DOMOTICA LABS

MYWAY
CONTROLLO ACCESSI IN IKON SERVER

MANUALE DI CONFIGURAZIONE

VERSIONE SOFTWARE 2.9.7

1 INTRODUZIONE....6
1.1 CONVENZIONI....6
1.2 NOVITÀ....6
1.3 INFORMAZIONI SULLA SICUREZZA....6
1.4 COPYRIGHT....7
2 PANORAMICA GENERALE....8
2.1 PREMESSA....8
2.2 SCOPO DI QUESTO DOCUMENTO....8
2.3 REQUISITI....8
2.4 FUNZIONALITÀ SUPPORTATE....9
2.5 RIFERIMENTI....9
3 IMPOSTAZIONI GENERALI....10
3.1 ACCESSO CON CODICE QR....10
3.2 CONFIGURAZIONE E-MAIL....12
3.3 IMPOSTAZIONI GENERALI....13
3.4 E-MAIL DI BENVENUTO....16
3.5 AGGIUNTA E-MAIL DI BENVENUTO....18
3.6 MESSAGGIO DI STAMPA....19
3.7 GESTIONE ACCESSI....20
4 STANZE....22
4.1 PREMESSA....22
4.2 CREAZIONE DI UNA STANZA....22
4.3 FUNZIONI....24
4.4 OGGETTI CONTENUTI....26
5 VARCHI....27
5.1 PREMESSA....27
5.2 NUOVO VARCO....27
6 DIFFERENZIAZIONE ACCESSI....28
6.1 PREMESSA....28
6.2 GRUPPI UTENTE....28
6.3 FASCE ORARIE....29
6.4 UTILIZZO CON LETTORI KNX....31
7 LOG ACCESSI E OPERAZIONI....32
7.1 FRONTEND....32
7.2 AMMINISTRAZIONE....33
8 TASTIERE MYWAY....34
8.1 PREMESSA....34
8.2 INSTALLAZIONE....34
8.2.1 test....35
8.3 NUOVA LINEA....35
8.4 CREAZIONE DI UNA TASTIERA....36
8.5 ASSOCIAZIONE A UNA STANZA....36
8.6 ASSOCIAZIONE AD UN VARCO....37
8.7 UTILIZZO DELLA STESSA TASTIERA PER PIÙ STANZE....37
9 TASTIERE KNX....39
9.1 PREMESSA....39

9.2 ASSOCIARE LA TASTIERA KNX A UNA STANZA..... 40
9.3 ASSOCIARE LA TASTIERA KNX A UN VARCO..... 40
10 DISPOSITIVO DICO/ACCEDO KEY..... 41
10.1 PREMESSA..... 41
10.2 ASSOCIARE DISPOSITIVO A UNA STANZA..... 41
10.3 ASSOCIARE DISPOSITIVO A UN VARCO..... 42
11 GESTIONE DA FRONTEND..... 43
11.1 PREMESSA..... 43
11.2 UTENTE DEDICATO..... 43
11.3 IMPOSTAZIONE HOME PAGE..... 44
11.4 GESTIONE ACCESSI..... 45
11.5 OSPITI..... 46
11.6 STANZE..... 49
11.7 PERSONALE..... 50
11.8 BADGE..... 50
11.9 QR CODE..... 52
12 ACCESSO DA APP..... 53
12.1 PREMESSA..... 53
12.2 E-MAIL DI BENVENUTO..... 53
12.3 INSTALLAZIONE E PRIMO ACCESSO ALLA APP..... 53
12.4 IMPORTAZIONE DI UN BADGE VIRTUALE..... 54
12.5 GEOLOCALIZZAZIONE..... 55
12.6 ACCESSO ALLA STRUTTURA..... 56
13 CONTROLLO ACCESSI v2.9.7..... 57
13.1 INTRODUZIONE..... 57
13.2 ARCHITETTURA..... 57
13.3 CONFIGURAZIONE..... 58
13.4 LICENZE..... 58
14 IMPOSTAZIONI..... 59
14.1 IMPOSTAZIONI GENERALI..... 59
14.1.1 INFORMAZIONI STRUTTURA..... 59
14.1.2 METODI DI ACCESSO..... 60
14.1.3 DICO / Accédo KEY..... 60
14.1.4 TASTIERE KNX..... 60
14.2 E-MAIL DI BENVENUTO..... 60
14.2.1 E-MAIL DI BENVENUTO DI DEFAULT..... 60
14.2.2 TAG DINAMICI..... 61
14.2.3 EMAIL AGGIUNTIVE..... 62
14.3 PAGINA GESTIONE STRUTTURA..... 62
14.4 RISCATTA VOUCHER..... 63
15 STANZE E VARCHI..... 63
15.1 INTRODUZIONE..... 63
15.2 STANZE..... 64
15.2.1 CREAZIONE DI UNA NUOVA STANZA..... 64
15.2.2 PROPRIETÀ DELLA STANZA..... 65
15.2.3 ALTRE INFORMAZIONI..... 66
15.3 VARCHI..... 67

16 ACCÉDO KEY..... 68
16.1 INTRODUZIONE..... 68
16.2 OPERAZIONI PRELIMINARI..... 68
16.3 CREARE UN NUOVO DISPOSITIVO..... 69
16.3.1 AUTENTICAZIONE AUTOMATICA..... 70
16.3.2 AUTENTICAZIONE MANUALE..... 70
16.3.3 SALVARE E CONTROLLARE LA CONNESSIONE..... 72
16.4 IMPOSTAZIONI AGGIUNTIVE..... 73
16.5 ASSEGNAZIONE STANZE E VARCHI..... 74
17 DICO..... 75
17.1 INTRODUZIONE..... 75
17.2 OPERAZIONI PRELIMINARI..... 75
17.3 CREARE UN NUOVO DISPOSITIVO..... 77
17.3.1 AUTENTICAZIONE AUTOMATICA..... 78
17.3.2 AUTENTICAZIONE MANUALE..... 78
17.3.3 SALVARE E CONTROLLARE LA CONNESSIONE..... 80
17.4 IMPOSTAZIONI AGGIUNTIVE..... 81
17.5 ASSEGNAZIONE STANZE E VARCHI..... 82
18 CONNESSIONI..... 83
18.1 INTRODUZIONE..... 83
18.2 COLLEGAMENTI DELLE STANZE..... 83
18.2.1 APERTURA SERRATURA TRAMITE DICO O ACCÉDO KEY..... 84
18.2.2 APERTURA SERRATURA CON ATTUATORE KNX..... 86
18.2.3 ESEMPIO DI COLLEGAMENTO: SCENARIO DI BENVENUTO AL CAMBIO DI STATO DI UNA STANZA..... 87
18.3 COLLEGAMENTI DEI VARCHI..... 88
19 AUTORIZZAZIONI..... 89
19.1 GRUPPI UTENTE..... 89
19.2 FASCE ORARIE..... 89
19.2.1 CREA UN NUOVO ORARIO..... 90
19.2.2 ORARI..... 90
19.2.3 RESTRIZIONI..... 91
20 LOG ACCESSI..... 92
21 PRESENZA VIRTUALE..... 93
21.1 INTRODUZIONE..... 93
21.2 ATTIVAZIONE E PARAMETRIZZAZIONE..... 93
21.3 CONFIGURAZIONE DELLA STANZA..... 94
22 INTEGRAZIONE CON PMS..... 97
22.1 INTRODUZIONE..... 97
22.2 FIAS..... 97
22.2.1 OPERAZIONI E COMANDI SUPPORTATI..... 97
22.2.2 CONFIGURAZIONE..... 99
22.2.3 UTILIZZO..... 100
23 UTILIZZO DELLA VISTA “VISUALIZATION”..... 101
23.1 INTRODUZIONE..... 101
23.2 OSPITI..... 101
23.2.1 ELENCO DEGLI OSPITI..... 101

23.2.2 AGGIUNTA DI UN NUOVO OSPITE....102
23.2.3 E-MAIL DI BENVENUTO....104
23.3 STANZE....105
23.4 VARCHI....106
23.5 LOG ACCESSI....106
23.6 PERSONALE....107
23.7 QR CODE TEMPORANEI....108
23.8 BADGE....108

1 INTRODUZIONE

1.1 CONVENZIONI

In questo documento sono adottate le seguenti convenzioni:

[KEY]	I tasti della tastiera che l'utente deve premere sono riportati tra parentesi quadra (es: [CTRL])
`Courier`	Messaggi a video o altri messaggi software sono riportati con il font “courier”
“...”	Nomi di pulsanti o altri elementi dell'interfaccia grafica sono riportati tra doppio apice
	Nota particolarmente importante

1.2 NOVITÀ

NEW 2.7.x

Le novità rispetto alla versione precedente sono evidenziate da un *marker* laterale, che riporta anche la versione software nella quale esse sono state introdotte.

1.3 INFORMAZIONI SULLA SICUREZZA

Questo manuale contiene le informazioni necessarie per poter operare in sicurezza con il dispositivo. Chiunque interagisca con il dispositivo deve prima aver letto questa documentazione, in particolar modo le presenti informazioni sulla sicurezza. Questo documento integra e non sostituisce qualunque normativa o direttiva di Legge in materia di sicurezza.

Il dispositivo è stato sviluppato utilizzando tecnologie allo stato dell'arte e seguendo le normative in termini di sicurezza vigenti al momento; non è possibile tuttavia escludere con certezza possibili danni o interazioni con altri dispositivi durante il suo esercizio. Il dispositivo è conforme alle guide linea EMC ed alle norme Europee armonizzate; eventuali modifiche al dispositivo possono inficiare la compatibilità EMC.

La tensione di alimentazione deve essere rigorosamente all'interno del range indicato in questo manuale e sul dispositivo; pericolo di incendio o di esplosione in caso di alimentazione al di fuori di questo range. L'apparecchiatura deve essere alimentata da un circuito di alimentazione limitato il cui isolamento dalla rete elettrica deve essere non inferiore a quello tra il circuito primario e secondario di un trasformatore di sicurezza secondo IEC 61558-2-6 o equivalente.

La dichiarazione di conformità CE del dispositivo può essere richiesta a Domotica Labs, ai riferimenti riportati sul sito www.domoticalabs.com



In conformità con la direttiva 2002/96/EC i dispositivi elettronici devono essere smaltiti nelle apposite strutture e non nella raccolta di rifiuti solidi urbani.

1.4 COPYRIGHT

Le istruzioni tecniche, i manuali ed il software di IKON SERVER sono soggetti a copyright; tutti i diritti sono riservati. La copia, riproduzione, traduzione e/o modifica, anche parziali, sono espressamente vietati salvo approvazione scritta da parte di Domotica Labs.

2 PANORAMICA GENERALE

2.1 PREMESSA

IKON SERVER può gestire e supervisionare l'accesso ad aree dell'edificio (stanze di hotel, uffici, aree comuni etc...) e l'apertura di varchi, potendo stabilire anche da remoto i permessi dei diversi utenti. Questa gestione è particolarmente indicata per le seguenti tipologie di applicazione, soprattutto laddove non ci sia un presidio locale continuativo:

- hotel
- B&B
- residence
- uffici

Il controllo delle elettroserrature può avvenire con una o più delle tecnologie supportate da IKON SERVER, anche contemporaneamente: KNX, MyHOME, Modbus, oppure i moduli I/O del catalogo Domotica Labs.

Una volta completata la configurazione iniziale, come illustrato in questo manuale, il gestore della struttura può gestire ospiti, personale, varchi ed ambienti, con un monitoraggio completo sulle operazioni effettuate, direttamente dalla app SUPERVISOR oppure tramite browser, anche da remoto.

Gli utenti finali utilizzano una app dedicata (MyWAY) per accedere alle strutture controllate da IKON SERVER, grazie ad un sistema di “badge virtuali” completamente automatizzato.

Il controllo accessi di IKON SERVER prevede una licenza aggiuntiva, in base al numero di stanze/ambienti da gestire; per ulteriori informazioni, si rimanda al nostro listino prezzi ed al nostro supporto clienti.

2.2 SCOPO DI QUESTO DOCUMENTO

Questo manuale contiene tutte le informazioni necessarie per installare, configurare ed utilizzare le funzioni specifiche del modulo c*ontrollo accessi MyWAY* all'interno di IKON SERVER. E' rivolto principalmente agli installatori, ma può essere una buona guida anche per gli utenti finali che siano interessati a personalizzare le funzionalità di supervisione del proprio impianto domotico.

Per una corretta installazione, si presuppone una buona conoscenza generale di IKON SERVER; molte sezioni di questo documento fanno riferimento a concetti generali della supervisione che possono essere approfonditi nei seguenti manuali, tutti disponibili liberamente per il download nell'area SUPPORTO del sito www.domoticalabs.com :

- IKON SERVER – MANUALE DI INSTALLAZIONE (GENERALE)
- IKON SERVER – MANUALE DI UTILIZZO

2.3 REQUISITI

Per poter accedere alle funzionalità descritte in questo manuale, è necessario disporre di:

- Un IKON SERVER aggiornato alla versione 2.7.0 o superiore
- La licenza di attivazione del modulo CONTROLLO ACCESSI; va inserita la versione di licenza in base al numero di stanze / ambienti che si desidera controllare.
- Elettroserratura comandabile via KNX, MyHOME, Modbus, oppure tramite un modulo I/O del catalogo Domotica Labs

Per inserire la licenza di attivazione, procedere come segue:

- Accedere all'amministrazione di IKON SERVER
- Selezionare la voce “SETUP” dal menu laterale, quindi “GESTIONE MODULI E LICENZE”
- Identificare la voce “CONTROLLO ACCESSI” ed inserire il codice di attivazione
- Premere il pulsante “SALVA” ed attendere il ricaricamento della pagina

Per ulteriori dettagli si rimanda al MANUALE DI INSTALLAZIONE di IKON.

2.4 FUNZIONALITÀ SUPPORTATE

L'integrazione tra IKON ed il controllo accessi permette di gestire le seguenti funzionalità:

- Gestione degli ospiti
- Gestione del personale
- Gestione delle stanze e dei varchi
- Visualizzazione degli accessi effettuati

2.5 RIFERIMENTI

Si consiglia la consultazione preventiva del MANUALE DI INSTALLAZIONE di IKON SERVER, disponibile per il download nell'area SUPPORTO del sito www.domoticalabs.com

3 IMPOSTAZIONI GENERALI

Al fine di garantire un corretto funzionamento del CONTROLLO ACCESSI, è necessario in via preliminare configurare le seguenti sezioni generali di IKON SERVER:

- Accesso con codice QR
- Email

Inoltre, la configurazione prevede l'inserimento / configurazione delle seguenti voci relative al CONTROLLO ACCESSI:

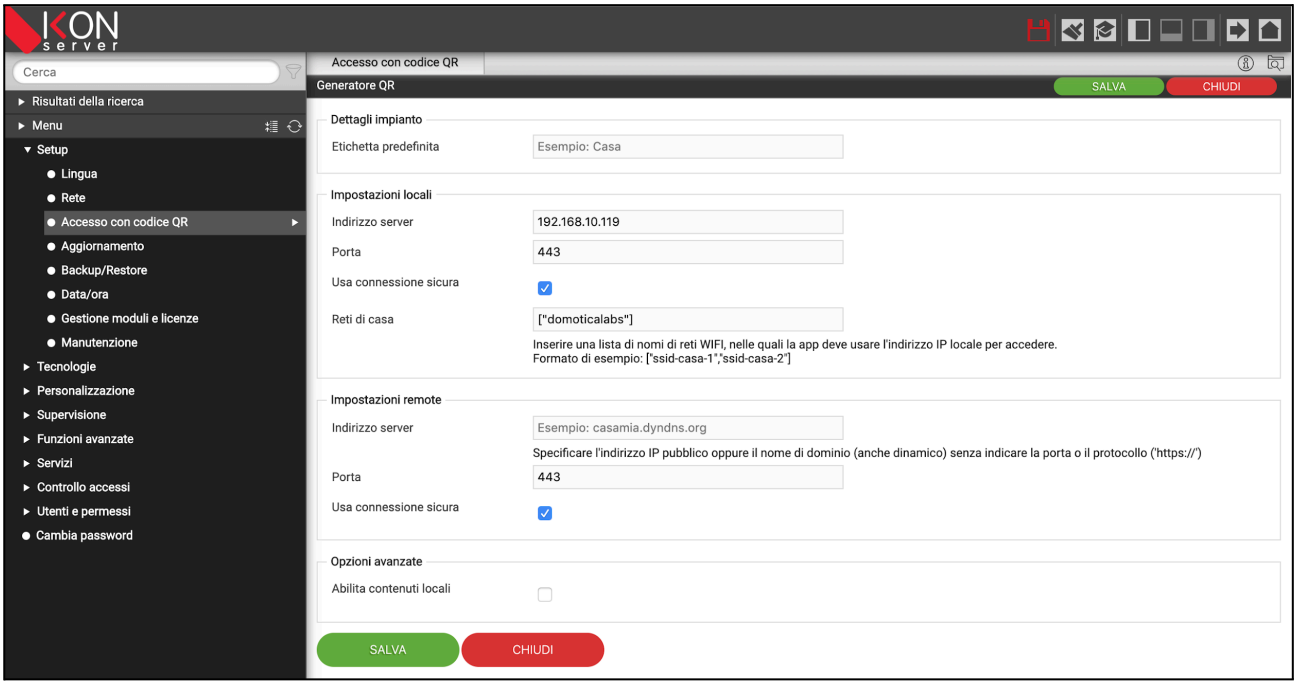
- Impostazioni generali
- Email di benvenuto (consigliato)
- Messaggio di stampa (consigliato)
- Gestione Accessi (opzionale)

3.1 ACCESSO CON CODICE QR

Poiché agli utenti della struttura verranno inviati dei *badge virtuali* basati su tecnologia QR, è fondamentale che sia correttamente configurato l'accesso con codice QR ad IKON SERVER, tramite l'apposita sezione nel menu SETUP.

Per aprire la pagina ACCESSO CON CODICE QR procedere come segue:

- Accedere all'amministrazione di IKON
- Aprire la sezione SETUP del menu laterale
- Premere la voce ACCESSO CON CODICE QR: si accederà automaticamente alla seguente pagina:



Nella sezione “DETTAGLI IMPIANTO” è disponibile il seguente parametro:

ETICHETTA PREDEFINITA	Permette di definire il nome della struttura: se presente questo campo sarà visualizzato dall'utente finale all'interno dell'applicazione e sarà il nome del mittente che verrà visualizzato nelle mail inviate agli utenti

Nella sezione “IMPOSTAZIONI LOCALI” sono disponibili i seguenti parametri:

INDIRIZZO SERVER	inserire l'indirizzo IP locale del webserver
PORTA	inserire la porta locale, dato che per sicurezza si utilizzerà il protocollo https nella comunicazione tra webserver e APP, **la porta da inserire deve essere 443**
USA CONNESSIONE SICURA	Questo flag indica se si vuole utilizzare o meno il protocollo https; nella configurazione del controllo accessi **questo flag va obbligatoriamente spuntato** per la stessa motivazione indicata nella descrizione del parametro PORTA
RETI DI CASA	Questo campo permette di inserire l’elenco dei nomi delle reti WiFi, nelle quali la app deve usare l'indirizzo IP locale per accedere, nel formato descritto nell’esempio. Formato di esempio: ["ssid-casa-1","ssid-casa-2"]

La sezione “IMPOSTAZIONI REMOTE” offre viceversa i parametri seguenti:

INDIRIZZO SERVER	inserire l'indirizzo IP remoto del webserver (o il suo DNS) inserire la porta locale,
PORTA	inserire la porta remota per la comunicazione https
USA CONNESSIONE SICURA	Questo flag indica se si vuole utilizzare o meno il protocollo https; nella configurazione del controllo accessi questo flag va **obbligatoriamente spuntato** per la stessa motivazione indicata nella descrizione del parametro PORTA



Si consiglia di configurare solo l’accesso pubblico e non quello locale, per evitare disservizi nel passaggio tra rete WIFI della struttura e connessione internet del telefono da cui viene usata la app MyWAY.

Al termine della configurazione premere sul pulsante SALVA, altrimenti la configurazione non verrà salvata.

Per ulteriori informazioni sull'accesso con QR ad IKON SERVER, si rimanda al MANUALE DI INSTALLAZIONE GENERALE.

3.2 CONFIGURAZIONE E-MAIL

Poiché IKON SERVER invierà automaticamente e-mail agli utilizzatori della struttura, contenenti le istruzioni per l'accesso ed il badge virtuale da utilizzare con la app MyWAY, è un requisito fondamentale che il server sia correttamente predisposto per inviare e-mail.

Per configurare i parametri del server SMTP da utilizzare per l'invio delle e-mail, procedere come segue:

- Aprire la sezione PERSONALIZZAZIONE del menu laterale
- Aprire la sotto-sezione OPZIONI del menu laterale
- Premere la voce EMAIL : si accede automaticamente alla seguente pagina:

La sezione OPZIONI PER INVIO MAIL permette di impostare i seguenti parametri:

SERVER SMTP	Indirizzo o nome del server SMTP a cui appoggiare l'invio delle email
PORTA	Porta con cui comunicare con il server SMTP
UTILIZZO PROTOCOLLO SSL	Abilitazione della cifratura SSL, in base a come richiesto dal server SMTP
ABILITA AUTENTICAZIONE SUL SERVER	Attivazione o meno dell'autenticazione sul server (solitamente richiesta)
UTENTE PASSWORD	Credenziali con cui autenticarsi sul server SMTP
INDIRIZZO MITTENTE	Specificare l'indirizzo mittente con cui devono essere visualizzate le email qualora diverso da quello con cui ci si autentica sul server (se consentito dal server SMTP)

Esempio di configurazione per GMAIL:

SERVER SMTP	smtp.gmail.com
PORTA	465
UTILIZZO PROTOCOLLO SSL	Si
ABILITA AUTENTICAZIONE SUL SERVER	Si
UTENTE PASSWORD	*Inserire il proprio indirizzo Gmail completo e la propria password di accesso*
INDIRIZZO MITTENTE	*Specificare nuovamente il proprio indirizzo Gmail completo, oppure lasciare vuoto*

E’ possibile anche inviare le notifiche tramite cloud, in questo caso selezionare l’apposita modalità di invio nel primo selettore. Per ulteriori informazioni si rimanda al MANUALE GENERALE.

3.3 IMPOSTAZIONI GENERALI

Per una esperienza ottimale per gli utenti finali, è opportuno inserire una serie di informazioni relative alla struttura gestita da IKON SERVER; queste informazioni verranno in parte comunicate al cliente tramite la app MyWAY, in parte utilizzate per configurare il comportamento del CONTROLLO ACCESSI.

Per aprire la pagina IMPOSTAZIONI GENERALI procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Aprire la sotto-sezione IMPOSTAZIONI del menu laterale
- Premere la voce IMPOSTAZIONI GENERALI per aprire la seguente pagina di impostazioni

Informazioni struttura

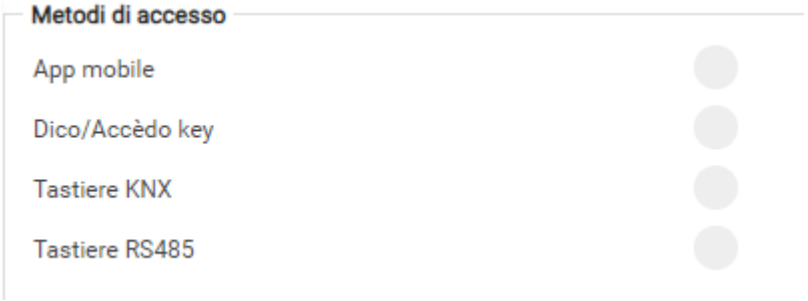
E' possibile inserire le seguenti informazioni:

NOME STRUTTURA	Permette di definire il nome della struttura: se presente questo campo sarà visualizzato dall'utente finale all'interno dell'applicazione e sarà il nome del mittente che verrà visualizzato nelle mail inviate agli utenti N.B. Se questo campo è presente va a sostituire le funzioni del campo **Etichetta predefinita** inserito precedentemente nella sezione ACCESSO CON QR.
INDIRIZZO	Permette di definire la via e il numero civico della struttura, se inserito l'utente finale potrà visualizzare su google maps la struttura premendo l'apposito pulsante all'interno della APP
NUMERO DI TELEFONO	Permette di definire il numero di telefono, se inserito l'utente finale potrà visualizzare e chiamare il numero direttamente premendo l'apposito pulsante all'interno della APP
EMAIL DI CONTATTO	Permette di definire la mail a cui l'utente può scrivere per qualsiasi evenienza, direttamente dalla APP
SITO WEB	Sito web pubblico della struttura, che verrà visualizzato all'interno della app e nella mail di benvenuto
NOME RETE WIFI	Nome della rete WiFi della struttura Se inserito, viene comunicato nella mail di benvenuto agli utenti finali, affinché possano connettersi per usufruire dell'accesso ad internet, ed utilizzare le funzioni di CONTROLLO ACCESSI di IKON SERVER senza dover necessariamente passare attraverso collegamento remoto
PASSWORD RETE WIFI	Password della rete WiFi della struttura
ORARIO DI CHECK-IN PREDEFINITO	Se impostato, quando si inserisce un nuovo ospite, viene utilizzato come orario predefinito di inizio validità del badge virtuale
ORARIO DI CHECK-OUT PREDEFINITO	Se impostato, quando si inserisce un nuovo ospite, viene utilizzato come orario predefinito di fine validità del badge virtuale

TEMPO DEL TRIGGER PER APERTURA VARCHI	Tempo in secondi per eccitazione elettroserratura, se gestita direttamente da IKON SERVER (con attuatori che non prevedono nativamente la temporizzazione)
CONTROLLO CAMERA OCCUPATA	Effettua un controllo in fase di creazione ospite e segnala se la stanza è già occupata nel periodo che è stato scelto. Se si disattiva questa opzione, è possibile assegnare la stessa stanza a più utenti nello stesso giorno.

Metodi di accesso

È necessario selezionare i metodi di accesso desiderati.



In base alla selezione vengono mostrate le sezioni corrispondenti

- **APP MOBILE**

RAGGIO	Scegliere il raggio d'azione all'interno del quale, è consentito l'accesso
LINK APP ANDROID	Link per il download della APP MyWAY per i clienti che utilizzano smartphone Android. Non modificare questo link, se non in caso di necessità specifiche.
LINK APP IOS	Link per il download della APP MyWAY per i clienti che utilizzano Apple IPhone. Non modificare questo link, se non in caso di necessità specifiche.
ABILITA RICHIESTA PIN	Se questo flag è abilitato, in assenza di altre tecnologie di identificazione del varco (es: BEACON BLUETOOTH) o in caso di problemi con queste ultime, la app richiede un PIN per aprire il varco. Se disabilitato, permette di aprire direttamente i varchi, una volta all'interno della app MyWAY.
CONTROLLO DOMOTICO (LOCALE)	Se attivo, questo flag permette all'utente finale di gestire le funzioni domotiche della propria stanza, una volta che sarà entrato all'interno dell'applicazione con le impostazioni locali (collegato in WiFi a una delle reti elencate nel parametro RETI DI CASA [punto **3.1**])

CONTROLLO DOMOTICO (REMOTA)	Se attivo, questo flag permette il controllo della domotica di stanza anche da remoto
ORDINA VARCHI PRIMA DELLE STANZE NELLA LISTA (APP)	Opzione che modifica l'ordinamento di Stanze e Varchi sull'app
VISUALIZZA QR CODE NELLA MAIL	Se attivo, questo flag permette di visualizzare il QR Code nella mail di benvenuto

- **DICO/ACCEDO KEY**

MODALITA' DI AUTENTICAZIONE CENTRALIZZATA	Sono disponibili due opzioni: - No = modalità distribuita questa modalità permette di far gestire l'autenticazione al citofono DICO, è disponibile solo l'accesso con PIN - Yes = modalità centralizzata questa modalità permette di far gestire l'autenticazione direttamente all'IKON, è disponibile l'accesso con PIN e QR CODE. NB. In caso di impianti in cui è necessario attivare uno o più relè del dispositivo DICO/ACCEDO KEY o relè esterni al dispositivo bisogna scegliere la modalità di autenticazione centralizzata
PIN	Abilita l'accesso tramite PIN numerico
QR CODE	Abilita l'accesso tramite QR Code
ABILITA LIMITE ACCESSI	Abilita la visualizzazione del campo "Limite Accessi" nel frontend di fianco ai varchi/stanze ed è possibile inserire il numero di accessi che il cliente potrà fare.

- **TASTIERE KNX**

FILTRO FASCE ORARIE	Permette di stabilire se le fasce orarie debbano poter essere impostate con la granularità delle ore oppure dei minuti. Per ulteriori informazioni si rimanda al capitolo dedicato alla differenziazione degli accessi.

- **TASTIERE RS485**

ABILITA GESTIONE BADGE	Se il flag è abilitato vengono mostrate nel FRONTEND le opzioni relative ai badge
LINEA PER LA SCAN DEI BADGE	Scelta della linea predefinita su cui effettuare la scansione dei badge. Per ulteriori informazioni si rimanda al capitolo dedicato.

3.4 E-MAIL DI BENVENUTO

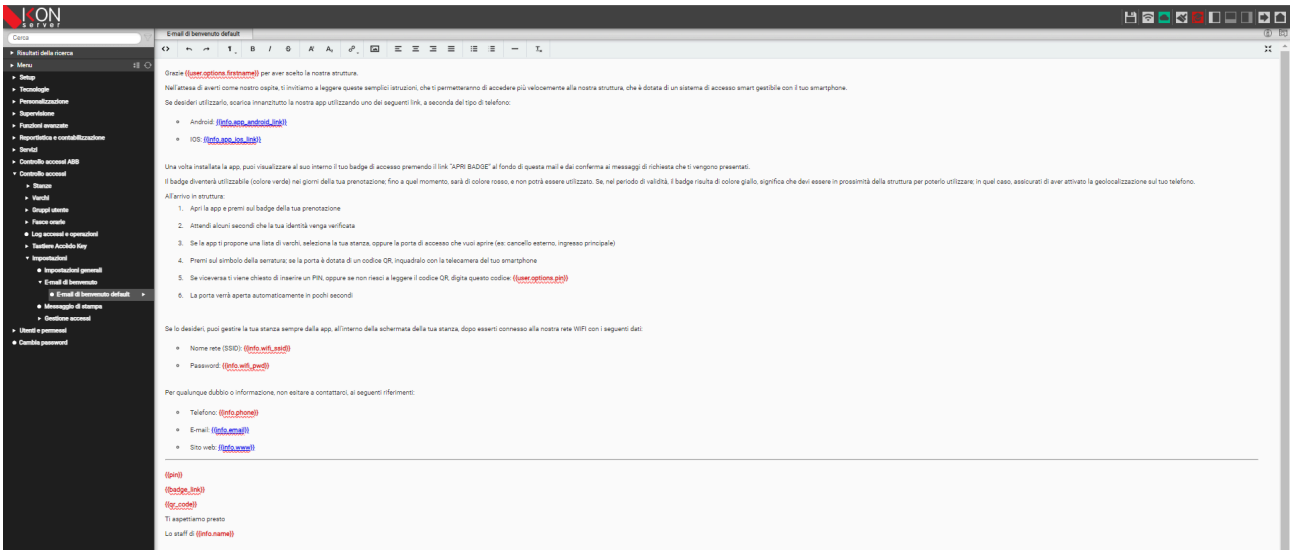
La pagina E-MAIL DI BENVENUTO permette di personalizzare la mail di benvenuto che verrà inviata all'utente, per informarlo sui passi che dovrà eseguire per accedere alla struttura.

IKON SERVER prevede un testo generico, contenente tutte le informazioni che è possibile inviare all'utente; nel testo sono inseriti elementi dinamici (evidenziati in rosso) che vengono sostituiti con i dati della struttura e dell'utente in fase di invio delle e-mail.

Il testo può essere completamente o parzialmente rivisto, mantenendo gli elementi dinamici.

Per aprire la pagina E-MAIL DI BENVENUTO procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Aprire la sotto-sezione IMPOSTAZIONI del menu laterale
- Premere la voce E-MAIL DI BENVENUTO : si accede automaticamente alla seguente pagina:



Tramite l'editor integrato si può visualizzare e modificare la mail da inviare, partendo dal testo predefinito.

E' possibile configurare separatamente i seguenti testi:

- OGGETTO MAIL
- CONTENUTO DEL MESSAGGIO

In ciascuna di queste è possibile inserire dei tag dinamici, che permetteranno per esempio di inviare mail contenenti il nome dell'utente a cui è indirizzata; questi tag sono definiti all'interno di due parentesi graffe: {{ }}.

I tag sono definiti da due o più parti separate da un punto; la prima parte può contenere le seguenti parole chiave:

- **user**: tag dinamico che sostituisce le proprietà dell' utente a cui si invierà la mail
- **info**: tag dinamico che sostituisce le informazioni della struttura inserite nella configurazione

La tabella seguente contiene tutti i possibili tag dinamici che è possibile inserire nel testo:

INFORMAZIONI UTENTE / OSPITE

user.name	Cognome e nome dell'utente a cui è indirizzata la mail
user.options.firstname	Nome dell'utente a cui è indirizzata la mail
user.options.lastname	Cognome dell'utente a cui è indirizzata la mail
user.options.pin	Codice pin dell'utente a cui è indirizzata la mail, che gli permetterà di accedere ai varchi se l'opzione PIN è abilitata nella configurazione del web server
user.rooms	Lista di camere/varchi
user.options.valid_from user.options.valid_to	Permette di inserire le date di validità Da - A

INFORMAZIONE STRUTTURA

info.name	Nome della struttura, inserito nella configurazione
info.app_android_link	Link della APP android, inserito nella configurazione
info.app_ios_link	Link della APP iOS, inserito nella configurazione
info.wifi_ssid	Nome della rete wifi, inserita nella configurazione
info.wifi_pwd	Password della rete wifi, inserita nella configurazione
info.phone	Numero di telefono, inserito nella configurazione
info.email	Email di contatto, inserita nella configurazione
info.www	Sito della struttura, inserito nella configurazione

OPZIONI DI ACCESSO

pin	Codice pin dell'utente a cui è indirizzata la mail, che gli permetterà di accedere ai varchi se l'opzione PIN è abilitata nella configurazione del web server
badge_link	Link per la creazione di un nuovo badge sull'applicazione. Nel caso sia configurato anche il QR Code, verrà visualizzato nella mail e sarà possibile scansionarlo da app My Way.
qr_code	QR Code che deve essere scansionato dai dispositivi DICO/ACCEDO KEY per l'accesso alle stanza/varchi

Le "Opzioni di accesso" verranno nascoste nella mail finale in base ai flag impostati nelle impostazioni generali della sezione "Metodi di accesso"

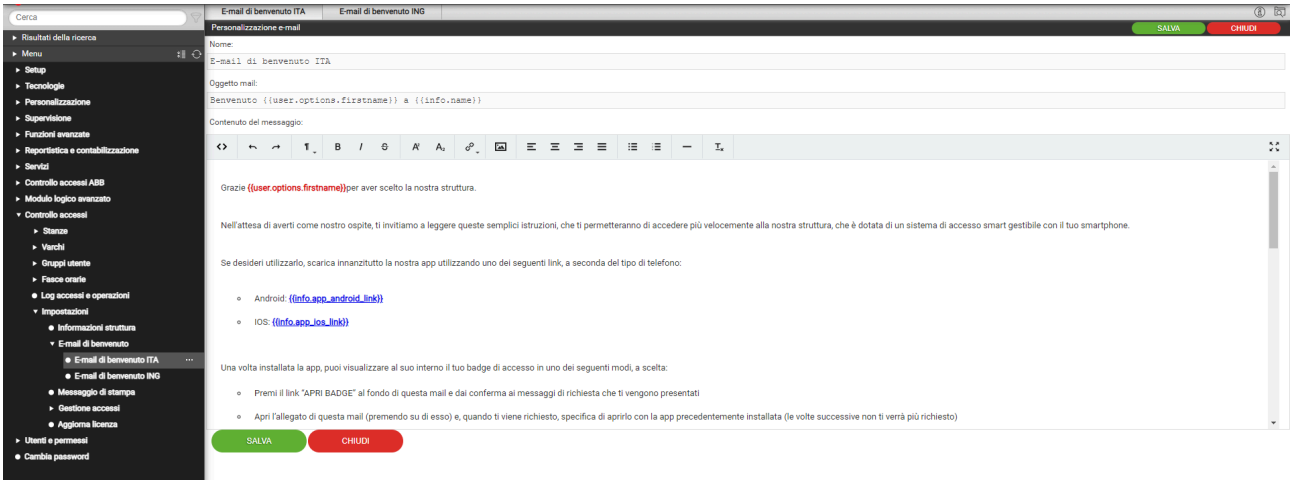
Al termine della modifica della mail, premere sul pulsante SALVA, altrimenti le modifiche non verranno apportate.

3.5 AGGIUNTA E-MAIL DI BENVENUTO

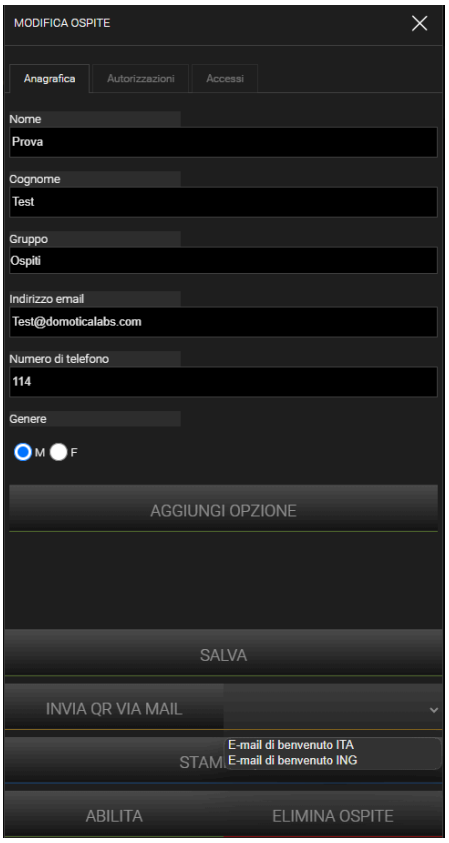
Per aggiungere una nuova E-MAIL DI BENVENUTO procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Aprire la sotto-sezione IMPOSTAZIONI del menu laterale
- Selezionare la voce E-MAIL DI BENVENUTO
- Premere il pulsante + in basso a sinistra

A questo punto sarà possibile, come visto in precedenza, andare a creare una nuova E-MAIL DI BENVENUTO, per esempio nel caso in cui si voglia avere una mail in Italiano e una in Inglese.



Lato frontend sarà poi disponibile un menu a tendina in modo da poter selezionare la mail desiderata.



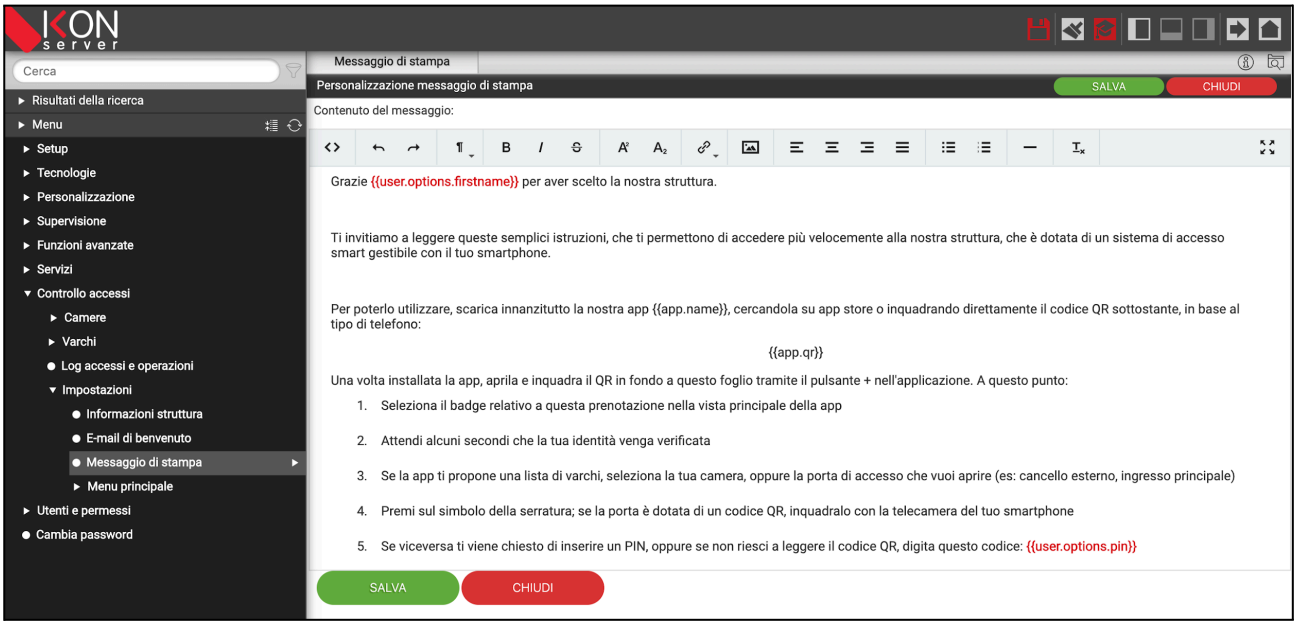
3.6 MESSAGGIO DI STAMPA

La pagina MESSAGGIO DI STAMPA permette di personalizzare il testo che può essere stampato all'utente, nel caso in cui non si voglia inviare la mail di benvenuto, ad esempio perché l'ospite è direttamente in reception.

Anche in questo caso, come per la mail di benvenuto, è presente un messaggio predefinito contenente istruzioni all'utente, che spiegano i passi da effettuare per iniziare a utilizzare l'APP e il codice PIN, diverso per ogni utente, che andrà inserito nel caso in cui l'opzione PIN è abilitata nella configurazione del web server.

