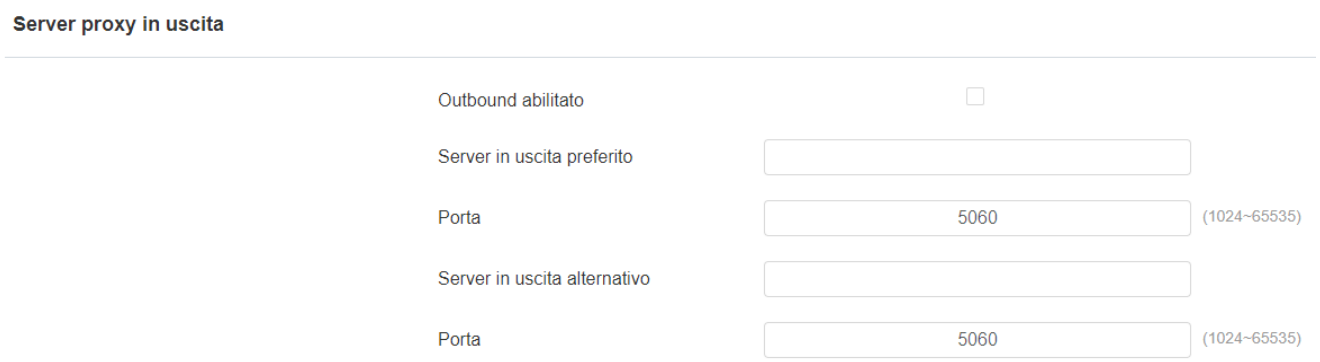
Impostazione parametri:

- **Indirizzo del server (preferito):** immettere il numero dell'indirizzo IP del server primario o il relativo indirizzo IP o dominio.
- **Indirizzo del server (alternativo):** immettere l'indirizzo IP o il dominio del server SIP di backup.
- **Porta del server SIP:** configurare una porta del server SIP per la trasmissione dei dati.
- **Periodo di registrazione:** impostare l'intervallo di tempo di registrazione dell'account SIP. La ri-registrazione SIP verrà avviata automaticamente se la registrazione dell'account non riesce durante il periodo di registrazione. Il valore predefinito è 1800 secondi, ma è possibile inserire altri valori nell'intervallo 30-65535 secondi.

7.2.3 Configurare il server proxy in uscita sull'interfaccia web

Un server proxy in uscita viene utilizzato per ricevere tutti i messaggi di richiesta di avvio e instradarli al server SIP designato, per stabilire una sessione di chiamata tramite trasmissione dati basata sulla porta.

Per configurare il server proxy, è possibile accedere all'interfaccia Web e selezionare **Account > Base > Server proxy in uscita.**



Impostazione parametri:

- **Outbound abilitato:** per abilitare/disabilitare le chiamate in uscita.
- **Server (IP) in uscita preferito:** immettere l'indirizzo SIP del server proxy in uscita.
- **Porta:** immettere il numero di porta per stabilire una sessione di chiamata tramite il server proxy in uscita.
- **Server (IP) in uscita alternativo:** immettere l'indirizzo SIP del server proxy di backup in uscita.
- **Porta:** immettere il numero di porta per stabilire una sessione di chiamata tramite il server proxy di backup in uscita.

7.2.4 Configurare il tipo di trasmissione dati

I messaggi SIP possono essere trasmessi su tre protocolli di trasmissione dati: **UDP** (User Datagram Protocol), **TCP** (Transmission Control Protocol), **TLS** (Transport Layer Security) e **DNS-SRV**. Inoltre è possibile anche identificare il server da cui provengono i dati.

Per eseguire la configurazione, dall'interfaccia web selezionare **Account > Base > Tipo di trasporto**.

Impostazione parametri:

- **UDP**: selezionare UDP per un protocollo del livello di trasporto poco affidabile ma molto efficiente. UDP è il protocollo di trasporto predefinito.
- **TCP**: selezionare TCP per un protocollo del livello di trasporto affidabile ma meno efficiente.

- **TLS**: selezionare TLS per il protocollo del livello di trasporto protetto e affidabile.

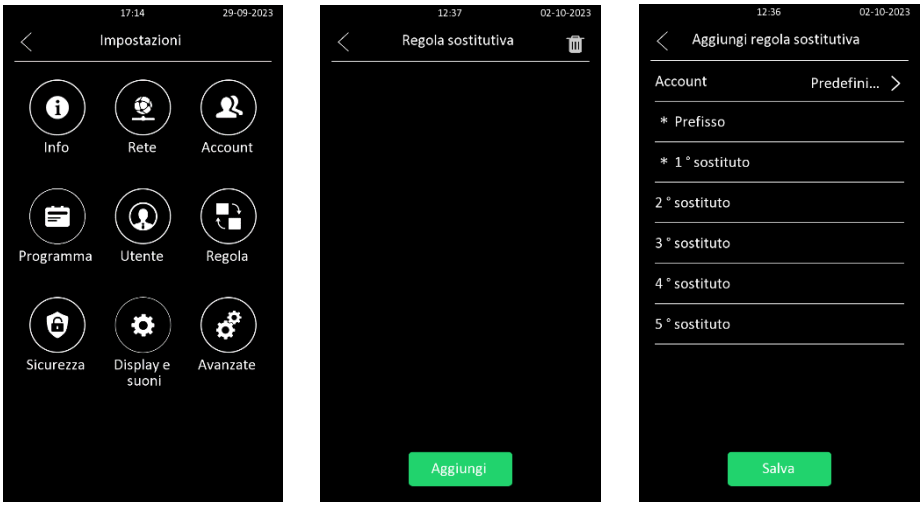
- **DNS-SRV**: selezionare DNS-SRV per ottenere un record DNS per specificare la posizione dei server. SRV non registra solo l'indirizzo del server ma anche la porta del server. Inoltre, SRV può essere utilizzato anche per configurare la priorità e il peso dell'indirizzo del server.

7.3 Configurazione delle opzioni di composizione numeri

Il dispositivo DICO offre diverse opzioni di composizione, per consentire una selezione rapida dai numeri da chiamare, sollevando l'utente dal carico di memoria dovuto alla composizione di numeri lunghi e complessi.

7.3.1 Composizione rapida mediante sostituzione del numero sul dispositivo

È possibile sostituire più numeri di composizione di un dispositivo, come indirizzi IP o numeri SIP, con un solo numero breve. Nella schermata delle impostazioni del dispositivo, selezionare **Regola**, poi cliccare su **Aggiungi**.



Impostazione parametri:

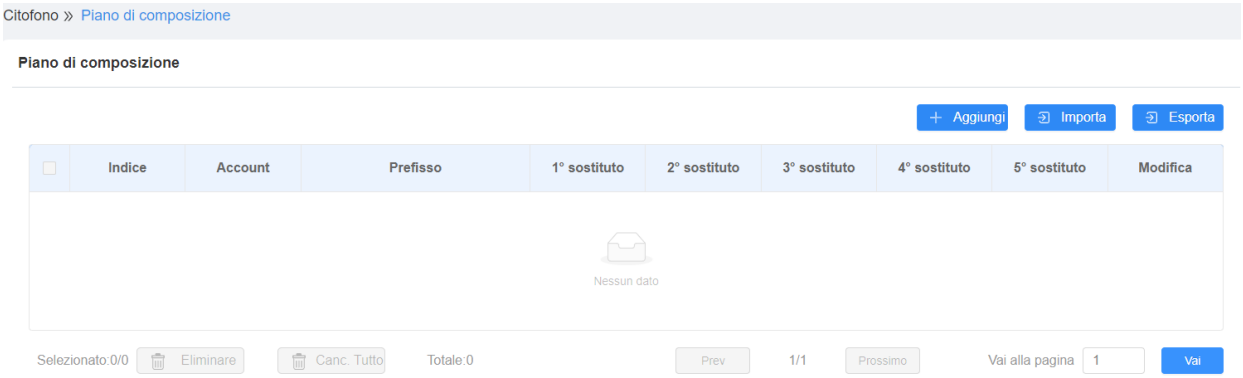
- **Account:** selezionare l'account a cui si desidera applicare la sostituzione del numero di composizione. Per impostazione di default, l'account è **Predefinito** (per effettuare chiamate in uscita dall'account in cui è stato registrato il numero chiamato). È possibile selezionare **Account1** o **Account2** da cui è possibile comporre il numero. Se il numero composto è stato registrato sia in Account1 che in Account2, allora il numero verrà chiamato dall'Account1 di default.

- **Prefisso:** inserire il numero breve per sostituire il numero lungo che si desidera sostituire.

- **1° / 2° / 3° / 4° / 5° sostituto:** inserire il/i numero/i selezionato/i che si desidera sostituire. Supporta fino a un massimo di 5 numeri per la sostituzione della configurazione del dispositivo. Ad esempio, se si sostituiscono cinque numeri composti originariamente con un numero breve comune come 101, i cinque dispositivi interfonici con il numero composto verranno chiamati contemporaneamente quando si compone 101.

7.3.2 Composizione rapida mediante sostituzione del numero da interfaccia web

È possibile sostituire un numero SIP/IP lungo con un numero breve sull'interfaccia web. Per configurarlo, occorre andare su **Citofono > Piano di composizione.**

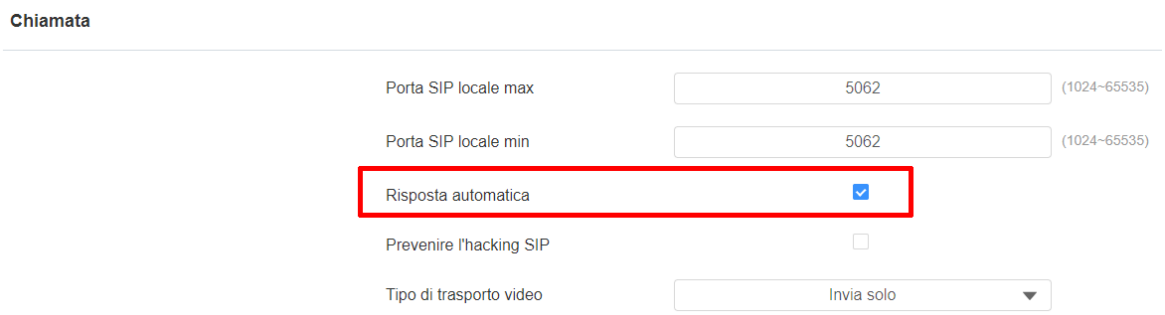


7.4 Configurazione della risposta automatica

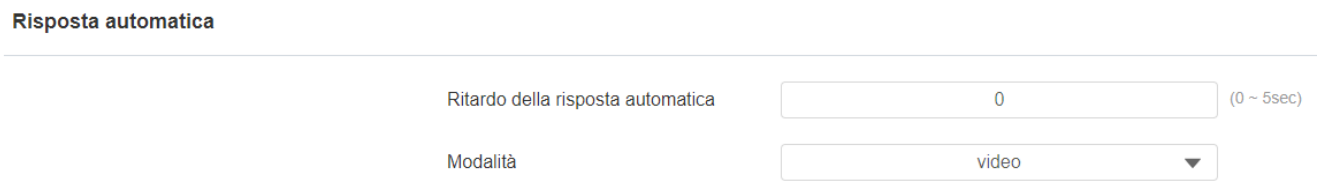
La funzione di risposta automatica consente al videocitofono di rispondere automaticamente alle chiamate in arrivo, ad esempio dal monitor interno del residente, dall'app Smarplus o dal telefono della guardia.

Inoltre, si può selezionare la modalità di risposta automatica audio o video in base alle necessità.

Per abilitare la modalità di risposta automatica da interfaccia web, andare su **Account > Avanzate > Chiamata**.



Per configurare la funzione di risposta automatica, dall'interfaccia web andare su **Citofono > Funzione di chiamata > Risposta automatica.**



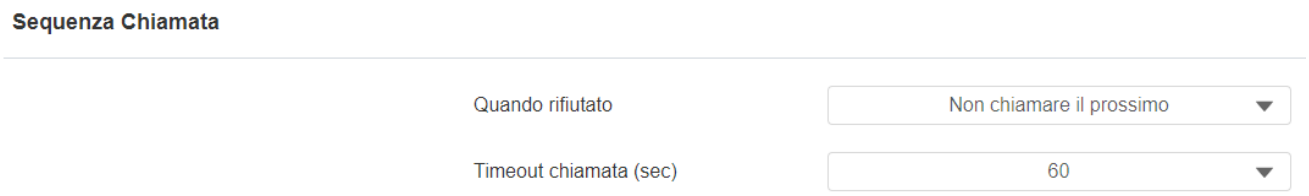
Impostazione parametri:

- **Ritardo della risposta automatica**: imposta il tempo di ritardo (da 0 a 5 secondi) prima di rispondere automaticamente alla chiamata. Ad esempio, se si imposta il tempo di ritardo su 1 secondo, la chiamata riceverà risposta automaticamente entro 1 secondo.
- **Modalità**: imposta la modalità **Video** o **Audio** preferita per la risposta automatica alle chiamate.

7.5 Configurazione delle chiamate in sequenza

È possibile chiamare un gruppo specifico di numeri (ad esempio i numeri di interno della cucina, della camera da letto, ecc.) in ordine sequenziale finché non si riceve risposta alla chiamata. La chiamata in sequenza verrà completata non appena verrà risposto alla chiamata da uno qualsiasi dei dispositivi interni di destinazione.

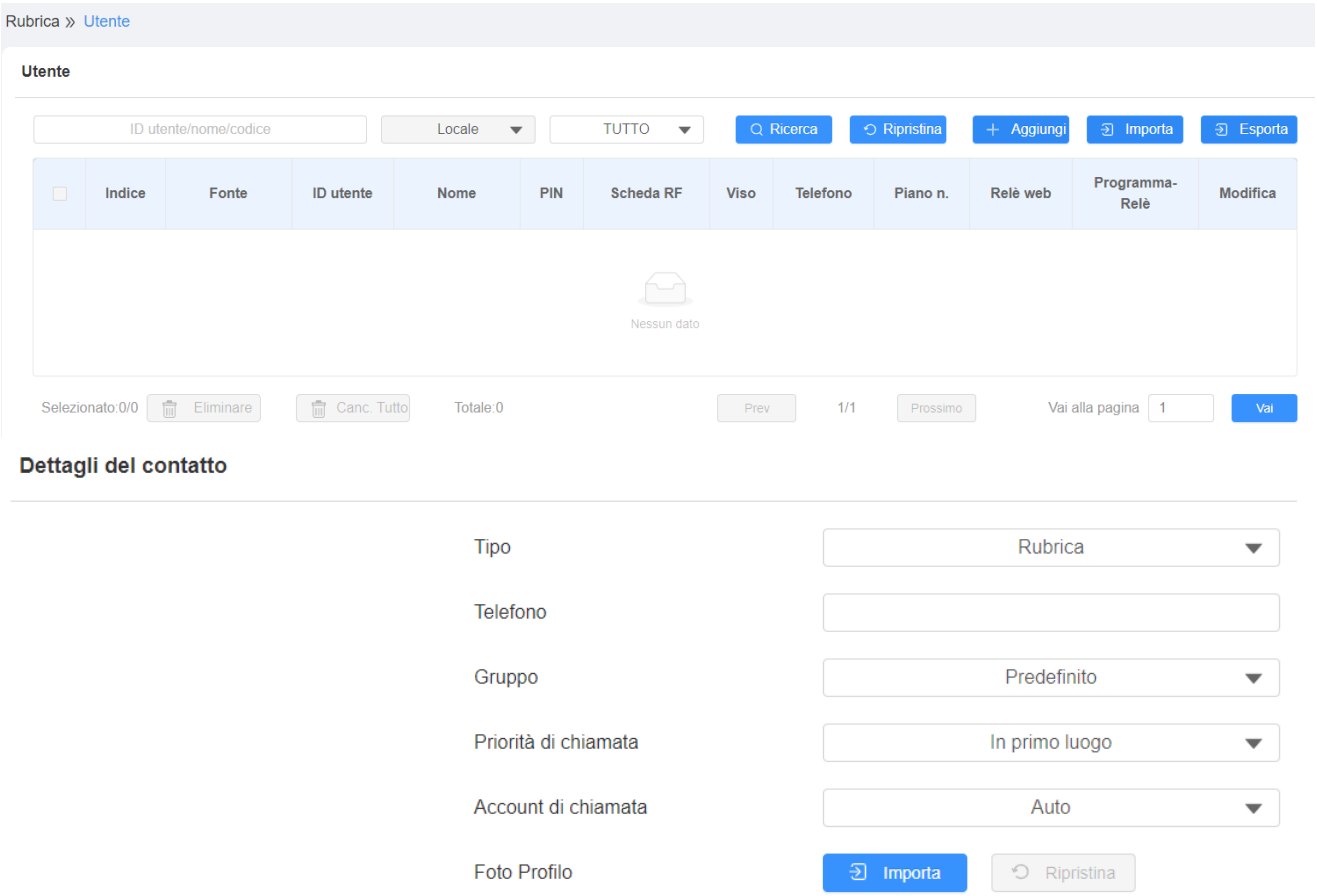
Questa funzione può essere configurata nell'interfaccia web accedendo a **Citofono > Base > Sequenza chiamata.**



Impostazione parametri:

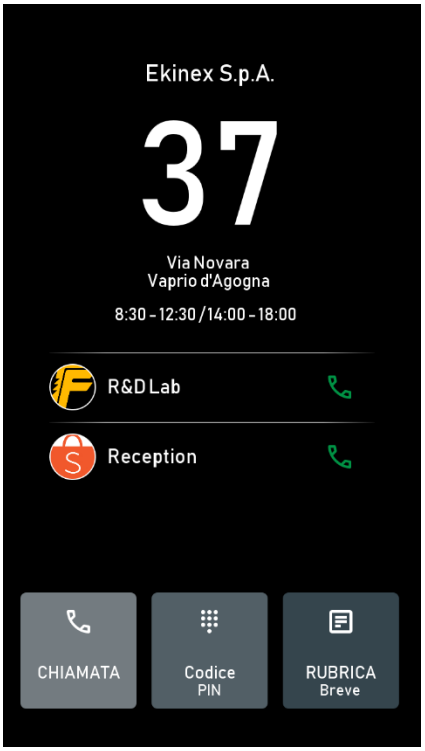
- **Quando rifiutato**: selezionando **Non chiamare il prossimo,** la sequenza verrà interrotta non appena verrà rifiutata una chiamata. Selezionando **Chiama il prossimo**, la chiamata verrà trasferita a quella successiva.
- **Timeout chiamata (sec)**: consente di impostare la durata del tentativo di chiamata tra i numeri di chiamata in sequenza all'interno del gruppo. Ad esempio, se si imposta l'intervallo di tempo su 10 secondi, la chiamata (se non si risponde entro 10 secondi) verrà terminata automaticamente e trasferita in sequenza al numero di chiamata successivo nel gruppo.

Per impostare la sequenza di chiamata, da interfaccia web andare su **Rubrica > Utente > Aggiungi/Modifica > Dettagli del contatto**



Impostazione parametri:

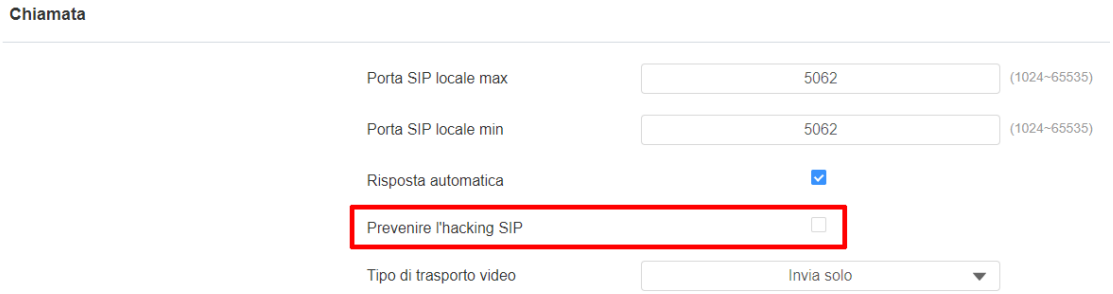
- **Tipo**: per inserire il contatto nella **Rubrica** (quindi con un Gruppo, Priorità di chiamata e Account di chiamata), oppure nella **Rubrica breve**.
- **Telefono**: il numero da chiamare.
- **Gruppo**: consente di assegnare il numero ad un gruppo creato in precedenza.
- **Priorità di chiamata**: assegna una priorità alla chiamata (**in primo luogo**, **secondario**, **ultimo**).
- **Account di chiamata**: consente di selezionare l'account di chiamata (**Automatico**, **Account1**, **Account2**).
- **Foto profilo**, per inserire una foto dell'utente. Cliccando su Importa, permette di selezionare un file immagine da utilizzare come sfondo. La dimensione massima consentità è di 200 kB, il formato può essere .jpg, .jpeg, .bmp, .png.



7.6 Abilitazione della prevenzione dell'hacking SIP

È possibile abilitare la prevenzione dell'hacking SIP in modo che il citofono riceva chiamate solo dai numeri SIP registrati nello stesso server SIP e da contatti aggiunti localmente o sincronizzati da Ekinex Delégo.

Questa funzione può essere configurata nell'interfaccia web accedendo a **Account > Avanzate > Chiamata**



Nota

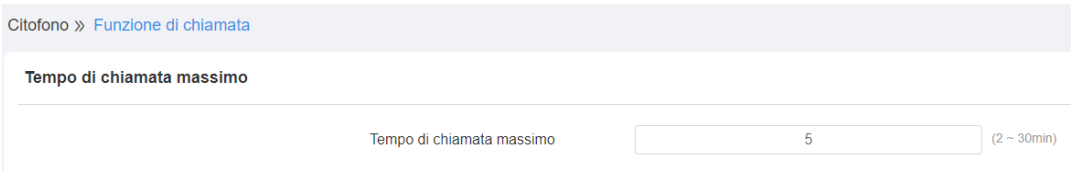
Le chiamate IP dirette verranno bloccate se l'IP diretto è disabilitato.

7.7 Impostazioni di chiamata

7.7.1 Impostazione della durata massima di una chiamata

Il videocitofono DICO consente di impostare la durata massima delle chiamate ricevute. Ciò è utile, in quanto il chiamante potrebbe dimenticarsi di riagganciare. Una volta raggiunta la durata massima della chiamata, il videocitofono terminerà automaticamente la chiamata.

Per personalizzare la configurazione sull'interfaccia web, si può utilizzare il link **Citofono > Funzione di chiamata > Tempo di chiamata massimo**



Impostazione parametri:

- **Tempo di chiamata massimo**: inserire la durata massima desiderata della chiamata (in un intervallo compreso tra 2 e 30 minuti). La durata predefinita della chiamata è 5 minuti.

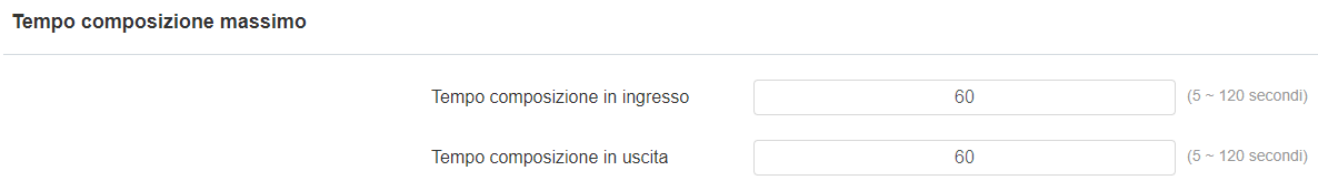
Nota

- La durata massima di chiamata per il dispositivo è correlata anche al tempo massimo di chiamata SIP. Se si utilizza un account SIP per effettuare una chiamata, prestare attenzione al tempo massimo di chiamata del server SIP. Se il tempo massimo di chiamata del server SIP è inferiore al tempo massimo di chiamata del dispositivo, verrà applicato il tempo massimo di chiamata del server SIP.

7.7.2 Setting Impostazione della durata massima della composizione

La durata massima della composizione è costituita dalla durata massima del tempo di chiamata in entrata e dal tempo massimo di chiamata in uscita. Il tempo massimo di chiamata in entrata si riferisce alla durata massima del tempo prima che il citofono ricevente riagganci la chiamata, se il citofono non risponde alla chiamata. Al contrario, per tempo massimo di chiamata in uscita si intende il tempo massimo trascorso prima che il citofono riagganci automaticamente quando la chiamata effettuata dal citofono non riceve risposta dall'apparecchio chiamato.

La configurazione può essere effettuata via interfaccia web in **Citofono > Funzione di chiamata > Tempo composizione massimo.**



Impostazione parametri:

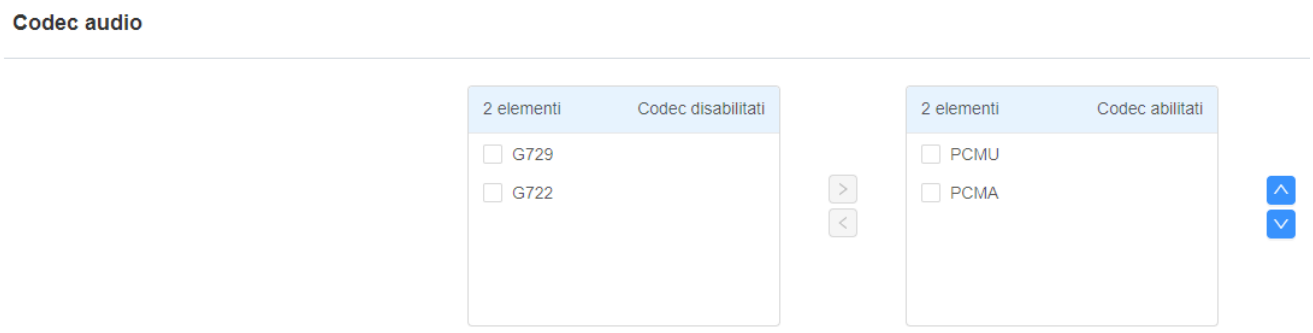
- **Tempo composizione in ingresso:** immettere la durata del tempo di connessione per il citofono (compreso tra 5 e 120 secondi). Ad esempio, se si imposta la durata del tempo di connessione su 60 secondi nel citofono, questo riaggancerà automaticamente la chiamata in arrivo se questa non viene accettata entro 60 secondi. Per impostazione predefinita, la durata del tempo di connessione è di 60 secondi.
- **Tempo composizione in uscita**: immettere la durata del tempo di connessione in uscita per il videocitofono (compreso tra 5 e 120 secondi). Ad esempio, se si imposta la durata del tempo di composizione in uscita su 60 secondi nel videocitofono, questo riaggancerà la chiamata composta automaticamente se non riceve risposta dal dispositivo chiamato entro 1 minuto.

7.7.3 Configurazione codec audio/video per chiamate SIP

7.7.3.1 Configurazione codec audio

Il videocitofono DICO supporta quattro tipi di Codec (**PCMU**, **PCMA**, **G729**, **G722**) per la codifica e decodifica dei dati audio durante la sessione di chiamata. Ogni tipo di codec si differenzia in termini di qualità del suono. È possibile selezionare il codec specifico con diverse larghezze di banda e frequenze di campionamento in modo flessibile in base all'ambiente di rete reale.

Per configurare il codec Audio dall'interfaccia web, andare in **Account > Avanzate > Codec Audio.**



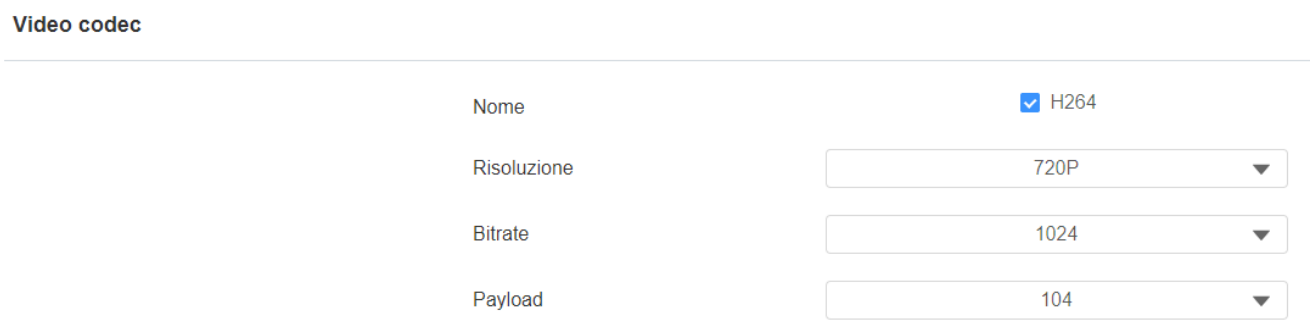
Fare riferimento alla larghezza di banda e alla frequenza di campionamento per i quattro tipi di codec come indicato nella tabella seguente:

Tipo codec	Larghezza di banda	Frequenza di campionamento
PCMA	64 kbit/s	8kHZ
PCMU	64 kbit/s	8kHZ
G729	8 kbit/s	8kHZ
G722	64 kbit/s	16kHZ

7.7.3.2 Configurazione codec video

Il videocitofono DICO supporta il codec H.264, che fornisce una migliore qualità video con un bit rate molto più basso, con qualità video e payload diversi.

Per impostare la configurazione tramite l'interfaccia web, andare su **Account > Avanzate > Codec video.**



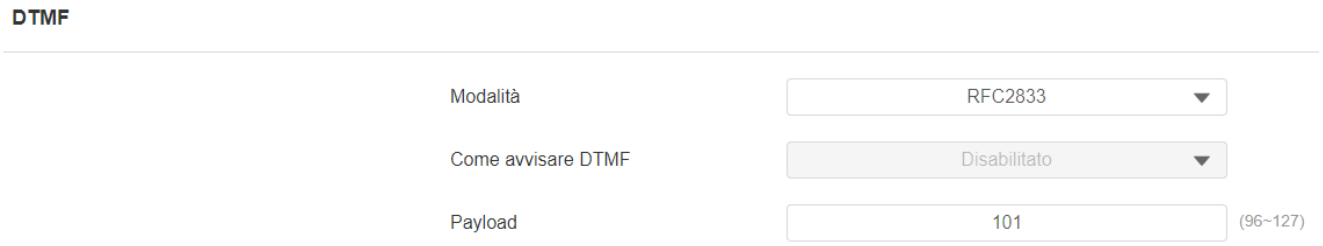
Impostazione parametri:

- **Nome**: spuntare per selezionare il formato del codec video H264 per il citofono. H264 è il codec video predefinito.
- **Risoluzione:** selezionare la risoluzione della codifica per la qualità video tra cinque opzioni: **QCIF**, **CIF**, **VGA**, **4CIF** e **720P**, in base al sistema di rete. La risoluzione del codice predefinita è 720P.
- **Bitrate:** selezionare il bitrate del flusso video (compreso tra 320 e 2048 bit/s). Maggiore è il bitrate, maggiore sarà la quantità di dati trasmessi ogni secondo, quindi il video risulterà più nitido. Il valore predefinito per il bitrate della codifica è 2048 bit/s.
- **Payload:** selezionare il tipo di payload (compreso tra 90 e 118) per configurare il codec audio. Il payload del videocitofono e del corrispondente dispositivo interfonico deve essere identico. Il valore predefinito per il payload è 104.

