

**Portale e APP utente per
il sistema antintrusione**



Manuale completo

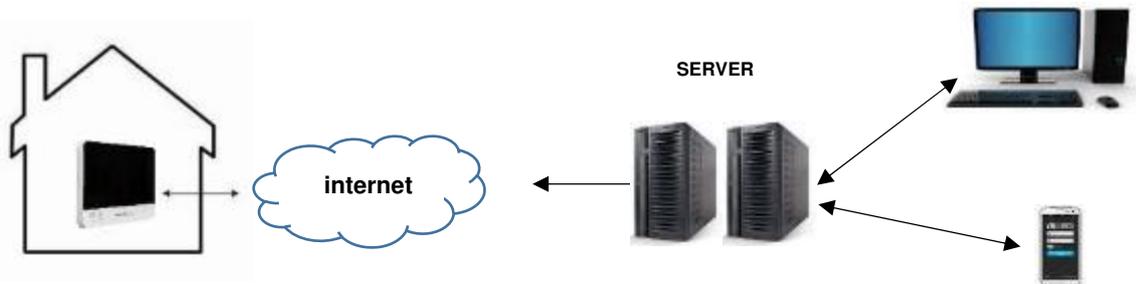
SOMMARIO

1	INTRODUZIONE	3
2	REQUISITI MINIMI E BROWSER COMPATIBILI	3
3	GESTIONE REMOTA DEL SISTEMA	4
3.1	Configurazione di base della centrale.....	4
4	REGISTRAZIONE DI UN NUOVO UTENTE DA PORTALE E APP	5
5	ACCESSO AL PORTALE	9
6	VIDEATA HOME.....	10
6.1	Area Stati del sistema.....	10
6.1.1	Attivazione in presenza di anomalie nel sistema.....	12
6.2	Area Dispositivi	14
6.3	Area Menu e Area connessione	15
6.4	Area telecamere IP	16
7	MENU EVENTI	17
8	TELECAMERE IP	19
9	MENU CONFIGURAZIONI	20
9.1	Modifica Dispositivi.....	21
9.2	Aggiunta e Modifica codici	22
10	IMPOSTAZIONI DI ACCESSO DEGLI UTENTI	23
10.1	Notifiche	25
10.2	Uscita dal portale.....	25
11	UTILIZZO DELLA APP PER SMARTPHONE.....	26
11.1	Tasti di spostamento all'interno della App	30
12	AVVERTENZE GENERALI PER L'USO DI PORTALE E APP	31
12.1	Attivazione con anomalie.....	31
12.2	Connessioni lente o critiche alla rete Internet.....	31
12.3	Uso di codici errati	32

1 INTRODUZIONE

Urmel Zeno è un sistema di sicurezza completo e affidabile per salvaguardare e sorvegliare i vostri ambienti più preziosi, di vita e di lavoro. La gestione e la supervisione avvengono attraverso Internet e sono garantite dal **server Urmel** che, per ogni utente autorizzato, permette il controllo da remoto dello stato del sistema, il monitoraggio degli eventi e la loro verifica in formato immagine e video e la ricezione di notifiche e allarmi. Le funzionalità disponibili sono state progettate per una facile e intuitiva fruizione da qualsiasi pc e tablet sul **portale Urmel multi-browser** e dal vostro **smartphone Android** o **iOS** utilizzando l'APP dedicata.

Il sistema ZENO protegge la vostra casa da qualsiasi luogo vi troviate:



LA TECNOLOGIA UTILIZZATA

Il sistema **ZENO** basa la sua tecnologia wireless sulla doppia connettività ADSL - IP/4G.

Entrambe sono garantite da una piattaforma dedicata alla quale l'utente può connettersi tramite la propria rete di casa e da remoto tramite cellulare, assicurandosi i servizi di controllo e monitoraggio.

- ☞ la rete ADSL permette migliori prestazioni nell'accesso remoto e nel caricamento di video e foto;
- ☞ la doppia connessione garantisce che, in caso di interruzione di una di esse, il sistema continui a funzionare in tutte le sue funzionalità.

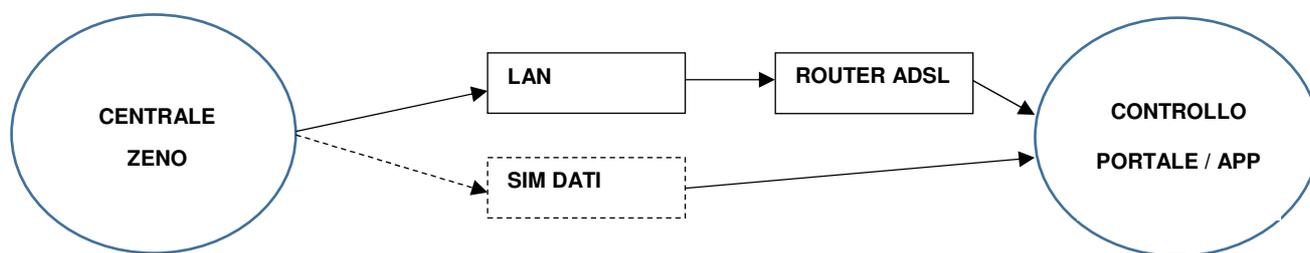
2 REQUISITI MINIMI E BROWSER COMPATIBILI

- Sistema operativo Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista, 7, 8 o 10.
- Microsoft Internet Explorer 5.x o successivo o Google Chrome (consigliato).
- CPU: Intel Pentium II 266 MHz o superiore.
- Memoria: 64 MB o più.
- Risoluzione VGA: 800x600 o superiore.

STRUTTURA DEL SISTEMA

Il sistema di comunicazione tra la centrale e i dispositivi utilizza segnali radiofrequenza a 868 MHz e 2,4 GHz.

La tecnologia radio e l'alimentazione a batteria dei dispositivi ZENO consentono di non modificare l'infrastruttura elettrica esistente con cablaggi complessi.



Per maggiori dettagli vedere il manuale di installazione della Centrale ZENO.

3 GESTIONE REMOTA DEL SISTEMA

Accesso al portale

Per accedere al portale è sufficiente digitare, da uno dei browser internet indicati, il seguente indirizzo: <https://www.zeno.urmet.com/home>.

Nei capitoli dedicati al portale del presente manuale verrà descritta la procedura di registrazione al portale e il suo utilizzo.

Accesso alla APP

L'applicazione **MyZeno** è disponibile sul Play Store o sull'APP Store per smartphone e per tablet Android e iOS. La versione minima richiesta per dispositivi Android è Android 5.0. Per dispositivi iOS è iOS 7.

La migliore visualizzazione dell'interfaccia si ha con display di dimensioni maggiori di 4,5 pollici.

Nei capitoli dedicati alla APP del presente manuale verrà descritto il suo utilizzo.

<NOTA>

Per accedere alla APP occorre essere già registrati. La registrazione come nuovo utente deve essere effettuata dal portale o dalla stessa APP e la password ottenuta dalla procedura di registrazione è valida per accedere al sistema ZENO sia con la APP che con il portale.

3.1 CONFIGURAZIONE DI BASE DELLA CENTRALE

Questo manuale vi guiderà attraverso le modalità di registrazione al portale e il funzionamento dello stesso e della APP utente: dal controllo dello stato di attivazione e disattivazione del sistema di sicurezza alla gestione dei singoli dispositivi e all'invio di report in caso di allarme.

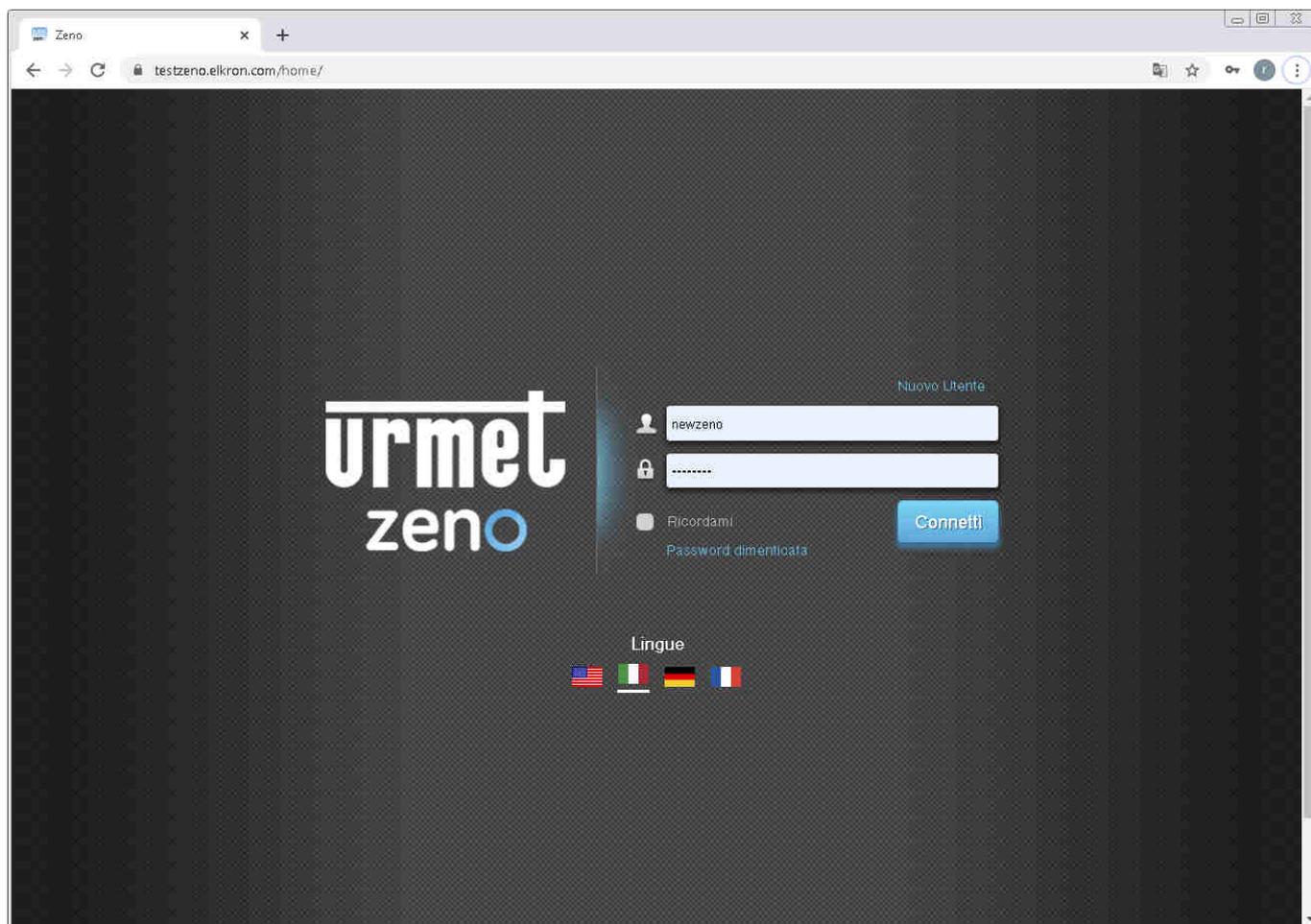
La registrazione al portale presuppone la configurazione completa della centrale da parte dell'installatore. A tale scopo si può fare riferimento ai manuali tecnici di installazione e programmazione forniti a corredo della centrale, verificando le impostazioni di rete e lo stato di connessione attiva al server Urmet.

4 REGISTRAZIONE DI UN NUOVO UTENTE DA PORTALE E APP

La registrazione di un nuovo utente richiede alcune operazioni preliminari sulla centrale da parte dell'installatore, che iniziano con il distacco dell'alimentazione e della batteria della centrale e si concludono con l'inserimento dei dati identificativi dell'utente e della centrale, a cura dell'utente stesso. Questa procedura deve concludersi entro un tempo di 15 minuti dal momento in cui la centrale viene alimentata. Terminato questo tempo senza aver concluso la procedura, si dovrà nuovamente togliere alimentazione alla centrale per far ripartire i 15 minuti di tempo.

Passo 1.

Da uno dei browser indicati, digitare l'indirizzo <https://www.zeno.urmet.com/home>. Apparirà la seguente videata:



<NOTA>

In caso di problemi nel caricamento del portale web, occorre regolare il livello di protezioni del browser.

Passo 2.

Cliccate su **Nuovo Utente** per avviare la procedura di registrazione, grazie alla quale verrà effettuato l'abbinamento del **Mac Address** (indirizzo identificativo univoco) della vostra centrale al vostro Account (utente master). Per completare le operazioni di registrazione come nuovo utente, utilizzate il tasto SUCCESSIVO per procedere da una videata all'altra e il tasto INDIETRO per visualizzare quella precedente. Procedete nel seguente modo:

- 1) *Togliere alimentazione e batteria dalla centrale e connettere il router*
- 2) *Ridare alimentazione alla centrale **ricordandosi di abilitare la batteria***
- 3) *Attendere che i led della centrale si illuminino*

Passo 3.

Terminate le operazioni sulla centrale, un ulteriore click sul tasto SUCCESSIVO aprirà la videata per l'inserimento delle informazioni di accesso richieste all'utente.

In questa videata si dovrà creare un nome utente e una password per l'utente principale (master), che serviranno per accedere normalmente sia al portale che alla APP.

The screenshot shows a registration form titled 'Informazioni' (Information). At the top, there are three progress indicators: 'Informazioni' (active), 'Info Personali' (Personal Info), and 'Informazioni registrazione' (Registration Info). The form contains the following fields:

- Utente: portzeno
- Password: [masked with dots]
- Conferma Password: [empty]
- Indirizzo Email: [empty]
- Conferma l'Email: [empty]
- Prefisso: Italia (dropdown menu)
- Cellulare: [empty]
- Tel. fisso: Tel. fisso

At the bottom, there is a checkbox labeled 'Ho letto e approvo la seguente documentazione [Termini e Condizioni](#)'. Below the checkbox are two buttons: 'Indietro' (Back) and 'Successivo' (Next).