Per aprire la pagina MESSAGGIO DI STAMPA procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Aprire la sotto-sezione IMPOSTAZIONI del menu laterale
- Premere la voce MESSAGGIO DI STAMPA : si accederà automaticamente alla seguente pagina:



La pagina si presenta in modo simile a quella della configurazione della mail di benvenuto: anche qui è presente una pagina di editing con un messaggio modificabile anche con i tag dinamici; oltre ai tag descritti in precedenza [punto 3.4 di questa guida] in questo messaggio c'è la possibilità di inserire i seguenti tag:

app.name	Sarà visualizzato il nome della APP
app.qr	Genera una tabella contenente due codici QR, al centro della pagina, da utilizzarsi per scaricare velocemente le app rispettivamente per Android e IOS

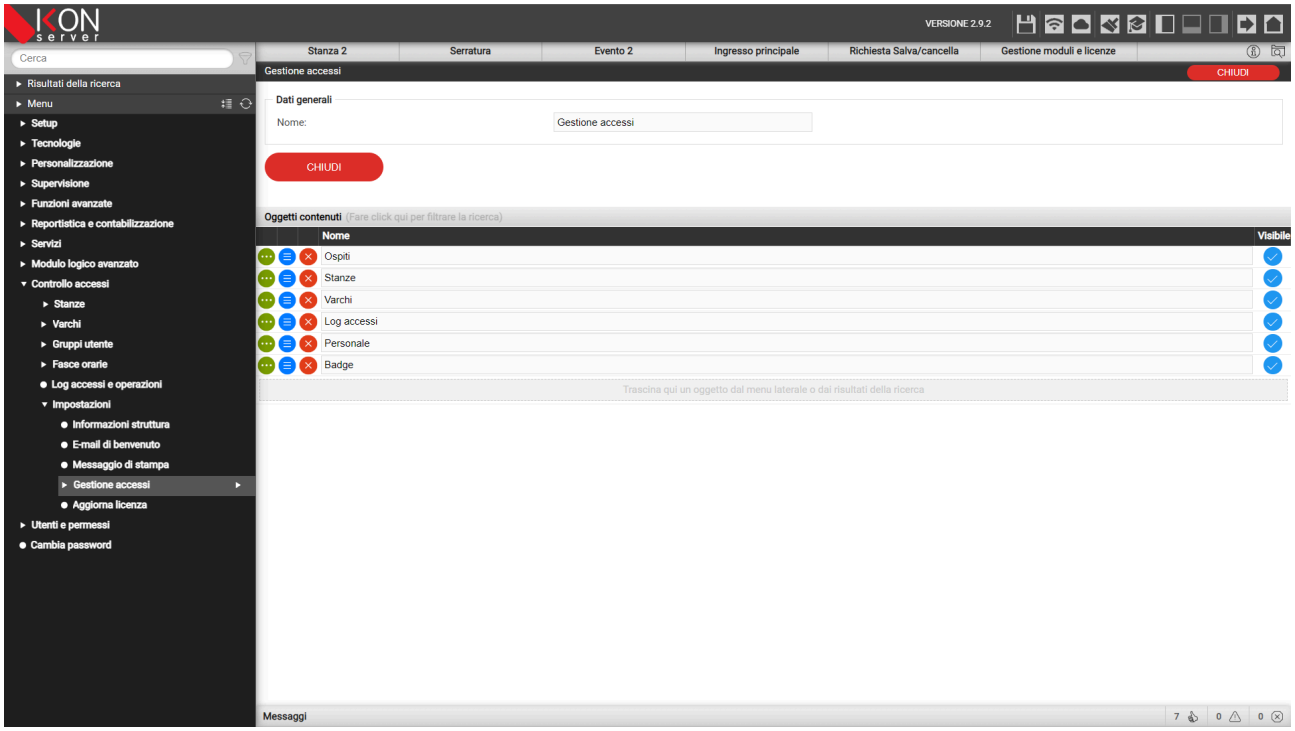
Al termine della modifica del messaggio di stampa, premere sul pulsante SALVA, altrimenti le modifiche non verranno apportate.

3.7 GESTIONE ACCESSI

La sezione GESTIONE ACCESSI permette di personalizzare il menù principale che verrà utilizzato, nell'area di frontend di IKON SERVER, da parte del gestore della struttura, per la gestione degli accessi.

Per aprire la pagina GESTIONE ACCESSI, procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Aprire la sotto-sezione IMPOSTAZIONI del menu laterale
- Selezionare la voce GESTIONE ACCESSI e aprire la pagina premendo sui tre puntini a fianco del nome: si accederà alla seguente pagina:



Nella sezione DATI GENERALI è possibile modificare il titolo della pagina che funge da menù, mentre nella sezione OGGETTI CONTENUTI è possibile modificare le diciture delle seguenti sezioni:

OSPITI	Sezione che permette di consultare l'elenco degli ospiti già configurati, e crearne di nuovi
STANZE	Sezione contenente l'elenco degli ambienti gestiti tramite il controllo accessi
VARCHI	Sezione contenente l'elenco dei varchi gestiti tramite il controllo accessi
LOG ACCESSI	Tabella contenente un elenco di operazioni effettuate dagli utenti tramite il sistema di controllo accessi
PERSONALE	Sezione che permette di gestire il personale della struttura, e creare nuovi utenti abilitati
BADGE	Sezione dove è possibile gestire e creare i badge

Per ulteriori informazioni sul menu di gestione del controllo accessi, si rimanda a capitolo successivo di questo manuale.

4 STANZE

4.1 PREMESSA

La gestione CONTROLLO ACCESSI di IKON SERVER prevede tipicamente la regolamentazione dell'accesso ad uno o più ambienti, per i quali viene utilizzata la dicitura di “stanze” in ottica alberghiera. Qualora si desideri gestire ambienti che non sono stanze, è sufficiente assegnare a loro una nomenclatura differente, come meglio illustrato qua di seguito.

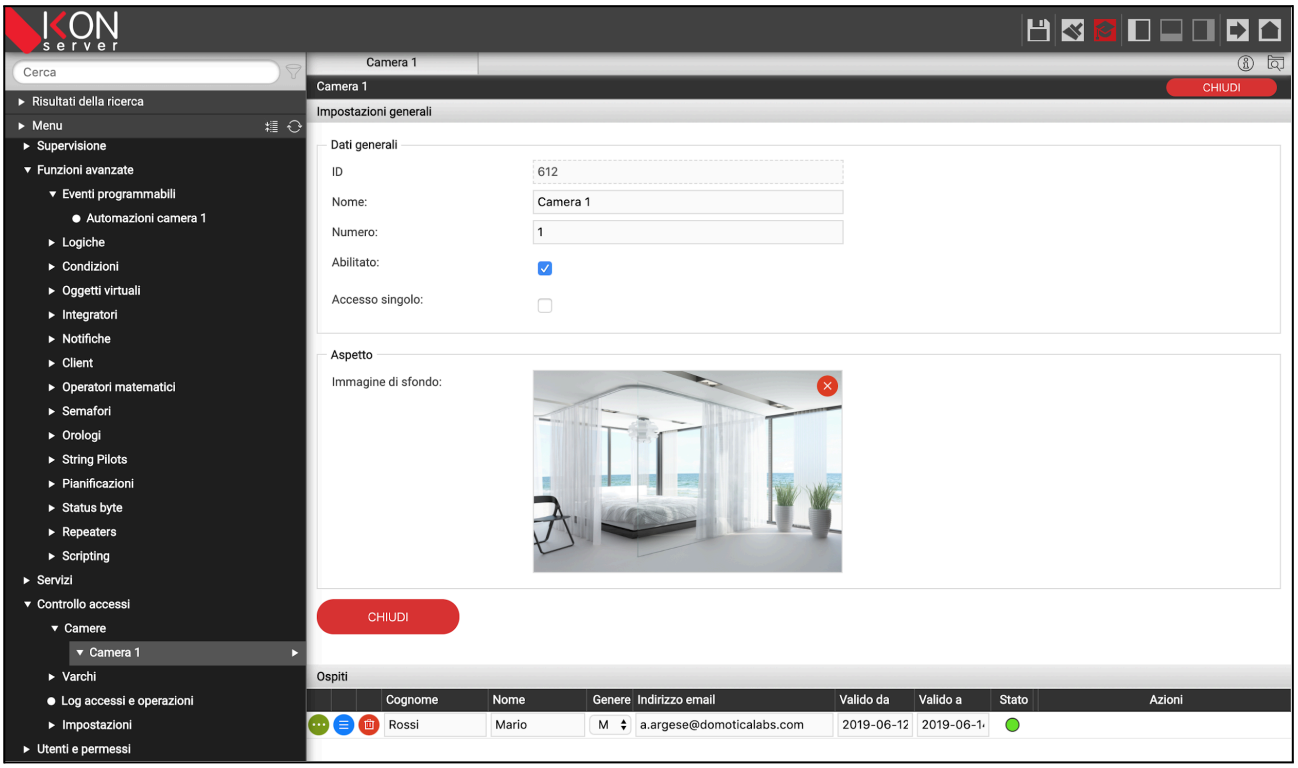
Oltre ad aprire la porta di accesso, è possibile consentire sia al gestore dell'edificio, sia agli utenti finali, la gestione della domotica all'interno di tale ambiente, il tutto tramite la medesima app MyWAY.

4.2 CREAZIONE DI UNA STANZA

Per creare una nuova stanza procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Premere la sotto-sezione STANZE del menu laterale
- Premere il pulsante '+' che si trova in basso a sinistra

Selezionando la nuova stanza e premendo la sua scorciatoia (“tre puntini”) nel menu, si accede alla sua scheda di configurazione:



Nella sezione DATI GENERALI è possibile modificare i seguenti dati:

NUMERO	Questo parametro indica il numero della stanza, cambiandolo si aggiornerà automaticamente il nome della stanza con il numero inserito in questo campo
ABILITATO	Questo flag indica se è possibile o meno interagire con le funzioni di stanza; se disattivato, non sarà permesso ad

	alcun utente di interagire con la stanza tramite il CONTROLLO ACCESSI
ACCESSO SINGOLO	Se questo flag è attivo, l'utente finale (ospite) può aprire la porta di accesso alla stanza UNA SOLA VOLTA tramite app MyWAY. Questa funzione è pensata per strutture non presidiate, per far trovare all'utente il badge o la chiave all'interno della sua stanza, e fare in modo che dopo il primo accesso tramite app, usi questi ultimi per accedere alla struttura. *Nota: in questa particolare configurazione, per ripristinare eventualmente la possibilità di aprire la porta (per una seconda volta) ad un ospite, è sufficiente disabilitarlo, e ri-abilitarlo, come meglio illustrato in seguito.*
UID ANDROID DEL DISPOSITIVO APRIPORTA ASSOCIATO:	E' presente l'app OpenDoor per touch che permette di svolgere la stessa funzione di un tastierino. Per collegare il touch ad una determinata stanza è necessario inserire il codice UID del touch che si trova nelle impostazioni dell'applicazione. Per ulteriori informazioni si rimanda al manuale relativo alla app MyWAY per IMAGO NEXT disponibile nell'area SUPPORTO del sito www.domoticalabs.com

Attivando la modalità avanzata (toolbar in alto a destra) nella sezione DATI GENERALI è inoltre possibile modificare il seguente parametro:

NOME	Questo parametro permette di personalizzare il nome della stanza / ambiente rispetto alla dicitura standard "Stanza X" (dove X è il suo numero)

Nella sezione ASPETTO è possibile modificare inoltre il seguente parametro:

IMMAGINE DI SFONDO	Questo parametro permette di scegliere un'immagine che nel frontend farà da sfondo alla stanza corrente; Sono presenti alcune immagini pre-caricate

Nella sezione OSPITI è possibile visualizzare tutti gli ospiti che sono autorizzati ad interagire con la stanza corrente.

4.3 FUNZIONI

Alla creazione di una stanza, vengono predisposte le seguenti funzioni, che è possibile comandare tramite IKON SERVER:

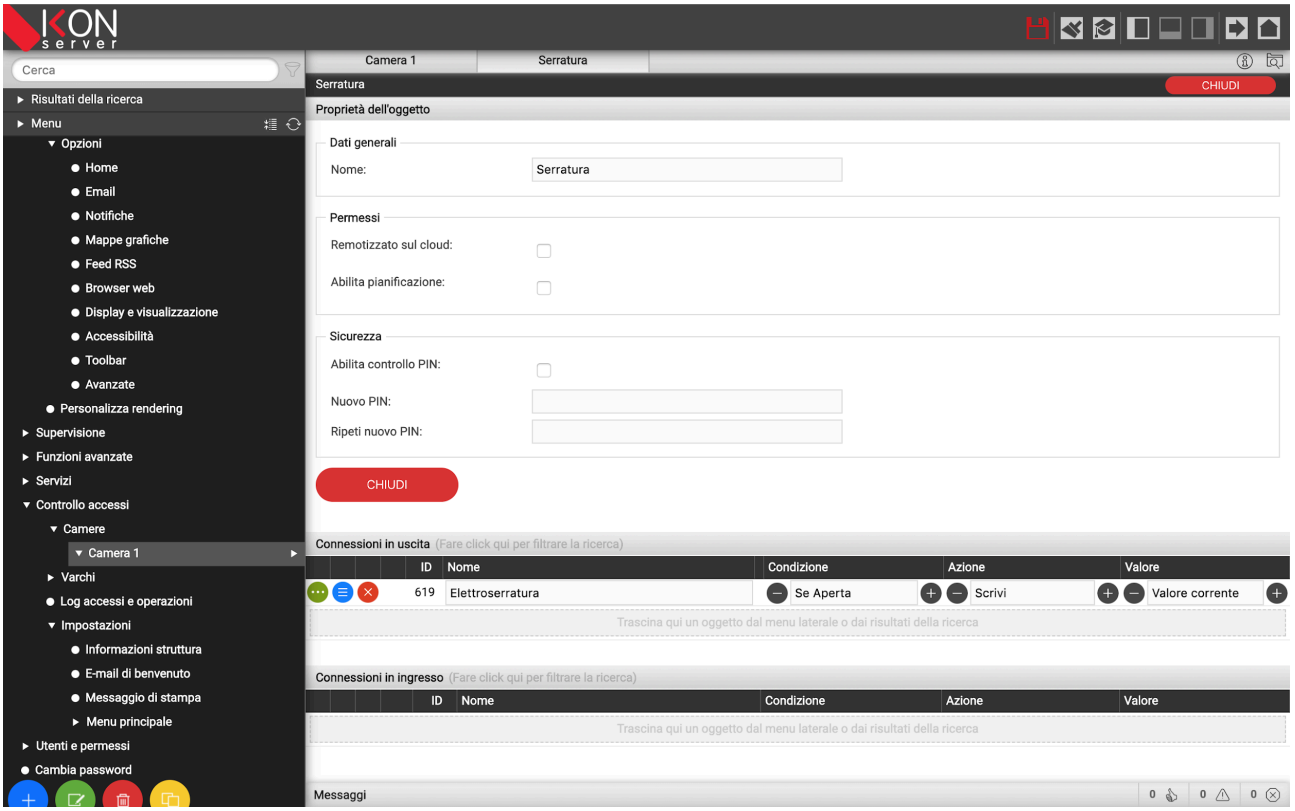
SERRATURA	Rappresenta l'apertura del varco di accesso alla stanza
NON DISTURBARE PULIZIA STANZA (visibile solo se App Mobile è stato selezionato nel percorso Impostazioni > Impostazioni Generali > Metodo di Accesso)	Rappresentano rispettivamente la funzione “DO NOT DISTURB” e “MAKE UP ROOM” tipicamente utilizzate, nelle strutture alberghiere, per richiedere al personale di non accedere alla stanza, oppure di pulirla
PRESENZA (visibile solo se App Mobile è stato selezionato nel percorso Impostazioni > Impostazioni Generali > Metodo di Accesso)	Identifica la presenza o meno all'interno della stanza
ALLARME (visibile solo se App Mobile è stato selezionato nel percorso Impostazioni > Impostazioni Generali > Metodo di Accesso)	Rappresenta un allarme rilevato nella stanza, ad esempio con il tirante nel bagno, oppure un sensore
STATO (visibile solo se App Mobile è stato selezionato nel percorso Impostazioni > Impostazioni Generali > Metodo di Accesso)	Rappresenta lo stato generale della stanza; può essere in uno dei seguenti stati: Libera Prenotata Assegnata Occupata Service

Per vedere le funzioni, è necessario abilitare la visualizzazione AVANZATA con l'apposito pulsante della toolbar in alto a destra

Queste funzioni, alla creazione della stanza, sono completamente virtuali; se si desidera utilizzarle materialmente, è necessario associarle ad un dispositivo fisico, sia esso un indirizzo KNX / MyHOME, oppure un canale di un dispositivo di I/O. A seconda del tipo di funzione, è previsto che tale associazione sia “in uscita” (per comandare un dispositivo, come ad esempio nel caso della serratura) oppure “in ingresso” (per far cambiare di stato la funzione di stanza, partendo da un modulo di ingresso su bus).

Per fare tale associazione, è possibile accedere alla scheda della funzione, e trascinare gli oggetti tecnologici con cui deve interagire, nelle sezioni CONNESSIONI IN USCITA o CONNESSIONI IN INGRESSO.

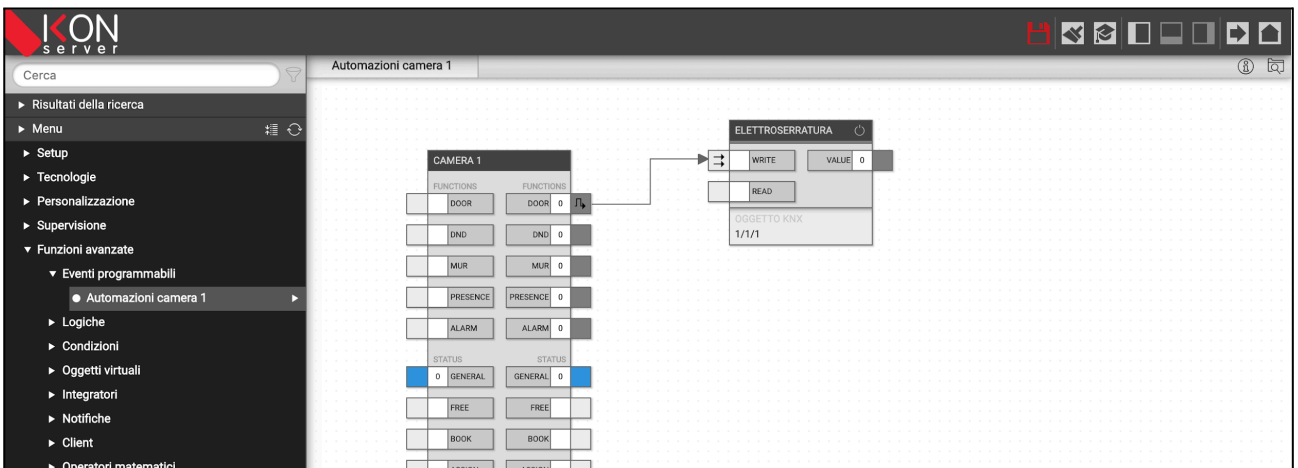
Nella seguente figura di esempio, è stata associata una elettroserratura KNX alla funzione “SERRATURA” della stanza, trascinando il corrispondente OGGETTO KNX nella sezione CONNESSIONI IN USCITA:



I seguenti campi vanno opportunamente compilati, in base alle esigenze specifiche, ed al tipo di oggetto che viene trascinato:

CONDIZIONE	Specifica per quale valore della funzione si desidera comandare l'oggetto tecnologico Es: solo se la serratura viene aperta
AZIONE	In caso di oggetti di IKON SERVER che prevedono più azioni, scegliere quella desiderata. Normalmente va lasciato il valore predefinito “SCRIVI”.
VALORE	Valore da passare all'oggetto tecnologico. Può essere, ad esempio, un “ON” o “OFF”; selezionando la voce “VALORE CORRENTE”, viene utilizzato lo stato della funzione di partenza.

In alternativa a questa modalità di configurazione, si può creare un EVENTO PROGRAMMABILE (sezione FUNZIONI AVANZATE), e trascinarvi al suo interno direttamente l'oggetto STANZA, e gli oggetti tecnologici che si desidera comandare:



Per ulteriori informazioni sulle CONNESSIONI e sugli EVENTI PROGRAMMABILI di IKON SERVER, si rimanda al MANUALE DI INSTALLAZIONE GENERALE.

All'atto della creazione, le funzioni sono contrassegnate come NON VISIBILI; questo implica che sono disponibili per eventuali automazioni (necessarie, come ad esempio per la serratura, per poter azionare l'apertura della porta / varco di accesso) ma non gestibili tramite il FRONTEND, né tramite app MyWAY dagli utilizzatori finali (ospiti).

Se si desidera gestire una o più di queste funzioni dal frontend, è sufficiente abilitare il corrispondente flag di visibile; se una determinata funzione non deve essere né utilizzata per automazioni, né visualizzata, può essere definitivamente rimossa, con il corrispondente pulsante di eliminazione (icona cestino).

4.4 OGGETTI CONTENUTI

In aggiunta alle funzioni, è possibile associare ad una stanza uno o più oggetti tecnologici, affinché questi possano essere gestiti sia dal gestore, sia dagli utenti finali, nella loro GESTIONE STANZA.

A tale scopo, è sufficiente trascinare gli oggetti desiderati dai rispettivi menu nella sezione TECNOLOGIE, oppure dai risultati della ricerca, nella sezione OGGETTI CONTENUTI.

5 VARCHI

5.1 PREMESSA

Oltre alle stanze, IKON SERVER può gestire anche l'apertura di varchi, che non sono associati ad ambienti, come ad esempio un cancello esterno o una porta principale di accesso alla struttura, oppure ancora la porta di accesso a parti comuni.

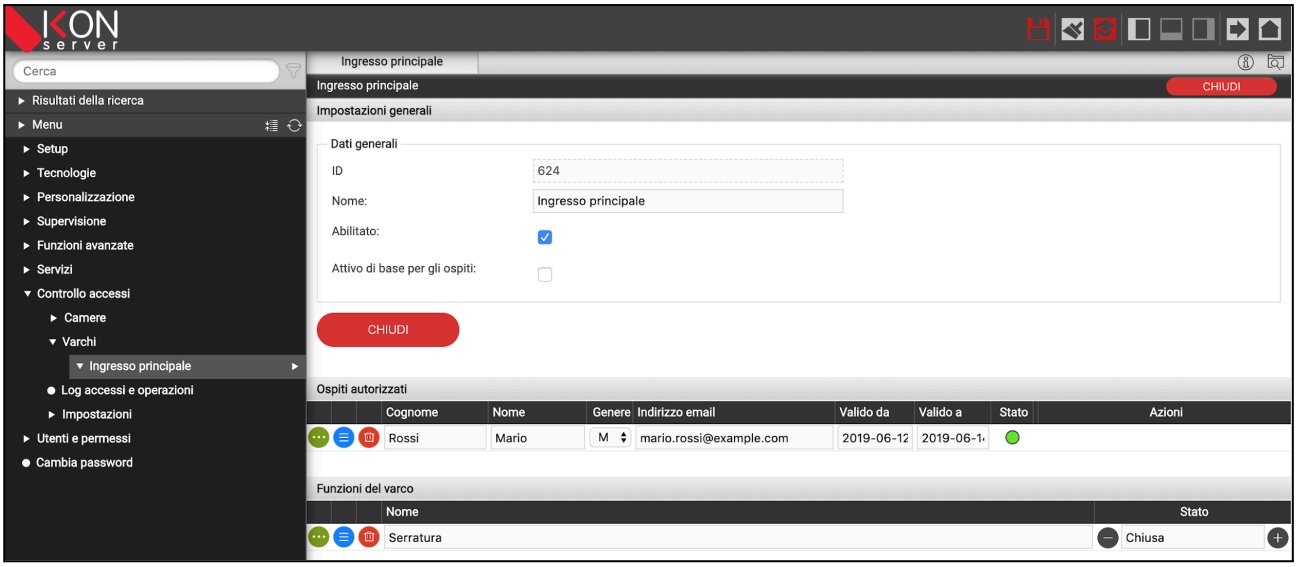
Questi varchi devono essere abilitati per tutti gli utenti, a prescindere dalla loro stanza, altrimenti non avranno modo di accedere alla struttura, prima ancora di presentarsi di fronte al proprio ambiente assegnato.

Come vedremo, i varchi si configurano in modo molto simile alle stanze, ma hanno alcune funzionalità in meno, perché non prevedono una visualizzazione da parte degli utenti, né pertanto la possibilità di inserire al loro interno degli oggetti.

5.2 NUOVO VARCO

La creazione e gestione di un varco è identica a quella di una stanza con delle piccole differenze:

- Il varco non ha un numero da associare, ma è comunque possibile cambiargli il nome.
- Il varco non ha un'immagine di sfondo che si può impostare.
- Come funzione del varco è disponibile solamente la serratura.
- Offre, per contro, il flag ATTIVO DI BASE PER GLI OSPITI: se attivato, al momento della creazione di un ospite questo varco sarà assegnato come predefinito; in quel momento si potrà comunque decidere di togliere questa assegnazione. Questo flag è utile per velocizzare la creazione degli utenti ed è pensato per varchi accessibili a tutti i clienti (come ad esempio il cancello esterno)



L'associazione di un dispositivo fisico all'apertura della serratura, avviene in modo del tutto analogo a quanto visto per le stanze, accedendo alla scheda della funzione serratura, ed associando l'oggetto da comandare mediante le CONNESSIONI IN USCITA (oppure, in alternativa, predisponendo un EVENTO PROGRAMMABILE).

6 DIFFERENZIAZIONE ACCESSI

6.1 PREMESSA

E’ possibile differenziare i permessi di accesso per gli utenti del sistema attraverso la definizione di GRUPPI UTENTE, ai quali è possibile associare delle FASCE ORARIE all’interno delle quali, gli utenti appartenenti a quel determinato gruppo possono entrare in uno o più varchi / stanze.

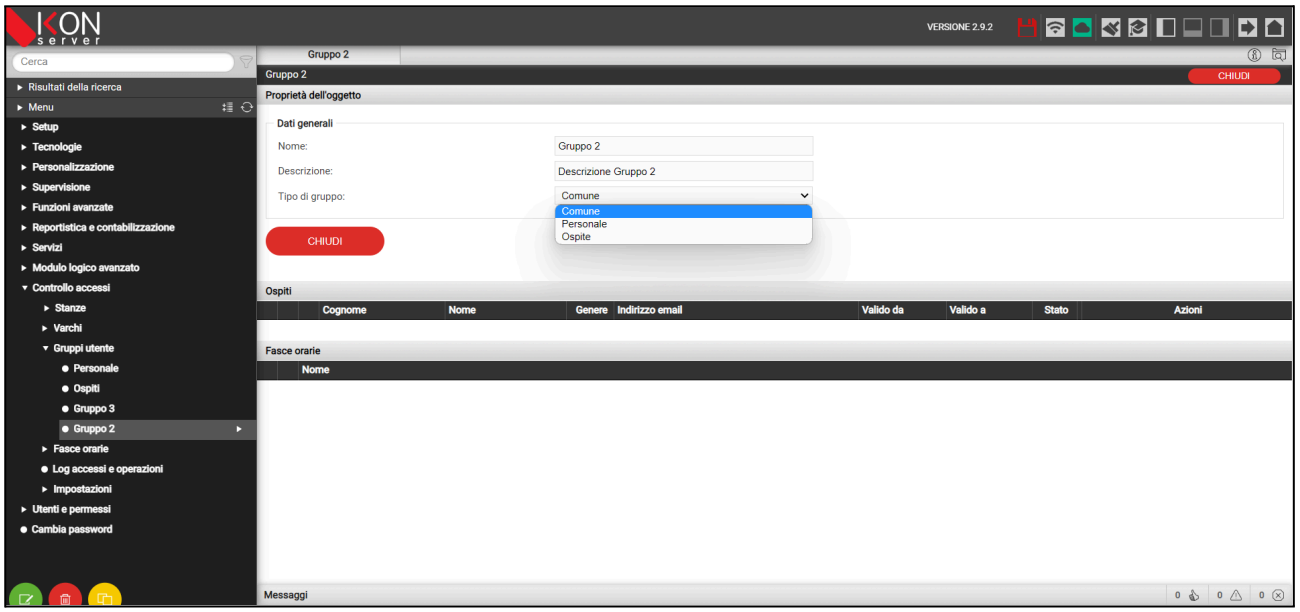
Se un varco ha una fascia oraria associata, gli utenti appartenenti ai gruppi utente abbinati a quella fascia oraria, sono soggetti a quella limitazione oraria, e pertanto possono aprire il varco solo negli orari stabiliti. Gli altri utenti (non appartenenti a questi gruppi) possono aprire il varco senza limitazioni, purché siano abilitati ad operare su quel varco / stanza.

6.2 GRUPPI UTENTE

Per creare un nuovo gruppo utente procedere come segue:

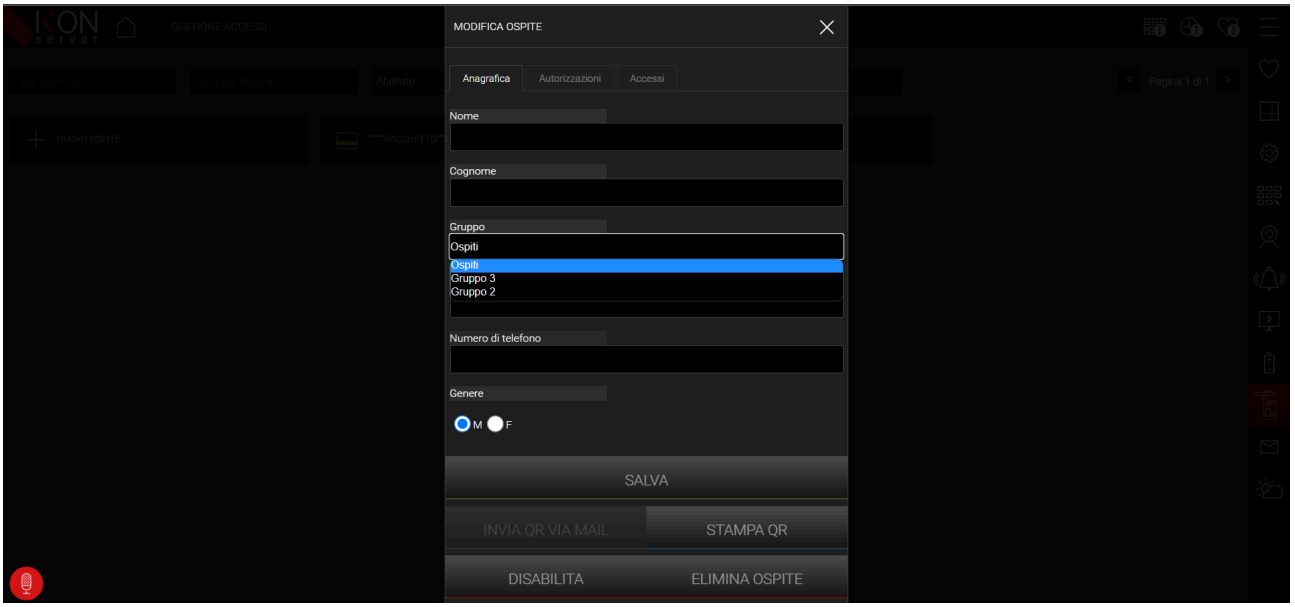
- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Premere la sotto-sezione GRUPPI UTENTE del menu laterale
- Premere il pulsante '+' che si trova in basso a sinistra

Selezionando il nuovo gruppo e premendo la sua scorciatoia (“tre puntini”) nel menu, si accede alla sua scheda di configurazione



Vengono resi disponibili i seguenti campi:

NOME	Nome del gruppo
DESCRIZIONE	Possibilità di fornire una descrizione (opzionale)
TIPO DI GRUPPO	Di default sono presenti 3 categorie così suddivise: - personale - ospite - comune (visibile sia per personale che ospite) In base a questa scelta, il nuovo gruppo viene mostrato tra quelli disponibili quando si crea un nuovo utente, a seconda che si tratti di personale di servizio, ospiti, o entrambi.



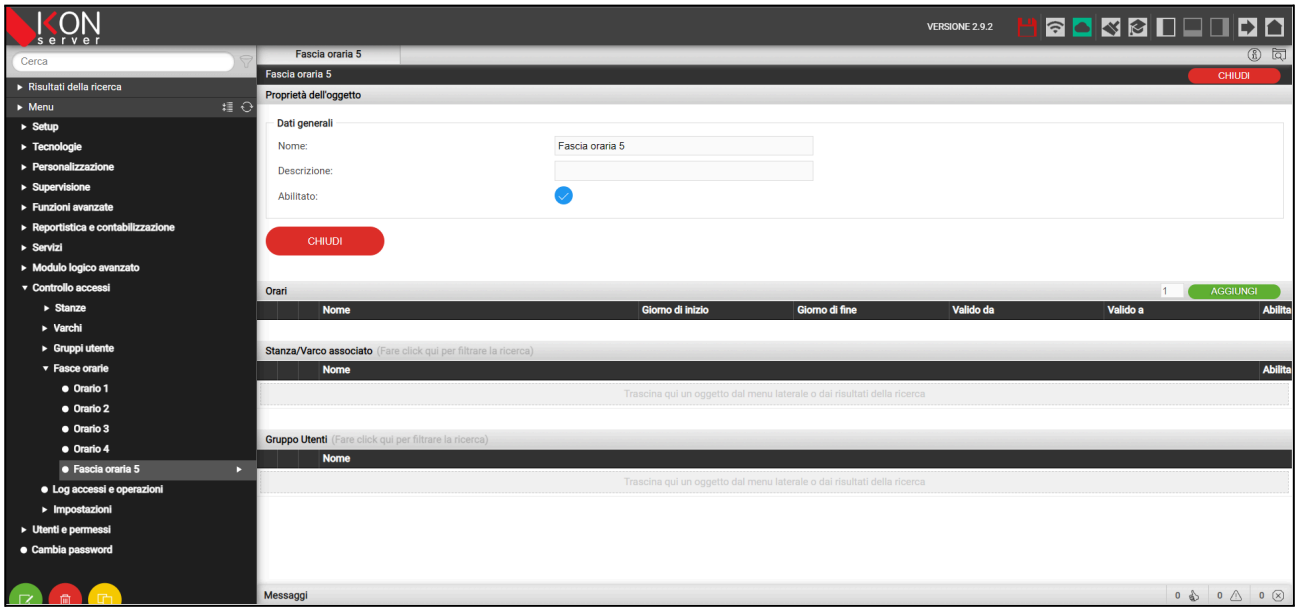
6.3 FASCE ORARIE

La sezione FASCE ORARIE ampia maggiormente la possibilità di gestire gli accessi in base agli orari. Permette in particolare di definire un accesso temporizzato ad una determinata stanza o varco, legato ad uno o più gruppi utente.

Per creare una nuova fascia oraria procedere come segue:

- Aprire la sezione CONTROLLO ACCESSI del menu laterale
- Premere la sotto-sezione FASCE ORARIE del menu laterale
- Premere il pulsante '+' che si trova in basso a sinistra

Selezionando la nuova fascia oraria, e premendo la sua scorciatoia (“tre puntini”) nel menu, si accede alla sua scheda di configurazione:



Vengono resi disponibili i seguenti campi:

NOME	Nome della fascia oraria
DESCRIZIONE	Possibilità di fornire una descrizione (opzionale)
ABILITATO	Permette di abilitare o disabilitare la fascia oraria creata

Come nella figura di esempio sotto, ci sono 3 sezioni da popolare:

- ORARI: è possibile usare il pulsante verde “Aggiungi” per aggiungere intervalli orari, nei quali la fascia oraria è attiva e quindi si può accedere al varco.

  Per ognuno degli orari, è necessario inserire le seguenti informazioni:

  - giorno (della settimana) di inizio
  - giorno (della settimana) di fine
  - valido da (ora di inizio dell’orario consentito)
  - valido a (ora di fine dell’orario consentito)

- STANZE/VARCO ASSOCIATO: premendo sul filtro di ricerca, nel menu a sinistra vengono visualizzate tutte le stanze/varco create e si può scegliere quale inserire semplicemente trascinandole.

- GRUPPI UTENTI: analogamente al menu descritto sopra, cliccare sul filtro e trascinare al suo interno il gruppo di utenti che che si vuole abilitare al controllo della fascia oraria

Segue uno screenshot di esempio di una configurazione per una fascia oraria, con un orario consentito, un varco associato ed un gruppo utenti abbinato:



6.4 UTILIZZO CON LETTORI KNX

Se si utilizza MyWAY con lettori KNX, le fasce orarie vengono trasmesse in fase di configurazione ai lettori, in modo che siano essi stessi ad abilitare o meno l'accesso di un determinato PIN (a differenza delle tastiere MyWAY su RS485, laddove viceversa la validazione viene fatta a livello centralizzato sul server).

Questo tipo di tastiere supporta solo fasce orarie che iniziano o finiscono con ore "intere" (es: dalle 8:00 alle 12:00, non è possibile specificare dalle 8:30). Per questo motivo, in questa particolare situazione, è necessario impostare il flag FILTRO FASCE ORARIE nella sezione

CONTROLLO ACCESSI > IMPOSTAZIONI > IMPOSTAZIONI GENERALI

alla voce ORE, in modo da costringere la configurazione degli orari senza poter stabilire i minuti.

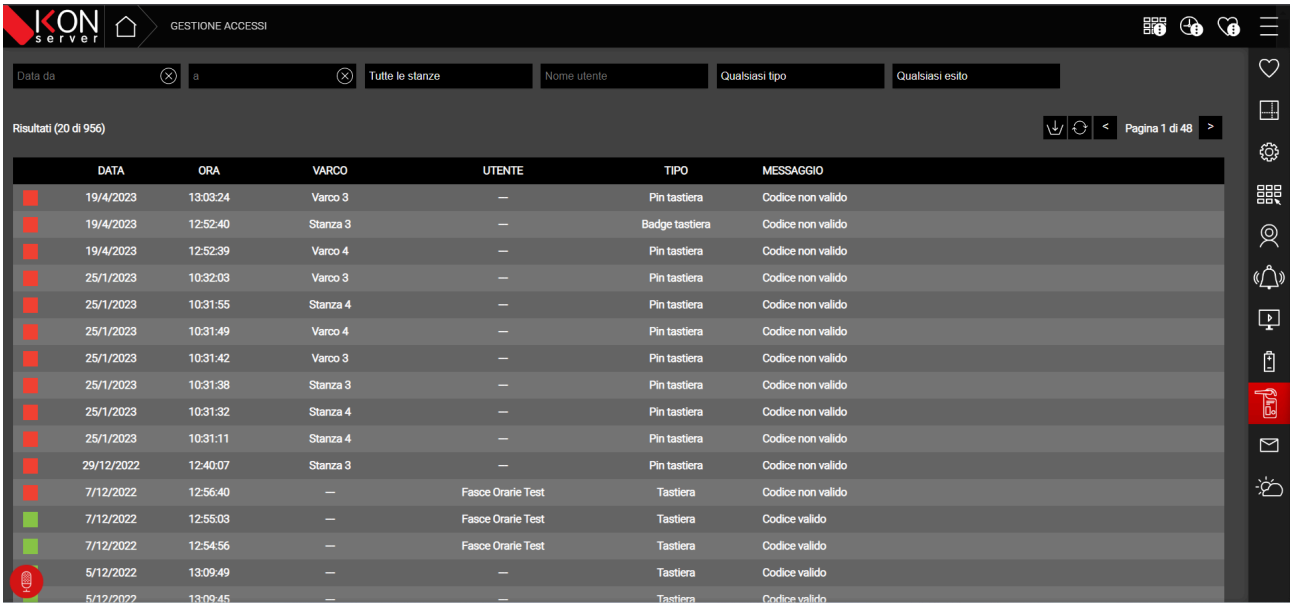
7 LOG ACCESSI E OPERAZIONI

La sezione LOG ACCESSI E OPERAZIONI permette di tenere traccia di tutte le operazioni avvenute nella struttura, sia in caso di accesso valido, sia di tentativi di accesso non validati.

La lista degli accessi e delle operazioni è disponibile sia in Frontend che in Backend.

7.1 FRONTEND

Segue un esempio di lista di operazioni consultabile dal menu principale degli accessi:

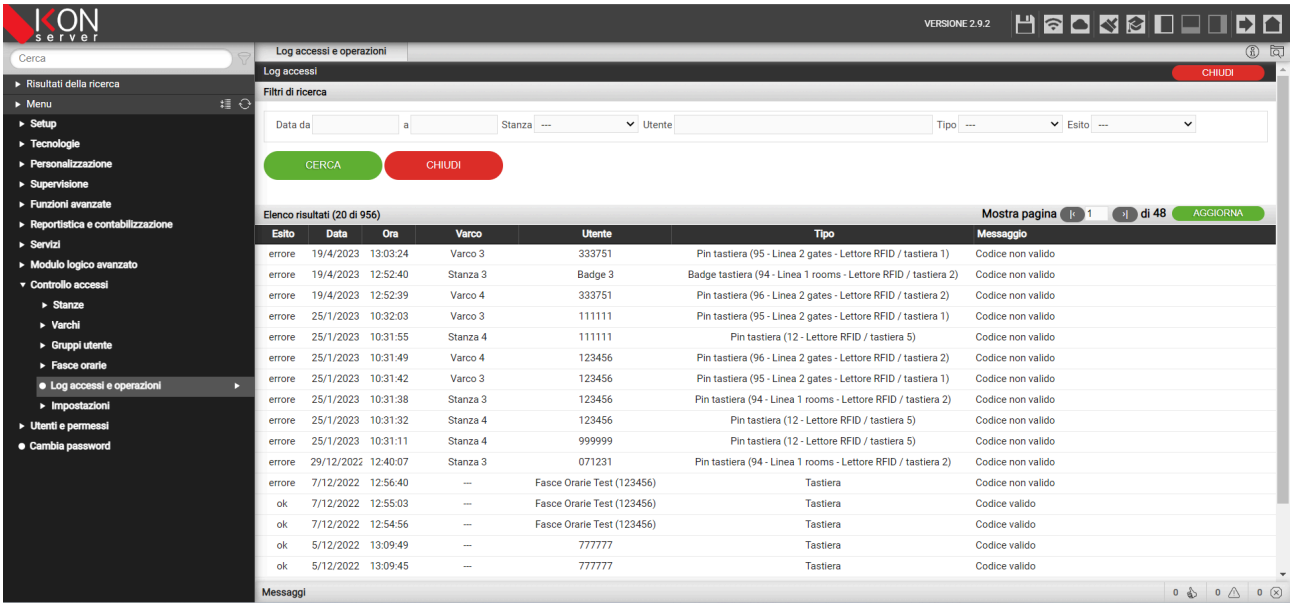


In particolare, sono disponibili le seguenti colonne:

DATA / ORA	Orario dell'evento storicizzato
VARCO	Varco o stanza interessato all'evento
UTENTE	Se presente, il riferimento all'ospite o al personale che ha effettuato l'operazione
TIPO	Tipologia di accesso: con PIN da tastiera, con badge, tramite app etc…
MESSAGGIO	Descrittivo dell'evento: codice valido o non valido etc…

7.2 AMMINISTRAZIONE

In modo del tutto analogo, è possibile consultare il log degli eventi in amministrazione; la schermata seguente mostra un esempio di tale visuale:



In entrambi i casi è possibile inserire dei filtri di ricerca utilizzando i campi:

- Data da - a
- Stanza
- Utente
- Tipo
- Esito

8 TASTIERE MYWAY

8.1 PREMESSA

Oltre al controllo tramite app MyWAY, è possibile installare una o più tastiere numeriche MyWAY, attraverso le quali i visitatori possono aprire i varchi digitando il medesimo codice PIN (a 6 cifre) ricevuto via email.

Per poter gestire i lettori MyWAY all'interno di IKON SERVER è necessario accertarsi di avere la relativa tecnologia abilitata nella sezione

SETUP > GESTIONE MODULI E LICENZE

in corrispondenza della voce

MyWAY (RFID / TASTIERE)

Se il modulo non è attivo, richiedere una licenza di attivazione al nostro servizio assistenza tecnica.

8.2 INSTALLAZIONE

Le tastiere numeriche MyWAY richiedono i seguenti collegamenti:

- Alimentazione 12V DC
- RS485

E' possibile collegare più lettori sullo stesso cablaggio RS485, avendo cura di rispettare la medesima polarità nel collegamento entra-esci.

Il cavo RS485 deve essere collegato alla porta RS485 integrata di IKON SERVER, oppure ad un adattatore USB-RS485 (se la porta RS485 di IKON SERVER è già occupata per altra applicazione), avendo cura di invertire la polarità rispetto a quella indicata sui lettori, quindi:

MORSETTO TASTIERA	MORSETTO IKON SERVER	ADATTATORE USB-485
B+	-	-
B-	+	+

Non è necessario infine collegare il GND.

