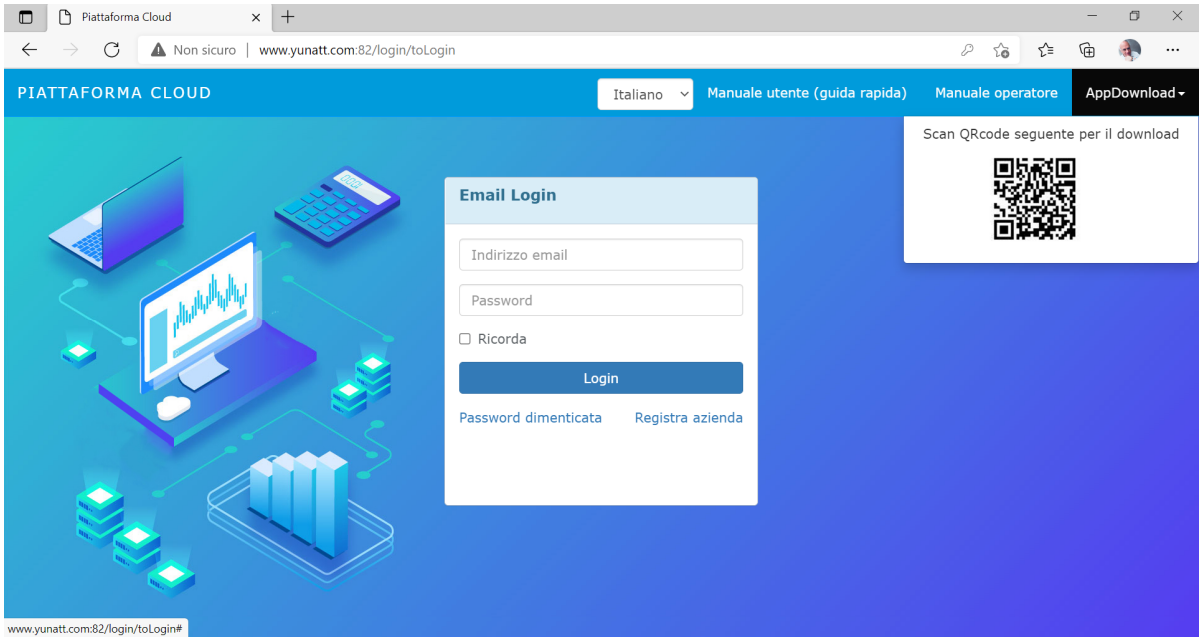


Software Cloud per Terminali GP08L

Guida Utilizzatore

Versione 3.1, Agosto 2021

© *2007 – 2021 DoingSecurity*, all rights reserved

ING. GIANNI SABATO
Via S. Stefano 74, I-40125 Bologna
GSM +39 335 238046
Ph. +39 051 6211553
Fax +39 051 3370960
E-mail: info@doingsecurity.it
Web: www.doingsecurity.it

DOINGSECURITY si riserva il diritto di apportare qualunque cambiamento al presente manuale in qualunque parte senza preavviso scritto.

DoingSecurity SAS ha dedicato il massimo sforzo per assicurare che il presente documento sia preciso nelle informazioni fornite; tuttavia, DoingSecurity SAS non si assume alcuna responsabilità per eventuali errori ed omissioni, con ciò includendo qualsiasi danno risultante dall'uso delle informazioni contenute nel presente manuale.

Assistenza tecnica Tel.: +39 329 2288344 / +39 051 6211553

Tel.: +39 335 238046 email: info@doingsecurity.it

Indice

1 Introduzione

Il presente Manuale descrive come utilizzare il software in cloud per il Terminale GP08 per la gestione accessi "Green Pass". Il servizio cloud permette di usare i terminali GP08L/LN da un qualsiasi PC connesso in Internet.

Il requisito affinché il software cloud possa lavorare è di avere sia il PC che il terminale GP08 (o i terminali, in caso di azienda con accessi multipli) connessi alla medesima rete e con accesso ad Internet. Qualora sia richiesto l'accesso con QRCode per i visitatori, anche il terminale Android per generare questi QRCode deve essere connesso in WiFi alla medesima rete.

Il PC dal quale effettuare le configurazioni deve poter avere un Browser di ultima generazione: le schermate nel seguito illustrate sono state catturate dal Browser "Edge" di Windows vers. 10.0 build 19041.

La presente guida presuppone che il terminale (o i terminali) GP08 siano configurati per essere gestiti in cloud e che abbiano nella propria memoria l'elenco dei dipendenti, ciascuno con un proprio ID, un nome ed almeno una credenziale di identificazione - immagine del volto, codice RFID (sia 125 kHz che Mifare 13,56 MHz), PIN. Ai fini della gestione "Green Pass" in modalità totalmente anonima (**senza alcuna registrazione di dato sensibile di nessun utente**) il codice utilizzatore è "99999999".

Per utilizzare il software in cloud è quindi sufficiente digitare l'indirizzo corretto del server sulla barra del proprio Browser (Google Chrome, Mozilla Firefox, Windows Edge, Safari, ...).

Immagini e fotografie o altre informazioni di carattere grafico sono inseriti nel presente Manuale esclusivamente a titolo descrittivo ed esplicativo. Si rammenta che le informazioni contenute nel presente Manuale sono soggette a modifiche, senza preavviso, a fronte di aggiornamenti del firmware o per altri motivi.

Tutte le informazioni, comprese, tra le altre, formulazioni, immagini e grafica sono di proprietà di DOINGSECURITY Sas. Questo manuale non può essere riprodotto, modificato in alcun modo o distribuito anche in parte con qualsiasi mezzo senza la preventiva autorizzazione scritta di DOINGSECURITY Sas.

Salvo disposizioni contrarie, DOINGSECURITY non rilascia alcuna garanzia, assicurazione o dichiarazione, esplicita o implicita, in merito al presente Manuale.

Entro i limiti previsti dalla Legge in vigore, il prodotto - completo di hardware, software e firmware - viene fornito "così com'è" compresi gli eventuali difetti e gli errori: DOINGSECURITY Sas non fornisce alcuna garanzia, esplicita o implicita, incluse, senza limitazione, garanzia di commerciabilità, di qualità soddisfacente, di idoneità per uno scopo particolare e di non violazione di diritti di terzi. In nessun caso DOINGSECURITY Sas, i suoi Dirigenti, Funzionari, Dipendenti o Agenti saranno responsabili per eventuali danni speciali, consequenziali, incidentali o indiretti, compresi, tra gli altri, danni per perdita di profitti, interruzione dell'attività o perdita di dati o di documentazione connessi all'uso di questo prodotto, anche qualora DOINGSECURITY Sas fosse stata informata della possibilità del verificarsi di tali danni. L'utente si assume interamente

ogni rischio correlato dall'utilizzo del prodotto con accesso Internet: DOINGSECURITY Sas declina ogni responsabilità per anomalie di funzionamento, perdita di privacy o altri danni derivanti da un attacco cibernetico, attacco da parte di hacker, virus o altri rischi e minacce alla sicurezza, correlati all'utilizzo di Internet. Tuttavia DOINGSECURITY Sas fornirà supporto tecnico tempestivo, se necessario.

Considerata la variabilità di normativa applicabile, si prega di controllare tutte le Leggi pertinenti e vigenti nella propria giurisdizione prima di utilizzare questo prodotto, al fine di garantire che l'utilizzo sia conforme alle Leggi vigenti: DOINGSECURITY Sas declina ogni responsabilità nel caso in cui questo prodotto venga utilizzato per scopi illeciti. In caso di eventuali conflitti tra il presente Manuale e la Legge applicabile, prevale quest'ultima.

1.1 Organizzazione del presente manuale

Il presente Manuale Utente è diviso in sezioni. Il capitolo "**Avvio Software**" descrive gli step necessari per il primo utilizzo del servizio in cloud e la configurazione iniziale del sistema, mentre il capitolo "**Controllo Green Pass in cloud**" illustra il funzionamento del software nella gestione dei QRCode dei Green Pass e funzionamento del sistema come controllo degli accessi.

1.2 Terminologia

- **Ethernet -** tecnologia di comunicazione per la realizzazione di reti di computer in ambito locale (LAN)
- **LAN -** rete locale, rete di computer per un'area di piccole dimensioni, per es. un ufficio, un'abitazione o un gruppo di edifici come una scuola o un aeroporto
- **10Base-T -** 10 Mbit/s, usa un connettore modulare a 8 vie, generalmente chiamato RJ45, nell'ambito Ethernet con coppie twistate. I cavi generalmente usati sono a 4 coppie twistate (sebbene 10BASE-T e 100BASE-TX usino solamnete due di tali coppie). Ciascun stardard supporta la comunicazione sia full-duplex che half-duplex. Operano su distanze fino a 100 metri
- **100Base-TX -** noto come **Fast Ethernet**, usa due coppie UTP o STP, CAT5
- **Coppia Twistata -** è un cablaggio nel quale due conduttori sono twistati insieme per cancellare l'interferenza elettromagnetica (EMI) proveniente da sorgenti esterne, per esempio la radiazione elettromagnetica da cavi non schermati, e il crosstalk da coppie poste nelle vicinanze
- **UTP**, Unshielded Twisted Pair - coppia twistata non schermata
- **STP**, Shielded Twisted Pair - coppia twistata schermata; uno schermo metallico è posto attorno a ciascuna coppia per proteggere il cavo da interferenze elettromagnetiche (EMI)
- **WEB -** World Wide Web (WWW), applicazione del protocollo internet HTTP
- **HTTP -** Hypertext Transfer Protocol; è un protocollo internet usato originariamente per lo scambio di documenti ipertestuali in formato HTML

- **USB -** Universal Serial Bus; metodo per la connessione seriale di dispositivi esterni al computer
- **Video codec** - compressione **H.263** derivata da MPEG-4, **H.264** è un codec per il formato AVC MPEG-4. **MPEG-4** è un tipo di compressione video
- **JPEG** è un metodo standard di compressione usato per salvare immagini digitali
- **Voice over Internet Protocol** (**VoIP**) è una tecnologia che permette la trasmissione di voce digitalizzata all'interno di paccetti del protocollo **UDP/TCP/IP** nelle reti di computer. È usato per effettuare telefonate via Inernet, Intranet o altri tipologie di connessioni dati
- **TCP/IP** contiene un set di protocolli per la comunicazione nelle reti di computered è il protocollo principale di Internet
- **IP address** è un numero che identifica chiaramente una interfaccia nella rete di computer che usa il protocollo IP
- **DHCP** (Dynamic Host Configuration Protocol) è un protocollo della famiglia TCP/IP. È usato per assegnare automaticamente indirizzi IP a singoli PC nelle reti di computer, semplificando il lavoro dell'amministratore di rete
- **Internet** è un sistema di reti di computer connessi a livello mondiale
- **Intranet** è una rete di computer simile a Internet, ma di tipo privato. Questo significa che è usata esclusivamente da un gruppo di utenti limitato (es. Una azienda e le sue filiali)
- **PoE** (Power over Ethernet) è un sistema di alimentazione attraverso il cavo di rete che non necessita di ulteriori cablaggi per la fornitura di energia elettrica
- **NTP** (Network Time Protocol) è un protocollo per la sincronzzazione degli orologi interni ai computer
- **DTMF** (dual tone multi frequency) è il segnale del fornitore di servizio telefonico che è generato quando si preme un tasto di un normale telefono.