7.8 Configurazione della trasmissione dati DTMF

Per ottenere l'accesso alla porta tramite codice DTMF o altre applicazioni, è necessario configurare correttamente i parametri DTMF. Così facendo si potrà stabilire una trasmissione dati basata su DTMF tra il videocitofono e altri dispositivi interfonici, per l'integrazione di terze parti.

Per configurare la trasmissione dei dati DTMF tramite l'interfaccia web, andare su **Account > Avanzate > DTMF.**



Impostazione parametri:

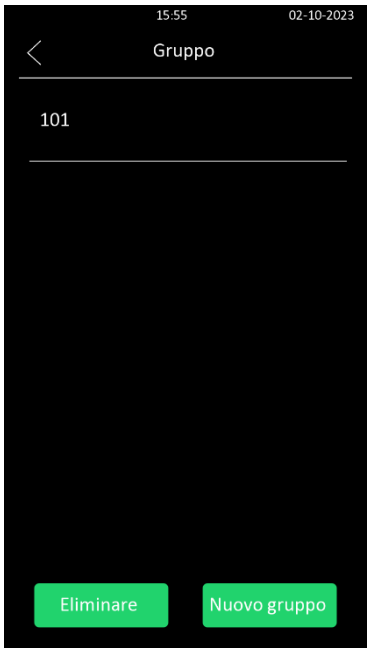
- **Modalità:** selezionare la modalità DTMF fra cinque opzioni: **Inband**, **RFC2833**, **Info+Inband, Info+RFC2833** and **Info+Inband+RFC2833** in base al tipo di trasmissione DTMF specifico del dispositivo di terze parti da abbinare come destinatario per la ricezione dei dati del segnale.
- **Come avvisare DTMF:** selezionare fra quattro opzioni: **Disabilitato**, **DTMF**, **DTMF-Relay**, o **Telephone-Event** in base alla specifica tipologia adottata dal dispositivo di terze parti. È necessario configurarlo solo quando la modalità del dispositivo di terze parti include un'opzione Informazioni (vedere il parametro precedente).
- **Payload**: impostare il payload della trasmissione dati DTMF in base al payload di trasmissione dati specifico concordato tra il mittente e il destinatario.

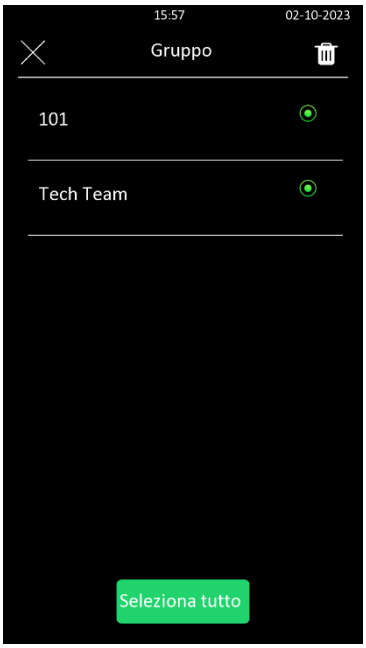
8. Configurazione rubrica

8.1 Configurazione rubrica sul dispositivo

DICO consente di configurare un elenco di contatti, con la possibilità di aggiungere e/o modificare gruppi di contatti o singoli contatti direttamente sul dispositivo.

Per configurare la rubrica del dispositivo, accedere alla pagina **Impostazioni** e selezionare **Utente > Gruppo**.

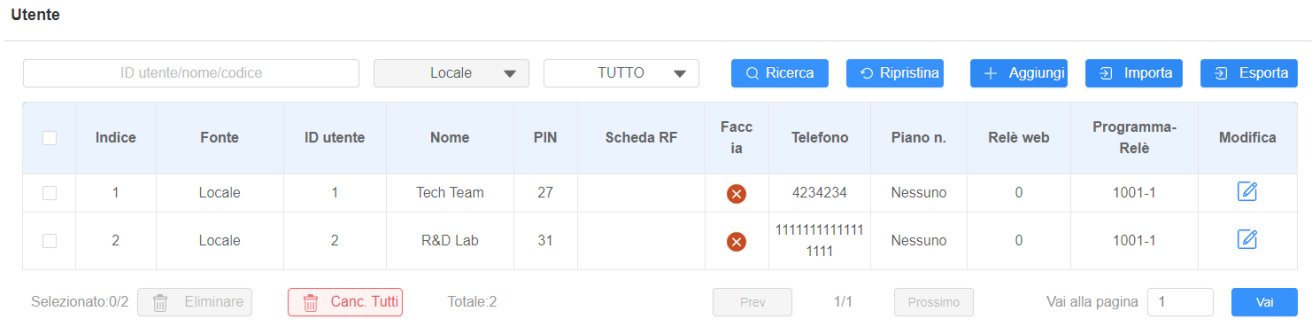




8.2 Configurazione rubrica da interfaccia web

8.2.1 Gestione dei contatti da interfaccia web

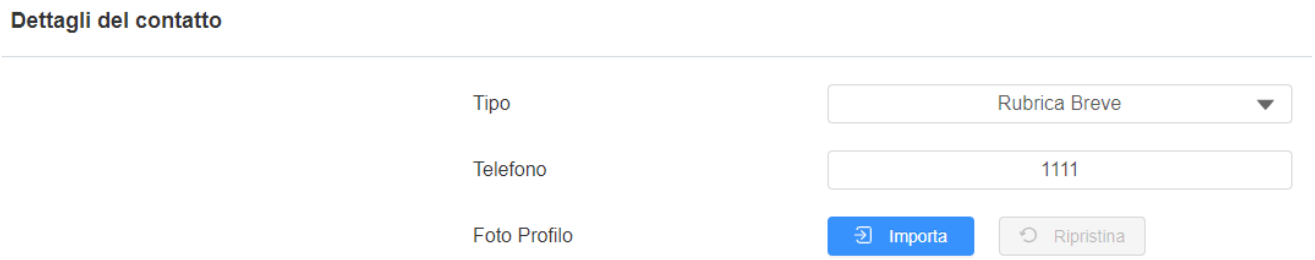
È possibile configurare i singoli contatti aggiungendoli e modificandoli sull'interfaccia web in **Rubrica > Utente > Utente.**



Cliccando su "**Aggiungi**", si accede all'interfaccia per creare un nuovo contatto utente.

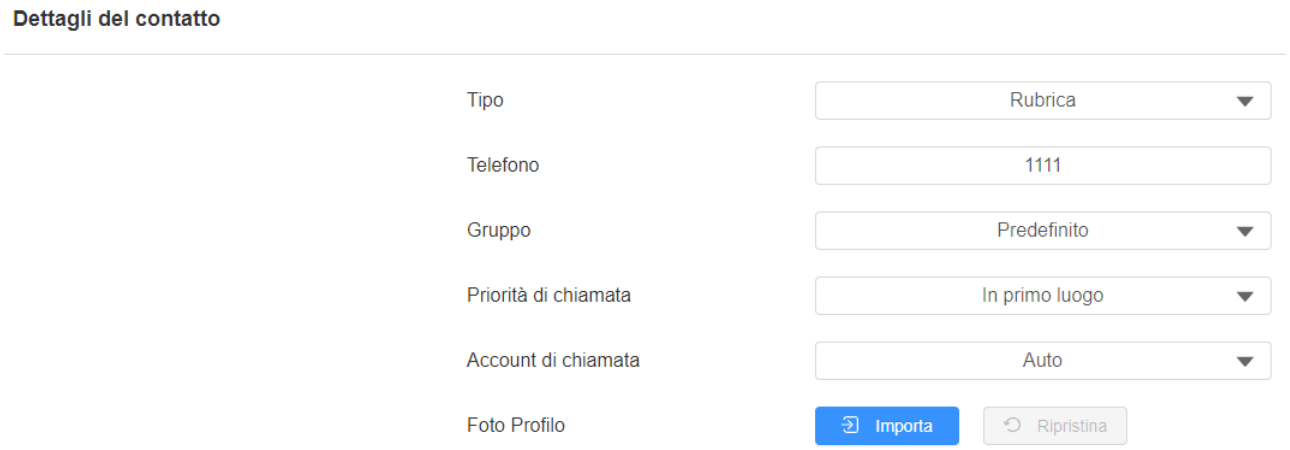
Nella sezione **Dettagli del contatto**, si possono inserire i seguenti parametri.

- **Tipo**: a scelta tra **Rubrica** (accessibile dal pulsante Inquilini sul display) e **Rubrica breve** (il contatto sarà visualizzato in Homepage)
- **Telefono**: il numero telefonico del contatto
- **Foto profilo**: per inserire una foto del contatto.



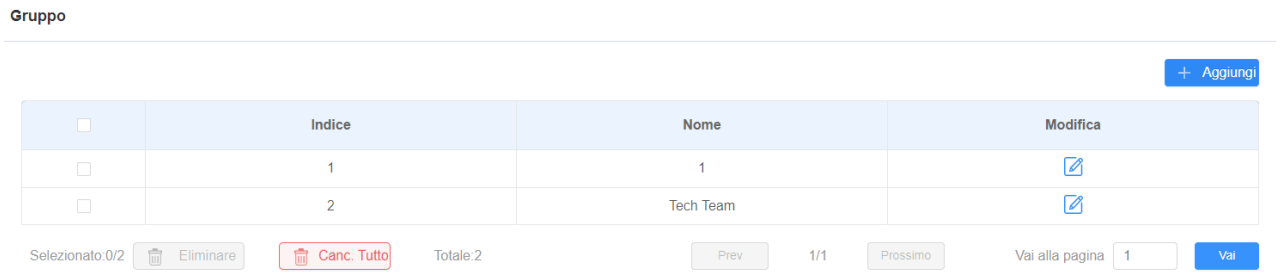
Selezionando *Tipo* = *Rubrica*, sono accessibili anche i seguenti parametri:

- **Gruppo**: per assegnare un gruppo di appartenenza al contatto
- **Priorità di chiamata**: a scelta fra **In primo luogo** (l'utente verrà chiamato per primo), **Secondario** oppure **Da ultimo**.
- **Account di chiamata**: a scelta tra **Auto**, oppure un account a scelta tra **Account1** o **Account2**.

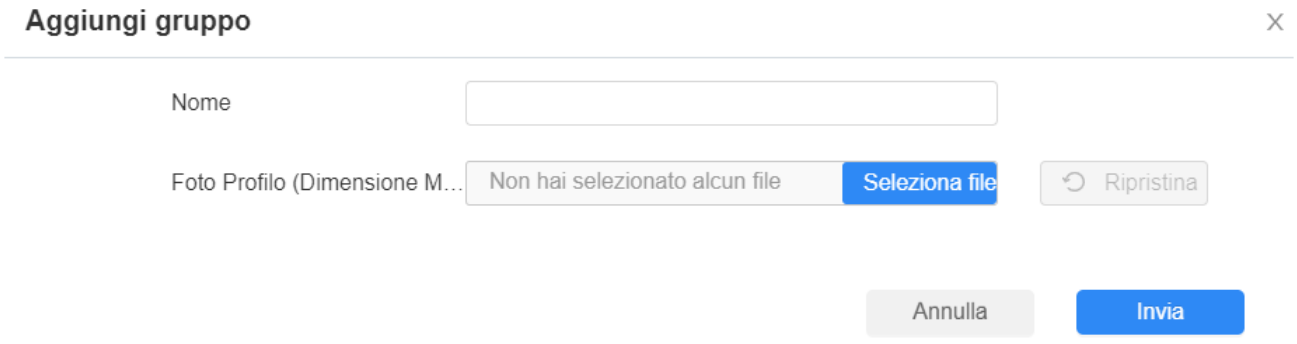


8.2.2 Gestione dei gruppi di contatti da interfaccia web

È possibile configurare gruppi di contatti aggiungendoli e modificandoli sull'interfaccia web in **Rubrica > Utente > Gruppo.**

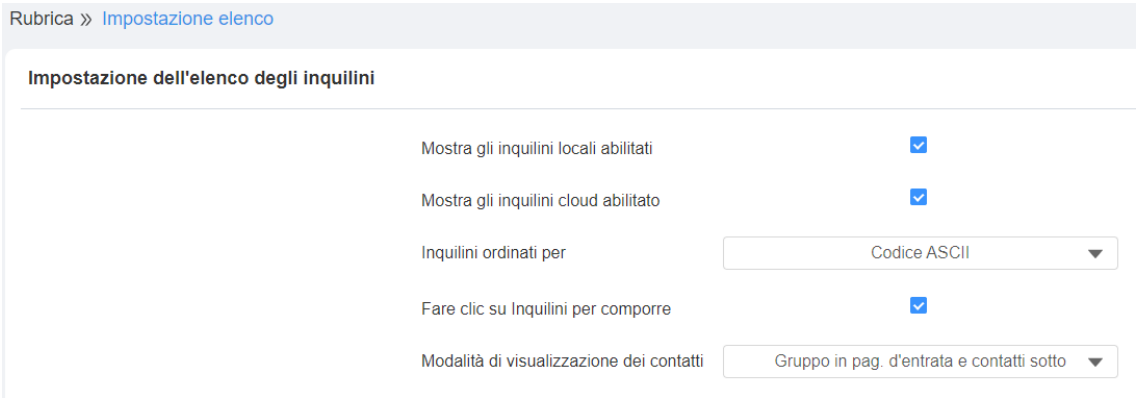


Cliccando su "**Aggiungi**", si accede all'interfaccia per creare un nuovo gruppo, inserendo il **Nome** ed eventualmente una **Foto profilo** (logo immagine):



8.2.3 Gestione delle impostazioni di visualizzazione dell'elenco dei contatti

Se si desidera personalizzare la visualizzazione dell'elenco dei contatti in base alle proprie preferenze visive, da interfaccia web andare su **Rubrica > Impostazione elenco > Impostazione dell'elenco degli inquilini.**



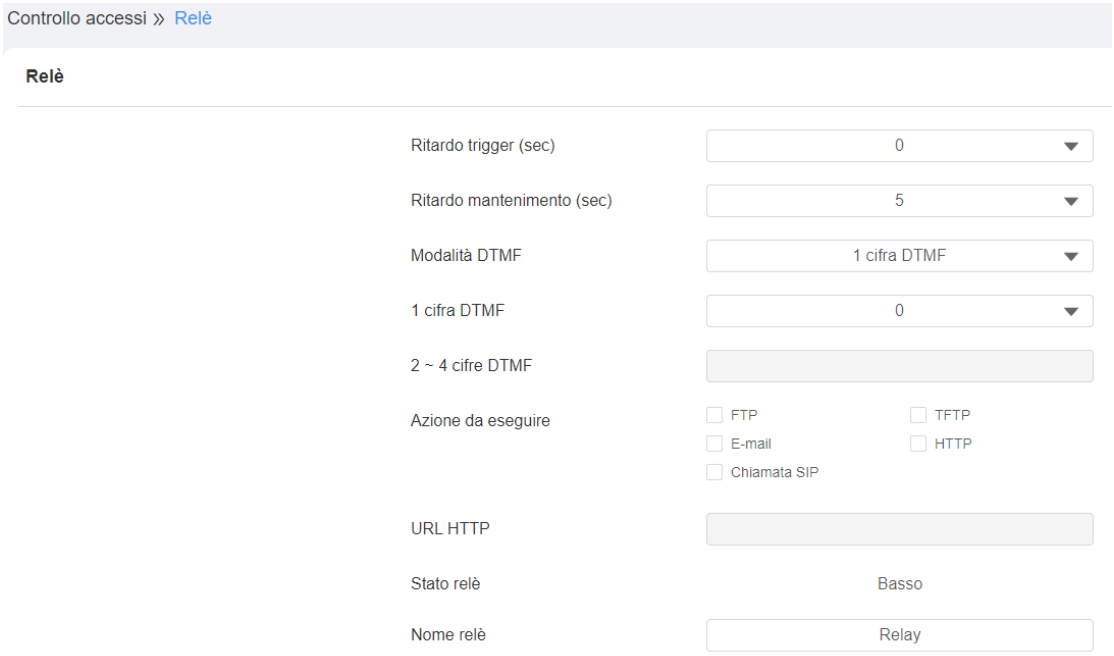
Impostazione parametri:

- **Mostra gli inquilini locali abilitati:** selezionare o deselezionare la casella di controllo per gestire la visualizzazione dell'etichetta del gruppo. Se si deseleziona la casella di controllo, verrà visualizzata solo la scheda del gruppo mentre la scheda dei contatti verrà nascosta e viceversa.
- **Mostra gli inquilini cloud abilitati:** selezionare la casella di controllo per mostrare gli inquilini cloud nell'elenco degli inquilini. Se si deseleziona la casella di controllo, gli inquilini cloud verranno nascosti.
- **Inquilini ordinati per:** selezionare tra le opzioni **Codice ASCII**, **Stanza No.** o **Importa**. Quando si seleziona “Codice ASCII”, gli inquilini verranno elencati in base ai loro nomi nella sequenza del codice ASCII. Quando si seleziona “N. stanza”, gli inquilini verranno ordinati in base al numero di stanza. Ciò è applicabile ai contatti locali e ai contatti sincronizzati dal cloud con Ekinex Delégo App.
- **Fare click su inquilini per comporre:** selezionare la casella di controllo per abilitare la possibilità di effettuare una chiamata in uscita premendo la scheda del contatto. Quando questa funzione è abilitata, è possibile premere un punto qualsiasi della scheda dei contatti per effettuare la chiamata. Questa funzione sarà disabilitata quando si deseleziona la casella di controllo e, quando è disabilitata, è necessario premere l'icona Chiama al centro della scheda per effettuare la chiamata.
- **Modalità di visualizzazione dei contatti:** le opzioni sono **Solo gruppi**, **Tutti i contatti** o **Gruppo in pag. d’entrata e contatti sotto**. Se si seleziona “Solo gruppi”, basta premere sul nome del gruppo per chiamare tutti i suoi contatti. Il nome del gruppo viene visualizzato durante la chiamata.

9. Impostazione del relè

9.1 Impostazione del relè

Gli interruttori relè e la modalità DTMF per l'accesso alla porta possono essere configurati nell'interfaccia web su **Controllo accessi > Relè > Relè.**



Impostazione parametri:

- **Ritardo trigger (sec):** imposta il ritardo di attivazione del relè (in un intervallo compreso tra 1 e 10 secondi). Ad esempio, se si imposta il tempo di ritardo su 5 secondi, il relè non verrà attivato fino a 5 secondi dopo aver premuto il pulsante di sblocco.
- **Ritardo mantenimento (sec):** imposta il tempo di attivazione del relè (nell'intervallo compreso tra 1 e 10 secondi). Ad esempio, se si imposta il ritardo di mantenimento su 5 secondi, il relè rimarrà attivato per 5 secondi dopo l'apertura della porta. Ciò significa che la porta rimarrà aperta per 5 secondi.
- **Modalità DTMF:** selezionare il numero di cifre DTMF per il controllo dell'accesso alla porta (da 1 a 4 cifre). Ad esempio, è possibile selezionare un codice DTMF a 1 cifra o un codice DTMF a 2 cifre, ecc., in base alle proprie necessità.
- **1 cifra DTMF:** imposta il codice DTMF a 1 cifra nell'intervallo compreso tra (0-9 e *, #).

- **2~4 cifre DTMF:** impostare il codice DTMF in base all'opzione selezionata in “Modalità DTMF”. Ad esempio, è necessario impostare il codice DTMF a 3 cifre se la modalità DTMF è impostata su “3 cifre DTMF”.
- **Azione da eseguire:** è possibile selezionare un'azione dopo l'attivazione del relè (invio FTP, e-mail, chiamata SIP, TFTP o HTTP).
- **URL HTTP:** se come “Azione da eseguire” è selezionato “HTTP”, è necessario aggiungere in questo campo l'URL da chiamare.
- **Stato relè: p**er impostazione predefinita, lo stato del relè è basso, ovvero normalmente chiuso (NC). Se lo stato del relè è alto, allora è nello stato normalmente aperto (NO).
- **Nome relè:** permette di assegnare un nome all'interruttore relè in base alle proprie necessità. Ad esempio, è possibile denominare l'interruttore relè in base alla posizione in cui si trova.

Nota

- Solo i dispositivi esterni collegati all'interruttore relè devono essere alimentati, poiché l'interruttore relè non fornisce alimentazione.

Nota

- Se la modalità DTMF è impostata su “1 cifra DTMF”, non è possibile modificare il codice DTMF nel campo “2-4 cifre DTMF”. Analogamente, se si imposta la modalità “DTMF a 2-4 cifre” nel campo “Modalità DTMF”, non è possibile modificare il codice DTMF nel campo “1 cifra DTMF”.

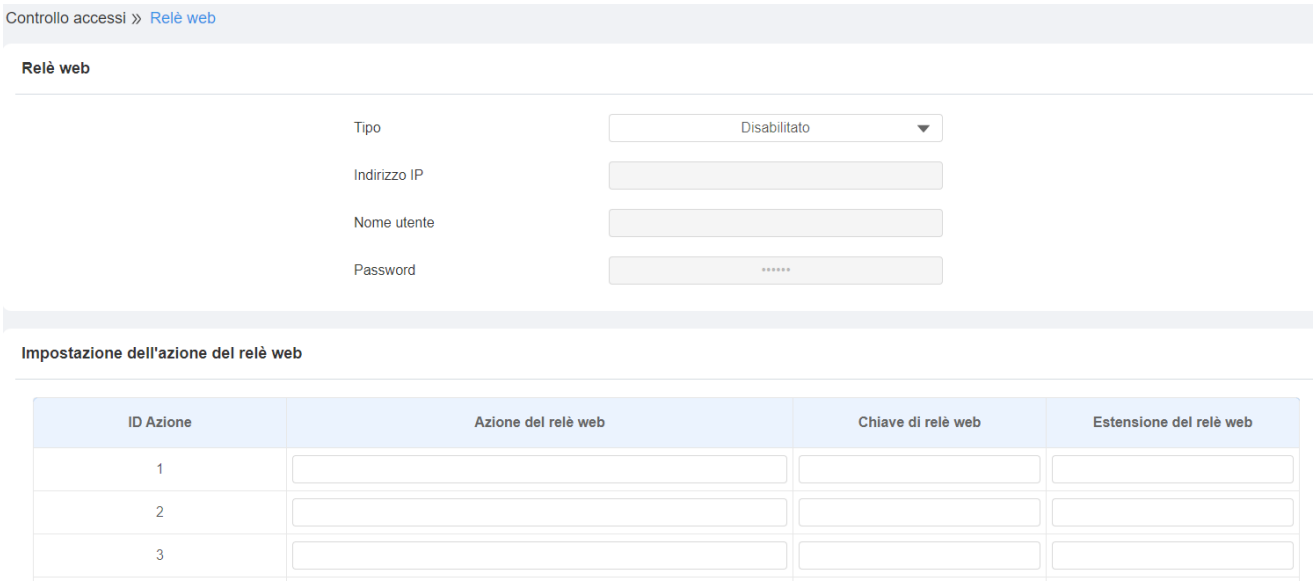
9.2 Impostazione relè web

Oltre al relè collegato al videocitofono, è possibile controllare l'accesso alla porta anche utilizzando il relè web basato sulla rete sul dispositivo e configurabile sull'interfaccia web del dispositivo.

9.2.1 Configurazione del relè web da interfaccia web

Il relè web deve essere configurato sull'interfaccia web. È necessario inserire informazioni quali indirizzo IP di inoltro e password. È inoltre possibile inserire un massimo di 50 comandi di azione di inoltro web per eseguire diversi comandi, che possono essere successivamente selezionati sullo schermo del dispositivo per il controllo dell'accesso alla porta.

Queste impostazioni sono disponibili nel seguente percorso: **Controllo accessi > Relè web.**



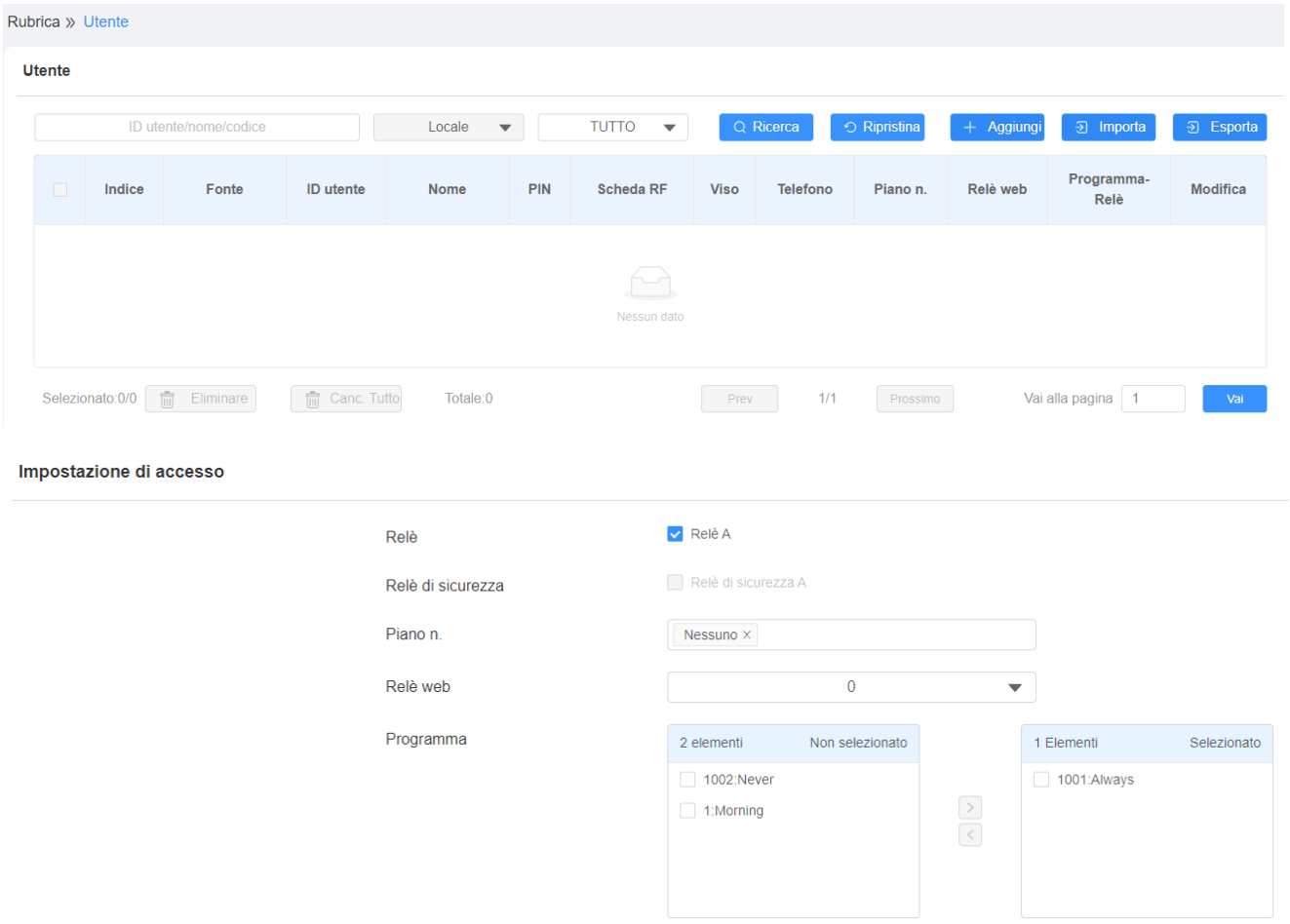
Impostazione parametri:

- **Tipo:** sono disponibili tre opzioni: **Disabilitato**, **Relè web** and **Relè locale+Relè web.** Selezionare **Relè web** per abilitare questa funzione, **Disabilitato** per escluderla. Selezionare **Relè locale+Relè web** per abilitare sia il relè locale che quello web. Se si sceglie "**Relè web**", il relè locale non sarà attivo.
- **Indirizzo IP:** immettere l'indirizzo IP del relè Web fornito dal produttore del relè Web.
- **Nome utente**: inserire il nome utente fornito dal produttore del relè web.
- **Password:** inserire la password fornita dal produttore del relè web. Le password vengono autenticate tramite HTTP ed è possibile definire le password utilizzando l'azione **http get.**
- **Azione del relè web:** immettere il comando specifico fornito dal produttore del relè, per le diverse azioni del relè web.
- **Chiave di relè web:** inserire il codice DTMF per la configurazione. Quando la porta viene sbloccata tramite il codice DTMF, il comando verrà inviato automaticamente al relè web.
- **Estensione del relè web:** inserire la relativa estensione del comando, ove disponibile.

Dopo aver configurato il relè web, è possibile selezionare l'azione specifica del relè web da eseguire.

Andare su **Rubrica > Utente,** poi cliccare su 

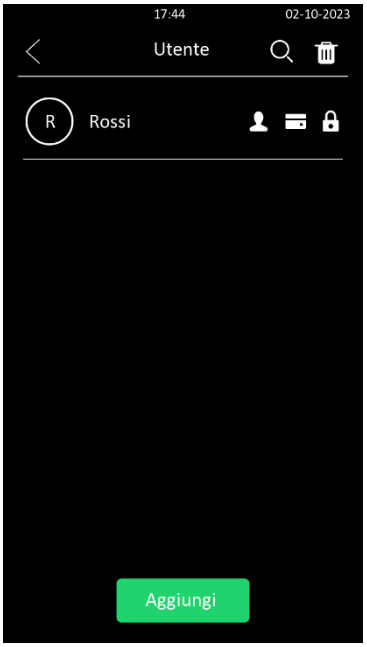
, infine spostarsi verso il basso su **Impostazione di accesso.**



9.2.2 Configurazione del relè web da dispositivo

Dopo aver inserito i comandi del relè web nell'interfaccia web, è possibile selezionare il numero di azioni che uno specifico utente può eseguire per lo sblocco della porta.