Sull'ultima tastiera va infine montato il jumper con resistenza di fine linea in corrispondenza della morsettiera RES JPTERM.

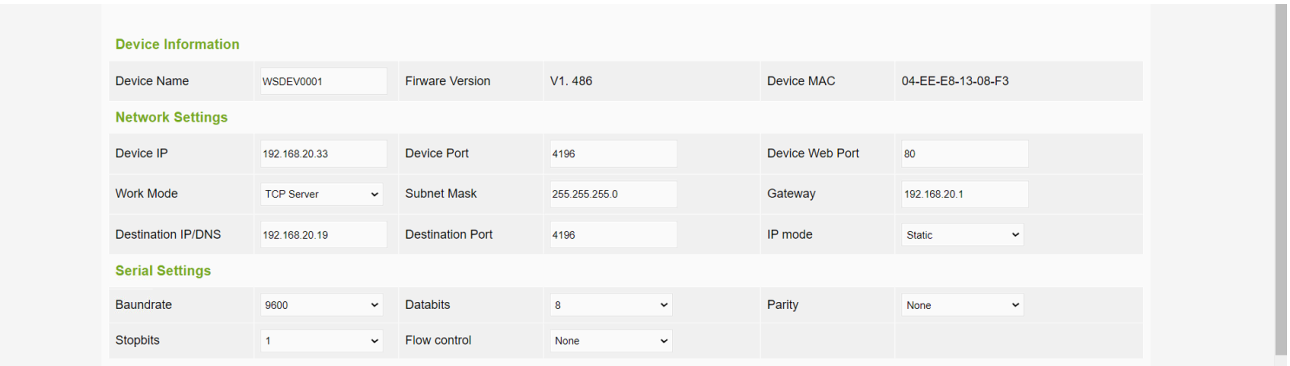
Per il cablaggio RS485 si consiglia l'adozione di cavi Belden 9841 (singola coppia) o Belden 9842 (doppia coppia) o analoghe prestazioni.

Attenzione: non è possibile utilizzare la medesima porta RS485 e medesima linea per gestire tastiere MyWAY e dispositivi I/O del catalogo Domotica Labs, così come più in generale altri dispositivi operanti in RS485. E' necessario a tale scopo utilizzare due porte di IKON SERVER, ricorrendo ad un adattatore USB-RS485.

8.2.1 CONVERTITORE IP/485

Nel caso in cui la porta 485 sia già occupata è possibile utilizzare il convertitore da 485 a ip e va configurato da pagina web con i seguenti passaggi:

1) IP DI DEFAULT 192.168.1.200 / 192.168.1.254
2) ACCEDERE DA PAGINA WEB CON CREDENZIALI admin o 1234
3) configurare il sistema come da immagine sotto
    a) DEVICE IP = IP convertitore
    b) DESTINATION IP = IP Ikon
4) Impostare su ikon nella sezione tecnologie > myway l'indirizzo ip del convertitore con porta 4196



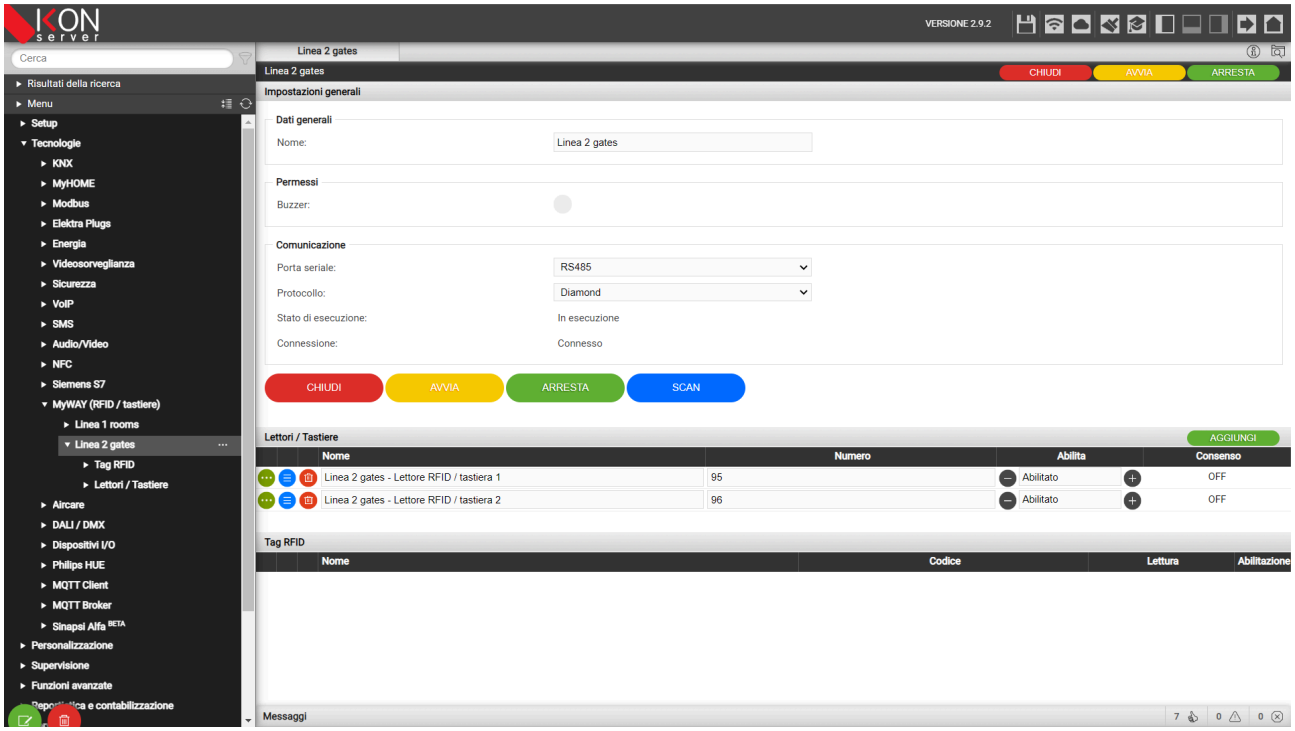


8.3 NUOVA LINEA

Per gestire una o più tastiere, è necessario innanzitutto evidenziare la sezione

TECNOLOGIE > MyWAY (RDIF / TASTIERE)

e premere il pulsante AGGIUNGI in basso nella toolbar; una volta creata la nuova linea nel menu, selezionarla per aprire la sua scheda di dettaglio. Viene mostrata una pagina simile alla seguente:



Sono richieste le seguenti informazioni:

BUZZER	Abilita o meno un effetto sonoro (sul primo lettore) all'avvio della comunicazione, per riscontro di corretto funzionamento
PORTA SERIALE	Selezionare la porta di IKON SERVER a cui sono collegate le tastiere
PROTOCOLLO	Selezionare “DIAMOND”

Una volta inserite le informazioni richieste, avviare la comunicazione tramite il pulsante AVVIA, verificando che lo stato di esecuzione passi in “IN ESECUZIONE”.

8.4 CREAZIONE DI UNA TASTIERA

Per ogni tastiera installata, procedere come segue:

- Premere il pulsante AGGIUNGI
- Personalizzare eventualmente la dicitura della nuova tastiera, per rendere più facile la sua identificazione successiva

- Inserire nell'apposito campo NUMERO l'indirizzo univoco associato alla tastiera, riportato sul prodotto
- Abilitare la comunicazione tramite l'apposito menu a tendina “ABILITA”
- Inoltre nella scheda della tastiera è possibile decidere se è abilitato o no alla scansione dei badge

Dopo aver creato e indirizzato tutte le tastiere, premere ARRESTA e successivamente AVVIA per recepire le modifiche. Verificare che lo stato di connessione passi a CONNESSO.

8.5 ASSOCIAZIONE A UNA STANZA

Se una tastiera è installata in corrispondenza della porta di accesso ad una stanza, essa va associata in IKON SERVER nel seguente modo:

- Identificare la sezione STANZA nella scheda della tastiera (accedendo alla sua scheda di dettaglio)
- Premere sul titolo della sezione, per filtrare il motore di ricerca con tutte le stanze precedentemente configurate
- Trascinare la stanza desiderata nella lista

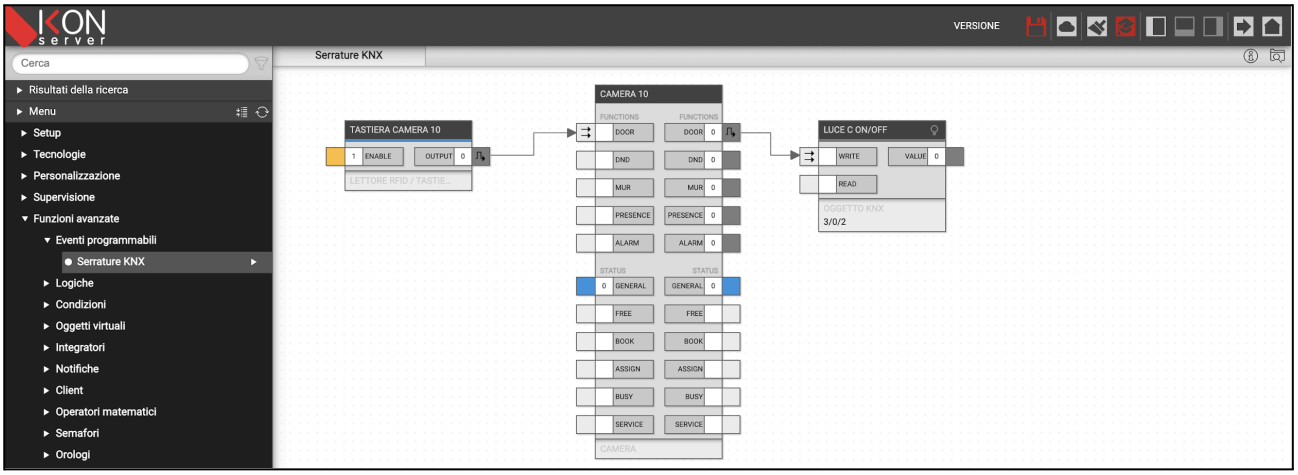
In questo modo, quando un ospite viene abilitato all'accesso alla stanza e riceve email di benvenuto con il codice PIN, oltre a poterlo utilizzare da app MyWAY, può digitarlo direttamente sul lettore. Al termine del soggiorno, il PIN viene automaticamente disabilitato.

Si ricorda che per l’utilizzo del PIN è necessario digitare **PIN#** .

Per far sì che all'inserimento corretto di un PIN venga aperta la serratura della stanza, è necessario associare il CONSENSO della tastiera alla funzione ELETTROSERRATURA della stanza. La modalità più semplice per effettuare questa associazione è la seguente:

- Creare un EVENTO PROGRAMMABILE
- Trascinare al suo interno la TASTIERA MyWAY
- Trascinare al suo interno anche la STANZA
- Collegare il nodo di uscita OUTPUT della TASTIERA all'ingresso DOOR della stanza

Si consiglia di utilizzare il medesimo evento programmabile per collegare in cascata all'uscita DOOR della STANZA l'oggetto che rappresenta la serratura, come in questo esempio:



Per consultare in un dato momento i PIN validi per un lettore, è sufficiente accedere alla sua scheda di dettaglio, e consultare la lista “PIN DI ACCESSO”.

8.6 ASSOCIAZIONE AD UN VARCO

L'associazione di una tastiera a un varco è identica a quella di una stanza, per cui si rimanda al punto precedente di questa guida consigliando di eseguire gli stessi passaggi su un varco anziché su una stanza.

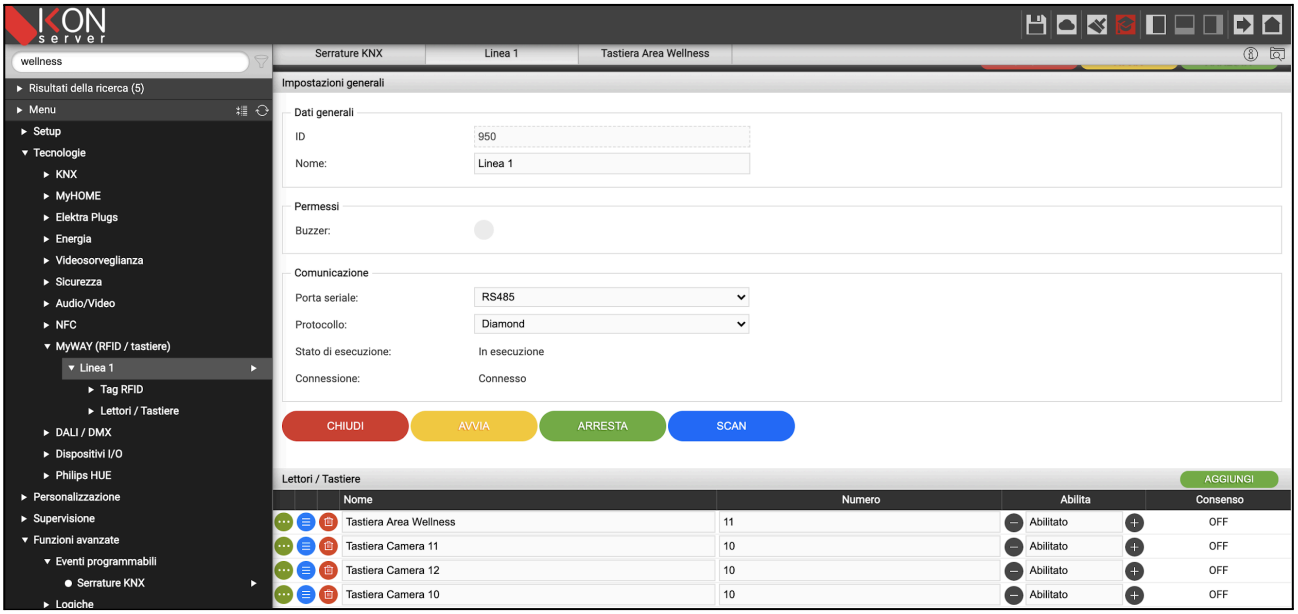
Anche nel caso dei varchi, è necessario associare il consenso del lettore alla serratura del varco e, in cascata, l'oggetto che rappresenta la serratura, come in questo esempio:



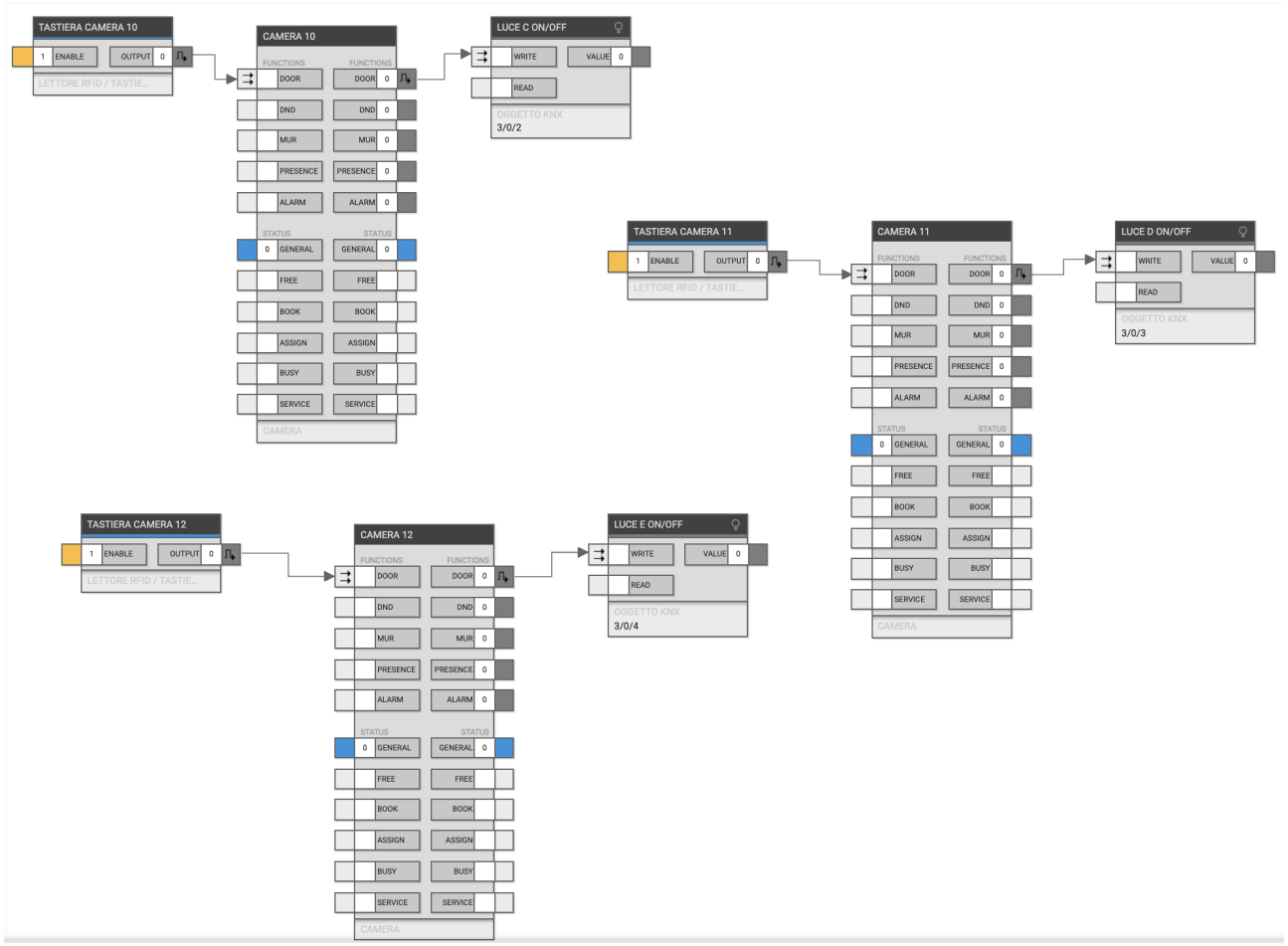
8.7 UTILIZZO DELLA STESSA TASTIERA PER PIÙ STANZE

A partire dalla versione 2.8.6 è possibile utilizzare la medesima tastiera per aprire più stanze o varchi; in base al PIN digitato, il sistema riconosce l'utente e il varco da aprire.

Questo tipo di configurazione prevede la creazione di più tastiere, nello stesso modo illustrato in precedenza, inserendo per ognuna di essere **lo stesso indirizzo RS485**, come in questo esempio (per le stanze 10, 11 e 12):



Le tastiere a quel punto possono essere associate alle stanze / varchi, e collegate alle relative serrature tramite eventi programmabili, nello stesso identico modo visto in precedenza; ad esempio, la figura seguente mostra un evento programmabile unico nel quale sono state inserite le associazioni tra tastiere, stanze e serrature KNX per le tre stanze 10, 11 e 12 (servite dalla stessa tastiera “fisica” con indirizzo RS485 numero 10):


TASTIERA CAMERA 10
1 ENABLE
OUTPUT 0
LETTORE RFID / TASTIE...
CAMERA 10
FUNCTIONS
DOOR
DND
MUR
PRESENCE
ALARM
STATUS
GENERAL
FREE
BOOK
ASSIGN
BUSY
SERVICE
CAMERA
LUCE C ON/OFF
WRITE
VALUE 0
READ
OGGETTO KNX
3/0/2
TASTIERA CAMERA 11
CAMERA 11
LUCE D ON/OFF
3/0/3
TASTIERA CAMERA 12
CAMERA 12
LUCE E ON/OFF
3/0/4

9 TASTIERE KNX

9.1 PREMESSA

E' possibile gestire in modo integrato una o più tastiere numeriche KNX della serie BLUMOTIX DOORY oppure EELECTRON 9025, alle quali è possibile inviare tramite bus uno o più codici PIN (a 6 cifre) abilitati all'apertura del varco, tramite un telegramma con lunghezza 10 byte (oggetto di comunicazione “Richiesta/Salva”).

Durante l'importazione, trattandosi di un tipo di dato non standard, viene richiesto di specificare manualmente la codifica – indicare “Tastierino numerico (10 byte)” - ed il rendering – utilizzare “Tastierino numerico”.



Una volta completata l'importazione, è possibile utilizzare gli oggetti KNX a 10 byte per abilitare, o disabilitare, i codici PIN degli ospiti, in modo completamente automatico.

Dopo aver importato gli indirizzi, aprire le impostazioni dell’indirizzo di gruppo 10 byte e selezionare il modello della tastiera EELECTRON / BLUMOTIX.

Successivamente riavviare i Servizi di Comunicazione dalla sezione Setup - Manutenzione.

In IKON per tastiere EELECTRON importare i 3 indirizzi sottolineati.

5/5/10	Cliente Abilita	No	No	enable	1 bit	1
5/5/9	Cliente Comando	No	No	switch	1 bit	1
5/5/8	Comando	No	No	switch	1 bit	1
5/5/0	Data Ingresso	No	No	date	3 bytes	1
5/5/6	HVAC	No	No	HVAC mo...	1 byte	1
5/5/2	Legacy	No	No		10 bytes	1
5/5/1	Ora Ingresso	No	No	time of day	3 bytes	1
5/5/3	Reset Legacy	No	No		10 bytes	1
5/5/5	Scenario	No	No	scene nu...	1 byte	1
5/5/7	Setpoint	No	No	temperat...	2 bytes	1
5/5/4	Transito	No	No	entrance...	4 bytes	1

In IKON per tastiere BLUMOTIX importare i 3 indirizzi sottolineati.

5/0/6	Abilitazione	No	No	enable	1 bit	1
5/0/5	Esaurita	No	No	boolean	1 bit	1
5/0/3	Esito Numero Salvati	No	No	pulses	2 bytes	1
5/0/1	Esito Richiesta Salva/cancella	No	No	entrance...	4 bytes	1
5/0/9	Esito Tentativo	No	No	entrance...	4 bytes	1
5/0/11	On/Off	No	No	switch	1 bit	1
5/0/4	Richiesta Cancellazione	No	No	boolean	1 bit	1
5/0/2	Richiesta Numero Salvati	No	No	counter p...	1 byte	1
5/0/7	Richiesta Per Indice	No	No	counter p...	1 byte	1
5/0/0	Richiesta Salva/cancella	No	No		10 bytes	1
5/0/8	Risposta Per Indice	No	No	entrance...	4 bytes	1
5/0/10	Simulazione	No	No	entrance...	4 bytes	1
5/0/13	Stato Abilita/Disabilita	No	No	switch	1 bit	1

9.2 ASSOCIARE LA TASTIERA KNX A UNA STANZA

E' possibile associare l'oggetto richiesta/salva a una stanza, in modo tale da automatizzare la richiesta di salvataggio e cancellazione dei PIN dei clienti e del personale di servizio in base al loro periodo di validità.

Per associare una tastiera KNX a una stanza procedere come segue:

- Aprire la pagina di editing della stanza a cui si vuole associare una tastiera KNX
- Ricercare l'oggetto 10 byte o 4 byte del tastierino nel menù laterale tramite la barra di ricerca in alto a sinistra o filtrando gli elementi facendo click sul filtro a fianco della nomenclatura “Tastiere KNX” posto nella sezione della pagina di editing della stanza
- Trascinare l'oggetto 10 byte o 4 byte all'interno della sezione “Tastiere KNX” della pagina di editing della stanza



- Trascinare l’oggetto Abilitazione/Comando a 1 bit nelle Connessioni in Ingresso della Serratura Virtuale della stanza, impostando Sempre > Scrivi > Valore Corrente

In questo modo si è creata un'associazione fra l'oggetto della tastiera KNX 10 byte o 4 byte e la stanza gestita tramite il controllo accessi.

Ciò significa che all'abilitazione di un utente su una stanza che possiede una tastiera KNX associata verrà inviata alla tastiera una richiesta di attivazione del codice PIN dell'utente; da quel momento in poi inserendo il pin dell'utente sul tastierino KNX associato alla stanza sarà permessa l'azione configurata.

Viceversa, alla scadenza,disabilitazione o al cambio stanza dell'utente verrà inviata alla tastiera una richiesta di eliminazione del PIN dell'utente, in modo tale da impedirne l'accesso nel periodo in cui non è abilitato ad interagire con la stanza.

9.3 ASSOCIARE LA TASTIERA KNX A UN VARCO

L'associazione di una tastiera KNX a un varco è identica a quella di una stanza, per cui si rimanda al punto precedente di questa guida consigliando di eseguire gli stessi passaggi su un varco anziché su una stanza.

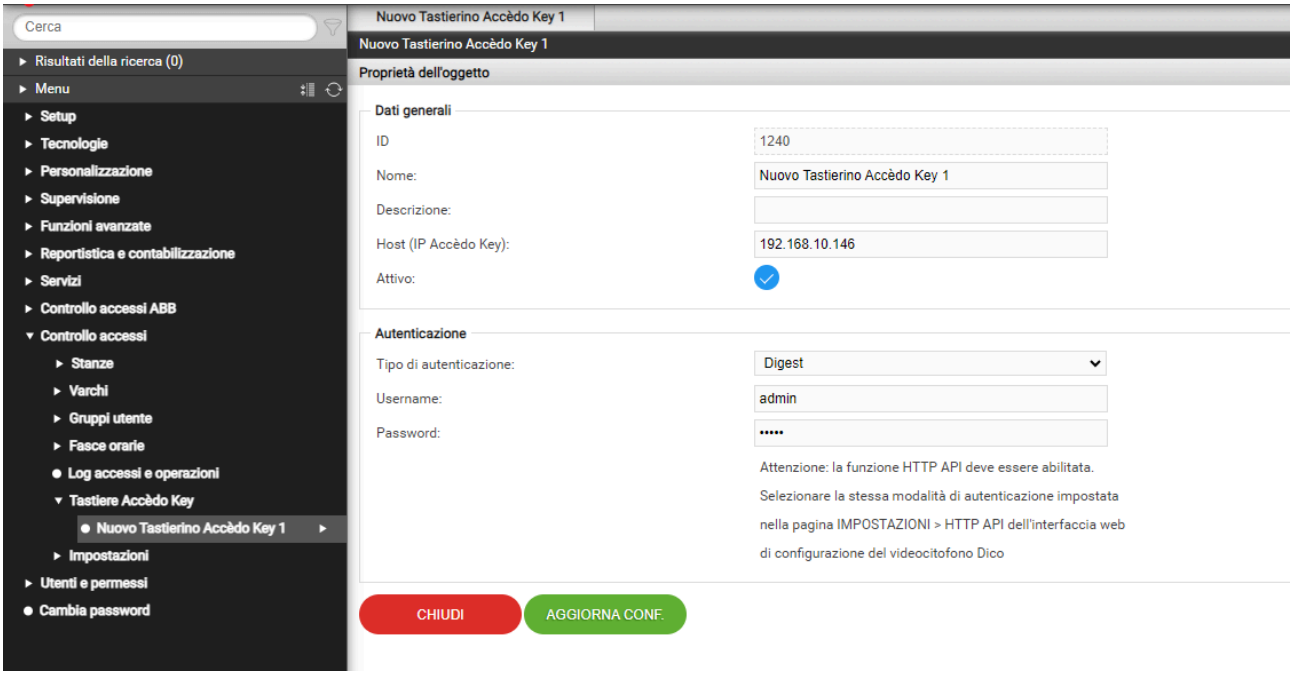
10 DISPOSITIVO DICO/ACCEDO KEY

10.1 PREMESSA

E' possibile gestire in modo integrato una o più tastiere della serie DICO/ACCEDO KEY

Per configurarle è necessario inserire l'ip del dispositivo e il tipo di autenticazione scelta tra quelle disponibili.

Successivamente deve essere configurata tramite il portale del dispositivo.



Al termine delle impostazioni è necessario premere su Aggiorna Conf per salvare, in questo modo viene inserito il flag su Attiva ed è la conferma che il dispositivo stia funzionando correttamente.

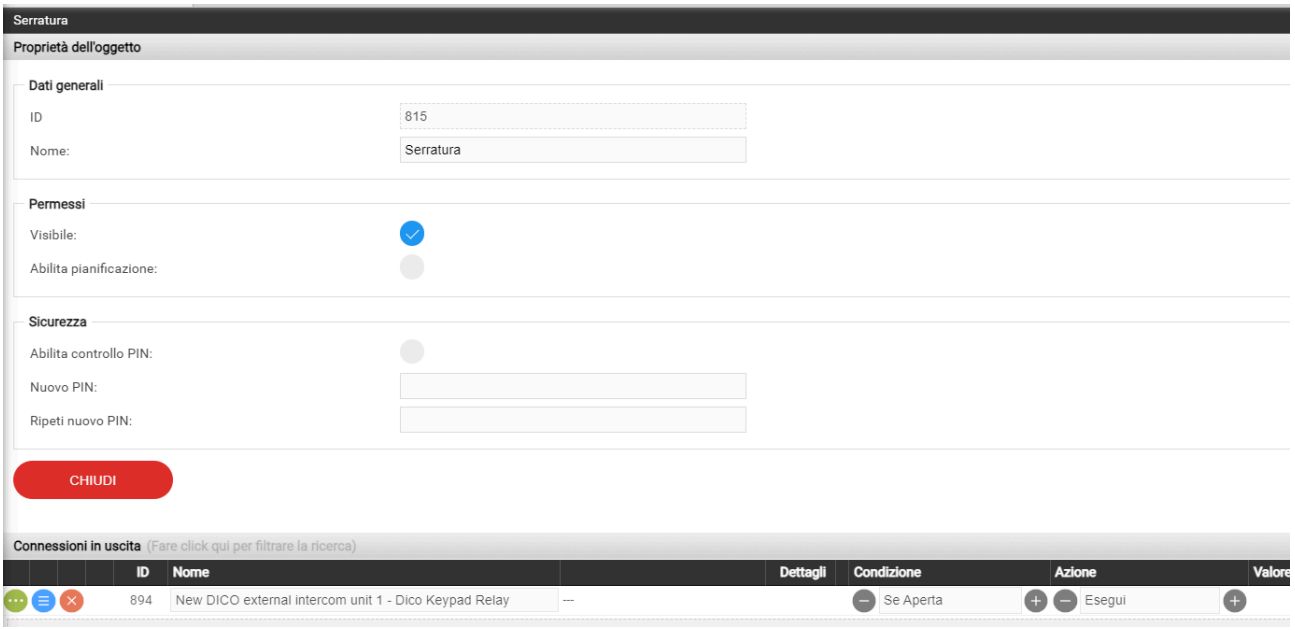
10.2 ASSOCIARE DISPOSITIVO A UNA STANZA

E' possibile associare il dispositivo a una stanza, in modo tale da automatizzare la richiesta di salvataggio e cancellazione dei PIN dei clienti e del personale di servizio in base al loro periodo di validità.

Per associare un dispositivo DICO/ACCEDO KEY a una stanza procedere come segue:

- Aprire la pagina di editing della stanza a cui si vuole associare il dispositivo
- Ricercare il dispositivo nel menù laterale tramite la barra di ricerca in alto a sinistra o filtrando gli elementi facendo click sul filtro a fianco della nomenclatura "Videocitofoni DICO/Tastiere Accèdo Key" posto nella sezione della pagina di editing della stanza
- Trascinare il dispositivo all'interno della sezione "Videocitofoni DICO/Tastiere Accèdo Key" della pagina di editing della stanza

Quando si aggiunge un dispositivo DICO/ACCEDO KEY ad una stanza, automaticamente viene aggiunto il relè principale del dispositivo stesso alla connessione in uscita dell'oggetto virtuale serratura della stanza.



10.3 ASSOCIARE DISPOSITIVO A UN VARCO

L'associazione di un dispositivo DICO/ACCEDO KEY a un varco è identica a quella di una stanza, per cui si rimanda al punto precedente di questa guida consigliando di eseguire gli stessi passaggi su un varco anziché su una stanza

11 GESTIONE DA FRONTEND

11.1 PREMESSA

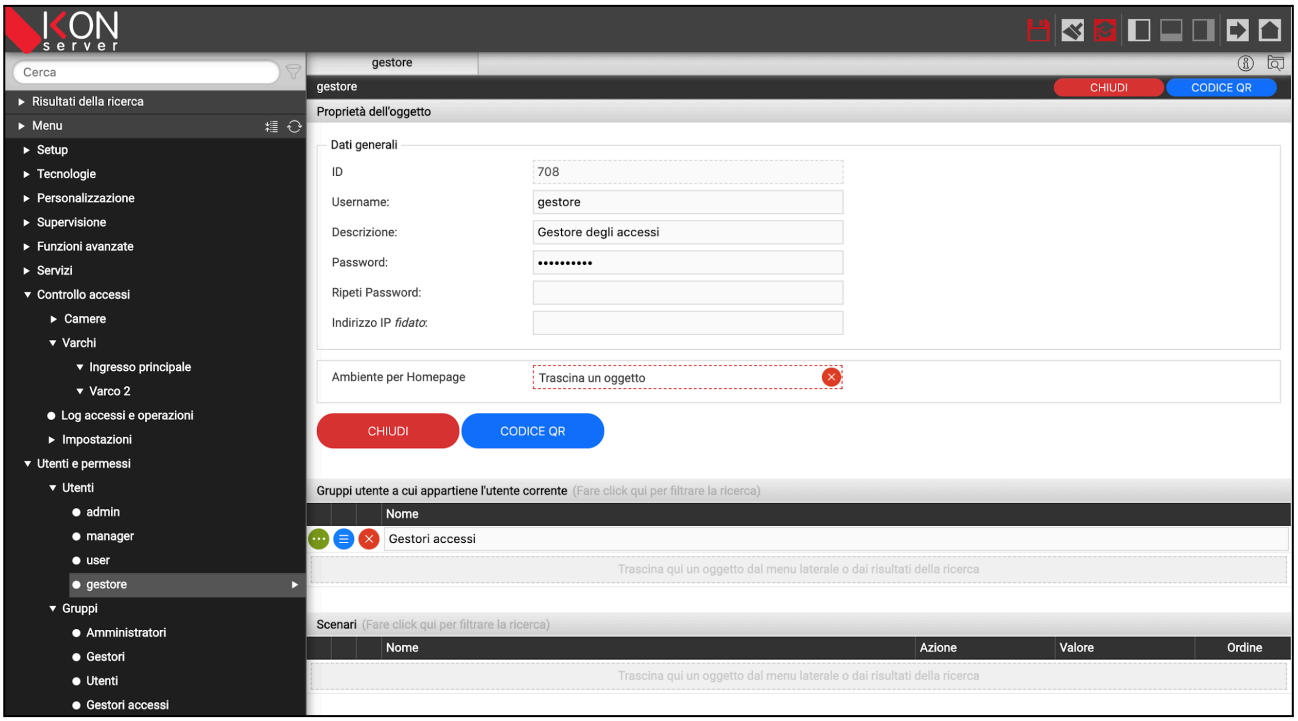
Una volta completata la configurazione, come visto in precedenza, il gestore dell'edificio può operare esclusivamente nel FRONTEND di IKON SERVER, per gestire ospiti, personale, e stanze.

11.2 UTENTE DEDICATO

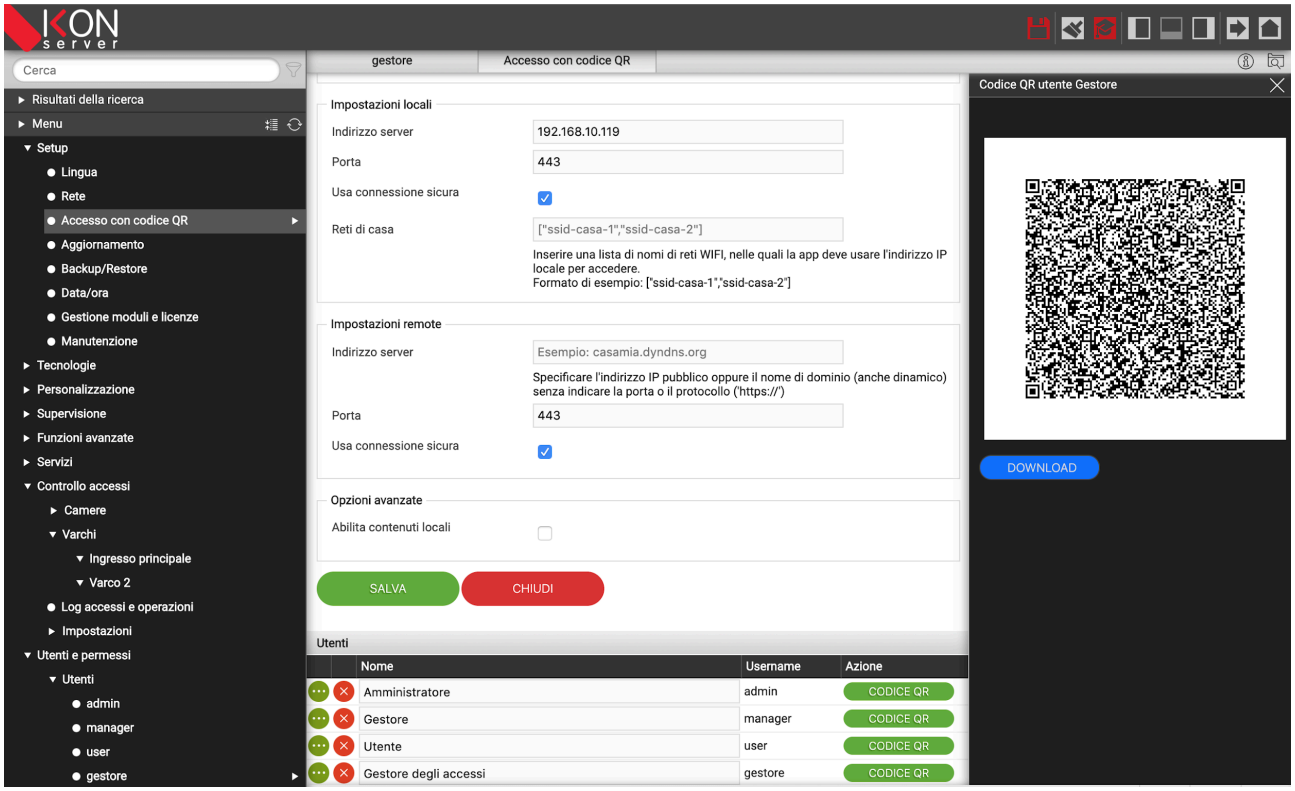
Si consiglia di predisporre (almeno) un utente dedicato in IKON SERVER per il gestore della struttura, diverso dall'utente admin; in questo modo, si limita la possibilità di errori accidentali nella configurazione del webserver.

Il modulo controllo accessi introduce un nuovo gruppo utenti denominato “GESTORI ACCESSI” che possiede tutti i diritti strettamente necessari per l'amministrazione degli accessi; si consiglia quindi di:

- Creare un utente nella sezione UTENTI E PERMESSI > UTENTI
- Una volta creato (ed associato ad una password) trascinare al suo interno il gruppo “GESTORI ACCESSI”



- Accedere alla sezione SETUP > ACCESSO CON QR
- Identificare il nuovo utente nella sezione in basso, e premere il pulsante “CODICE QR” corrispondente
- Fornire al gestore della struttura il codice QR generato da IKON, per velocizzare la sua configurazione della app SUPERVISOR

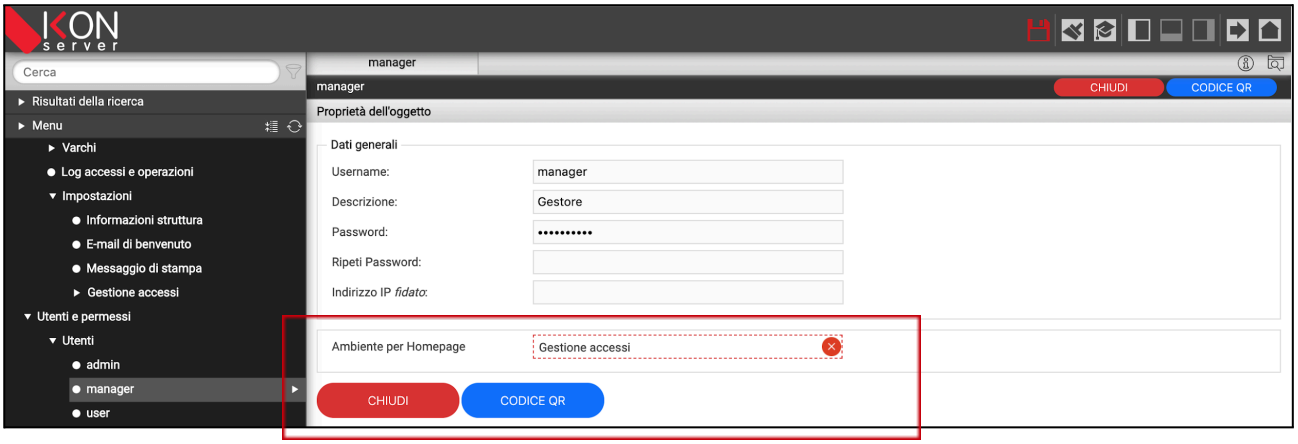


Il gestore dovrà utilizzare l'app SUPERVISOR per gestire gli accessi; l'app MyWAY, come si vedrà in seguito, è unicamente dedicata al personale ed agli ospiti della struttura, ed ha funzionalità strettamente legate all'apertura dei varchi ed alla gestione della propria stanza.