2 Avvio Software

2.1 Prerequisiti dei terminali GP08

I terminali GP08 per poter essere utilizzati dal software in cloud devono poter essere indirizzati al server.

L'impostazione richiesta è accessibile nel menu principale attraverso l'icona "INGRANAGGIO" che compare in basso nello schermo quando si tocca lo schermo del terminale GP08 - vd. Fig. 2.1

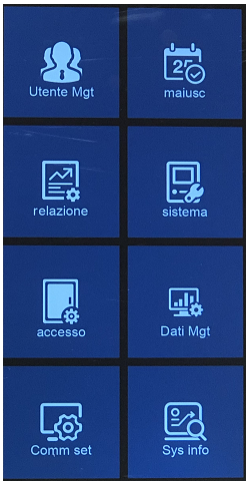


Fig. 2.1. *Menu di Configurazione GP08*

All'interno del sotto-menu "Comm set", selezionare la voce "Comm set" e impostare il parametro "ID dispositivo" sul valore desiderato. Per default il parametro è 1 e se nel sito questo è l'unico terminale, è sufficiente che sia lasciato al valore di default - vd. Fig. 2.2.

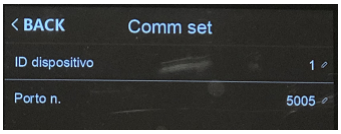


Fig. 2.2. *Menu Comm set*

Nella voce "Server" - vd Fig. 2.3 - impostare i parametri come segue:

- Req Server -> **Sì**
- Usa Domain Nm -> **Sì**
- DomainNm -> **www.yunatt.com**
- IP Server -> **047.106.068.143**
- Ser Port No -> **7792**
- Heartbeat -> **3**
- Approvazione Server -> **No**

NOTA.

Il terminale GP08 viene fornito già configurato in questa parte del sistema e di norma non dovrebbero essere effettuate variazioni rispetto a quanto sopra riportato.

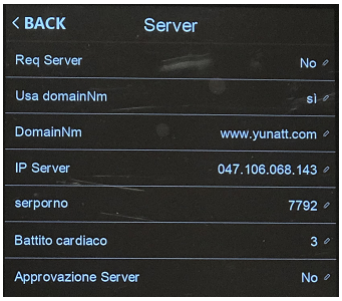


Fig. 2.3. *Menu Comm set - Server*

Selezionare poi la voce "ethernet" o "WiFi" in funzione di come si intende venga collegato il terminale alla rete - in Fig. 2.4 è illustrata la connessione WiFi. Abilitare la connessione con la modalità DHCP, scegliere la rete WiFi a cui collegarsi e inserire la password WiFi: al terminale viene assegnato automaticamente un indirizzo IP nella rete.

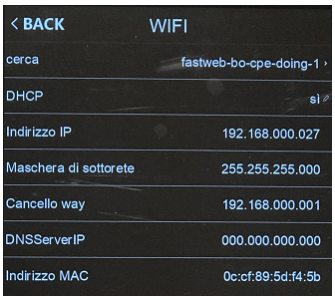


Fig. 2.4. *Menu Comm set -> Impostazioni WiFi*

Infine aprire il menu "Sys Info" per prendere nota del numero di serie del terminale (vd. Fig. 2.5 - voce SN): questo dato dovrà essere utilizzato all'interno del software cloud.

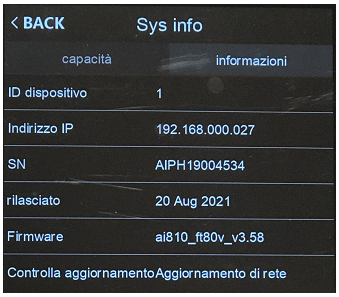


Fig. 2.5. *Menu Sys Info -> dispositivo info*

Nel terminale devono infine essere impostati l'ora ed eventualmente la data e devono essere caricate le credenziali degli utenti - se il terminale deve anche eseguire la gestione di credenziali Badge / PIN / Volto. Ai fini di un controllo accessi con riconoscimento "Green Pass", queste impostazioni non sono rilevanti e non vengono descritte in questo manuale.

2.2 Primo utilizzo del software

Una volta avviato il browser, scrivere sulla barra degli indirizzi:

www.yunatt.com:82

Si apre la pagina di login mostrata in Fig. 2.6.

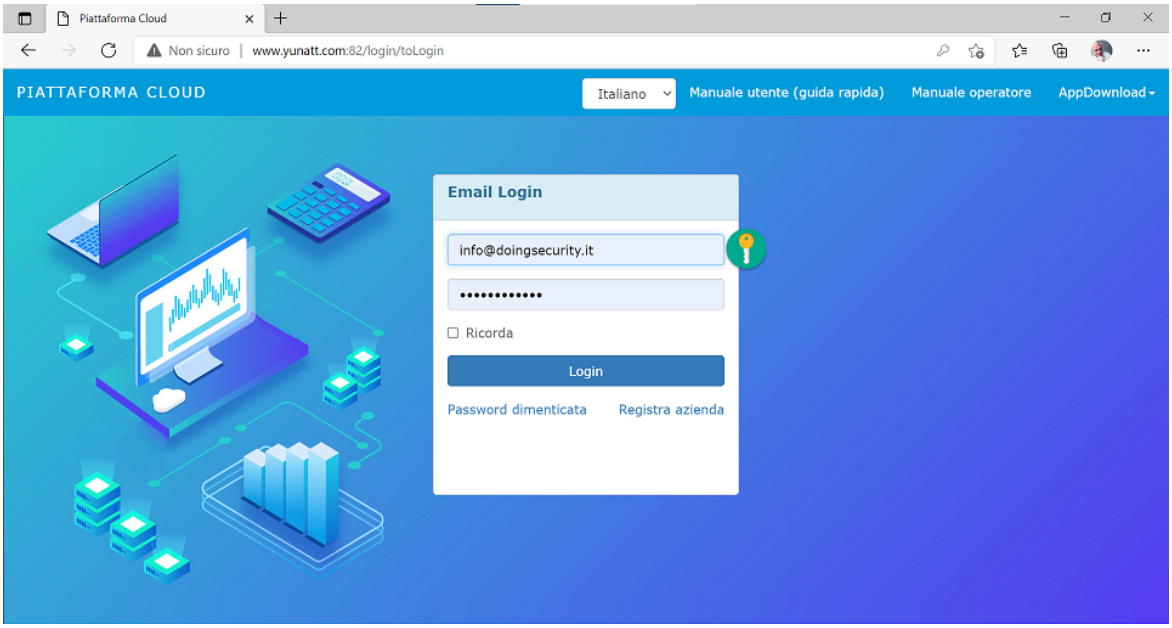


Fig. 2.6. *Login al software in cloud*

Per prima cosa selezionare la lingua "Italiano" dal menu a tendina posto al centro in alto.

È richiesto, quindi, che sia effettuata una registrazione mediante il comando "Registra azienda" posto sotto il pulsante di Login. Vd. Fig. 2.7.

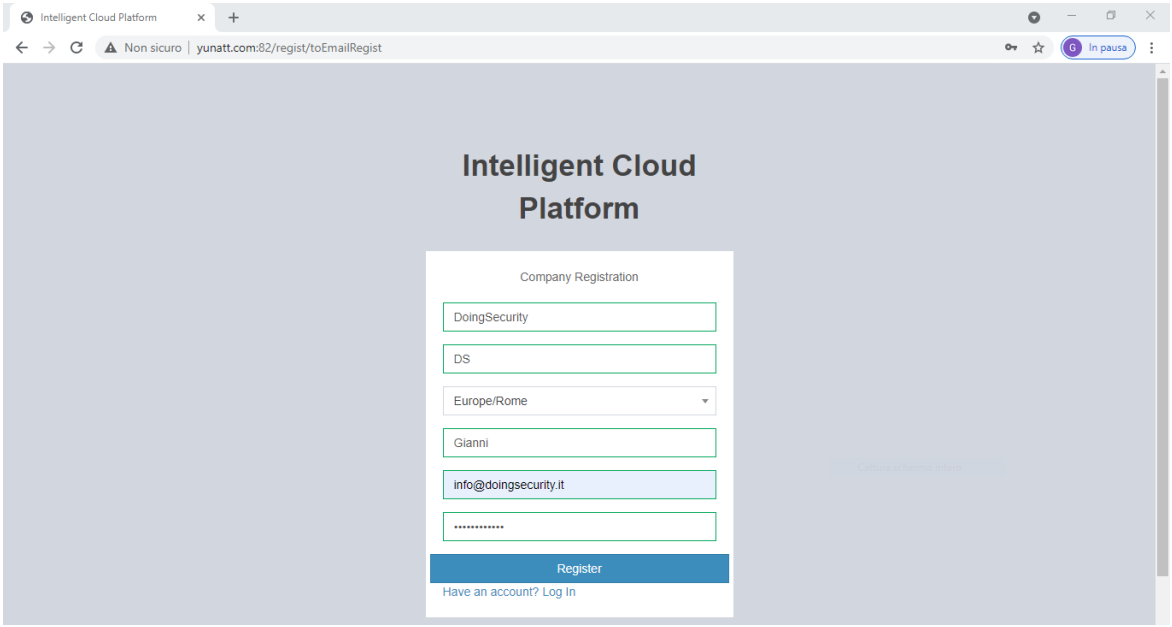


Fig. 2.7. *Registrazione account*

Devono essere fornite tutte le informazioni previste dal modulo di registrazione:

- Nome Azienda
- Nome breve dell'Azienda
- Scelta del fuso orario all'interno del menu a tendina
- Nome dell'amministratore
- Indirizzo email che sarà utilizzato come Nome Utente per il login
- Password con un minimo di 6 e un massimo di 12 caratteri (si consiglia di usare almeno una lettera maiuscola, almeno una cifra, almeno un carattere speciale).

