

DS80WL60-001A

CENTRALE ANTIFURTO

CR600WF
Centrale Wireless
IP/4G/WiFi

Manuale d'installazione e programmazione



INDICE

1. INTRODUZIONE	4
2. DESCRIZIONE DELLA CENTRALE	4
2.1 IDENTIFICAZIONE DELLE PARTI	4
2.2 INSERIMENTO DELLA SIM GSM (OPZIONALE)	5
2.3 INSTALLAZIONE DEL DONGLE ZIGBEE USB/ZIGBEE (OPZIONALE)	5
2.4 ALIMENTAZIONE	5
2.5 REGISTRAZIONE DEI MESSAGGI VOCALI	7
3. INSTALLAZIONE	8
3.1. REQUISITI DI BASE	8
3.2. FASI DI MONTAGGIO DELLA CENTRALE	8
3.3. PROGRAMMAZIONE DELLA CENTRALE CR600WF	10
3.4. INSTALLAZIONE DEL SOFTWARE FINDER	12
4. ACCESSO AL PANNELLO DI CONTROLLO DELLA CENTRALE	14
5. GESTIONE DEI DISPOSITIVI	16
5.1. APPRENDIMENTO	16
5.2. WALK TEST	17
5.3. MODIFICA DEI DISPOSITIVI	18
5.3.1 Rivelatori	18
5.3.2 Telecomandi RC600 e Tastiere KP600	21
5.3.3 Dispositivi foto/video	23
5.3.4 Sirene	25
6. IMPOSTAZIONI DEL SISTEMA	26
6.1. ACCESSO – INFORMAZIONI GENERALI	26
6.2. HOME PAGE	26
6.3. STORICO EVENTI	28
6.4. REPORT EVENTI	29
6.5. IMPOSTAZIONI CENTRALE	29
6.6. DATI UTENTI	32
6.7. CATTURA EVENTI	33
6.8. TRASMISSIONE EVENTI (MENU PER UTENTI SPECIALIZZATI)	34
6.9. STORICO DISPOSITIVI HA	34
7. GESTIONE RETE	35
7.1. GSM	35
7.2. LAN	36
7.3. WiFi	37
8. GESTIONE SISTEMA	38
8.1. CAMBIO PASSWORD	38
8.2. HOME AUTOMATION	38
8.3. SCENARI	38
8.4. REPORT	38
8.5. REPORT SMS	41

8.6. UPLOAD VIDEO	41
8.7. XMPP	42
8.8. DATA & ORA	42
8.9. FIRMWARE & FIRMWARE RF	43
8.10. RESET DI FABBRICA	43
8.11. BACKUP & RIPRISTINA	44
8.12. LOG SISTEMA	44
9. CARATTERISTICHE TECNICHE DELLA CENTRALE	45
10. STRUMENTI DI GESTIONE REMOTA	46
11. APPENDICI	48
11.1. TIPOLOGIE DI ALLARME ED EVENTI GENERATI NEL SISTEMA	48
11.2. ISTRUZIONI PER SOSTITUZIONE E SMALTIMENTO BATTERIE	49

1. INTRODUZIONE

Il presente manuale è dedicato all'installazione delle centrali CR600WF del sistema antintrusione wireless Egon con video verifica degli allarmi.

2. DESCRIZIONE DELLA CENTRALE

2.1 Identificazione delle parti

1. Led di stato della centrale (di colore verde o rosso)

LED ROSSO ACCESO - Sistema attivato totalmente

LED ROSSO LAMPEGGIANTE - Sistema attivato parzialmente

LED VERDE ACCESO - Sistema disattivato

LED VERDE LAMPEGGIANTE - Sistema in stato di apprendimento dispositivi

LED SPENTO - Sistema in stato di test

2. Led di stato allarmi ed errori (di colore rosso o giallo, con rosso prioritario)

LED ROSSO LAMPEGGIANTE - Sistema in stato di allarme

LED ROSSO ACCESO - Allarme avvenuto

LED GIALLO LAMPEGGIANTE - Assenza alimentazione rete elettrica

LED GIALLO ACCESO - Altra condizione di errore (diversa da assenza alimentazione)