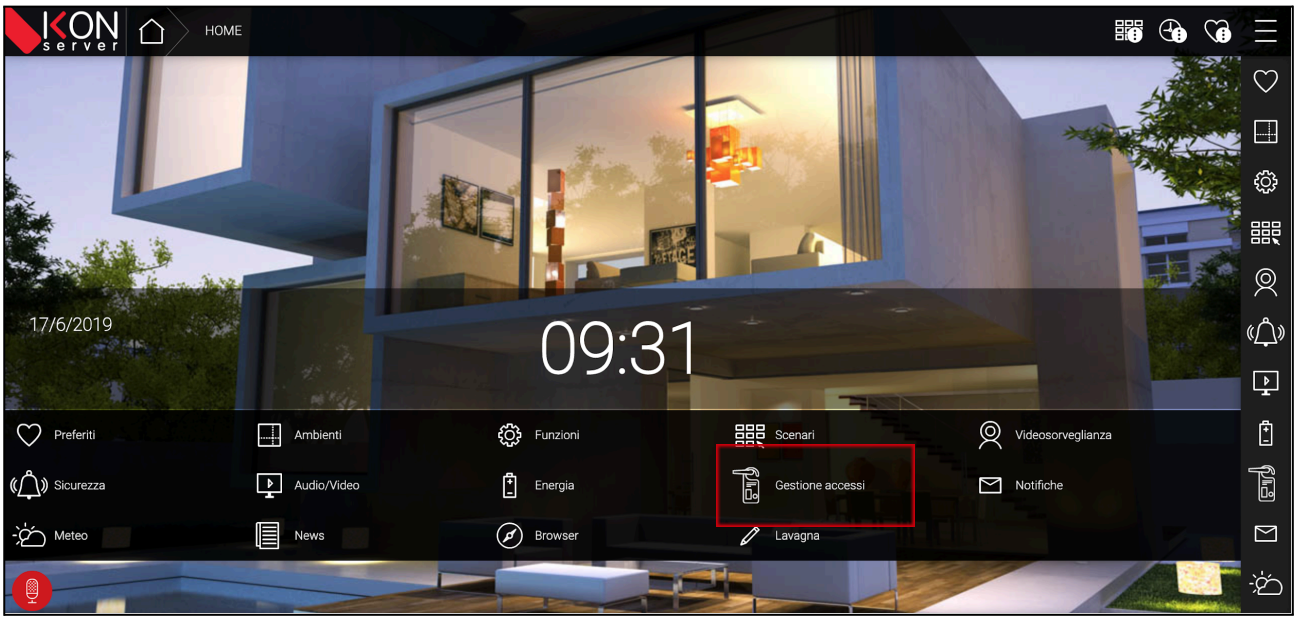
11.3 IMPOSTAZIONE HOME PAGE

Si consiglia di impostare il menu principale del CONTROLLO ACCESSI come homepage per l'utente gestore; a tale scopo:

- Aprire la scheda dell'utente creato al punto precedente
- Identificare il campo "AMBIENTE PER HOMEPAGE"
- Espandere il menu CONTROLLO ACCESSI > IMPOSTAZIONI
- Trascinare la sotto-voce GESTIONE ACCESSI

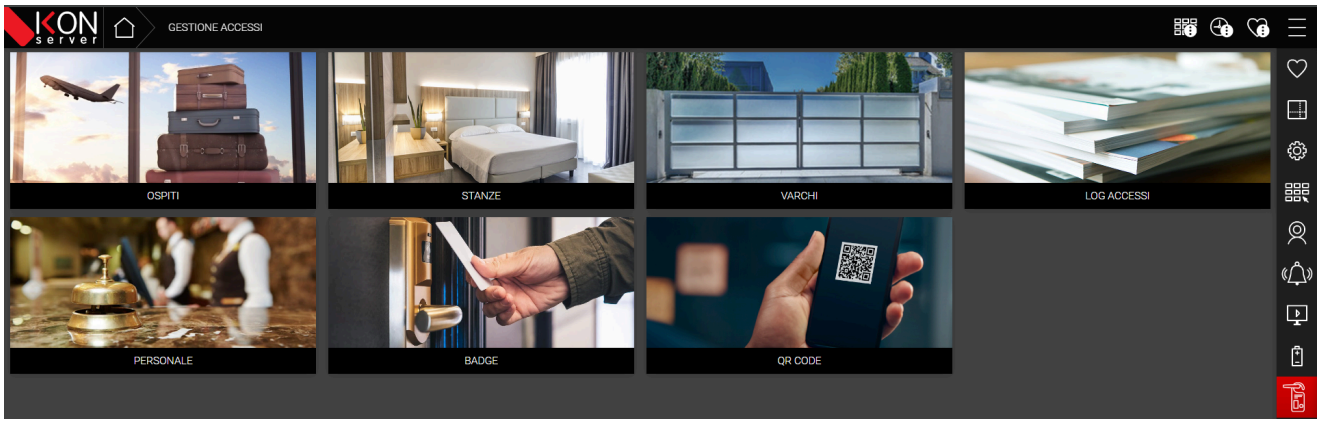


Se non si è impostato il controllo accessi come home predefinita, invece, è possibile accedere al suo menu dalla HOME PAGE, selezionando la voce GESTIONE ACCESSI.



11.4 GESTIONE ACCESSI

La schermata di gestione degli accessi si presente nel seguente modo:



Le voci di base disponibili sono:

- OSPITI
- STANZE
- VARCHI
- LOG ACCESSI
- PERSONALE
- BADGE
- QR CODE

E' possibile aggiungere ambienti di IKON SERVER a questo menu; questo è utile per mettere a disposizione pagine di supervisione al gestore della struttura, nel momento in cui la sua homepage diventi questo menu, come illustrato nel punto precedente. A tale scopo, è sufficiente:

- Aprire in modifica la voce CONTROLLO ACCESSI > IMPOSTAZIONI > CONTROLLO ACCESSI
- Trascinarvi dentro gli ambienti di IKON, avendo cura che essi abbiano una immagine di sfondo associata (che viene usata come immagine nel menu)

11.5 OSPITI

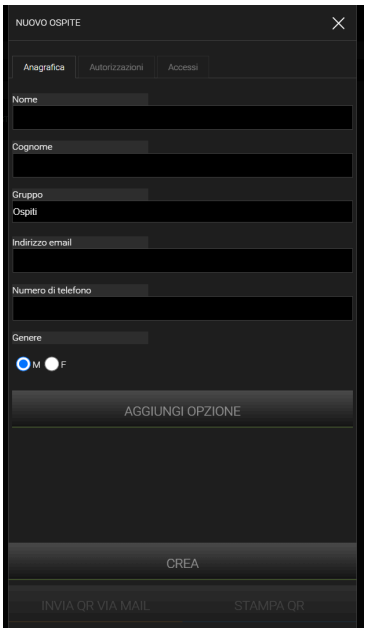
Questa voce permette di creare e gestire ospiti per la struttura. Viene aperta la seguente pagina, che permette di creare nuovi clienti e di gestire quelli creati in precedenza:

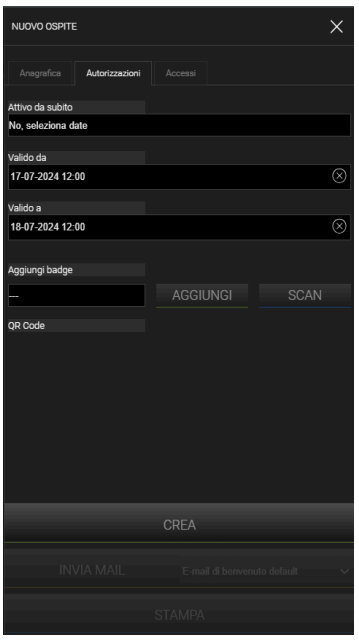


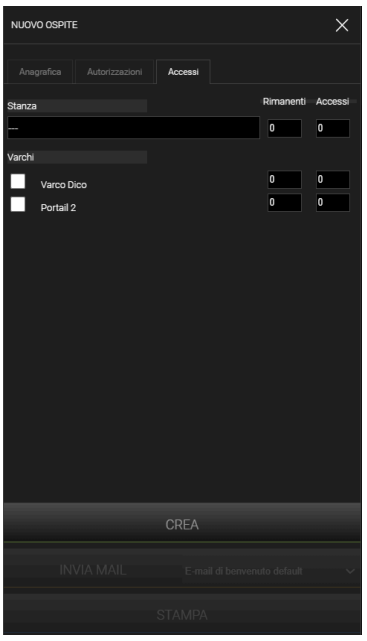
In alto sulla sinistra è presente una barra di ricerca, utile a trovare un utente specifico in base al NOME, alla STANZA assegnatagli o al suo stato (ABILITATO/DISABILITATO); inoltre è possibile ORDINARE la ricerca per NOME o PER DATA DI CREAZIONE (predefinito) in ORDINE CRESCENTE o DECRESCENTE (predefinito).

In alto sulla destra si trova il menù di navigazione delle pagine; nel caso in cui si abbiano più di 15 ospiti (numero massimo di ospiti visualizzati in una pagina) sarà possibile passare da una pagina all'altra per visualizzarli tutti.

Per creare un nuovo ospite, è sufficiente premere il pulsante NUOVO OSPITE, e compilare il form che viene proposto sotto forma di popup:







I parametri che si possono inserire sono suddivisi in diverse categorie:

ANAGRAFICA	Dati generali dell'ospite: nominativo, recapiti etc… e gruppo utente di appartenenza
AUTORIZZAZIONI	Impostazioni generali per l'accesso alla struttura: periodo di validità, eventuale badge, qr code, etc…
ACCESSI	Elenco dei varchi o delle stanze a cui ha diritto di poter accedere ed eventuale Limite accessi

In dettaglio, le informazioni richieste sono le seguenti:

NOME (campo obbligatorio) COGNOME (campo obbligatorio)	Nome e cognome dell'ospite
GRUPPO	Selezionare il GRUPPO UTENTE al quale deve appartenere l'ospite. Il gruppo influisce sui permessi e gli orari di accesso.
INDIRIZZO EMAIL	Indirizzo email dell'ospite Verrà usato per invio delle e-mail automatiche di benvenuto
NUMERO DI TELEFONO	Numero di telefono dell'ospite
GENERE	Specificare se maschio o femmina
ATTIVO DA SUBITO	Menù a tendina che definisce se l'ospite deve avere, come data e ora di check-in, la data e l'ora in cui viene creato, oppure altra data.
VALIDO DA	Data e ora di inizio validità del badge virtuale associato all'ospite.
VALIDO A	Data e ora di fine validità del badge virtuale
AGGIUNGI BADGE	Sezione dove è possibile associare un badge direttamente all'ospite. Nel menu a tendina vengono visualizzati solo i badge non già associati ad altri utenti; per aggiungere un nuovo badge, avvicinarlo al lettore predefinito e premere SCAN. Nel momento del salvataggio, al badge verranno assegnate tutte le stanze a cui l'utente può accedere.
QR CODE	Sezione dove è possibile visualizzare il QR CODE con cui è possibile accedere alla Stanza/Varco
STANZA	Questo menù a tendina contiene tutte le stanze disponibili (quelle create in backend). E' possibile assegnare una sola stanza a un singolo ospite Se abilitata la sezione Accessi/Rimanenti permette di settare un numero di accessi disponibile per quella Stanza

VARCHI	Uno o più varchi che l'ospite può aprire, in aggiunta a quello della sua stanza Se abilitata la sezione Accessi/Rimanenti permette di settare un numero di accessi disponibile per quel Varco

A fianco dei campi VALIDO DA e VALIDO A sono presenti delle X che permettono di lasciare vuoto il campo VALIDO DA, VALIDO A o tutti e due i campi.

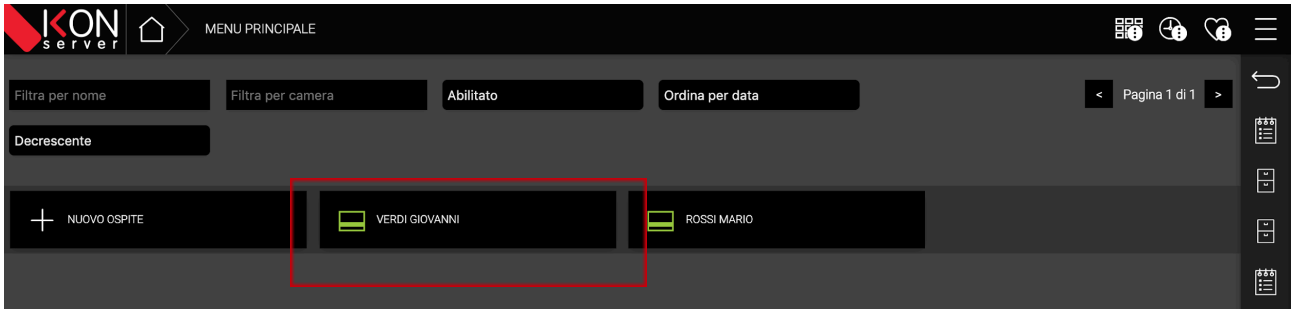
Si consiglia di fare attenzione a questi campi perché se lasciati vuoti, significa che l'utente che si sta andando a creare potrà SEMPRE accedere alle funzioni di stanza che gli spettano.

Alla fine della compilazione premere il pulsante CREA per creare il nuovo utente.

Una volta creato l'utente verranno attivati nuovi pulsanti:

INVIA MAIL	Questo pulsante si attiva solamente se è stata inserita una mail alla creazione dell'ospite; se premuto, invia in automatico la mail di benvenuto, utilizzando il testo pre-impostato, nel quale vengono sostituiti i *tag dinamici* con i dati della struttura e dell'ospite stesso
STAMPA QR	Apre un nuovo tab del browser, con il messaggio di benvenuto in formato adatto alla stampa Questo pulsante verrà visualizzato solo nel caso in cui ci sia abilitato come metodo di accesso App Mobile

Premendo il tasto X (in alto a destra), si torna alla pagina degli ospiti; l'utente appena creato apparirà nella lista.



Il colore dell'icona a sinistra rispetto al nome dell'ospite può essere diverso a seconda del periodo di validità (check-in/check-out) e della data e ora attuali:

VERDE	La data e ora attuale rientrano tra periodo di check-in e check-out di quell'utente; Significa che l'utente è abilitato a utilizzare le funzioni di stanza che gli spettano
ROSSO	La data e ora attuale non rientrano tra periodo di check-in e check-out di quell'utente; Significa che l'utente non è abilitato a utilizzare le funzioni di stanza in questo momento

Per modificare qualsiasi parametro compilato in fase di creazione, o per inviare nuovamente la mail o per stampare il foglio contenente il messaggio di stampa bisogna aprire l'utente su cui si desidera effettuare una di queste azioni in "modifica".

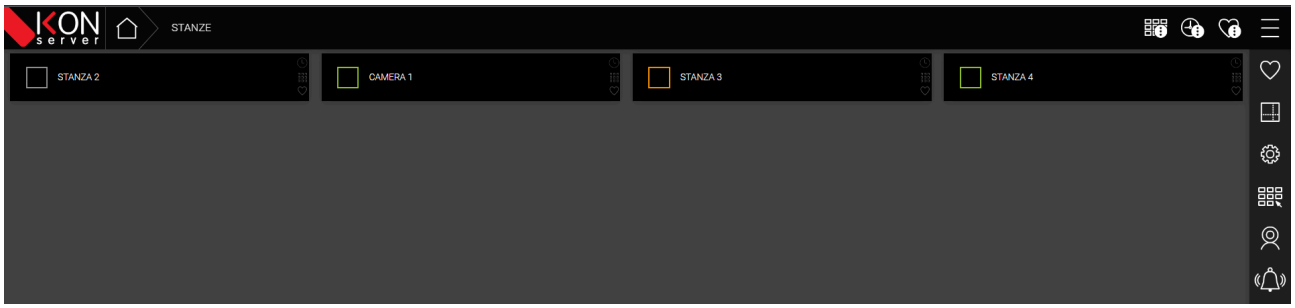
Per fare ciò basta premere sull'oggetto in griglia che corrisponde all'utente che si vuole selezionare; verrà aperto in automatico un popup simile al precedente, questa volta però in modalità "Modifica".

Al termine della modifica premere il bottone SALVA per salvare la configurazione o X (in alto a destra) per annullare le modifiche. In fase di modifica si presentano due nuovi pulsanti:

DISABILITA/ABILITA	Il pulsante disabilita è attivo quando l'utente in quel momento è abilitato; Questo pulsante, se premuto, cambia la data di check.out nella data e ora attuale e svuota la data di check-in in modo che da quel momento in poi l'utente non sarà più abilitato a utilizzare le funzioni di stanza. Viceversa, se l'utente è disabilitato, compare il bottone ABILITA, che modifica la data di check-in nella data e ora attuale e svuota la data di check-out in modo che da quel momento in poi l'utente sarà abilitato a utilizzare le funzioni di stanza. Dopo questa operazione è molto importante ricordarsi di inserire una data di scadenza, altrimenti l'utente sarà abilitato per sempre a utilizzare le funzioni di stanza. La funzione ABILITA oltre a modificare le date di check-in e di check-out assegna anche un nuovo PIN all'utente; Sarà quindi necessario comunicare il nuovo PIN all'utente
ELIMINA OSPITE	Questo pulsante apre una finestra di conferma; Se si conferma l'avviso l'utente viene eliminato

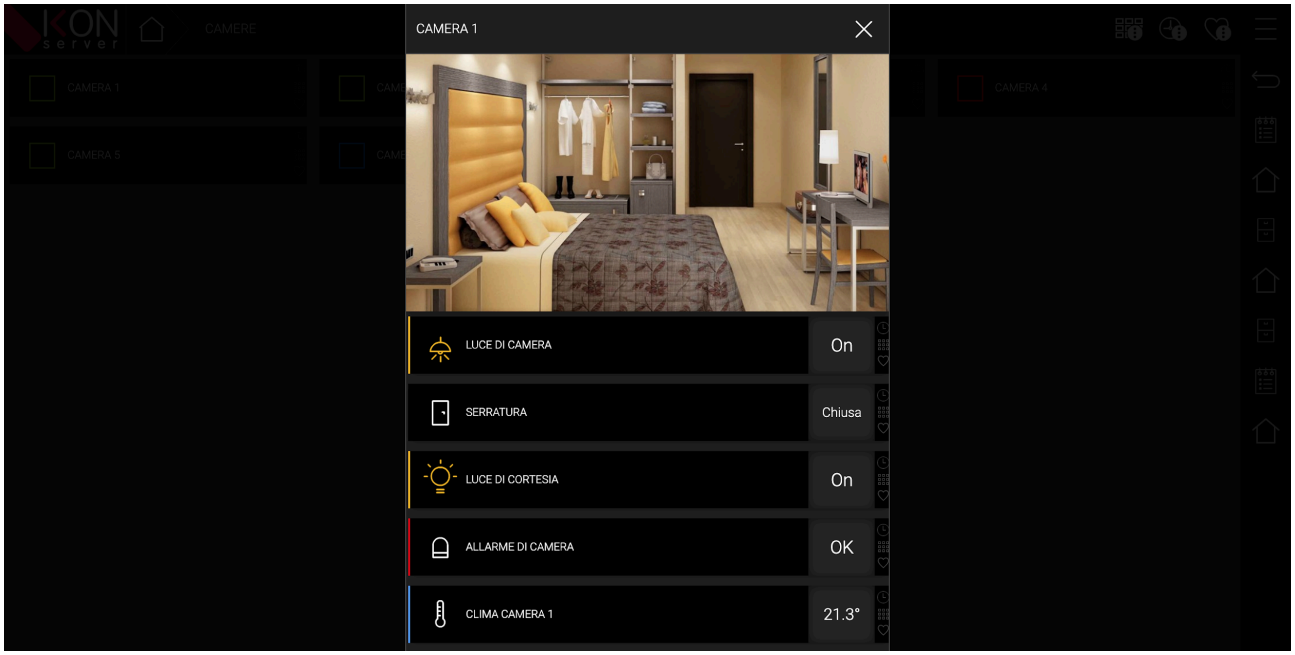
11.6 STANZE

Questa sezione del menu principale, permette al gestore di controllare tutte le stanze dell'edificio, agendo sugli oggetti associati nello stesso modo in cui gli ospiti, se la gestione stanza è abilitata, possono fare dalla app MyWAY, ognuno sulla propria.



La diversa colorazione dipende dallo STATO STANZA di ognuna; rendendo visibile questa *funzione* per le stanze (vedere sezione di configurazione delle stanze in precedenza) il gestore può modificarlo direttamente da questa sezione del FRONTEND, per identificare più facilmente in quale condizione si trovino le stanze.

Premendo su una stanza, verrà visualizzato il popup contenente gli oggetti associati:



Nota: alcuni oggetti, anche se resi visibili, non risultano gestibili per gli ospiti dalla app MyWAY, come ad esempio la serratura. Questo consente al gestore di poter aprire comodamente le porte delle stanze dalla app, mentre gli ospiti devono utilizzare la gestione della serratura prevista dalla app MyWAY, come illustrato in seguito.

11.7 PERSONALE

Questa sezione permette di creare e gestire uno o più utenti che rappresentano personale (tecnico, di servizio, di manutenzione etc...) che utilizzerà la app MyWAY per accedere alla struttura ed ai suoi ambienti protetti dal controllo accessi.

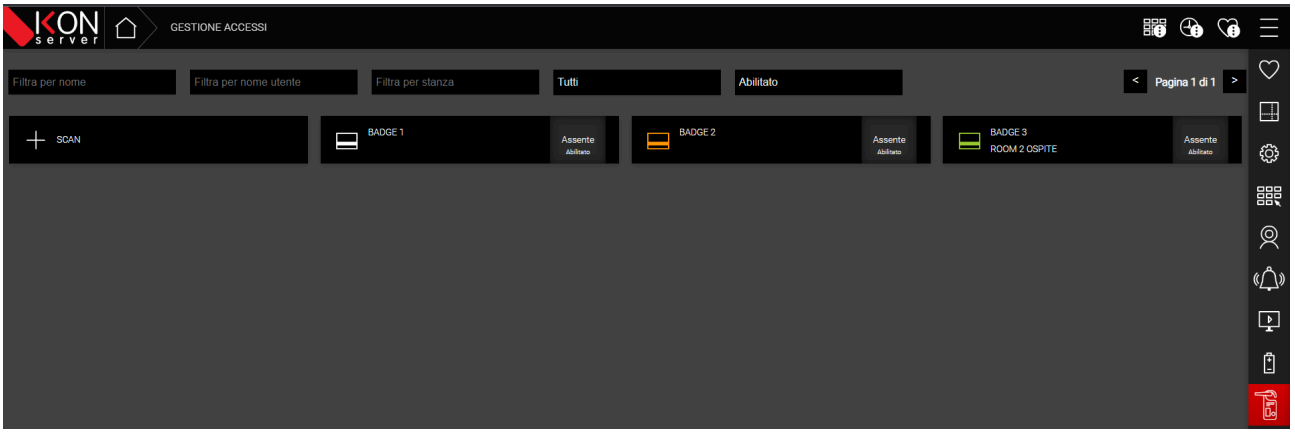
La gestione è del tutto analoga a quella degli ospiti, con la differenza che per il personale di servizio è possibile associare più di una stanza contemporaneamente, in modo da abilitarlo all'ingresso in tutti gli ambienti.

11.8 BADGE

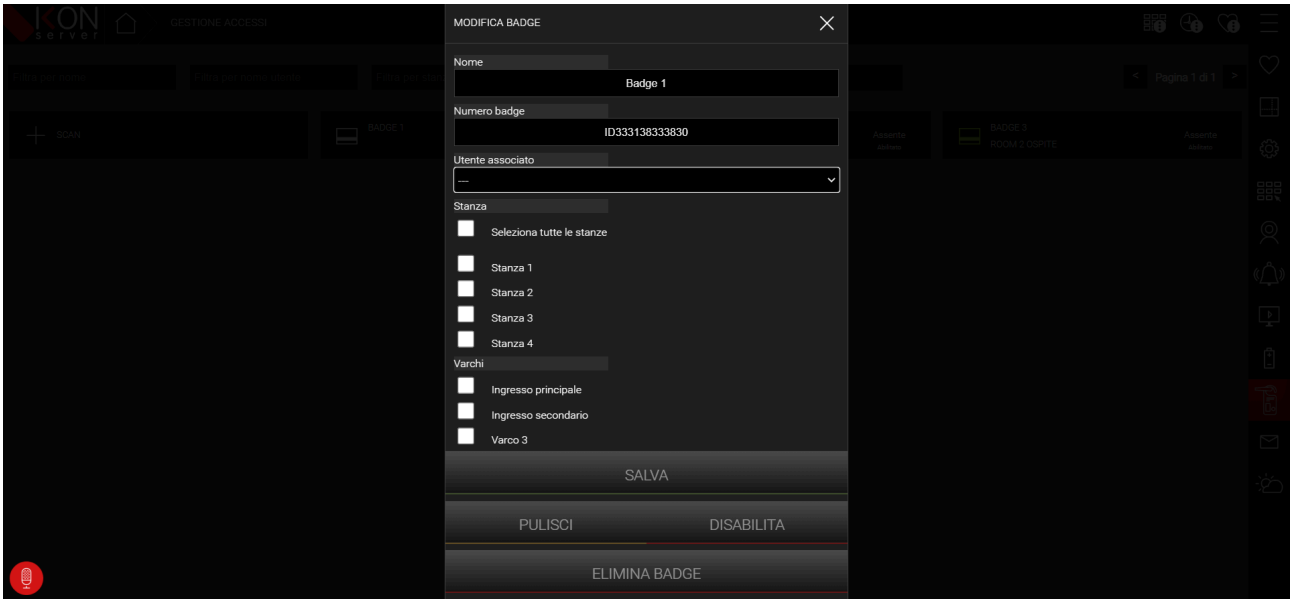
Questa sezione del menù principale, permette al gestore di controllare i badge, agendo sugli utenti e stanze/varchi associati.

Il colore dell'icona a sinistra rispetto al nome del badge può essere diverso a seconda dello stato

BIANCO	Il badge non è associato a utenti o stanze
VERDE	Il badge è associato ad un utente e una stanza
ARANCIONE	Il badge è associato a stanze senza utente
ROSSO	Il badge è disabilitato



Premendo su un singolo badge, viene aperto il popup di gestione, che si presenta come nell'esempio seguente:



In particolare, è possibile impostare quanto segue:

NOME	Etichetta abbinata al badge, per una sua più facile identificazione
NUMERO	Campo non modificabile, memorizzato all'interno del badge fisico
UTENTE ASSOCIATO	Se non già associato (nella scheda di un utente) è possibile attribuire il badge ad un ospite o al personale di servizio
STANZE VARCHI	Selezione multipla dei varchi e delle stanze che il badge può aprire

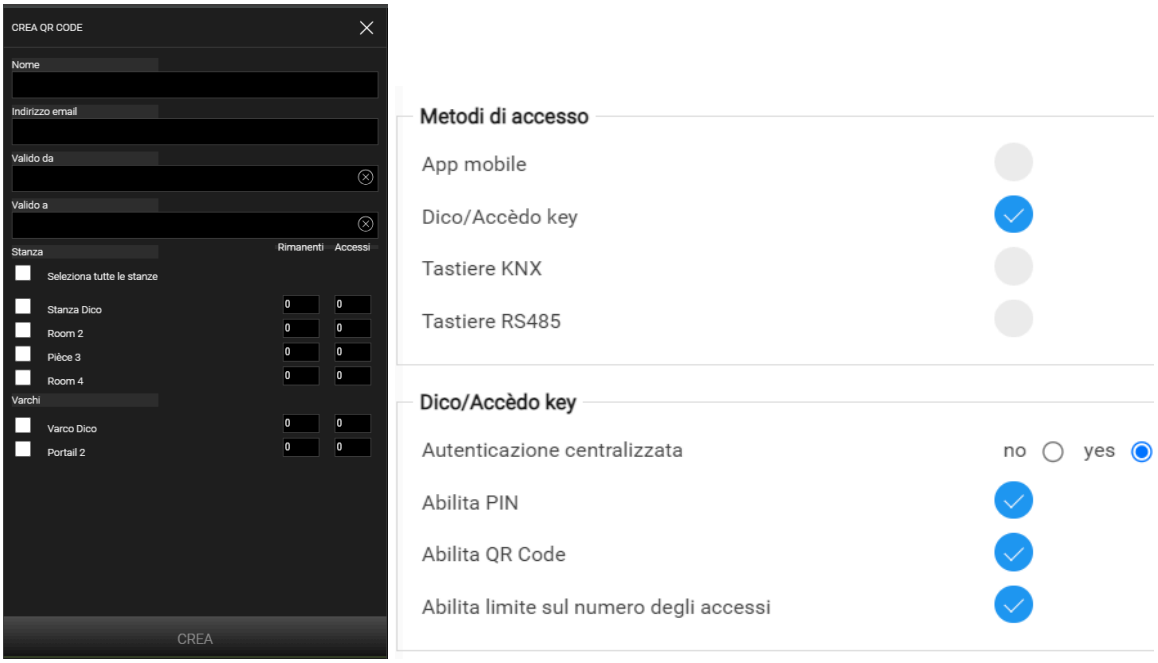
I seguenti pulsanti sono inoltre disponibili:

PULISCI	Elimina tutte le informazioni relative ad un badge, e permette di utilizzarlo nuovamente per un nuovo utente
DISABILITA	Inibisce temporaneamente l'accesso con il badge in questione
ELIMINA BADGE	Elimina definitivamente il badge dal sistema. Per aggiungerlo nuovamente, è necessaria una nuova SCAN.

11.9 QR CODE

Questa sezione del menù principale permette di creare dei QR Code temporanei con accessi limitati nel tempo o per numero di utilizzi ed è visibile solo se nelle Impostazioni Generali:

- è abilitato il flag DICO/ACCEDO KEY in "Metodi di accesso"
- se "Autenticazione Centralizzata" è abilitato nella sezione "DICO/ACCEDO KEY"
- se abilitato il flag "Abilita QR Code" nella sezione "DICO/ACCEDO KEY"



12 ACCESSO DA APP

12.1 PREMESSA

Come già anticipato, gli ospiti (o il personale di servizio) utilizzano una app dedicata per l'accesso alla struttura, denominata MyWAY e scaricabile negli store Android e IOS:

Android

https://play.google.com/store/apps/details?id=com.domoticalabs.pass

Apple IOS

https://apps.apple.com/it/app/myway/id1456347781

12.2 E-MAIL DI BENVENUTO

Come illustrato nel capitolo precedente, quando il gestore inserisce l'anagrafica di un ospite nel sistema, IKON SERVER può inviare automaticamente una e-mail di benvenuto, che contenga tutte le istruzioni per accedere alla struttura.

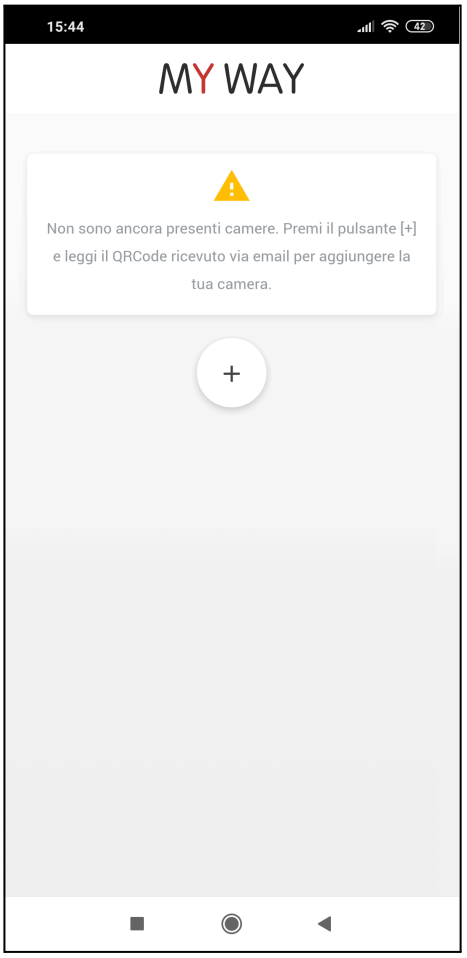
Nella e-mail di benvenuto, in base al testo pre-impostato in precedenza, sono tipicamente contenute le istruzioni per:

- Scaricare la app MyWAY
- Accedere alla app ed importare il badge virtuale
- Accedere alla rete WIFI della struttura
- Altre informazioni di carattere generale, come contatti, riferimenti, indirizzo etc…
- Accedere alla stanza/varco tramite QR Code

12.3 INSTALLAZIONE E PRIMO ACCESSO ALLA APP

Una volta installata l'APP, alla prima apertura di essa verrà richiesto di proteggere o meno l'accesso, in base alla propria impostazione di sicurezza di sblocco del dispositivo (sequenza, impronta digitale o riconoscimento facciale) se presente. Se si abilita questa modalità, anche in caso di smarrimento o furto del telefono, non sarà possibile accedere alla app, e quindi aprire i varchi, da parte di terzi.

La schermata di benvenuto della app si presenta in questo modo:



12.4 IMPORTAZIONE DI UN BADGE VIRTUALE

Inizialmente, la app non ha nessun badge virtuale; all'ospite viene fornito un badge virtuale, per ogni prenotazione, nei seguenti modi:

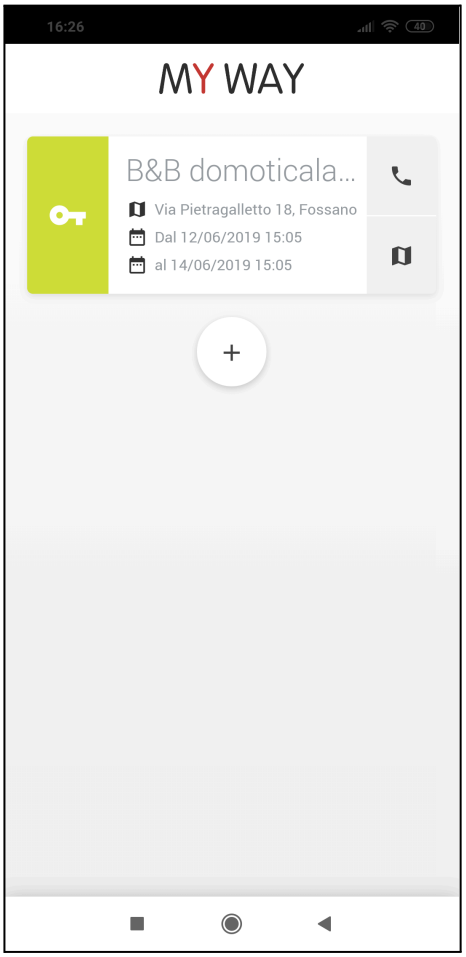
- Sotto forma di link presente all'interno del testo del messaggio email
- All'interno della e-mail di benvenuto, sotto forma di codice QR
- Come allegato alla e-mail di benvenuto stessa
- Sotto forma di codice QR, in caso di foglio stampato in reception

Se non si può accedere direttamente alla e-mail di benvenuto dal telefono, è necessario, dall'interno della app MyWAY:

- Premere il pulsante +
- Inquadrare il codice QR personale, contenuto nella email (inquadrando, ad esempio, il monitor del PC oppure una stampa della mail stessa)

Se invece si ha accesso alla mail direttamente dal telefono, è sufficiente premere sul pulsante APRI BADGE all'interno del testo. In alternativa, aprire il file allegato; il telefono chiede (in base alle impostazioni di sistema) con quale app si desidera aprirlo, a quel punto è necessario selezionare MyWAY.

In entrambe le modalità, si ottiene un nuovo badge virtuale nella lista principale, che riporta i dati di sintesi della struttura, e le date di validità dello stesso:



Il colore verde sta a indicare che è già possibile accedere all'applicazione e effettuare le operazioni relative alla stanza assegnata (lettura QR e comando oggetti).

Altri colori del badge possono essere:

- rosso: se l'utente non è autorizzato ad interagire con la stanza in quel momento;
- arancione: se l'utente sta per essere attivato, oppure se non è nel raggio di azione della geolocalizzazione.

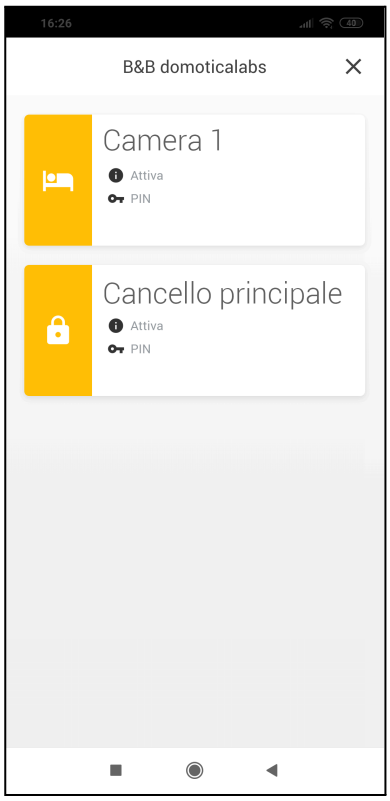
Se la struttura fornisce indirizzo e numero di telefono, essi risultano disponibili come scorciatoie, rispettivamente, per la app telefono e per il navigatore satellitare.

12.5 GEOLOCALIZZAZIONE

Se in configurazione sono state specificate le coordinate geografiche della struttura e scelto un raggio di azione, l'app controlla che il visitatore si trovi all'interno di quell'area.

Solo in questo caso, viene consentito l'accesso alla struttura con badge verde; in caso contrario, il badge risulta arancione (con dicitura “fuori zona”) e non è consentito il suo utilizzo. Questo controllo evita l'utilizzo inappropriato della app, quando non si è in struttura.

12.6 ACCESSO ALLA STRUTTURA



Se il badge è attivo, è possibile accedere alla struttura; premendo il badge virtuale, viene effettuata una chiamata di autenticazione ad IKON SERVER (in base alle impostazioni del telefono, tramite internet oppure localmente in WIFI, se ovviamente si è già fatto accesso alla rete senza fili della struttura).

In caso di successo, la app abilita la schermata successiva, nella quale viene proposto l'elenco dei varchi che è possibile aprire.

Se la struttura prevede un solo varco da aprire, questo passaggio viene omesso, e si passa immediatamente alla schermata successiva.

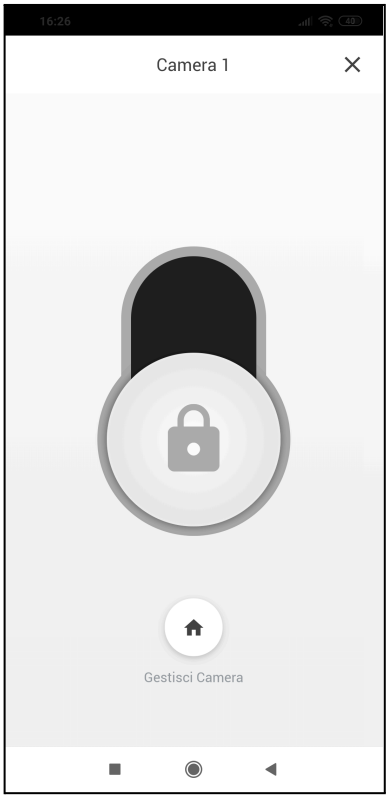
Se il varco (o la stanza) è di colore giallo, significa che è protetto da PIN, e sarà quindi necessario inserire il codice numerico ricevuto nella e-mail di benvenuto, per poterlo aprire.

Viceversa, se il varco è verde, è possibile aprirlo senza ulteriori passaggi di validazione.

Una volta selezionato il varco, l'app presenta una videata, nella quale è presente un widget che rappresenta la serratura, al centro della schermata. In alto è indicato il nome del varco che si sta per aprire.

Se il varco non è protetto da PIN, la serratura scatta immediatamente; viceversa, viene chiesto di inserire il codice personale di identificazione, ricevuto via e-mail (oppure nella stampa di benvenuto ricevuta in reception).

Se si è selezionata la propria stanza, e la struttura ha abilitato la gestione domotica, il corrispondente pulsante risulta disponibile in basso; premendolo, viene caricata la grafica di gestione della stanza, in modo del tutto analogo a quanto visto in precedenza.



NEW 2.9.7

13 CONTROLLO ACCESSI v2.9.7

I capitoli a partire da questa sezione sono applicabili solo ed esclusivamente a IKON Server con versione 2.9.7 e con HW nuovo.

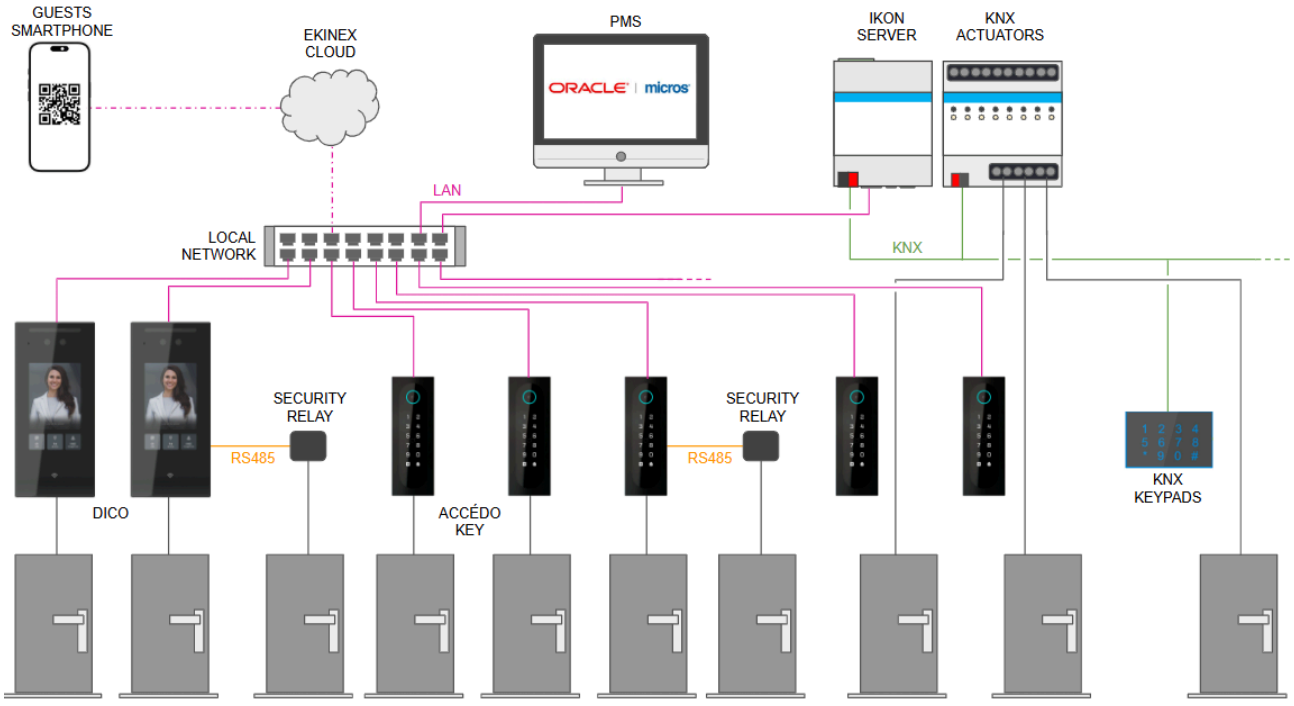
13.1 INTRODUZIONE

IKON SERVER può essere usato come gestore del CONTROLLO ACCESSI in abbinamento agli altri prodotti del catalogo EKINEX, con il modulo software integrato denominato ACCÉDO:

- DICO (posto esterno videocitofonico)
- ACCÉDO KEY (tastierino numerico)

13.2 ARCHITETTURA

IKON SERVER consente all'utente di configurare e gestire separatamente stanze e varchi. Una *stanza* è uno spazio “di proprietà” esclusiva di un ospite per un determinato periodo di tempo, mentre un *varco* è un punto di accesso all'edificio o ad un'area comune, ad esempio piscina, SPA, magazzino.



La serratura di una porta sotto il controllo di IKON SERVER può essere aperta in uno dei seguenti modi:

- Tramite il RELE' integrato nel DICO o nell’ ACCÉDO KEY.
- Tramite il RELE' DI SICUREZZA collegato tramite RS485 ad un DICO o ad un ACCÉDO KEY.
- Tramite un attuatore KNX

13.3 CONFIGURAZIONE

Affinché il modulo ACCÉDO funzioni correttamente è necessaria una procedura di CONFIGURAZIONE da parte dell'installatore/integratore del sistema, nello spazio di amministrazione del webserver.

La configurazione normalmente richiede l'esecuzione dei seguenti passaggi:

- Impostazioni generali:
  - Informazioni sulla struttura e preferenze.
  - Metodi e opzioni di accesso.
- Impostazioni dell'e-mail di benvenuto.
- Creazione e configurazione delle stanze e dei varchi.
- Impostazioni di DICO e ACCÉDO KEY:
  - Configurazione dei dispositivi.
  - Associazione con le stanze e/o varchi.

È possibile configurare i seguenti aspetti opzionali, in base alle esigenze specifiche di ciascuna installazione:

- Configurazione gruppi utenti e fasce orarie.
- Configurazione della presenza virtuale.
- Configurazione dell'integrazione PMS.

I capitoli successivi del presente manuale trattano tutti questi aspetti in dettaglio. La parte finale di questo documento è dedicata all'utilizzo del sistema di controllo accessi, una volta opportunamente configurato.