Inserite tutte le informazioni richieste di clicka sul pulsate "Registra" così da poter effettuare l'accesso con le credenziali scelte.

2.3 Home page e menu principale

La pagina home del software si apre con una dashboard - vd. Fig. 2.8.

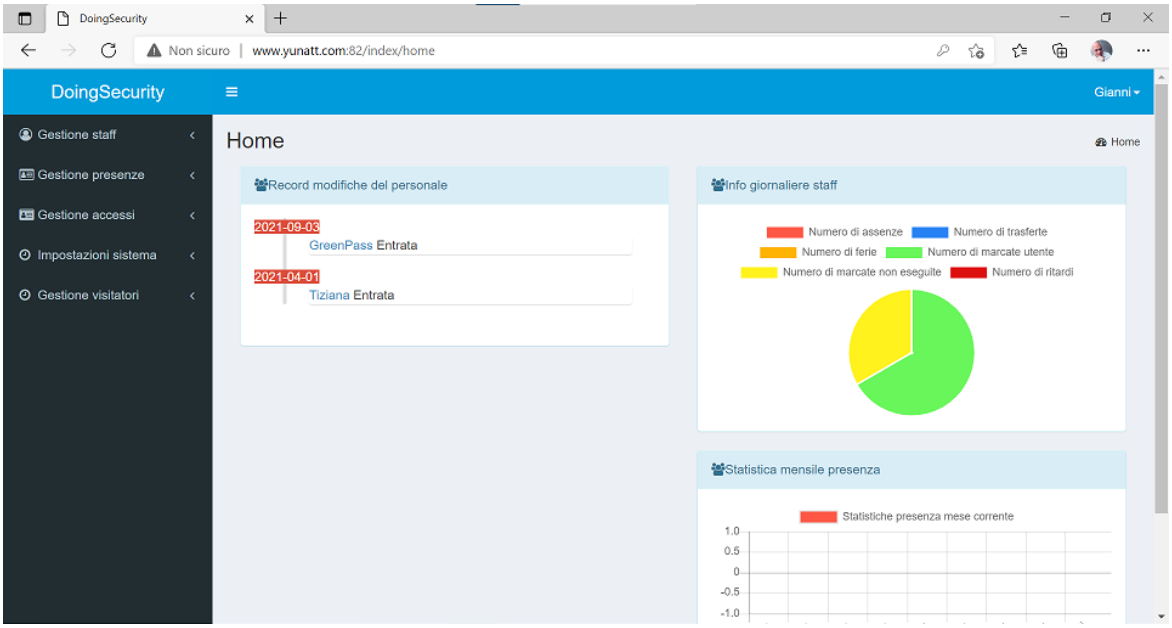


Fig. 2.8. *Home page*

Nel cruscotto compaiono le statistiche di accesso del personale e il menu delle funzioni sulla sinistra. Le voci del menu sono:

- Menu "Gestione staff" per la gestione del personale
- Menu "Gestione presenze" che permette di verificare le marcate degli utenti, di inserire i giustificativi di assenza ove necessario e di effettuare i report mensili di presenza
- Menu "Gestione accessi" per la gestione delle funzioni di controllo accessi
- Menu "Impostazioni sistema" necessario per l'impostazione dei dispositivi e dei parametri del sistema
- Menu "Gestione visitatori" per le funzionalità di controllo accesso dei visitatori dotati di QRcode.

NOTA.

Nel presente Manuale sono descritte le sole funzioni di "Gestione accessi" mediante Green Pass: per le rimanenti funzioni si faccia riferimento ai Manuali per il Controllo Presenza del terminale DF08.

2.4 Impostazione sistema

Il menu "Impostazioni sistema" si compone di sotto-menu affinché siano definiti tutti i parametri per il corretto uso del terminale GP08 nel sistema: infatti come prima cosa, occorre collegare al software in cloud i terminali GP08 che sono in dotazione in azienda.

2.4.1 Gestione dispositivi

Selezionare la prima voce "Gestione dispositivi" e clickare sul pulsante "+Agg" - vd. Fig. 2.9.

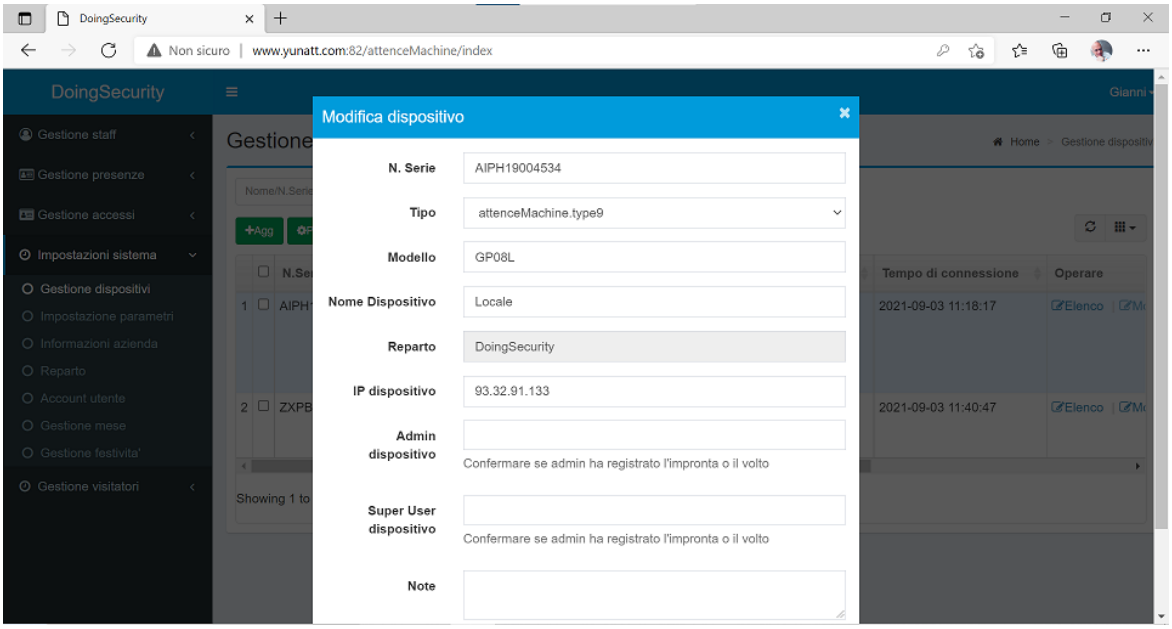


Fig. 2.9. *Impostazione sistema - Gestione dispositivi*

Per collegare un terminale GP08 al software in cloud, deve essere immesso il N. Serie che compare nel menu Sys Info (vd. Fig. 2.5). Deve essere inoltre selezionato il corretto "Tipo" di terminale (in questo caso "type9") e il modello; deve infine essere dato un nome al terminale. Salvando, il terminale compare nell'elenco dei terminali disponibili e collegati al software - vd. Fig. 2.10.

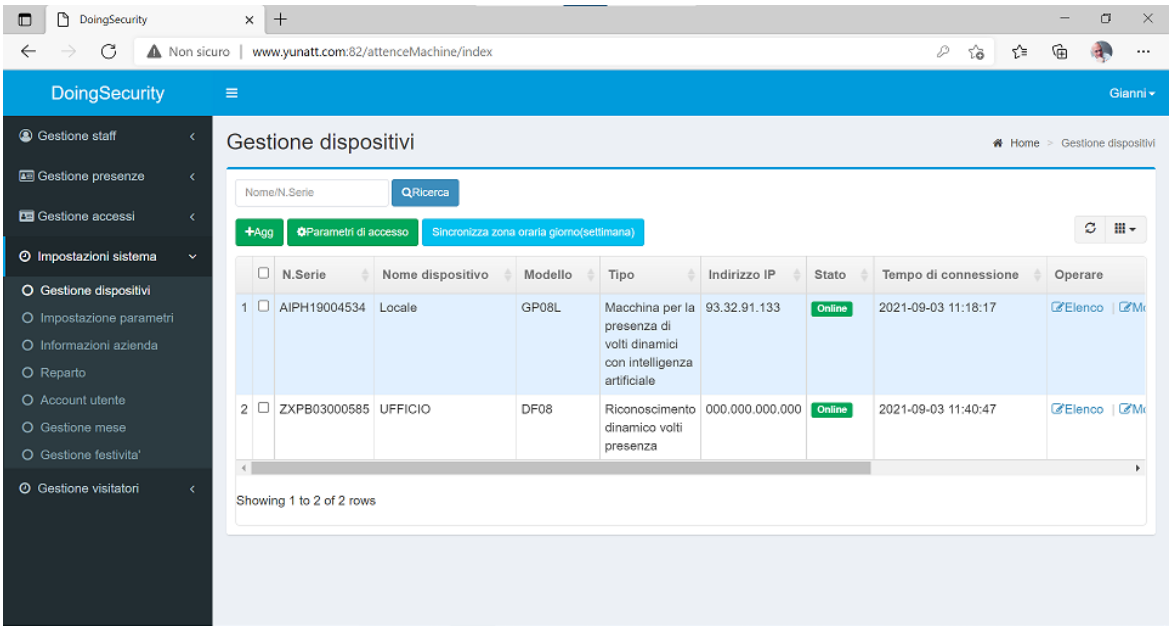


Fig. 2.10. *Impostazione sistema - Gestione dispositivi - Aggiungi*

Affinché il processo di aggiunta vada a buon fine, il software in cloud deve poter mostrare il terminale GP08 come "**Online**" - vd. Fig. 2.10.