Per configurarlo, aprire la pagina **Impostazioni** sul dispositivo e selezionare **Utente > Elenco utenti.**

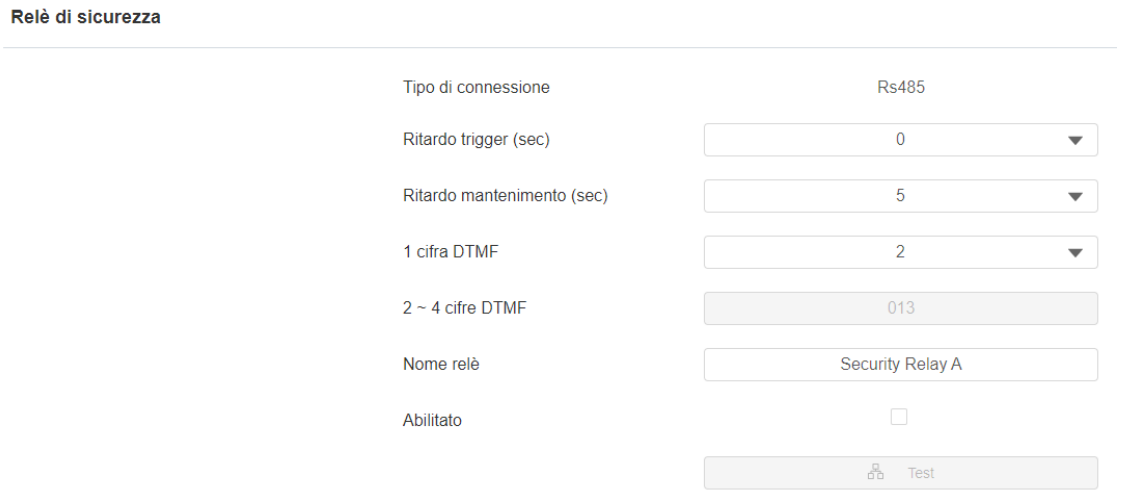


9.3 Relè di sicurezza

Il relè di sicurezza del videocitofono DICO è collegato alla serratura tramite il dispositivo stesso. Si installa all'interno della porta e funge da protezione aggiuntiva contro lo sblocco forzato della porta tramite manomissione del citofono. Il relè di sicurezza è consigliato in applicazioni che richiedono un livello di sicurezza più elevato.

Il modello consigliato è il prodotto ekinex **EK-SR1-VI**, da collegare esclusivamente alla porta RS485.

Per impostare il relè di sicurezza, accedere a **Controllo accessi > Relè > Relè di sicurezza** nell'interfaccia web.

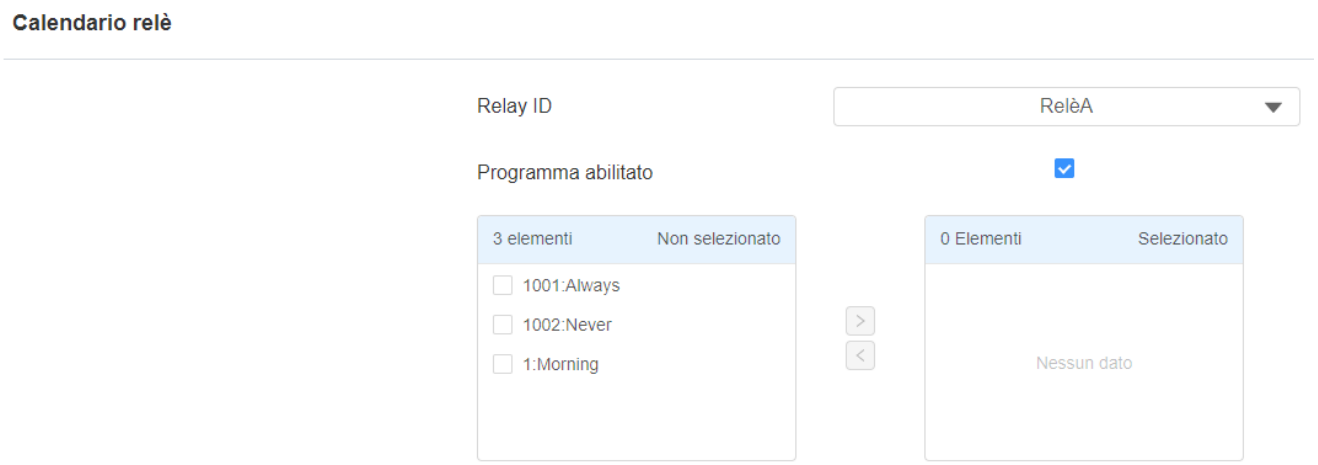


Impostazione parametri:

- **Ritardo trigger (sec):** imposta il ritardo di attivazione del relè (in un intervallo compreso tra 1 e 10 secondi). Ad esempio, se si imposta il tempo di ritardo su 5 secondi, il relè non verrà attivato fino a 5 secondi dopo aver premuto il pulsante di sblocco. Il valore di default è 0, ovvero il relè viene attivato immediatamente dopo la pressione del pulsante di sblocco.
- **Ritardo mantenimento (sec):** imposta il tempo di attivazione del relè (nell'intervallo compreso tra 1 e 60 secondi). Ad esempio, se si imposta il ritardo di mantenimento su 5 secondi, il relè rimarrà attivato per 5 secondi dopo l'apertura della porta. Ciò significa che la porta rimarrà aperta per 5 secondi.
- **1 cifra DTMF**: imposta il codice DTMF a 1 cifra nell'intervallo compreso tra (0-9 e *, #).
- **2~4 cifre DTMF**: impostare il codice DTMF in base all'opzione selezionata in "Modalità DTMF". Ad esempio, è necessario impostare il codice DTMF a 3 cifre se la modalità DTMF è impostata su "3 cifre DTMF".
- **Nome relè:** assegna un nome al relè se necessario. Questo può essere modificato da Ekinex Delégo App.
- **Abilitato**: questa casella di controllo consente di abilitare/disabilitare il relè di sicurezza.
- **Test**: premere il pulsante per testare il relè di sicurezza.

9.4 Programmazione oraria del relè

Permette di impostare il relè corrispondente sempre aperto in un orario specifico. Questa funzionalità è progettata per alcuni scenari specifici e ricorrenti, ad esempio il periodo di tempo dopo la scuola o l'orario di lavoro mattutino. Per configurare questa funzione, accedere a **Controllo accessi > Relè > Calendario relè** nell'interfaccia web.



Impostazione parametri:

- **Relay ID:** per selezionare il relè da impostare.
- **Programma abilitato**: è disabilitato per impostazione predefinita. Se abilitato, l'impostazione della pianificazione diventa disponibile. Per creare la pianificazione, fare riferimento alla programmazione di accesso alla porta (paragrafo 10.1)

Nota

• È possibile fare riferimento al paragrafo **Programmazione di acceso alla porta** per l'impostazione della pianificazione del relè.

10. Gestione della pianificazione degli accessi alle porte

È necessario configurare e programmare l'accesso alla porta da parte dell'utente tramite scheda RF, PIN privato e riconoscimento facciale.

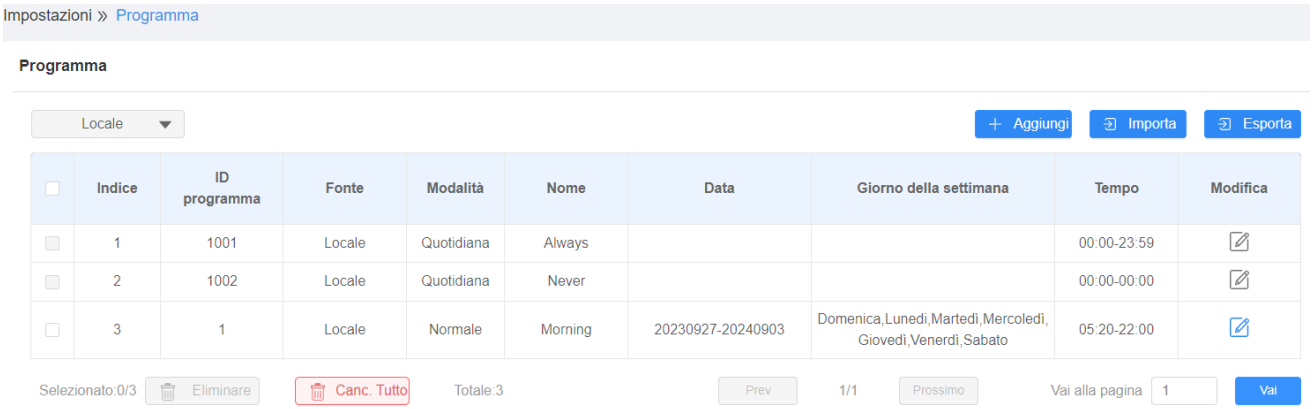
10.1 Programmazione di accesso alla porta

È possibile programmare orari di accesso alle porte in modo da poterli successivamente applicare comodamente al controllo accessi per singoli utenti o o per gruppi di utenti. Inoltre, è possibile modificare il programma di accesso alla porta, se necessario.

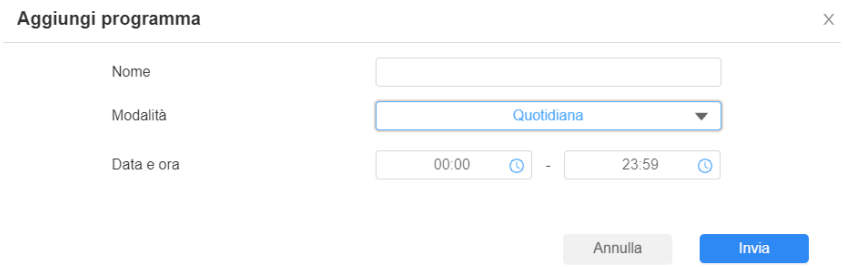
10.1.1 Creazione di un programma di accesso alla porta sull'interfaccia Web

È possibile creare una pianificazione dell'accesso alla porta su base giornaliera o mensile, nonché creare una pianificazione che consenta di impostare l'accesso per un periodo di tempo più lungo.

Per configurare la pianificazione da interfaccia web, andare su **Impostazioni > Programma**, quindi fare clic su + Aggiungi



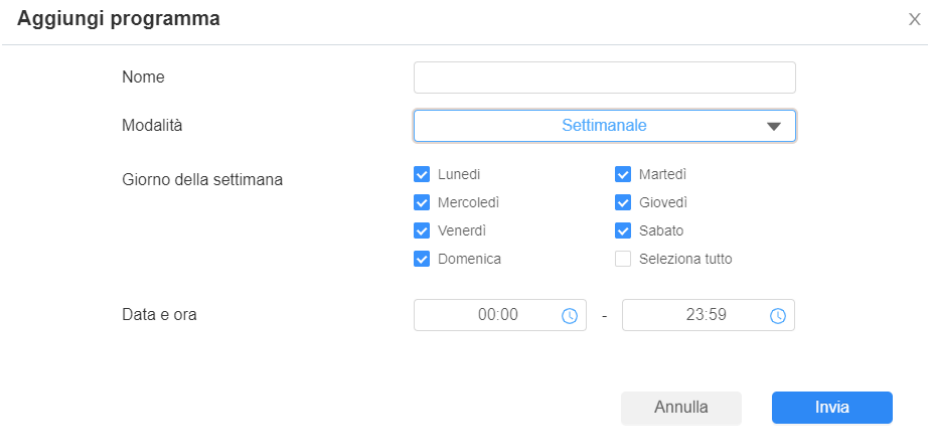
Per creare una programmazione giornaliera, selezionare la modalità "**Quotidiana**".



Impostazione parametri:

- **Nome:** inserire un nome per la programmazione giornaliera.
- **Modalità**: selezionare “Quotidiana”.
- **Data e Ora:** impostare la programmazione oraria per l’accesso alla porta durante la giornata.

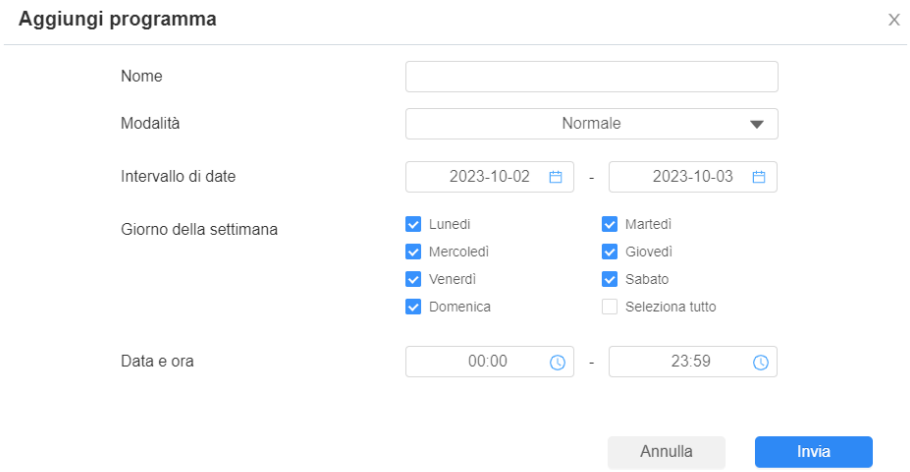
Per creare una programmazione settimanale, selezionare la modalità “**Settimanale**”.



Impostazione parametri:

- **Giorni della settimana:** selezionare il giorno/i nei quali l’accesso alla porta è abilitato nell’arco della settimana.
- **Data e Ora:** impostare la programmazione oraria per l’accesso alla porta durante la giornata.

Per programmare un periodo più lungo, scegliere Modalità “**Normale**”:



Impostazione parametri:

- **Intervallo di date:** imposta l'intervallo di date per l'accesso alla porta (data di inizio – data di fine).

10.1.2 Creazione di un programma di accesso alla porta sul dispositivo

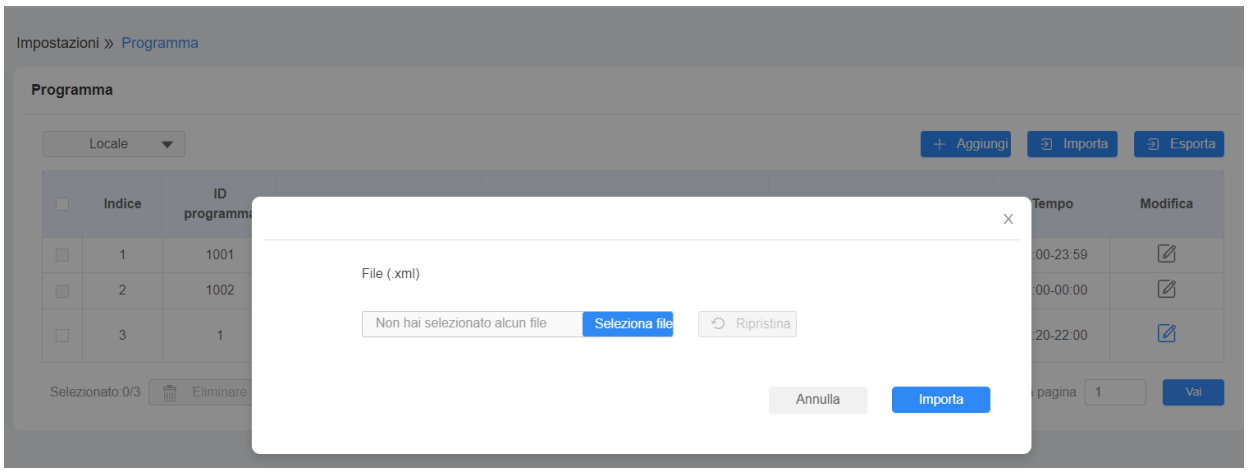
È inoltre possibile creare un programma di accesso alla porta sul dispositivo.

È necessario aprire la pagina **Impostazioni**, quindi andare su **Programma > Aggiungi**

10.1.3 Importare ed esportare la pianificazione degli accessi alle porte nell'interfaccia Web

Oltre a creare separatamente le pianificazioni degli accessi alle porte, si può anche importare o esportare comodamente le pianificazioni per massimizzare l'efficienza della loro gestione.

Nell'interfaccia web è necessario andare su **Impostazioni > Programma**, quindi fare clic su **Importa**.



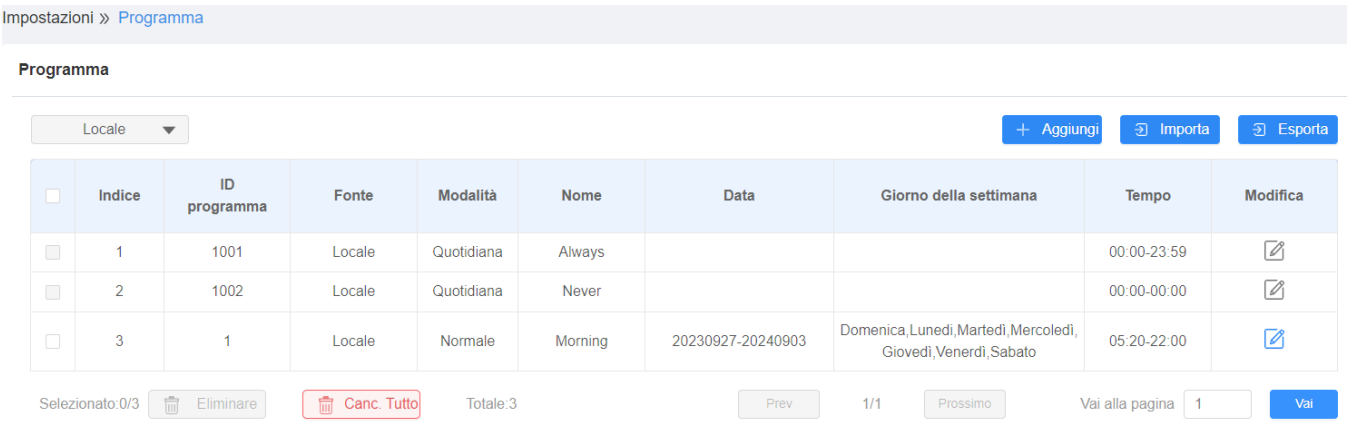
Nota

- Per l'importazione e l'esportazione della pianificazione sono supportati solo i file in formato .xml.

10.1.4 Modifica della pianificazione degli accessi alle porte

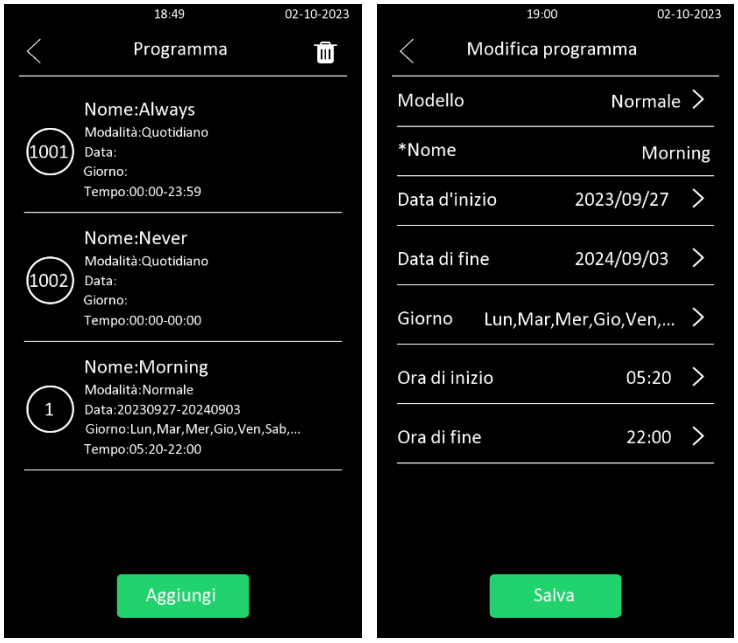
Se si desidera modificare o eliminare la pianificazione degli accessi alle porte creata, si può effettuare l'operazione singolarmente o in modalità multipla.

Per modificare la pianificazione dall'interfaccia web, andare su **Impostazioni > Programma.**



La cancellazione multipla è possibile mettendo un segno di spunta accanto all'indice della pianificazione e cliccando su "Eliminare".

Per modificare la pianificazione dal dispositivo, fare clic su **Programma** nella pagina **Impostazioni**, quindi scegliere la pianificazione che si desidera modificare.



11. Configurazione apertura porta

Il citofono DICO offre tre tipi di accesso alla porta: tramite codice PIN, scheda RF e riconoscimento facciale.

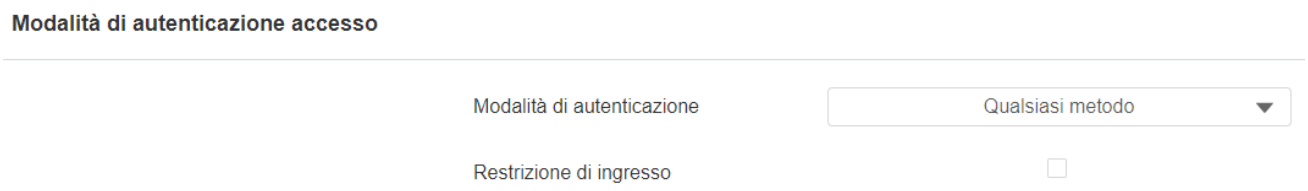
Questa funzionalità può essere configurata sia dal dispositivo che sull'interfaccia web.

Inoltre, è consentito importare o esportare i file configurati per massimizzare l'efficienza della configurazione della scheda RF.

11.1 Autenticazione accesso

È possibile impostare diverse modalità di autenticazione dell'accesso e configurare la sicurezza dell'autenticazione secondo specifiche necessità.

Nell'interfaccia web, accedere a **Controllo accessi > Relè > Modalità di autenticazione accesso.**



Impostazione parametri:

- **Modalità di autenticazione**: per questo parametro sono disponibili quattro opzioni:
  1. **Qualsiasi metodo:** per autorizzare tutti i metodi di accesso per sbloccare la porta.
  2. **Viso + PIN**: per applicare un doppio metodo di accesso (volto e PIN) per lo sblocco della porta.
  3. **Viso + RF Card**: se sono possibili sia il riconoscimento facciale che RF Card per lo sblocco della porta.
  4. **RF Card + PIN**: se sono consentiti sia Face che RF Card per lo sblocco della porta.
- **Restrizione di ingresso**: abilitarla per impostare un intervallo di tempo per lo sblocco della porta.

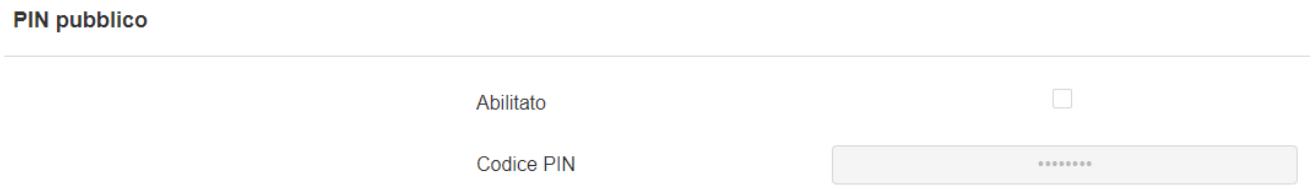
11.2 Configurazione dei codici PIN per l'accesso

Il videocitofono DICO consente di creare e modificare sia codici PIN pubblici che privati per l'accesso alla porta.

11.2.1 Configurare il codice PIN pubblico per lo sblocco della porta

Questa opzione consente di configurare e modificare i codici PIN pubblici.

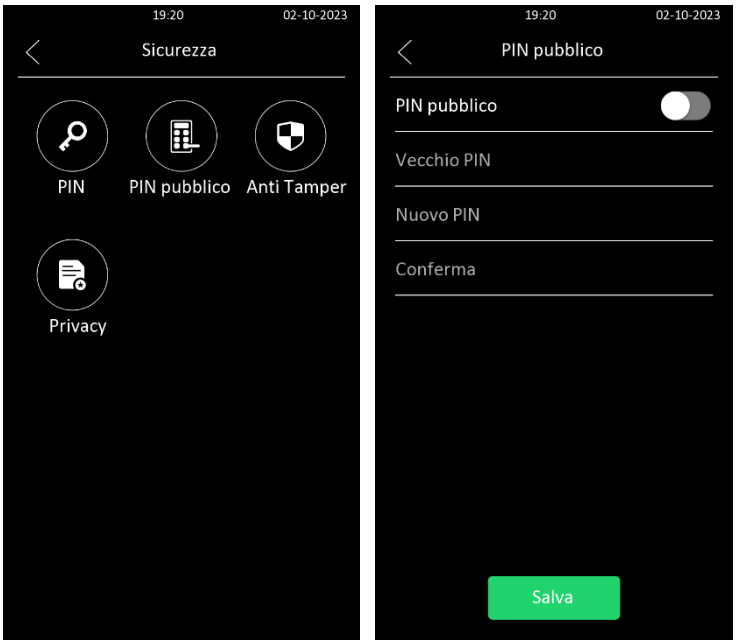
Nell'interfaccia web, andare in **Controllo accessi > Impostazione PIN > PIN pubblico.**



Impostazione parametri:

- **Abilitato**: permette di abilitare/disabilitare la gestione del codice PIN Pubblico.
- **Codice PIN**: per impostare il codice PIN con un numero di cifre compreso tra 4 e 8.

Per configurarlo il PIN pubblico sul dispositivo, accedere alla pagina **Impostazioni** e selezionare **Sicurezza > PIN pubblico**



Nota

- Il codice PIN pubblico inserito non sarà valido finché la funzione PIN non sarà attivata.

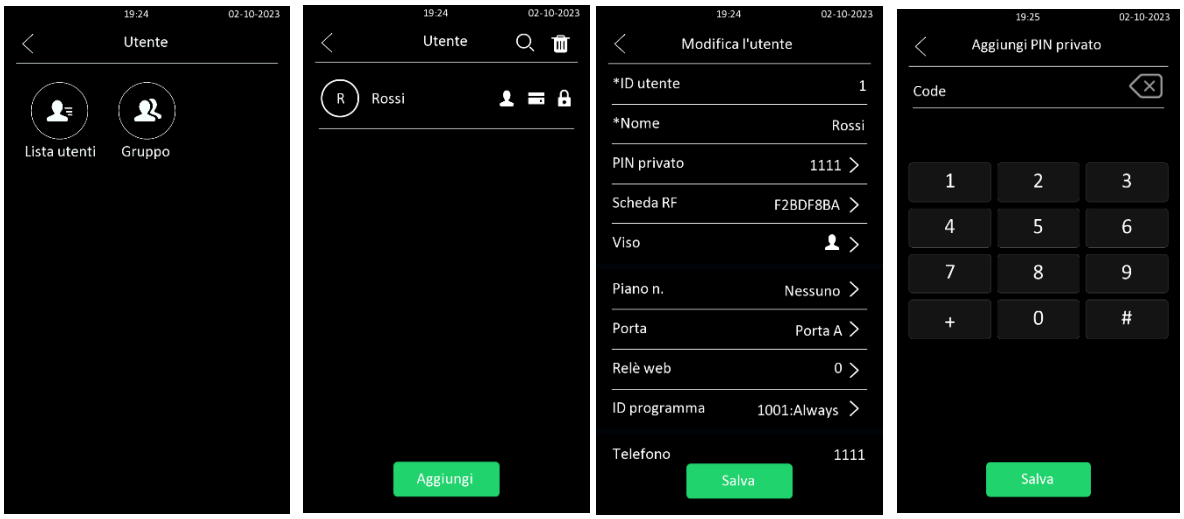
Nota

- **APT+PIN** è applicabile solo quando il dispositivo viene aggiunto ad Ekinex Delégo App.

11.2.2 Configurare il codice PIN privato da dispositivo

È possibile configurare da dispositivo l'accesso alla porta tramite codice PIN privato per uno specifico utente, inserendo il nome dell'utente e il codice PIN.

Sul dispositivo selezionare Impostazioni, quindi **Utente > Lista utenti**. Cliccando su qualsiasi utente è possibile aggiungere o modificare un PIN privato.

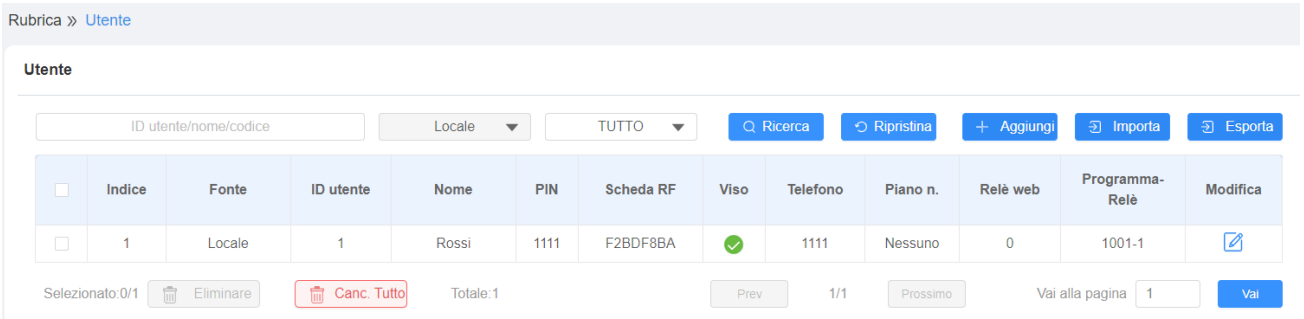


*11.2.3 Configurare il codice PIN privato dall'interfaccia web

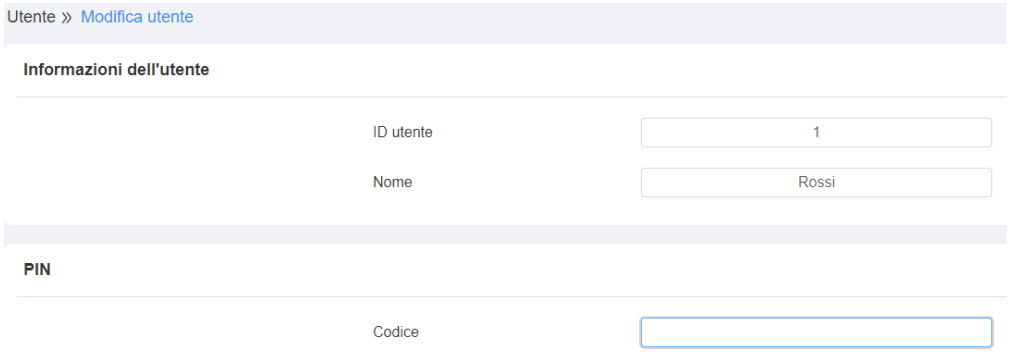
Sull'interfaccia web, non solo è possibile impostare un codice PIN privato ma anche impostare e selezionare il programma di accesso alla porta, che garantisce la validità dell'accesso con codice PIN durante un determinato intervallo di tempo pianificato.