LED SPENTO - Sistema in stato di funzionamento normale

3. Led di stato operativo (giallo/verde)

LED VERDE - Connessione Internet in stato di normale funzionamento

LED GIALLO LAMPEGGIANTE – Tentativo di connessione Internet in corso

LED GIALLO ACCESO - Assenza di connessione Internet

4. Altoparlante

5. Sirena

6. Alloggiamento per scheda SIM

7. Interruttore antimanomissione (tamper)

8. Morsetti di alimentazione per collegamento di rete elettrica

9. Presa jack alimentazione di rete (non disponibile)

10. Interruttore batteria

11. Pulsante Apprendimento locale / Reset

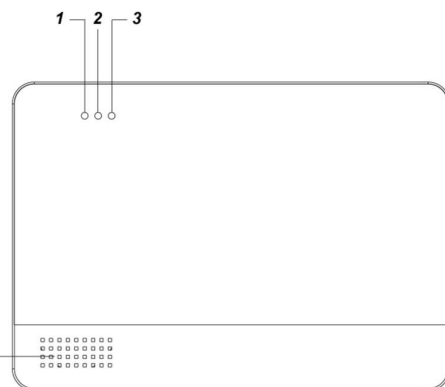
12. Porta interfaccia Ethernet

13. Microfono

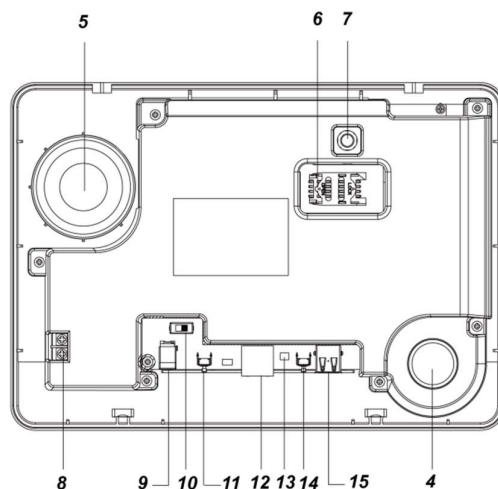
14. Pulsante per gestione registrazioni vocali

15. Porta USB per Dongle Zigbee (USB/Zigbee opzionale)

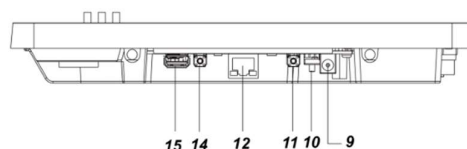
VISIONE FRONTALE



VISIONE POSTERIORE (INTERNA)



CONNESSIONI E COMANDI



2.2 Inserimento della SIM GSM (opzionale)

La centrale CR600WF sfrutta la connettività 4G integrata per monitorare e controllare gli stati del sistema e dei dispositivi. Per sfruttare la funzionalità 4G è necessario inserire una SIM card abilitata all'uso di voce e dati all'interno della centrale.

La scheda SIM GSM va inserita nello scomparto dedicato sul retro della Centrale:



SCOMPARTO SIM

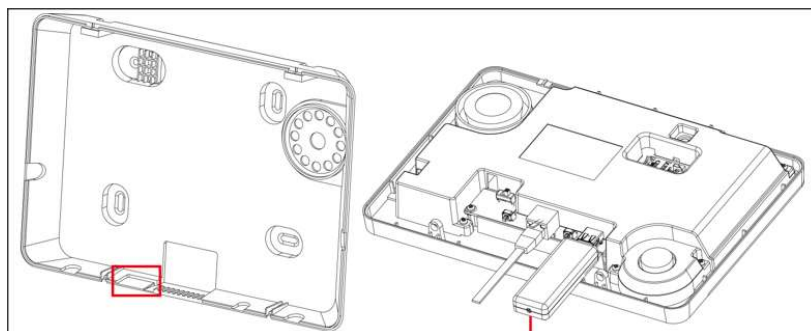
- Sbloccare l'accesso facendo scorrere il porta scheda verso sinistra
- Sollevare il porta scheda e inserire delicatamente la SIM con i contatti rivolti verso il basso.
- Abbassare il porta scheda e bloccare l'accesso facendolo scorrere verso destra

<NOTE>

Disattivare il codice PIN della SIM card prima di inserirla nella centrale se non è già stato disattivato (è possibile utilizzare SIM speciali dedicate a questo tipo di applicazioni).