NOTA.

Il terminale GP08 può impiegare qualche secondo per essere "Online": la velocità dipende dalla rete e dal tipo di collegamento Internet in dotazione in azienda.

Se il terminale GP08 rimane "Offline", significa che sono presenti errori nella configurazione e/o il collegamento in internet del terminale non è effettuato correttamente.

Nel menu di "Gestione dispositivi" è possibile elencare tutti i terminali GP08 che appartengono al sistema aziendale. I terminali si distinguono l'uno dall'altro mediante il N. Serie (codice univoco), grazie al diverso indirizzo IP nella rete locale e con un diverso ID - vd. Fig. 2.2, menu "Comm set", parametro "dispositivo No".

Clickando sul pulsante "Parametri di accesso" per il dispositivo selezionato, compare la finestra di Fig. 2.11.

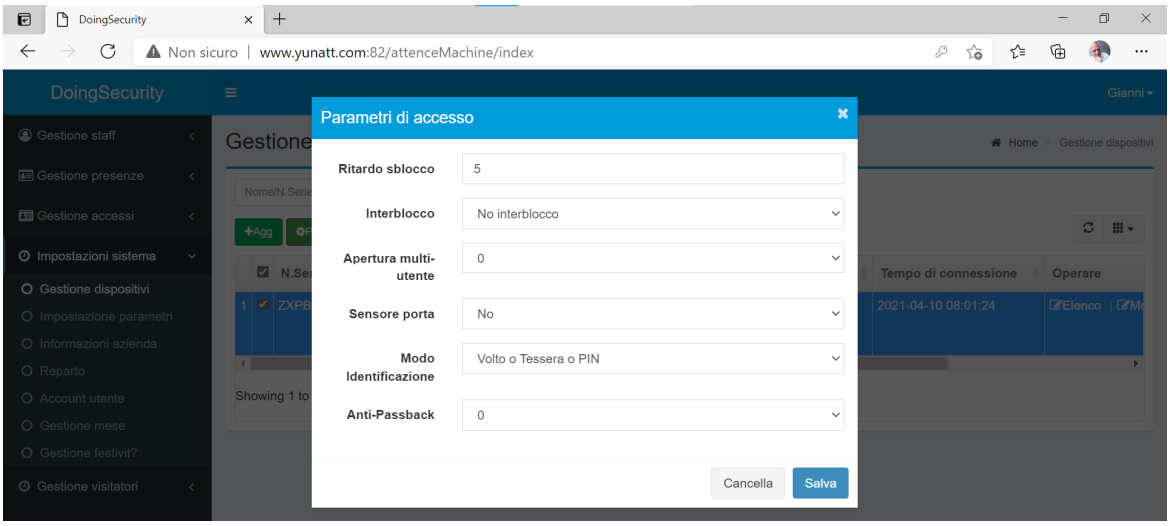


Fig. 2.11. *Impostazione sistema - Gestione dispositivi - Parametri di accesso*

La configurazione di questi parametri è attinente alle impostazioni di utilizzo del terminale ed è conforme a quanto impostato nel terminale. Notare la modalità di identificazione che può essere a doppia o tripla credenziale selezionando la voce dal menu a tendina: questa impostazione è utile per i soli utenti noti del sistema.

Infine tener presente che - se è necessario eliminare un terminale dall'elenco dei dispositivi di sistema - è necessario immettere la password di conferma (di default "**123456**"): questa password è richiesta se il terminale dovesse essere eliminato da un PC Client e ricollegato ad un altro. Un terminale è collegabile ad un solo PC Client alla volta.

2.4.2 Informazioni azienda

Il menu "Informazioni azienda" è mostrato in Fig. 2.12. È la scheda del software dove inserire tutti i dati di carattere aziendale. È necessario indicare oltre al nome anche la "zona oraria" scegliendola dal menu a tendina.

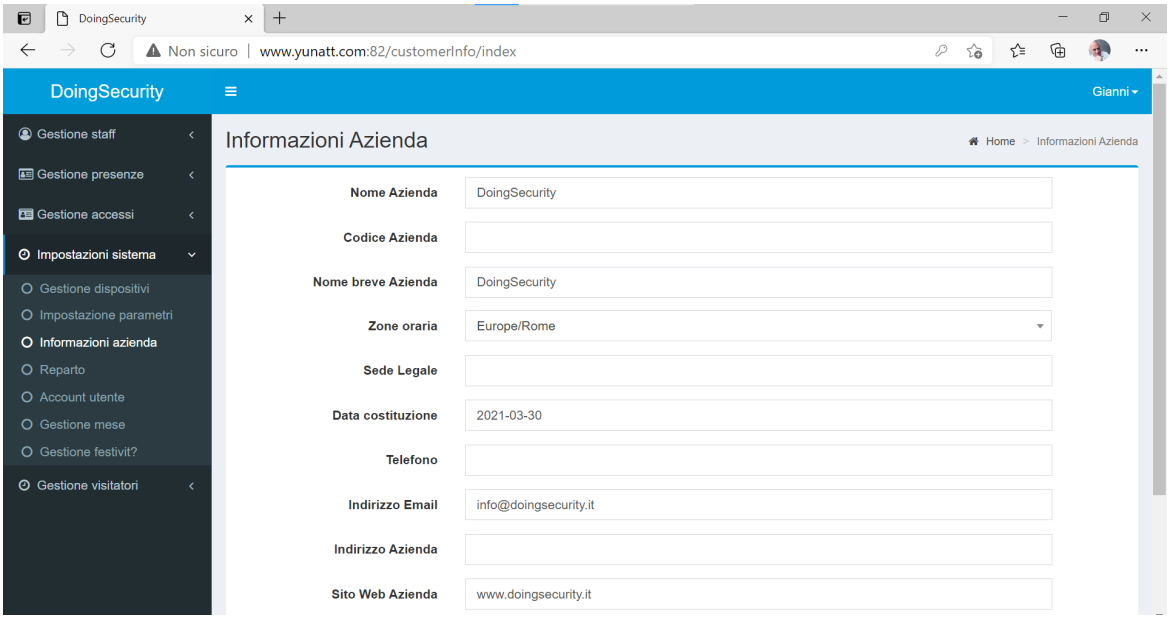


Fig. 2.12. *Impostazioni sistema - Informazioni azienda*

2.4.3 Reparto

Nel menu "Reparto" - mostrato in Fig. 2.13 - sono invece inseriti i reparti dell'azienda.

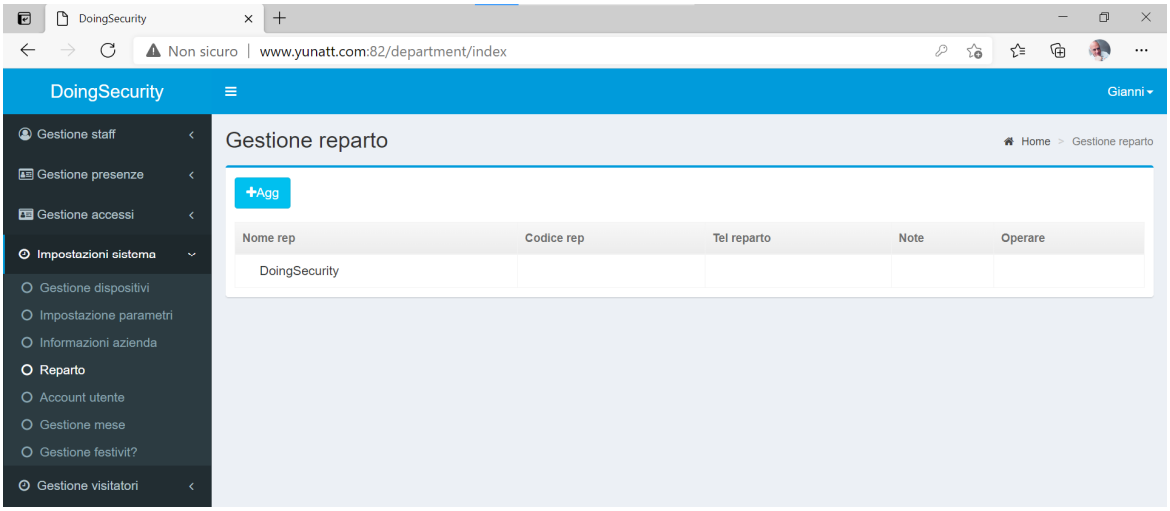


Fig. 2.13. *Impostazioni sistema - Reparto*

Nel menu "Reparto" utilizzare il pulsante "Agg" per aggiungere i mnemonici dei reparti che compongono l'azienda.

NOTA.

Definire i reparti può essere utile nel momento in cui sarà necessario stabilire un calendario mensile di "presenza" identico per un gruppo di dipendenti. Tale funzionalità non è descritta nel presente manuale.

2.4.4 Account utente

Nel menu "Account utente" - mostrato in Fig. 2.14 - sono invece elencati gli utenti che hanno le credenziali per l'accesso al software in cloud.

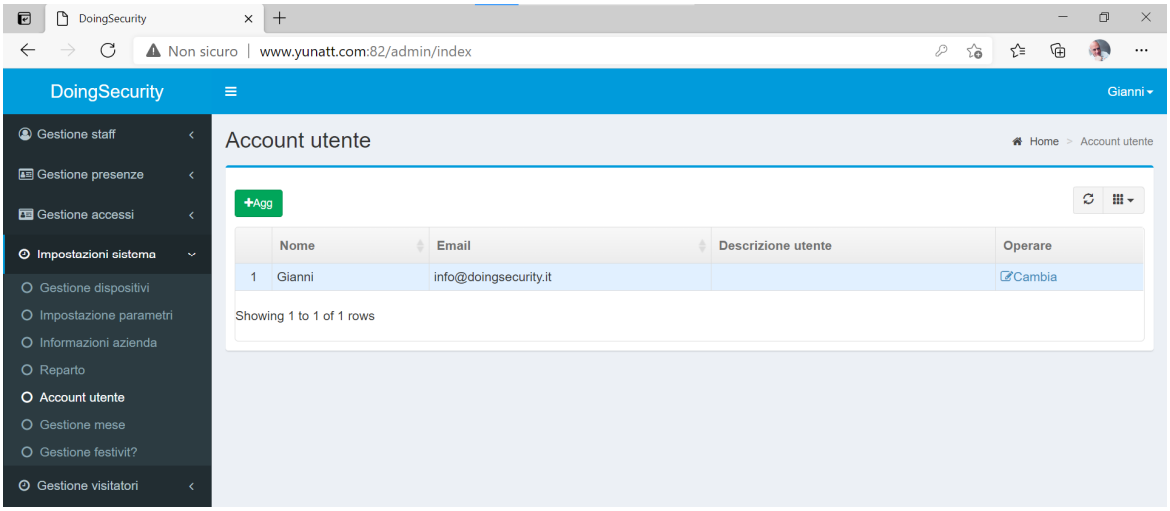


Fig. 2.14. *Impostazioni sistema - Account utente*

Notare che nel menu "Account utente" sono inseriti gli amministratori di sistema e che, nel terminale GP08, sono ammessi per default fino a 10 utenti amministratori.