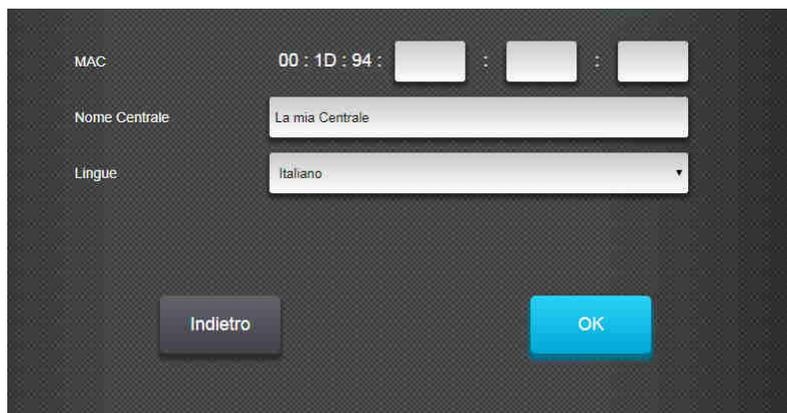
Le informazioni indispensabili in questa videata sono quelle relative a **Utente**, **Password** e **E-mail**. Dopo aver completato i campi, si potrà passare alla videata successiva, le *Informazioni Personali*:

The screenshot shows a registration form titled 'Info Personali' (Personal Info). At the top, there are three progress indicators: 'Informazioni' (inactive), 'Info Personali' (active), and 'Informazioni registrazione' (inactive). The form contains the following fields:

- Nome: [empty]
- Cognome: [empty]
- Indirizzo: [empty]
- Città: [empty]
- Stato: [empty]
- CAP: [empty]

At the bottom, there are two buttons: 'Indietro' (Back) and 'Successivo' (Next).

Cliccando su SUCCESSIVO si passa alla videata per l'inserimento delle *Informazioni di registrazione* della centrale:



MAC 00 : 1D : 94 : [] : [] : []

Nome Centrale La mia Centrale

Lingue Italiano

Indietro OK

MAC: il *mac address* è reperibile sul coperchio posteriore della centrale e consente al server Elkron di abbinare la vostra centrale al vostro Account, rendendo disponibili gli strumenti di controllo remoto sia dal portale che dalla APP.

NOME CENTRALE: è il nome che si può dare alla centrale e che comparirà nelle Notifiche e nelle Email

LINGUA: scelta Italiano/Inglese/Francese.

Passo 4.

Cliccando sul tasto OK verrà completata la procedura di registrazione. Il seguente messaggio di conferma apparirà a video e verrà inviato all'indirizzo email indicato. Cliccando su OK si ritornerà alla pagina iniziale con nome utente e password già inseriti.



La procedura di registrazione appena descritta può essere effettuata anche dalla APP (versione 1.8.31 o successiva).

Digitando sul tasto **CONNETTI** (tasto **ACCESSO** dalla APP) della pagina iniziale, si potrà accedere alle videate di gestione della centrale.

Se viene visualizzato un messaggio di errore come quello sottostante, significa che l'Account è già presente sul database Urmet. Occorre quindi reperire le credenziali dell'utente master che per primo ha effettuato la registrazione.



Altri messaggi di errore possono essere:

***“Non è possibile connettersi alla centrale,
controllare lo stato della connessione!”***

In questo caso, la centrale non è connessa al server: potrebbe non essere alimentata o esserci un problema di connessione a Internet. Verificate l'alimentazione e lo stato della connessione. Controllate la configurazione del filtro dei Mac Address impostato sul router, accertandosi che il mac address della centrale sia autorizzato.

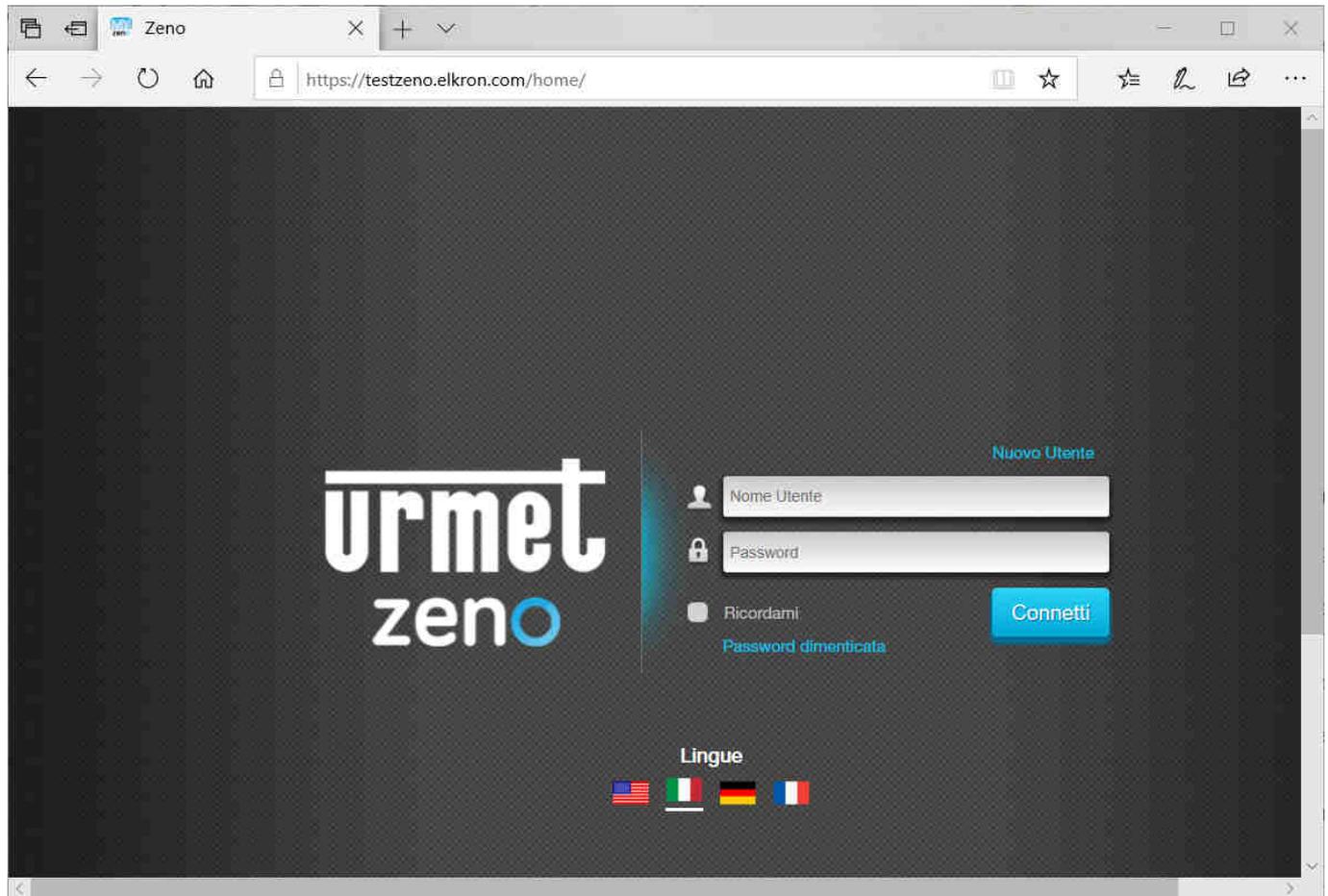
Tempo di registrazione scaduto

La registrazione della centrale non si è conclusa entro 15 minuti dal momento in cui la centrale viene alimentata.

Nel caso in cui il mac address sia corretto e la centrale connessa ma i problemi persistono, occorre rivolgersi al centro assistenza Urmet.

5 ACCESSO AL PORTALE

Una volta registrati al portale, dal link <https://www.zeno.urmet.com/home> inserite il vostro nome utente e password:

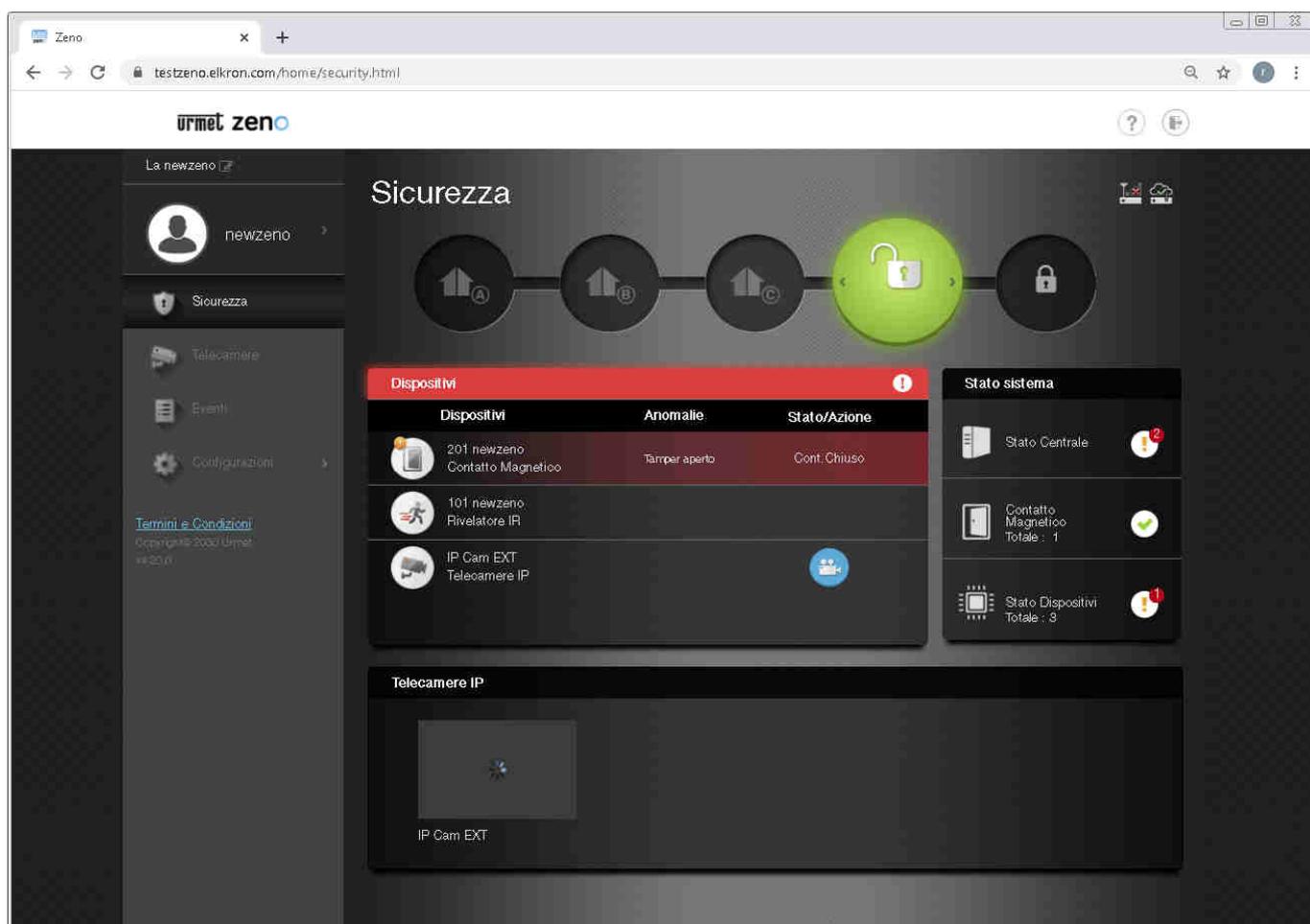


In questa prima videata è possibile **memorizzare** le credenziali di accesso per i successivi utilizzi e **recuperare** la password eventualmente dimenticata (in questo caso il server azzerà quella corrente e ne invia una nuova al vostro indirizzo email).

Cliccate su CONNETTI per accedere alle videate di gestione della vostra centrale.

6 VIDEATA HOME

Questa prima videata è la pagina principale del vostro account. Da qui è possibile accedere alle altre sezioni del portale e visualizzare lo stato del sistema e la lista dei dispositivi relativi all'impianto antifurto (Sicurezza), appresi all'interno della vostra centrale. Nel seguito verranno approfondite le varie aree di cui è composta la videata:

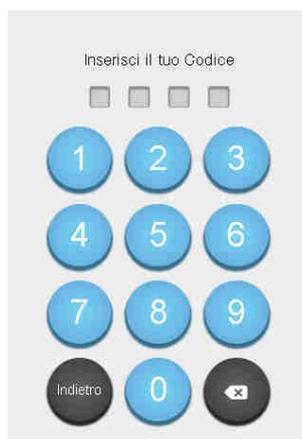


6.1 AREA STATI DEL SISTEMA

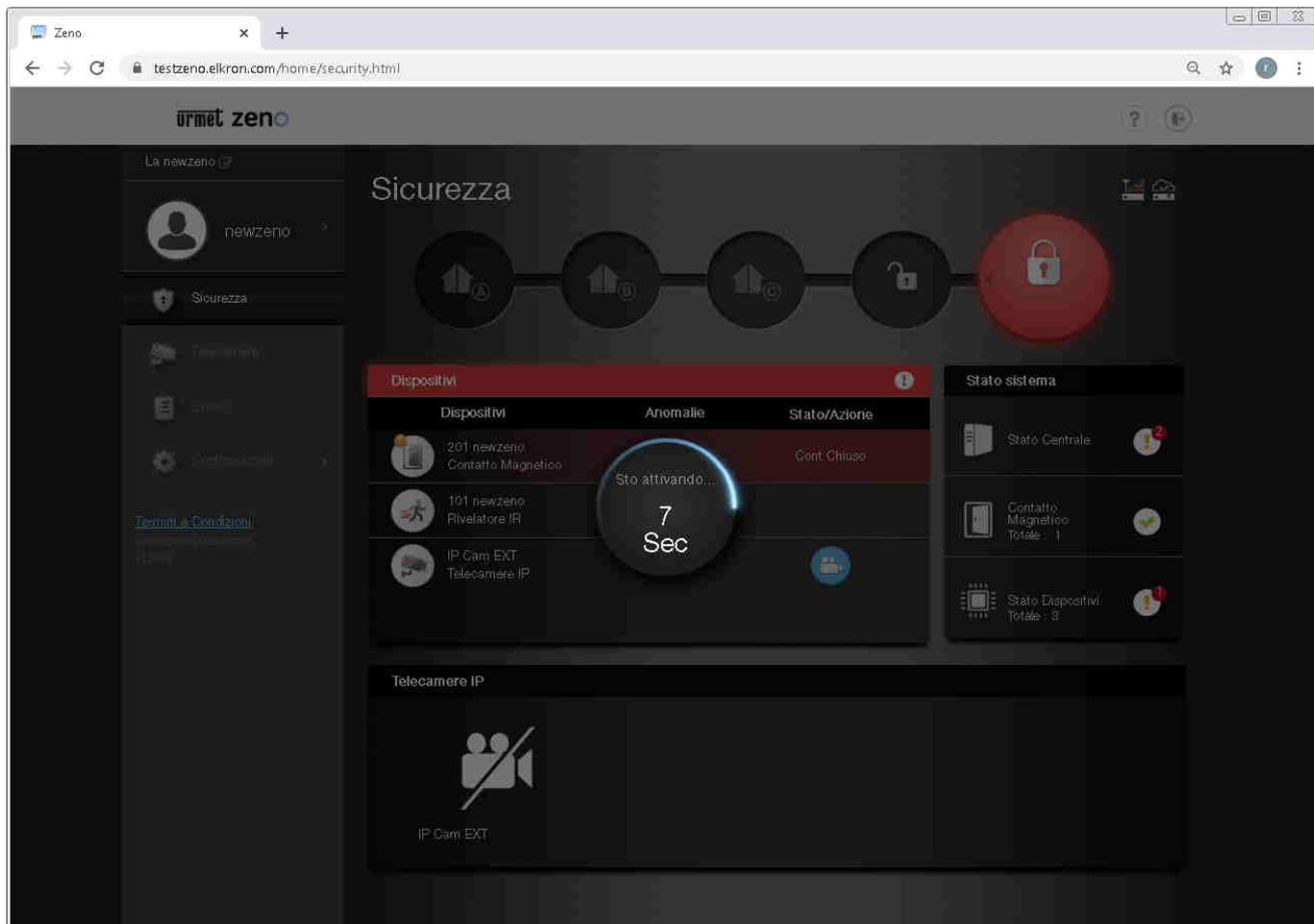
Lo stato del sistema è indicato dalle 5 icone nella parte superiore. L'icona evidenziata indica lo stato corrente del sistema. Nell'esempio, l'icona verde indica che il sistema è DISATTIVO.



Ogni volta che si vuole cambiare stato, cliccando sulla singola icona, viene richiesto l'inserimento del codice utente (default 1234). Digitare le singole 4 cifre del vostro codice:



Dopo aver digitato il codice corretto, il sistema passa dallo stato *DISATTIVO* allo stato *ATTIVO* o *ATTIVO PARZIALE* al termine del conteggio del Tempo di Uscita della centrale, se previsto:



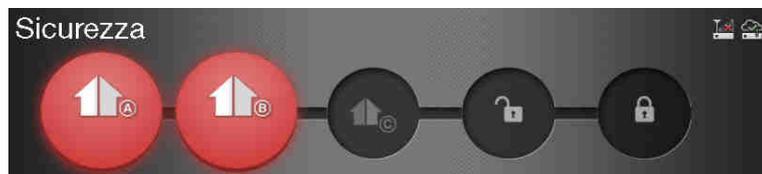
Lo stato *ATTIVO TOTALE* del sistema verrà visualizzato dall'accensione dell'icona corrispondente:



Lo stato di *ATTIVAZIONE PARZIALIZZATA* di uno o più settori del sistema verrà visualizzato dall'accensione dell'icona corrispondente (nell'esempio il settore A):



Per attivare più di un settore, ad esempio A+B come nell'esempio sottostante, premete sulle singole icone, vi verrà richiesto l'inserimento del codice per entrambi i settori.

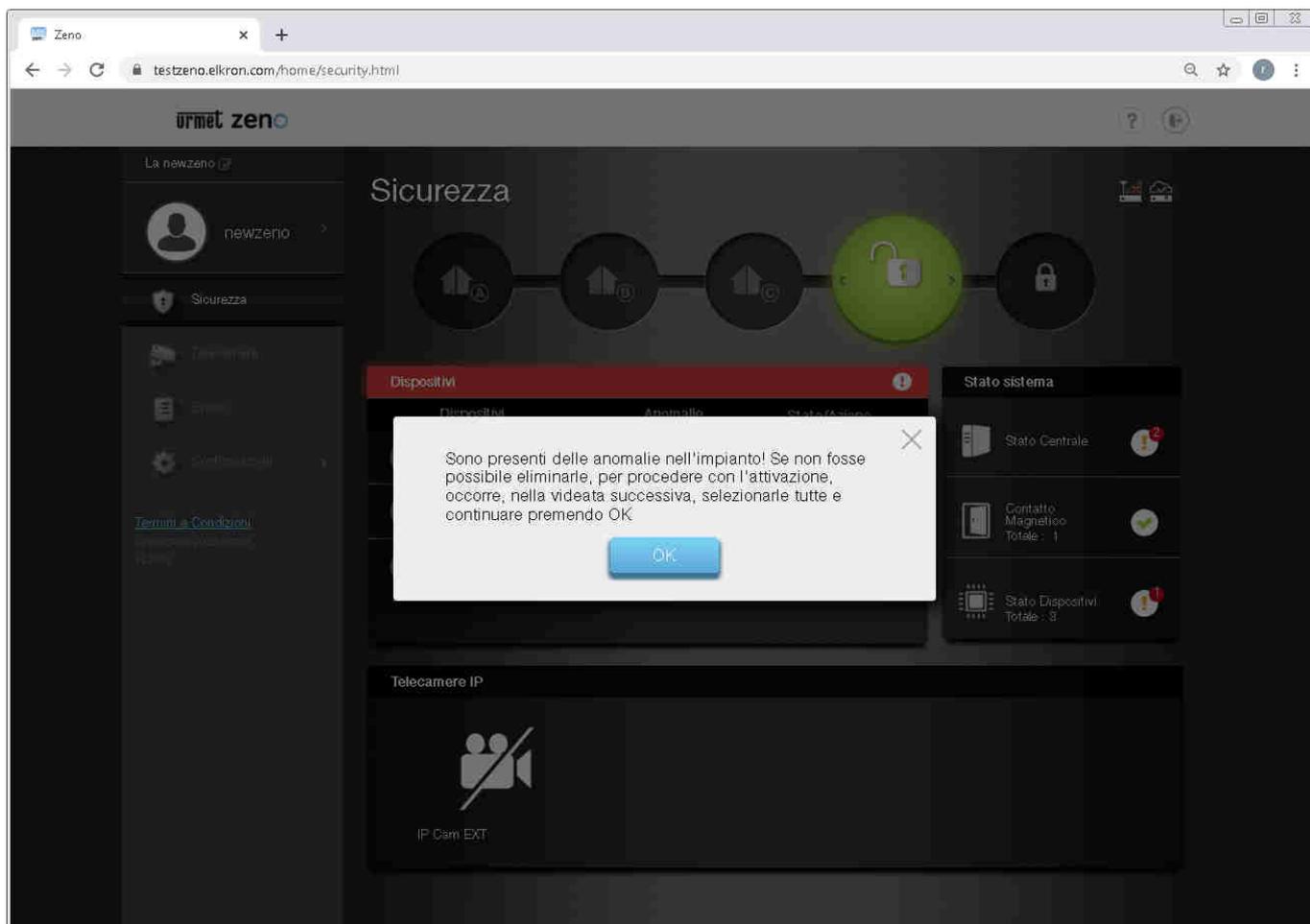


L'eventuale inserimento di un codice errato visualizzerà il seguente messaggio e l'azione voluta non avrà luogo fino all'inserimento di un codice corretto:



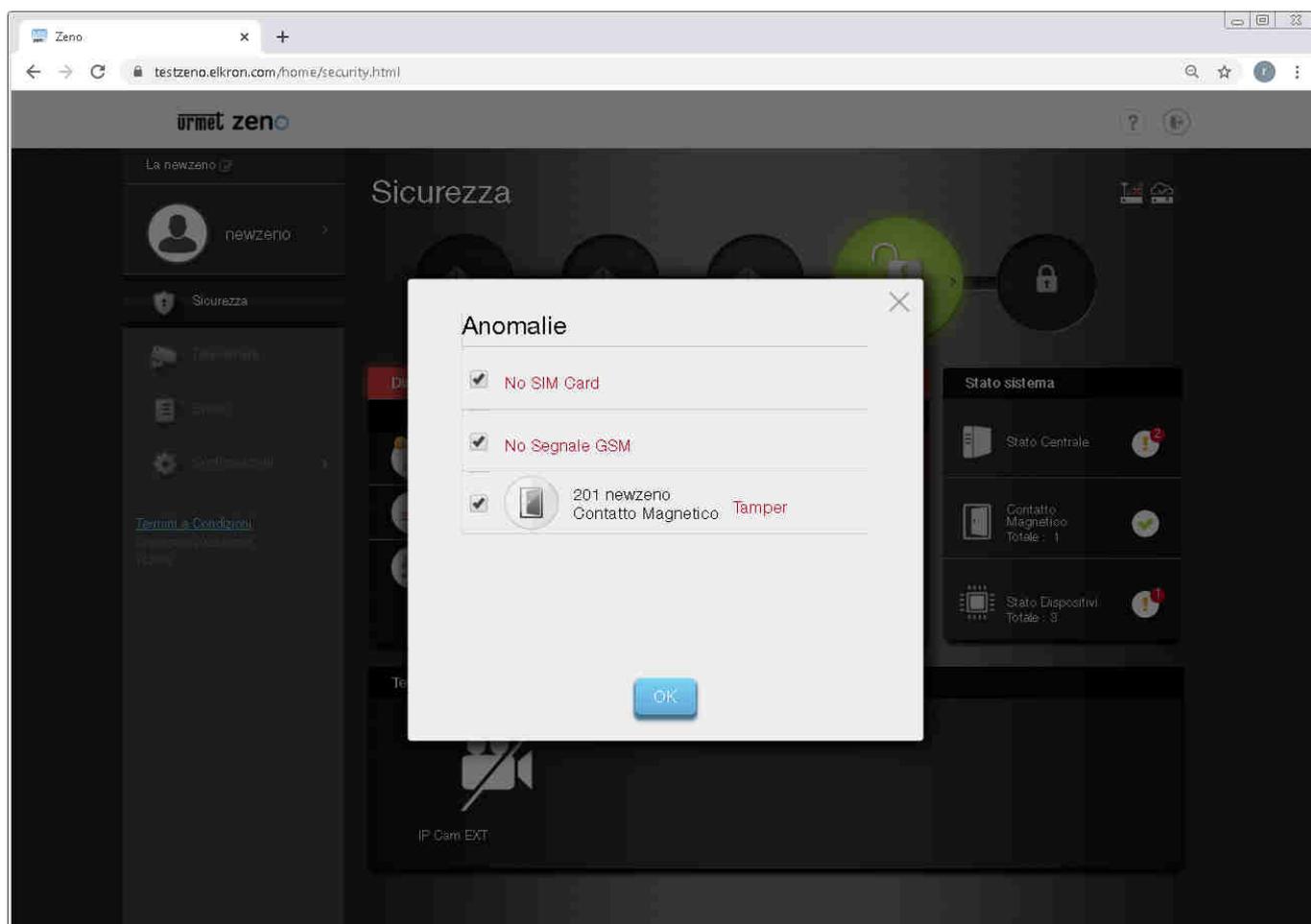
6.1.1 Attivazione in presenza di anomalie nel sistema

In fase di attivazione dell'impianto, il portale visualizzerà il seguente messaggio in presenza di eventuali anomalie nel sistema (ad esempio un contatto aperto):



Premendo il tasto OK per proseguire nell'attivazione, il portale visualizzerà l'elenco delle anomalie presenti nel sistema.

Per poter completare l'attivazione sarà necessario spuntarle tutte:

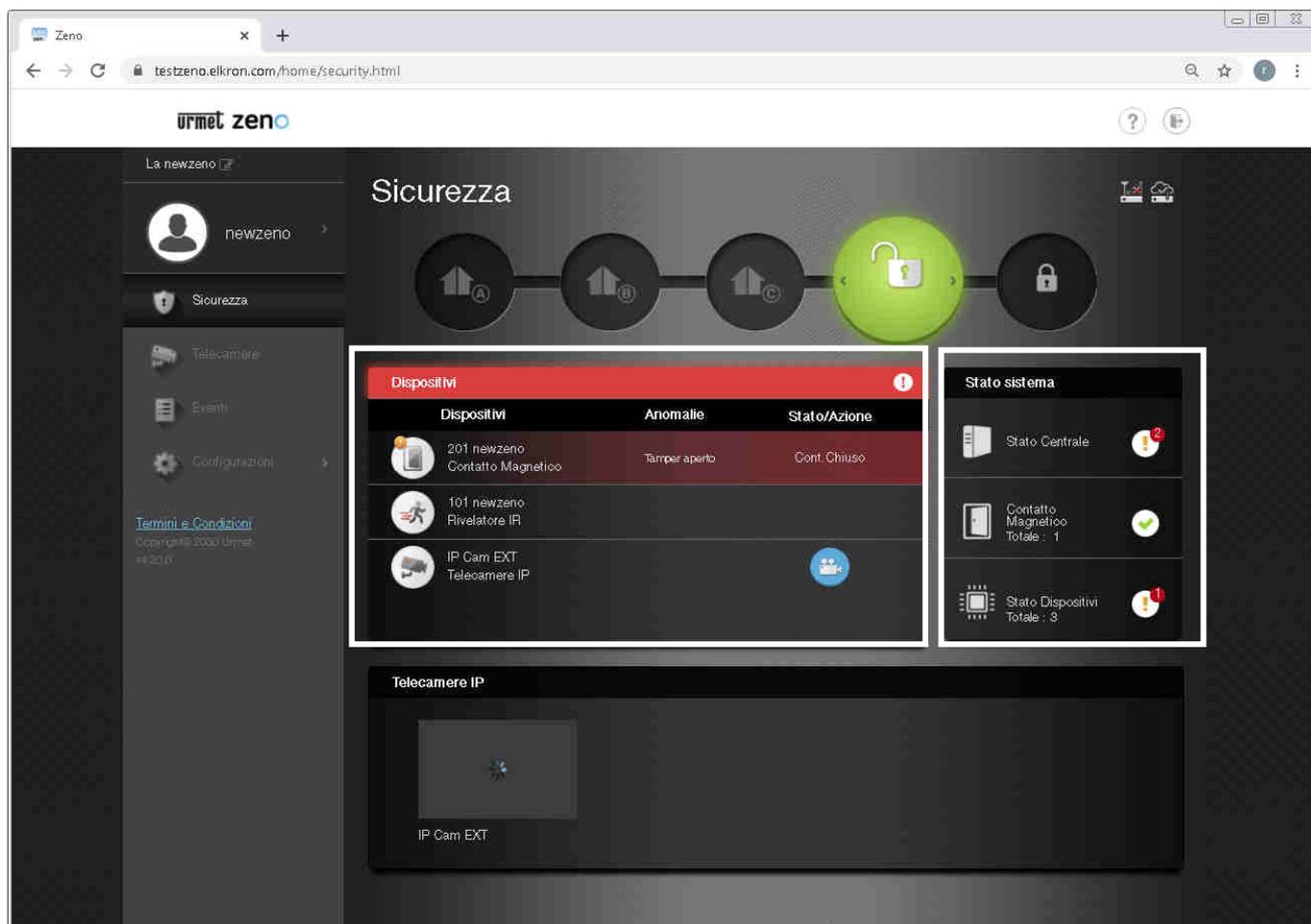


In presenza di Anomalie, raccomandiamo di leggere attentamente il paragrafo “Attivazioni con anomalie” nella sezione *Avvertenze* al fondo di questo manuale.