2.3 Installazione del Dongle Zigbee USB/ZIGBEE (opzionale)

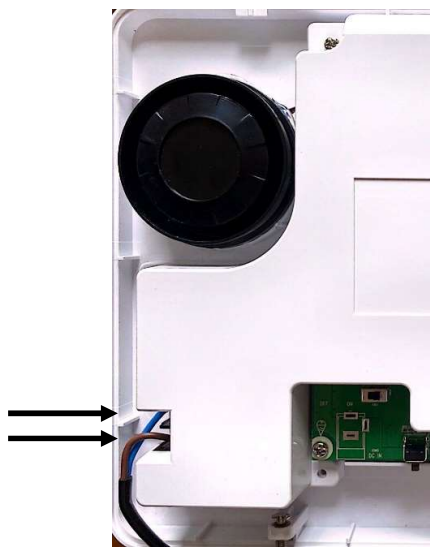
Nel caso sia necessario utilizzare il Dongle Zigbee, è necessario staccare la zona pre-tranciata indicata in figura:



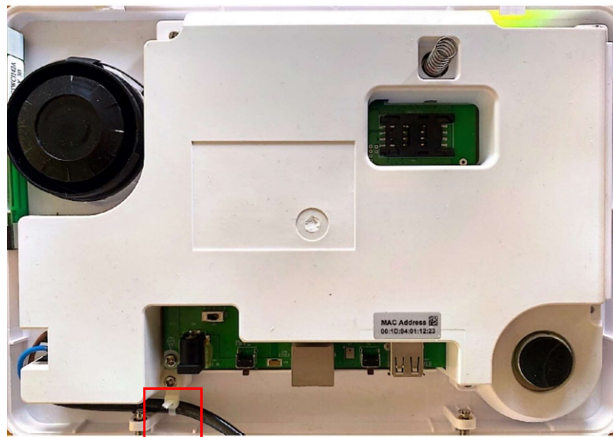
e inserire il dispositivo nel connettore USB.

2.4 Alimentazione

La centrale CR600WF è alimentata tramite la rete elettrica 230Vca. Collegare il cavo fornito a corredo sui due morsetti a lato della centrale, come indicato nelle figure sottostanti.



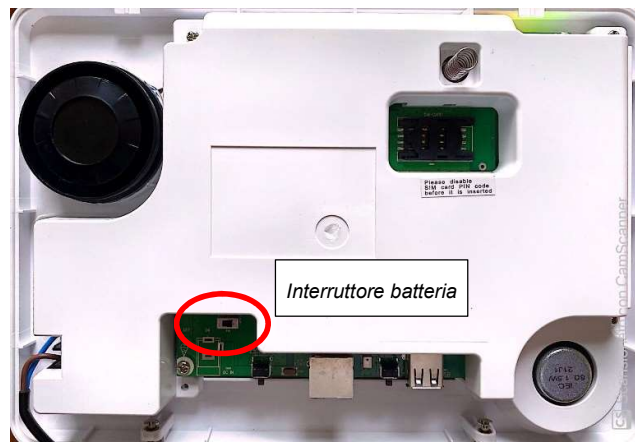
Utilizzare la fascetta con vite a corredo per fissare il cavo nella posizione indicata sotto e far fuoriuscire il cavo attraverso lo spazio dedicato sul fondo.



Infine riposizionare il coperchio posteriore della centrale avvitandolo con le due viti.

NOTA IMPORTANTE: COLLEGARE LA RETE ELETTRICA SOLO AL TERMINE DELLE OPERAZIONI

Batteria ricaricabile



- All'interno della centrale è presente una batteria ricaricabile che serve come batteria tampone in caso di assenza di alimentazione.
- Durante il normale funzionamento, l'alimentazione di rete viene utilizzata per alimentare la centrale e ricaricare contemporaneamente la batteria. Servono circa 72 ore per caricare completamente la batteria.

La posizione di fabbrica dell'interruttore della batteria è **OFF**. In questa condizione la batteria non viene ricaricata quando la centrale è collegata alla rete elettrica e non può essere utilizzata come batteria tampone in caso di assenza di alimentazione. È quindi necessario spostare l'interruttore su **ON** per garantirne il funzionamento.

<NOTA>

- ☞ Se l'alimentazione è assente e la batteria è quasi scarica, viene segnalato lo stato di batteria scarica tramite comunicazioni remote e la sirena interna viene disattivata per risparmiare energia.
- ☞ L'autonomia della centrale alimentata solo a batteria è di circa 15 ore se non è installato il Dongle Zigbee, in funzione del suo comportamento durante l'assenza di rete.
In caso di presenza del Dongle Zigbee, l'autonomia scende fino a 5 ore.
- ☞ Quando la centrale funziona con la sola batteria e non è presente la il Dongle Zigbee, utilizza una modalità di funzionamento a basso consumo in cui disabilita la connessione WiFi e limita le interazioni con le connessioni remote: continuerà ad inviare le segnalazioni degli eventi ma non potrà ricevere dei comandi da remoto in caso di richiesta di connessione remota da APP. Dal momento che anche il router potrebbe essere disalimentato, ovviamente la comunicazione è garantita se la centrale è dotata di una SIM.