Inoltre, è possibile impostare un limite per il numero totale di accessi alla porta con codice PIN valido.

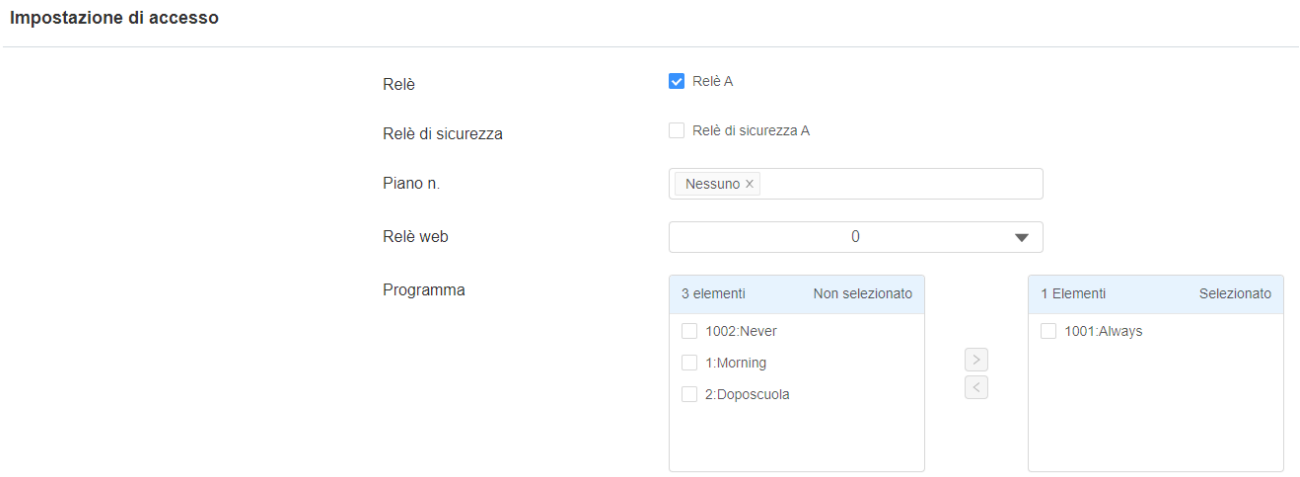
Per configurare il codice PIN, andare su **Rubrica > Utente** nell'interfaccia web.



Quindi, premere il simbolo Modifica per un utente specifico.



Dopo aver immesso le informazioni dell'utente e il codice PIN, è possibile scorrere verso il basso fino a **Impostazione di accesso** nella stessa pagina, per impostare la pianificazione dell'accesso alla porta con codice PIN privato:



Impostazione parametri:

- **Relè:** selezionare il relè di sblocco porta per l'utente specificato.
- **Relè di sicurezza**: permette di abilitare il relè di sicurezza.
- **Piano n.:** inserire il numero di piano dell'utente.
- **Relè web:** selezionare il numero di comandi per il relè web impostato da interfaccia web.
- **Programma:** selezionare uno o più programmi di accesso alla porta creati in precedenza e visualizzati nella casella a sinistra e spostare nella casella di destra quelli da applicare all'accesso alla porta con codice PIN specifico dell'utente.

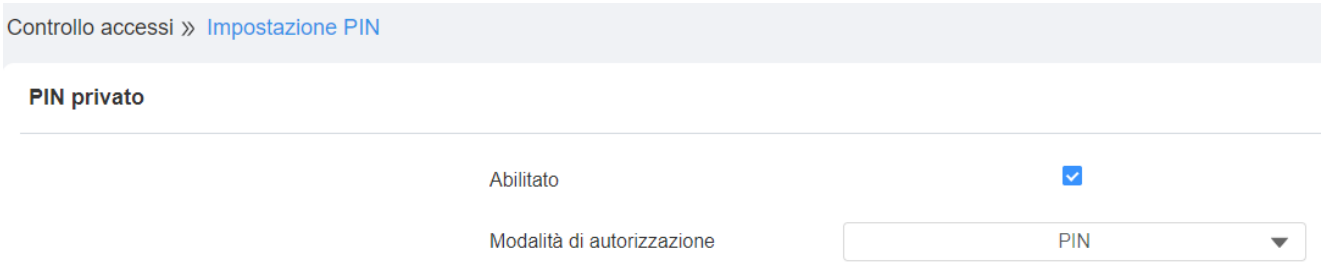
Nota

- Questo procedimento è applicabile anche all'accesso alla porta tramite scheda RF e riconoscimento facciale poiché sono identici nella configurazione.

11.2.4 Configurare la modalità di accesso con PIN privato

Il dispositivo DICO offre due tipi di modalità per l'accesso con codice PIN privato: **PIN** e **APT#+PIN**.

Nell'interfaccia web, andare su **Controllo accessi > Impostazione PIN > PIN privato** per abilitare/disabilitare il PIN privato.



Impostazione parametri:

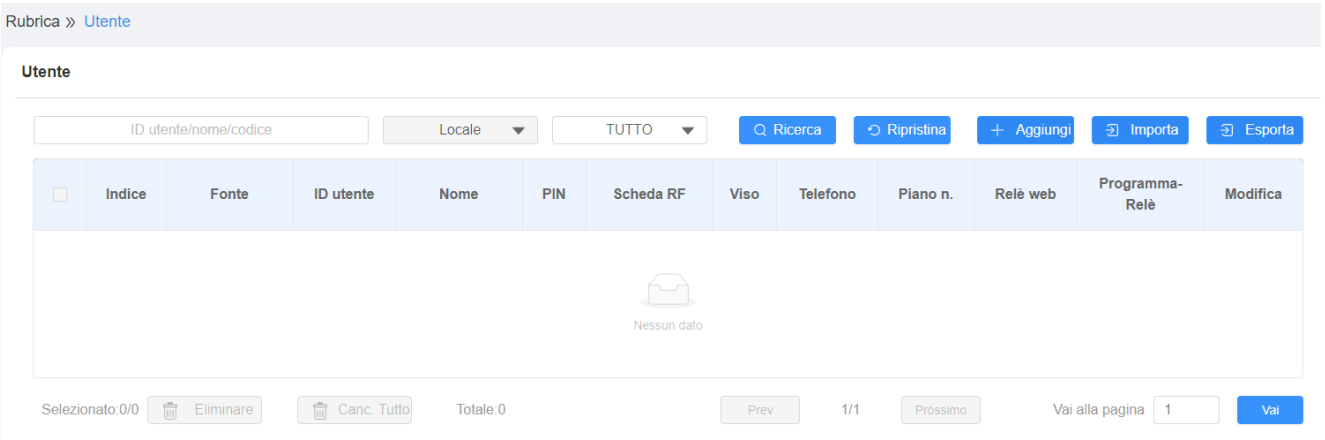
- **Modalità di autorizzazione:** selezionare la modalità di accesso tra **PIN** e **APT#+PIN**.

  Scegliendo “PIN”, all’utente verrà richiesto di inserire direttamente solo il codice PIN per l'accesso dalla porta; selezionando invece “APT#+PIN”, allora l’utente dovrà inserire prima il numero dell'appartamento e poi il codice PIN per l'accesso dalla porta.

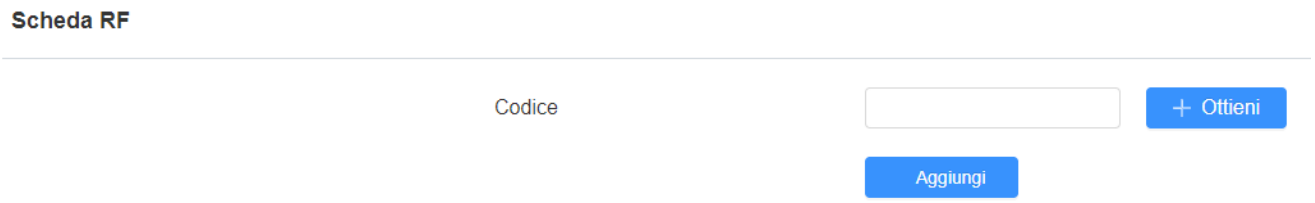
11.3 Configurare la RF card per l’accesso alla porta

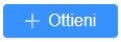
11.3.1 Aggiungere la RF card da interfaccia web

Per aggiungere RF card, da interfaccia web andare su **Rubrica > Utente** e premere 



Infine, muoversi nella pagina fino alla **Scheda RF**.



Successivamente premere il pulsante 

e avvicinare la tessera RF al lettore del dispositivo DICO per circa 5 secondi, in modo che la tessera venga riconosciuta ed associata all'utente selezionato.

Nota

- Per l'accesso alla porta specifico dell'utente/i con scheda RF, fare riferimento alla procedura per la selezione del programma di accesso tramite codice PIN

Nota

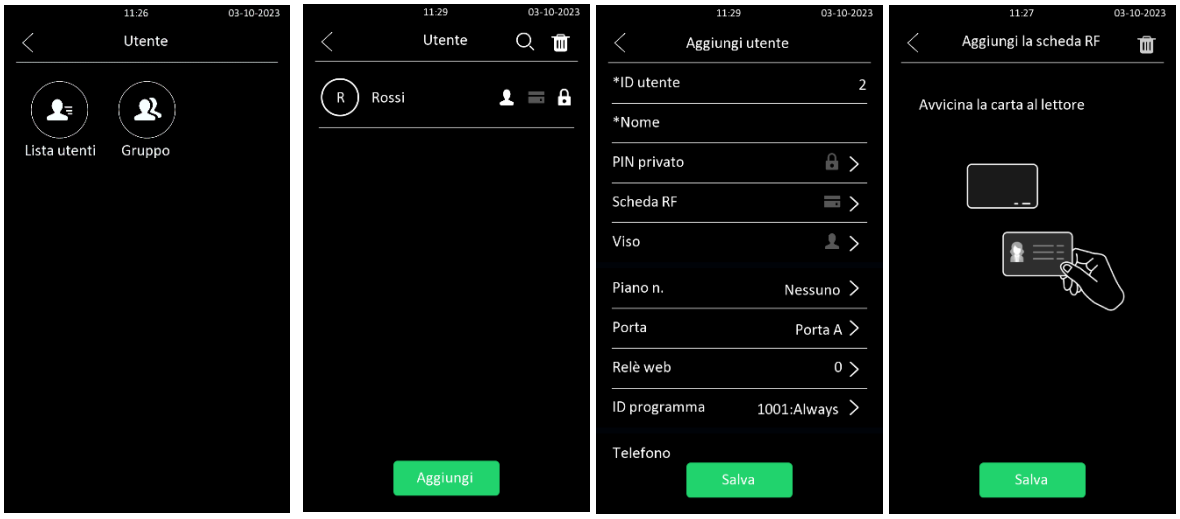
- Per l'accesso alla porta, il videocitofono considera RF card a 13,56 MHz e a 125 kHz

11.3.2 Aggiungere la RF card dal dispositivo

È possibile configurare la RF card per l'accesso dalla porta direttamente dal dispositivo, mentre si impostano le altre modalità di accesso (PIN, riconoscimento facciale, Web relè, ecc.) o la programmazione temporale per l'accesso di uno specifico utente.

Per aggiungere una scheda RF, dalla pagina **Impostazioni** premere **Utente**, quindi **Lista utenti** e poi + Aggiungi un nuovo utente, oppure si può modificare il profilo di un utente già registrato.

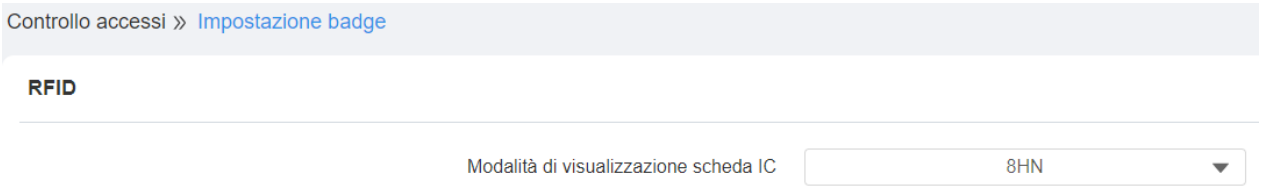
Infine, premere la voce **Scheda RF**:



11.3.3 Configurare il formato del codice per la RF card

Se si desidera realizzare l'integrazione con un sistema citofonico di terze parti in termini di accesso alla porta con scheda RF, è possibile modificare il formato del codice della scheda RF. In questo modo, questo può essere identico a quello applicato nel sistema di terze parti.

Per configurare la configurazione sull'interfaccia web, andare su **Controllo accessi > Impostazioni badge**.



Impostazione parametri:

- **Modalità di visualizzazione scheda IC**: selezionare il formato per la scheda IC per l'accesso alla porta tra sei opzioni: **8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 8HR10D.** Per impostazione predefinita, il formato del codice della scheda nel videocitofono DICO è 8HN.

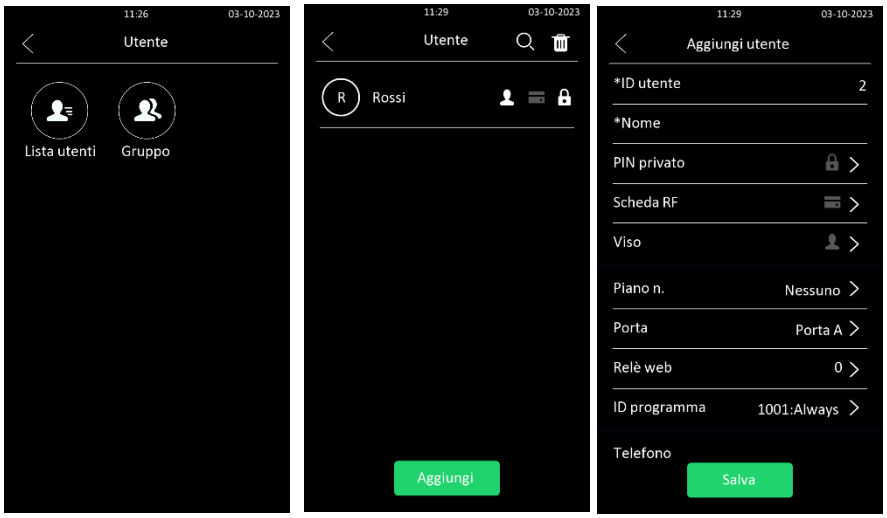
11.4 Configurazione del riconoscimento facciale per lo sblocco della porta

11.4.1 Registrazione dei dati del volto dal dispositivo

È possibile configurare l'accesso alla porta tramite riconoscimento facciale sul dispositivo inserendo il nome dell'utente e registrando l'ID facciale di accesso alla porta.

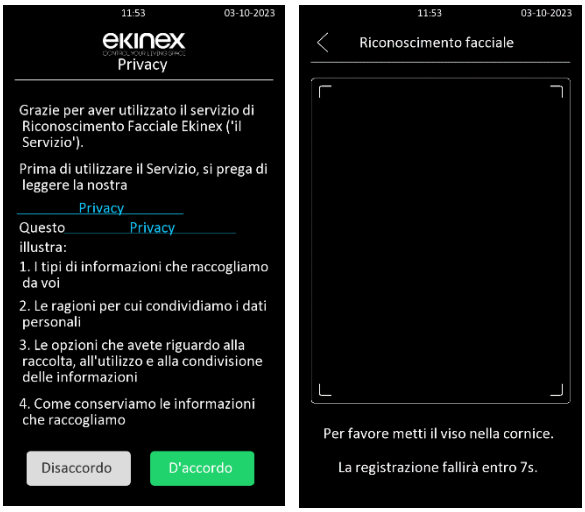
Sul dispositivo, accedere alla pagina **Impostazioni**, quindi premere **Utente > Elenco utenti**, poi + Aggiungi un nuovo utente, oppure si può modificare il profilo di un utente già registrato.

Infine, premere la voce **Viso:**



Il dispositivo visualizzerà una pagina dove sarà possibile accettare l'Informativa sulla privacy facendo clic sul pulsante "**D'accordo**".

Infine, la fotocamera procederà con il riconoscimento del volto in circa 10 secondi.

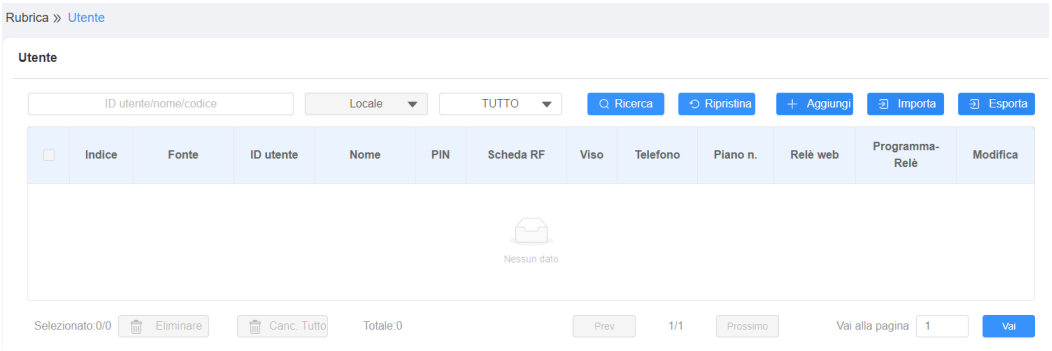


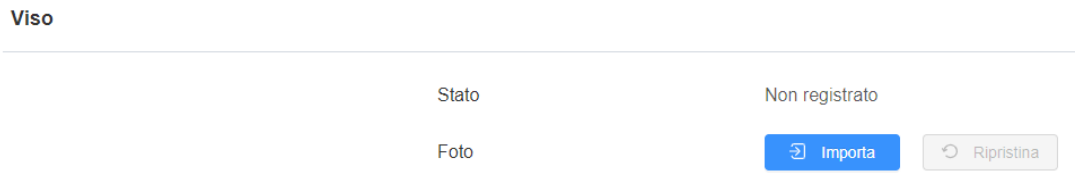
11.4.2 Caricamento dei dati del volto dall'interfaccia web

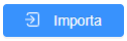
The user can upload the face data to the device via the web interface. To do so, go to **Directory > User,** then click **+Add** or **Edit** symbol. After that, upload the face photo.

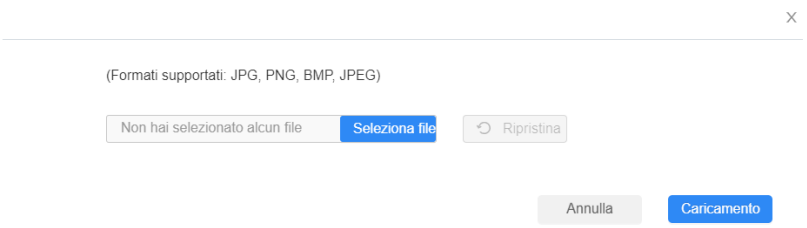
L'utente può caricare i dati del viso sul dispositivo tramite l'interfaccia web. Per fare ciò, occorre andare in **Rubrica > Utente**, quindi cliccare su 

o sul simbolo di Modifica  per un utente già presente.





Successivamente, caricare la foto del viso utilizzando la funzione 



Impostazione parametri:

- **Stato**: questo campo visualizza l'informazione relativa alla foto del volto caricata. Nello specifico, mostra "**Registrato**" quando l'immagine caricata è conforme al formato e allo standard richiesto. Altrimenti mostrerebbe "**Non registrato**" come predefinito. Tuttavia, lo stato tornerà a "Non registrato" se l'immagine caricata viene cancellata quando si preme "Ripristina".

- **Foto (jpg/png):** fare clic sul pulsante Importa per selezionare l'immagine e caricarla sul dispositivo. Cliccando su *"Ripristina"* l'immagine viene cancellata dal dispositivo.

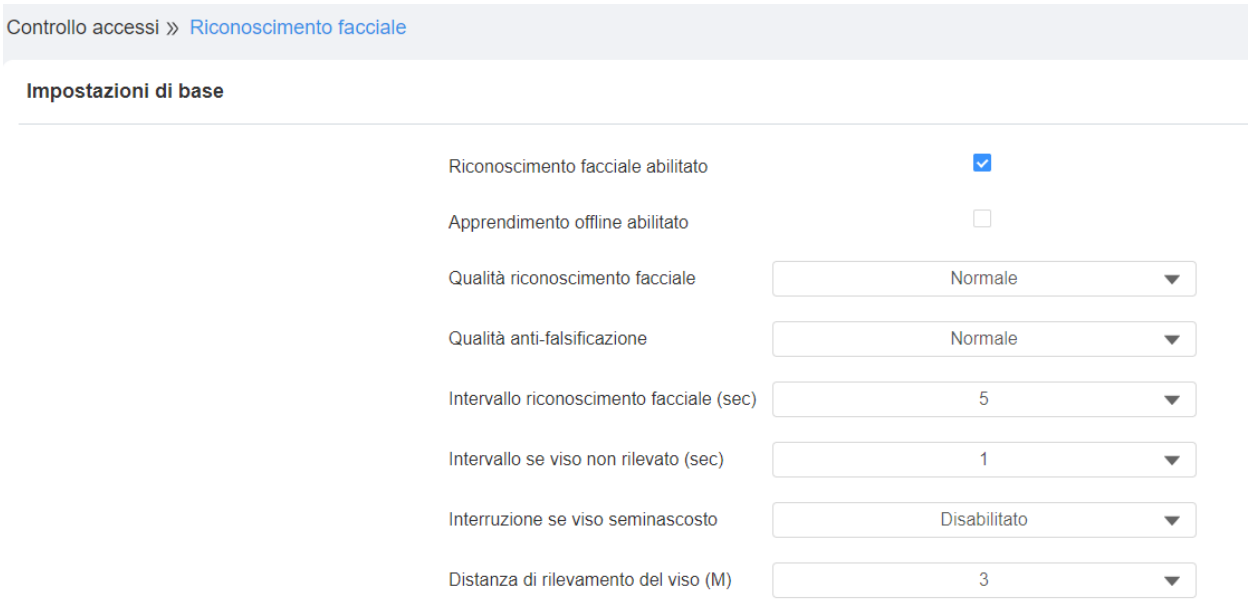
Nota

- Le immagini da caricare devono essere in formato jpg o png.

11.4.3 Configurazione del riconoscimento facciale

Il videocitofono DICO consente di regolare la precisione del riconoscimento facciale e gli intervalli di riconoscimento in base alle esigenze dell'utente. È possibile migliorare la qualità del rilevamento e l'esperienza dell'utente attraverso l'impostazione di base del riconoscimento facciale.

Per impostare la configurazione sull'interfaccia web, andare alla pagina **Controllo accessi > Riconoscimento facciale.**



Impostazione parametri:

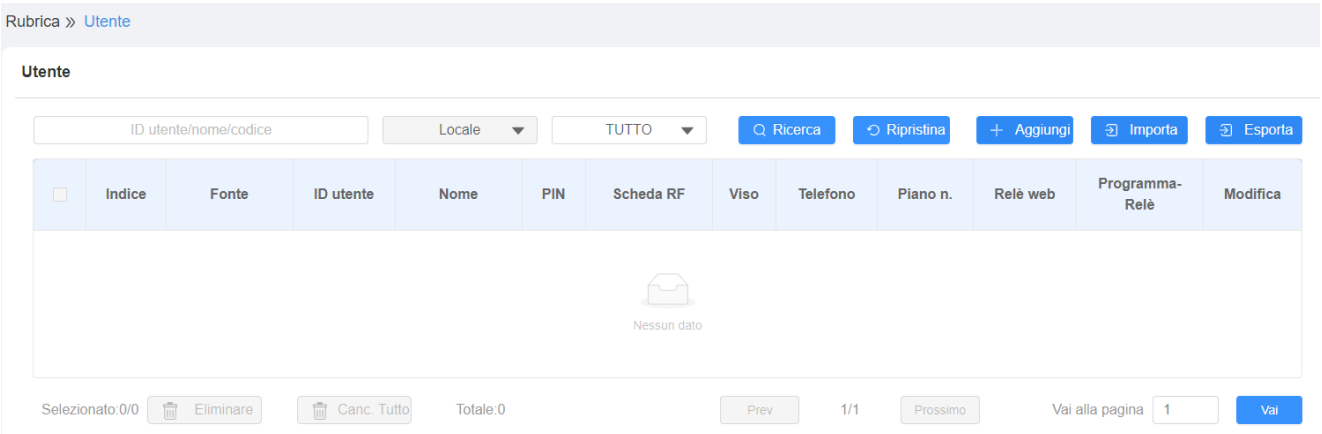
- **Riconoscimento facciale abilitato:** consente di abilitare/disabilitare la funzione.
- **Apprendimento offline abilitato:** abilitare questo parametro se si desidera migliorare la capacità di riconoscimento del dispositivo, concentrandosi sulle principali caratteristiche facciali ignorando i cambiamenti minori avvenuti sul viso. La precisione del riconoscimento facciale migliora con l'aumentare del numero di riconoscimenti facciali riusciti.
- **Qualità riconoscimento facciale:** da menù a tendina selezionare il livello di precisione del riconoscimento facciale tra quattro opzioni: **Basso**, **Normale**, **Alto** e **Massimo**. Ad esempio, selezionando “Massimo”, ci saranno meno possibilità che due utenti vengano confusi l’uno con l’altro durante il processo di riconoscimento facciale.

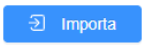
- **Qualità anti-falsificazione:** selezionare il livello anti-falsificazione tra cinque opzioni: **Chiudi**, **Basso**, **Normale**, **Alto**, **Massimo**. Ad esempio, se si seleziona “Massimo” ci saranno meno possibilità che il dispositivo venga ingannato da immagini digitali o fotomontaggi di qualsiasi tipo.
- **Intervallo riconoscimento facciale (sec):** selezionare l'intervallo di tempo tra due riconoscimenti facciali in un periodo compreso tra 1 e 8 minuti. Ad esempio, selezionando 5, occorrerà attendere 5 minuti prima che sia consentito eseguire nuovamente un altro riconoscimento facciale.
- **Intervallo se viso non rilevato (sec):** imposta il tempo massimo di attesa se non viene rilevato alcun volto, in un intervallo compreso fra 1 e 8 secondi.
- **Interruzione se viso seminascosto:** se **Abilitato**, permette di interrompere il riconoscimento del volto nel caso in cui un'immagine venga catturata parzialmente o non sia completamente visibile a causa della sovrapposizione di oggetti, indumenti e parti del corpo.
- **Distanza di rilevamento del viso (m):** imposta la distanza per il riconoscimento facciale. I valori possibili sono 1,2,3 m.

11.5 Impostare l'accesso alla porta utilizzando file di configurazione

Il citofono DICO consente di configurare rapidamente l'accesso alla porta specifico per ciascun l'utente in modalità multipla, importando i file di controllo dell'accesso alla porta in una sola volta. Questi incorporano le informazioni dell'utente, il tipo di accesso alla porta, il programma di accesso alla porta, ecc. Pertanto tutte le impostazioni di accesso alla porta possono essere caricate in un unico passaggio, risparmiando tempo e fatica rispetto alla configurazione separata dell'accesso alla porta per singolo utente, soprattutto quando gli utenti sono numerosi.

Per eseguire questa attività, l'utente può accedere all'interfaccia web e spostarsi su **Rubrica > Utente.**



In questa pagina, cliccare sul pulsante 

e caricare un file di archivio con le informazioni degli utenti.

I formati consentiti per tali file sono .tgz e .zip.

Nota

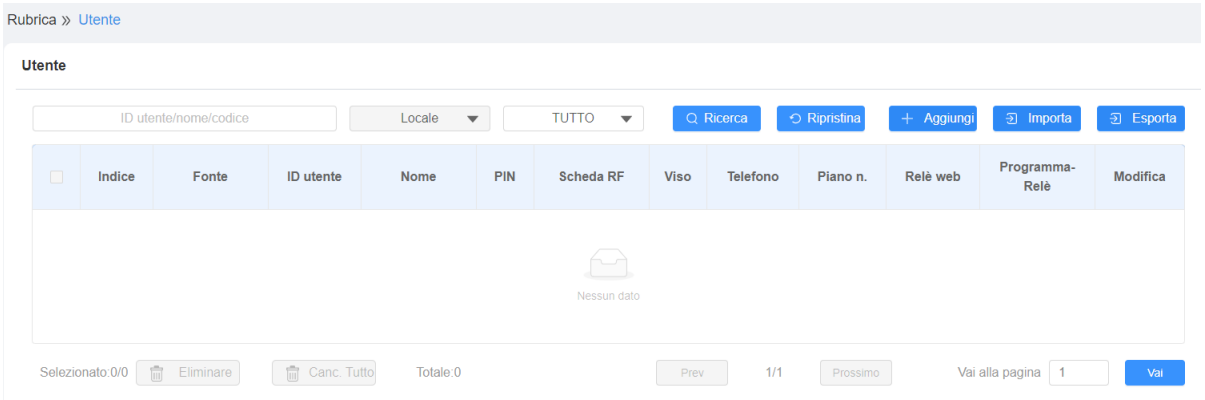
- I file di configurazione per il riconoscimento facciale e gli altri tipi di file di accesso alle porte sono separati con formati di file diversi.

11.5.1 Modifica dei dati di accesso alla porta specifici dell'utente

E' possibile effettuare ricerche sui dati di accesso alle porte specifici degli utenti e modificare i dati di accesso alle porte dall'interfaccia web.

Per farlo, occorre andare alla pagina **Rubrica > Utente** e cliccare su

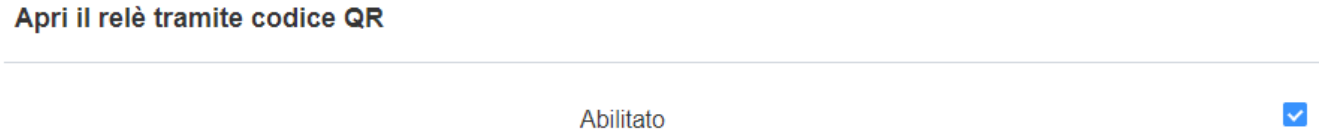
- **Ricerca**, fornendo un ID utente, nome o codice nel campo in alto a sinistra;
- **Modifica**, cliccando sull'icona alla fine di una riga utente.