6.2 AREA DISPOSITIVI

Nelle due aree evidenziate dai riquadri sono visibili:

1. il dettaglio di tutti i singoli **dispositivi** dell'area Sicurezza;
2. lo **stato del sistema**, cioè la visualizzazione di eventuali anomalie della centrale, dei dispositivi che controllano l'accesso dei varchi (stato di aperto/chiuso) e dei dispositivi che fanno parte del vostro sistema.



Per ogni dispositivo è possibile visualizzare:

- ☞ **Tipo dispositivo** (contatto porta, sirena, tastiera, telecomando, rivelatore, ripetitore, ecc.)
- ☞ **Nome assegnato** (modificabile da parte dell'utente master);
- ☞ **Anomalie del dispositivo** che possono essere:
 - tamper aperto, relativo all'involucro di un dispositivo manomesso
 - batteria scarica, indicante il livello insufficiente della batteria
 - fuori servizio (ad esempio, se alla richiesta di foto/video, un rivelatore non risponde)
 - supervisione (se la centrale non riceve segnali da un dispositivo per un periodo predefinito)

La presenza di anomalie sul dispositivo viene evidenziata con il colore rosso dell'intera riga che lo descrive.

☞ **Stato/Azione** che possono essere:

- aperto/chiuso, se si tratta di un contatto porta, di solito un dispositivo a protezione di un varco
- l'azione che si può intraprendere cliccando sulla corrispondente icona, se si tratta di un rivelatore con fotocamera o videocamera



"Scatta una foto"



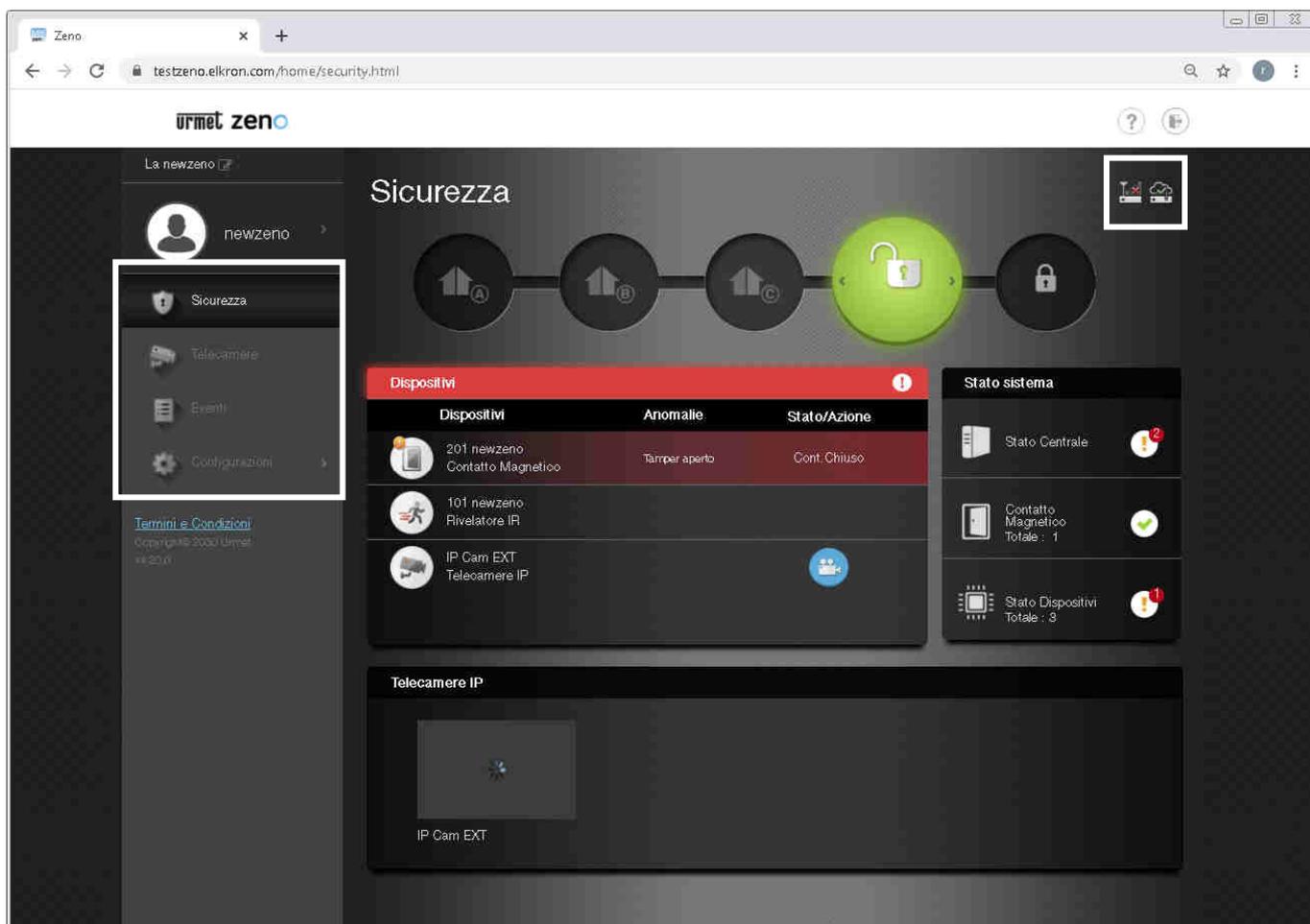
"Riprendi una scena"

☞ **Dispositivo escluso**. Qualora un dispositivo fosse stato escluso.

L'esclusione del dispositivo viene evidenziata con il colore giallo dell'intera riga che lo descrive.

6.3 AREA MENU E AREA CONNESSIONE

A sinistra della videata si trova l'area di accesso agli altri menu del portale, mentre in alto a destra si trova l'area della connessione.



AREA MENU

Da quest'area è possibile ritornare sempre alla **Home**, cliccando sul menu **Sicurezza**. In quest'area sono disponibili i seguenti menu:

- 👉 **Telecamere IP**: gestione delle telecamere IP associate alla centrale
- 👉 **Eventi**: dove viene visualizzato l'elenco completo delle varie interazioni da parte dell'utente con la centrale e le situazioni di allarme che si verificano.
- 👉 **Configurazioni**: sezione dedicata alla configurazione dei dispositivi, degli utenti e delle modalità di ricezione dei report. Inoltre da qui è possibile generare il codice temporaneo per l'installatore che deve effettuare una manutenzione sul sistema.

*NOTA. Il menu **Configurazioni** è riservato esclusivamente all'utente master e non è visibile agli utenti secondari.*

Nelle pagine successive, questi menu verranno descritti in dettaglio.

AREA CONNESSIONE

Le due icone nella parte alta a destra della videata **Home** forniscono informazioni sullo stato della connessione.



la centrale è connessa al server (con rete Ethernet e router o con rete 4G)



la centrale è disconnessa dal server



la SIM della centrale è connessa alla rete cellulare GSM ed è in grado di inviare chiamate vocali e SMS.

ATTENZIONE! questa informazione non è relativa all'effettiva connessione alla rete dati 4G.

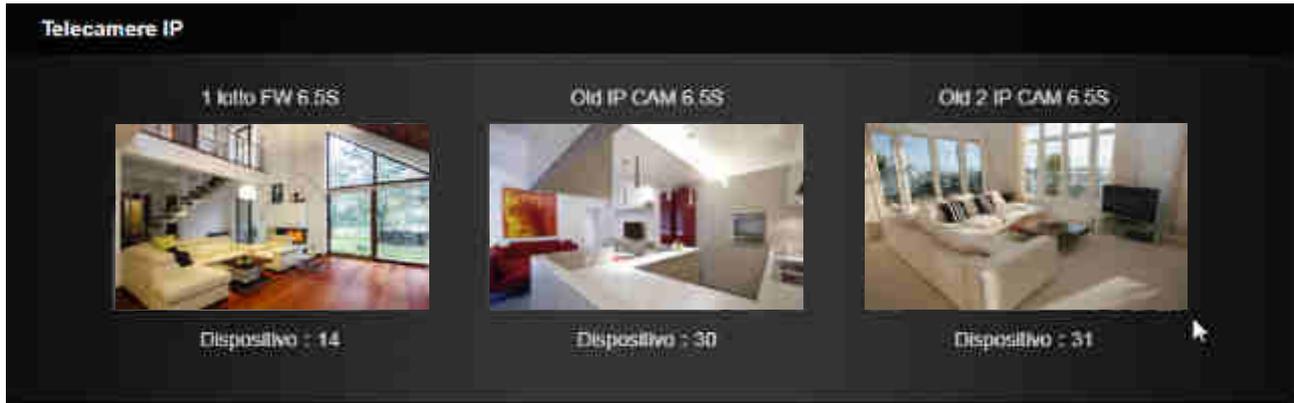


la SIM della centrale potrebbe essere mancante o non connessa alla rete cellulare GSM, oppure potrebbe avere una connessione critica o non stabile.

ATTENZIONE! In questo caso è indispensabile garantire una connessione fissa via cavo su rete Ethernet

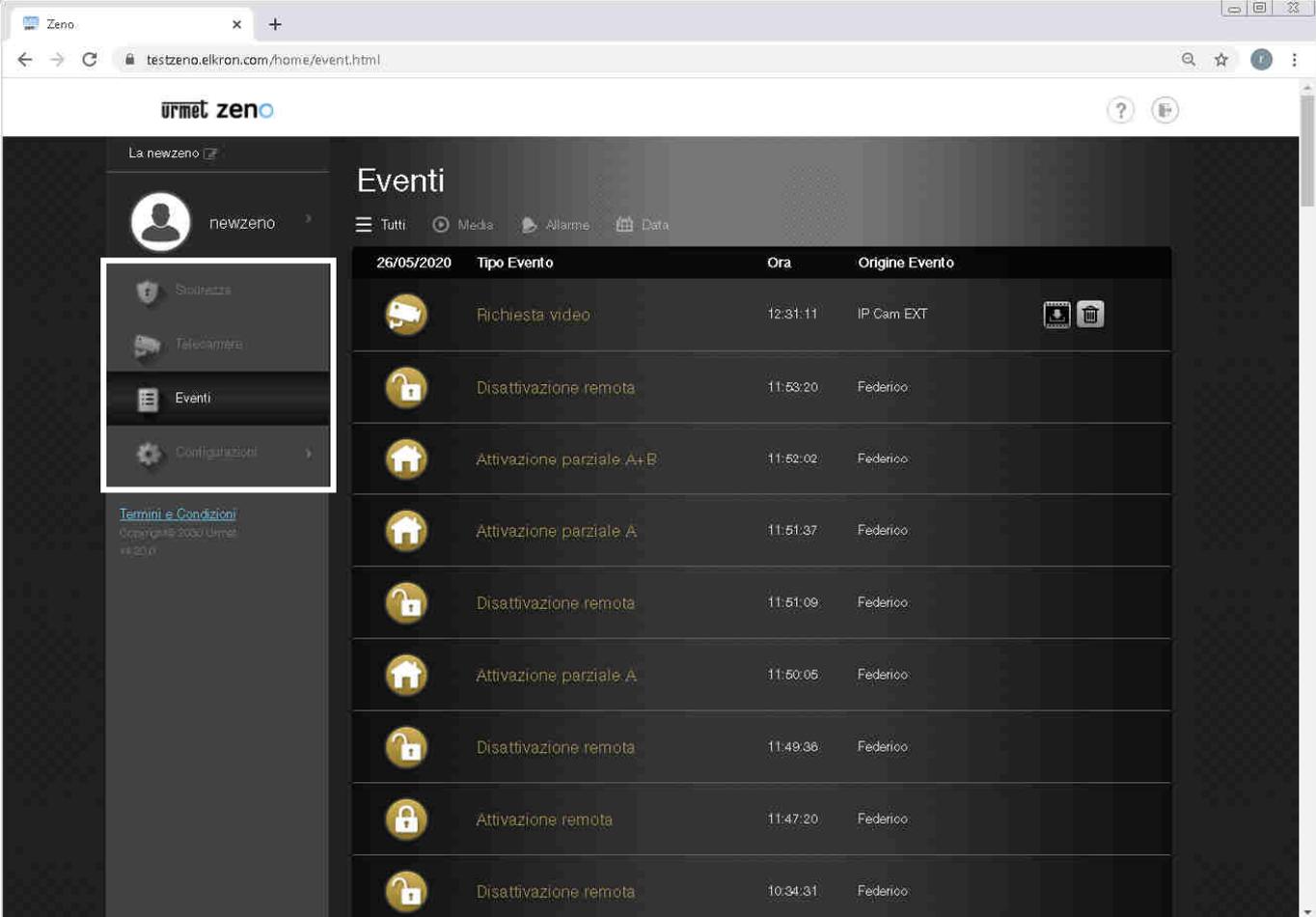
6.4 AREA TELECAMERE IP

L'area delle telecamere IP mostra le immagini relative alle telecamere associate alla centrale. Con un doppio click del mouse è possibile ingrandire l'immagine e accedere alla pagina dedicata al controllo.