Il pulsante "Agg" è utilizzato per aggiungere un nuovo account, mentre con "Cambia" viene editato il profilo di un account.

2.5 Gestione Staff

Terminate le impostazioni di carattere generale, il menu "Gestione Staff" permette di gestire le anagrafiche dei dipendenti e i relativi profili di controllo presenza.

Clickando su "Informazioni staff" si apre l'elenco degli staff cioè i dipendenti che sono registrati nelle anagrafiche del terminale - vd. Fig. 2.15.

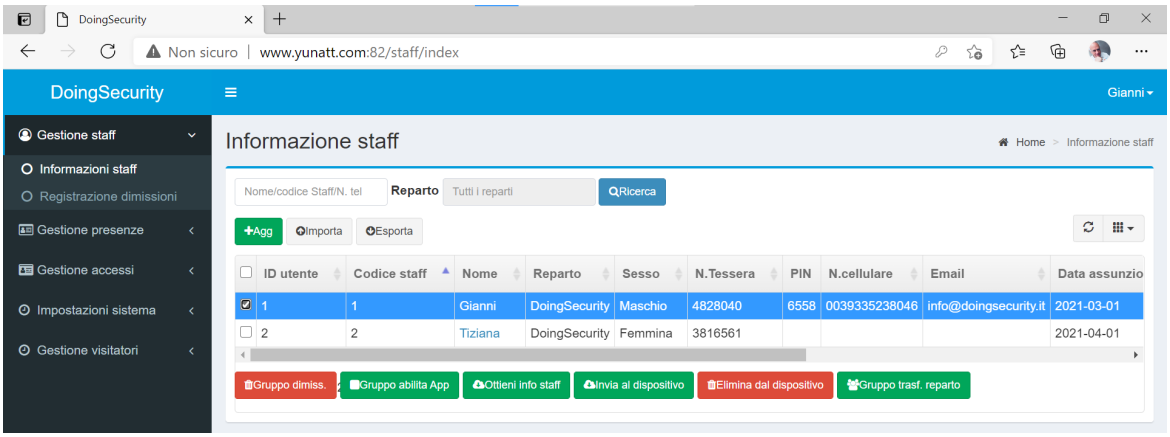


Fig. 2.15. *Gestione staff - Informazioni staff*

Notare il pulsante "Ottieni info staff" che permette di acquisire automaticamente dai terminali GP08 configurati nel sistema le informazioni del personale.

Con un click sul nome (colonna "Nome") si apre la scheda dello staff scelto (vd. Fig. 2.16).

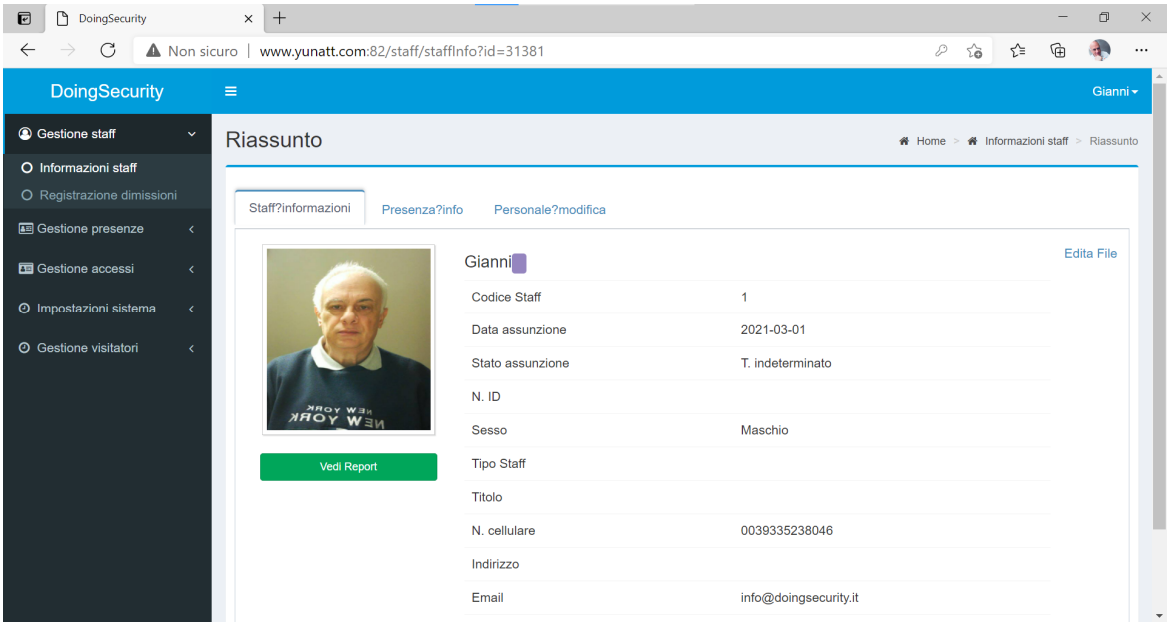
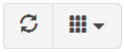


Fig. 2.16. *Gestione staff - Informazioni staff - Riassunto*

Per eseguire delle modifiche, clickare su "Edita File" posto in alto a destra. Con il pulsante "Vedi report" si ottiene il report giornaliero del dipendente con le indicazioni di dettaglio circa la presenza al (o assenza dal) lavoro. Questa funzionalità non è presa in esame nel presente Manuale.

Aprendo la seconda scheda, "Presenza info", si ottengono le credenziali dello staff e in particolare il codice "staff", il codice RFID eventualmente associato, il PIN e l'indicazione se esiste il file relativamente all'immagine del volto.

Notare che le icone  poste normalmente sulla destra all'inizio di un elenco (Fig. 2.15) servono a selezionare / deselezionare alcune colonne presenti nella tabella per ottenere una visione personalizzata dei dati.

Una volta che uno o più staff fossero stati oggetto di modifica, ricordarsi di inviare i dati ai dispositivi GP08 mediante il pulsante "Invia al dispositivo" - vd. Fig. 2.15.

Il pulsante "Elimina dal dispositivo" è invece utilizzato per eliminare uno o più staff dall'elenco.

I comandi posti in alto a sinistra della finestra sono utilizzati per:

- Eseguire delle ricerche per Nome/codice staff/N. Cellulare
- Aggiungere uno staff inserendo i dati manualmente
- Importare / Esportare i dati relativi ai dipendenti

Ai fini della gestione "**Green Pass**" va definito un utente con il nome generico e l'ID "99999999". Le informazioni Green Pass infatti non sono mai memorizzate, per evidenti motivi di Privacy.

Con un click sul pulsante "+Agg" posto all'inizio dell'elenco, si apre la pagina mostrata in Fig. 2.17.

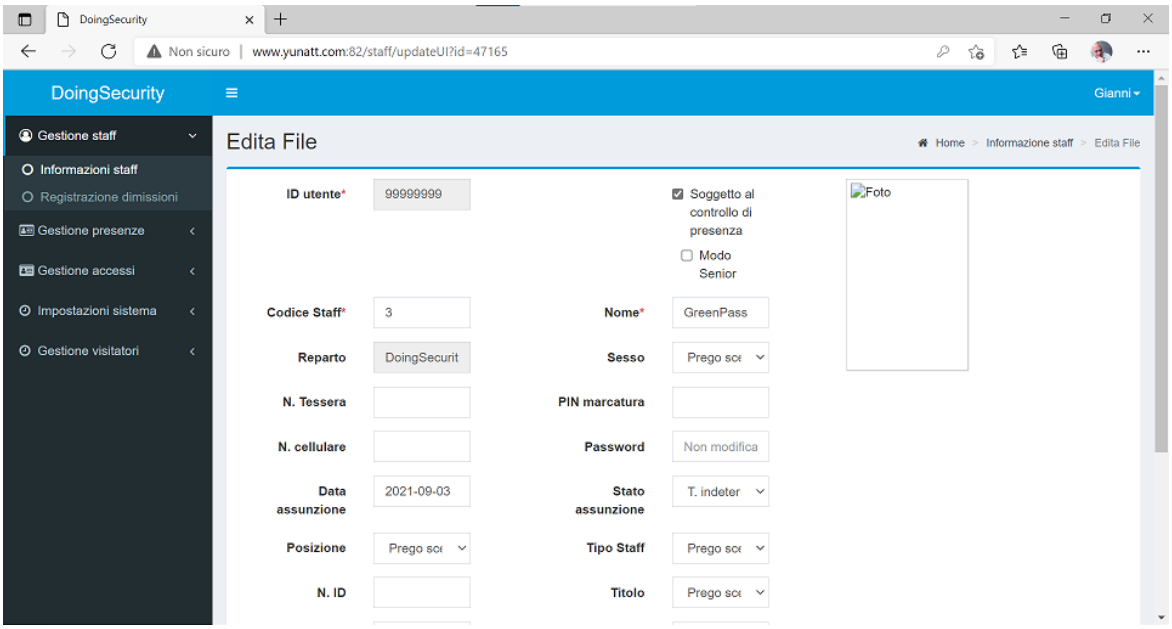


Fig. 2.17. *Gestione staff - Aggiungi*

L'ID utente deve essere riportato come indicato in Fig. 2.17. Può essere liberamente scelto il campo "Nome" - per es. Green Pass" - e il codice Staff: nel caso in esame è stato scelto il Codice "3".