11.6 Apertura porta con codice QR

Il codice QR è un'altra opzione per lo sblocco della porta.

Per utilizzarlo è necessario abilitare la funzione QR code da interfaccia web cliccando su **Controllo Accessi > Relè > Apri Relè tramite codice QR.**



Nota

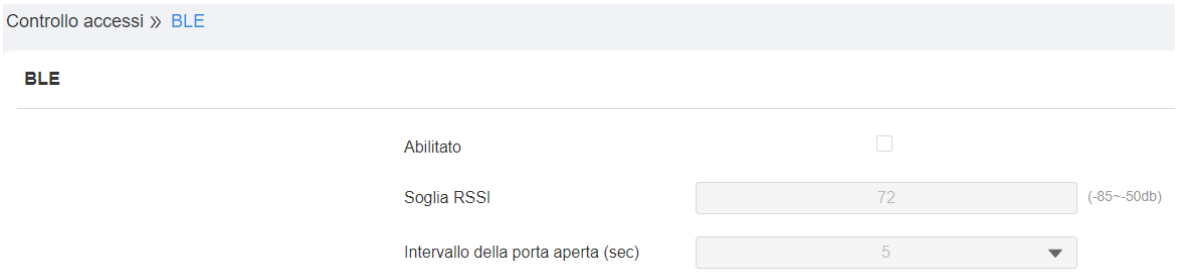
- La funzione è compatibile con Ekinex Delégo App.

11.7 Apertura porta tramite Bluetooth

L'utente può aprire la porta anche tramite telefono cellulare con funzione Bluetooth.

La funzione si attiva muovendo lo smartphone vicino al terminale di controllo accessi e consente l'accesso alla porta.

Per configurarlo sull'interfaccia web, abilitare la funzione nella pagina web Controllo accessi > BLE > BLE.



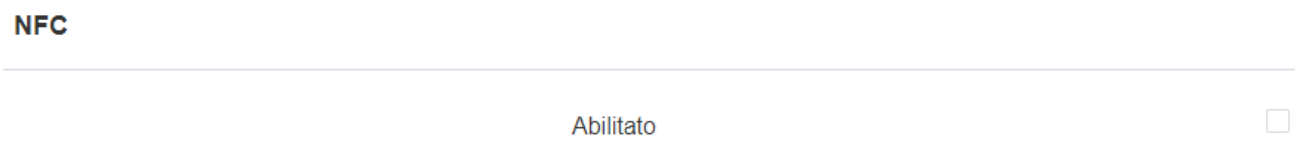
Impostazione parametri:

- **Soglia RSSI:** seleziona la potenza di ricezione del segnale nell'intervallo -85~-50db. Più alto è il valore, maggiore è la sua potenza. Il valore predefinito è 72 dB.
- **Intervallo della porta aperta (sec)**: permette di impostare l'intervallo di tempo tra due accessi via Bluetooth.

11.8 Apertura porta tramite NFC

È inoltre possibile accedere alla porta tramite smartphone con funzione NFC, utilizzato con Ekinex Delégo App. È sufficiente tenere il telefono cellulare vicino al citofono per accedere dalla porta.

Per abilitare questa funzione dall'interfaccia web, andare in **Controllo accessi > Impostazione badge > NFC**.

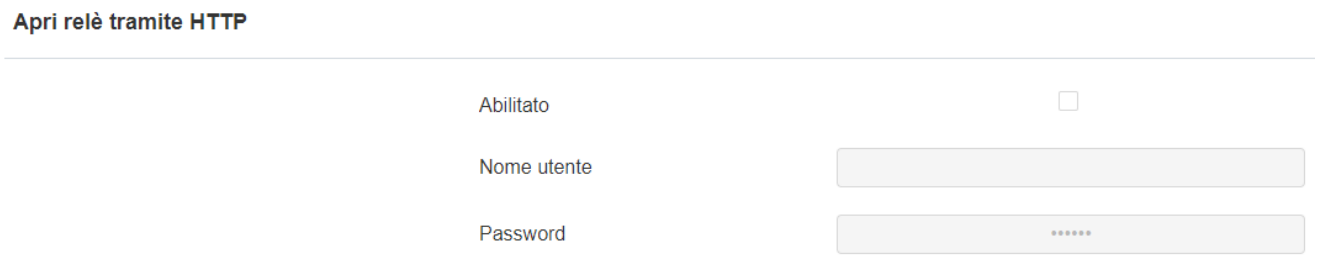


11.9 Apertura porta via comando HTTP su browser Web

È possibile sbloccare la porta da remoto senza essere fisicamente vicini al dispositivo DICO.

In questo caso, l'utente può digitare un comando HTTP (URL) su un browser web, per attivare il relè quando non si è fisicamente presenti presso la porta per l'accesso.

Per impostare la configurazione sull'interfaccia web, andare su **Controllo accessi > Relay > Apri relè tramite HTTP**.



Impostazione parametri:

- **Abilitato**: per abilitare/disabilitare lo sblocco porta tramite richiesta http
- **Nome utente:** immettere il nome utente dell'interfaccia web del dispositivo, ad esempio **admin**.
- **Password**: immettere la password per il comando HTTP. Ad esempio, 12345.

Fare riferimento al seguente esempio, con i parametri impostati come sopra:

http://YOUR_DEVICE_IP/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

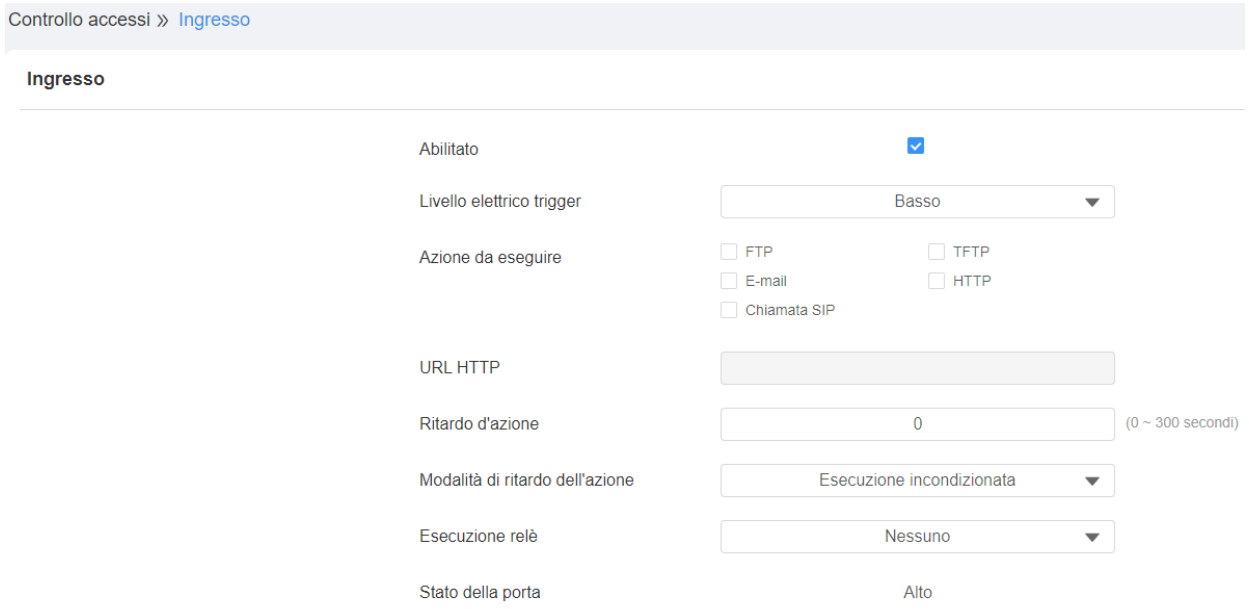
Nota

- **DoorNum** nel comando HTTP precedente si riferisce al relè n. 1 da attivare per l'accesso alla porta.

11.10 Sblocco tramite pulsante di uscita vicino alla porta

Quando l'utente deve aprire la porta dall'interno di un edificio utilizzando il pulsante di uscita installato sulla porta, è possibile configurare la funzione **Ingresso** del videocitofono DICO per attivare il relè di apertura della porta.

Per impostare tale configurazione sull'interfaccia web, andare su **Controllo accessi > Ingresso > Ingresso.**



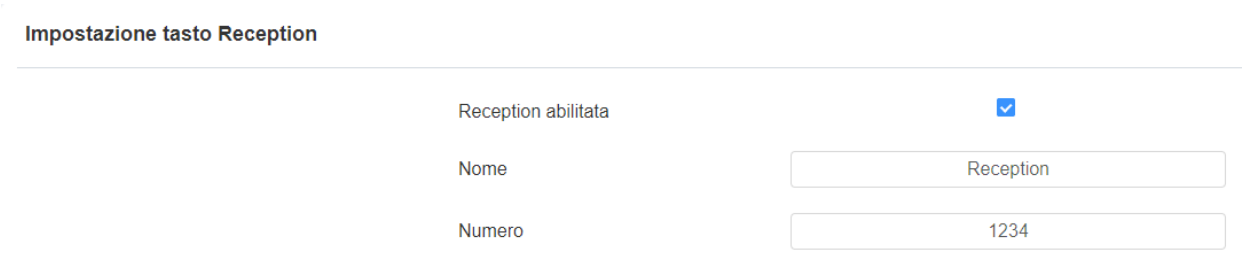
Impostazione parametri:

- **Abilitato**: consente di abilitare o disabilitare la funzione.
- **Livello elettrico trigger:** selezionare il livello elettrico del trigger tra le opzioni **Alto** e **Basso,** in base all'operazione da effettuare sul pulsante di uscita.
- **Azione da eseguire:** selezionare il metodo per eseguire l'azione tra cinque opzioni: **FTP, Email, SIP Call, HTTP** e **TFTP.**
- **URL HTTP:** inserire l'URL se è stata selezionata la modalità **HTTP** per eseguire l'azione.
- **Ritardo d'azione:** impostare il ritardo per l'esecuzione dell'azione, in un intervallo tra 0 e 300 secondi. Ad esempio, se si imposta il tempo di ritardo dell'azione su 5 secondi, le azioni corrispondenti verranno eseguite 5 secondi dopo aver premuto il pulsante (l'ingresso viene attivato).
- **Modalità di ritardo dell'azione:** se si seleziona **Esecuzione incondizionata**, l'azione verrà eseguita quando viene attivato l'ingresso. Se si seleziona **Esegui se l'input è ancora attivato**, l'azione verrà eseguita se l'ingresso rimane attivato. Ad esempio, se la porta rimane aperta dopo aver attivato l'ingresso, verrà eseguita un'azione, ad esempio l'invio di una e-mail, per avvisare il destinatario.
- **Esecuzione relè:** imposta i relè attivati dall'ingresso.

11.11 Apertura porta tramite tasto Reception

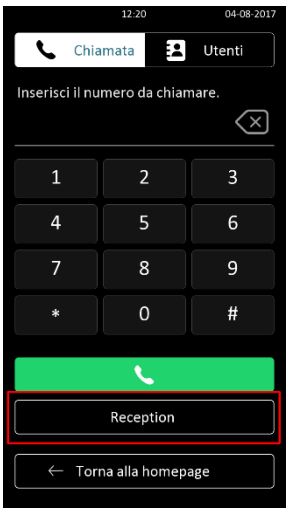
Nella schermata iniziale del dispositivo, il videocitofono DICO fornisce ai residenti e ai visitatori un accesso rapido alla porta premendo il tasto **Reception**, posizionato nella parte inferiore della schermata.

Per impostare la configurazione, accedere all'interfaccia web e andare su **Citofono > Base > Impostazione tasto Reception**



Impostazione parametri:

- **Reception abilitata**: consente di abilitare o disabilitare il tasto "*Reception*";
- **Nome:** inserire il nome per l'icona **Reception** nella schermata iniziale.
- **Numero:** inserire il numero SIP/IP da chiamare dopo aver premuto l'icona "*Reception"* per l'accesso alla porta.

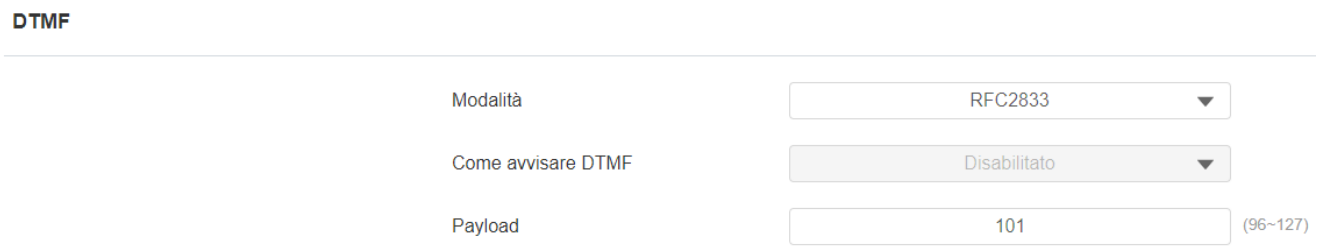


11.12 Apertura porta tramite codice DTMF

DTMF codes can be configured on the intercom web interface. By setting identical DTMF codes on corresponding intercom devices such as an indoor monitor, you can allow users to enter the DTMF code on the virtual keypad or press the attached DTMF code to unlock the door for visitors, etc., during a call

I codici DTMF possono essere configurati dall'interfaccia web del videocitofono. Impostando codici DTMF identici su dispositivi interfonici collegati nella stessa rete (ad esempio, un monitor interno), è possibile consentire agli utenti di inserire il codice DTMF sulla tastiera virtuale o premere il codice DTMF allegato per sbloccare la porta per i visitatori, ecc., durante una chiamata.

Per abilitare la configurazione DTMF dall'interfaccia web, accedere a **Account > Avanzate > DTMF**.



Impostazione parametri:

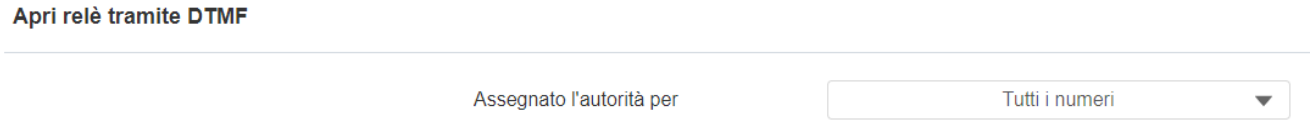
- **Modalità:** selezionare la modalità DTMF tra sei opzioni: **Info**, **Inband, RFC2833, Info+Inband, Info+RFC2833** and **Info+Inband+RFC2833** secondo la preferenza.
- **Come avvisare DTMF:** questa opzione è disponibile solo se la "*Modalità*" scelta al punto precedente contiene l'opzione "*Info"* e consente di scegliere tra quattro possibili valori: **Disabilitato, DTMF, DTMF-Relay,** e **Telephone-Event.**
- **Payload:** per selezionare il payload per l'identificazione della trasmissione dati. Il valore predefinito è 101, l'intervallo di valori ammessi è 96-127.

Note

- Fare riferimento al capitolo *7.8 - Configurazione della trasmissione dati DTMF* per dettagli sull'impostazione del codice DTMF.
- I dispositivi interfonici coinvolti devono essere coerenti nel tipo DTMF altrimenti il codice DTMF non può essere applicato.

11.12.1 Configurazione di una lista di utenti autorizzati (whitelist) con codice DTMF

Per proteggere l'accesso alla porta tramite codici DTMF, è possibile impostare una lista di utenti autorizzati DTMF ("whitelist") dall'interfaccia web in **Controllo accessi > Relè > Apri relè tramite DTMF,** in modo che solo i numeri chiamanti designati nel videocitofono possano utilizzare il codice DTMF per ottenere accesso alla porta.



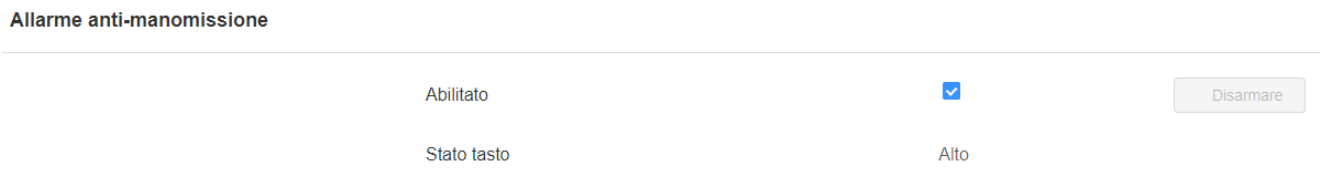
Le opzioni sono: **Nessuno, Solo elenco degli inquilini** e **Tutti i numeri** (default).

12. Sicurezza

12.1 Impostazione dell'allarme anti-manomissione

La funzione di allarme manomissione (tamper) funge da protezione contro qualsiasi rimozione non autorizzata del dispositivo, attivando l'allarme tamper sul videocitofono.

Per configurarla da interfaccia web, andare su **Sistema > Sicurezza > Allarme anti-manomissione.**



Impostazione parametri:

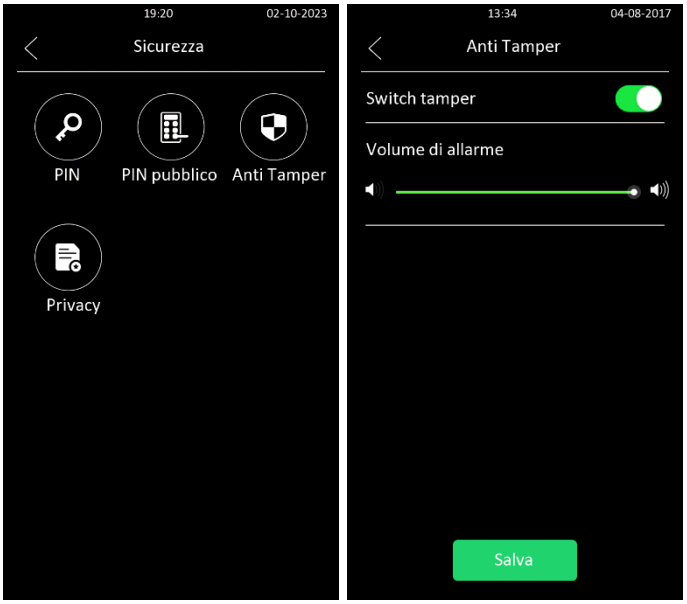
- **Abilitato**: spuntare la casella di controllo per abilitare la funzione di allarme manomissione. Quando l'allarme manomissione si attiva, è possibile premere il tasto "*Disarmare*" accanto alla casella di controllo per disattivare l'allarme.
- **Stato chiave**: quando viene premuto il pulsante *"Disarmare"*, lo stato cambierà da basso ad alto. Lo stato normale è alto.

Note

• Il pulsante *"Disarmare"* diventerà grigio quando l'allarme manomissione sarà rientrato.

• Il pulsante rotondo in gomma sul retro del dispositivo deve essere premuto altrimenti la funzione antimanomissione non verrà attivata.

Per attivare la funzione antimanomissione dal dispositivo, basta accedere alla pagina **Impostazioni** e spostarsi su **Sicurezza > Anti Tamper.**

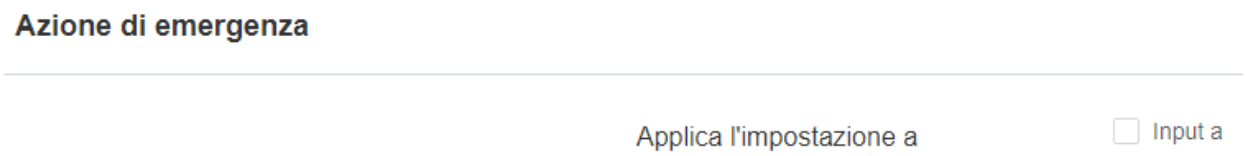


12.2 Azione di emergenza

È possibile tenere la porta aperta in caso di emergenza, in modo che le persone possano uscire dall'edificio.

In the web interface, go to **System > Security > Emergency Action**.

Nell'interfaccia web, andare alla scheda **Sistema > Sicurezza > Azione di emergenza.**



Nota

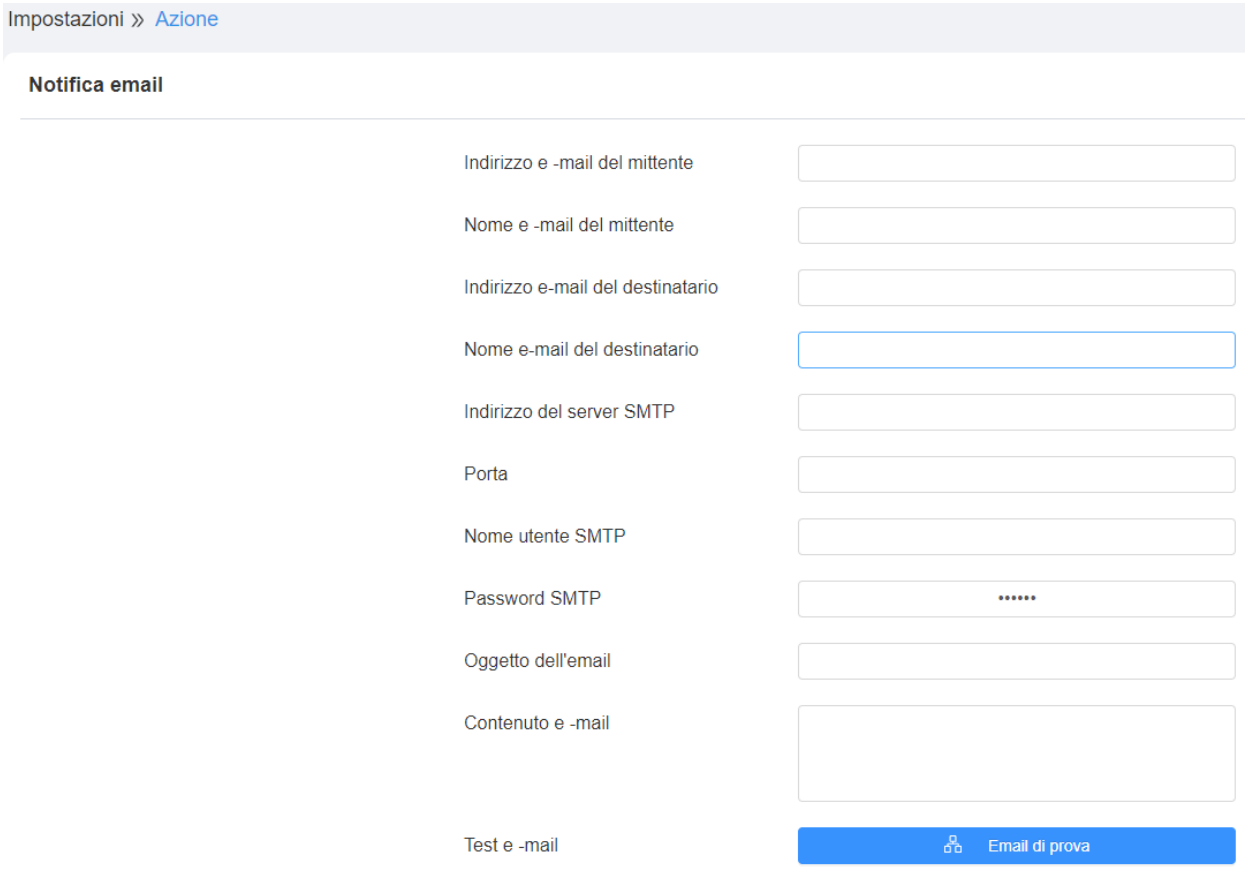
- Questa opzione necessita di Ekinex Delégo App per il suo funzionamento.

12.3 Impostazione delle notifiche di sicurezza

Sul citofono DICO sono disponibili diverse notifiche di sicurezza. I paragrafi successivi descrivono come impostarle.

12.3.1 Impostazioni delle email di notifica

Per ricevere le notifiche di sicurezza via e-mail, è necessario configurare correttamente le impostazioni e-mail dall'interfaccia web. Questa operazione può essere eseguita nella scheda al seguente percorso: **Impostazioni > Azione > Notifica e-mail.**



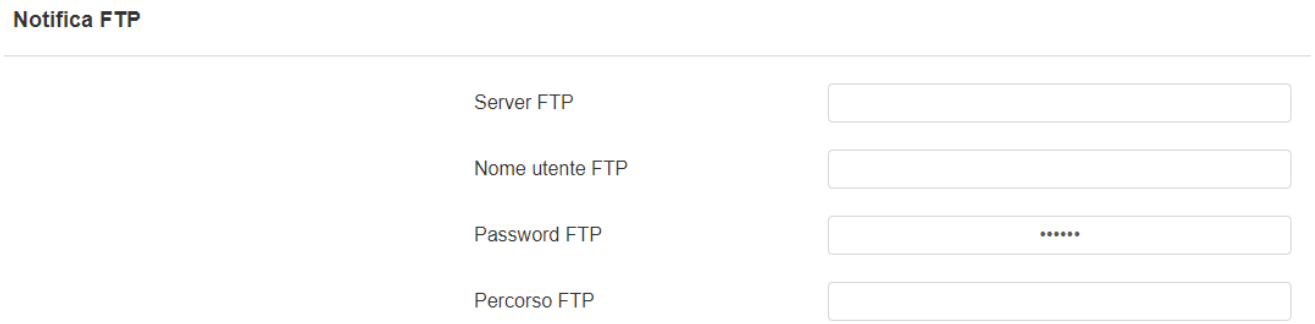
Impostazione parametri:

- **Indirizzo e-mail del mittente:** inserire l'indirizzo e-mail del mittente dal quale verrà inviata la notifica e-mail.
- **Nome e-mail del mittente:** inserire il nome del mittente e-mail.
- **Indirizzo e-mail del destinatario:** inserire l'indirizzo e-mail del destinatario.
- **Nome e-mail del destinatario:** inserire il nome del destinatario delle e-mail.

- **Indirizzo del server SMTP:** inserire l'indirizzo del server SMTP del mittente.
- **Porta:** inserire il numero della porta dalla quale verranno inviate le e-mail.
- **Nome utente SMTP:** inserire il nome utente SMTP, che solitamente corrisponde all'indirizzo email del mittente.
- **Password SMTP: c**onfigurare la password del servizio SMTP, che è la stessa dell'indirizzo e-mail del mittente.
- **Oggetto dell'e-mail:** inserire l'oggetto della e-mail.
- **Contenuto dell'e-mail:** inserire il contenuto della e-mail.

12.3.2 Impostazione delle notifiche FTP

È anche possibile ricevere le notifiche di sicurezza tramite FTP. In questo caso, è necessario configurare la notifica FTP dall'interfaccia web nella scheda **Impostazioni > Azione > Notifica FTP**



Impostazione parametri:

- **Server FTP**: inserire l'indirizzo (URL) del server FTP per l'invio delle notifiche FTP.
- **Nome utente FTP**: inserire il nome utente del server FTP.
- **Password FTP**: inserire la password del server FTP.
- **Percorso FTP**: inserire il nome della cartella creata nel server FTP.

12.3.3 Impostazione delle notifiche TFTP

If the user wants to receive the security notification via TFTP, it is necessary to configure the TFTP notification on the web interface at **Setting > Action > TFTP Notification**

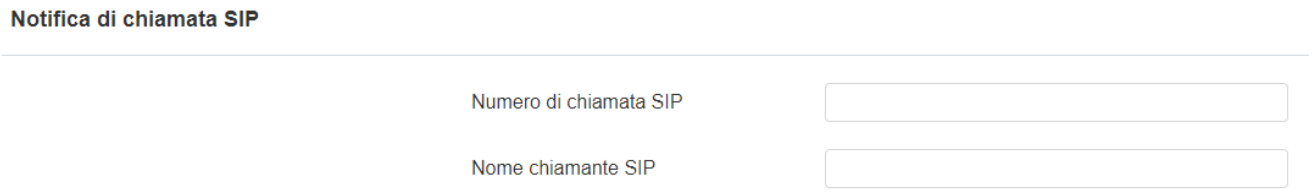
Se l'utente desidera ricevere la notifica di sicurezza tramite TFTP, è necessario configurare la notifica FTP sull'interfaccia web in **Impostazioni > Azione > Notifica TFTP**

Impostazione parametri:

- **Server TFTP**: inserire l'indirizzo (URL) del server TFTP per l'invio delle notifiche TFTP.

12.3.4 Impostazione delle notifiche con chiamata SIP

Se si desidera ricevere la notifica di sicurezza tramite chiamata SIP, è possibile configurare la relativa notifica sull'interfaccia web in **Impostazioni > Azione > Notifica di chiamata SIP**.



Impostazione parametri:

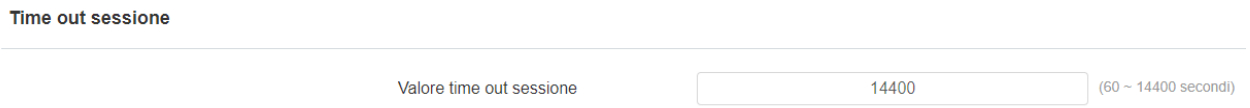
- **Numero di chiamata SIP**: inserire il numero per la chiamata SIP di notifica.
- **Nome chiamante SIP**: inserire il nome del chiamante per la notifica.

12.4 Impostazione del log-out automatico da interfaccia web

L'amministratore può impostare il timer di disconnessione automatica dall'interfaccia web. Allo scadere di questo timer è necessario effettuare nuovamente l'accesso inserendo il nome utente e la password.

Il log-out automatico può essere configurato per scopi di sicurezza o per comodità di funzionamento.

Per impostarlo, navigare sull'interfaccia web al seguente percorso: **Sistema > Sicurezza > Time out sessione**



Impostazione parametri:

- **Valore time out sessione:** per impostare il tempo di disconnessione automatica dell'interfaccia web, con valore compresi nell'intervallo da 60 secondi a 14400 secondi. Il valore predefinito è 300.