2.5 Registrazione dei messaggi vocali

La centrale CR600WF è in grado di registrare un proprio messaggio vocale con l'identificativo dell'abitazione dell'utente; il messaggio sarà inviato dalla centrale e riprodotto insieme alla descrizione dell'evento avvenuto in caso di allarme. La massima durata del messaggio è di 10 secondi.

Per registrare un nuovo messaggio vocale o sostituire quello esistente, alimentare la centrale e premere il pulsante di registrazione (vedere cap. 2. DESCRIZIONE DELLA CENTRALE) per 5 secondi; la centrale emetterà un beep per indicare che l'utente potrà iniziare la registrazione. Una volta completata la registrazione, premere il pulsante di registrazione un'altra volta e verificare che il messaggio sia stato registrato correttamente.

3. INSTALLAZIONE

3.1. Requisiti di base

La centrale è progettata per essere montata a parete. Per una corretta installazione, si consiglia di considerare le seguenti linee guida:

- La centrale necessita di una connessione Ethernet ed è consigliata l'aggiunta di scheda SIM.
- La centrale deve essere installata in una posizione nascosta alla vista dall'esterno.
- Evitare di montare la centrale in prossimità di grandi oggetti metallici che potrebbero influenzare il livello dei segnali radio.
- La centrale deve essere protetta per mezzo di rivelatori in modo che nessun intruso possa arrivare in prossimità di essa senza aver prima generato un allarme.

3.2. Fasi di montaggio della centrale

Fase 1. Allentare le viti in basso sulla centrale (**Figura 1**) e rimuovere il coperchio posteriore della centrale facendolo slittare verso l'alto per evitare di danneggiare gli agganci interni.

Fase 2. Il coperchio posteriore ha 4 zone pre-tranciate in cui praticare i fori per il montaggio a parete (**Figura 2**). Sul bordo del coperchio sono inoltre presenti altre zone pre-tranciate adibite al passaggio cavi.

Figura 1

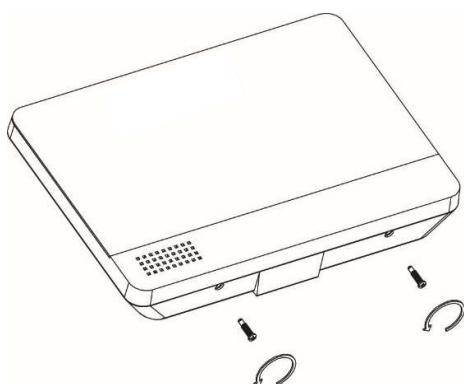
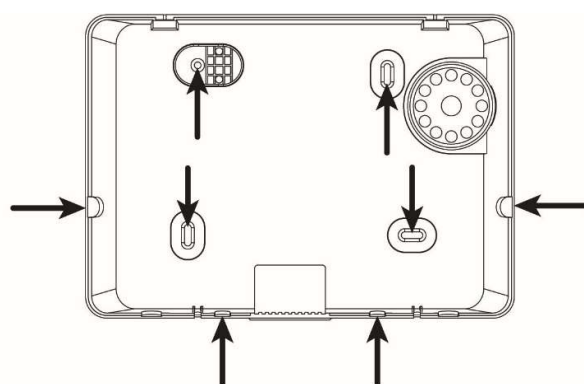


Figura 2



Fase 3. Utilizzare la base come dima per segnare le posizioni dei fori di montaggio sulla parete (**Figura 3**). Utilizzando i tasselli a corredo, fissare la centrale sulla parete (**Figure 4 e 5**)