Si ottiene dunque l'elenco di Fig. 2.18.

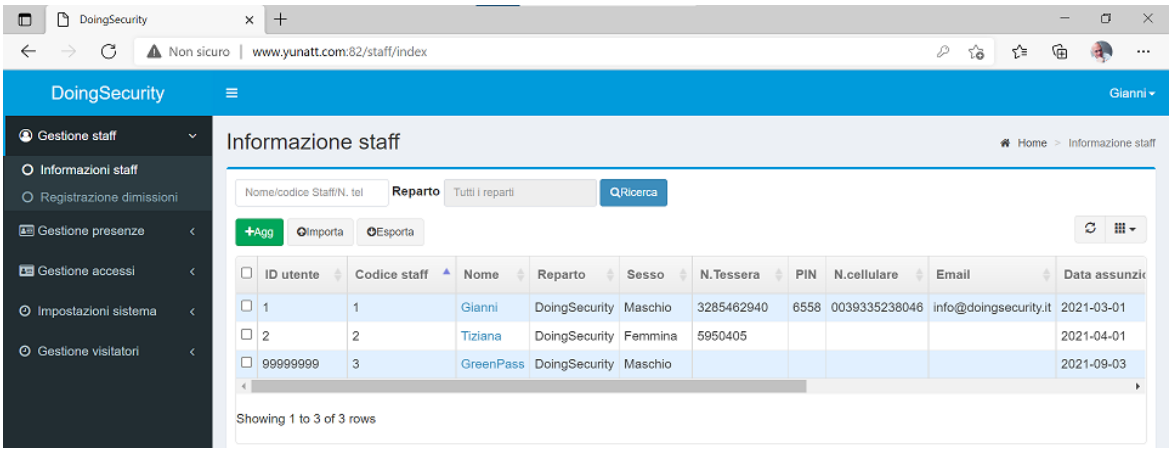


Fig. 2.18. *Gestione staff - Elenco Staff*

3 Controllo Green Pass in cloud

3.1 Gestione accessi

Il terminale GP08 è sviluppato per essere usato in modalità "Controllo Accessi" per la gestione dei "Green Pass".

Una volta che i dispositivi siano collegati al software e in modo "Online" e che siano stati definiti gli utenti come descritto nel paragrafo 2.5 Gestione staff", il menu da utilizzare è quello che riporta la dicitura "Gestione Accessi".

In una logica di "controllo degli accessi" si prevede la definizione di orari di permesso di accesso - sia a fasce orarie giornaliere che per i giorni della settimana; si impostano quindi le autorizzazioni circa gli utenti a cui fornire o meno l'autorizzazione all'accesso. Le voci di questo menu sono:

- Orario giornaliero
- Orario settimanale
- Permessi accesso
- Monitor tempo-reale
- Record stato porta

3.2 Orario giornaliero

L'orario giornaliero (vd. Fig. 3.1) è un elenco di fasce orarie (con un'ora di inizio e una di fine) all'interno delle quali si ha l'autorizzazione di accesso. Per definire una zona oraria giornaliera si usa il pulsante "+Agg" e si crea la Zona oraria con un ID, un nome e fino ad un massimo di 5 "intervalli" orari.

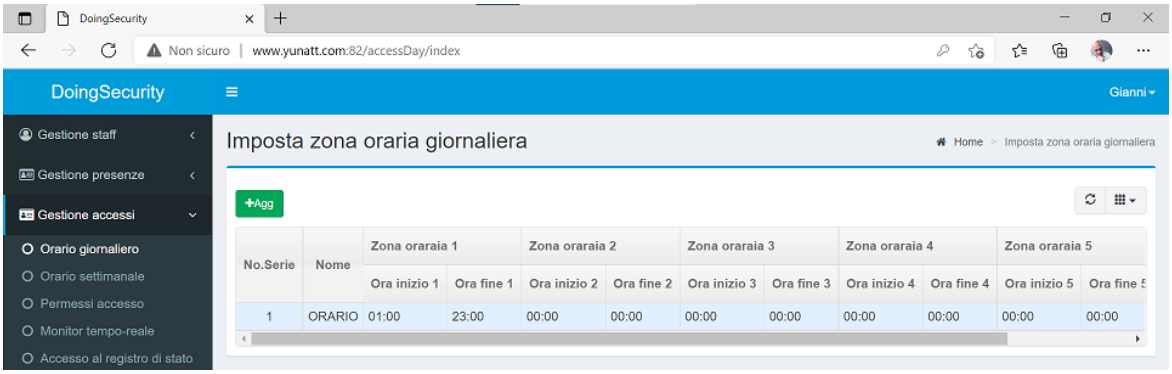


Fig. 3.1. *Gestione accessi - Orario giornaliero*

Con un click sul pulsante "+Agg" si definisce la nuova zona oraria - vd. Fig. 3.2:

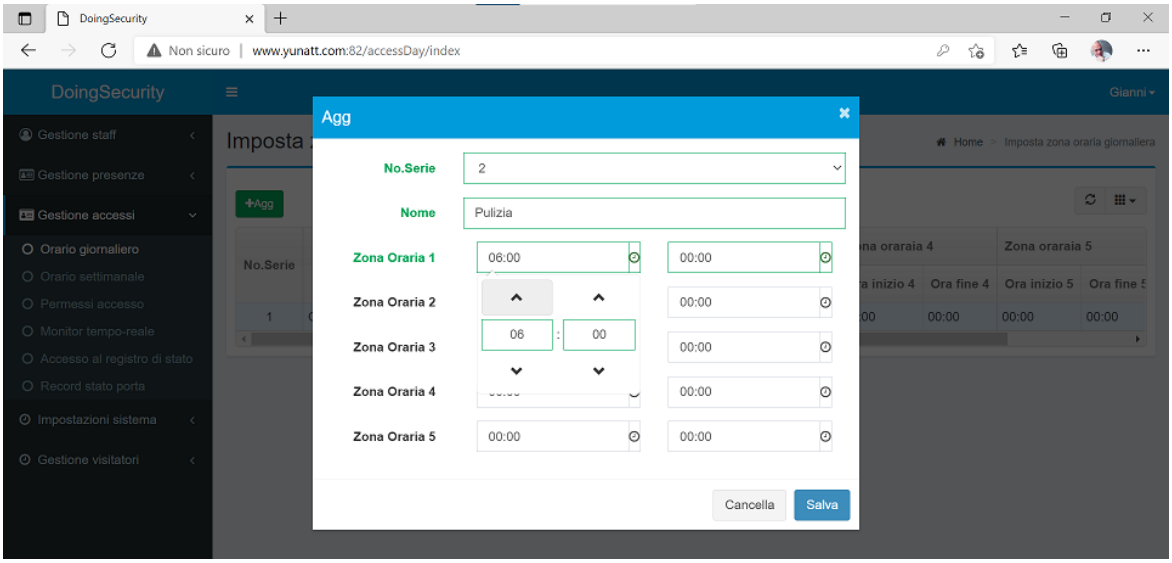


Fig. 3.2. *Gestione accessi - Orario giornaliero: aggiunta novo orario*

Il No.Serie è un numero che identifica univocamente l'orario, mentre il Nome è un campo definibile a piacere. Le 5 zone orarie hanno un valore HH:MM di inizio e di fine. Clickare su "Salva" per memorizzare le modifiche apportate o su "Cancella" per uscire senza salvare.

3.3 Orario settimanale

L'orario settimanale (vd. Fig. 3.3) definisce per i giorni della settimana quale Zona Oraria giornaliera è valida.

Per esempio, nella Fig. 3.3, i giorni dal lunedì al venerdì hanno associata la Zona ID = 1 "ORARIO", cioè quella mostrata in Fig. 3.1 con la fascia oraria dalle 01:00 alle 23:00, mentre i giorni sabato e domenica sono giorni interdetti all'acceso.

Salvare le impostazioni con il pulsante "Salva" o usare "Cancella" per uscire dalla finestra di dialogo senza salvare.

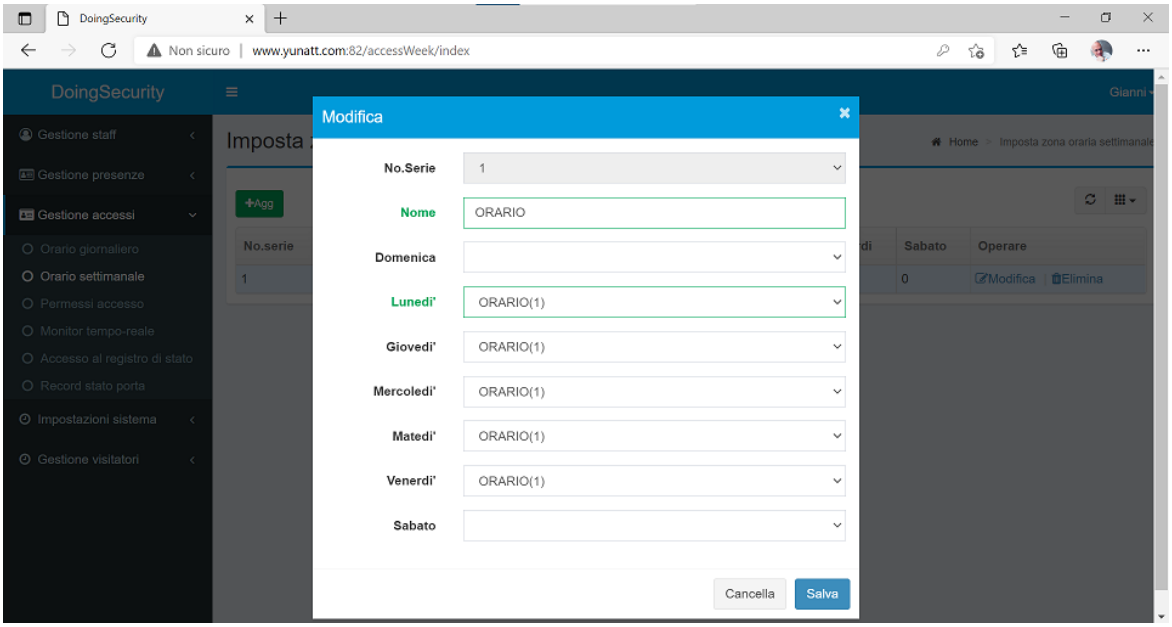


Fig. 3.3. *Gestione accessi - Orario settimanale*

3.4 Permessi accesso

Nel menu "Permessi accesso" (vd. Fig. 3.4) si attribuiscono le autorizzazioni agli utenti le cui credenziali possono essere usate per l'accesso. Lo spostamento di un utente dalla Lista non-autorizzati alla Lista autorizzati (e viceversa) si ottiene con i pulsanti quadrati Rosso/Blu con la doppia freccia, rispettivamente, verso destra e verso sinistra.