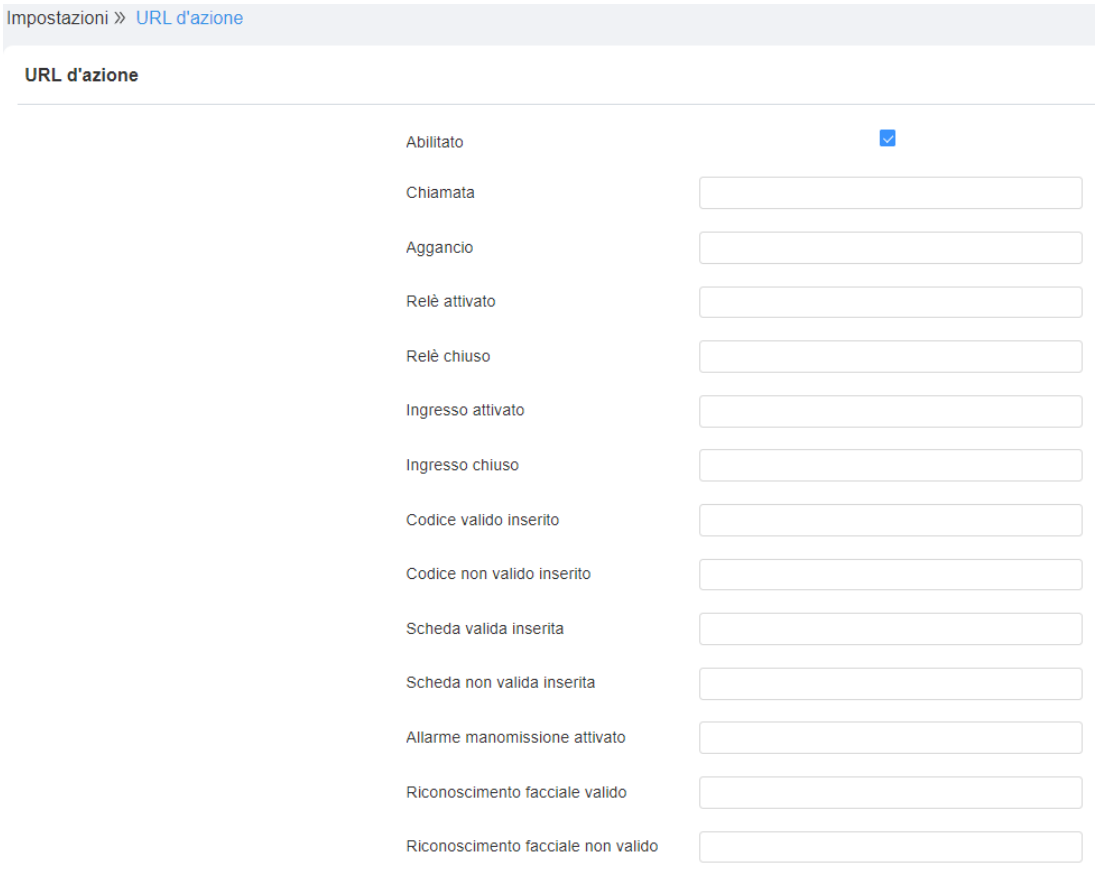
12.5 Comandi via URL

Il videocitofono DICO consente di impostare alcuni comandi HTTP con URL specifiche che verranno inviati al server HTTP per eseguire azioni predefinite. Verranno avviate le azioni pertinenti in base a eventuali modifiche allo stato del relè, allo stato dell'ingresso, agli accessi con codice PIN o con la RF Card, o ancora per motivi di sicurezza.

Questi comandi URL si possono impostare dall'interfaccia web nella scheda in **Impostazioni > URL d'azione.**

Nota

- Le URL delle azioni e il loro formato specifico sono forniti da un produttore di terze parti. Il citofono DICO invia soltanto l'URL ai dispositivi di terze parti.



Ad esempio:

http://YOUR_DEVICE_IP/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_s n=$card_sn

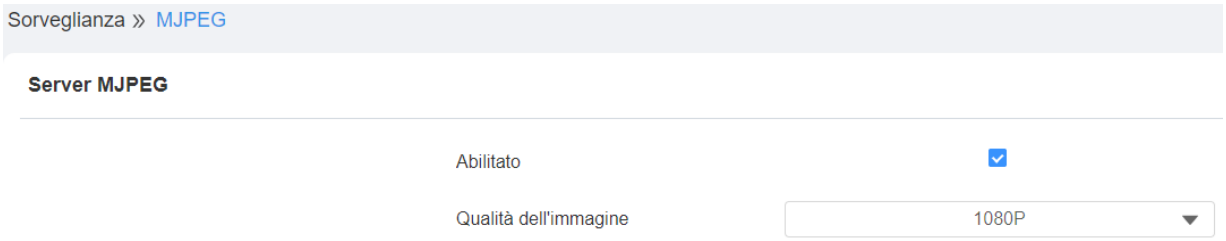
Il citofono DICO supporta il seguente formato di parametri per gli eventi elencati nella tabella seguente.

No.	Evento	Formato parametri	Esempio
1	Chiamata	$remote	http://server_ip/Callnumber=$remote
2	Aggancio	$remote	http://server_ip/Callnumber=$remote
3	Relè attivato	$relay1status	http://server_ip/relaytrigger=$relay1status
5	Relè chiuso	$relay1status	http://server_ip/relayclose=$relay1status
6	Ingresso attivato	$input1status	http://server_ip/inputtrigger=$input1status
7	Ingresso chiuso	$input1status	http://server_ip/inputclose=$input1status
8	Codice valido inserito	$code	http://server_ip/validcode=$code
9	Codice non valido inserito	$code	http://server_ip/invalidcode=$code
10	Scheda valida inserita	$card_sn	http://server_ip/validcard=$card_sn
11	Scheda non valida inserita	$card_sn	http://server ip/invalidcard=$card_sn
12	Allarme manomissione attivato	$alarm status	http://server ip/tampertrigger=$alarm status

13. Monitoraggio e immagini

13.1 Acquisizione di immagini in formato MJPEG

Il citofono DICO è dotato di una funzione per acquisire le immagini di monitoraggio in formato MJPEG, se necessario. È possibile abilitare questa funzione MJPEG e impostare la qualità dell'immagine da interfaccia web. Per configurarla, passare alla scheda **Sorveglianza > MJPEG > Server MJPEG.**



Impostazione parametri:

- **Abilitato**: consente di abilitare o disabilitare la funzione di acquisizione MJPEG.
- **Qualità dell'immagine:** permette di selezionare la qualità di acquisizione delle immagini fra sette opzioni: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P.**

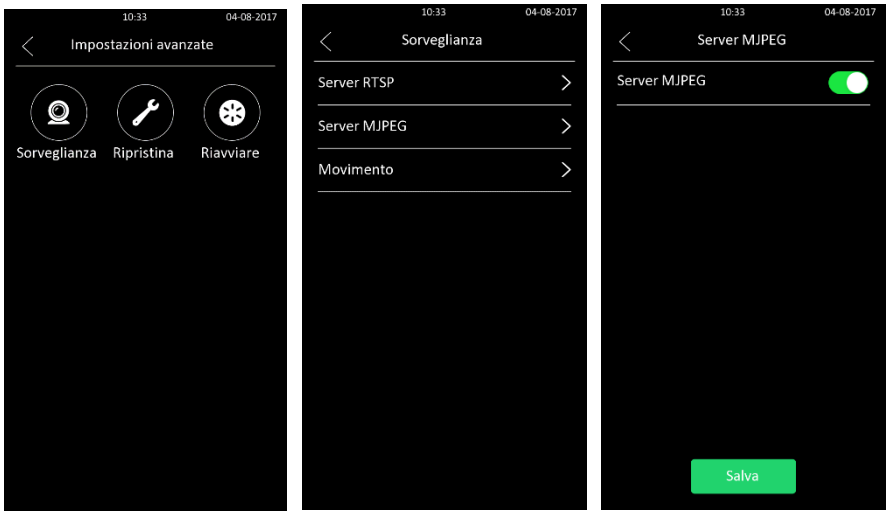
Una volta abilitato il servizio MJPEG, l'utente può acquisire le immagini dal videocitofono utilizzando i seguenti tre tipi di formato URL:

- http://device_ip:8080/picture.cgi
- http://device_ip:8080/picture.jpg
- http://device_ip:8080/jpeg.cgi

Ad esempio, per acquisire un immagine in formato jpg da un videocitofono con l'indirizzo IP: 192.168.1.104, l'utente può digitare in un web browser la seguente URL: http://192.168.1.104:8080/picture.jpg.

The MJPEG server function can be enabled also on the device directly. From the Setting window, it is necessary to tap on **Advanced > Surveillance > MJPEG server**.

La funzione server MJPEG può essere abilitata anche direttamente dal dispositivo. Dalla finestra **Impostazioni** è necessario entrare in **Avanzate > Sorveglianza > Server MJPEG**.

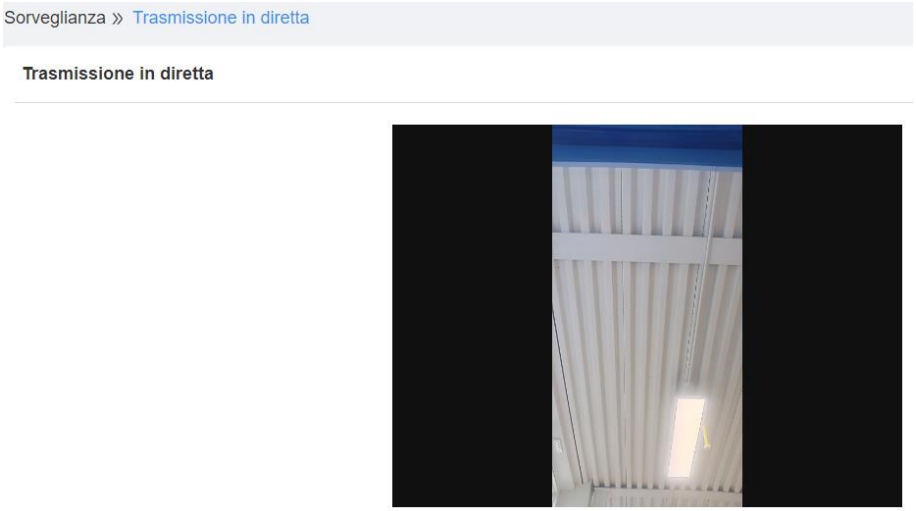


13.2 Trasmissione in diretta

Per controllare il video in tempo reale dal citofono DICO, l'utente può vedere direttamente dall'interfaccia web il flusso video in diretta.

In alternativa è possibile inserire una URL specifica in un browser web e visualizzare direttamente da questo.

Per impostare questa funzione dall'interfaccia web, andare in **Sorveglianza > Trasmissione in diretta.**



Per controllare il video in tempo reale utilizzando una URL, l'utente può inserire l'URL appropriata in un browser web (**http://IP_address:8080/video.cgi**).

Ad esempio: http://192.168.2.5:8080/video.cgi

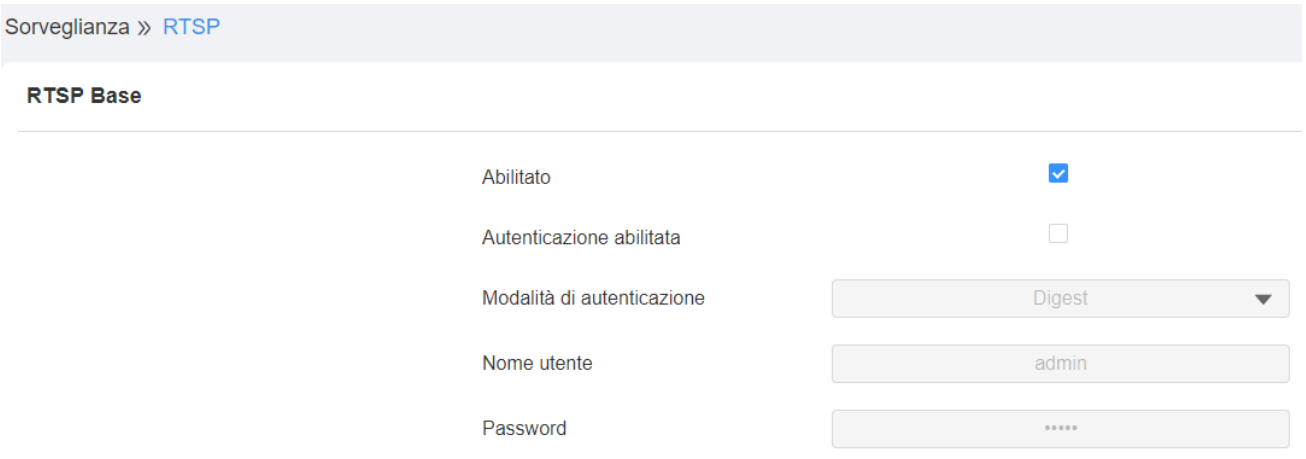
13.3 Monitoraggio del flusso RSTP

Il videocitofono DICO supporta il flusso RTSP, che consente ai dispositivi interfonici (come un monitor interno o un'unità di monitoraggio di terze parti) di controllare o ottenere audio/video in tempo reale (flusso RTSP) dal videocitofono utilizzando l'URL appropriata.

13.3.1 Impostazioni di base RSTP

La funzione RTSP deve essere configurata in termini di autorizzazione RTSP, autenticazione, password, e altri parametri.

Per impostare questa funzione dall'interfaccia web, l'utente deve andare su **Sorveglianza > RTSP > RTSP Base**



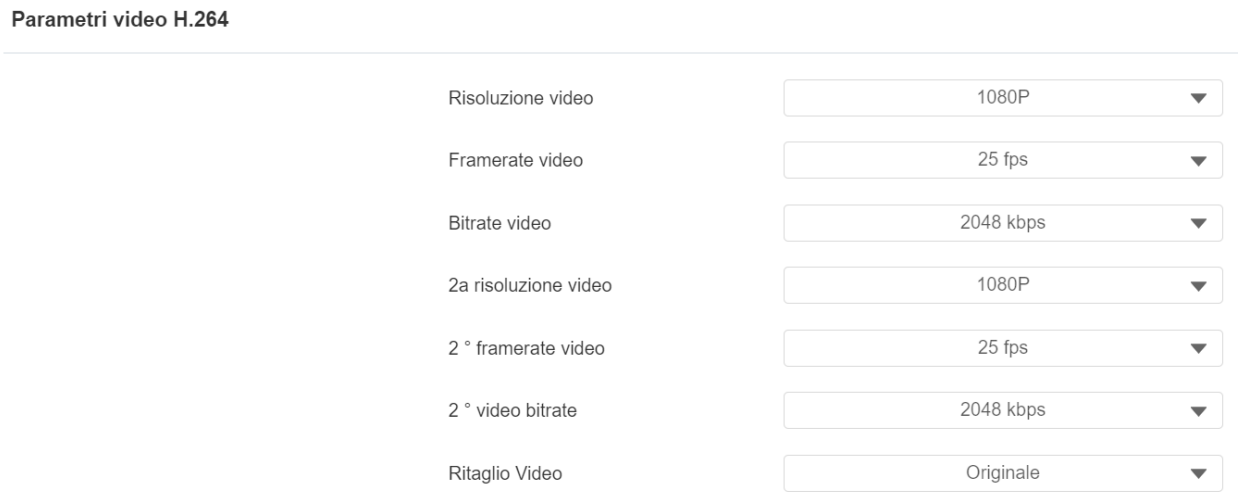
Impostazione parametri:

- **Abilitato**: per abilitare o disabilitare la funzione RSTP.
- **Autenticazione abilitata**: spuntare la casella di controllo per abilitare/disabilitare l'autorizzazione RTSP. Se si abilita l'autorizzazione RTSP, è necessario inserire il tipo di autenticazione RTSP, il nome utente RTSP e la password RTSP sul dispositivo interfonico, quale ad esempio un monitor interno, per l'autorizzazione.
- **Modalità di autenticazione**: selezionare il tipo di autenticazione RTSP tra **Base** e **Digest**. “Base” è il tipo di autenticazione predefinito. La differenza consiste nel fatto che il meccanismo di autenticazione “*Base*” invia le credenziali in "testo non crittografato". Invece, l'autenticazione “*Digest*” invia le credenziali in formato hash MD5.
- **Nome utente**: inserire il nome utente utilizzato per l’autorizzazione RTSP.
- **Password**: inserire la password per l’autorizzazione RTSP.

13.3.2 Impostazione del flusso RSTP

È possibile selezionare il formato del codec video del flusso RTSP per l'attività di monitoraggio e configurare la risoluzione video, il bitrate e altri parametri in base all'ambiente di rete installato.

Nell'interfaccia web, queste impostazioni possono essere effettuate accedendo a **Sorveglianza > RTSP > Parametri video H.264**



Impostazione parametri:

- **Risoluzione video**: può essere selezionata tra sette opzioni: **QCIF**, **QVGA**, **CIF**, **VGA**, **4CIF**, **720P** e **1080P**. La risoluzione video predefinita è **720P** e il video del citofono potrebbe non essere visualizzato sul monitor interno se la risoluzione è impostata su un valore superiore a 720P.
- **Framerate video**: la frequenza dei fotogrammi video predefinita è **25fps**.

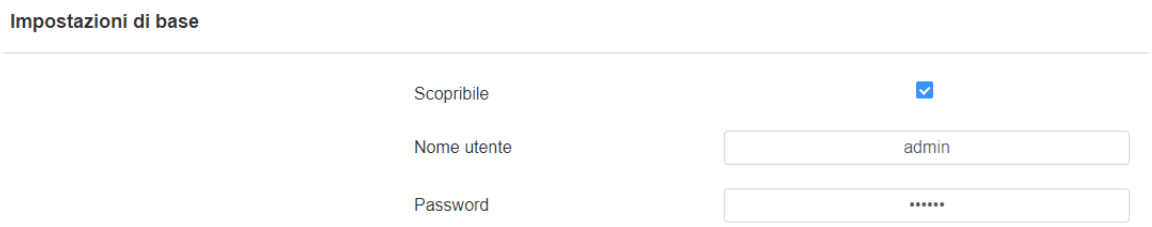
- **Bitrate video**: è possibile scegliere il bit-rate video tra 6 opzioni: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps,** e **4096 kbps** in base all'ambiente di rete. Il bitrate video per default è **2048 kbps**.
- **2a risoluzione video**: per selezionare la risoluzione video per il secondo canale del flusso video. La risoluzione video predefinita è **VGA**.
- **2° framerate video**: seleziona la frequenza dei fotogrammi video per il secondo canale del flusso video. Il valore predefinito è **25 fps**.
- **2° video bitrate**: consente la selezione del bit rate video per il secondo canale del flusso video, tra sei opzioni: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps,** e **4096 kbps** in base all'ambiente di rete. Il valore di default è **512 kbps**.
- **Ritaglio video**: selezionare **Originale** per la visualizzazione del video a schermo intero oppure **Predefinito** se si desidera selezionare solo un'area specifica del video da visualizzare. Con questa scelta, cliccando su "*Modifica*" viene avviata la selezione del video.

Nota

- Il videocitofono DICO supporta due canali di flusso video per il codec H.264.

13.4 Acquisizione in standard ONVIF

Il video in real-time reale ripreso dalla telecamera del terminale di controllo accessi DICO può essere visualizzato da dispositivi di terze parti come NVR (Network Video Recorder). È possibile configurare la funzione ONVIF nel terminale di controllo accessi in modo che altri dispositivi collegati possano visualizzare lo streaming video È possibile abilitare questa funzione dalla scheda **Sorveglianza > ONVIF.**



Impostazione parametri:

- **Scopribile**: consente di attivare o disattivare la modalità ONVIF. Riprendendo un video dalla telecamera del videocitofono, altri dispositivi collegati possono visualizzarlo. La modalità ONVIF è Scopribile per impostazione predefinita.
- **Nome utente**: inserire il nome utente. Il nome utente predefinito è admin.
- **Password**: inserisci la password. La password predefinita è admin.

Una volta completata l'impostazione, si può inserire l'URL ONVIF sul dispositivo di terze parti per visualizzare il flusso video.

Ad esempio: **http://indirizzo IP:80/onvif/device_service**

Dove indirizzo_IP è l'indirizzo IP specifico del videocitofono.

13.4.1 Modalità telecamera

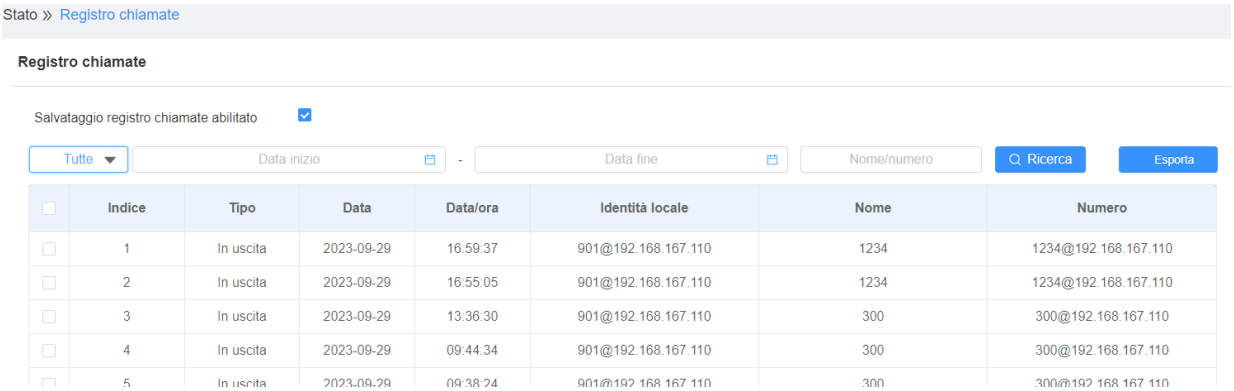
È possibile selezionare la modalità telecamera per una migliore qualità video, a seconda di dove è stato installato il videocitofono. Le opzioni consentite sono **Interno**, per una migliore immagine video (RTSP, ONVIF e Mjpeg) se il citofono è posizionato in uno spazio interno. Al contrario, se il video citofono è stato installato all'esterno, è opportuno selezionare la modalità **All'aperto**.

14. Registri

14.1 Registro chiamate

È possibile controllare le chiamate (in uscita, ricevute e perse) avvenute in un certo periodo di tempo, aprendo e ricercando il registro chiamate dall'interfaccia web del dispositivo. Inoltre, se necessario, è possibile esportare il registro delle chiamate dal dispositivo.

Per controllare il registro delle chiamate, dall'interfaccia web aprire la scheda **Stato > Registro chiamate**



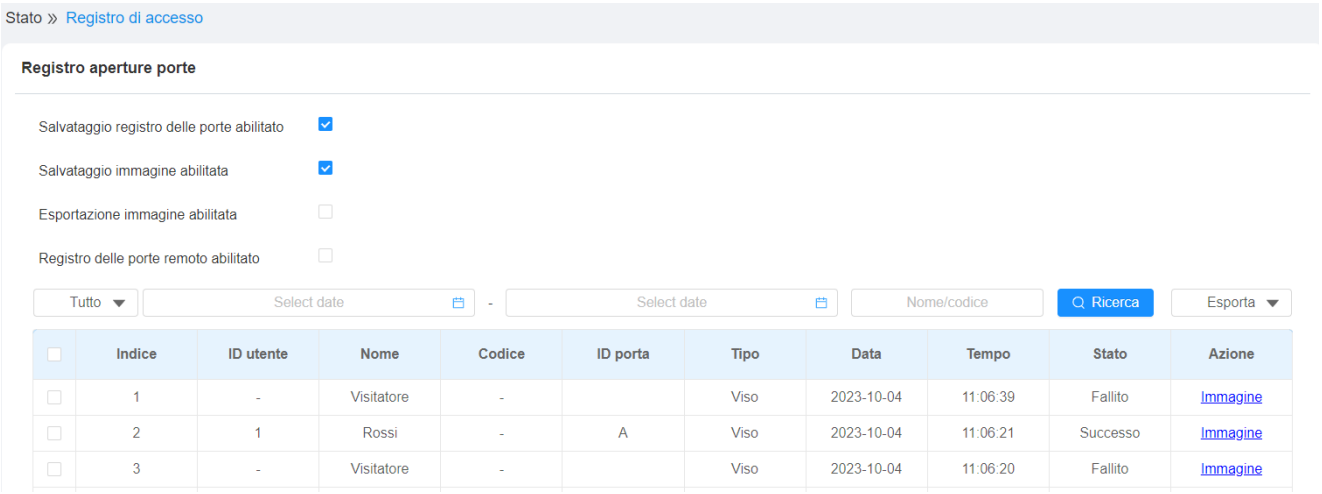
Impostazione parametri:

- **Salvataggio registro chiamate abilitato:** mettere una spunta alla casella per abilitare la funzione di salvataggio del registro chiamate.
- **Registro chiamate**: impostare la visualizzazione del registro tra quattro opzioni: **Tutte**, **In uscita**, **Ricevute** e **Perse**, per visualizzare un tipo specifico di chiamate.
- **Data di inizio ~ Data di fine**: permette di impostare l'intervallo di tempo specifico dei registri delle chiamate che si desidera cercare, visualizzare o esportare.
- **Identità locale**: visualizza l'account SIP o l'indirizzo IP del videocitofono che riceve le chiamate in entrata.
- **Nome/Numero**: selezionare le opzioni **Nome** e **Numero** per cercare nel registro chiamate in base al nome o al numero SIP o IP.

14.2 Registro accessi

Oltre ai registri delle chiamate, l'utente può consultare e controllare anche la cronologia degli accessi alla porta.

Per accedere a questo registro, dall'interfaccia web andare su **Stato > Registro di accesdso.**



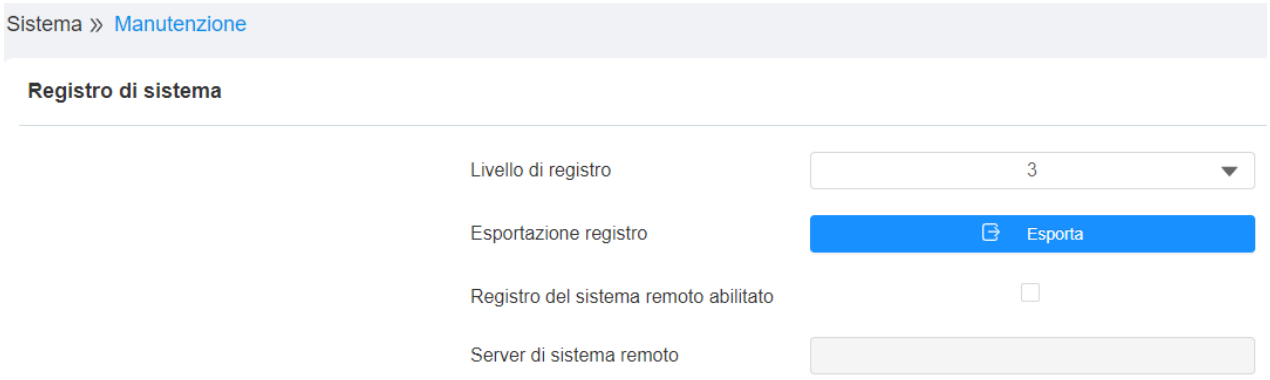
Impostazione parametri:

- **Salvataggio registro delle porte abilitato**: mettere una spunta alla casella per abilitare la funzione di salvataggio del registro accessi.
- **Salvataggio immagine abilitata**: mettere una spunta alla casella per abilitare la funzione di salvataggio dell'immagine scattata durante l'accesso o il tentativo di accesso.
- **Esportazione immagine abilitata**: mettere una spunta alla casella per abilitare la funzione di esportazione delle immagini salvate nel registro accessi.
- **Registro delle porte remoto abilitato**: per abilitare o disabilitare il salvataggio degli accessi alla porta su un registro remoto.
- **Stato:** scegliere un'opzione tra **Tutto, Successo** o **Fallito** per cercare accessi alle porte riusciti, accessi alle porte non riusciti o entrambi.
- **Data di inizio ~ Data di fine:** selezionare l'intervallo di tempo nel registro che si desidera cercare, controllare o esportare.
- **Nome/Codice**: selezionare le opzioni **Nome** o **Codice** per ricercare il registro delle porte in base al nome o al codice PIN.
- **Azione**: cliccare su "*immagine*" per visualizzare la foto scattata durante un determinato evento di accesso.

15. Debug

15.1 Registro di sistema per il debug

La funzione di registro di sistema del videocitofono DICO può essere utilizzata per scopi di debug. Se si desidera esportare il sistema su un PC locale o su un server remoto per il debug, è possibile impostare la funzione sull'interfaccia web in **Sistema > Manutenzione > Registro di sistema**



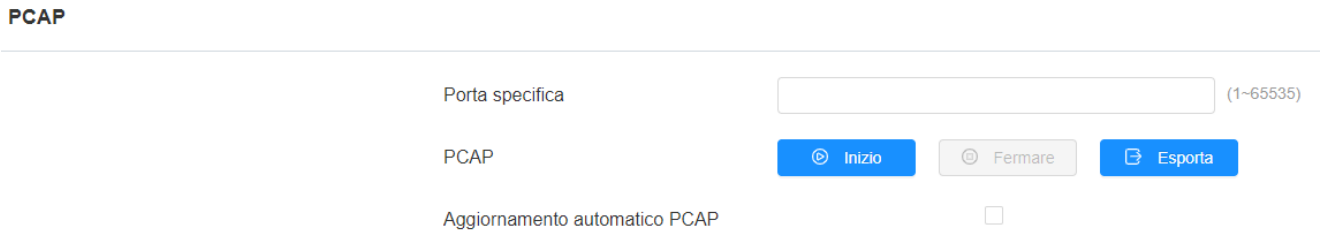
Impostazione parametri:

- **Livello di registro**: selezionare i livelli di registro in un intervallo di valori da 0 a 7. Il livello di registro predefinito è 3, il più alto è 5, il più completo è 7.
- **Esportazione registro**: cliccare su "*Esporta*" per esportare un file di registro di debug temporaneo su un PC locale.
- **Registro del sistema remoto abilitato**: per abilitare o disabilitare il registro del sistema remoto.
- **Server di sistema remoto**: immettere l'indirizzo del server remoto su cui salvare il registro di sistema del dispositivo.

15.2 PCAP per il debug

PCAP è un servizio utilizzato per acquisire in tempo reale sulla rete i pacchetti di dati ricevuti e trasmessi per il citofono DICO, a scopo di debug e risoluzione dei problemi.

Il servizio PCAC può essere configurato tramite l'interfaccia web in **Sistema > Manutenzione > PCAP** prima di utilizzarlo.