13.4 LICENZE

Il modulo ACCÉDO prevede un modello di licenza specifico, in base al numero di stanze e/o varchi da utilizzare. Un numero base di stanze e varchi è disponibile gratuitamente nel webserver; per incrementarlo è necessario:

- Acquistare uno o più VOUCHER.
- Accedere alla seguente sezione dello spazio amministrativo di IKON SERVER:

  CONTROLLO ACCESSI > IMPOSTAZIONI > RISCATTA VOUCHER

- Copia e incolla il codice del voucher nella prima casella di testo della pagina.
- Per riscattare più voucher contemporaneamente, premere il pulsante AGGIUNGI VOUCHER tante volte quanto necessario.
- Premere il pulsante SALVA e attendere il completamento della procedura.



IKON SERVER deve essere connesso a Internet per poter riscattare i voucher di controllo degli accessi. Si prega di contattare il supporto tecnico in caso di applicazioni offline.

Anche l'integrazione con PMS di terze parti è soggetta a licenza. In tal caso, procedere nel seguente modo:

- Acquistare il VOUCHER DI LICENZA per l'integrazione PMS
- Accedere al PORTALE VOUCHER al seguente indirizzo

  `https://www.domoticalabs.com/voucher`

  e riscattare il voucher creando una licenza per il numero di serie del IKON SERVER

- Inserire la licenza nella pagina SETUP > GESTIONE MODULI E LICENZE.

Per ulteriori informazioni sulle licenze e sui voucher di IKON SERVER, fare riferimento al proprio rappresentante commerciale in EKINEX.

14 IMPOSTAZIONI

14.1 IMPOSTAZIONI GENERALI

Accedendo alla sezione

CONTROLLO ACCESSI > IMPOSTAZIONI > IMPOSTAZIONI GENERALI

nello spazio di amministrazione è possibile impostare le seguenti informazioni generali.

14.1.1 INFORMAZIONI STRUTTURA

NOME STRUTTURA	Il nome dell'edificio/struttura ricettiva. Viene utilizzato nei messaggi email automatici inviati all'ospite.
INDIRIZZO	Indirizzo della struttura. Utilizzato nell'e-mail di benvenuto.
NUMERO DI TELEFONO	Numero di telefono della struttura. Utilizzato nell'e-mail di benvenuto.
E-MAIL DI CONTATTO	E-mail della struttura. Utilizzato nell'e-mail di benvenuto.
SITO WEB	URL della struttura. Utilizzato nell'e-mail di benvenuto.
NOME RETE WIFI	Informazioni sulla rete WIFI utilizzabile dagli ospiti per accedere ad internet. Queste informazioni possono essere aggiunte nell'e-mail di benvenuto.
PASSWORD RETE WIFI	La password per accedere al WIFI. Queste informazioni possono essere aggiunte nell'e-mail di benvenuto con il NOME RETE WIFI.
ORARIO DI CHECK-IN PREDEFINITO ORARIO DI CHECK-OUT PREDEFINITO	Orario predefinito per l'inizio e la fine della validità. Può essere modificato durante la creazione di un ospite.
DURATA IMPULSO ELETTRICO SULLA SERRATURA (IN SECONDI)	Durata dell'impulso da dare alle elettroserrature per l'apertura delle porte

EVITA PRENOTAZIONI MULTIPLE SULLA STESSA STANZA	Se abilitato, prima di concedere l'accesso ad una stanza ad un nuovo ospite, viene effettuato un controllo per un'altra prenotazione nella stessa stanza e le date di check-in e check-out.

14.1.2 METODI DI ACCESSO

Le seguenti opzioni determinano le modalità con cui gli ospiti o il personale di servizio possono accedere alla struttura:

DICO / ACCÉDO KEY	Abilita la gestione dei dispositivi di controllo accessi EKINEX
TASTIERE KNX	Abilitata la gestione dei tastierini numerici KNX di terze parti

14.1.3 DICO / Accédo KEY

Quando è abilitata la modalità di accesso con prodotti EKINEX è possibile impostare le seguenti opzioni per l'autenticazione tramite i dispositivi EKINEX installati:

ABILITA PIN	Abilita l'autenticazione degli ospiti tramite un PIN personale, generato automaticamente e inviato nella email di benvenuto.
ABILITA QR CODE	Abilita l'autenticazione degli ospiti con un QR CODE personale, inviato automaticamente insieme alla email di benvenuto.
ABILITA GESTIONE BADGE	Abilita l'accesso alle stanze e ai varchi tramite Tessera RFID
ABILITA LIMITE SUL NUMERO DEGLI ACCESSI	Se questa opzione viene abilitata, è possibile attivare, per ognuna delle precedenti modalità di autenticazione, una limitazione del numero di accessi per ciascun ospite, durante la sua permanenza nella struttura.

14.1.4 TASTIERE KNX

Le seguenti opzioni, specifiche per le tastiere KNX, sono disponibili se è abilitata la modalità di accesso corrispondente:

GRANULARITÀ FASCE ORARIE	Normalmente gli orari possono essere definiti con orari di inizio/fine espressi in minuti. Alcuni dispositivi KNX di terze parti supportano solo gli orari di inizio/fine in ore; in tal caso è necessario modificare questa impostazione, per far funzionare correttamente le tastiere KNX in abbinamento a IKON SERVER.

14.2 E-MAIL DI BENVENUTO

14.2.1 E-MAIL DI BENVENUTO DI DEFAULT

Entrando in questa sezione è possibile personalizzare il messaggio predefinito inviato via email a nuovi ospiti o personale di servizio, per fornire loro informazioni sulla struttura, modalità di accesso e il proprio PIN/QR CODE.

Il messaggio predefinito riflette la lingua del webserver; quando l'impostazione della lingua viene modificata, la mail viene tradotta nella nuova lingua. Per gestire messaggi diversi per ospiti che parlano lingue diverse, fare riferimento al paragrafo successivo.

La pagina contiene i seguenti pulsanti:

SALVA	Salva l'oggetto e il corpo del nuovo modello
CHIUDI	Chiude l'editor senza salvare il modello
OPZIONI EMAIL	Dà accesso alle opzioni di invio della posta elettronica. Per ulteriori dettagli sulle modalità di invio delle email si rimanda al manuale [D2]
HELP	Un aiuto contestuale contenente l'elenco dei tag dinamici (vedi sotto)

14.2.2 TAG DINAMICI

Sia l'oggetto che il corpo della mail possono contenere dei *tag dinamici* che vengono automaticamente sostituiti con le corrispondenti informazioni sulla struttura e sull'ospite:

INFORMAZIONI UTENTE (OSPITE).

{{user.name}}	Il nome utente completo dell'ospite
{{user.options.firstname}}	Il nome dell'ospite
{{user.options.lastname}}	Il cognome dell'ospite
{{user.options.valid_from}}	Il giorno di inizio del periodo di validità per l'ospite nella struttura
{{user.options.valid_to}}	Il giorno di fine del periodo di validità per l'ospite nella struttura
{{user.rooms}}	L'elenco delle camere assegnate all'ospite. In caso di più stanze (solo per personale di servizio), queste vengono separate con una virgola.
{{user.gates}}	L'elenco dei varchi che l'ospite può aprire. In caso di più porte queste vengono separate con una virgola.

INFORMAZIONI SULLA STRUTTURA

{{info.name}}	Il nome della struttura
{{info.location}}	L'indirizzo della struttura
{{info.phone}}	Il numero di telefono della struttura
{{info.www}}	L'URL del sito web della struttura
{{info.wifi_ssid}}	Il nome della rete Wi-Fi
{{info.wifi_pwd}}	La password della rete Wi-Fi

INFORMAZIONI DI ACCESSO

{{pin}}	Il PIN personale da digitare sulle tastiere
{{qr_code}}	L'immagine del QR CODE da presentare davanti ai dispositivi DICO e ACCÉDO KEY

14.2.3 EMAIL AGGIUNTIVE

Selezionando la voce di menu

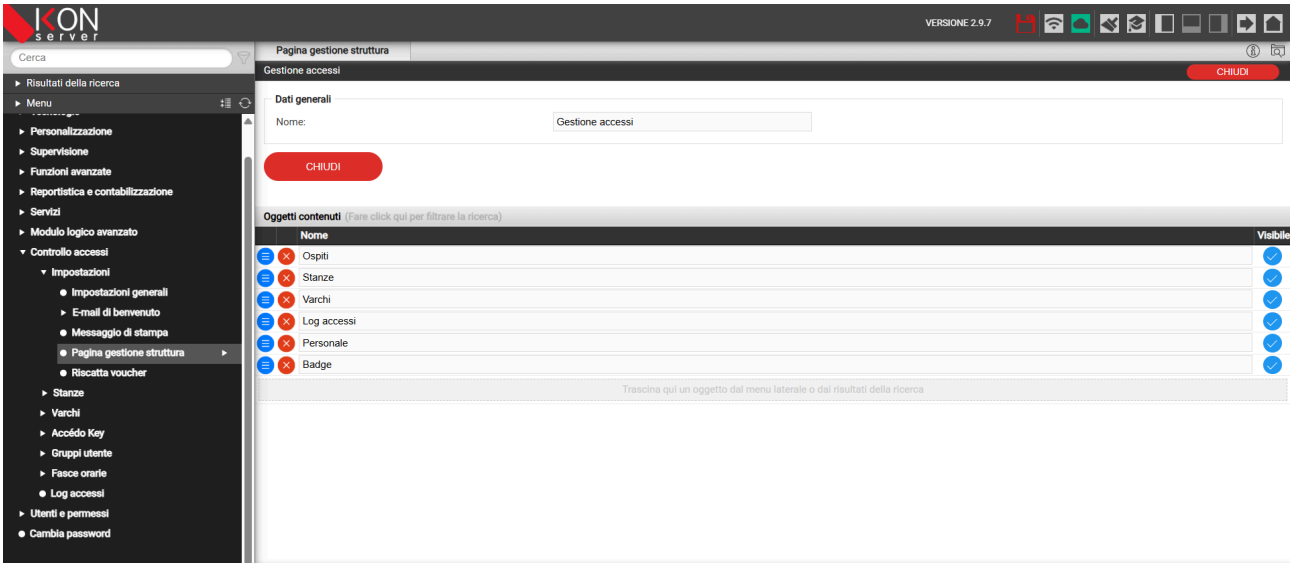
CONTROLLO ACCESSI > E-MAIL DI BENVENUTO

E premendo il pulsante [+] nella barra degli strumenti è possibile aggiungere altri template di email; ognuno di essi può essere personalizzato nella maniera già vista per quello di default.

In questo modo è possibile creare più template per diverse lingue, o per diverse categorie di ospiti.

14.3 PAGINA GESTIONE STRUTTURA

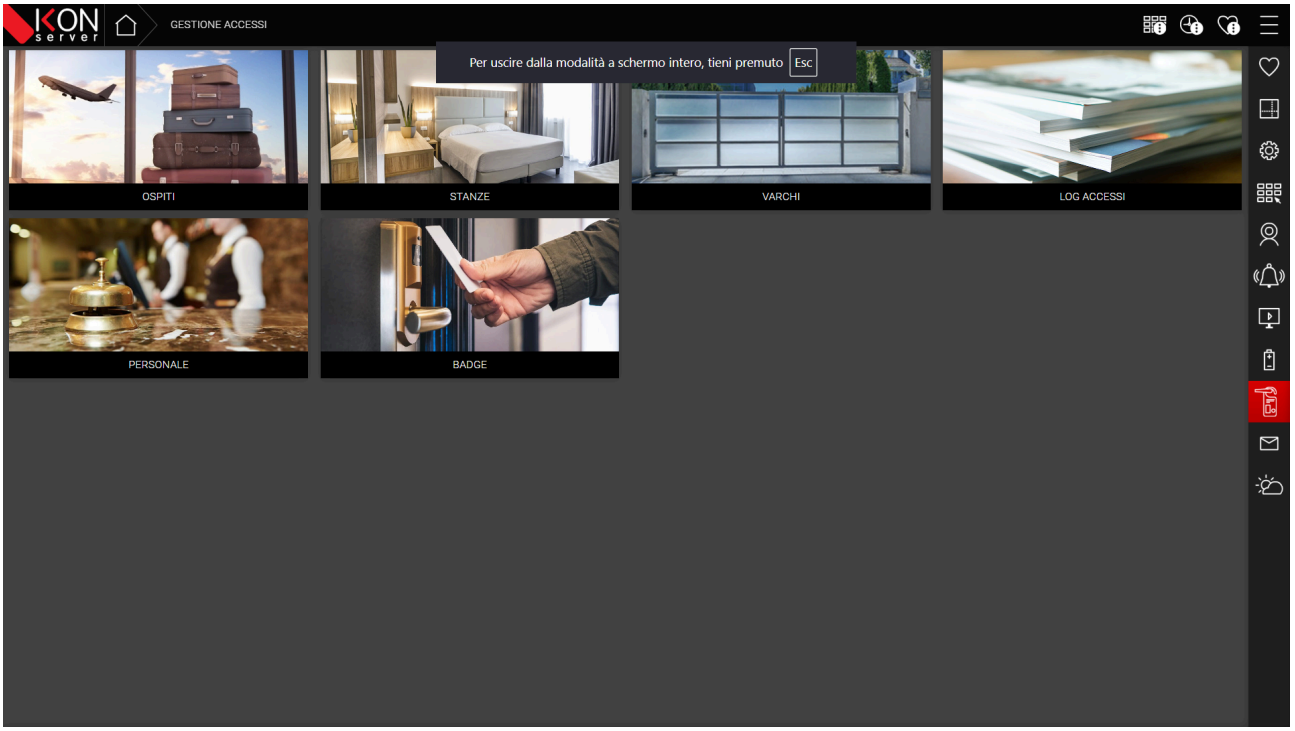
Questa pagina contiene l'elenco degli elementi visibili nel file visualizzazione, quando si accede alla voce CONTROLLO ACCESSI del menù di navigazione:



Questa pagina offre la possibilità di:

- Cambiare il nome del menu di navigazione, modificando l'etichetta NOME predefinita all'inizio della pagina.
- Cambiare l'etichetta per ciascuno degli elementi nella pagina.
- Nascondere uno o più elementi, se non idonei alle specifiche esigenze della struttura (selezionando il corrispondente checkbox nella colonna VISIBILE).

Il risultato corrispondente nella visualizzazione è simile alla seguente immagine:



14.4 RISCATTA VOUCHER

Come accennato precedentemente, questa pagina permette di ampliare il numero di stanze e di varchi, inserendo uno o più voucher di licenza.

15 STANZE E VARCHI

15.1 INTRODUZIONE

Nella terminologia di ACCÉDO, per STANZA si intende uno spazio protetto da una o più porte sotto il controllo del modulo di controllo accessi di un IKON SERVER. Normalmente una stanza è occupata da un ospite alla volta.

Un varco è una porta sotto il controllo del webserver, che garantisce l'accesso all'edificio stesso (dall'esterno) o ad un'area comune interna (ad esempio una SPA).

Normalmente un OSPITE è associato ad una sola STANZA alla volta, ma può avere diritto ad aprire più di un varco.

15.2 STANZE

15.2.1 CREAZIONE DI UNA NUOVA STANZA

Selezionando la voce di menu

CONTROLLO ACCESSI > STANZE

E premendo il pulsante [+] viene creata una nuova STANZA.

Entrando nella sua pagina di dettaglio è possibile impostare le seguenti informazioni generali; alcune delle seguenti informazioni richiedono la modalità ESPERTO ( ) per essere visualizzate.

INFORMAZIONI GENERALI

NOME	Etichetta identificativa della STANZA. Lasciare questo campo nel suo stato di default, in modo da riflettere il NUMERO fornito; per assegnare un nome diverso modificare **prima** il NUMERO e quindi assegnare un'etichetta.
NUMERO	Identificativo numerico della STANZA. Quando si modifica il NUMERO, il NOME viene automaticamente adattato per riflettere il nuovo numero,
ABILITATO	Se questa casella non è selezionata, la STANZA non viene mostrata nella lista delle opzioni per l'assegnazione agli ospiti e non è possibile l'accesso.
LIMITE DI ACCESSI DEFAULT	Visibile solo se nelle Impostazioni Generali è abilitato il flag ABILITA LIMITE SUL NUMERO DI ACCESSI. Consente all'utente di inserire un numero limite di accesso predefinito alla stanza quando crea un nuovo Ospite o Personale di servizio.

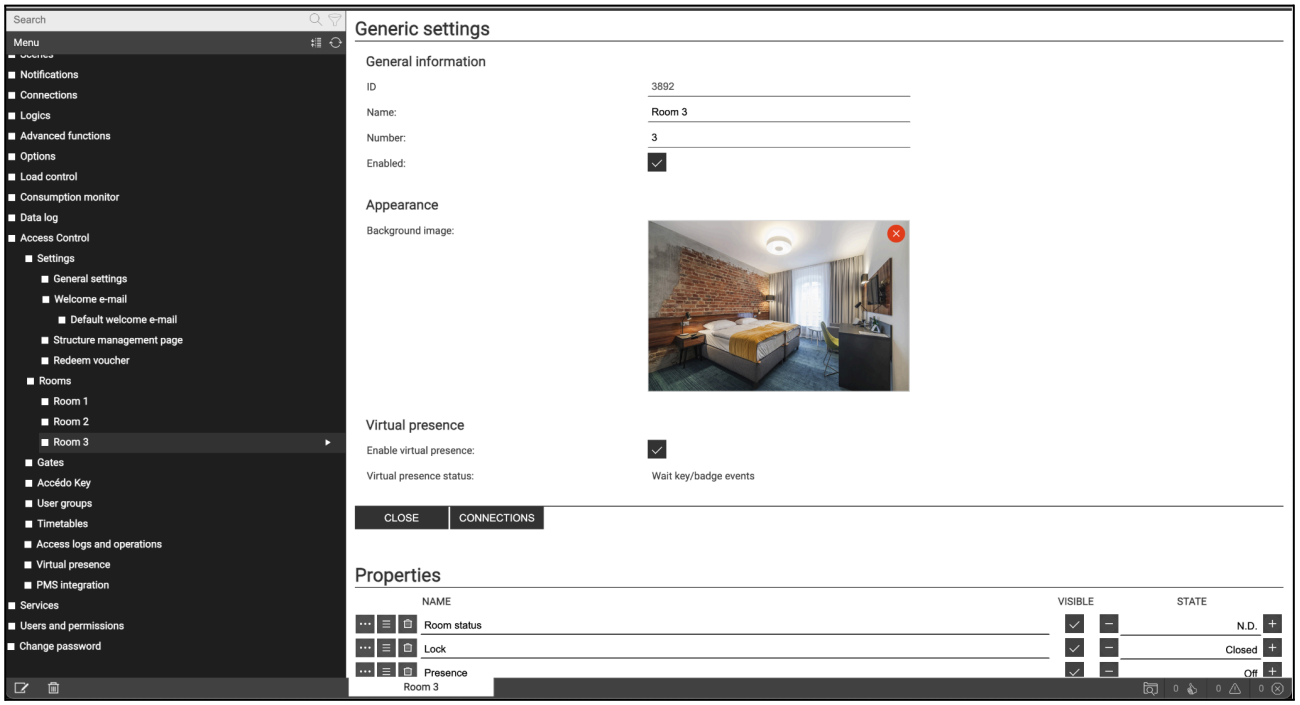
ASPETTO

IMMAGINE DI SFONDO	Carica e assegna un'immagine personalizzata alla STANZA, da visualizzare nella visualizzazione, all'apertura del popup della stanza.

PRESENZA VIRTUALE

Se l'algoritmo della presenza virtuale è attivo, per ogni STANZA è possibile visualizzare le seguenti opzioni/info:

ABILITA PRESENZA VIRTUALE	Quando abilitato, viene calcolata la presenza virtuale per la STANZA corrente, per determinare se nella stanza è presente almeno un ospite.
STATO PRESENZA VIRTUALE	Lo stato dell'algoritmo per la determinazione della presenza in stanza



15.2.2 PROPRIETÀ DELLA STANZA

Abilitando la modalità ESPERTO ( ) viene visualizzato l'elenco di tutte le PROPRIETA' disponibili per la STANZA. Questi elementi sono attributi dinamici della STANZA, che possono essere impostati manualmente (qui o nella visualizzazione) o relazionati ad altri oggetti, tramite CONNESSIONI o TRIGGERS). Le proprietà di una stanza possono essere nascoste nella visualizzazione selezionando la casella di controllo VISIBILE corrispondente.

Una stanza ha le seguenti proprietà:

STATO STANZA	Lo stato attuale della STANZA, che cambia in base alle operazioni effettuate da un ospite. Vedere la tabella seguente per tutti i possibili valori dello STATO STANZA. È possibile attivare un'azione su altri oggetti (es. SCENE, WIDGETS KNX o OGGETTI ecc…) quando cambia lo stato.
SERRATURA	Questa proprietà verrà impostata automaticamente su APERTA quando gli ospiti o il personale di servizio utilizzano un PIN, un CODICE QR o una carta RFID valida per aprire la porta. La proprietà mantiene il valore di Open per il tempo di impulso impostato nel settaggio generale. Una *relazione* con l'oggetto che rappresenta il comando della serratura occorre stabilire, affinché la porta possa effettivamente aprirsi.
PRESENZA	L'effettiva presenza di almeno un ospite all'interno della STANZA. Questa informazione può essere fornita da sensori fisici (ad es *Porta carte RFID*) o calcolato dall'algoritmo VIRTUAL PRESENCE.

	In una qualsiasi delle due situazioni, questa proprietà può essere associata a a *relazione* ad un oggetto da comandare quando qualcuno è nella STANZA, es. il relè carichi della stanza, l'aria condizionata, una luce ecc…
NON DISTURBARE	Attivo quando gli ospiti chiedono di non essere disturbati dal personale durante il soggiorno, anche per la pulizia della stanza.
ALLARME	Attivo quando scatta un allarme (e.g., fuoco e fumi, allarme doccia).
PULIZIA STANZA	Attivo quando gli ospiti richiedono una pulizia aggiuntiva della STANZA
SENSORE PORTA SENSORE MOVIMENTO SENSORE MOVIMENTO 2	Ingressi richiesti dall'algoritmo VIRTUAL PRESENCE, Queste proprietà non sono visibili nella visualizzazione.

Lo STATO STANZA può assumere uno dei seguenti valori:

STATO STANZA	DESCRIZIONE	NUMERO
LIBERA	Disponibile per la prenotazione ad un ospite	1
PRENOTATA	Prenotato per un ospite che non è ancora entrato nella struttura (prima dell'inizio del periodo di validità)	2
ASSEGNATA	Concesso in uso esclusivo ad un ospite, che al momento non si trova all'interno della stanza (ma si trova nella struttura, o comunque nel periodo di validità del suo soggiorno)	3
OCCUPATA	L'ospite è all'interno della stanza	4
SERVICE	In fase di pulizia o manutenzione	5
ND	Nessuno degli stati precedenti	0



Le informazioni generali e le PROPRIETA' della stanza vengono scritte nella lingua corrente del webserver. Se si cambia la lingua del webserver. queste voci non verranno tradotte.

15.2.3 ALTRE INFORMAZIONI

La pagina di dettaglio di una STANZA può contenere anche le seguenti informazioni, a seconda delle impostazioni generali (e in particolare, delle modalità di accesso abilitate alla struttura):

- Fasce orarie
- Ospiti
- Dico
- Accédo Keys
- Tastiere KNX - programmazione (10 byte)
- Tastiere KNX - consenso (4 byte)

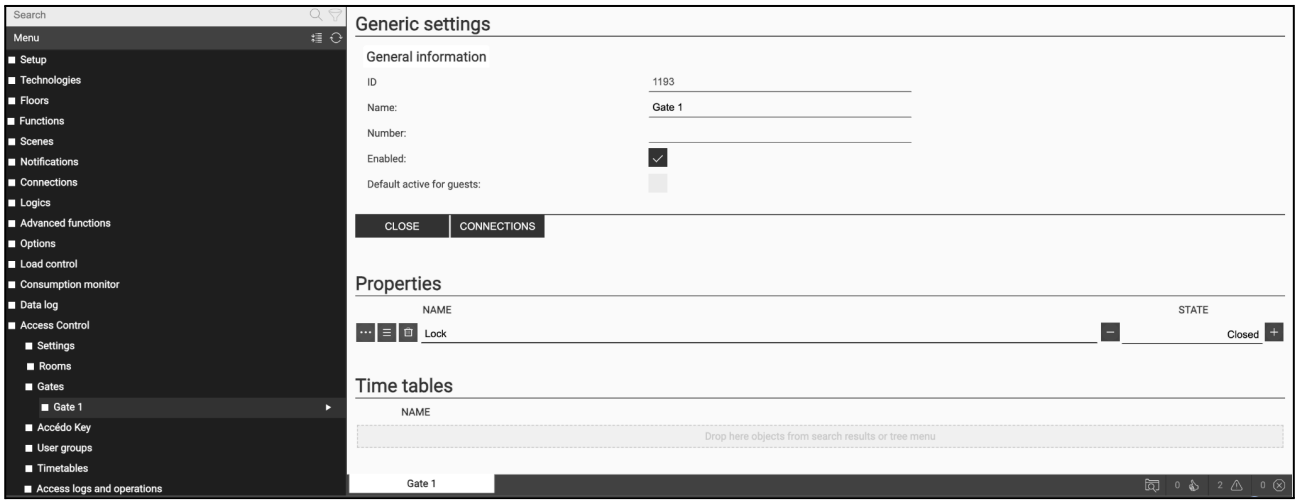
Fare riferimento ai capitoli successivi per la spiegazione degli argomenti corrispondenti e la loro configurazione.

15.3 VARCHI

I VARCHI sono simili alle STANZE, ma l'unica proprietà che ha un varco è la SERRATURA.

Nelle IMPOSTAZIONI GENERALI sono disponibili i seguenti attributi:

NOME	Etichetta identificativa del VARCO
NUMERO	Rappresentazione numerica del VARCO
ABILITATO	Se questa casella non è selezionata, il VARCO non viene presentato nella lista delle opzioni per l'assegnazione agli ospiti e non è possibile l'accesso.
ATTIVO DI BASE PER GLI OSPITI	Se questa casella è selezionata, il VARCO verrà selezionato per impostazione predefinita nella visualizzazione, quando verrà creato un nuovo ospite
LIMITE DI ACCESSI DEFAULT	Visibile solo se nelle Impostazioni Generali è abilitato il flag ABILITA LIMITE SUL NUMERO DI ACCESSI. Consente all'utente di inserire un numero limite di accesso predefinito alla stanza quando crea un nuovo Ospite o Personale di servizio.



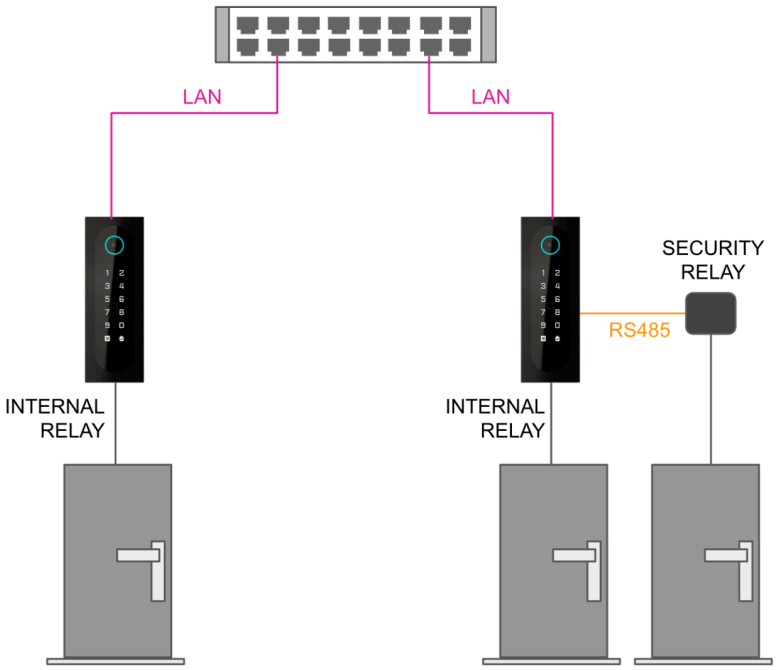
16 ACCÉDO KEY

16.1 INTRODUZIONE

Un ACCÉDO KEY è una tastiera numerica basata su IP con la capacità di scansionare un CODICE QR e leggere una tessera RFID. L'alimentazione può essere fornita sia con cavo di rete POE, sia con alimentatore dedicato.

Una serratura elettrica si può aprire in due modi:

- Attivando il relè interno del tastierino.
- Attivando il RELE' DI SICUREZZA collegato al tastierino tramite la porta RS485 integrata.

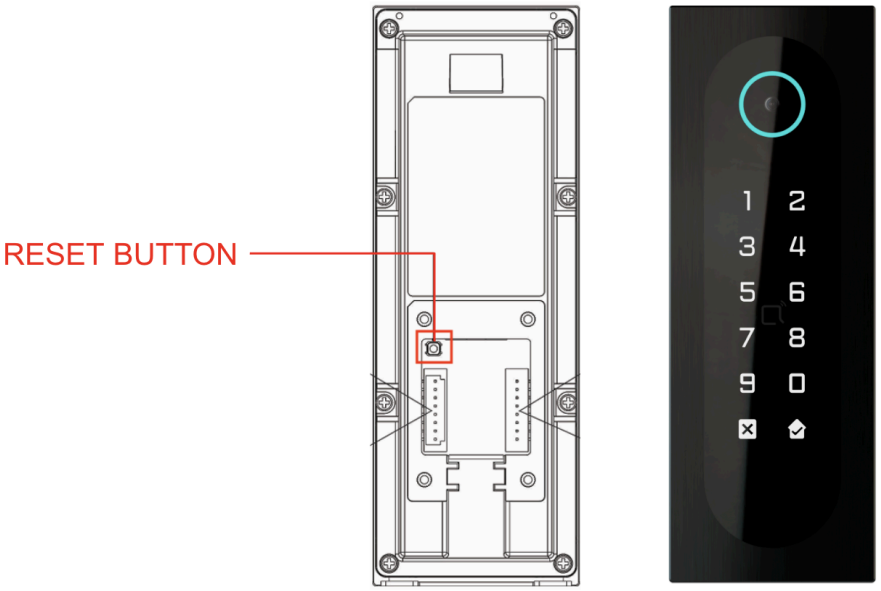


16.2 OPERAZIONI PRELIMINARI

Per utilizzare un ACCÉDO KEY in abbinamento ad un IKON SERVER per il controllo accessi è necessario:

- Collegarlo alla/e serratura/e da aprire
- Collegarlo alla LAN con un cavo RJ45
- Collegare l'alimentatore (se non provvisto di cavo di rete POE)
- Identificare l'indirizzo IP assegnato dal server DHCP

Per scoprire l'indirizzo IP effettivo di una ACCÉDO KEY, premere il pulsante RESET sul retro del dispositivo. Una voce detterà l'indirizzo IP (in lingua inglese).



Per maggiori dettagli si rimanda alla documentazione tecnica e al manuale applicativo del prodotto nella relativa sezione del sito EKINEX

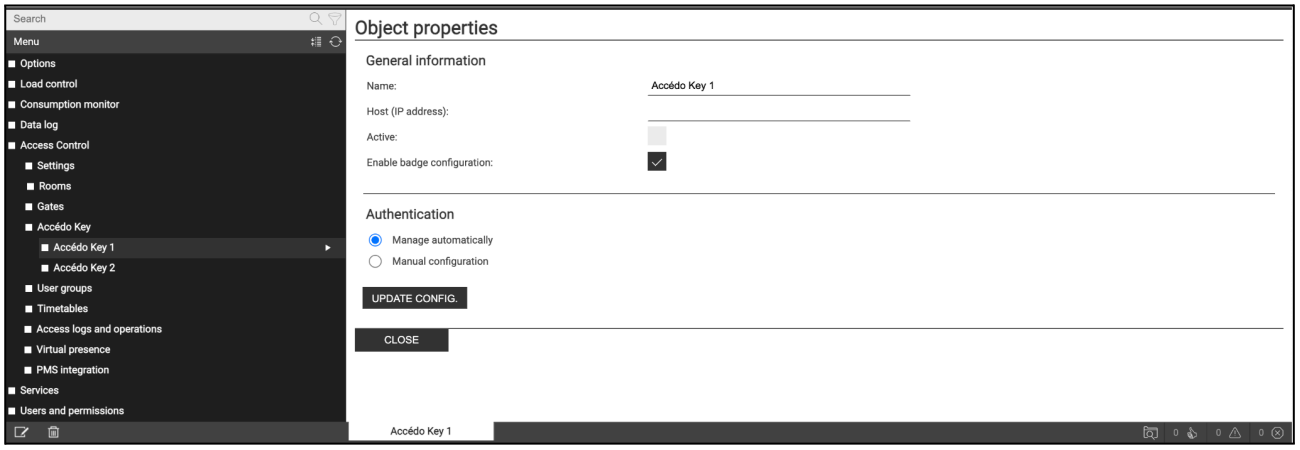
16.3 CREARE UN NUOVO DISPOSITIVO

Navigando dal menu nella sezione

CONTROLLO ACCESSI > ACCÉDO KEY

e premendo il pulsante [+] nella parte inferiore della barra degli strumenti, viene creato un nuovo dispositivo ACCÉDO KEY.

Nella figura seguente è raffigurata la pagina di dettaglio della CHIAVE ACCÉDO.



L'utente dovrà inserire le seguenti informazioni:

INFORMAZIONI GENERALI

NOME	Etichetta identificativa dell'ACCÉDO KEY
HOST (INDIRIZZO IP)	L'indirizzo IP dell'ACCÉDO KEY nella rete locale
ATTIVO	Questo campo (in sola lettura) viene flaggato solo quando l'ACCÉDO KEY è configurato con successo.
ABILITA CONFIGURAZIONE BADGE	Se è abilitata la gestione delle Card RFID, quando questa casella è selezionata, questo ACCÉDO KEY può essere utilizzato per abilitare una Tessera RFID ad aprire una Stanza o un varco tramite la funzione SCAN

AUTENTICAZIONE

GESTISCI AUTOMATICAMENTE	Una volta selezionata, la configurazione dell'ACCÉDO KEY viene gestita automaticamente da IKON SERVER che fornirà un nome utente e una password per impostare una comunicazione sicura tra la tastiera e il server. Questa configurazione automatica è consigliata per la maggior parte dei casi d'uso, poiché è più sicura e semplice rispetto alla configurazione manuale.
CONFIGURA MANUALMENTE	Quando selezionata, la configurazione della comunicazione sicura tra ACCÉDO KEY e IKON SERVER deve essere gestita dall'utente che deve selezionare il tipo di autenticazione (nessuna, lista consentita, base, digest) e se vengono selezionate basic o digest, si devono inserire nome utente e password.

16.3.1 AUTENTICAZIONE AUTOMATICA

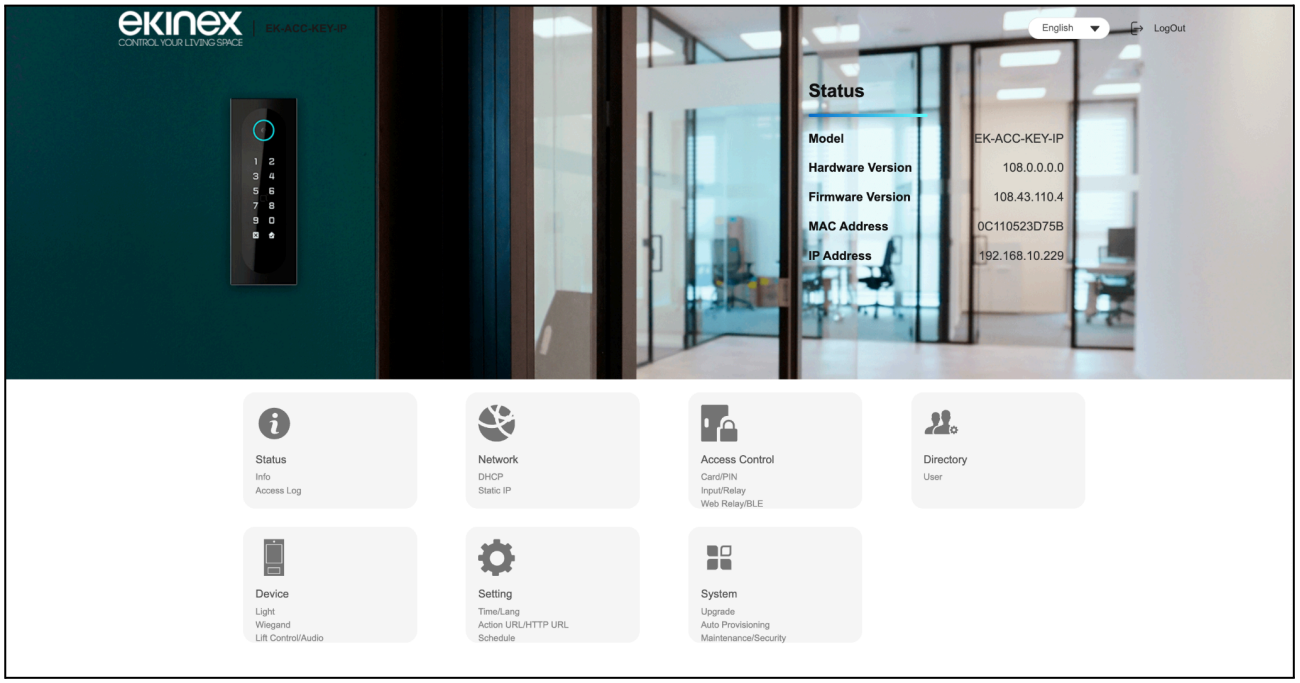
In questo caso, il IKON SERVER gestisce centralmente l'autenticazione della ACCÉDO KEY, impostando automaticamente i seguenti parametri:

- Credenziali per l'accesso al web.
- Credenziali per la comunicazione API HTTP (e il corrispondente flag di abilitazione).
- Credenziali per il comando di inoltro attraverso la rete (e relativo flag di abilitazione).

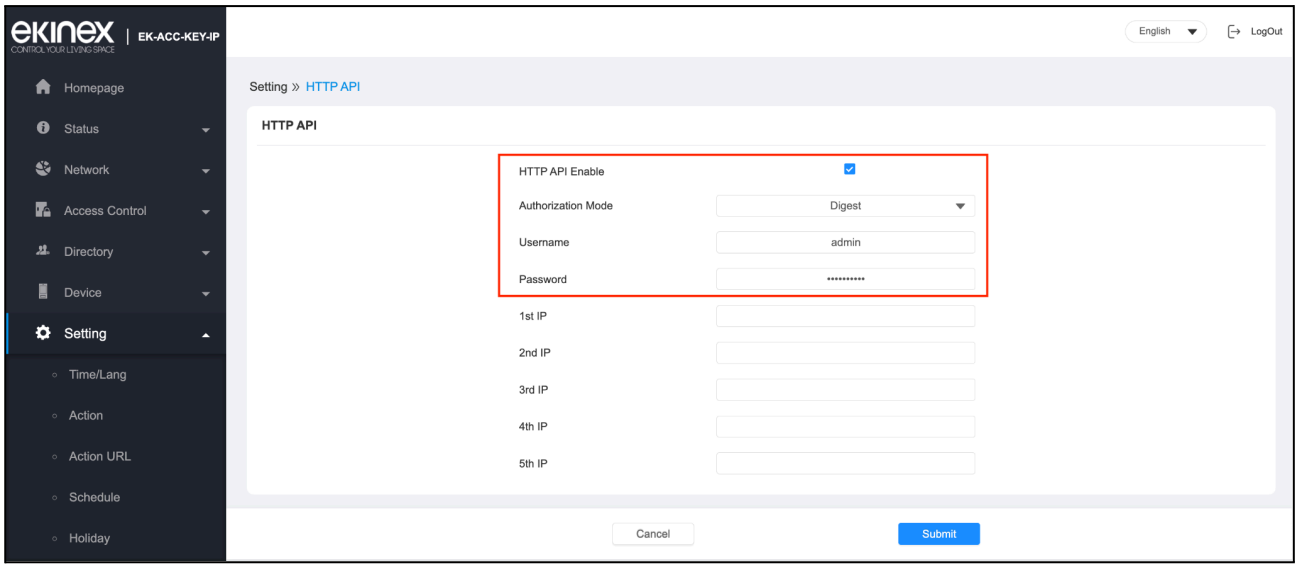
16.3.2 AUTENTICAZIONE MANUALE

Se si seleziona .CONFIGURA MANUALMENTE, prima di procedere con la configurazione su IKON SERVER è necessario eseguire le seguenti precondizioni:

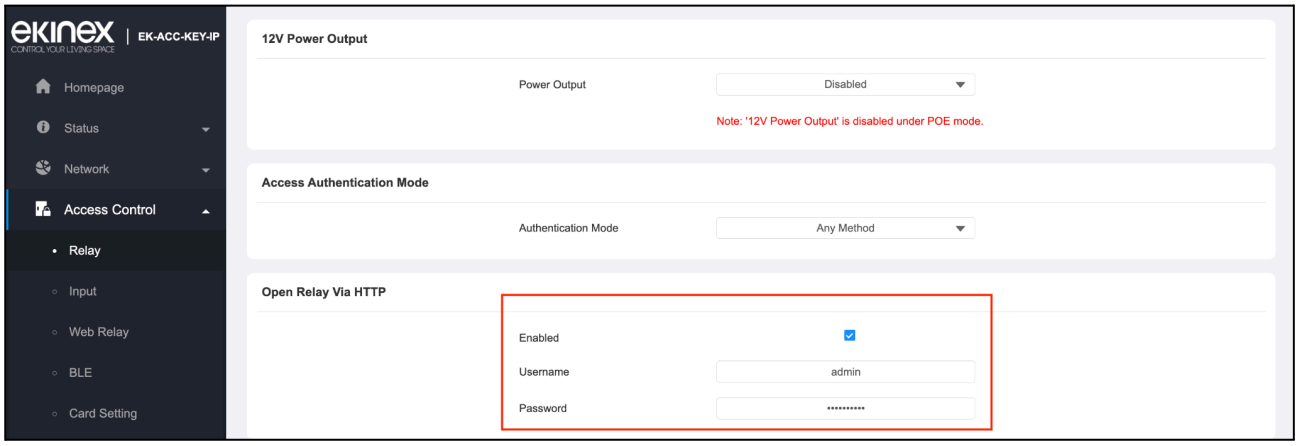
- Aprire un browser e cercare l'indirizzo IP del dispositivo ACCÉDO KEY che si desidera configurare.