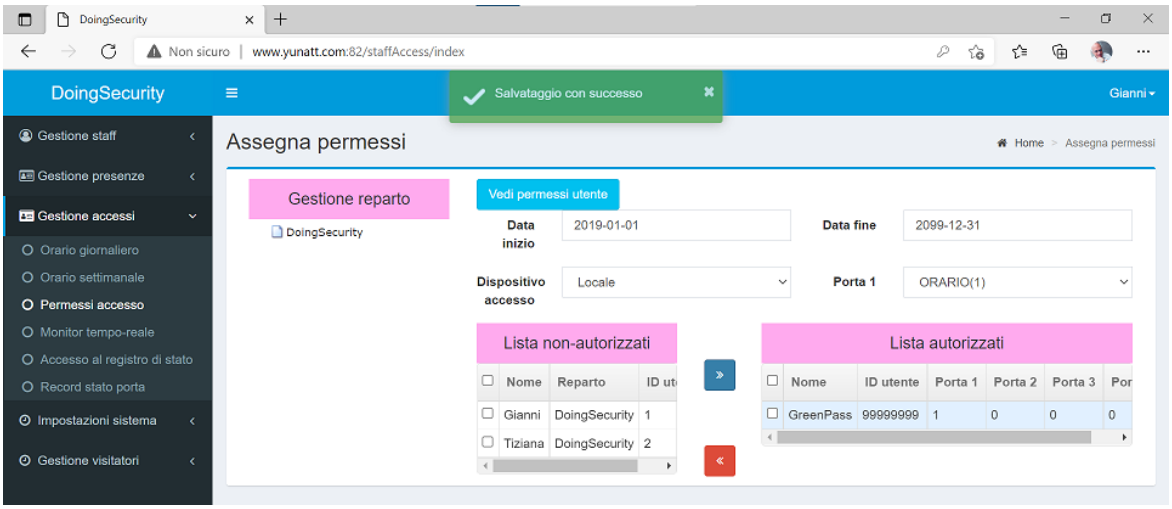


Fig. 3.4. *Gestione accessi - Permessi accesso*

Nell'esempio mostrato in Fig. 3.4, si prevede che usando il terminale denominato "Locale" negli orari indicati dall'Orario Settimanale "ORARIO", possano accedere gli utenti muniti di Green Pass valido. Questa autorizzazione di accesso ha validità fino al 31 Dicembre 2099.

3.5 Monitor tempo-reale

Nel menu "Monitor tempo-reale" (vd. Fig. 3.5) le icone "porta" rappresentano i diversi accessi del sistema e il loro stato (porta chiusa, porta aperta). Ogni varco di accesso è inoltre identificato come "online" oppure "offline", rendendo possibile una semplice diagnostica di rete.

L'evento di accesso viene mostrato in tempo reale nella matrice del monitor.

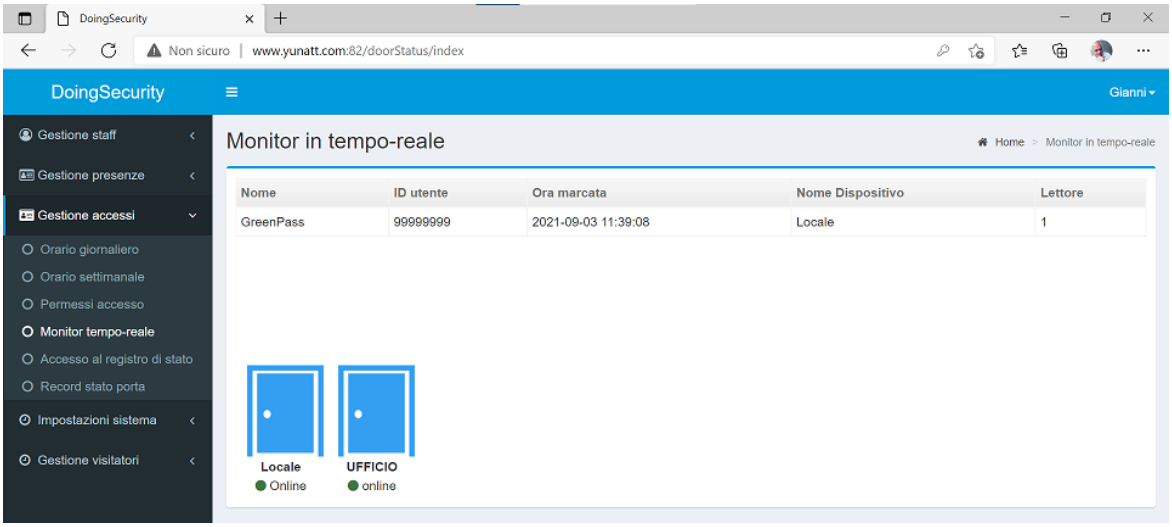


Fig. 3.5. *Gestione accessi - Monitor tempo-reale*

3.6 Record stato porta

Nel menu "Record stato porta" si possono ricercare i log degli accessi così da anlizzare il comportamento del sistema (vd. Fig. 3.6). Una volta che si sia scelto il tipo di dato su cui eseguire una analisi dei log, si ottiene l'estrazione delle informazioni dal data-base: per esempio, se si vuole sapere quando una porta è stata aperta, dal menu a tendina si sceglie la voce "porta aperta" - vd. Fig. 3.7.

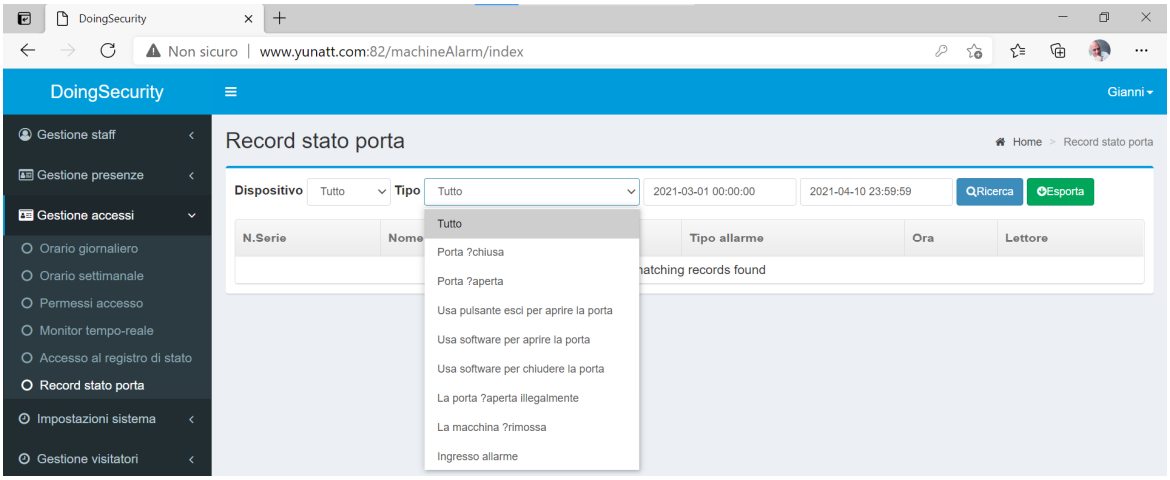


Fig. 3.6. *Gestione accessi - Record stato porta*

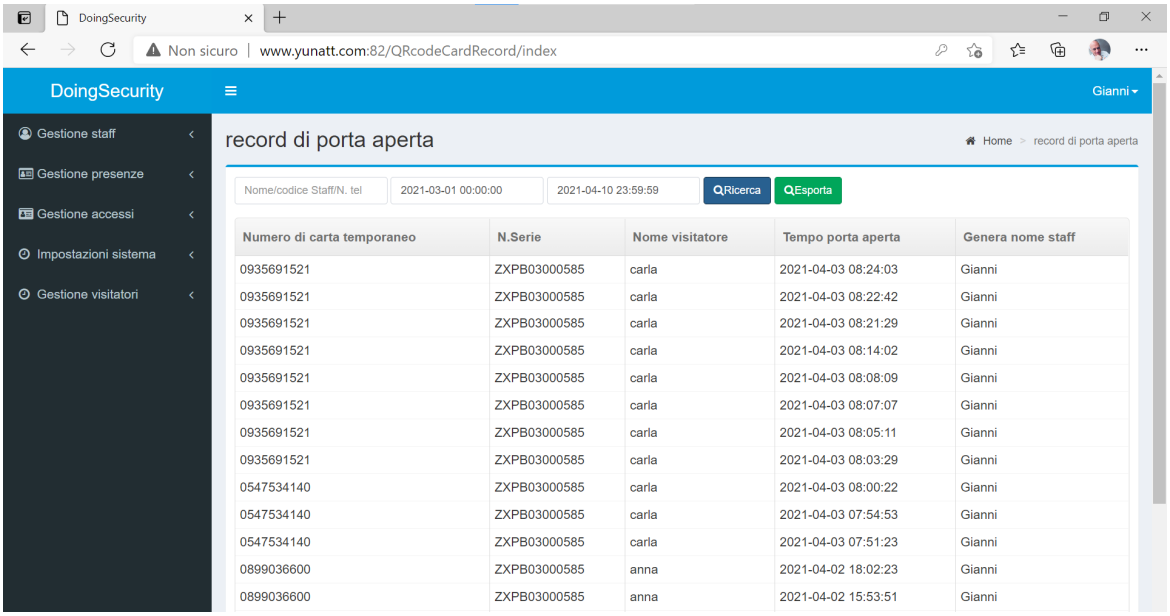


Fig. 3.7. *Gestione accessi - Record stato porta*

3.7 Gestione visitatori

I terminali GP08 sono in grado di leggere anche le credenziali in formato QRCode. Queste credenziali sono destinate ai soli utenti visitatori, che quindi sono abbinati al QRCode come un titolo di accesso temporaneo.