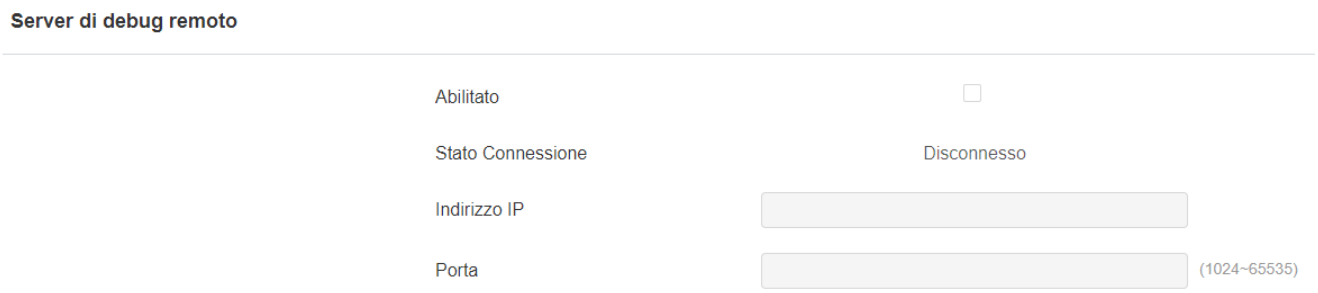
Impostazione parametri:

- **Porta specifica**: consente di selezionare le porte specifiche da 1 a 65535 in modo che possa essere catturato solo il pacchetto di dati dalla porta specifica. E' consentito lasciare il campo vuoto per impostazione predefinita.
- **PCAP**: premere il pulsante **Inizio** per acquisire un determinato intervallo di pacchetti di dati; premere il pulsante **Fermare** per interrompere l'acquisizione di pacchetti dati; premere **Esporta** per esportare i pacchetti di dati sul tuo PC locale.
- **Aggiornamento automatico PCAP**: spuntare la casella di controllo per attivare o disattivare la funzione di aggiornamento automatico PCAP. Se **abilitata**, il PCAP continuerà ad acquisire i pacchetti di dati anche dopo che i pacchetti di dati hanno raggiunto la capacità massima di 1 Mbyte. Se **disabilitata**, il PCAP interromperà l'acquisizione dei pacchetti di dati quando il pacchetto di dati catturato raggiungerà la capacità di acquisizione massima di 1 MByte.

15.3 Server di debug remoto

L'utente può configurare un server di debug remoto, in modo che il team di supporto Ekinex possa ottenere da remoto il registro per il debug del dispsoitivo.

Per configurare il server tramite l'interfaccia web, andare su **Sistema > Manutenzione > Server di debug remoto.**



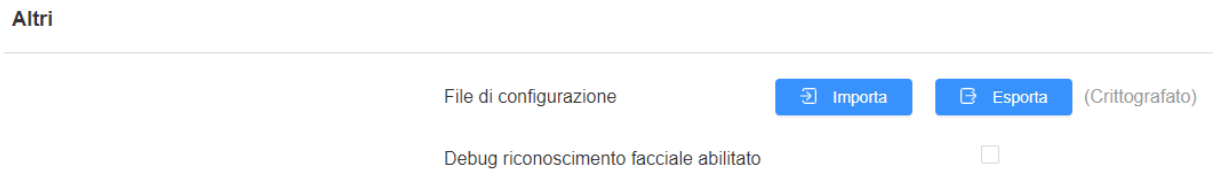
Impostazione parametri:

- **Abilitato**: per abilitare o disabilitare la funzione di server di debug remoto.
- **Stato connessione**: visualizza lo stato della connessione al server di debug remoto (connesso o disconnesso).
- **Indirizzo IP**: inserire l'indirizzo IP del server di debug remoto. Chiedere al support tecnico Ekinex l'indirizzo IP del server.
- **Porta**: inserire la porta del server di debug remoto.

15.4 Debug del riconoscimento facciale

Non appena si verifica un problema di riconoscimento facciale, è possibile eseguirne il debug se la relativa funzione di debug è stata abilitata in precedenza.

Per abilitarla dall'interfaccia web, andare in **Sistema > Manutenzione > Altri.**



Impostazione parametri:

- **File di configurazione**: per importare o esportare un file di configurazione per il servizio di debug del riconoscimento facciale.
- **Debug riconoscimento facciale abilitato**: per abilitare o disabilitare la funzione di debug per il riconoscimento facciale.

15.5 User Agent

Lo User Agent SIP (UA) è un dispositivo endpoint che supporta SIP, utilizzato per stabilire connessioni e abilitare sessioni tra due dispositivi endpoint. Uno UA è composto da UAC (User Agent Client) e UAS (User Agent server) con l'UAC utilizzato per inviare richieste e l'UAS utilizzato per inviare risposte.

Lo UA funge da fornitore di servizi SIP per l'utente specifico (dispositivo). È possibile personalizzare il campo dello UA nel messaggio SIP. Se lo UA è impostato su un valore specifico, gli utenti possono visualizzare le informazioni da PCAP. Se lo UA è vuoto, per impostazione predefinita gli utenti possono vedere il nome dell'azienda "Ekinex", il numero del modello e la versione del firmware da PCAP.

L'UA può essere configurato al seguente collegamento nell'interfaccia web: **Account > Avanzate > User Agent**

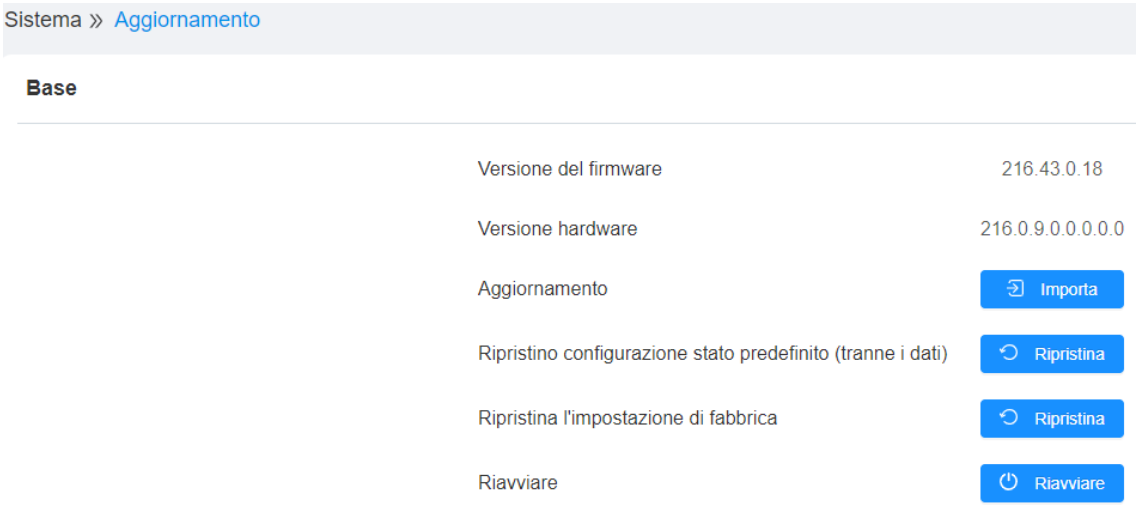
Impostazione parametri:

- **User Agent:** Ekinex è il valore di default, ma è possibile inserire un altro valore.

16. Aggiornamento firmware

Il firmware dei videocitofoni DICO può essere aggiornato tramite l'interfaccia web del dispositivo.

Questa funzionalità è disponibile al seguente collegamento: **Sistema > Aggiornamento**.



Nota

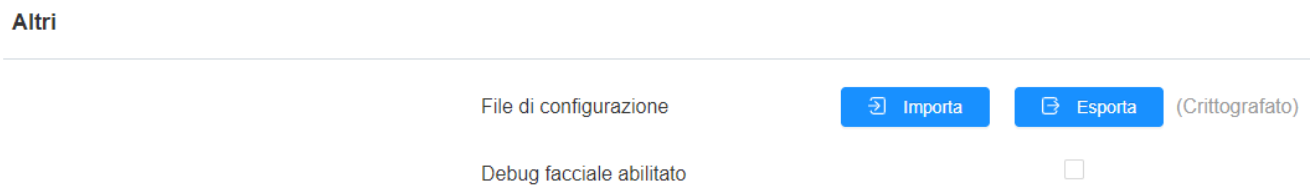
- I file del firmware devono essere disponibili in formato .**zip**

Impostazione parametri:

- **Versione del firmware**: visualizza la versione FW corrente del dispositivo.
- **Versione hardware:** visualizza la versione FW corrente del dispositivo.
- **Aggiornamento**: permette di caricare una nuova versione FW nel dispositivo.
- **Ripristino configurazione stato predefinito (tranne i dati)**: ripristina lo stato predefinito del dispositivo.
- **Ripristina l'impostazione di fabbrica**: ripristina i dati del dispositivo con i valori di fabbrica predefiniti.
- **Riavviare**: esegue un riavvio del dispositivo.

17. Backup

Per importare o esportare file di configurazione crittografati sul tuo PC locale, andare al seguente collegamento dell'interfaccia web: **Sistema > Manutenzione > Altri.**



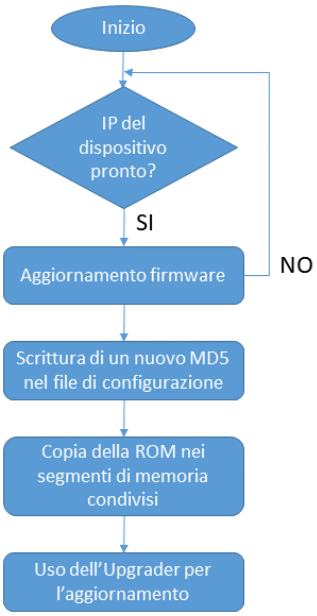
18. Provisioning automatico tramite file di configurazione

Le configurazioni e gli aggiornamenti sul citofono DICO possono essere eseguiti da interfaccia web tramite provisioning automatico una tantum, oppure con provisioning automatico pianificato tramite file di configurazione, evitando così di impostare manualmente le configurazioni necessarie una per una sul citofono.

18.1 Principi di provisioning

Il provisioning automatico è una funzionalità utilizzata per configurare o aggiornare i dispositivi in modo massivo, tramite server di terze parti. **DHCP**, **PNP**, **TFTP**, **FTP** e **HTTPS** sono i protocolli utilizzati dal dispositivo interfonico Ekinex DICO per accedere all'URL dell'indirizzo del server di terze parti che memorizza file di configurazione e firmware.

Questi file verranno poi utilizzati per aggiornare il firmware ed i relativi parametri del citofono.



18.2 File di configurazione per il provisioning automatico

I file di configurazione per il provisioning automatico hanno due formati: il primo è un file di configurazione generale utilizzato per il provisioning generale, l'altro è il provisioning della configurazione basato su MAC address.

La differenza tra i due tipi di file di configurazione è così riassumibile:

- **File di configurazione generale**: un file generale è archiviato in un server dal quale tutti i dispositivi correlati potranno scaricare lo stesso file di configurazione per aggiornare i parametri sui dispositivi. Ad esempio, un file .cfg
- **File di configurazione basato su MAC address**: I file di configurazione basati su MAC vengono utilizzati per il provisioning automatico su un dispositivo specifico contraddistinto dal suo MAC address univoco. I file di configurazione denominati con il numero MAC del dispositivo verranno abbinati automaticamente al numero MAC del dispositivo, prima di essere scaricati per il provisioning sul dispositivo specificato.

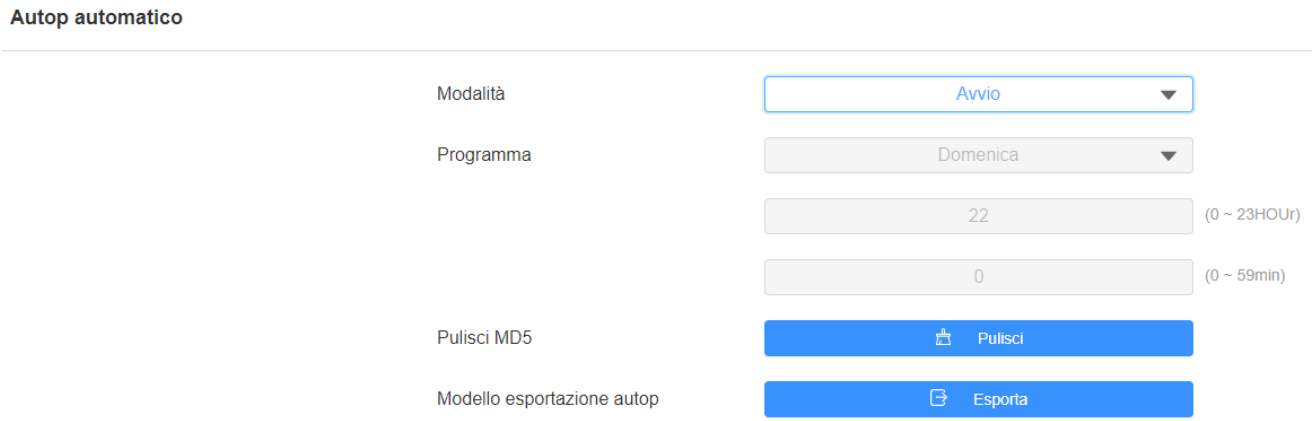
Nota

- Se un server dispone di entrambi i tipi di file di configurazione, i dispositivi IP accederanno innanzitutto ai file di configurazione generale, prima di accedere ai file di configurazione basati su MAC.

18.3 Programmazione del provisioning automatico (Autop)

Ekinex fornisce diversi metodi AutoP che consentono al videocitofono di eseguire il provisioning da solo in un momento specifico, in base alla pianificazione.

Per la configurazione, andare su **Sistema > Auto Provisioning > Autop automatico** nell'interfaccia web.



Impostazione parametri:

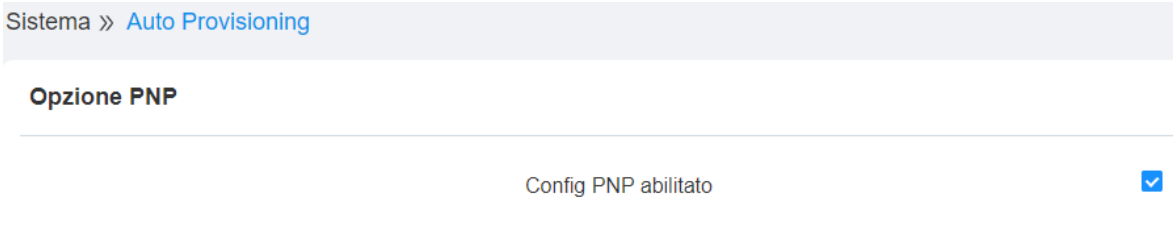
- **Modalità:** le opzioni disponibili sono:
    1. **Disabilitato**, se il servizio non è attivo.
    2. **Avvio**, se si vuole che il dispositivo esegua Autop ogni volta che si avvia;

3. **Da programma:** se si desidera che il dispositivo esegua l'Autop in base alla pianificazione impostata;
4. **Avvio + Da programma:** se si desidera combinare la modalità "*Avvio*" e la modalità "*Da programma*". Ciò consentirà al dispositivo di eseguire Autop ogni volta che si avvia e in base alla pianificazione impostata;
5. **Ripetizione oraria**: se si desidera che il dispositivo esegua l'Autop ogni ora.

18.4 Configurazione Plug-and-play (PNP)

Plug and Play (PNP) è una combinazione di supporto hardware e software che consente a un sistema informatico di riconoscere e adattarsi alle modifiche della configurazione hardware con un intervento minimo o nullo da parte dell'utente.

Per impostare la configurazione PNP da interfaccia web, andare su **Sistema > Auto Provisioning > Opzione PNP**.



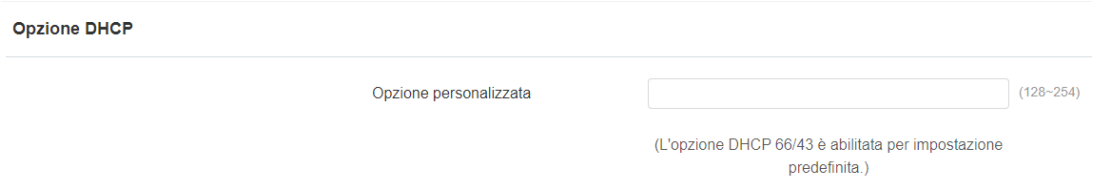
Impostazione parametri:

- **Config PNP abilitato:** per abilitare o disabilitare la configurazione PNP.

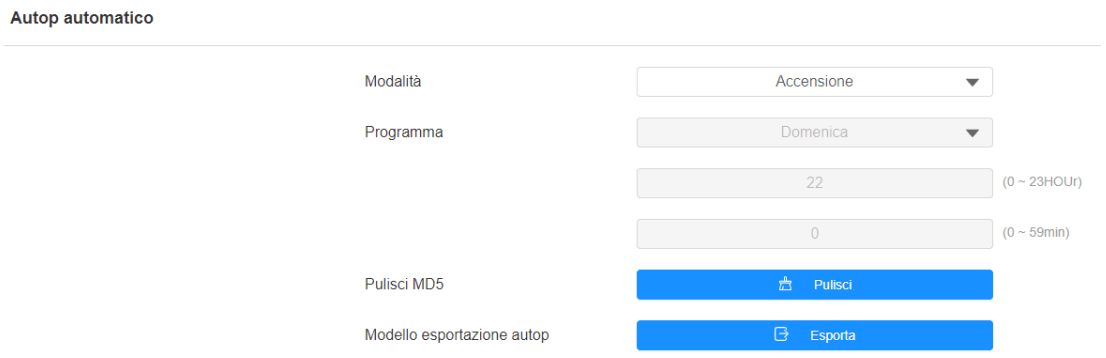
18.5 Configurazione del provisioning DHCP

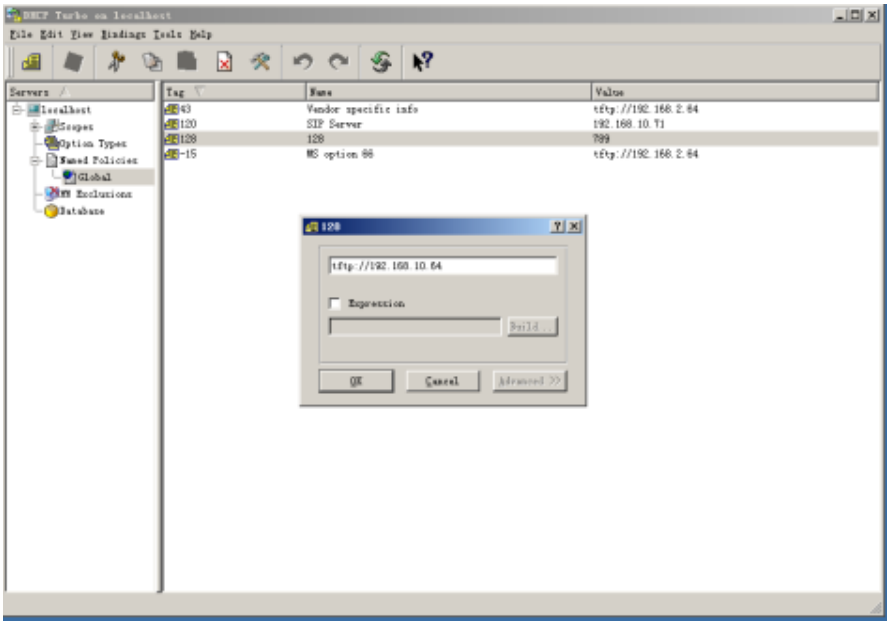
L'URL di provisioning automatica può essere ottenuta anche utilizzando l'opzione DHCP, che consente al dispositivo di inviare una richiesta a un server DHCP per un codice opzione DHCP specifico.

Se l'utente desidera utilizzare l'opzione personalizzata con codice opzione compreso tra 128 e 255, è tenuto a configurarla sull'interfaccia web in **Sistema > Auto Provisioning > Opzione DHCP**



Per impostare AutoP con DHCP, con “Opzione personalizzata” e modalità “Accensione”, seguire il collegamento **Sistema > Auto Provisioning > Autop automatico** sull'interfaccia web. Quindi cliccare il pulsante Esporta in “*Modello esportazione Autop*” per esportare il modello Autop. Infine, impostare l'opzione DHCP sul server DHCP.





Impostazione parametri:

- **Opzione personalizzata:** le possibili opzioni sono:

Nota

- L’opzione personalizzata deve essere Il valore nell’URL del server TFTP

1. **Personalizzata:** inserire il codice DHCP che corrisponde all'URL corrispondente in modo che il dispositivo trovi il file server di configurazione per la configurazione o l'aggiornamento.
2. **Opzione DHCP 66:** se non viene impostata l'opzione precedente, il dispositivo utilizzerà automaticamente l'opzione DHCP 66 per ottenere l'URL del server di aggiornamento. Questo viene fatto all'interno del software e l'utente non ha bisogno di specificarlo. Per farlo funzionare, è necessario configurare il server DHCP per l'opzione 66 con l'URL del server aggiornato al suo interno.
3. **Opzione DHCP 43:** se il dispositivo non ottiene un URL dall'opzione DHCP 66, utilizzerà automaticamente l'opzione DHCP 43. Questa operazione viene eseguita all'interno del software e non è necessario che l'utente lo specifichi. Per farlo funzionare, è necessario configurare il server DHCP per l'opzione 43 con l'URL del server aggiornato al suo interno.

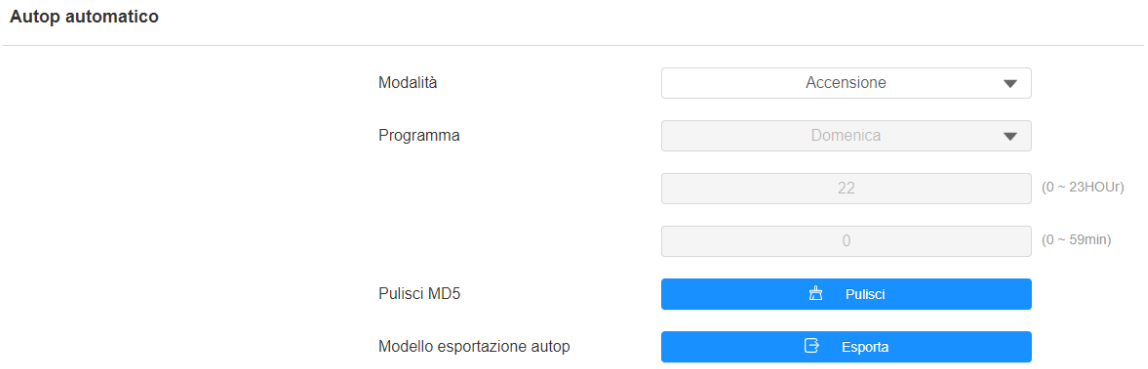
Nota

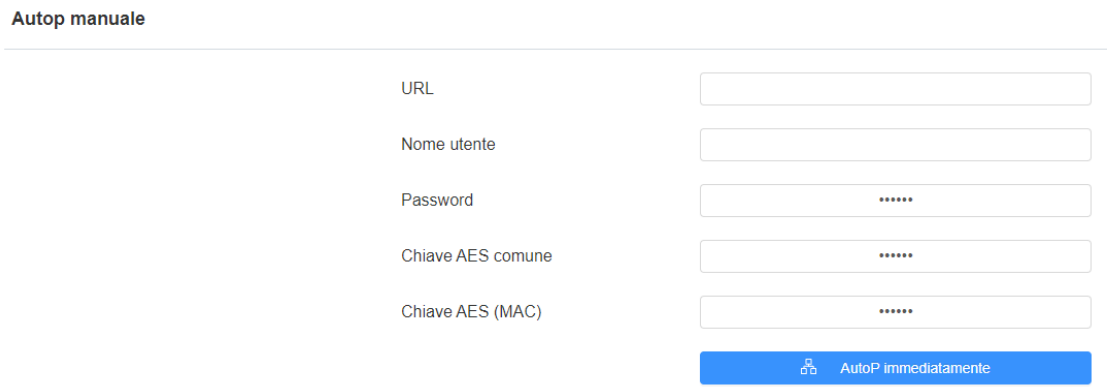
- Il file di configurazione generale per il provisioning in batch è nel formato **rcfg**. Ad esempio, con E16 diventa r000000000116.cfg (9 zeri in totale). Invece il file di configurazione basato su MAC per il provisioning del dispositivo specifico ha il formato MAC_Address del dispositivo con estensione .cfg, ad esempio **0C110504AE5B.cfg**.

18.6 Configurazione del provisioning statico

È possibile impostare manualmente una URL del server specifica per scaricare il firmware o il file di configurazione. Se è impostata una pianificazione Autop, il videocitofono eseguirà l'auto-provisioning in un momento specifico, in base alla pianificazione Autop precedentemente configurata. Inoltre, TFTP, FTP, HTTP e HTTPS sono i protocolli che possono essere utilizzati per aggiornare il firmware e la configurazione del dispositivo.

Per scaricare il modello Autop, seguire **Sistema > Auto Provisioning > Autop automatico** dall'interfaccia Web e configurare il server Autop su **Sistema > Auto Provisioning > Autop manuale.**





Impostazione parametri:

- **URL**: imposta gli indirizzi dei server TFTP, HTTP, HTTPS e FTP per il provisioning.
- **Nome utente**: imposta un nome utente se il server necessita di un nome utente per accedere, altrimenti può rimanere vuoto.
- **Password**: impostare una password se il server necessita della password per accedere altrimenti può rimanere vuoto.
- **Chiave AES comune**: impostare il codice AES sul videocitofono, per decifrare i file di configurazione generali del provisioning automatico.
- **Chiave AES (MAC)**: impostare il codice AES per decifrare il file di configurazione del provisioning automatico basato su MAC.

Note:

- AES è un algoritmo di cifratura, deve essere configurato solo quando il file di configurazione è crittografato con AES, altrimenti lasciare il campo vuoto.
- Esempio di formati dell'indirizzo server:
  - TFTP: tftp://192.168.0.19/
  - FTP:
    - ftp://192.168.0.19/ (consente login anonimo)
    - ftp://username:password@192.168.0.19/ (richiede nome utente e password)
  - HTTP:
    - http://192.168.0.19/ (usa come default la porta 80)
    - http://192.168.0.19:8080/ (usa altre porte, come la 8080)
    - HTTPS: https://192.168.0.19/ (usa come default la porta 443)

Nota

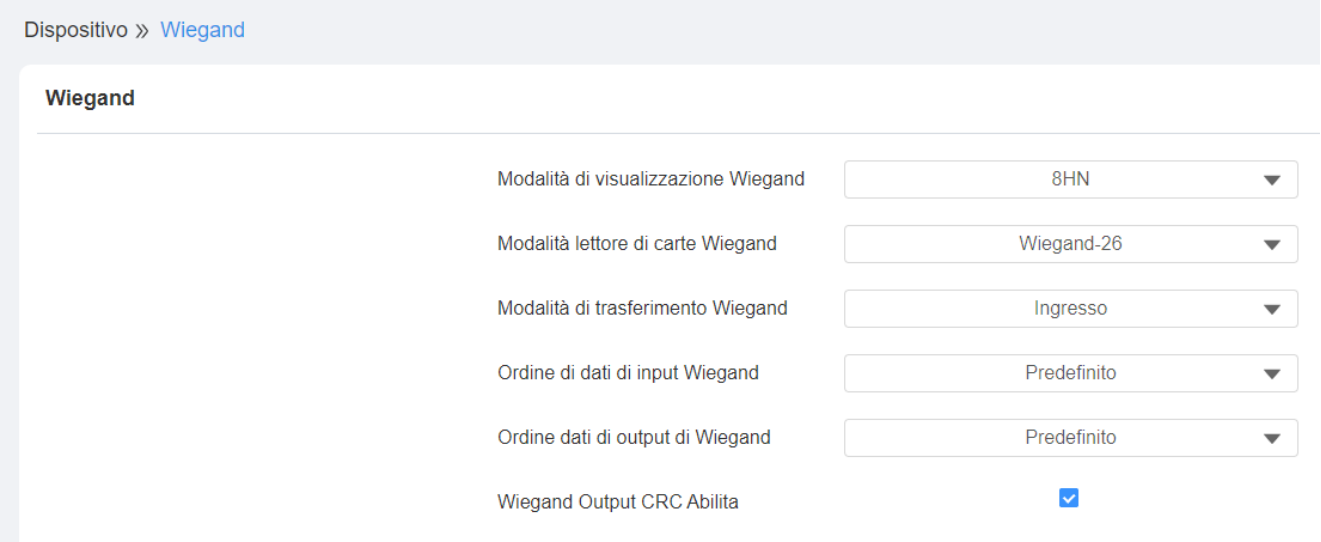
- Ekinex non fornisce server specifici per l'utente.
- L'utente è invitato a configurare autonomamente il server TFTP/FTP/HTTP/HTTPS.

19. Integrazione con dispositivi di terze parti

19.1 Integrazione Wiegand

Il dispositivo DICO consente di configurare una connessione Wiegand, un protocollo standard comunemente utilizzato nei sistemi di controllo degli accessi.

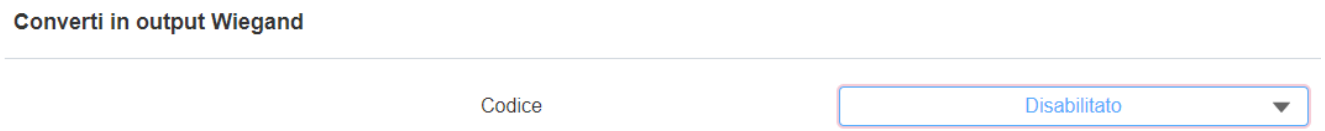
Se si desidera integrare il videocitofono DICO con dispositivi di terze parti tramite Wiegand, è possibile impostare i parametri dall'interfaccia **Dispositivo > Wiegand.**



Impostazione parametri:

- **Modalità di visualizzazione Wiegand**: selezionare il formato del codice Wiegand Card tra **8H10D, 6H3D5D, 6H8D, 8HN, 8HR**, **RAW** e **8HR10D**.
- **Modalità lettore di carte Wiegand**: consente di impostare il formato di trasmissione dati Wiegand tra tre opzioni: **Wiegand-26**, **Wiegand-34**, **Wiegand-58**. Il formato di trasmissione tra il videocitofono e il dispositivo da integrare deve essere il medesimo.
- **Modalità di trasferimento Wiegand**: permette di impostare la modalità di trasferimento tra **Ingresso**, **Uscita** o **Converti in Output scheda n**., a seconda che il videocitofono sia utilizzato come ricevitore o come trasmettitore.
- **Ordine di dati input Wiegand**: imposta la sequenza dei dati di Input Wiegand tra **Predefinito** e **Compatibile**. Nel secondo caso, il numero della scheda di input verrà invertito.
- **Ordine dati di output Wiegand**: imposta la sequenza dei dati di Output Wiegand tra **Predefinito** e **Compatibile**. Nel secondo caso, il numero della scheda di output verrà invertito.
- **Wiegand output CRC abilita**: questa funzione è utilizzata per l'ispezione dei dati Wiegand. È attivata di default. Se non è attivata, l'integrazione del videocitofono con dispositivi di terze parti potrebbe non essere realizzabile.