- Se è la prima volta che si accede alla Pagina Web, si devono inserire le credenziali predefinite (nome utente: admin / password: admin) **e poi modificarli secondo necessità, per motivi di sicurezza**
- Entrare nel menù **IMPOSTAZIONE > API HTTP** e modificare le seguenti impostazioni:
    - Selezionare la casella "API HTTP ABILITATA"
    - Seleziona un metodo di autenticazione (si consiglia di utilizzare DIGEST/SOMMARIO)
    - Inserire un USERNAME e una PASSWORD da utilizzare per la comunicazione tra il dispositivo e IKON SERVER (e/o software di terze parti)
    - Conferma le modifiche premendo il pulsante INVIA/SUBMIT



- Entrare nel menù **CONTROLLO ACCESSI > RELE'** e nella sezione “APRI RELE’ TRAMITE HTTP”:
    - Seleziona la casella di controllo "Abilitato"
    - Entra **lo stesso USERNAME e PASSWORD** impostato nel menu **"API HTTP"**
    - Confermare le modifiche premendo il pulsante INVIA



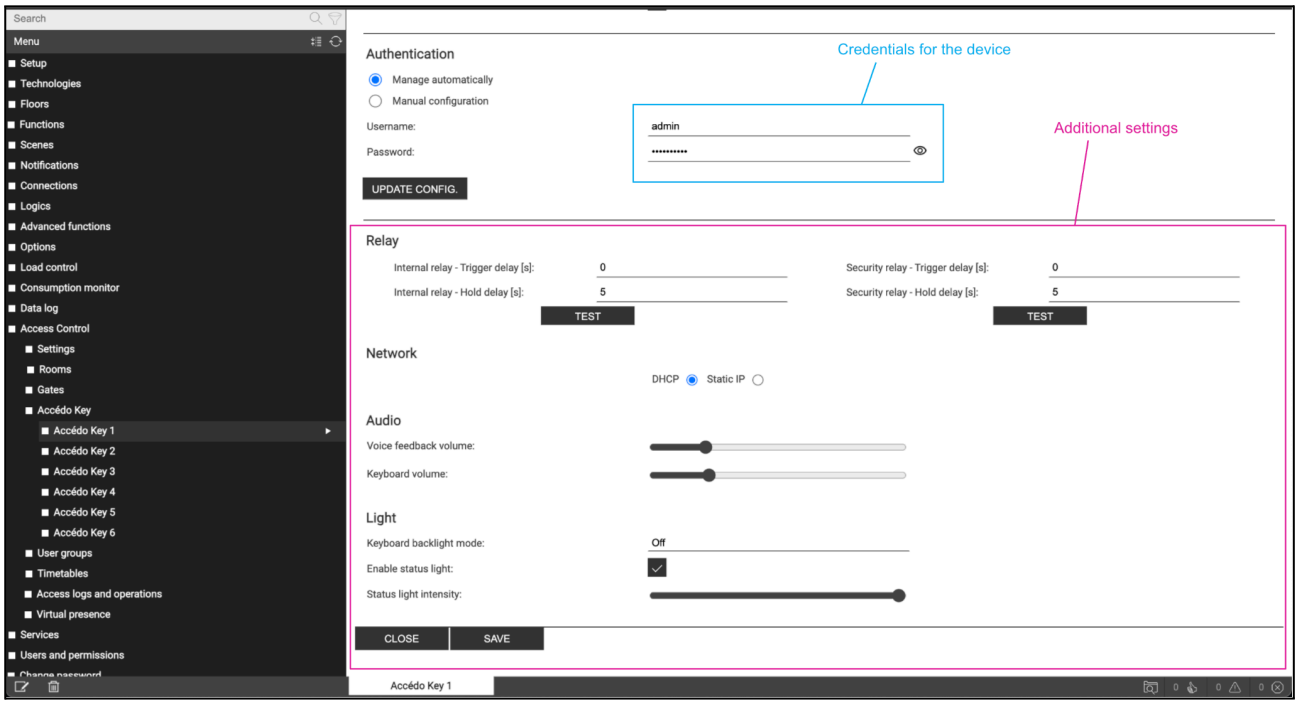
Una volta completate le precondizioni, tornare alla configurazione del menu ACCÉDO KEY sulla pagina web del IKON SERVER e inserire le seguenti informazioni:

TIPO DI AUTENTICAZIONE	Seleziona lo stesso metodo di autenticazione impostato nell'interfaccia web del dispositivo
NOME UTENTE PASSWORD	Credenziali per l'autenticazione DIGEST o BASE

16.3.3 SALVARE E CONTROLLARE LA CONNESSIONE

Indipendentemente dal metodo di configurazione selezionato, per completare la configurazione è necessario premere il pulsante AGGIORNA CONF. IKON SERVER tenterà di stabilire un canale di comunicazione con il dispositivo e, in caso di successo, si verificheranno le seguenti modifiche:

- La casella di controllo ATTIVO verrà contrassegnata.
- In caso di configurazione automatica, il nome utente e la password diventeranno visibili.
- Verranno visualizzate le *impostazioni aggiuntive* come illustrato nella seguente immagine:



Nelle *impostazioni aggiuntive* l'utente può

- verificare se il relè interno e il relè di sicurezza dell'ACCÉDO KEY funzionano correttamente e possono modificare il ritardo di attivazione e mantenimento di entrambi i relè.
- Modificare la configurazione di rete (DHCP o IP statico, si consiglia di mantenere l'opzione DHCP predefinita).
- Modificare il volume dell'audio e le impostazioni della luce della tastiera.

Se la configurazione non viene completata con successo, nella parte superiore del menu viene visualizzato un messaggio di errore. I possibili problemi possono essere i seguenti:

- Il campo dell'indirizzo IP è vuoto.
- L'indirizzo IP inserito non è corretto (ovvero il dispositivo non ha quell'indirizzo IP) o ha un formato non valido (solitamente deve essere 192.168.XXX.YYY).
- In caso di configurazione manuale, i passaggi preliminari spiegati sopra non sono stati seguiti correttamente.
- In caso di configurazione manuale, le informazioni di autenticazione non venivano popolate correttamente come nella pagina web ACCÉDO KEY.

16.4 IMPOSTAZIONI AGGIUNTIVE

RELÈ

TRIGGER DELAY	Il ritardo di l'apertura del relè. Il valore minimo è 0 e il valore massimo è 10. L'opzione è la stessa sia per il RELE' INTERNO che per il RELE' DI SICUREZZA (collegato alla porta RS485 dell'ACCÉDO KEY)
HOLD DELAY	Il tempo per il quale rimane attivo il relè eccitato (ad esempio il tempo per il quale la serratura della stanza o del varco viene tenuta aperta). Il valore minimo è 0 e il valore massimo è 60. L'opzione è la stessa sia per il RELE' INTERNO che per il RELE' DI SICUREZZA (collegato alla porta RS485 dell'ACCÉDO KEY)

RETE

MODALITÀ DI RETE	Permette di determinare se il dispositivo deve essere indirizzato automaticamente (DHCP) o manualmente (IP statico)
INDIRIZZO IP MASCHERA GATEWAY PREDEFINITO DNS PRIMARIO DNS SECONDARIO	Nel caso in cui venga selezionato l'IP statico, inserire le informazioni per l'assegnazione dell'IP statico: - Indirizzo IP - Maschera di sottorete - Gateway predefinito - DNS primario - DNS secondario Una volta salvato, se l'indirizzo IP è stato modificato è necessario modificare anche l'indirizzo IP nella sezione Informazioni generali e rifare la configurazione della comunicazione dell'ACCÉDO KEY.

AUDIO

VOLUME FEEDBACK VOCALE	Volume del feedback audio
VOLUME TASTIERA	Volume del feedback quando si preme il tastierino numerico

LEGGERO

MODALITÀ RETROILLUMINAZIONE TASTIERA	Permette di determinare quando la retroilluminazione della tastiera numerica deve essere accesa: • Mai (SPENTO) • Sempre (ACCESO) • Quando il sensore di prossimità rileva un movimento (AUTOMATICO)
ABILITA LUCE DI STATO	Abilita o meno la luce attorno alla webcam
INTENSITÀ DELLA LUCE DI STATO	Luminosità della luce intorno alla webcam

Quando si modifica una o più delle impostazioni sopra elencate, confermare le modifiche premendo SALVA.

16.5 ASSEGNAZIONE STANZE E VARCHI

Dopo aver creato e configurato un dispositivo ACCÉDO KEY, è ora possibile associarlo ad una STANZA o ad un VARCO. Per collegare una tastiera a una stanza/varco:

- Aprire la pagina dei dettagli della STANZA o del VARCO desiderato
- Abilitare la modalità ESPERTO ( )
- Dal menù della barra laterale selezionare l'ACCÉDO KEY che si vuole mappare alla Stanza o al Varco e trascinarlo nella sezione ACCÉDO KEY della STANZA o del VARCO.

Con questa operazione il RELE' INTERNO della ACCÉDO KEY verrà automaticamente abbinato alla SERRATURA della STANZA/VARCO. Tramite la funzione CONNESSIONI è possibile modificare questa relazione.

Un ACCÉDO KEY può essere associato a più STANZE o VARCHI. In questo modo quando un Ospite o un Personale di Servizio accede con successo alla Stanza o al varco a lui assegnato (tramite PIN, QR Code o Tessera RFID), il sistema aprirà solo la porta relativa alla Stanza o al varco dell'utente.

In questo tipo di configurazione è fondamentale impostare la relazione per la SERRATURA di ogni STANZA/VARCO con l'apposito

- Relè interno
- Relè di sicurezza
- Attuatore KNX

Lo stesso relè di una CHIAVE ACCÉDO non può essere correlato a più CAMERE o VARCHI. Altrimenti tutte le serrature si aprirebbero contemporaneamente.

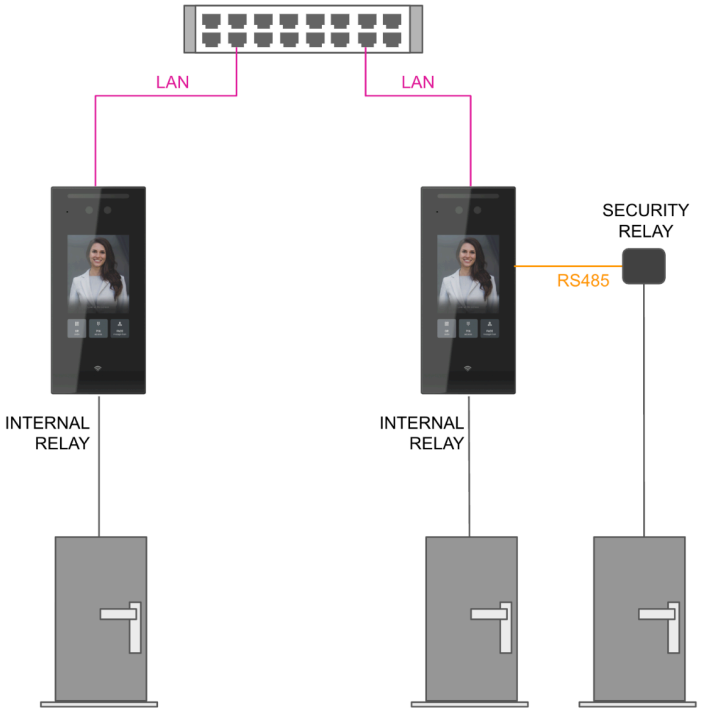
17 DICO

17.1 INTRODUZIONE

DICO è un videocitofono basato su IP che può consentire all'utente di digitare un PIN sul display, scansionare un QR CODE con la webcam integrata e leggere una tessera RFID. L'alimentazione può essere fornita sia con cavo di rete POE, sia con alimentatore dedicato.

Come l'ACCÉDO KEY, offre la possibilità di aprire una serratura elettrica:

- tramite il suo relè interno.
- Tramite un RELE' DI SICUREZZA, collegato al DICO tramite la porta RS485 integrata

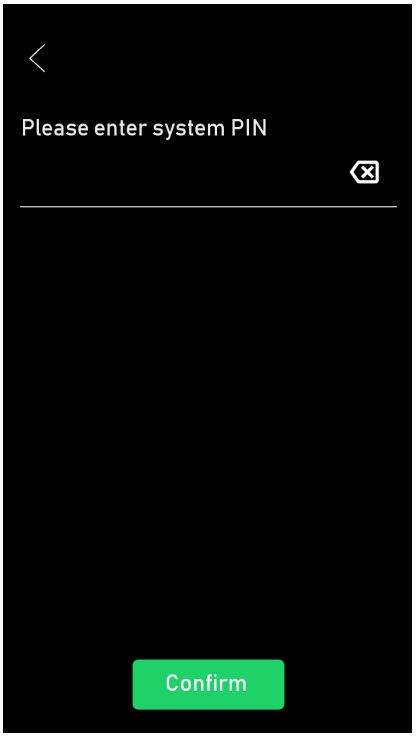


17.2 OPERAZIONI PRELIMINARI

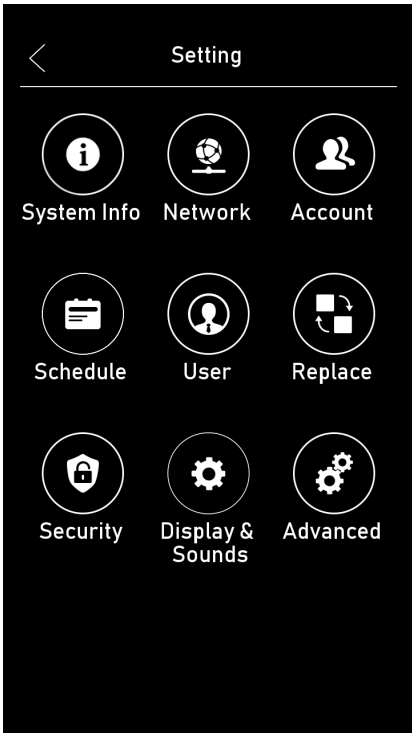
Per utilizzare un DICO in abbinamento a IKON SERVER per il controllo accessi è necessario:

- Collegarlo alla/e serratura/e da aprire
- Collegarlo alla LAN con un cavo RJ45
- Collegare l'alimentatore (se non provvisto di cavo di rete POE)
- Identificare l'indirizzo IP assegnato dal server DHCP

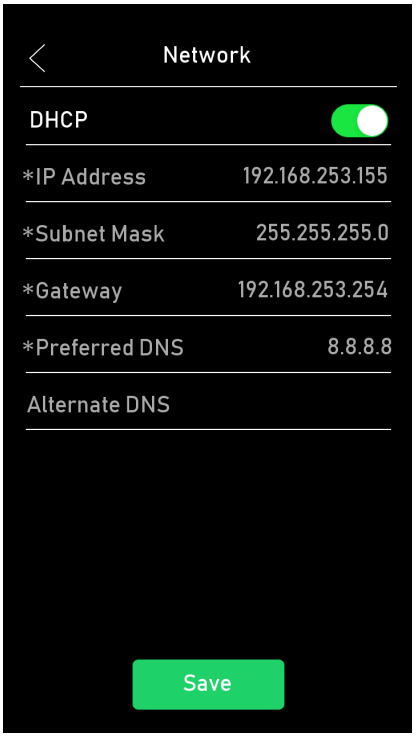
Per conoscere l'Indirizzo IP di un DICO è necessario accedere alle impostazioni del videocitofono nel seguente modo:



Premere un punto qualsiasi dello schermo del DICO e tenere premuto il dito per più di 10 secondi finché non verrà richiesta la password.
Digitare *admin* e premere Conferma



Selezionare *Rete*



Prendere nota dell'indirizzo IP dell'unità esterna

Per maggiori dettagli si rimanda alla documentazione tecnica e al manuale applicativo del prodotto nella relativa sezione del sito EKINEX

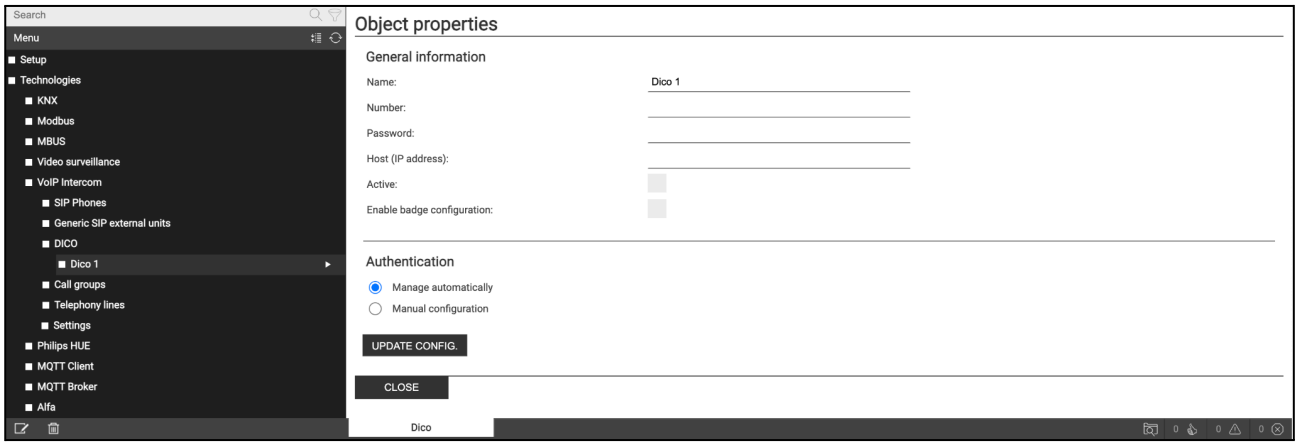
17.3 CREARE UN NUOVO DISPOSITIVO

Per aggiungere un nuovo dispositivo DICO, nella pagina web IKON SERVER, accedere alla sezione

TECNOLOGIE > VIDEOCITOFONIA > DICO

e premere il pulsante [+] nella barra degli strumenti.

La figura seguente mostra la pagina dei dettagli del DICO.



L'utente dovrà inserire le seguenti informazioni:

INFORMAZIONI GENERALI

NOME	Etichetta identificativa del DICO
NUMERO	Numero VoIP da utilizzare per chiamare il dispositivo DICO. Da compilare se IKON SERVER è il server SIP. Nota: per le funzionalità di controllo accessi questa voce può essere ignorata.
PASSWORD	Password per proteggere la funzione VoIP. Da compilare se IKON SERVER è il server SIP. Nota: per le funzionalità di controllo accessi questa voce può essere ignorata.
HOST (INDIRIZZO IP)	L'indirizzo IP del DICO nella rete locale
ATTIVO	Questo campo (in sola lettura) viene contrassegnato solo quando il DICO è configurato correttamente.
ABILITA CONFIGURAZIONE BADGE	Se è abilitata la gestione delle tessere RFID, quando questo checkbox è selezionato, questo DICO può essere utilizzato per abilitare una Tessera RFID ad aprire una Stanza o un Varco tramite la funzione SCAN

AUTENTICAZIONE

GESTISCI AUTOMATICAMENTE	Quando selezionato, la configurazione del DICO viene gestita automaticamente da IKON SERVER che fornirà un nome utente e una password per impostare una comunicazione sicura tra l'interfono e il server. Questa configurazione automatica è consigliata per la maggior parte dei casi d'uso, poiché è più sicura e semplice rispetto alla configurazione manuale.
CONFIGURA MANUALMENTE	Quando selezionata, la configurazione della comunicazione sicura tra il DICO e il IKON SERVER deve essere gestita dall'utente che deve selezionare il tipo di autenticazione (nessuna, consentiti, basic, digest) e se sono selezionate basic o digest, deve inserire un nome utente e una password.

17.3.1 AUTENTICAZIONE AUTOMATICA

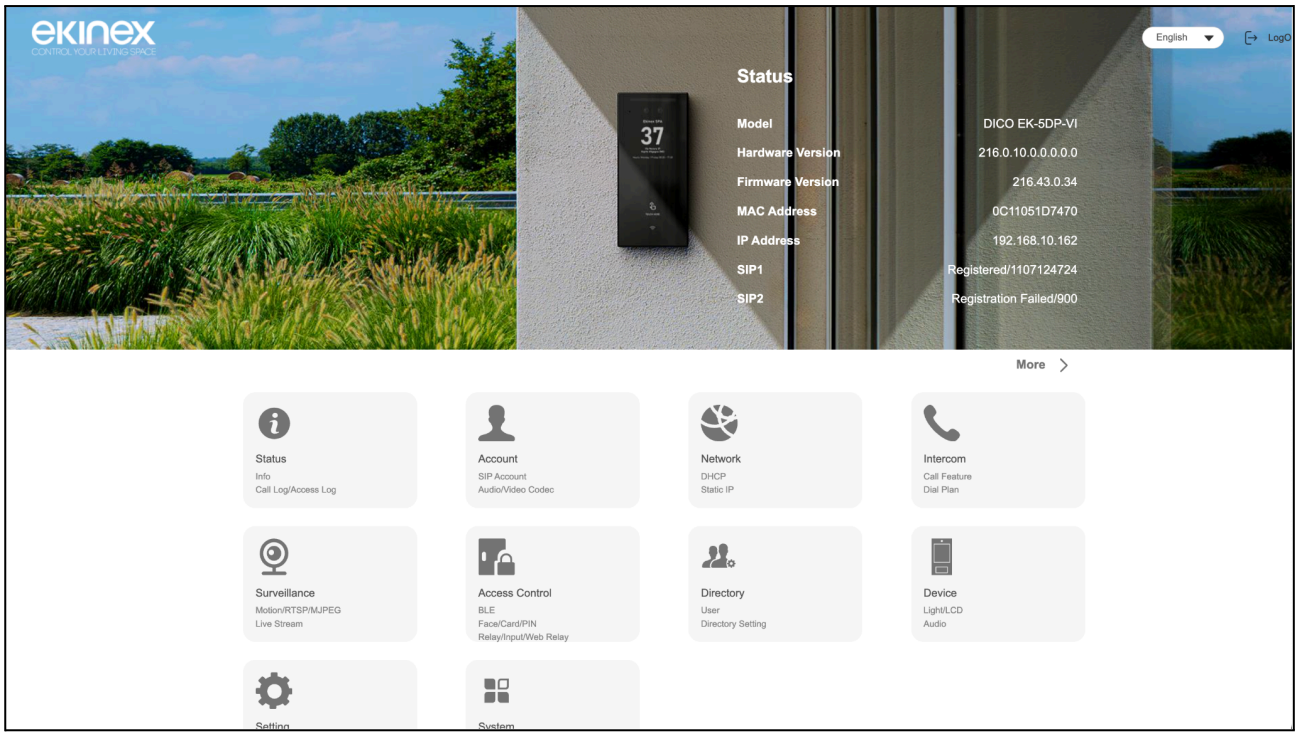
In questo caso, IKON SERVER gestisce centralmente l'autenticazione del DICO, impostando automaticamente i seguenti parametri:

- Credenziali per l'accesso al web.
- Credenziali per la comunicazione API HTTP (e il corrispondente flag di abilitazione).
- Credenziali per il comando di inoltro attraverso la rete (e relativo flag di abilitazione).

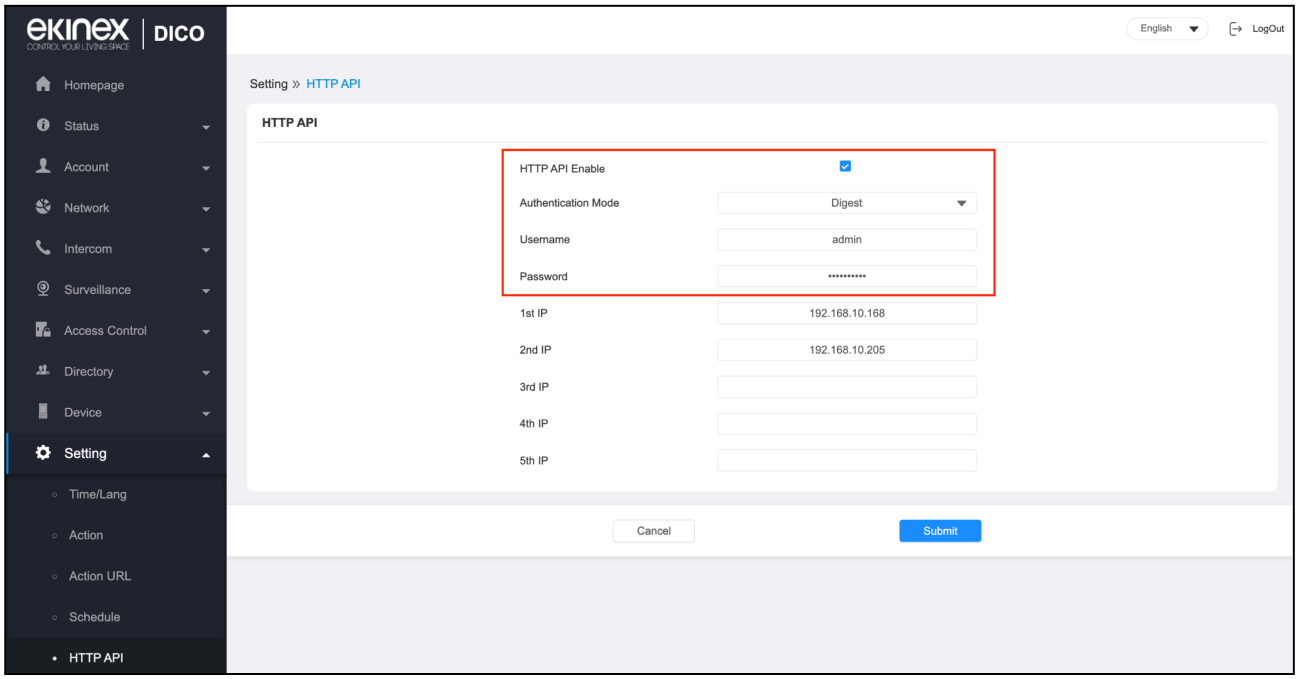
17.3.2 AUTENTICAZIONE MANUALE

Se si seleziona CONFIGURA MANUALMENTE, prima di procedere con la configurazione su IKON SERVER è necessario eseguire le seguenti precondizioni:

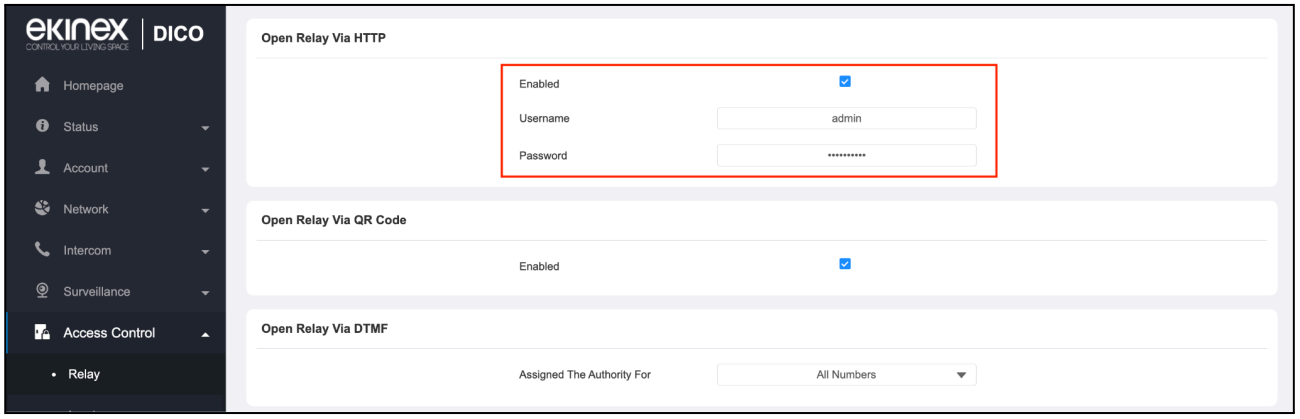
- Aprire un browser e cercare l'indirizzo IP del dispositivo DICO che desideri configurare



- Se è la prima volta che si accede a questa Pagina Web, inserire le credenziali predefinite (nome utente: admin / password: admin) **e modificarli secondo necessità, per motivi di sicurezza**
- Entrare nel menù **IMPOSTAZIONE > API HTTP** e modificare le seguenti impostazioni:
    - Seleziona la casella di controllo "Abilita API HTTP"
    - Seleziona un metodo di autenticazione (si consiglia di utilizzare DIGEST)
    - Inserire un USERNAME e una PASSWORD da utilizzare per la comunicazione tra il dispositivo e IKON SERVER (e/o software di terze parti)
    - Conferma le modifiche premendo il pulsante INVIA



- Entrare nel menù **CONTROLLO ACCESSI > RELE'** e nella sezione “APRI RELE’ TRAMITE HTTP”:
    - Seleziona la casella di controllo "Abilitato"
    - Entra **lo stesso USERNAME e PASSWORD** impostato nel menu **"API HTTP"**
    - Confermare le modifiche premendo il pulsante INVIA



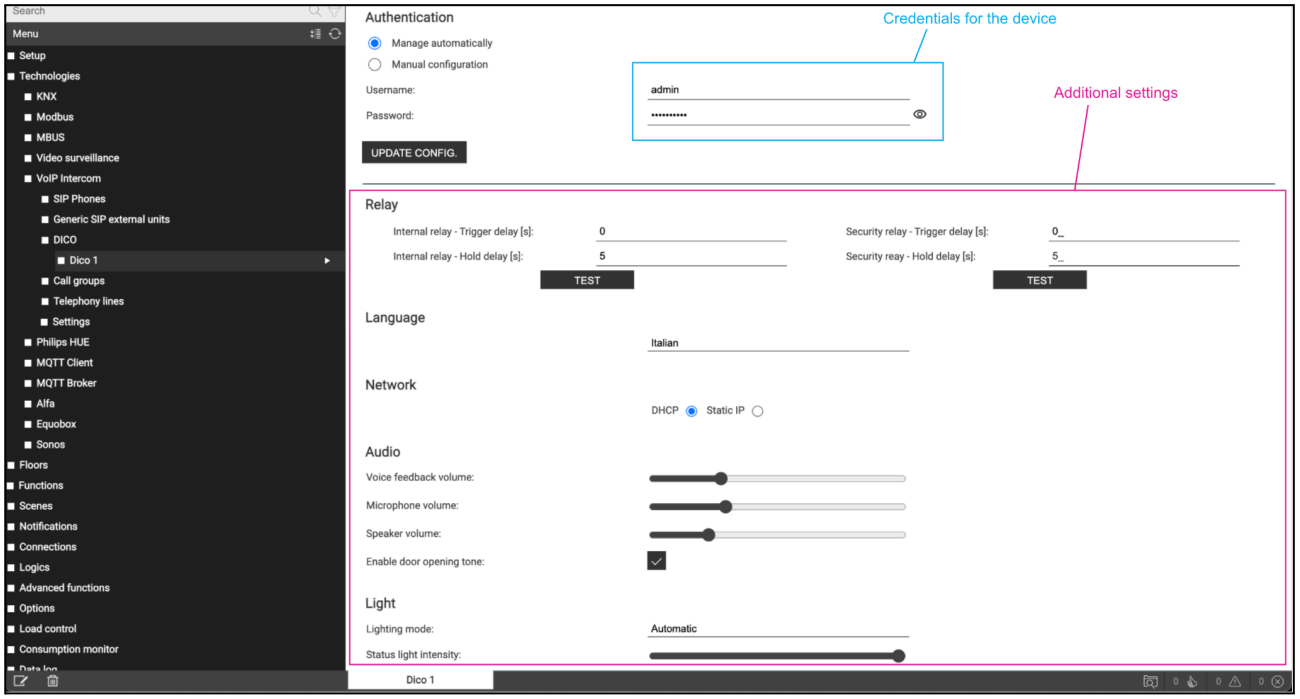
Una volta completati i passaggi di precondizione, tornare alla configurazione del menu DICO sulla pagina web IKON SERVER e inserire le seguenti informazioni:

TIPO DI AUTENTICAZIONE	Seleziona lo stesso metodo di autenticazione impostato nell'interfaccia web del dispositivo
NOME UTENTE PASSWORD	Credenziali per l'autenticazione DIGEST o BASE

17.3.3 SALVARE E CONTROLLARE LA CONNESSIONE

Indipendentemente dal metodo di configurazione selezionato, per completare la configurazione è necessario premere il pulsante AGGIORNA CONF. Il IKON SERVER tenterà di stabilire un canale di comunicazione con il dispositivo e, in caso di successo, si verificheranno le seguenti modifiche:

- La casella di controllo ATTIVO verrà contrassegnata.
- In caso di configurazione automatica, il nome utente e la password diventeranno visibili.
- Verranno visualizzate le *impostazioni aggiuntive* come illustrato nella seguente immagine:



Nelle *impostazioni aggiuntive* l'utente può

- Verificare se il relè interno e il relè di sicurezza del DICO funzionano correttamente e possono modificare il ritardo di attivazione e mantenimento di entrambi i relè.
- Modificare la configurazione di rete (DHCP o IP statico, si consiglia di mantenere l'opzione DHCP predefinita).
- Cambia il volume dell'audio, la luce e le impostazioni video.

Se la configurazione non viene completata con successo, nella parte superiore del menu viene visualizzato un messaggio di errore. I possibili problemi possono essere i seguenti:

- Il campo dell'indirizzo IP è vuoto.
- L'indirizzo IP inserito non è corretto (ovvero il dispositivo non ha quell'indirizzo IP) o ha un formato non valido (solitamente deve essere 192.168.XXX.YYY).
- In caso di configurazione manuale, i passaggi preliminari spiegati sopra non sono stati seguiti correttamente.
- In caso di configurazione manuale, le informazioni di autenticazione non venivano popolate correttamente come nella pagina web DICO.

17.4 IMPOSTAZIONI AGGIUNTIVE

RELÈ

TRIGGER DELAY	Il ritardo di apertura del relè. Il valore minimo è 0 e il valore massimo è 10. L'opzione è la stessa sia per il RELE' INTERNO che per il RELE' DI SICUREZZA (collegato alla porta RS485 del DICO)
HOLD DELAY	Il tempo per il quale resta attivo il relè eccitato (ad esempio il tempo per il quale la serratura della stanza o del varco viene tenuta aperta). Il valore minimo è 0 e il valore massimo è 60. L'opzione è la stessa sia per il RELE' INTERNO che per il RELE' DI SICUREZZA (collegato alla porta RS485 del DICO)

RETE

(MODALITÀ RETE)	Permette di determinare se il dispositivo deve essere indirizzato automaticamente (DHCP) o manualmente (IP statico)
INDIRIZZO IP MASCHERA GATEWAY PREDEFINITO DNS PRIMARIO DNS SECONDARIO	Nel caso in cui venga selezionato l'IP statico, inserire le informazioni per l'assegnazione dell'IP statico: - Indirizzo IP - Maschera - Gateway predefinito - DNS primario - DNS secondario Una volta salvato, se l'indirizzo IP è stato modificato è necessario modificare anche l'indirizzo IP nella sezione Informazioni generali e rifare la configurazione di comunicazione del DICO.

AUDIO

VOLUME FEEDBACK VOCALE	Livello del volume del feedback audio del DICO all'accesso alla Stanza o al varco
VOLUME MICROFONO	Livello del volume per il microfono integrato del DICO
VOLUME SPEAKER	Livello del volume dell'altoparlante durante una chiamata
ABILITA TONO APERTURA PORTA	Abilita o meno l'effetto audio quando il relè è aperto

LUCE

MODALITÀ ILLUMINAZIONE	Stato di attivazione del LED sulla parte superiore del prodotto: ● Sempre SPENTO ● Automatico con sensore di prossimità e luminosità
INTENSITÀ LUCE DI STATO	Luminosità del LED

VIDEO

ABILITA RTSP	Abilita lo streaming video per le chiamate vocali
FORMATO	Ritaglio video dello streaming video: • Verticale • Orizzontale

Quando si modifica una o più delle impostazioni sopra elencate, confermare le modifiche premendo SALVA.

17.5 ASSEGNAZIONE STANZE E VARCHI

Dopo aver creato e configurato un dispositivo DICO, è ora possibile associarlo ad una STANZA o ad un VARCO. Per collegare un videocitofono ad una stanza/varco:

- Aprire la pagina dei dettagli della STANZA o del VARCO desiderato
- Abilitare la modalità ESPERTO ()
- Dal menù della barra laterale selezionare il DICO che si vuole mappare alla Stanza o al Varco e trascinarlo nella sezione DICO della STANZA o del VARCO.

Con questa operazione il RELE' INTERNO del DICO verrà automaticamente abbinato alla SERRATURA della STANZA/VARCO. Tramite la funzione CONNESSIONI è possibile modificare questa relazione.

Un DICO può essere associato a più STANZE o VARCHI. In questo modo quando un Ospite o un Personale di Servizio accede con successo alla Stanza o al varco a lui assegnato (tramite PIN, QR Code o Tessera RFID), il sistema aprirà solo la porta relativa alla Stanza o al varco dell'utente.

In questo tipo di configurazione è fondamentale impostare la relazione per la SERRATURA di ogni STANZA/VARCO con l'apposito:

- Relè interno.
- Relè di sicurezza.
- Attuatore KNX .



Lo stesso relè di un DICO non può essere correlato a più STANZE o VARCHI. Altrimenti tutte le serrature si aprirebbero contemporaneamente.

18 CONNESSIONI

18.1 INTRODUZIONE

Quando un OSPITE utilizza un PIN, un QR CODE o una Tessera RFID validi, la proprietà SERRATURA della STANZA o del varco corrispondente viene settata su APERTO per un certo numero di secondi (come configurato nelle IMPOSTAZIONI GENERALI).

Questo è un *oggetto virtuale* rappresentante la serratura della porta associata; questa proprietà deve essere associata (con una *relazione*) con l'oggetto reale che invia il comando al relè, il quale è fisicamente collegato all'elettroserratura.

Come accennato in precedenza, può essere:

- Il RELE' integrato di un DICO o ACCÉDO KEY.
- Un RELE' DI SICUREZZA collegato ad un DICO o ACCÉDO KEY tramite connessione RS485.
- Il canale di un attuatore KNX (rappresentato con un WIDGET KNX all'interno di IKON SERVER)

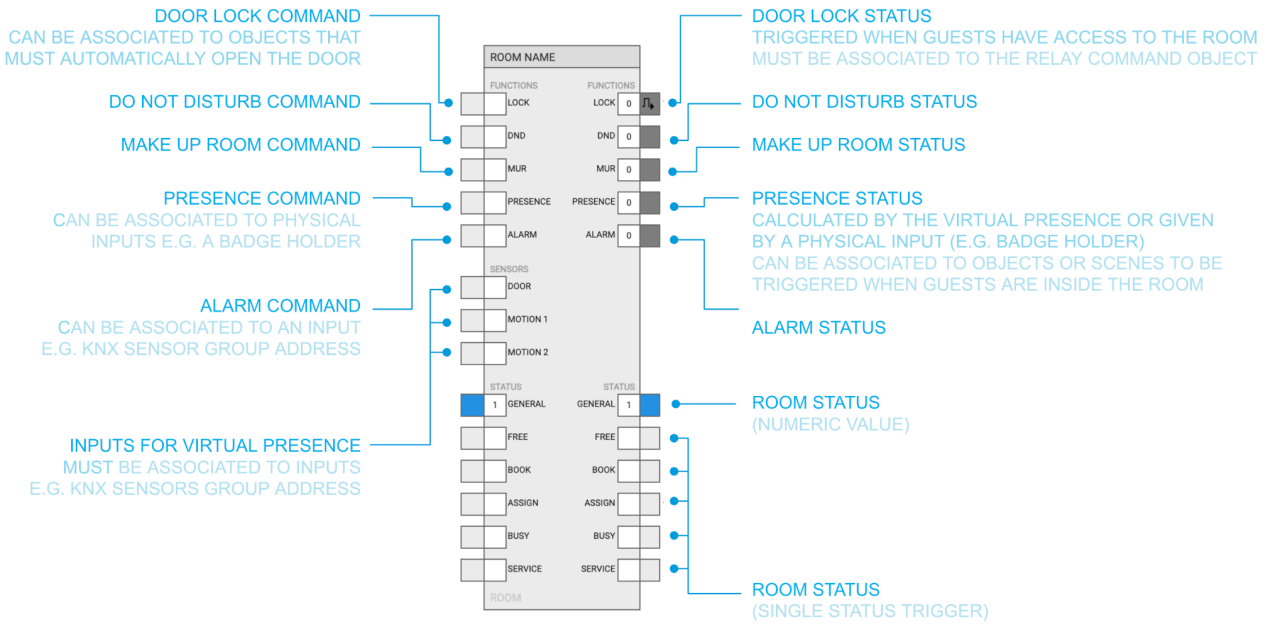
Questa relazione può essere realizzata in 3 modi[1]:

- Con una CONNESSIONE
- Con un TRIGGER
- Con una LOGICA

Per facilitare la configurazione di tali relazioni, la pagina di configurazione di una STANZA o di un VARCO offrono la possibilità di modificare una CONNESSIONE “implicita”. Questo editor è accessibile premendo il pulsante CONNESSIONI.

18.2 COLLEGAMENTI DELLE STANZE

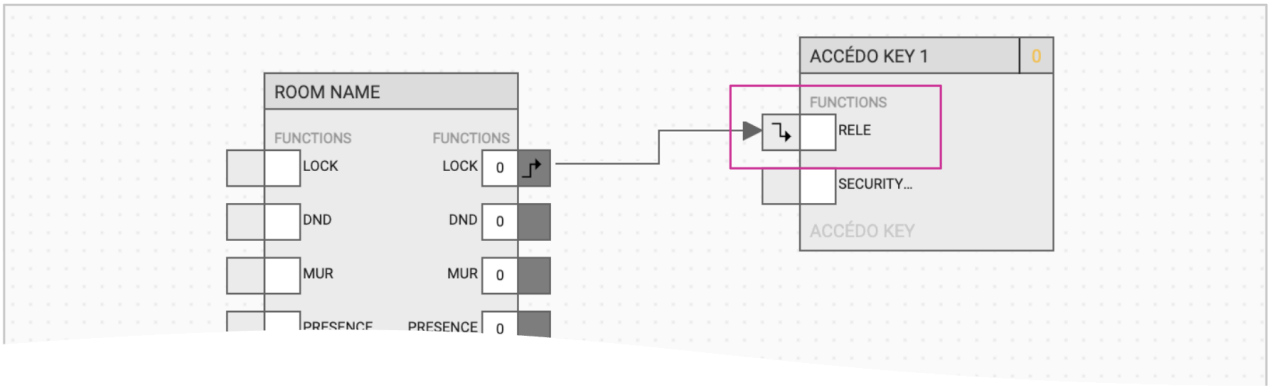
Il blocco che rappresenta la STANZA nell'editor delle connessioni offre i seguenti nodi:



[1] Per informazioni più generali su queste automazioni fare riferimento al manuale applicativo AUTOMAZIONI di IKON SERVER.

18.2.1 APERTURA SERRATURA TRAMITE DICO O ACCÉDO KEY

Se alla stanza è associata un DICO o un ACCÉDO KEY, il suo relè interno viene automaticamente associato con una *relazione* alla proprietà PORTA della Stanza, come illustrato nell'esempio seguente:

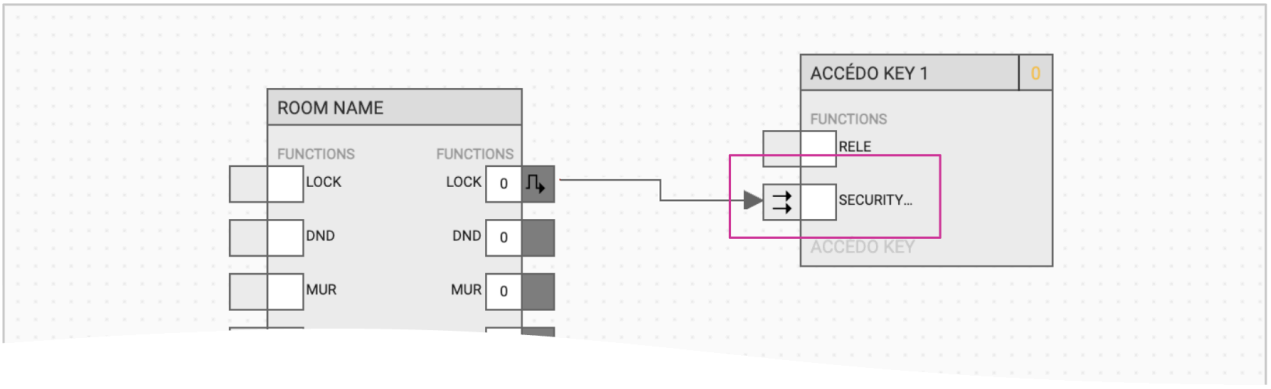


Con questa relazione, quando un Ospite o un Personale di Servizio accede alla stanza attraverso l'ACCÉDO KEY 1, la porta viene aperta senza bisogno di alcuna altra configurazione.