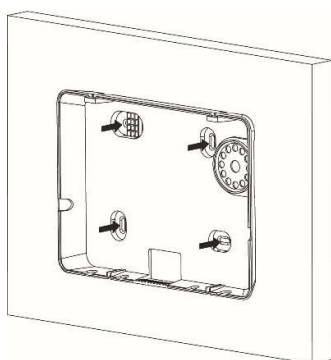


Figura 3

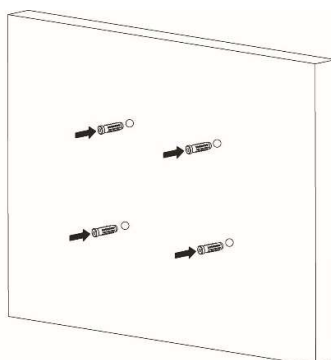


Figura 4

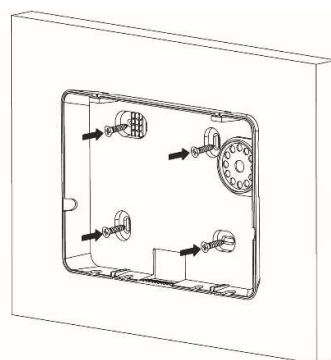


Figura 5

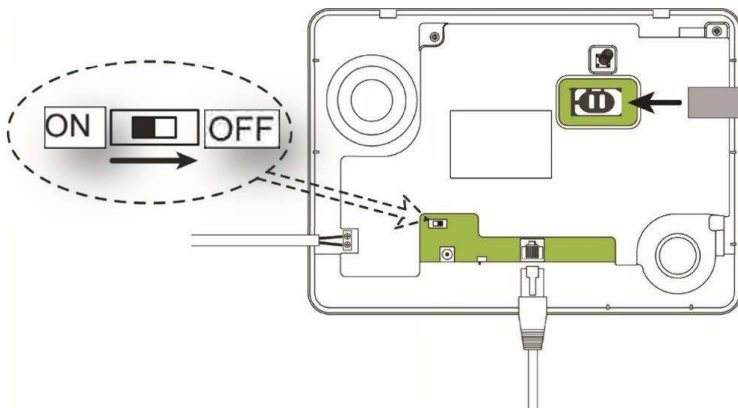
Fase 4. Collegare il cavo Ethernet fornito a corredo alla centrale. (**Figura 6**)

Nel caso si intenda utilizzare la connessione 4G, inserire una scheda SIM nella relativa sede. Prima di inserire la scheda SIM, accertarsi che il codice PIN della scheda sia disabilitato.

NOTA BENE: la SIM può impiegare un certo tempo a registrarsi sulla rete cellulare: dopo l'accensione della centrale occorre aspettare quindi alcuni minuti prima di utilizzarla.

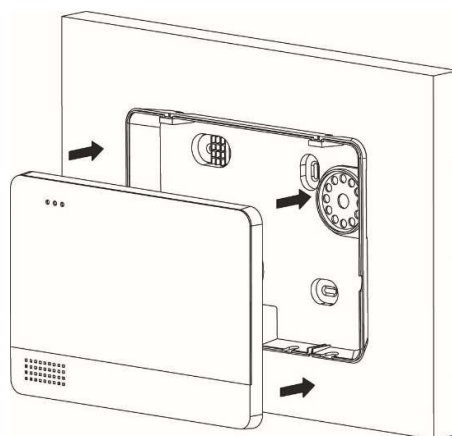
Fase 5. Alimentare la centrale e far scorrere l'interruttore della batteria in posizione ON.

Figura 6



Fase 7. Agganciare la centrale alla base e fissarla con le apposite viti (**Figura 7**).

Figura 7



3.3. Programmazione della Centrale CR600WF

La Centrale deve essere programmata per il suo uso tramite un PC.

Requisiti del PC

Per installare il sistema, il computer con il quale dovrà essere effettuata la programmazione deve avere i seguenti requisiti:

- sistema operativo Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista, 7, 8, 10 o 11
- Google Chrome (consigliato) o Firefox. Si sconsiglia l'uso di Internet Explorer
- CPU: Intel Pentium II 266 MHz o superiore
- Memoria: 64 MB o più
- Risoluzione VGA: 800x600 o superiore

PREDISPOSIZIONE DELLA RETE LOCALE (LAN) E INTERNET (WAN)

Requisiti per il collegamento su Internet

Per garantire il completo funzionamento del sistema Egon, la centrale deve essere collegata:

1. ad un Router ADSL tramite cavo Ethernet o connessione WiFi

e/o:

2. alla rete dati cellulare 4G tramite utilizzo di una SIM abilitata al traffico dati da inserire all'interno della centrale.

Per garantire la massima sicurezza e le massime prestazioni, è consigliabile prevedere entrambe le connessioni:

- ☞ 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

Per il corretto funzionamento non sono richieste sul Router né la funzione di Port Forwarding né il servizio di DDNS (Dynamic Domain Name System). È invece consigliabile l'abilitazione del Server DHCP sul Router stesso.