7 MENU EVENTI

Cliccando sulla voce **Eventi** nell'area dei menu, si accede alla tabella in cui vengono tracciati e tenuti in memoria tutti gli eventi verificatisi nel sistema.



The screenshot shows a web browser window with the URL `testzeno.elkron.com/home/event.html`. The interface is dark-themed and features a sidebar menu on the left with options: **Struttura**, **Telecamera**, **Eventi** (highlighted), and **Configurazioni**. The main content area is titled **Eventi** and includes filter buttons for **Tutti**, **Media**, **Allarme**, and **Data**. Below the filters is a table of events for the date 26/05/2020.

26/05/2020	Tipo Evento	Ora	Origine Evento
	Richiesta video	12:31:11	IP Cam EXT
	Disattivazione remota	11:53:20	Federico
	Attivazione parziale A+B	11:52:02	Federico
	Attivazione parziale A	11:51:37	Federico
	Disattivazione remota	11:51:09	Federico
	Attivazione parziale A	11:50:05	Federico
	Disattivazione remota	11:49:36	Federico
	Attivazione remota	11:47:20	Federico
	Disattivazione remota	10:34:31	Federico

Gli eventi vengono registrati per data, tipo, ora e origine dell'evento. A seconda del tipo di evento, nell'ultima colonna "Origine evento" possono essere visualizzati:

- ☞ i **dispositivi** che vengono coinvolti nell'evento di segnalazione e di allarme o richiesta foto/video
- ☞ l'**utente** che ha provocato un cambiamento di stato
- ☞ il **sistema** per test periodici, allarme tamper della centrale, guasti di supervisione e assenza di rete o batteria della centrale

Gli eventi possono essere filtrati attraverso le selezioni disponibili:

- ☞ **Tutto**: vengono visualizzati tutti gli eventi (in rosso gli allarmi, in giallo tutti gli altri) e le immagini/video ripresi
- ☞ **Media**: vengono visualizzati immagini e video acquisiti automaticamente dai rivelatori con fotocamera e videocamera in caso di allarme o richiesti dall'utente nella sezione *Home* attraverso le icone fotocamera e videocamera.

<NOTA>

Immagini e video rimangono disponibili sul server per 30 giorni, dopodiché vengono eliminati.

- ☞ **Allarmi**: vengono notificati gli allarmi intrusione, panico e tamper di qualsiasi dispositivo di sicurezza. Le immagini e i filmati acquisiti in caso di intrusione possono essere consultati selezionando *Tutto* o *Media*.
- ☞ **Data**: si può scegliere di visualizzare gli eventi di un giorno specifico. Cliccare sul campo **Data** e inserire il giorno di interesse nel formato GG/MM/AAAAA (giorno, mese e anno, ad esempio 20/04/2020).

Nelle selezioni *Tutto* e *Media*, per visualizzare immagini e video o per cancellarli, utilizzare le icone disponibili in corrispondenza del dispositivo con fotocamera/videocamera:



cancella



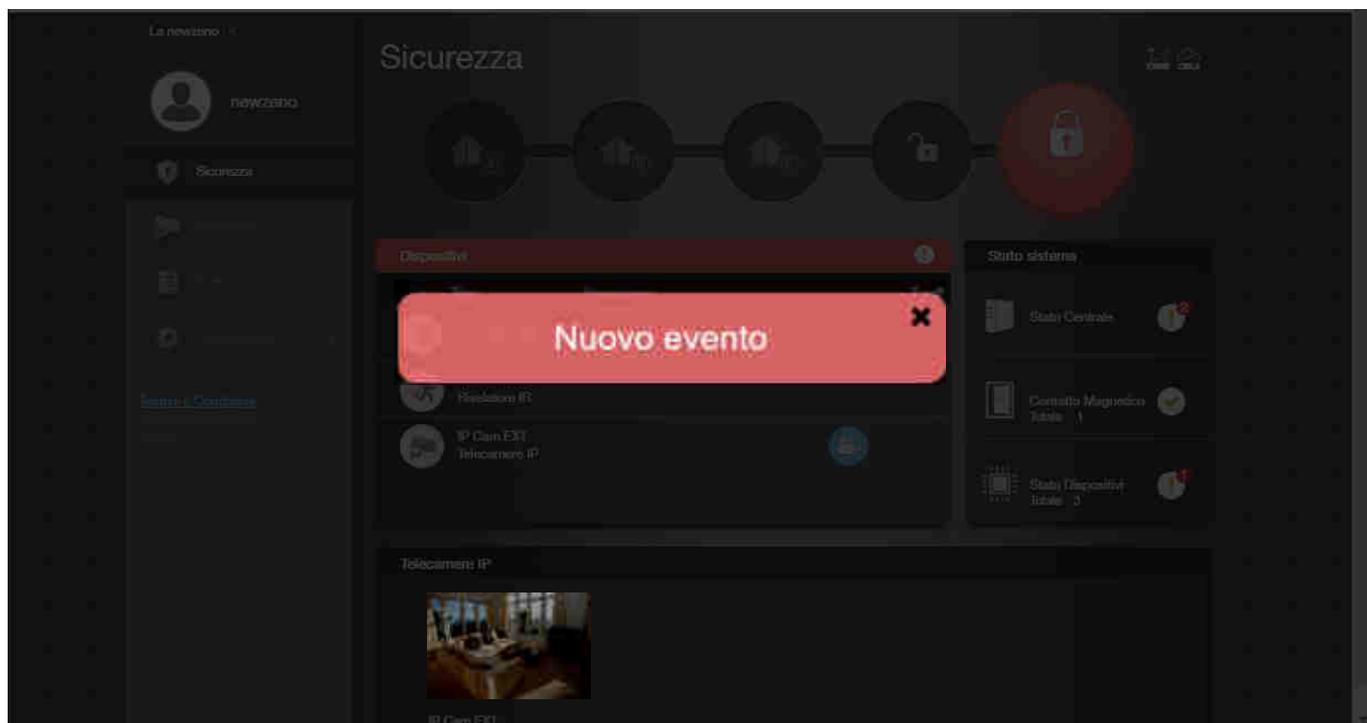
visualizza video



visualizza immagine

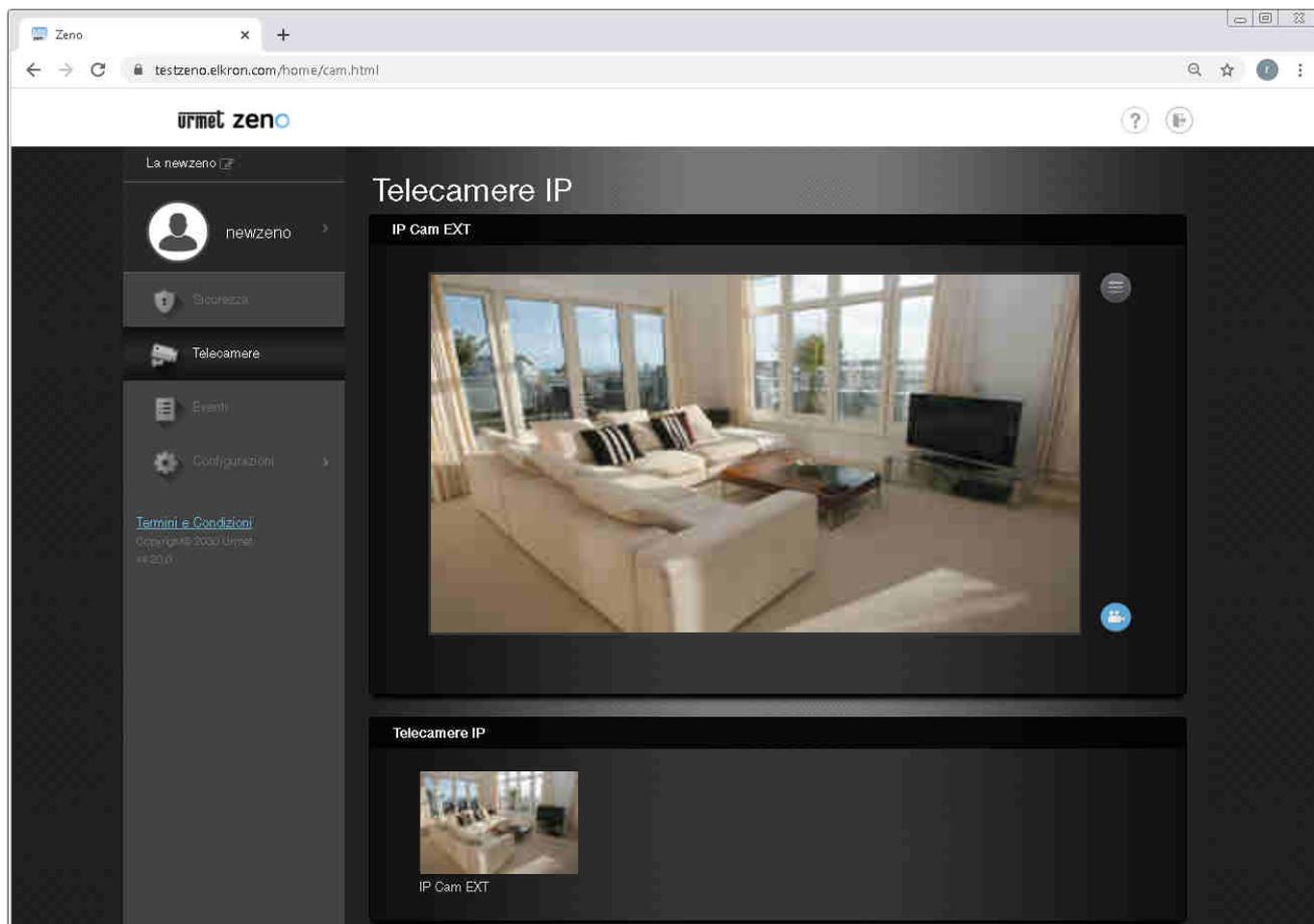
In presenza di un evento di intrusione, il portale visualizza il pop up **NUOVO EVENTO**. Nella lista **Eventi**, l'allarme viene immediatamente registrato ed è subito visibile. Nel caso in cui un dispositivo fotocamera/videocamera venga allarmato, le immagini o i video ripresi impiegano qualche minuto prima di essere resi consultabili sul portale, il tempo necessario al server per acquisirli e inviarli all'applicativo.

Esempio di notifica di allarme sul portale in caso di intrusione:



8 TELECAMERE IP

Questa pagina fornisce la visione delle telecamere IP associate alla centrale.



LISTA TELECAMERE IP

L'area *Telecamere IP* mostra le immagini relative alle telecamere associate alla centrale. Con un doppio click del mouse è possibile ingrandire l'immagine e accedere alla pagina dedicata al controllo.

Regolazioni Video

-  Questa icona permette di accedere al menu delle regolazioni video.

Registrazioni Video

-  Cliccando su questa icona si può richiedere la registrazione di un video. I parametri di registrazione sono definiti nella configurazione della telecamera (vedere manuali dedicati).

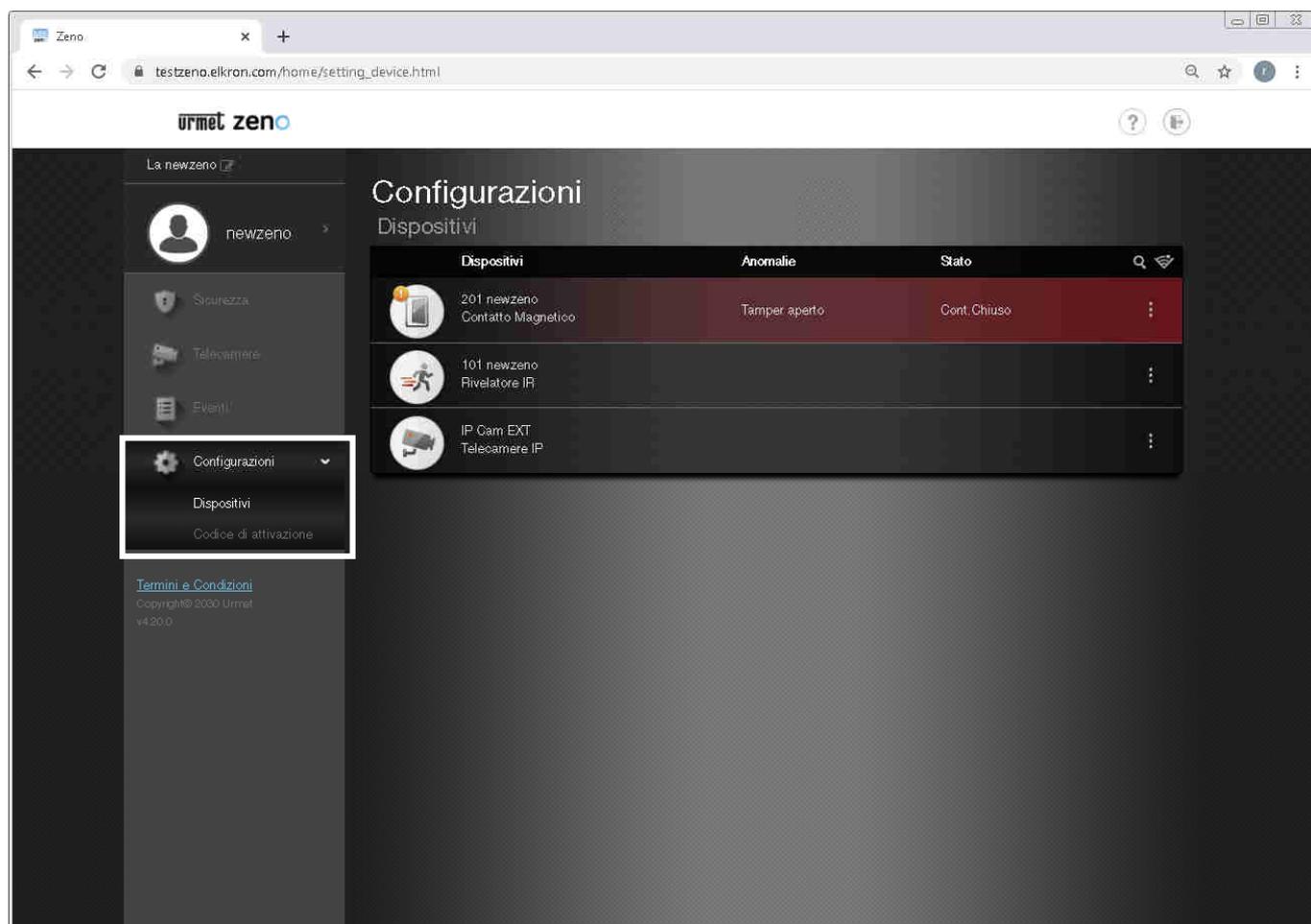
<NOTA>

-  Altre configurazioni relative alle telecamere IP sono disponibili nel menu Configurazioni/Dispositivi. Per le spiegazioni complete sull'uso delle programmazioni relative alle telecamere IP, fare riferimento al manuale della telecamera stessa.