Nel caso in cui la porta non sia fisicamente collegata al relè interno del dispositivo di controllo accessi, è necessario modificare la *relazione*. Un esempio è l'utilizzo di un RELE' DI SICUREZZA collegato all'ACCÉDO KEY o al DICO: in questo caso è necessario:

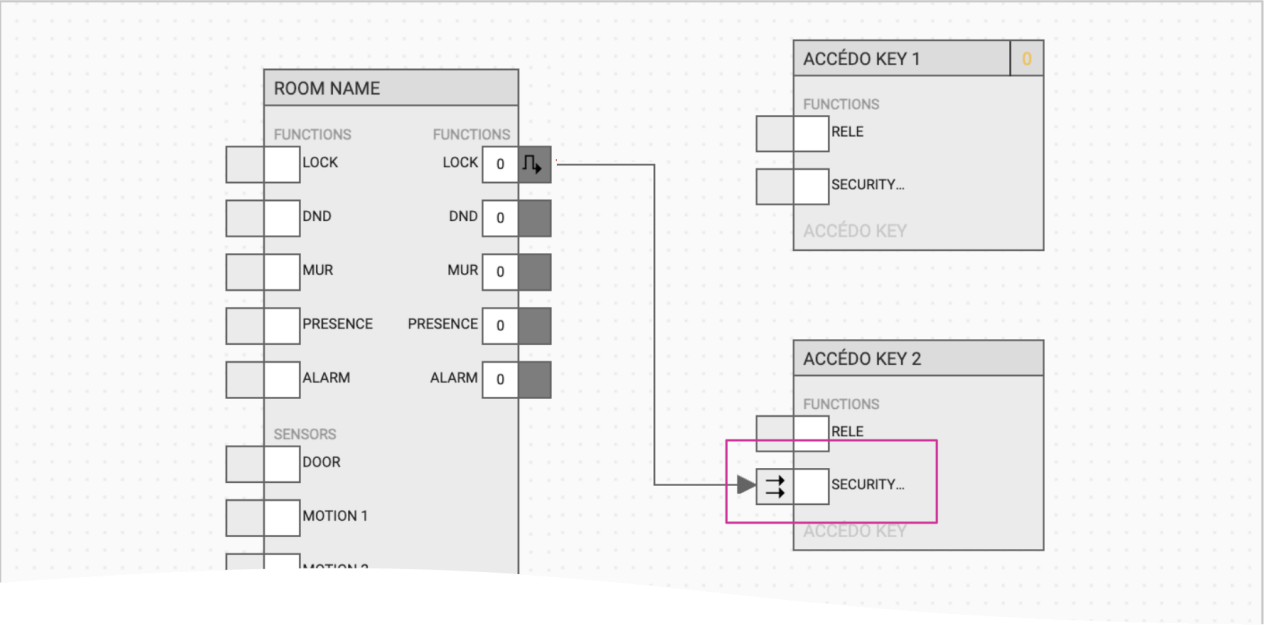
- Rimuovere la relazione predefinita selezionando la freccia e premendo il tasto CANC.
- Trascinare una nuova *freccia* partendo dal nodo di uscita PORTA (sul lato destro del blocco stanze) nel nodo SICUREZZA.

Il risultato apparirà come nella figura seguente:



Se la porta viene aperta da un relè collegato ad un altro dispositivo DICO o ACCÉDO KEY è necessario:

- Trascinare il nuovo dispositivo dal menu laterale nell'editor CONNESSIONI.
- Spostarlo nella finestra dell'editor (perché inizialmente è *sovrapposto* rispetto al dispositivo precedente)
- Rimuovere le frecce che non servono.
- Collegare con una freccia la PORTA all'apposito relè.


ROOM NAME
FUNCTIONS
LOCK
DND
MUR
PRESENCE
ALARM
SENSORS
DOOR
MOTION 1
FUNCTIONS
LOCK 0
DND 0
MUR 0
PRESENCE 0
ALARM 0
ACCÉDO KEY 1
0
FUNCTIONS
RELE
SECURITY...
ACCÉDO KEY
ACCÉDO KEY 2
FUNCTIONS
RELE
SECURITY...
ACCÉDO KEY

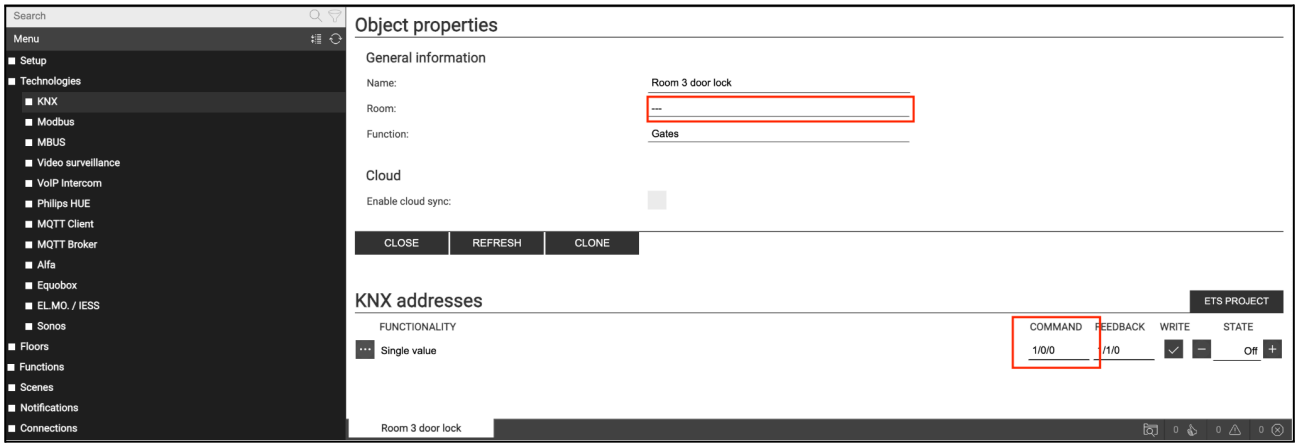
18.2.2 APERTURA SERRATURA CON ATTUATORE KNX

Nel caso in cui la porta o il varco venga aperto da un attuatore KNX, la procedura per creare una relazione nell'editor CONNESSIONI è la seguente:

- Dal menu IKON SERVER accedere alla sezione

  TECNOLOGIE > KNX > WIDGET KNX > ALTRO

  e aggiungere un nuovo widget VALORE SINGOLO premendo il pulsante AGGIUNGI.
- Dare un nome significativo al WIDGET (es. "SERRATURA STANZA X").
- Entrare nella pagina dei dettagli e inserire l'indirizzo del gruppo KNX nel campo COMANDO (o trascina e rilascia l'indirizzo appropriato dal menu ad albero PROGETTO ETS sul pannello di destra). Lasciare vuoto il campo Ambiente.

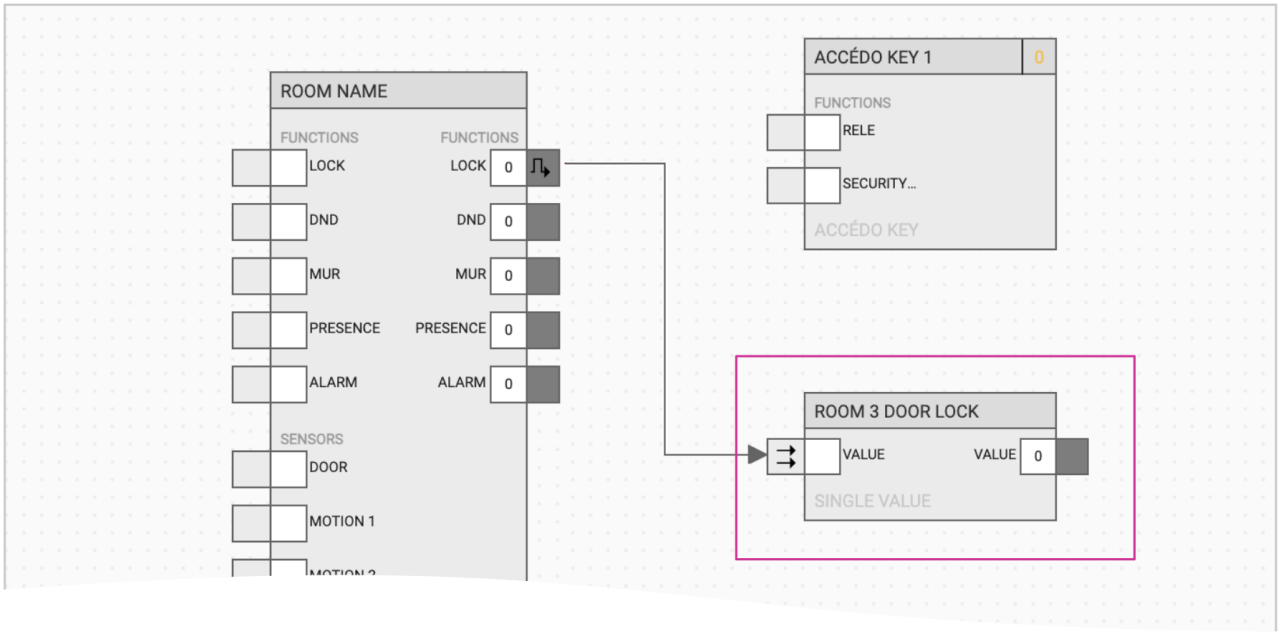


- Aprire l'editor CONNESSIONE della Stanza e cerca il widget creato nei passaggi precedenti utilizzando il motore di RICERCA o il FILTRO digitando il nome del widget; in alternativa è possibile ricercare l'OGGETTO KNX digitando l'indirizzo del gruppo KNX.
- Trascinare e rilasciare il WIDGET / OGGETTO KNX nell'editor delle CONNESSIONI.
- Collegare con una freccia il nodo di uscita SERRATURA della STANZA al nodo di ingresso del widget KNX.

Nel/i KNX i WIDGET che vengono creati solo per un'automazione, come nell'esempio, non necessitano di essere aggiunti ad una Ambiente (nella menu del webserver si trova in PIANI → PIANO X → AMBIENTE Y) perché non necessitano di essere comandati direttamente dall'app.

Anche l'assegnazione ad una FUNZIONE è facoltativa.

L'immagine seguente mostra un esempio di COLLEGAMENTO tra una Stanza ed un WIDGET KNX:

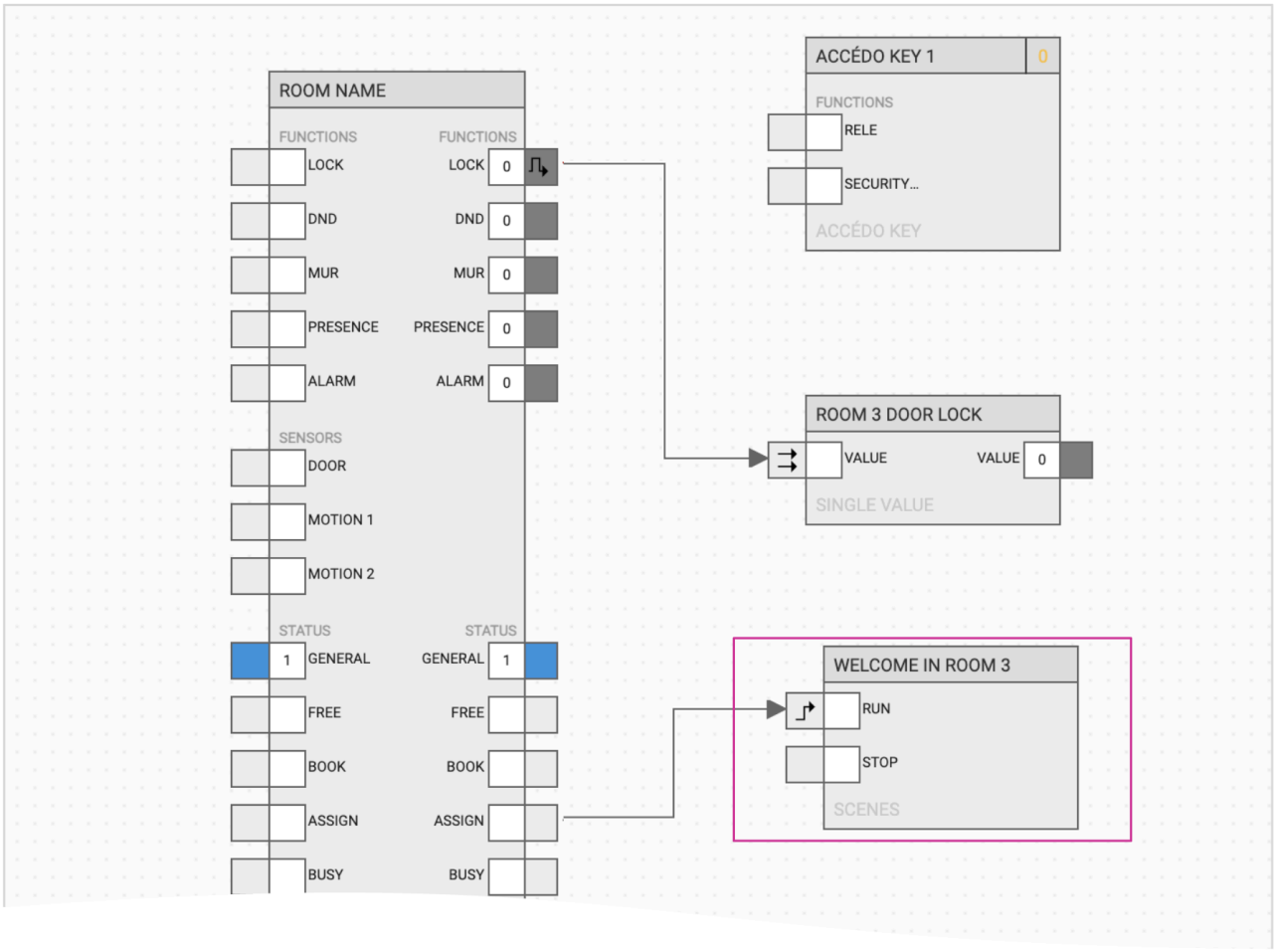


18.2.3 ESEMPIO DI COLLEGAMENTO: SCENARIO DI BENVENUTO AL CAMBIO DI STATO DI UNA STANZA

Uno scenario automatico interessante è l'esecuzione di uno “scenario di benvenuto” quando una stanza viene assegnata a un ospite, ovvero sta iniziando il periodo di validità dell'ospite e l'ospite arriverà presto in struttura.

La procedura per realizzare questo tipo di automazione è la seguente:

- Nel menu del IKON SERVER, andare alla sezione SCENARI e creare un nuovo scenario.
- Trascinare tutte le azioni necessarie nella sezione AZIONI ESEGUITE DALLO SCENARIO (ad esempio, avviare il riscaldamento o l’aria condizionata, impostare le persiane ad un determinato livello, ecc…).
- Trascinare lo scenario creato nell'editor CONNESSIONI.
- Trascinare una freccia dal nodo di uscita ASSIGN della Stanza e collegarla al nodo di ingresso RUN dello scenario, come mostrato nell'esempio seguente.



18.3 COLLEGAMENTI DEI VARCHI

La gestione delle connessioni tra un DICO o ACCÉDO KEY ed un varco è simile a quello descritto per le CAMERE. La differenza è che il varco ha come nodo solo la PORTA.

19 AUTORIZZAZIONI

19.1 GRUPPI UTENTE

I Gruppi utente possono essere utilizzati per definire regole di accesso per più ospiti e/o personale di servizio con esigenze simili.

Il sistema offre due gruppi di utenti predefiniti:

SERVIZIO	Personale della struttura
OSPITI	Visitatori della struttura

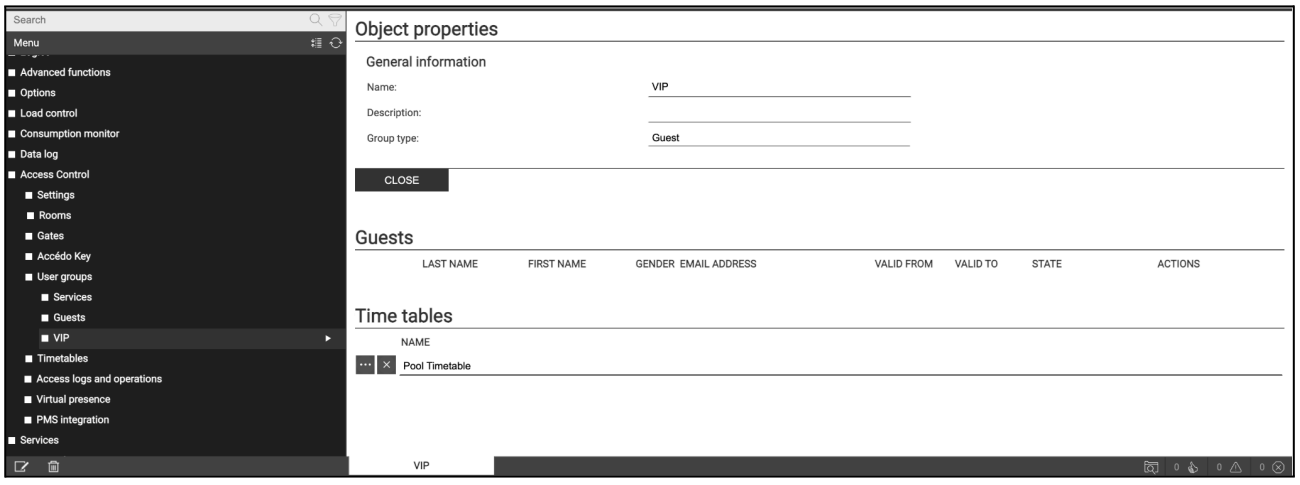
È possibile creare ulteriori gruppi di utenti navigando nel menu IKON SERVER

CONTROLLO ACCESSI > GRUPPI UTENTE

e premendo il pulsante [+] nella barra degli strumenti. Nei DATI GENERALI sono richieste le seguenti informazioni:

NOME	Etichetta associata al gruppo utenti (es. VIP, Pulizia, ecc.)
DESCRIZIONE	Descrizione aggiuntiva facoltativa
TIPO	La tipologia di utenti associabili al gruppo: ● Comune (ovvero sia Personale che Ospiti) ● Personale ● Ospiti

Esempio di configurazione per un gruppo di utenti:



19.2 FASCE ORARIE

Le fasce orarie vengono utilizzate per limitare l'accesso ad una o più Stanze/Varchi in determinati giorni della settimana e orari.

19.2.1 CREA UN NUOVO ORARIO

Per creare un nuovo orario, navigare nel menu IKON SERVER

CONTROLLO ACCESSI > FASCE ORARIE

e premere il pulsante [+] nella barra degli strumenti.

Nei DATI GENERALI sono richieste le seguenti informazioni:

NOME	Etichetta associata alla fascia oraria
DESCRIZIONE	Descrizione aggiuntiva facoltativa
ABILITATO	Determina se la fascia oraria può essere usata o meno

19.2.2 ORARI

Un orario garantisce l'accesso in una o più fasce orarie; nella sezione ORARI premere il pulsante AGGIUNGI per aggiungere un nuovo orario. Per definire un orario sono necessarie le seguenti informazioni:

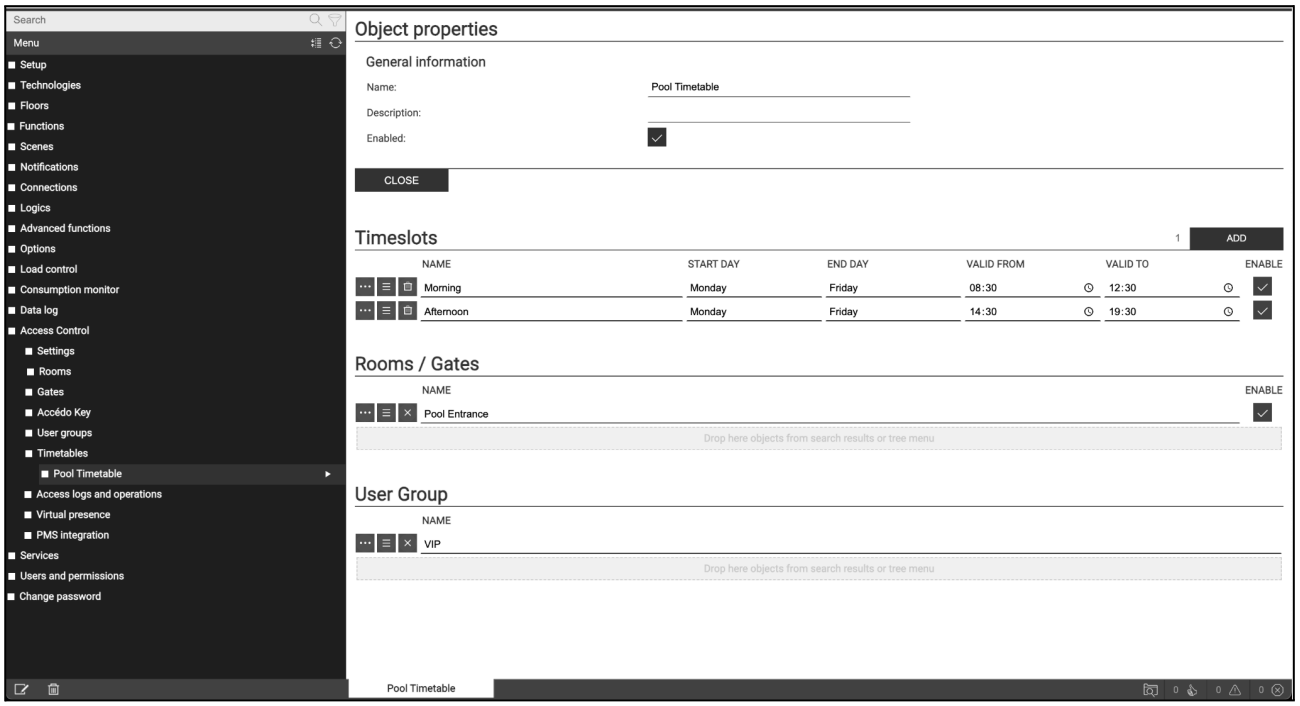
NOME	Etichetta identificativa della fascia oraria
GIORNO DI INIZIO	Giorno della settimana da cui inizia la fascia oraria
GIORNO DI FINE	Giorno della settimana in cui finisce la fascia oraria
VALIDO DA	Ora di inizio in hh:mm di validità della fascia oraria
VALIDO A	Ora di fine in hh:mm della validità della fascia oraria
ABILITA	Determina se la fascia oraria è attiva o meno

19.2.3 RESTRIZIONI

Una Fascia oraria si applica ad una o più Stanze/Varchi quando gli utenti appartenenti ad uno o più GRUPPI UTENTI tentano l'accesso.

Per applicare una restrizione ad una Stanza o Varco, si deve trascinare la stanza o il varco corrispondente nella sezione STANZE / VARCHI, e i gruppi utente a cui si vuole applicare la restrizione della fascia oraria nella lista GRUPPO UTENTI.

La figura seguente mostra un esempio di orario configurato:



20 LOG ACCESSI

Nella seguente sezione del menu di IKON SERVER

CONTROLLO ACCESSI > LOG ACCESSI

E' possibile consultare lo storico delle attività legate ai dispositivi di controllo accessi. È possibile filtrare i risultati inserendo uno o più di uno dei seguenti filtri:

DATA DA	Data di inizio per la ricerca nel log
DATA A	Data finale per la ricerca nel registro
STANZA	Una stanza specifica a cui limitare il registro
UTENTE	Utente a cui limitare il registro
TIPO	Una modalità di accesso specifica (PIN, QR Code, RFID Card)
ESITO	Il risultato di un accesso alla Stanza o Varco (ok o errore)



21 PRESENZA VIRTUALE

21.1 INTRODUZIONE

IKON SERVER è in grado di determinare la presenza di uno o più ospiti in una STANZA valutando lo stato di sensori di movimento mediante un algoritmo chiamato “VIRTUAL PRESENCE”.

Se almeno una STANZA necessita di questa funzionalità è necessario avviare l'algoritmo; è possibile abilitare la PRESENZA VIRTUALE per ogni STANZA che la richiede; non è necessario attivarla su tutte le stanze.

Affinché l'algoritmo funzioni è necessario configurare una connessione tra la/le STANZA/E ed il/i corrispondente/i sensore/i di presenza, come spiegato nei paragrafi successivi.



La PRESENZA VIRTUALE è supportata solo dalla nuova versione hardware a 4 moduli DIN di IKON SERVER.

21.2 ATTIVAZIONE E PARAMETRIZZAZIONE

Navigare nel menu di amministrazione di IKON SERVER alla sezione

CONTROLLO ACCESSI > PRESENZA VIRTUALE

e spuntare la casella “ESEGUI ALL'AVVIO”, per avviare l'algoritmo. Attivando la modalità ESPERTO () è possibile impostare i seguenti parametri per regolare l'algoritmo:

PARAMETRO	DESCRIZIONE	PREDEFINITO
TEMPO SCADENZA EVENTO BADGE [ms]	Tempo in millisecondi di attesa della tessera RFID prima della scansione successiva.	20000
TEMPO SCADENZA APERTURA/CHIUSURA PORTA [ms]	Tempo di attesa in millisecondi per un evento di apertura/chiusura della porta dopo la scansione della tessera RFID. Se questo evento non si verifica dopo il timeout, l'algoritmo VIRTUAL PRESENCE ritorna nello stato di attesa per un evento di scansione della tessera RFID.	20000
TEMPO SCADENZA RILEVAMENTO PRESENZA [ms]	Tempo di attesa in millisecondi per un evento di rilevazione da parte del sensore di movimento dopo un evento di apertura/chiusura della porta. Se il sensore non registra un evento di movimento dopo il timeout, l'algoritmo VIRTUAL PRESENCE ritorna allo stato di attesa per un evento di scansione della Tessera RFID.	20000
TEMPO RIPRISTINO SENSORE MOVIMENTO [ms]	Tempo in millisecondi per fermare e resettare la rilevazione di presenza dell'algoritmo dopo aver già rilevato una prima presenza nella stanza. Utilizzare il valore del parametro del sensore. Se il sensore non registra un evento di uscita dalla stanza, l'algoritmo VIRTUAL PRESENCE ritorna nello stato di attesa per un evento di scansione della Tessera RFID.	20000

Una volta impostate tutte le informazioni, premere il pulsante START e aspettare che lo STATO DI ESECUZIONE passi da *Fermo* a *In esecuzione*, e procedere con i passaggi successivi della configurazione come spiegato nelle sezioni seguenti.

21.3 CONFIGURAZIONE DELLA STANZA

Nella pagina dei dettagli di una STANZA, selezionare la casella ABILITA PRESENZA VIRTUALE per abilitare l'algoritmo per quella stanza; un messaggio pop-up informerà che l'algoritmo è attivato.

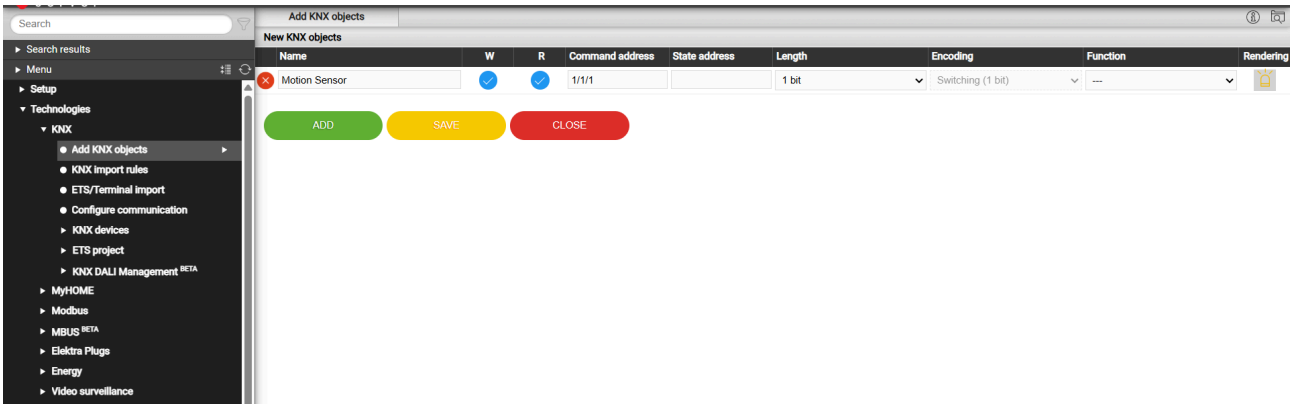
L'algoritmo VIRTUAL PRESENCE determina la presenza di un ospite nella STANZA con l'elaborazione dei segnali provenienti da un sensore porta o da sensori di movimento. Maggiore è il numero di sensori collegati, più accurato sarà l'algoritmo.

La connessione tra i sensori e l'algoritmo avviene creando *relazioni* con le PROPRIETÀ della STANZA, nella vista CONNESSIONI. In particolare le proprietà interessate sono elencate nella seguente tabella:

PROPRIETÀ	NECESSARIO	DESCRIZIONE/NOTE
SERRATURA	SÌ	Stato dell'elettroserratura. Questo è *implicito* nel comando per l'apertura della porta.
SENSORE PORTA	SÌ	Stato di un sensore collegato alla porta, che ha valore 1 (ON) quando la porta è APERTA e 0 (OFF) quando è CHIUSA.
SENSORE MOVIMENTO 1	SÌ	Stato di un sensore di movimento installato nella stanza, assegnando un valore 1 (ON) quando viene rilevato un movimento e 0 (OFF) dopo un certo tempo di non rilevamento
SENSORE MOVIMENTO 2	NO	Simile al precedente, per un secondo sensore se presente (es. sensore di movimento nel bagno)

Solitamente lo stato dei sensori viene reso disponibile tramite indirizzi di gruppo KNX. In tal caso, la procedura è la seguente:

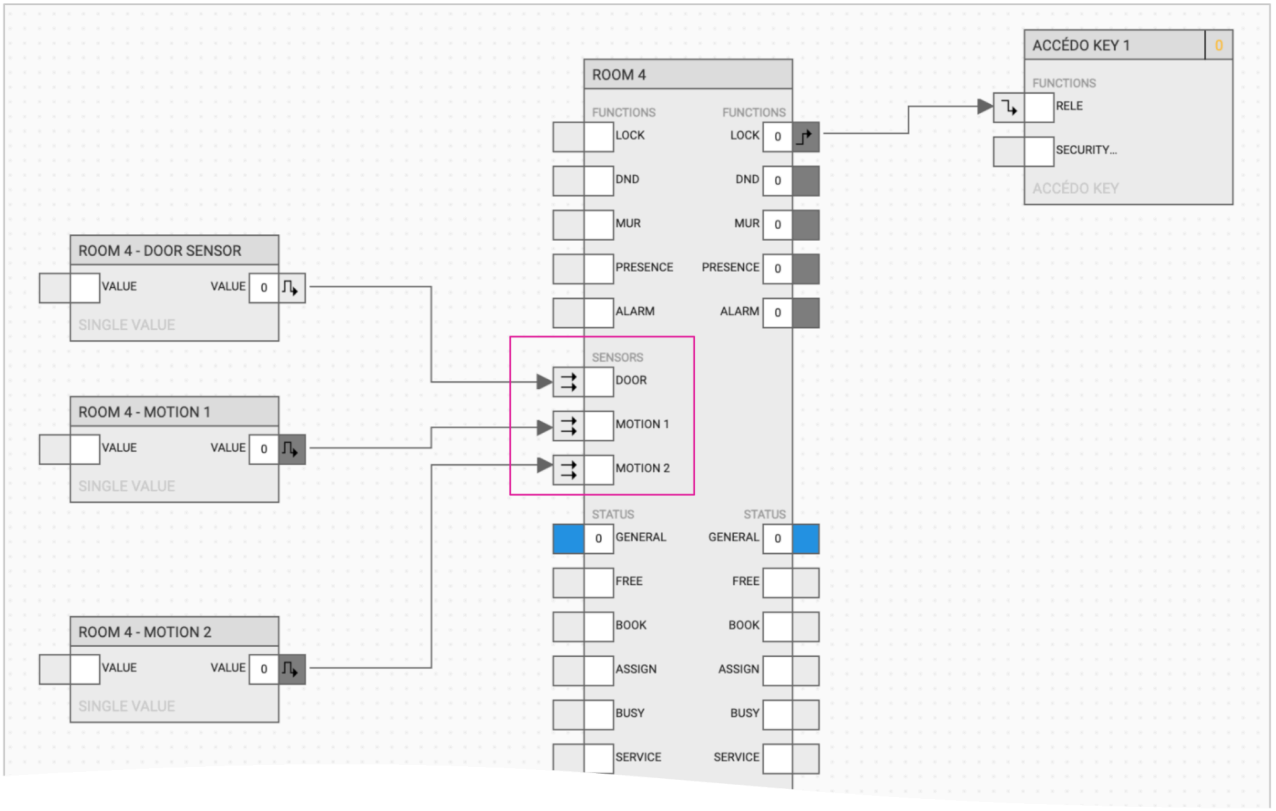
- Creare un OGGETTO KNX (in TECNOLOGIE > KNX > Aggiungi Oggetto KNX) ed entrare nella pagina dei dettagli del widget. Inserire l'indirizzo del gruppo KNX.



- Trascinare gli oggetti KNX dei sensori nell'editor CONNESSIONI della stanza.
- Disegnare una freccia (relazione) tra il sensore ed il corrispondente nodo della STANZA.

Non è necessario stabilire un collegamento con la SERRATURA perché è *implicito*.

L'immagine seguente mostra un esempio di relazione tra una STANZA e i sensori di movimento in ingresso nell'editor CONNESSIONI:



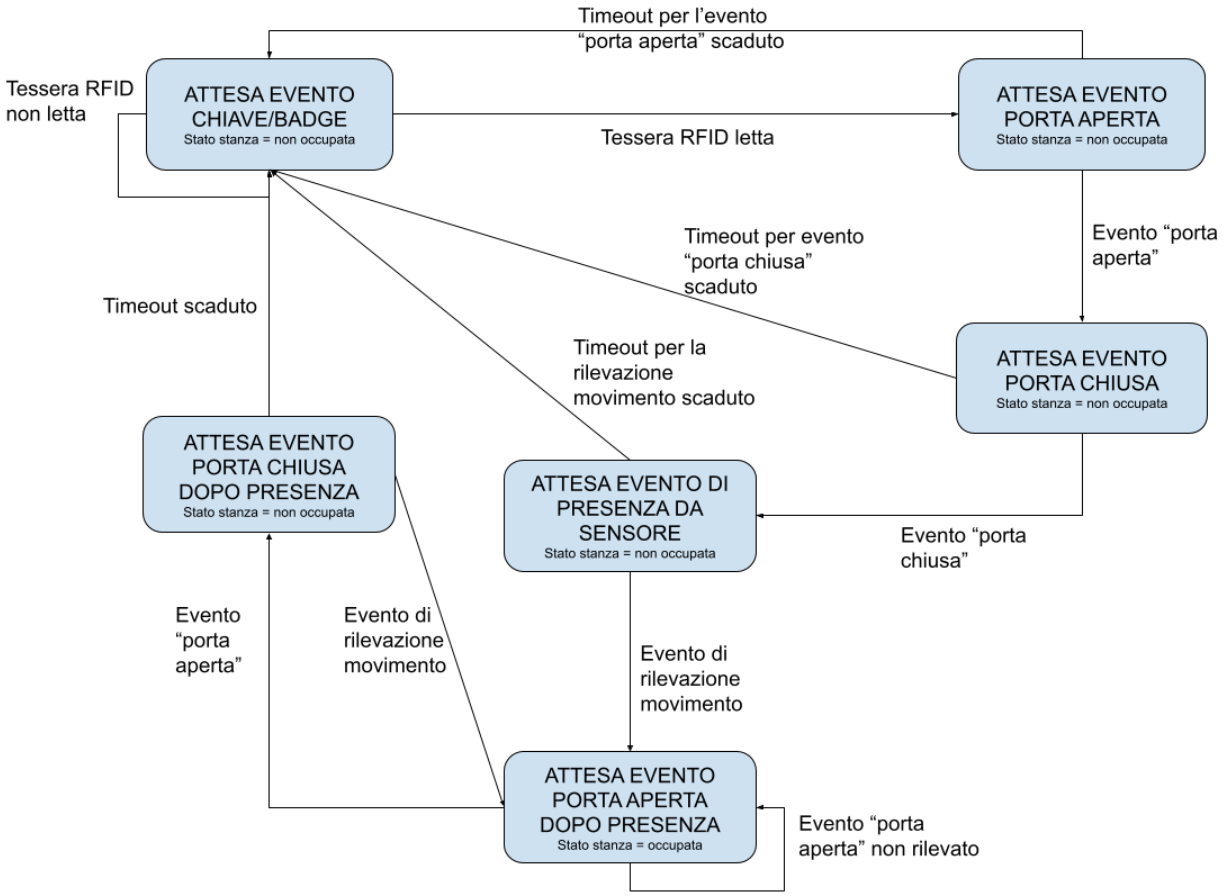
Nella sezione PRESENZA VIRTUALE della pagina di dettaglio della STANZA è possibile monitorare in quali condizioni si trova l'algoritmo, tramite l'indicatore STATO PRESENZA VIRTUALE.

I possibili stati dell'algoritmo sono:

ATTESA EVENTO CHIAVE/BADGE	L'algoritmo VIRTUAL PRESENCE è in uno stato di attesa per la lettura di una Tessera RFID.
ATTESA EVENTO PORTA APERTA	Quando viene letta una Tessera RFID valida, la PRESENZA VIRTUALE transita in uno stato di attesa per un evento di "porta aperta". Se la porta non viene aperta entro un timeout, l'algoritmo ritorna nello stato ATTESA EVENTO CHIAVE/BADGE e lo stato della stanza resta "non occupata".
ATTESA EVENTO PORTA CHIUSA	Se la porta viene aperta dopo la lettura di una tessera RFID, l'algoritmo VIRTUAL PRESENCE va in uno stato di attesa per un evento di "chiusura porta". Se la porta non viene chiusa entro un timeout, l'algoritmo ritornerà nello stato ATTESA EVENTO CHIAVE/BADGE e lo stato della stanza resta "non occupata".
ATTESA EVENTO DI PRESENZA DA SENSORE	Se nello stato ATTESA EVENTO PORTA CHIUSA la porta viene chiusa, l'algoritmo attenderà un rilevamento di movimento dal sensore di movimento. Se dopo un timeout il sensore non rileva alcun movimento nella stanza l'algoritmo ritornerà nello stato ATTESA EVENTO CHIAVE / BADGE e lo stato della stanza resta "non occupata", altrimenti la stanza passerà nello stato "occupata".

ATTESA EVENTO PORTA APERTA DOPO PRESENZA	Se nello stato ATTESA EVENTO DI PRESENZA DA SENSORE l'algoritmo rileva tramite un sensore di movimento la presenza dell'ospite nella stanza, la stanza sarà nello stato “occupata” e la PRESENZA VIRTUALE rimarrà in uno stato di inattività finché non si verifica un evento di “porta aperta”.
ATTESA EVENTO PORTA CHIUSA DOPO PRESENZA	Se, mentre l'algoritmo è nello stato ATTESA EVENTO PORTA APERTA DOPO PRESENZA, viene rilevato un evento di “porta aperta”, l'algoritmo entrerà in uno stato di attesa per un evento di “porta chiusa”. Se la porta non viene chiusa dopo un timeout, l'algoritmo entra in uno stato di attesa per un evento di rilevamento del sensore di movimento nella stanza. Se in questo stato l'algoritmo non riceve alcuna rilevazione di movimento dopo un timeout, la stanza passa nello stato “non occupata” e l’algoritmo tornerà nello stato ATTESA EVENTO CHIAVE/BADGE.

L'immagine seguente rappresenta lo Stato Macchina dell'algoritmo:



22 INTEGRAZIONE CON PMS

22.1 INTRODUZIONE

IKON SERVER può essere integrato con un PMS (Property Management System) per centralizzare tutte le funzioni di controllo accessi in un'unica UI. In questa condizione, IKON SERVER funziona “in background” senza la necessità di interagire con le pagine web o app.

L'integrazione PMS richiede uno specifico voucher di licenza.

22.2 FIAS

IKON SERVER è compatibile con **Oracle® Micros® Opera™ Hotel Property Management System** attraverso il **FIAS** (Fidelio Interface Application Specification). Un SERVER FIAS deve soddisfare i seguenti requisiti di compatibilità per essere raggiungibile dal IKON SERVER e stabilire una connessione:

PMS	• Opera 5 (On-Premise / Hosted) • Opera Cloud • Fedelio Suite8
INTERFACCIA	Famiglia Key Services System (Door Locking)
VERSIONE DEL SISTEMA DEL FORNITORE	1.10
CONNETTIVITÀ	TCP/IP

22.2.1 OPERAZIONI E COMANDI SUPPORTATI

Sono supportate le seguenti operazioni dal PMS:

PRENOTAZIONE	Assegnazione di una o più stanze ad un ospite prima dell'inizio del periodo di validità di soggiorno.
CHECK-IN	Abilitazione immediata all’accesso di una o più stanze ad un ospite.
MODIFICA	Cambio di una stanza e periodo di permanenza per un ospite esistente.
CHECK-OUT	Disabilitazione dell’accesso ad una o più stanze ad un ospite.