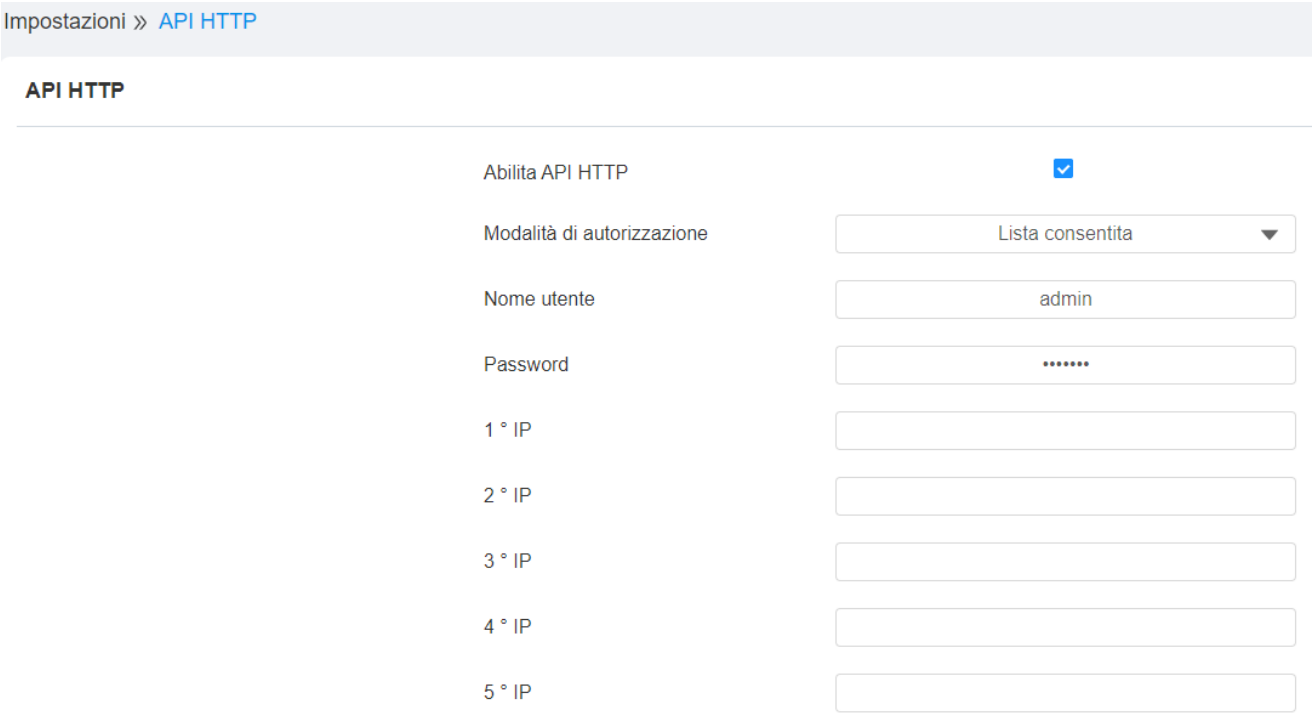
Se si seleziona **Modalità di trasferimento Wiegand = Uscita**, allora è possibile impostare il codice per la conversione input/output:



- **Codice:** consente di impostare il tipo di codifica per la conversione, a scelta tra le opzioni **Disabilitato**, **8 bit per cifra**, **4 bit per cifra** o **Tutto in una volta.**

19.2 Integrazione con API HTTP

L'API HTTP è progettata per ottenere un'integrazione basata sulla rete tra il dispositivo di terze parti con il dispositivo interfonico Ekinex DICO. È possibile configurare la funzione API HTTP sull'interfaccia web in **Impostazioni > API HTTP**



Impostazione parametri:

- **Abilita API HTTP:** abilita o disabilita la funzione API HTTP per l'integrazione di terze parti. Ad esempio, se la funzione è disabilitata, qualsiasi richiesta di avvio dell'integrazione verrà negata e verrà restituito lo stato *HTTP 403 forbidden*.

- **Modalità di autorizzazione:** selezionare tra cinque opzioni: **Nessuno**, **Lista abilitata**, **Base**, **Digest** e **Token** per il tipo di autorizzazione.

- **Nome utente:** immettere il nome utente quando è selezionata la modalità di autorizzazione "*Base*" o "*Digest*". Il nome utente predefinito è **Admin**.
- **Password:** immettere la password quando è selezionata la modalità di autorizzazione "*Base*" o "*Digest*". Il nome utente predefinito è **Admin**.
- **1°IP-5°IP:** inserire l'indirizzo IP dei dispositivi di terze parti quando viene selezionata l'impostazione "*Lista abilitata*" come Modalità di autorizzazione.

19.3 Controllo ascensore

È possibile collegare il videocitofono DICO con un controller per ascensore Ekinex o con un controller di terze parti compatibile, in modo da effettuare la gestione dell'ascensore. È possibile chiamare l'ascensore per scendere al piano terra quando si è autorizzati tramite vari tipi di metodi di accesso sul citofono.

Per impostare il controllo dell'ascensore, dall'interfaccia andare su **Dispositivo > Controllo ascensore > Elenco di controllo ascensore.**

Impostazione parametri:

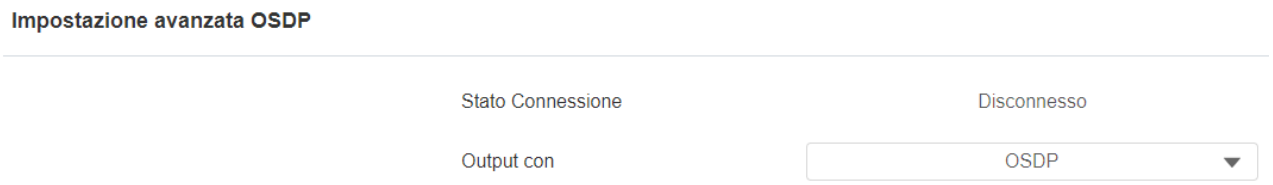
- **Elenco di controllo ascensore:** selezionare la modalità di integrazione tra le seguenti opzioni: **Nessuna**, **OSDP**, **Ekinex**, **KEYKING**. I dettagli per le opzioni sono riportati forniti nella seguente tabella.

Num.	Modalità di integrazione	Descrizione
1	Nessuna	Integrazione disabilitata
2	OSDP	Selezionando questa modalità, l'integrazione tra il videocitofono DICO e il dispositivo di terze parti avviene tramite protocollo OSDP. E' necessario controllare il protocollo di integrazione del dispositivo e dell'ascensore, per assicurarsi che utilizzino lo stesso protocollo di integrazione.

Num.	Modalità di integrazione	Descrizione
3	Ekinex	Selezionare Ekinex se si desidera collegare il dispositivo al controller di sollevamento Ekinex.
4	KEYRING	Selezionare KEYKING se si desidera l'integrazione con il controller dell'ascensore KEYKING.

19.3.1 Modalità di integrazione OSDP

Se la modalità di integrazione selezionata è OSDP, l'utente deve configurare alcune impostazioni avanzate:

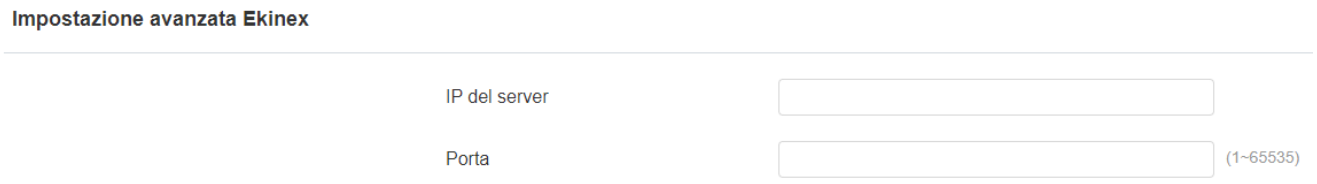


Impostazione parametri:

- **Stato connessione**: le opzioni disponibili sono **Connesso** o **Disconnesso**
- **Output con**: le opzioni sono **OSDP** o **Nessuno**.

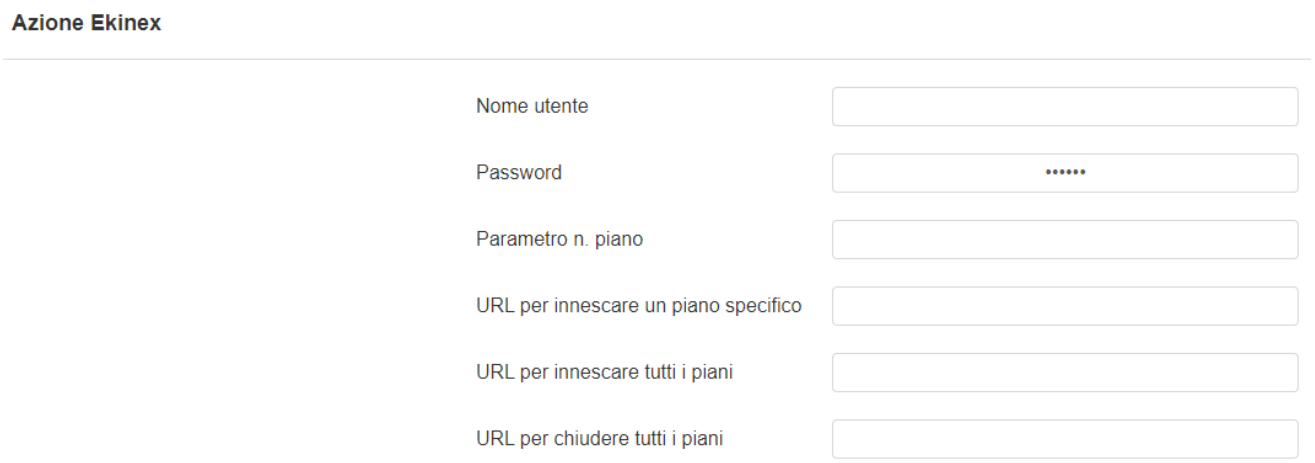
19.3.2 Modalità di integrazione Ekinex

Se la modalità di integrazione selezionata è Ekinex, sono disponibili i seguenti parametri:



Impostazione parametri:

- **IP del server**: l'indirizzo IP del server a cui è connesso il controller
- **Porta**: la porta di comunicazione del controller



- **Nome utente:** il nome utente per connettersi al servizio ascensore
- **Password**: la password per il servizio
- **Parametro n. piano:** il parametro per identificare il numero del piano
- **URL per innescare un piano spefico**: inserire qui l'URL del server per un numero di piano specifico
- **URL per innescare tutti i piani**: inserire qui l'URL del server per rendere raggiungibili tutti i piani
- **URL per chiudere tutti i piani**: inserire qui l'URL del server per configurare i piani inaccessibili.

19.3.3 Modalità di integrazione KEYRING

Se la modalità di integrazione selezionata è KEYRING, sono disponibili i seguenti parametri:

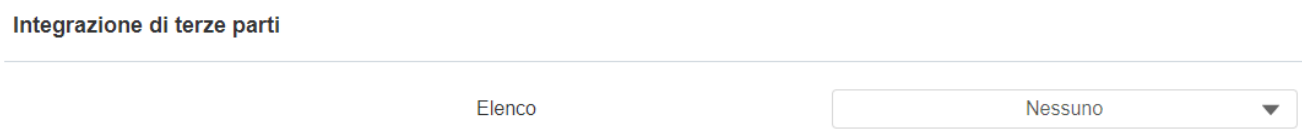
Impostazione parametri:

- **Indirizzo**: seleziona qui l'indirizzo per l'integrazione KEYRING.

19.4 Integrazione con server di controllo accessi di terze parti

È possibile accedere al videocitofono utilizzando il codice QR o la tessera di accesso generata da un server di terze parti. Ad esempio, quando si utilizza il codice QR sul citofono, il codice QR verrà inviato al server di terze parti per la verifica. All'utente verrà concesso l'accesso se il codice QR supera la verifica.

Per configurarlo, andare su **Controllo accessi > Relè > Integrazione di terze parti** nell'interfaccia web.



Impostazione parametri:

- **Elenco**: permette di selezionare le modalità di integrazione, fra le seguenti opzioni:
  1. Per disabilitare la funzione, scegliere **Nessuno**.
  2. Per usare soltanto il codice QR, selezionare **Generale**.
  3. Per scegliere un codice QR e una tessera d'accesso con caratteristiche personalizzate, selezionare **Personalizzato.**
- **URL HTTP:**
  1. Per la modalità "*Generale*": inserire l'URL HTTP ottenuta dal fornitore di servizi di terze parti. Dopo aver scansionato il codice QR, l'URL HTTP conterrà automaticamente le informazioni del codice QR dinamico e potrà inviarle al server del codice QR per la verifica.

     Si veda l'esempio seguente:

     http://wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode} &deviceId={DeviceID}
  2. Per la modalità "*Personalizzare*": mettere un segno di spunta come **Verifica remota** su **QR code** o **Carta**.
  3. Per la verifica remota con QR code, inserire la URL HTTP del codice QR ottenuta dal fornitore di servizi di terze parti.

     Si veda l'esempio seguente:

     http://www.server.com/<base>/hs/ACS/checking/QRCode/{DeviceID}/{Card}
  4. Per la verifica remota con Carta, inserire la URL HTTP del carta di accesso ottenuta dal fornitore di servizi di terze parti.

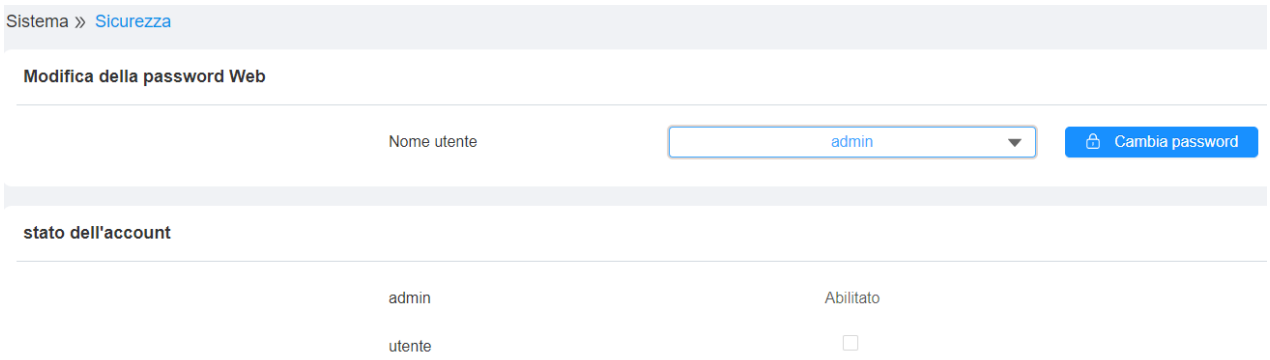
     Si veda l'esempio seguente:

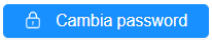
     http://www.server.com/<base>/hs/ACS/checking/{QRCode}/{DeviceID}/Card
- **Prompt su LCD**: selezionare **Predefinito**, se si vuole adottare la notifica del videocitofono Ekinex per l'accesso alla porta. Selezionare **Valore di ritorno** se si preferisce utilizzare il valore restituito dal server di terze parti come notifica.
- **Verifica remota**: selezionare la verifica da remoto basata su **QR code, Carta,** o entrambe.
- **ID del dispositivo**: inserire l'ID del proprio dispositivo, che verrà aggiunto automaticamente all'URL HTTP quando si utlizza un codice QR o una scheda per l'accesso.

20. Modifica password

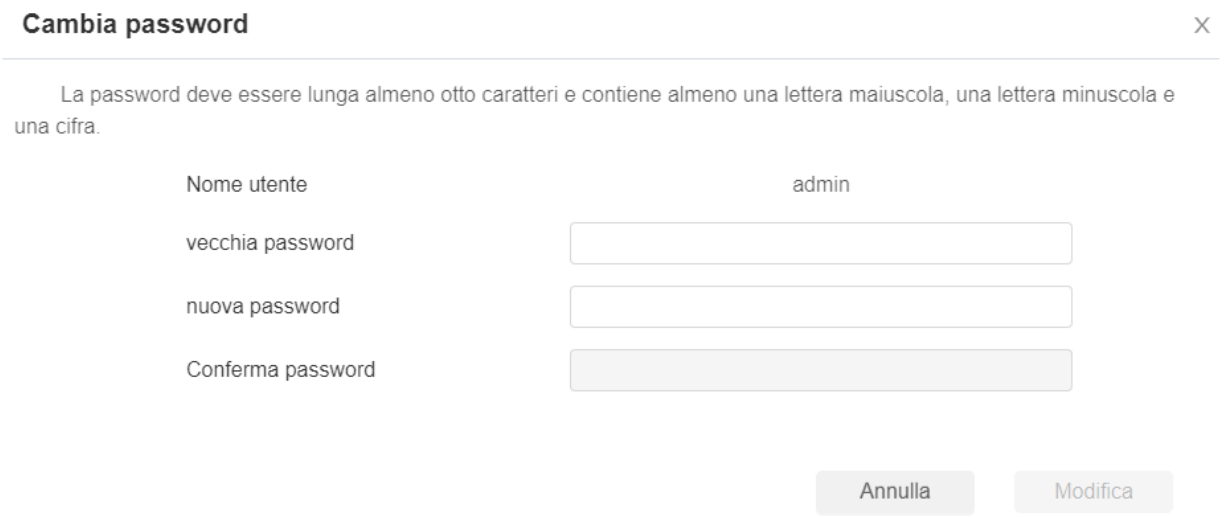
L'utente può impostare e modificare sia il codice PIN di sistema per accedere alle impostazioni del dispositivo sia la password di accesso all'interfaccia web. Inoltre, può anche selezionare il ruolo (amministratore o utente) durante l'impostazione delle password.

Per impostare la password, nell'interfaccia web andare su **Sistema > Sicurezza > Modifica password web**



Premendo il pulsante 

, all'utente verrà richiesto di inserire le informazioni come di seguito:



Per impostare il codice PIN di sistema l'utente può fare riferimento alla sezione **PIN di sistema** nella stessa pagina.

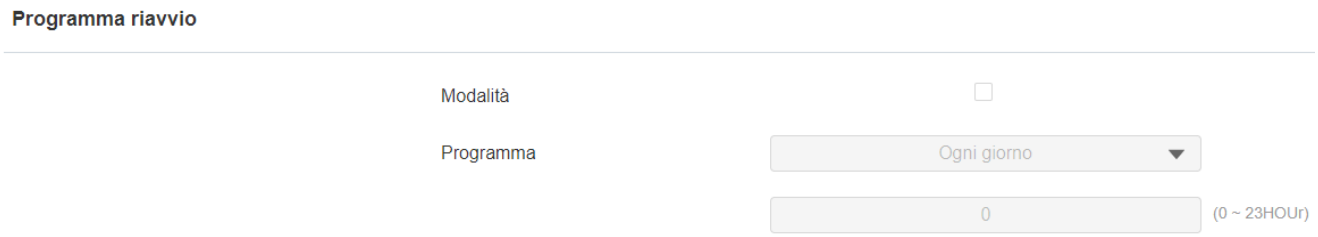
21. Riavvio e ripristino del sistema

21.1 Riavvio

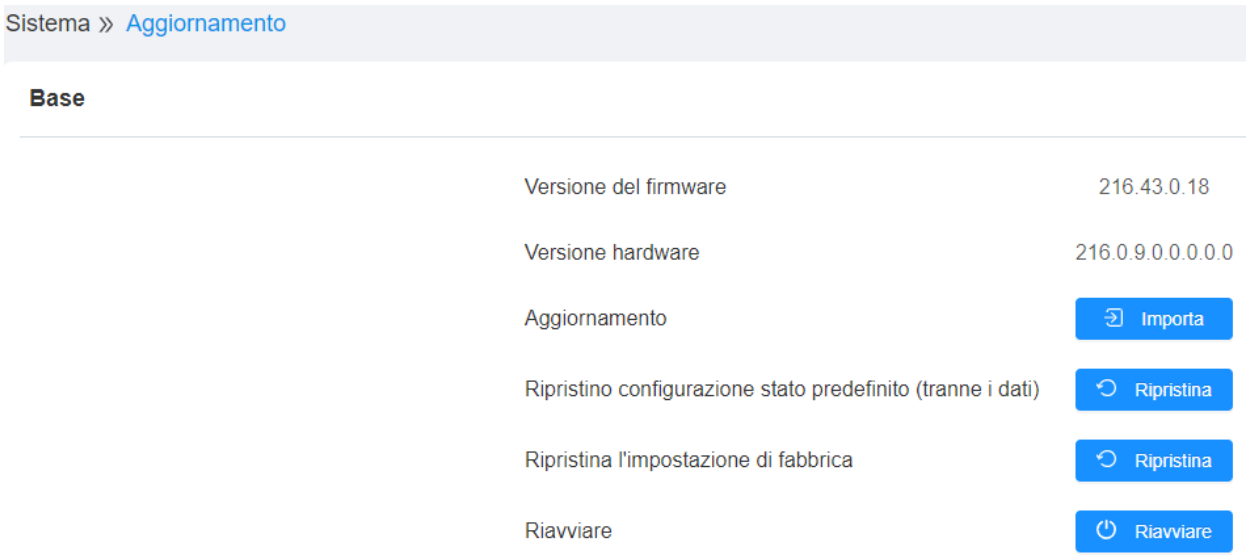
L'utente può riavviare il dispositivo dall'interfaccia web.

Inoltre, è possibile impostare un programma orario per il riavvio del dispositivo.

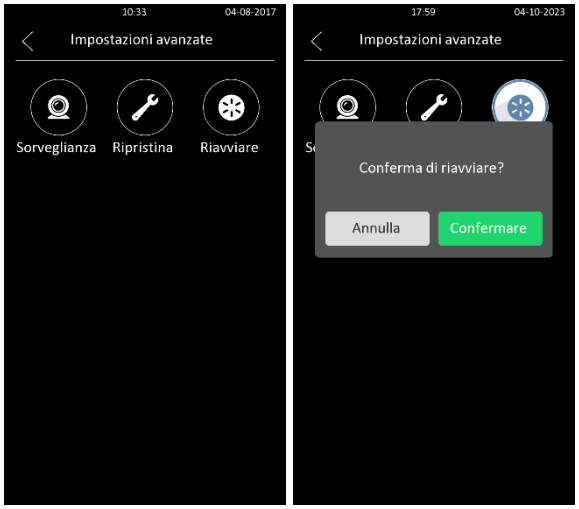
Per impostare la pianificazione del riavvio del dispositivo, nell'interfaccia web andare su **Sistema > Auto Provisioning automatico > Programma riavvio.**



Per riavviare manualmente il dispositivo, andare su **Sistema > Aggiornamento > Base** nell'interfaccia web e cliccare sul pulsante **Riavviare**.



Per effettuare un riavvio dal dispositivo stesso, accedere alla pagina **Impostazioni** e cliccare su Avanzate > Riavvia.

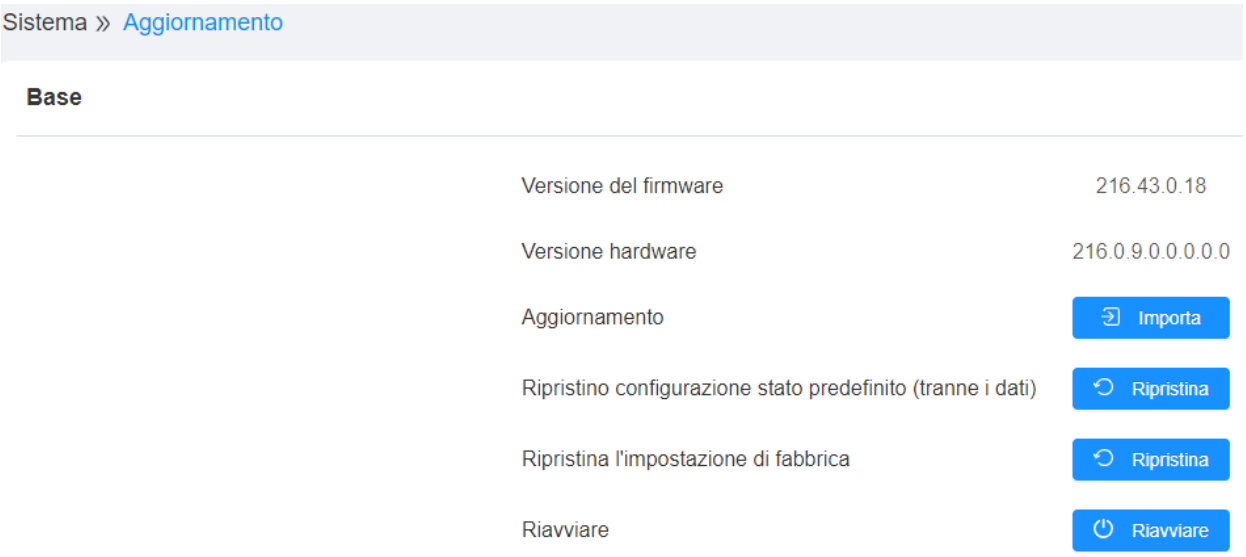


21.2 Reset

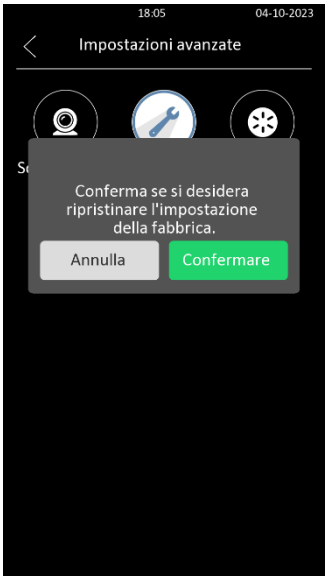
L'utente può selezionare l'opzione **Ripristina l'impostazione di fabbrica** per riportare il dispositivo alle condizioni originali e quindi eliminare sia i dati di configurazione che i dati utente, come schede RF, dati facciali e così via.

Nel caso in cui sia selezionato **Ripristina configurazione stato predefinito (tranne i dati)**, il dispositivo viene ripristinato ma i dati utente vengono mantenuti memorizzati.

Per ripristinare il dispositivo, andare su **Sistema > Aggiornamento > Base** nell'interfaccia web.



Per ripristinare le impostazioni di fabbrica del dispositivo, accedere alla pagina **Impostazioni** e andare su Avanzate > Ripristina.



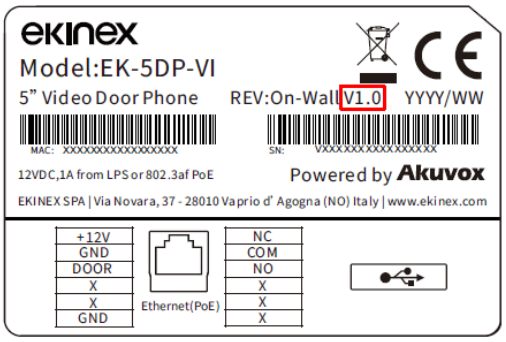
22. FAQ – Domande frequenti

D: Come verificare se il dispositivo è la versione hardware 1.0 o una versione successiva?

R: Questa informazione si può ottenere in 2 modi

1. Controllare l'etichetta sul dispositivo

- **Hardware versione 1.0**



2. Dall'interfaccia web, andare alla scheda **Stato > Informazioni > Informazioni sul prodotto** e controllare la versione del firmware e dell'hardware.

Versione del firmware	216.43.0.18
Versione hardware	216.0.9.0.0.0.0.0

- **Versione del firmware**

Il firmware è diverso tra la versione hardware 1 e le versioni successive:

- 216.X.X.X indica Hardware versione 1.0.

- **Versione hardware**

Se la versione dell'hardware riportata è 216.X, allora l'hardware è versione 1.0.

23. Marcatura

CE, UKCA: il prodotto è conforme alla Direttiva RoHS III (2011/65/UE) e alla Direttiva sulla Compatibilità Elettromagnetica (2014/30/UE).

Test eseguiti in conformità alle seguenti normative:

- EN 61000-3-2
- EN 61000-3-3
- IEC/EN 61000-6-1
- IEC/EN 61000-6-3
- EN 55014
- EN 50491

24. Manutenzione

L'apparecchio è privo di manutenzione. Per la sua pulizia adoperare un panno asciutto. È assolutamente da evitare l'utilizzo di solventi o altre sostanze aggressive.

25. Smaltimento

Il prodotto descritto nella presente scheda tecnica al termine della sua vita utile è classificato come rifiuto proveniente da apparecchiature elettroniche secondo la Direttiva Europea 2002/96/CE (RAEE), recepita in Italia con il D.Lgs. n.151 del 25 luglio 2005, e non può essere conferito tra i rifiuti solidi urbani indifferenziati.

Avvertenza! Lo smaltimento non corretto del prodotto può causare gravi danni all'ambiente e alla salute umana. Per il corretto smaltimento informarsi sulle modalità di raccolta e trattamento previste dalle autorità locali.

26. Avvertenze generali

- Il montaggio, il collegamento elettrico, la configurazione e la messa in servizio dell'apparecchio possono essere eseguiti esclusivamente da personale specializzato in osservanza delle norme tecniche applicabili e delle leggi in vigore nei rispettivi paesi.
- L'apertura della custodia dell'apparecchio determina l'interruzione immediata del periodo di garanzia.
- In caso di manomissione, non è più garantita la rispondenza ai requisiti essenziali delle direttive applicabili per i quali l'apparecchio è stato certificate.
- Apparecchi ekinex® difettosi devono essere restituiti al produttore al seguente indirizzo: EKINEX S.p.A. Via Novara 37, I-28010 Vaprio d'Agogna (NO).

27. Altre informazioni

Questo manuale è rivolto agli amministratori del sistema.

Per ulteriori informazioni sul prodotto contattare il supporto tecnico ekinex® all'indirizzo e-mail: support@ekinex.com oppure visitare il sito www.ekinex.com.