9 MENU CONFIGURAZIONI

In questa sezione, **riservata e visibile esclusivamente all'utente master**, è possibile impostare alcune caratteristiche dei dispositivi, i codici di gestione della centrale, l'invio di report e il Codice Installatore temporaneo.

Per accedere a questo menu cliccate su **Configurazioni** dal menu di destra.



La videata **Configurazioni** si presenta con la lista dei dispositivi che fanno parte del sistema, corrispondente al sottomenu *Dispositivi*.

Le colonne hanno il seguente significato:

- ☞ **Dispositivo**: tipo di sensore e nome attribuito.
- ☞ **Anomalie**: viene fornita una sintetica spiegazione dell'errore.
- ☞ **Stato**: indica lo stato di Fuori Servizio o di Contatto aperto (solo per i Contatti Magnetici).
- ☞  in quest'area è possibile eseguire il Walk Test per verificare la portata radio di ogni singolo dispositivo. Cliccando sull'icona, la centrale si predispone per ricevere un codice di test da parte del dispositivo (vedere le singole istruzioni per l'invio).
- ☞  tramite la funzione lente è possibile cercare uno specifico dispositivo all'interno dell'elenco.

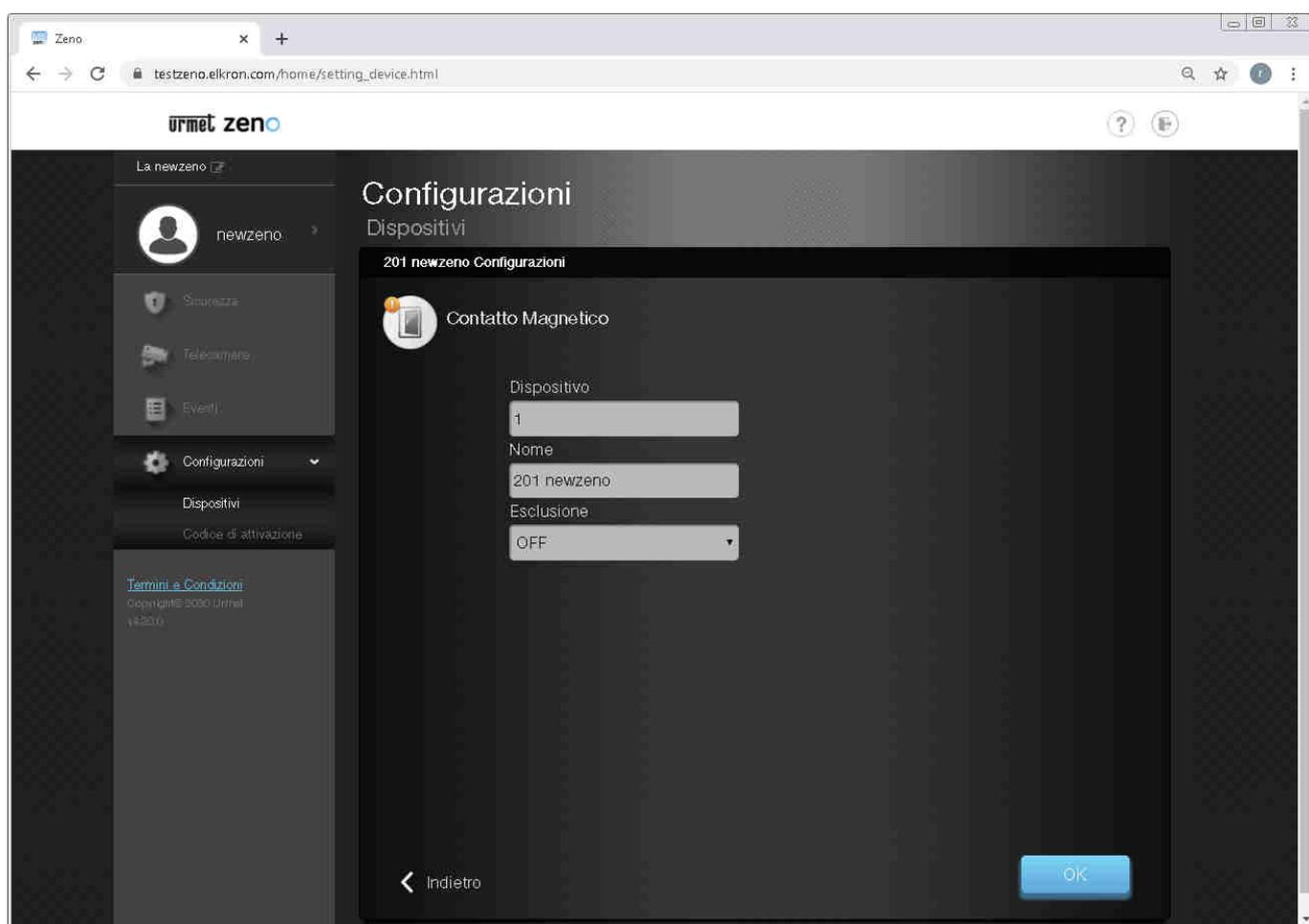
Esempio Walk Test

Nell'esempio sottostante sono visualizzati i dispositivi appartenenti alla centrale su cui è stato effettuato il Walk Test. La risposta della centrale viene inserita nella colonna **RSSI** e indica il valore della portata radio (9 massima):



9.1 MODIFICA DISPOSITIVI

Per accedere alle impostazioni di un dispositivo, cliccate sull'icona  in fondo alla riga del dispositivo. Verranno visualizzati la tipologia del dispositivo, il numero univoco con cui è riconosciuto all'interno del sistema, il nome che gli è stato attribuito e la scelta di *Esclusione*.



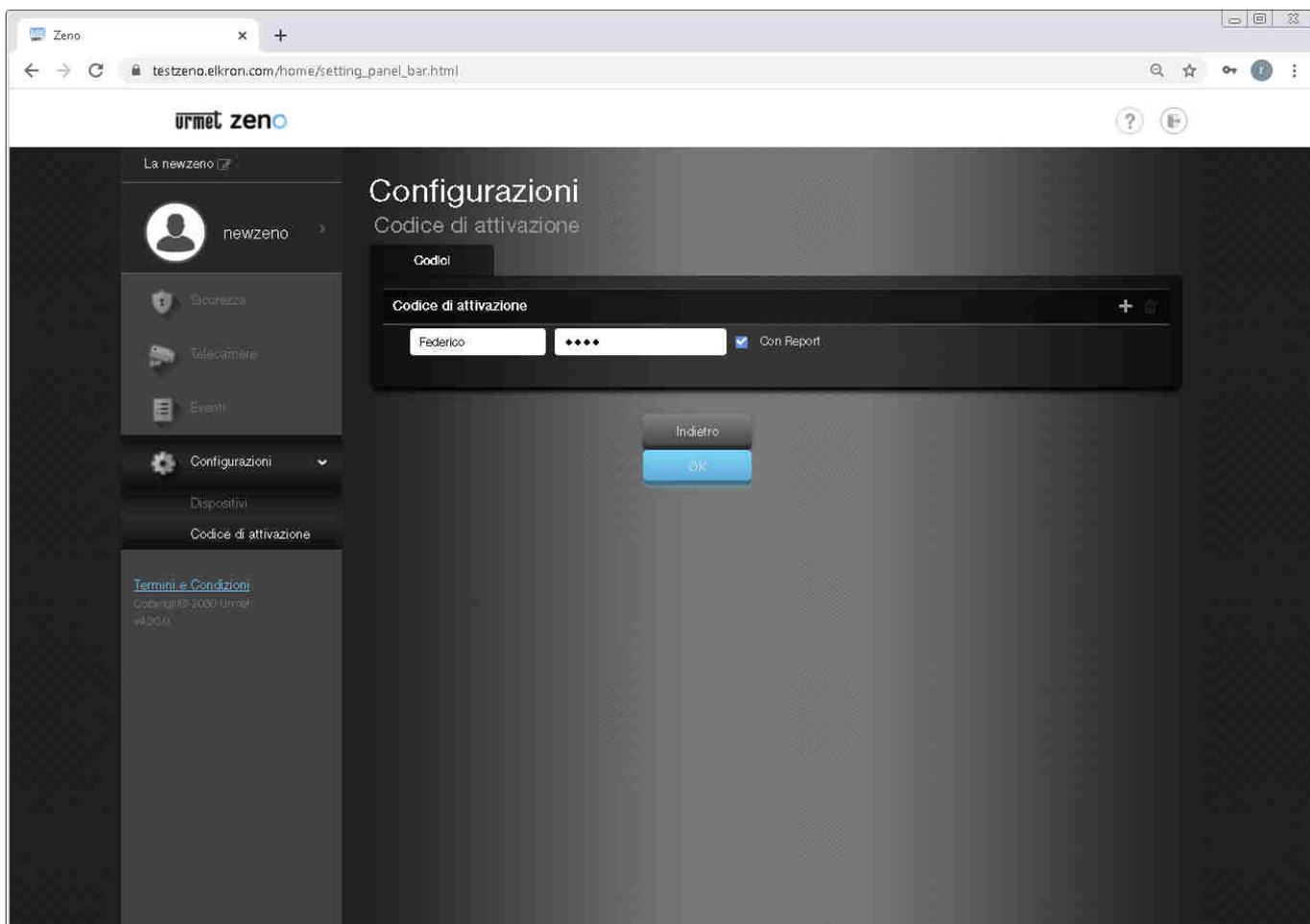
L'esclusione disabilita in modo permanente un dispositivo. Dopo aver selezionato l'esclusione e aggiornato la centrale con il tasto **INVIA**, tutti gli allarmi di intrusione verranno ignorati. Le eventuali situazioni di batteria scarica e manomissione vengono invece sempre segnalate dal dispositivo escluso.

ATTENZIONE! La funzione di Esclusione, riferita a un dispositivo "Sirena", non la disattiva completamente ma blocca l'invio dei report delle sue anomalie.

Per confermare la programmazione effettuata e aggiornare i dati nella centrale, premere il tasto OK, altrimenti premere **INDIETRO** per tornare alla tabella **Dispositivi**.

9.2 AGGIUNTA E MODIFICA CODICI

All'interno di questo sottomenu della sezione **Configurazioni**, accessibile cliccando su **Codice di attivazione**, è possibile gestire fino a sei utenti che possono accedere al sistema con i relativi codici. L'utente master, che compare nella prima riga, non può essere cancellato, ma può eliminare quelli secondari da lui creati. La spunta sul campo "Con Report" indica che gli accessi al sistema vengono registrati nella lista degli Eventi. Se, per questioni di privacy, non si volessero registrare questi eventi, occorre eliminare il segno di spunta.