Per generare un QRCode, è necessario che uno o più staff (vd. Paragrafo 2.5) siano in possesso di smartphone Android. L'utente quindi può scansionare il QRCode che compare in alto a destra nella pagina di Login (vd. Immagine di copertina): in sostanza la scansione esegue il download di un file .APK per creare un'app sul desktop del terminale Android. L'app è mostrata in Fig. 3.8 (icona "Attendance").

Eseguendo l'accesso con le stesse credenziali utilizzate per accedere al software (vd. Fig. 2.6) si ottiene quando raffigurato in Fig. 3.8. Pertanto l'APP è utilizzabile da un utente di amministrazione, cioè da chi è in grado di eseguire l'accesso al software.

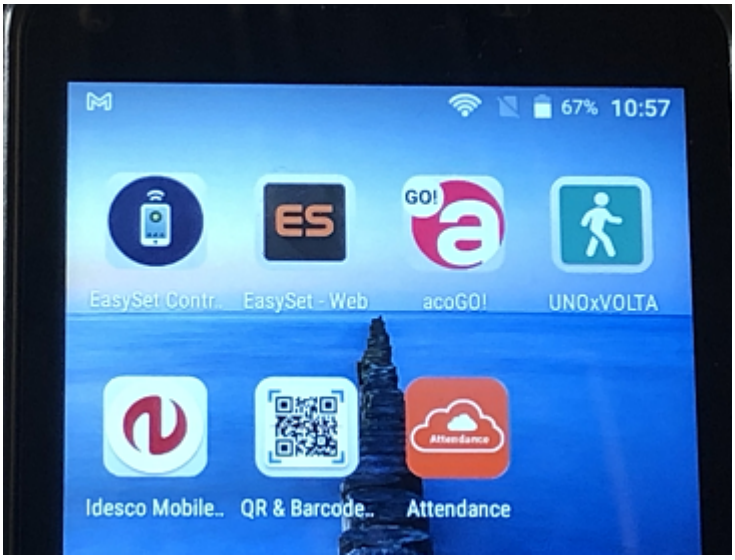


Fig. 4.7. *Gestione visitatori - app Android*

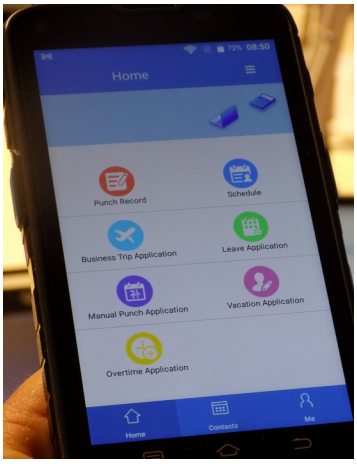


Fig. 3.8. *Gestione visitatori - app Android*

L'APP oltre alle funzionalità per il controllo di presenza (che permettono all'amministratore di usare le stesse funzionalità del controllo presenza anche su APP - quindi la possibilità di verificare le marcature, di definire le schedulazioni e di gestire i giustificativi di assenza - ferie, permessi, trasferte, ...), prevede un comando in alto a destra che, quando si esegue un "tap" sulle tre lineette orizzontali, mostra il menu di Fig. 3.9.

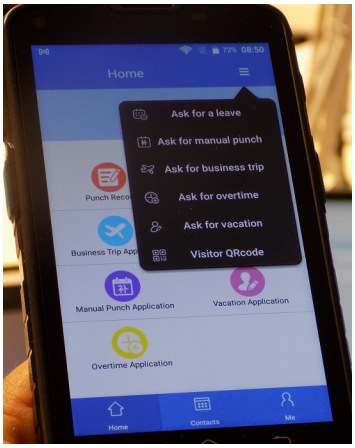


Fig. 3.9. *Gestione visitatori - app Android*

L'ultima voce del menu mostrato in Fig. 3.9 è "Visitor QRCode". Con questo comando si apre una schermata dove indicare:

- VISITOR NAME: nome del visitatore
- START TIME: data e ora di inizio (per default la data corrente con ora 00:00)
- VALID PERIOD: data e ora di fine (per default la data corrente con ora 23:59)
- OPEN DEVICE: scelta dell'accesso su cui poter usare il QRCode
- OPEN DOOR TIME: numero di volte in cui il QRCode rimarrà valido (per default il parametro è pari a 1)
- REMARK: evantuali note

A parte l'ultimo campo, tutti gli altri devono essere specificati.

Notare che per ragioni di sicurezza il QRCode è di fatto una credenziale a tempo e con limitazioni nel proprio utilizzo: è normalmente la credenziale da usare per una porta di una zona contigua alla reception, per esempio per accedere ad una saletta riunioni. L'uso del QRCode permette anche una semplice automazione di alcune funzioni di check-in che il visitatore compie quando si reca in visita ad una azienda. Nel momento in cui il QRCode è stato generato, può essere usato come credenziale di accesso ponendolo di fronte alla telecamera del terminale. Vd. Fig. 3.10.

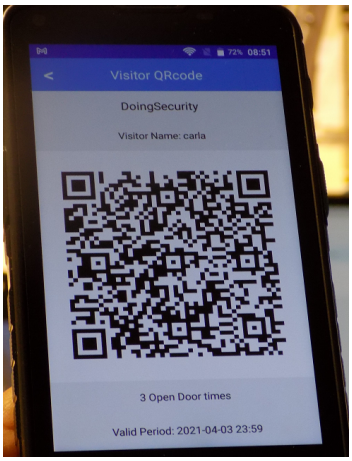


Fig. 3.10. *Gestione visitatori - app Android QRCode*

4 Appendice

Il terminale GP08 è una evoluzione del terminale di controllo accessi e controllo presenza DF08: la prestazione aggiunta al sistema è quella di poter essere usato in modalità "Controllo Accessi" per la gestione dei "Green Pass".

Il tipo di "Green Pass" che deve essere accettato non prevede alcuna registrazione di dati sensibili (ai fini della compatibilità con la Privacy) e sono al massimo riportati solo i time stamp di quando è stato utilizzato un Green Pass per accedere.

Nel menu di configurazione del terminale è comunque possibile agire per determinare l'identificazione mediante Green Pass.

Accedere al menu del terminale grazie al touch screen (vd. Fig. 2.1). Una volta che compare il menu, scegliere "sistema": compare la lista di selezione di Fig. 4.1.

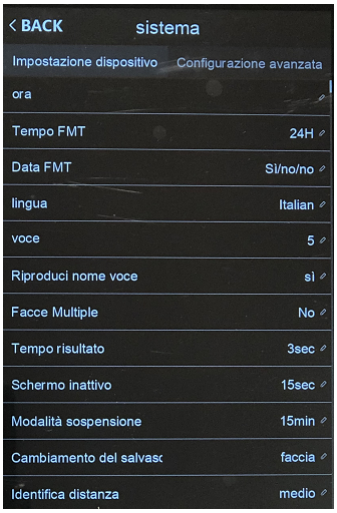


Fig. 4.1. *Menu sistema -> Impostazione dispositivo*

I parametri modificabili hanno le seguenti funzioni:

- Ora -> regola l'ora del terminale
- Tempo FMT -> modifica il formato con cui è mostrata l'ora
- Data FMT -> modifica il formato con cui è mostrata la data
- Lingua -> seleziona la lingua
- Voce -> regola il volume dei messaggi vocali (scala da 1 a 10)
- Riproduci nome voce -> seleziona se all'identificazione dell'utente deve essere pronunciato il nome utente
- Facce Multiple -> indica se il terminale è predisposto per il riconoscimento volti per gruppi di utenti (fino a 5 volti contemporanei)
- Tempo risultato -> stabilisce il tempo durante il quale il risultato di identificazione utente permane sullo schermo

- Schermo inattivo -> regola il tempo per l'avvio del salva-schermo
- Modalità sospensione -> stabilisce il tempo dopo il quale lo schermo si spegne e il terminale va in sospensione
- Cambiamento del salvaschermo -> stabilisce con quale metodo il terminale si attiva dalla condizione di salvaschermo
- Identifica distanza -> regola la distanza entro la quale eseguire il riconoscimento del volto dell'utente

Con un touch sulla voce "Configurazione avanzata" si ottiene la lista di parametri mostrata in Fig. 4.2.

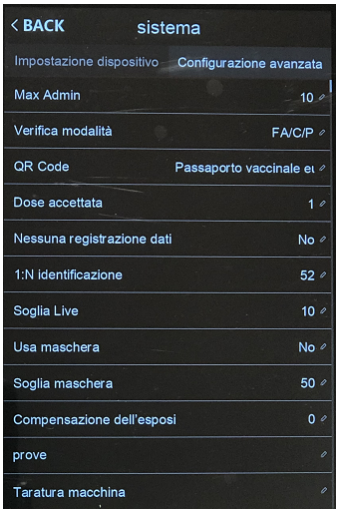


Fig. 4.2. *Menu sistema -> Configurazione avanzata*

I parametri modificabili hanno le seguenti funzioni:

- Max Admin -> numero massimo di utenti con diritti di amministratore
- Verifica modalità -> modalità con la quale eseguire i riconoscimenti di utenti registrati
- QR Code -> modalità con la quale è utilizzata la funzione "QRCode": con la selezione "Passaporto vaccinale Europeo" il terminale diventa un verificatore Green Pass
- Dose accettata -> numero di dosi di vaccino accettate per l'accesso
- Nessuna registrazione dati -> stabilisce che i dati vaccinali non debbano essere memorizzati
- 1:N identificazione -> numero di identificazione nella modalità 1:N
- Soglia Live -> soglia per regolare la sensibilità "live" del terminale
- Usa maschera -> parametro per la selezione della verifica mascherina indossata sul volto
- Soglia maschera -> soglia di lavoro per il riconoscimento della mascherina indossata sul volto
- Compensazione dell'esposizione -> parametro di regolazione dell'esposizione
- Prove -> verifica dell'esposizione IR del terminale
- Taratura macchina -> funzione di taratura del terminale