Connessione della Centrale ad un PC per la messa in servizio

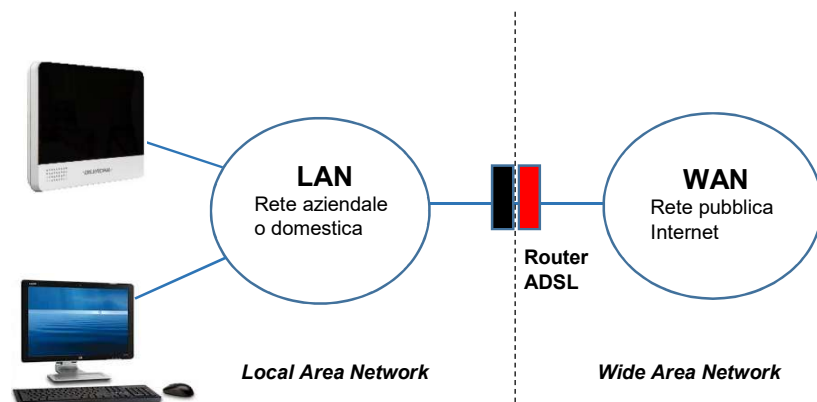
La messa in servizio della centrale deve essere realizzata tramite l'uso di un PC.

La connessione può essere realizzata tramite due tipi di collegamento tramite cavo:

- ☞ attraverso il router ADSL utilizzato per connessione della centrale alla rete Internet, tramite un collegamento via cavo Ethernet fornito in dotazione (metodo consigliato)
- ☞ attraverso la connessione diretta al PC, utilizzando il cavo Ethernet fornito in dotazione

NOTA BENE: la programmazione non può essere realizzata tramite una connessione WiFi, è necessaria la connessione via cavo. La connessione WiFi potrà invece essere utilizzata nel normale uso a regime.

Connessione con Router



Per connettersi alla propria centrale, utilizzare un PC collegato al router.

La centrale è già configurata per funzionare con la maggior parte delle possibili configurazioni di rete. I suoi parametri di fabbrica sono:

- IP = **192.168.1.xxx (DHCP)**
- DNS = 8.8.8.8; DNS2 = 8.8.4.4
- Gateway = 192.168.1.1
- NetMask = 255.255.255.0
- DHCP = ON

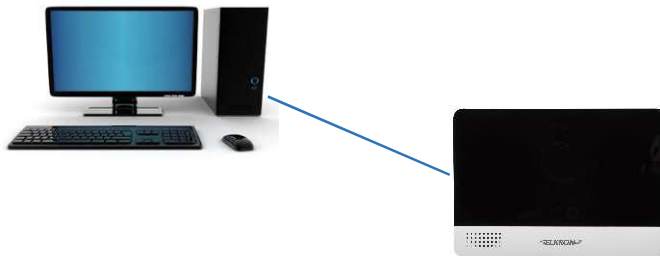
Se il router utilizzato è dotato di Server DHCP, è consigliabile lasciare l'indirizzamento DHCP anche sulla centrale, tramite il programma Finder, come indicato nel paragrafo successivo.

Se il router non è dotato di Server DHCP, sarà necessario configurare sulla centrale un indirizzo statico della stessa famiglia della rete LAN utilizzata.

ATTENZIONE! Se il router non è dotato di Server DHCP e sulla centrale viene abilitato l'indirizzamento DHCP, questa diventerà irraggiungibile !!

<NOTA>

Connessione con collegamento diretto:



Per poter configurare la centrale tramite la connessione diretta a un PC, occorre agire in uno dei seguenti modi:

1. Configurare il PC con un indirizzamento IP della stessa famiglia della centrale, quindi utilizzare un indirizzo 192.168.1.xxx (con xxx diverso da 130) e una NET MASK 255.255.255.0
2. Oppure tramite il programma Finder (si veda oltre), configurare la centrale con un indirizzamento IP della stessa famiglia del PC. Se per esempio il PC ha un indirizzo appartenente alla famiglia 192.168.0.xxx, configurare la centrale con un indirizzo appartenente alla stessa famiglia, ma diverso da quello del PC, e una NET MASK 255.255.255.0