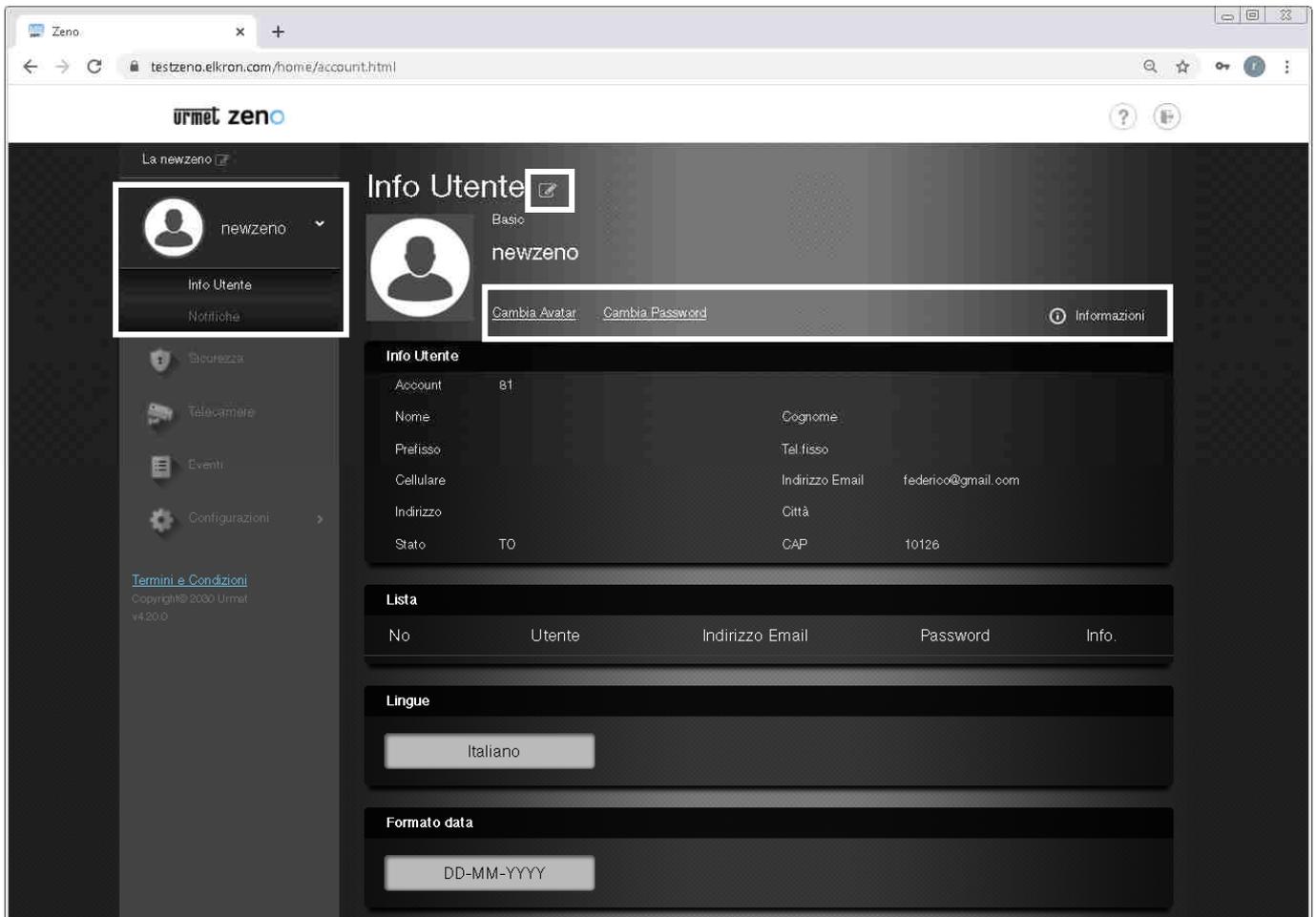


Per aggiornare la centrale con le modifiche apportate cliccate sul tasto **OK**.

NOTA BENE: non è consentito l'utilizzo del valore 1111 per il codice utente.

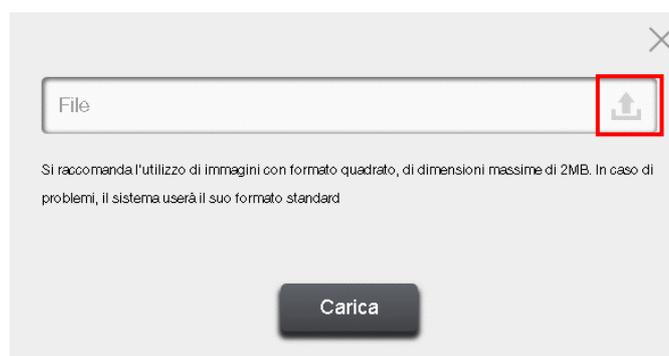
10 IMPOSTAZIONI DI ACCESSO DEGLI UTENTI

Cliccando sul nome della centrale in alto a sinistra si accede alla videata sottostante che corrisponde all'area *info Utente*. Da qui è possibile accedere anche all'area *Notifiche*.

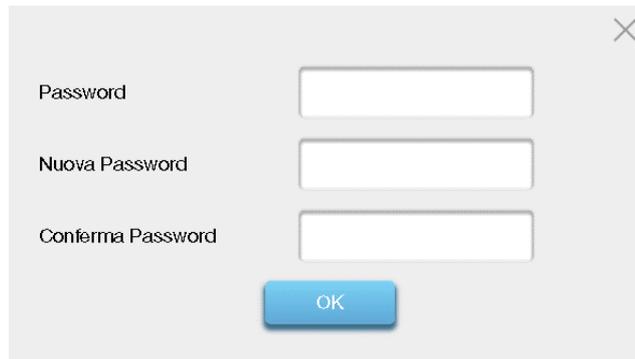


In questa videata è possibile personalizzare i seguenti campi:

- **Cambio avatar**, che permette di personalizzare il proprio account con un'immagine. Scegliere un file cliccando nel punto indicato dal riquadro e confermare premendo il tasto Carica.



- **Cambio password:** per variare la password di accesso al portale. Digitarla negli appositi campi e premere OK.



Dialog box for password change with the following fields and button:

- Password
- Nuova Password
- Conferma Password
- OK

- **Informazioni:** in questo pop up viene visualizzato il MAC address e i parametri con cui la centrale viene identificata sul database del server. Il tasto permette di reinviare alla centrale i dati di configurazione di rete memorizzati sul server:



Dialog box titled 'Informazioni' with the following data:

MAC	00:1d:94:08:8b:7d
Numero Accesso	127037639549

Reinvia Configurazione

Infine, scorrendo la videata in basso, è possibile gestire la lingua d'uso disponibile per il Portale e impostare il formato della data. In Italia scegliere DD-MM-YYYY.

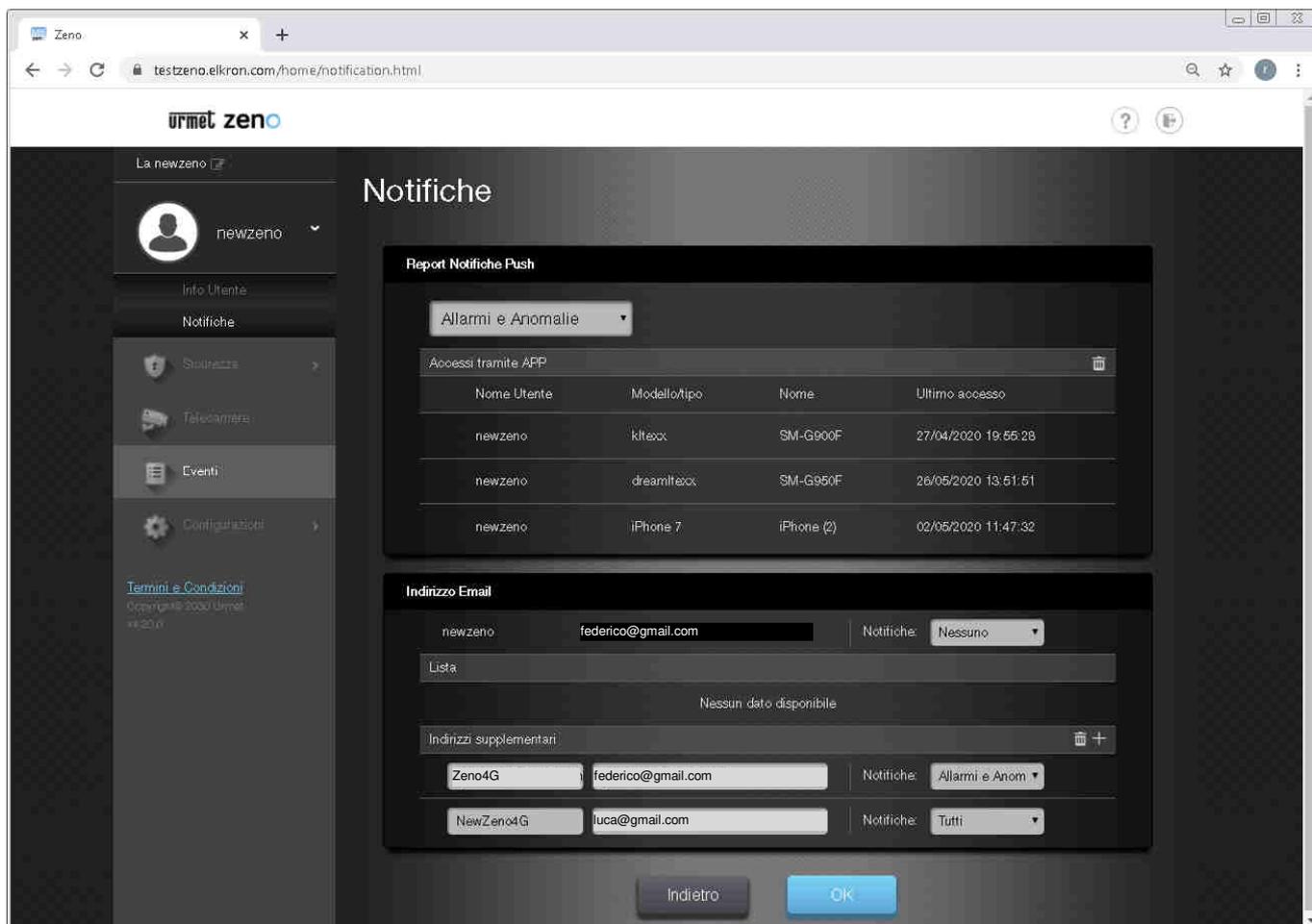
Per modificare i dati dell'utente visualizzati nel menu **Info Utente**, cliccare sull'icona .

Nella parte centrale della videata, l'utente master ha a disposizione un'area in cui inserire **Altri Utenti**, autorizzati a interagire con il sistema **Zeno**. I nuovi Utenti potranno accedere al sistema ma non alle funzioni di configurazione dei dispositivi.

Per inserire un nuovo utente, cliccare su **+**, per cancellare . Per modificare i dati del singolo utente premere sull'icona  accanto al nome.

10.1 NOTIFICHE

La pagina delle **Notifiche** consente di selezionare le *notifiche push* legate alla APP installata sul proprio smartphone.



La scelta effettuata nei menu a tendina per le notifiche e per le email si estende a tutti gli utenti che abbiano installato la App e che si siano connessi almeno una volta con l'account del portale. Le opzioni sono le seguenti:

- ☞ **Tutti**, tutte le notifiche di eventi
- ☞ **Allarmi e Anomalie**, sia le notifiche di allarme che di anomalie
- ☞ **Allarmi**, solo le notifiche di allarme
- ☞ **Nessuno**, per non ricevere alcuna Notifica Push.

10.2 USCITA DAL PORTALE

Cliccare sull'icona  per uscire dal portale.

11 UTILIZZO DELLA APP PER SMARTPHONE

Cercate l'applicazione **MyZeno** all'interno dello store utilizzato dal vostro smartphone (Play Store o App Store).

Procedete con l'installazione, accettando le richieste di accesso alle sezioni del vostro smartphone, indispensabili per gestire tramite la APP il vostro sistema Zeno.

Aprire l'applicazione per completare l'installazione sul vostro smartphone.

Cliccate sull'icona appena creata  per visualizzare la pagina di Accesso dove inserire la password registrata precedentemente sul portale:

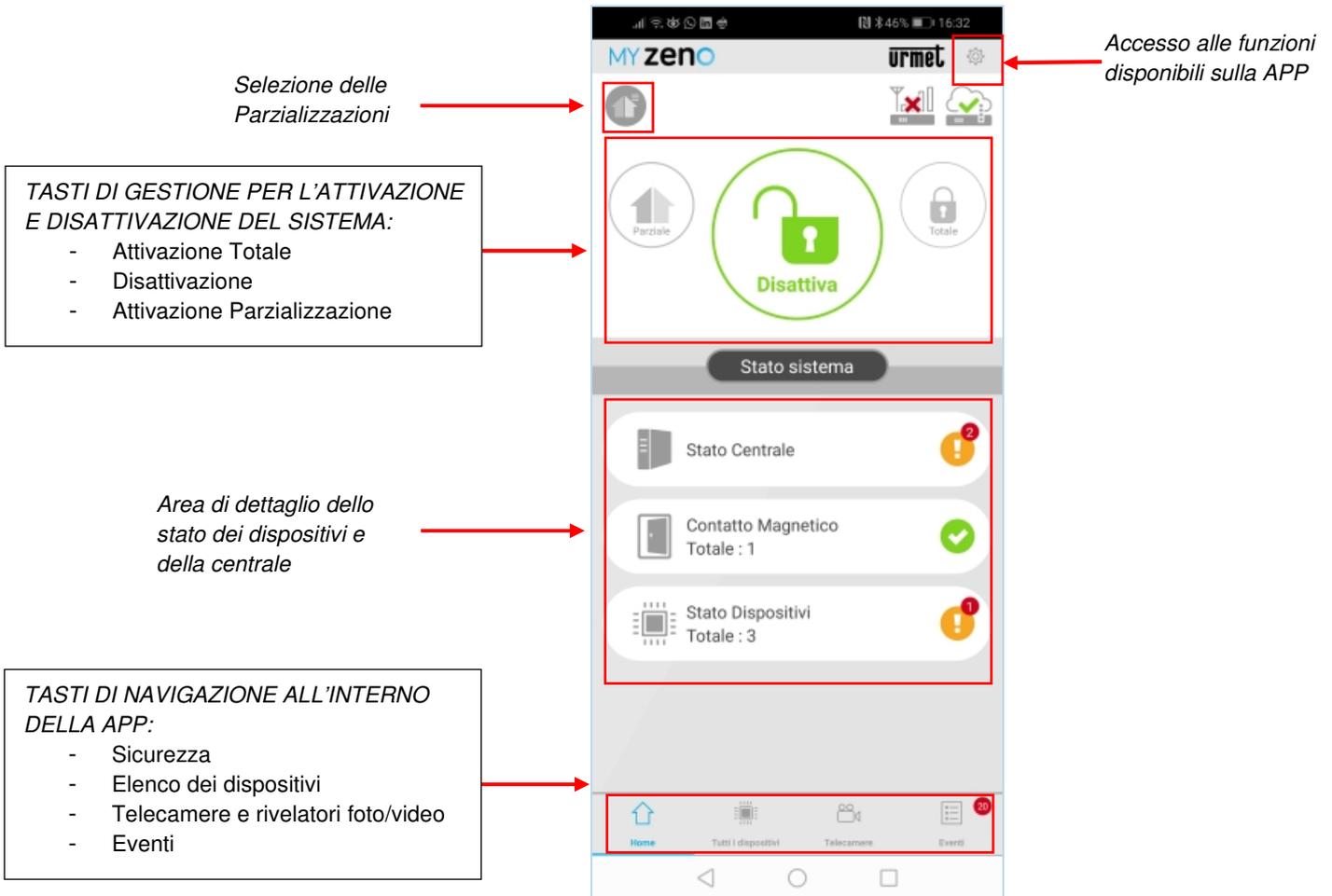


Attivando la funzione **Ricordami** non sarà più necessario digitare le credenziali di accesso ogni volta che si vorrà utilizzare l'App.