Nella tabella di seguito sono elencati i comandi del protocollo FIAS sono supportati da IKON SERVER:

COMANDO	CAMPO	DESCRIZIONE
KR - Key Request (richiesta tessera per prenotazione, check-in)	KC	Key Coder (obbligatorio nel protocollo FIAS, ma non utilizzato)
	WS	ID workstation (obbligatorio nel protocollo FIAS, ma non utilizzato)
	DA	Data attuale
	TI	Ora corrente
	KT	Key Type (Tipo di tessera). Può essere N per creare una nuova Tessera RFID, D per creare un duplicato della Tessera RFID per un numero di prenotazione esistente.
	RN	Room Number (Numero della stanza)

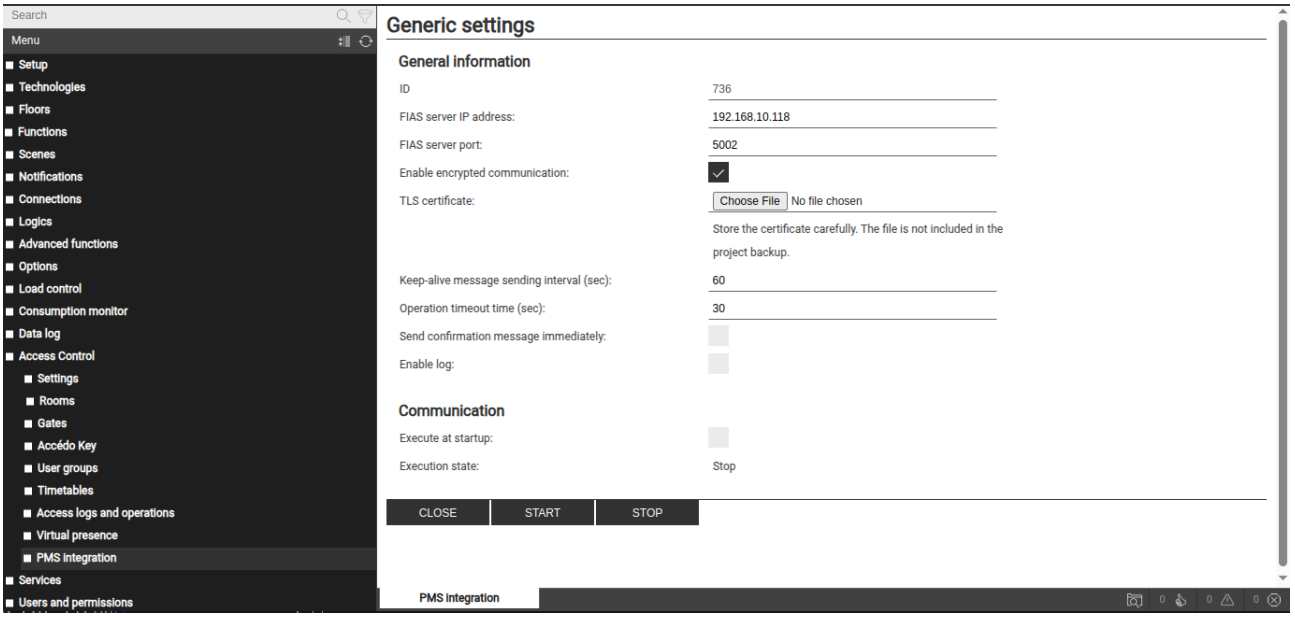
	SI	Suite Info (stanze addizionali)
	GA	Guest Arrival date (data di arrivo dell'ospite)
	GD	Guest Departure date (data di partenza dell'ospite)
	G#	Numero di prenotazione
KD - Key Delete (cancellazione tessera per check-out)	KC	Key Coder (obbligatorio nel protocollo FIAS, ma non utilizzato)
	WS	ID workstation (obbligatorio nel protocollo FIAS, ma non utilizzato)
	DA	Data attuale
	TI	Ora corrente
	RN	Room Number (Numero della stanza)
	SI	Suite Info (stanze addizionali)
	G#	Numero di prenotazione
KM - Key Data Change (modifica dei dati della tessera per modificare prenotazioni)	KC	Key Coder (obbligatorio nel protocollo FIAS, ma non utilizzato)
	WS	ID workstation (obbligatorio nel protocollo FIAS, ma non utilizzato)
	DA	Data attuale
	TI	Ora corrente
	RO	Old Room Number (numero della stanza vecchio)
	RN	Room Number (numero della stanza nuova)
	UO	Old additional rooms (eventuali vecchie stanze aggiuntive)
	SI	Suite Info (eventuali nuove stanze aggiuntive)
	GA	Guest Arrival date (data di arrivo dell'ospite)
	GD	Guest Departure date (data di partenza dell'ospite)
	G#	Numero di prenotazione

Tutti gli altri comandi/campi eventualmente ricevuti vengono ignorati.

22.2.2 CONFIGURAZIONE

Nel menù IKON SERVER navigare alla sezione

CONTROLLO ACCESSI > INTEGRAZIONE PMS



In questa pagina è possibile configurare le seguenti impostazioni; alcune delle seguenti informazioni richiedono la modalità ESPERTO ( ) per essere visibili (tali campi sono mostrati qui tra parentesi):

INFORMAZIONI GENERALI

INDIRIZZO IP DEL FIAS	Indirizzo IP del server FIAS
PORTA DI ASCOLTO DEL FIAS	Porta di ascolto del server FIAS
ABILITA COMUNICAZIONE CIFRATA	Quando selezionato, la comunicazione è crittografata.
(CERTIFICATO TLS)	Solo se è impostato il flag "Abilita comunicazione crittografata". Se si utilizza una connessione crittografata, è richiesto un certificato TLS. Con questa opzione il certificato generato dal PMS può essere aggiornato sul server.
(INTERVALLO DI INVIO MESSAGGI DI KEEP-ALIVE (sec))	Definisce quanti secondi devono passare tra un messaggio keep-alive e l'altro. Si consiglia di mantenere il valore predefinito (60 secondi).
(TEMPO DI TIMEOUT OPERAZIONE (sec))	Definisce per quanti secondi l'integrazione deve considerare l'operazione richiesta non riuscita prima di inviare un messaggio di errore al PMS. Si consiglia di lasciare il valore predefinito (30 secondi).
(INVIA SUBITO MESSAGGIO DI CONFERMA)	Se l'opzione è contrassegnata, un messaggio di OK al PMS verrà inviato subito dopo la ricezione del comando. In caso contrario, verrà inviata una risposta solo quando l'intera operazione sarà stata completata. Si consiglia di mantenere il valore predefinito (non contrassegnato).
(ABILITA LOG)	Abilita i log di debug. Utilizzato dall'assistenza tecnica.

COMUNICAZIONE

ESEGUI ALL'AVVIO	Spuntare questa casella per avviare il gateway FIAS con il webserver
STATO DI ESECUZIONE	Informa sullo stato del gateway FIAS (stop o play)

Premere il pulsante START per abilitare e avviare una comunicazione con il server FIAS.



Affinché l'integrazione funzioni correttamente, è importante che il NUMERO delle CAMERE configurate in IKON SERVER corrisponda al numero di camere nel PMS. Si prega di verificare questo aspetto prima di iniziare la comunicazione con il PMS.

22.2.3 UTILIZZO

Una volta configurato e abilitato, il modulo di integrazione si collegherà al software PMS e attenderà i comandi da esso emessi.
Quando la funzionalità di Controllo Accessi del IKON SERVER è controllata da un PMS, solo le tessere RFID possono essere utilizzate per accedere ad una Stanza. Altri metodi di accesso (QR Code e PIN) non sono attualmente supportati.

Per configurare il IKON SERVER e i lettori di Tessere RFID (ACCÉDO KEY, DICO o dispositivi di terze parti) utilizzare le procedure descritte in questo manuale nei capitoli relativi agli ACCÉDO KEY e DICO.

Quando viene ricevuto un comando dal PMS:

- In caso di prenotazione di un ospite, check-in o richiesta di duplicato della tessera RFID, il webserver attenderà che una tessera RFID venga posizionata su uno dei lettori abilitati. Una volta abilitata, la tessera potrà essere utilizzata dall'ospite per accedere alla Stanza e ai Varchi durante il suo periodo di permanenza.
- In caso di richiesta di modifica della prenotazione da parte dell'ospite, la tessera RFID associata all'ospite durante la procedura di prenotazione verrà modificata di conseguenza (ad esempio, cambiando il numero della Stanza di un ospite da 2 a 3, la Tessera RFID sarà in grado di aprire la Stanza 3, ma non più la Stanza 2).
- In caso di richiesta di check-out o di cancellazione della prenotazione, tutte le Tessere RFID associate all'ospite smetteranno di funzionare per qualsiasi serratura.

23 UTILIZZO DELLA VISTA “*VISUALIZATION*”

23.1 INTRODUZIONE

Nella vista *Visualisation* del IKON SERVER, entrando nella sezione CONTROLLO ACCESSI del menù di navigazione, verrà visualizzata la seguente schermata (su PC/MAC o Smartphone):



Tutte le opzioni danno accesso a tutte le sezioni necessarie alla gestione degli ospiti, delle camere, ecc. Alcune opzioni potrebbero mancare a seconda della configurazione effettuata dall'installatore/integratore di sistema.

23.2 OSPITI

In quest'area è possibile creare o modificare gli ospiti della struttura, e gestire tutti i relativi permessi di accesso; questa è la sezione “core” della gestione del controllo degli accessi.

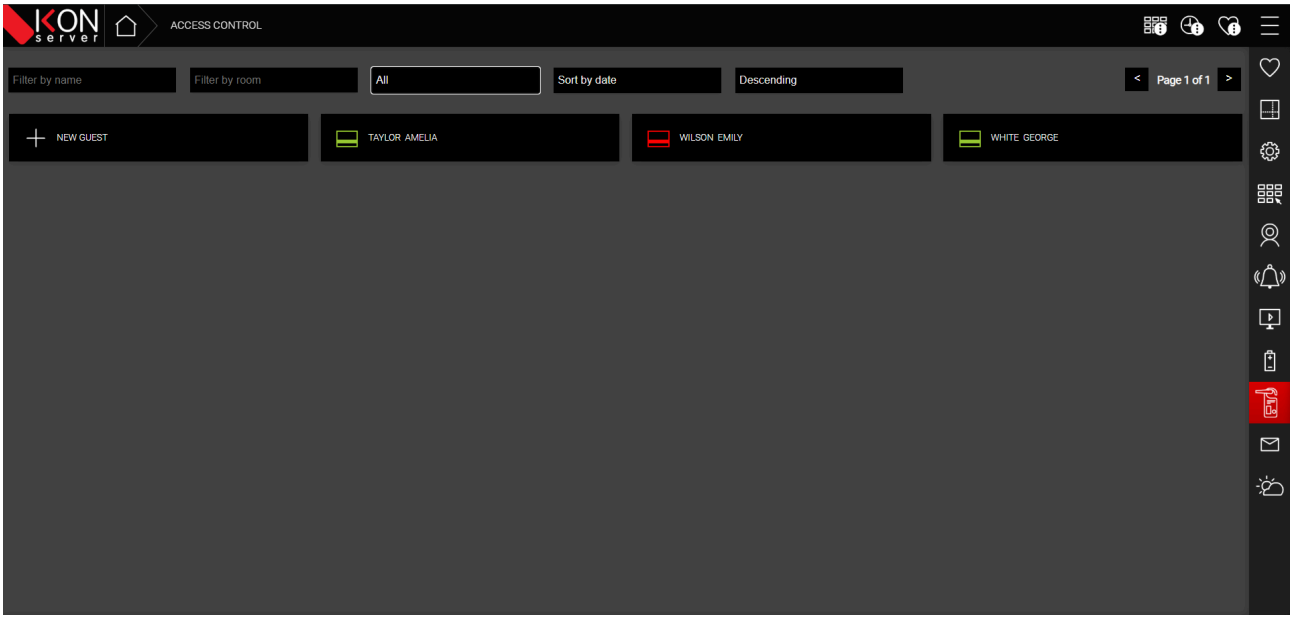
23.2.1 ELENCO DEGLI OSPITI

Entrando nella sezione viene visualizzato l'elenco degli ospiti (se presenti), con la possibilità di filtrare l'elenco in base ad uno o più tra i seguenti criteri:

FILTRA PER NOME	In questo form è possibile inserire una o più parole chiave (nome e cognome) da cercare
FILTRA PER STANZA	In questo form è possibile inserire il numero della stanza assegnata all'ospite che si sta cercando.
ABILITATO	Menù a tendina che permette di selezionare uno dei possibili stati di un ospite: ● Abilitato ● Disabilitato ● Tutti

I risultati del filtro possono essere ordinati con i seguenti criteri (entrambi i criteri sono menu a tendina):

ORDINA PER	Uno dei seguenti campi: • Data • Nome
ORDINE DI ORDINE	Crescente o decrescente



23.2.2 AGGIUNTA DI UN NUOVO OSPITE

Premendo il pulsante NUOVO OSPITE viene visualizzato un menu pop-up, dove è possibile inserire tutte le informazioni relative al nuovo ospite. Ci sono tre finestre principali da popolare con le informazioni dell'Ospite:

ANAGRAFICA

NOME	Nome dell'ospite
COGNOME	Cognome dell'ospite
GRUPPO	Selezionare il Gruppo Utente a cui l'ospite deve appartenere. Il gruppo di utenti determina i permessi e l'eventuali limitazioni (tramite fasce orarie) di accesso a Stanze o Varchi.
INDIRIZZO E-MAIL	Inserire l'indirizzo email dell'Ospite.
NUMERO DI TELEFONO	Inserire il numero di telefono dell'ospite, senza spazi né punteggiatura.
GENERE	Seleziona l'opzione appropriata tra M (maschio) o F (femmina)

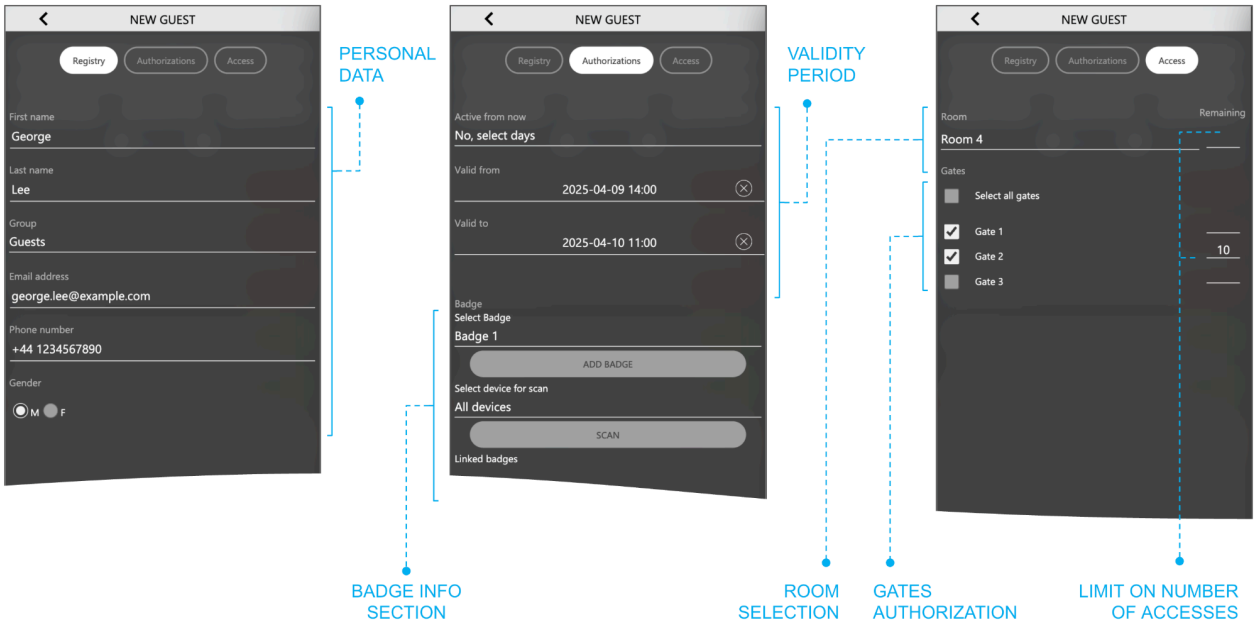
AUTORIZZAZIONI

ATTIVO DA SUBITO	Questo campo può essere: • Sì (valido dalla data e ora attuali. È necessario impostare solo una data di fine permanenza) • No (deve essere impostata una data di inizio ed un giorno di fine per la validità della permanenza dell'ospite)
VALIDO DA	Inserisci la data/ora di inizio del periodo di validità.

	L'ospite avrà diritto ad entrare nella struttura solo a partire da tale periodo.
VALIDO A	Inserisci la data/ora di fine del periodo di validità. Da tale giorno l'ospite non avrà più diritto ad accedere alla struttura.
INFORMAZIONI SULLA TESSERA RIFD	Visibile solo se è stata selezionata l'opzione ABILITA GESTIONE BADGE. Permette al gestore della struttura di assegnare ad un Ospite una Tessera RFID oppure di scansionare una Tessera RFID per l'Ospite.

ACCESSI

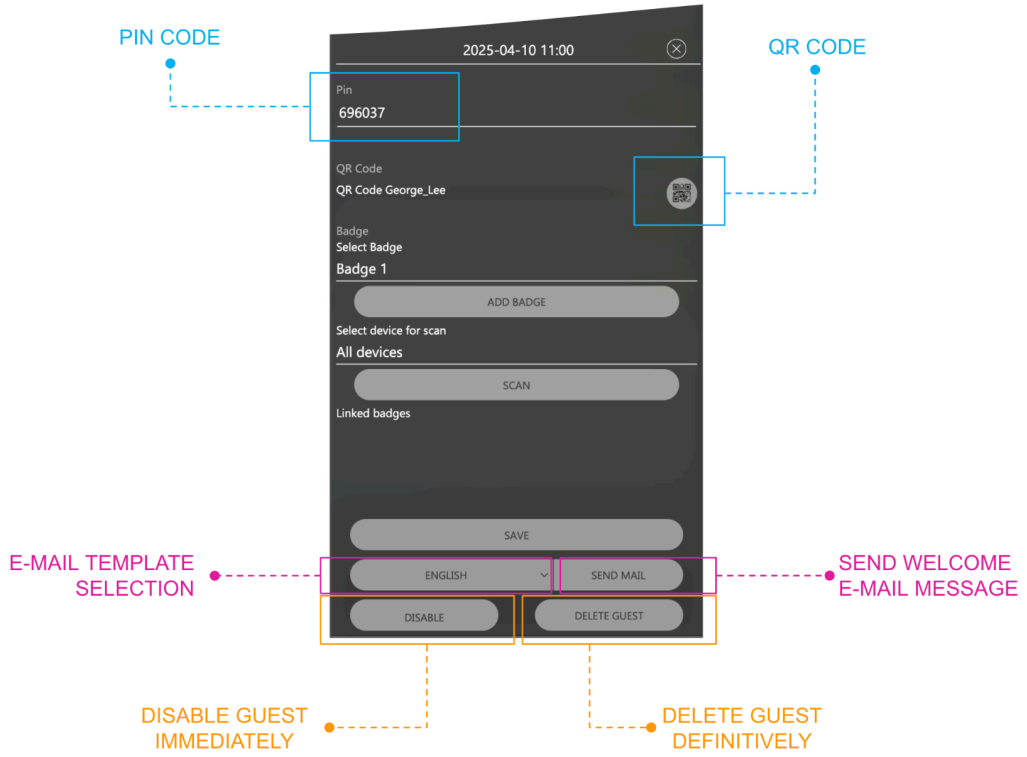
STANZA	Un menù a tendina che permette all'utente di selezionare e assegnare ad un ospite una delle Stanze disponibili. Un ospite può anche non essere associato ad una stanza.
VARCHI	Elenco di tutti i Varchi che sono disponibili e a cui un ospite può accedere. Un ospite può anche non essere associato ad un varco.
RIMANENTI	Se l'opzione ABILITA LIMITE SUL NUMERO DEGLI ACCESSI è stata selezionata, è possibile digitare per ogni stanza o varco, un numero limitato di volte affinché l'ospite possa entrare in quella stanza o varco.



Premendo il pulsante CREA, il nuovo ospite viene aggiunto al sistema, ed eventualmente abilitato (se sono valide le date selezionate nella finestra Autorizzazioni).

Se un Ospite non è stato assegnato ad una Stanza o Varco e il gestore della struttura crea l'Ospite, il sistema mostrerà pop-up con un messaggio che informa l'utente che il nuovo Ospite è stato creato ma non ha accesso ad alcuna Stanza o Varco.

Dopo la creazione, nella scheda AUTORIZZAZIONI vengono generati un PIN casuale (6 cifre) ed un QR CODE (a seconda della modalità di accesso scelta per la struttura in fase di configurazione) che vengono assegnati all'ospite:



E' possibile modificare il PIN con una sequenza preferita di 6 cifre. Premere il pulsante SALVA dopo averlo modificato, ed eventualmente inviare l'e-mail di benvenuto.

Dopo la creazione del Guest, nel pop-up diventeranno visibili i seguenti elementi:

SELETTORE DEL MODELLO DI E-MAIL	Quando sono stati creati più modelli di email (ad esempio una mail di benvenuto in più lingue), il menu a tendina consente la selezione prima dell'invio all'ospite la mail che si vuole inviare
INVIA MAIL	Invia un'email di benvenuto all'ospite.
DISABILITA	Permette di disabilitare immediatamente l'ospite, anche durante il periodo di validità.
ELIMINA OSPITE	Rimuove definitivamente l'ospite dal sistema.

Per l'autorizzazione con Tessera RFID fare riferimento al capito BADGE.

23.2.3 E-MAIL DI BENVENUTO

Alla pressione del pulsante INVIA MAIL, il IKON SERVER invierà una e-mail di benvenuto all'ospite a partire da quella selezionata con il SELETTORE DEL MODELLO E-MAIL (il modello deve essere prima creato nel menu E-MAIL DI BENVENUTO), sostituendo il *tag dinamici* con i dati dell'ospite e della struttura.

L'e-mail conterrà le seguenti informazioni utili per l'accesso alla struttura (secondo quanto configurato nella pagina web Amministrazione e modalità di accesso):

- Il PIN numerico, digitabile sul DICO o sull'ACCÉDO KEY.
- Il QR CODE, che può essere scansionato (da un foglio stampato o dallo smartphone) davanti alla wbcam del DICO o dell'ACCÉDO KEY.

23.3 STANZE

Questa sezione contiene tutte le stanze configurate nella vista *Administration* del IKON SERVER. Per ogni Stanza viene visualizzato il nome e, se abilitati nella sezione PROPRIETÀ della configurazione Stanza, i relativi pittogrammi (Presenza virtuale, Non disturbare, Allarme, Pulizia stanza e Stato della stanza).

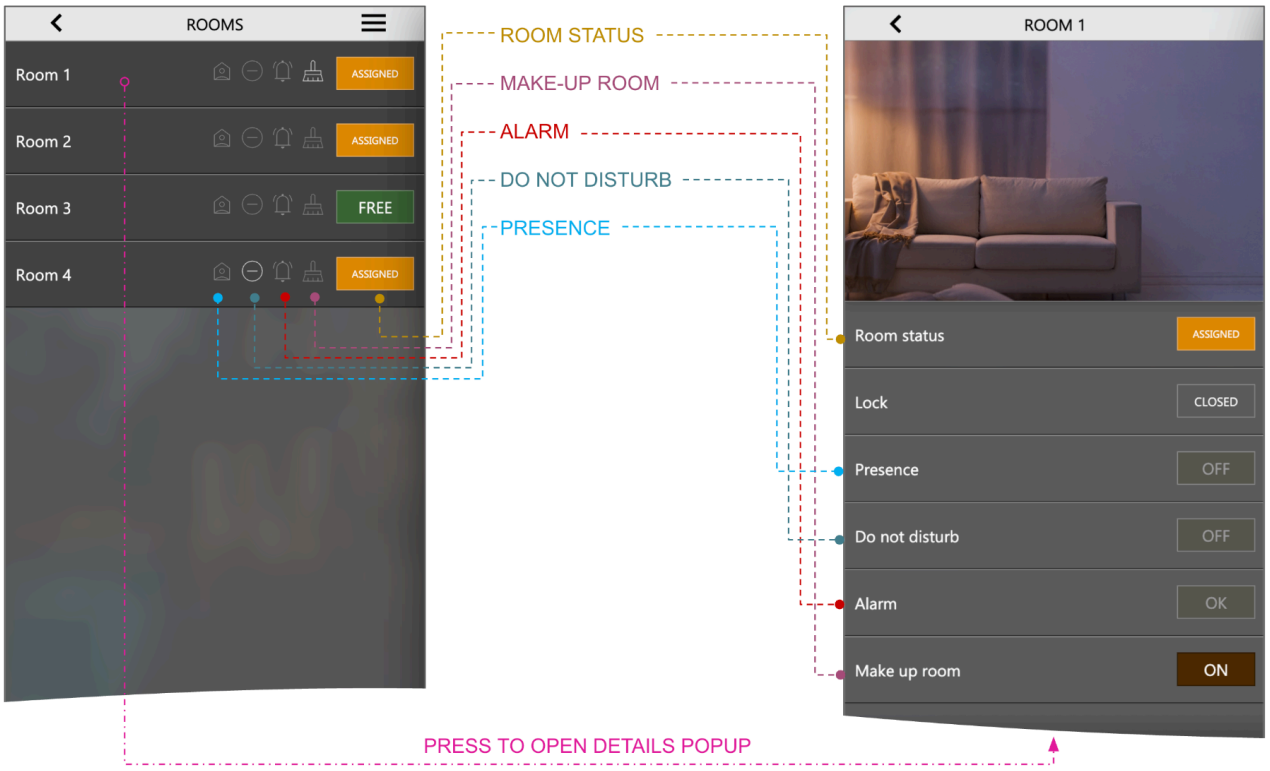
Cliccando su una stanza, il sistema aprirà una finestra pop-up che dettaglia tutti i pittogrammi:

<table>
<tr><td>STATO STANZA</td><td>Può essere uno dei seguenti:

<table><tr><td>LIBERA</td><td>Disponibile per nuovi ospiti</td></tr><tr><td>PRENOTATA</td><td>Riservata ad un ospite che non è ancora nel periodo di validità</td></tr><tr><td>ASSEGNATA</td><td>Riservato ad un ospite nel periodo di validità (presumibilmente presente nella struttura)</td></tr><tr><td>OCCUPATA</td><td>L'ospite è all'interno della stanza</td></tr><tr><td>SERVICE</td><td>Stanza da pulire o in manutenzione</td></tr><tr><td>N.D.</td><td>Nessuno dei precedenti</td></tr></table></td></tr>
<tr><td>SERRATURA</td><td>Lo stato della serratura elettrica. Normalmente chiuso (CHIUSA).</td></tr>
<tr><td>PRESENZA</td><td>Indica la presenza dell'ospite/i nella stanza.</td></tr>
<tr><td>NON DISTURBARE</td><td>La richiesta da parte dell'ospite di non essere disturbato dal personale.</td></tr>
<tr><td>ALLARME</td><td>Lo stato del sensore di allarme interno (e.g., allarme bagno).</td></tr>
<tr><td>PULIZIA STANZA</td><td>La richiesta da parte dell'ospite di effettuare una pulizia aggiuntiva della stanza.</td></tr>
</table>

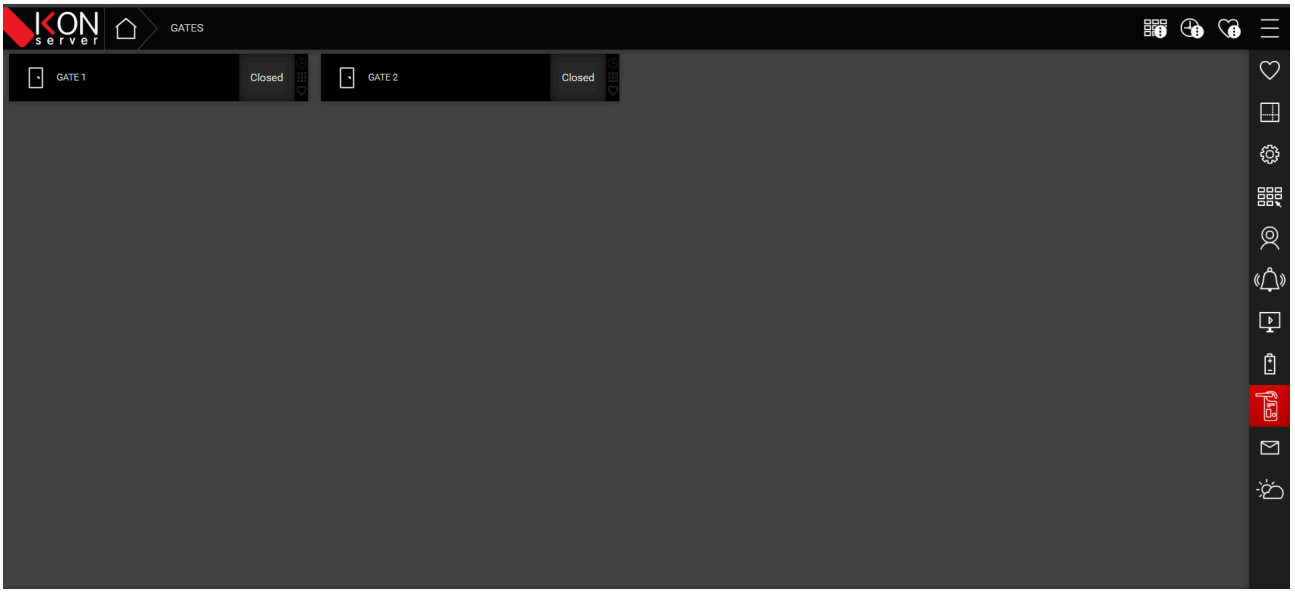
Le seguenti proprietà possono essere comandate direttamente dal popup dei dettagli:

- SERRATURA (per aprire la porta a distanza).
- Non disturbare.
- Pulizia stanza.



23.4 VARCHI

Questa sezione è simile alle STANZE, ma contiene tutti i VARCHI. In questo caso la porta può essere aperta direttamente premendo l'elemento rettangolare presente nell'elenco.

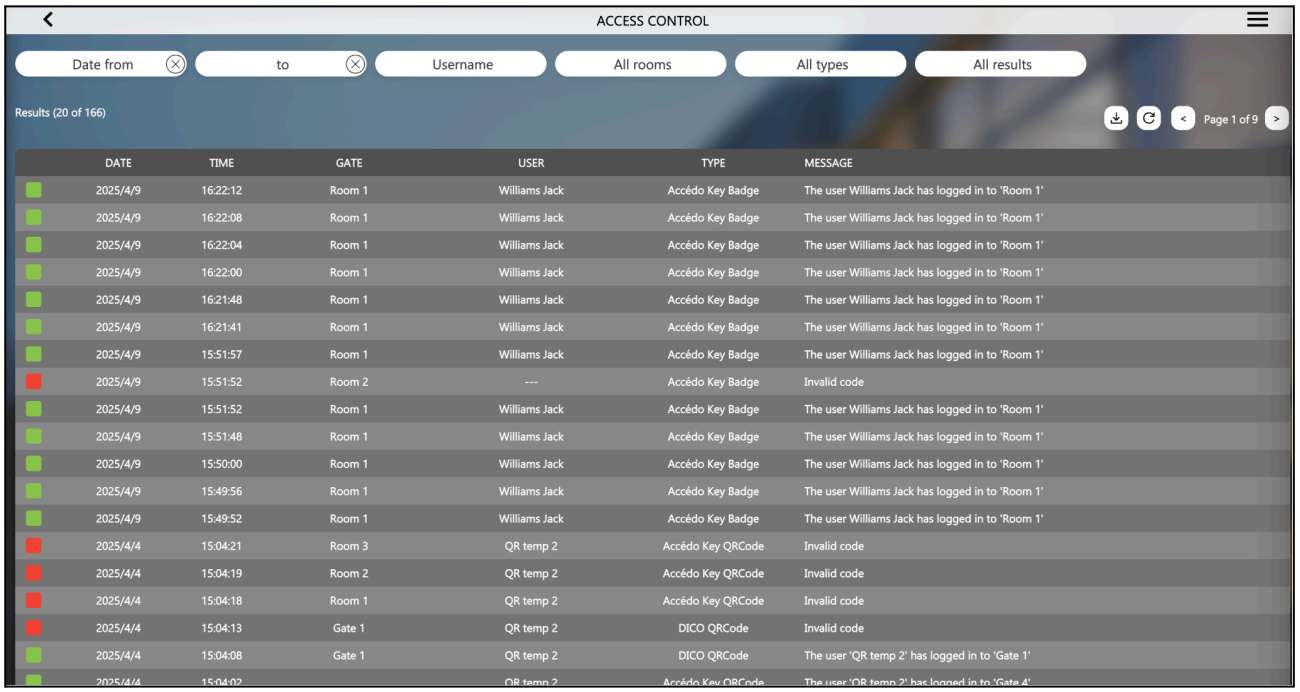


23.5 LOG ACCESSI

Questa sezione contiene lo storico di tutti gli accessi effettuati alle Stanze o ai Varchi. È lo stesso log presente nella vista Administration. E' possibile applicare i seguenti filtri:

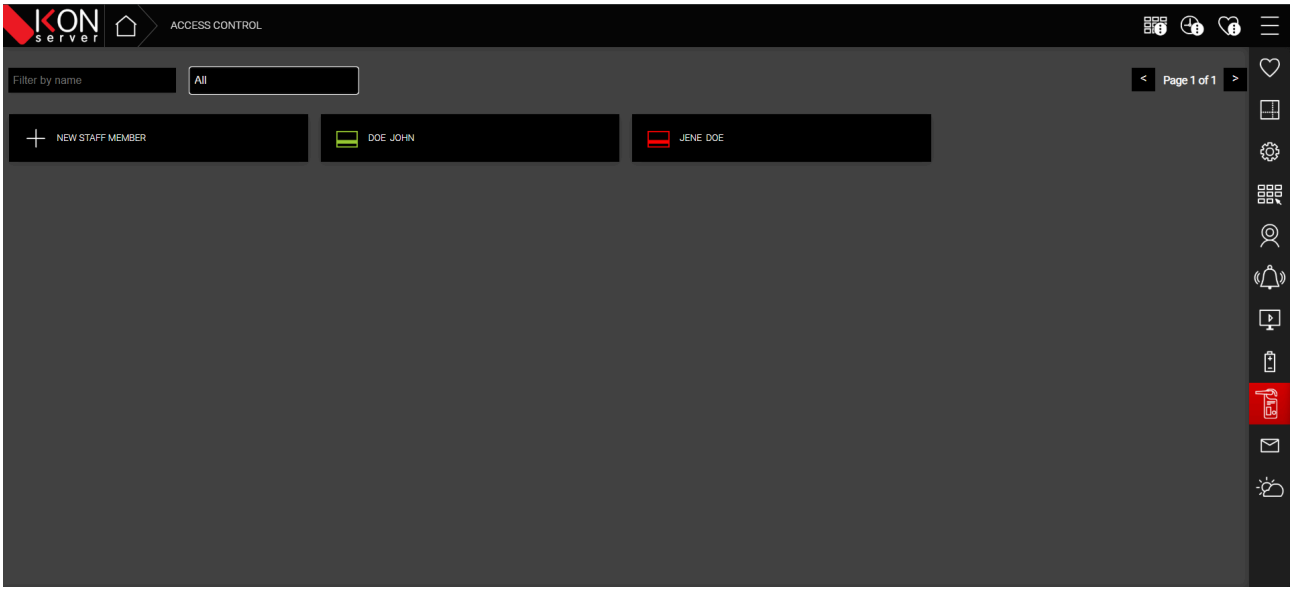
DATA DA DATA A	Intervallo delle date

NOME UTENTE	Una o più parole chiave (nome e cognome) dell'ospite da cercare
PUNTO DI ACCESSO	Menu a tendina che permette di selezionare il punto di accesso (Stanza, Varco o tutto) per cui si vuole avere il log
TIPO	La modalità di accesso (o il tentativo di accesso) utilizzata. Può essere il QR Code, la tessera RFID o il PIN.
RISULTATO	Permette di restringere la ricerca ai transiti riusciti o falliti (ok o errore)



23.6 PERSONALE

Questa sezione è simile all'area OSPITI, ma è dedicata alla creazione del personale di servizio della struttura. La differenza tra membri dello staff e ospiti, è che i membri dello staff possono essere associati a più stanze (in modo da poter entrare potenzialmente in tutte).



23.7 QR CODE TEMPORANEI

Questa sezione permette la creazione di QR CODE non legati ad uno specifico ospite o membro dello staff e utilizzabili solo per un periodo limitato (es. gli addetti alla manutenzione devono accedere ad una o più camere della struttura).

Nel popup che appare quando si clicca CREA QR CODE è possibile impostare le seguenti informazioni:

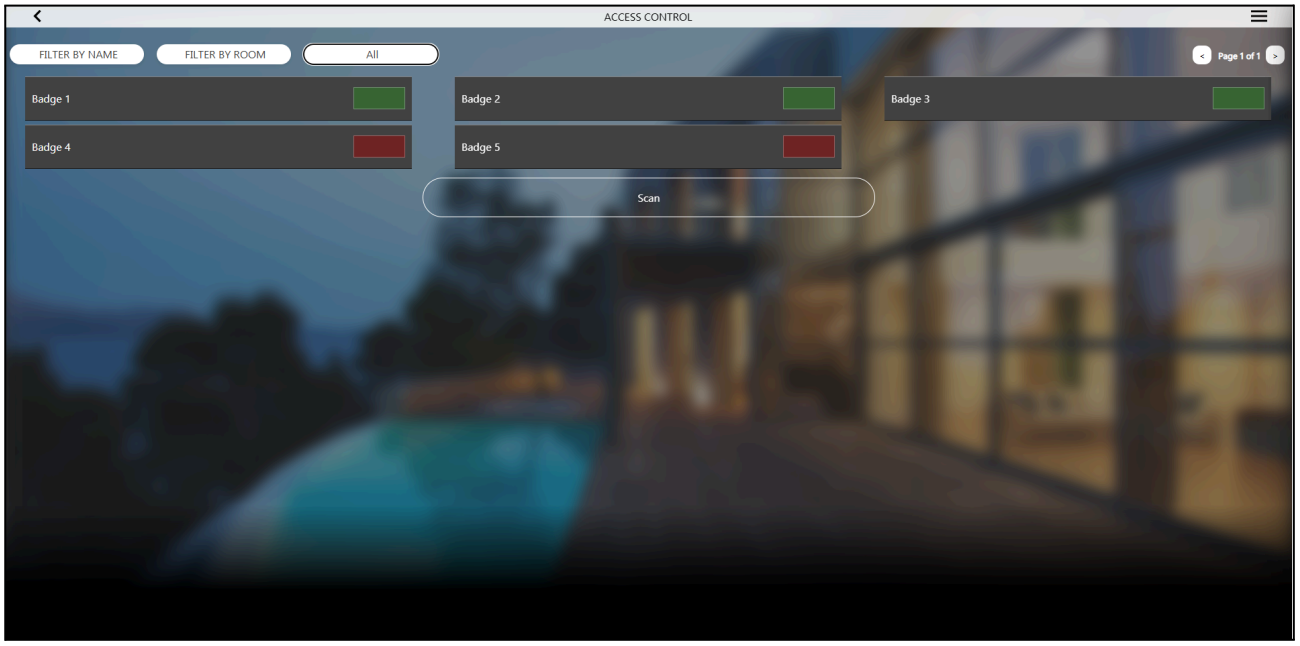
NOME	Etichetta utile per identificare il QR CODE
INDIRIZZO EMAIL	La mail a cui inviare il QR Code (se desiderato)
VALIDO DA	Data e ora di inizio del periodo di validità del codice QR
VALIDO A	Data e ora di fine del periodo di validità del codice QR
STANZA	Elenco di checkbox delle Stanze per le quali è possibile assegnare il QR Code per accedere.
VARCHI	Elenco di checkbox dei Varchi per i quali è possibile assegnare il QR Code per accedere.

Quando si genera il QR Code dopo aver cliccato CREA Sono disponibili i seguenti pulsanti:

SALVA	Conferma le eventuali modifiche al QR CODE.
INVIA QR CODE VIA MAIL	Se viene inserito un indirizzo e-mail, consente all'utente di inviare la email con il QR Code.
STAMPA	Apre in una nuova tab del browser il QR CODE con un formato adatto alla stampa.
ELIMINA QR CODE	Elimina il codice QR temporaneo.

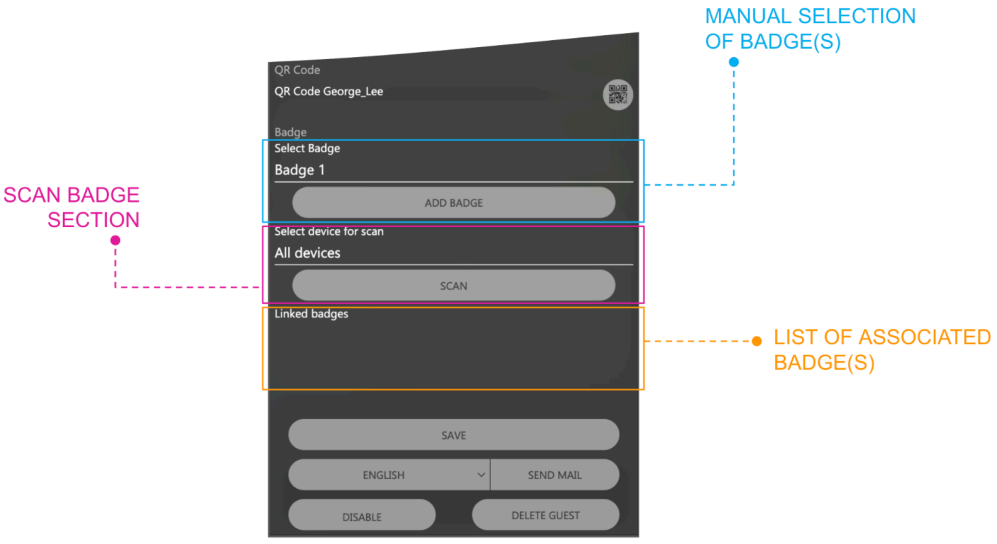
23.8 BADGE

Questa sezione della *Visualisation* del IKON SERVER permette all'utente di visualizzare tutte le tessere RFID create o di generare una nuova tessera RFID. Le Tessere RFID sono compatibili con lo standard MIFARE con frequenza 13,56 MHz. La modalità di accesso alla struttura tramite Tessera RFID deve essere abilitata nella schermata *Administration*.



Cliccando sul pulsante SCAN il sistema aprirà un pop-up in cui verrà visualizzato quale dispositivo (DICO o ACCÉDO KEY) l'utente desidera utilizzare per scansionare la Tessera RFID. Dopo aver scelto il dispositivo e premuto nuovamente SCAN, il sistema aprirà un nuovo pop-up con un messaggio informativo che chiederà all'utente di far passare la Tessera RFID sul dispositivo. Una volta letta la tessera un messaggio chiederà conferma all'utente per aggiungere la tessera. Dopo la conferma la carta verrà aggiunta alla lista delle tessere RFID utilizzabili.

È possibile garantire l'accesso alla struttura anche dalla creazione Ospite o Personale, assegnando agli ospiti e al personale una o più Tessere RFID. La parte del popup dedicata a questa modalità di accesso è composta dalle seguenti sezioni:



SELEZIONE MANUALE DEL/I BADGE	Se questa sezione è attivata nella vista *Administration*, il menu a tendina permette all'utente di selezionare da un elenco tutte le Tessere RFID precedentemente create. Premere il pulsante AGGIUNGI BADGE dopo la selezione, per aggiungerlo all'elenco BADGE COLLEGATI.

	Nota: questo approccio è particolarmente indicato per strutture con un numero limitato di Tessere RFID.
SEZIONE SCANSIONE BADGE	Se più di un ACCÉDO KEY è abilitato alla scansione di una tessera, selezionare dal menu a tendina il dispositivo prima di effettuare una SCAN, altrimenti lasciare l'opzione “tutti i dispositivi”. Premere il pulsante SCAN e posizionare la Tessera RFID davanti al dispositivo; una volta rilevato, viene aggiunto all'elenco BADGE COLLEGATI. Se la tessera RFID scansionata è già nel sistema, verrà eventualmente visualizzato un messaggio di errore.
ELENCO DEI BADGE COLLEGATI	In questa sezione è presente l'elenco delle Tessere RFID associate all'ospite (o al membro dello staff).