3.4. Installazione del software Finder

QUESTA INSTALLAZIONE È NECESSARIA SOLO AL PRIMO UTILIZZO

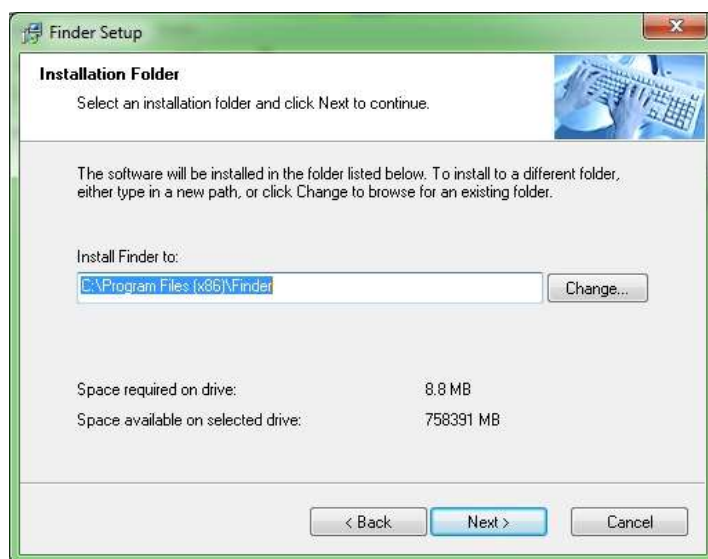
Allo scopo di programmare e controllare la centrale, viene fornito lo speciale software “**Finder**” (funzionante con sistema operativo Microsoft Windows 7 o superiore) che permette di identificare e localizzare la centrale nella rete locale (LAN). Per installare il software “**Finder**”:

Fase 1. Collegarsi al sito internet www.elkron.it: il software è disponibile sul sito web <https://www.elkron.it>, nella sezione **Download → Software**

ATTENZIONE! Per accedere a quest'area del sito è necessario essere registrati come installatori.


Fase 2. Scaricare il software **Finder**.

Fase 3. Cliccare due volte su **Finder** per avviare l'installazione dell'applicativo. In caso di blocco da parte del vostro pc dovuto alla presenza di protezioni o firewall, acconsentire all'installazione dell'applicativo secondo le modalità previste dal sistema operativo in uso.

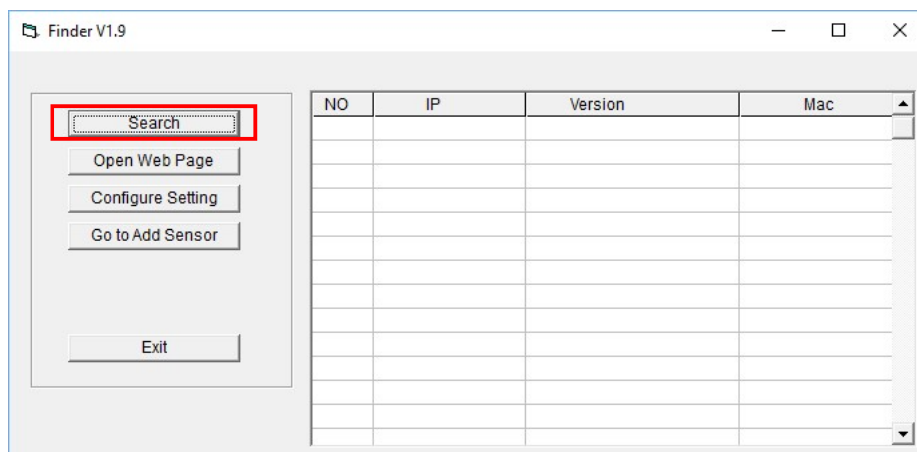


Fase 5. Cliccare su “**Change**” per selezionare la cartella del file; se non è necessario cambiare il percorso, cliccare su “**Next**” per proseguire.

Fase 6. Cliccare su “**Next**” per avviare l'installazione. Al termine dell'installazione, cliccare su “**Finish**”.