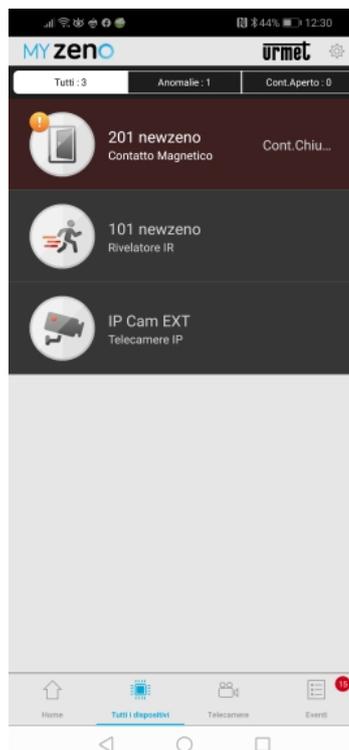
In questa pagina è possibile effettuare la prima registrazione. La procedura è del tutto simile a quella descritta per il portale al capitolo 4 del presente manuale.

VIDEATA PRINCIPALE

Dopo aver inserito le credenziali registrate, cliccando sul tasto **ACCESSO** si apre la videata principale, di default **Sicurezza**, così composta:

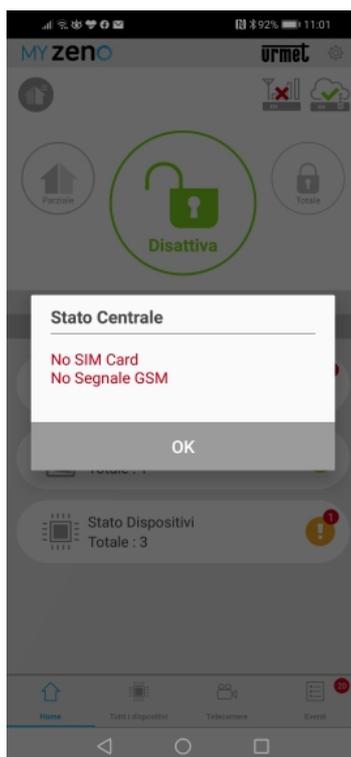


Cliccando sull'**elenco dei dispositivi**, viene visualizzata la lista dei dispositivi presenti nel vostro sistema:



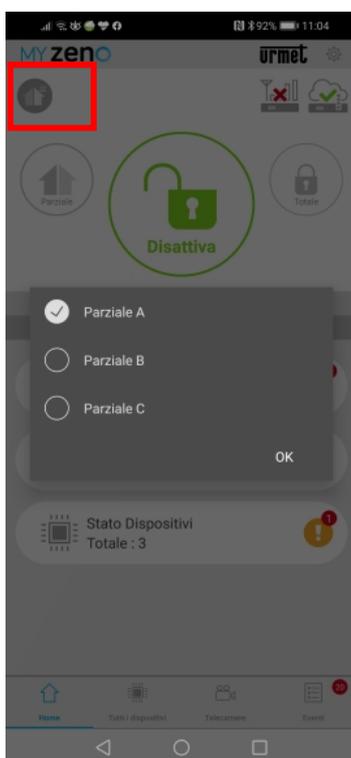
Se presenti rivelatori con fotocamera o videocamera, in questa lista dei dispositivi è possibile richiedere un'immagine o un video. Premendo il corrispondente tasto a lato, la richiesta viene registrata nella lista degli Eventi. Trascorso il tempo necessario di upload/download dal server, sarà possibile visualizzare il media richiesto.

La presenza di anomalie viene visualizzata nella schermata **Sicurezza** in corrispondenza dell'**area di dettaglio dello stato della centrale e dei dispositivi**, dandone evidenza con un punto esclamativo e un numero. Cliccandoci sopra viene fornita una descrizione sintetica delle problematiche rilevate:



SELEZIONE DELLE PARZIALIZZAZIONI

Cliccando sul tasto evidenziato in alto a sinistra vengono visualizzate le 3 parzializzazioni disponibili nel sistema **ZENO**. Se ne può scegliere più di una e cliccando sul tasto **OK**, la scelta viene registrata nella centrale. Premendo successivamente il tasto di **Attivazione Parzializzazione** verranno attivati soltanto il settore o i settori selezionati in quest'area.



ACCESSO ALLE FUNZIONI DISPONIBILI

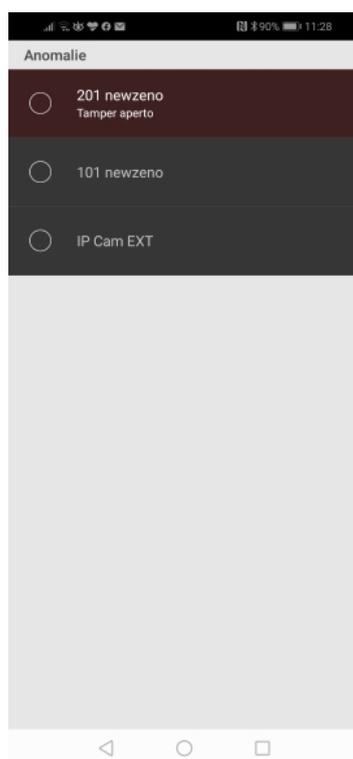
Cliccando sull'icona in alto a destra di ogni videata si passa alla pagina di gestione delle funzioni disponibili:



*** Non è consentito l'utilizzo dei valori 1111 e 7982 per il codice utente, in quanto già utilizzati dal sistema.**

SEZIONE ESCLUSIONI

Nell'area delle funzioni disponibili, selezionare la voce **Dispositivi esclusi**. L'esclusione disabilita in modo permanente un dispositivo di sicurezza. Dopo aver selezionato il dispositivo da escludere, esso viene immediatamente ignorato dal sistema. Le eventuali situazioni di batteria scarica e manomissione continuano a essere segnalate dal dispositivo escluso.



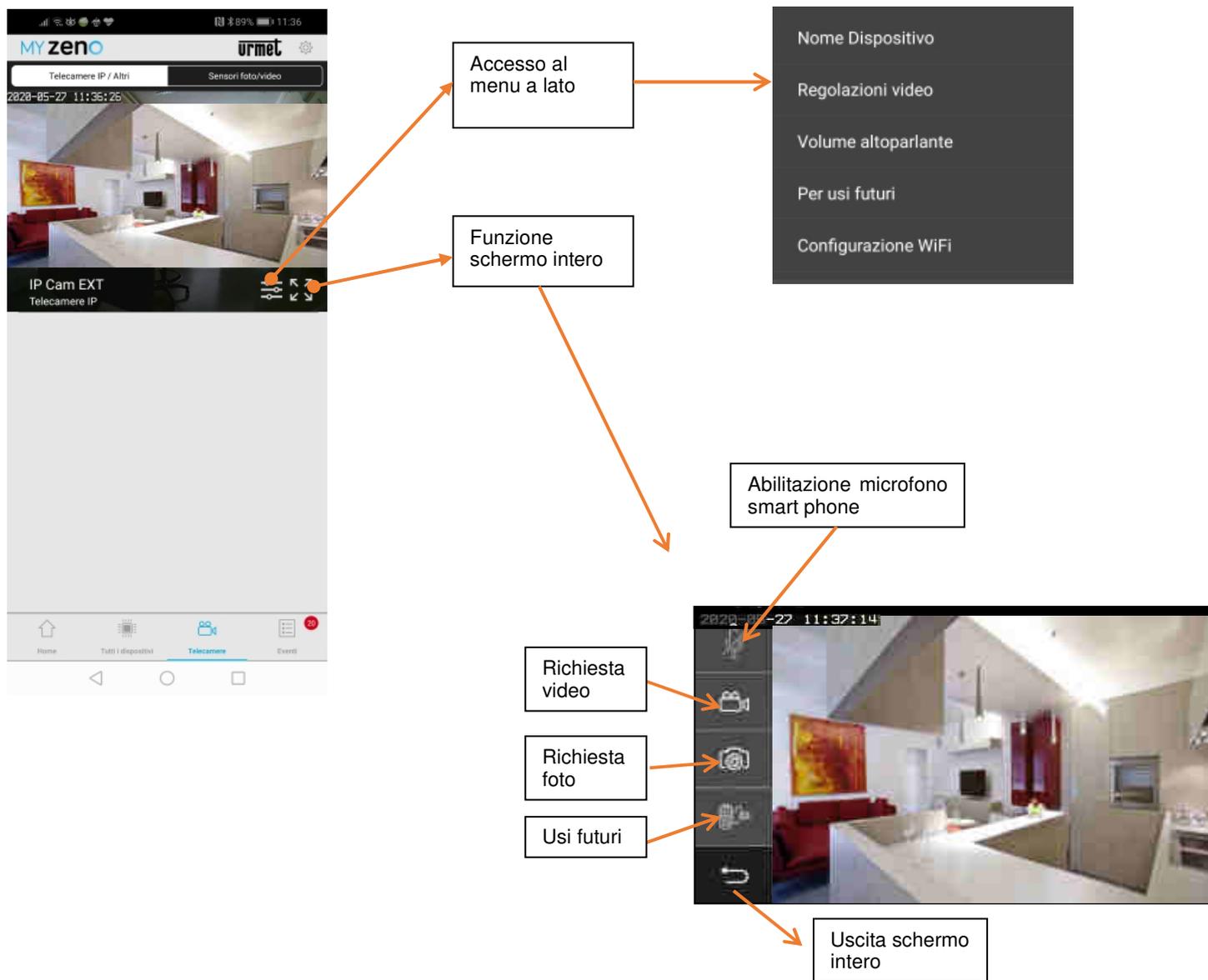
ATTENZIONE! La funzione di Esclusione, riferita a un dispositivo "Sirena", non la disattiva completamente ma blocca l'invio dei report delle sue anomalie.

<NOTA>

Per includere nuovamente un dispositivo nel sistema, occorre eliminare il flag di **Esclusione** dal dispositivo. Si consiglia di uscire dalla APP e accedervi nuovamente per avere le corrette informazioni sul dispositivo riabilitato.

MENU TELECAMERE

Questo menu è stato introdotto dalla versione **1.8.50 della APP di Android** e dalla versione **1.45 della APP di iOS**. In questa sezione vengono visualizzate le immagini di tutte le telecamere e i sensori con foto o video associati alla centrale. Sotto, in dettaglio, uso dei tasti di comando nella configurazione multischermo e a schermo intero.



11.1 TASTI DI SPOSTAMENTO ALL'INTERNO DELLA APP

Per spostarsi tra le varie sezioni all'interno della APP sono disponibili tasti e icone dedicati. Per tornare alla pagina precedente usare il tasto INDIETRO del proprio smartphone.

<NOTA>

☞ Sul sistema Android, usare il tasto funzione INDIETRO per nascondere la tastiera virtuale.

12 AVVERTENZE GENERALI PER L'USO DI PORTALE E APP

12.1 ATTIVAZIONE CON ANOMALIE

Nel caso il sistema presenti delle anomalie al momento dell'**attivazione totale o parziale**, dopo aver digitato il codice di attivazione, sullo schermo comparirà il seguente messaggio:



Premendo il tasto OK per proseguire nell'attivazione, verrà visualizzato l'elenco delle anomalie presenti nel sistema. Per poter completare l'attivazione sarà necessario spuntarle tutte. Solo in questo caso il tasto OK diventerà disponibile e sarà possibile cliccarci sopra.

Le anomalie possono essere:

- Lo **stato di contatto aperto**, ad esempio per una finestra rimasta socchiusa. Queste informazioni sono evidenziate in rosso nella lista dei dispositivi del portale e della APP e nella sezione **Sicurezza** del portale e della APP.
- Lo **stato dei dispositivi del sistema che risultano manomessi** (allarmi Tamper), con **batteria quasi scarica**, fuori servizio, ecc. Anche queste informazioni sono evidenziate in rosso.
- Lo stato di anomalia della centrale come la sua manomissione (allarme tamper), l'assenza di rete elettrica e l'assenza di connessione dati (Internet o 4G), sono informazioni che non appartengono ai dispositivi ma sono presenti nella sezione **Sicurezza**.

<NOTA>

È possibile configurare la centrale in modo che ignori le anomalie durante le attivazioni. Ciò si può fare in due modi: 1) prevedendo una attivazione diretta (vedere "Parametri del sistema - Attivare con anomalie" nel manuale di installazione della centrale); 2) escludendo il controllo di ciascuna anomalia (vedere "Info - Anomalie sistema" nel manuale di installazione della centrale).

12.2 CONNESSIONI LENTE O CRITICHE ALLA RETE INTERNET

Nel caso di connessioni lente alla rete Internet (per esempio quando la connessione disponibile sia solo in 3G o GPRS), una volta entrati nel portale o nella APP, è consigliabile attendere qualche secondo prima di agire sul sistema, per permettere alla connessione di stabilizzarsi.

Lo stato di connessione può essere verificato tramite l'icona , descritta nel paragrafo 6.3 del presente manuale.

12.3 USO DI CODICI ERRATI

Dopo aver digitato per 5 volte consecutive un *codice utente errato* sul portale o sulla APP, il sistema andrà in blocco e si manterrà nello stato in corso per circa 9 minuti. Durante questo tempo, non sarà possibile sbloccare il sistema neanche introducendo il codice corretto e la tastiera risulterà inutilizzabile. Il sistema potrà cambiare stato ed essere ripristinato soltanto tramite il telecomando, o trascorso il tempo di blocco.

Nell'ipotesi che la reiterazione di un codice errato sia un atto fraudolento, per motivi di sicurezza sia sulla APP che sul portale viene mostrato il messaggio CODICE ERRATO e ogni successivo inserimento andrà a sommare ulteriori 9 minuti al tempo di blocco del sistema. Sul pannello di controllo locale, nello "Storico", verrà registrato "Codice Bloccato".