Fase 7. Sul desktop viene visualizzata una nuova icona:  **Finder.exe**

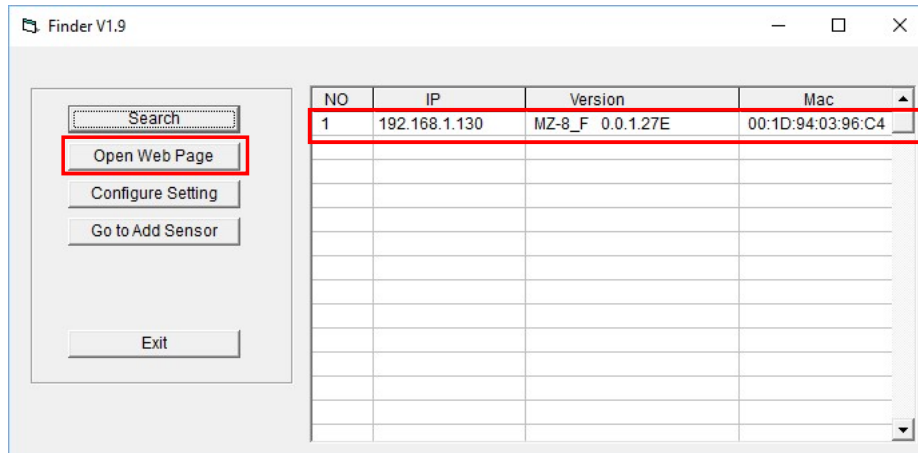
Fase 8. Cliccare due volte su “**Finder.exe**” per avviare l'installazione. Viene visualizzata la seguente finestra:



Fase 9. Cliccare su “**Search**”: il programma avvia la ricerca degli indirizzi IP noti nella rete locale.

Fase 10. Individuare l'indirizzo IP della centrale dall'elenco. Vengono visualizzati anche l'indirizzo MAC e la versione

firmware del prodotto.

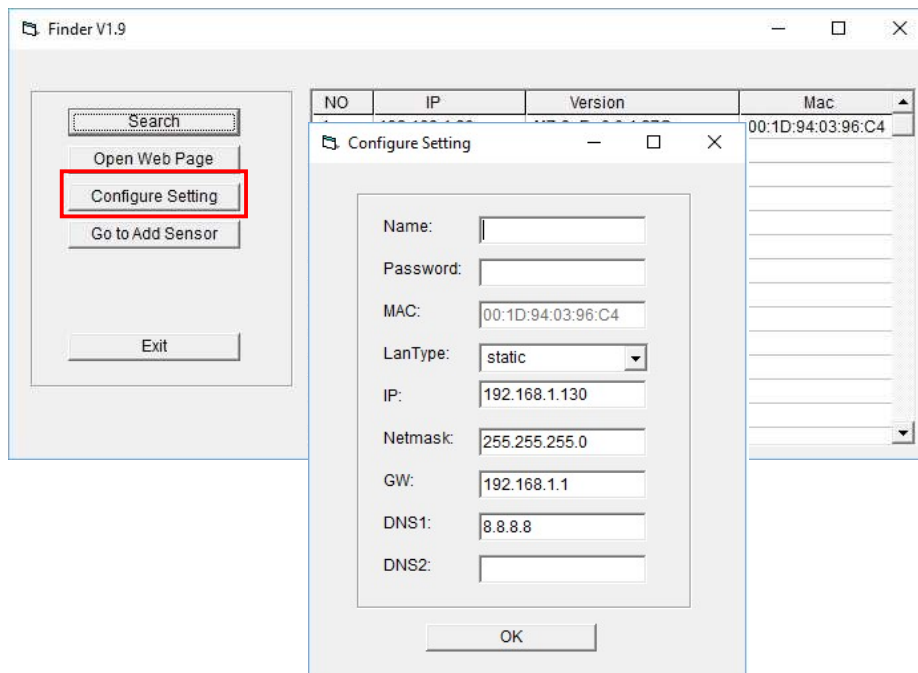


Fase 11. Una volta identificata la centrale, selezionarla e cliccare su “**Open Web Page**” per collegarsi al Pannello di controllo locale della centrale CR600WF. Verrà richiesto l’inserimento delle credenziali di accesso, descritto nel capitolo 4.

CONFIGURARE LE IMPOSTAZIONI DI RETE DELLA CENTRALE

Questa funzione serve solo se si desidera configurare manualmente le impostazioni di rete.

Fase 1. Selezionare la centrale e poi cliccare su **Configure Setting**: viene visualizzata la seguente finestra:



Fase 2. Digitare il nome utente e una password per la configurazione delle impostazioni.

Nome Utente (predefinita): **admin**

Password (predefinita): **cX+HsA*7F1**

ATTENZIONE! per ottemperare a recenti disposizioni anti-hackeraggio, la Centrale Egon adotta il seguente meccanismo per la generazione della password. Dopo il primo inserimento della password predefinita **cX+HsA*7F1** il sistema richiede, al primo accesso di modificarla inserendo la propria. Se questo non avviene entro un’ora, il sistema impedisce l’accesso e sarà necessario disalimentare completamente e rialimentare la centrale per eseguire l’operazione completa.

NOTA BENE: in seguito a Reset di Fabbrica, la centrale riadotta la password predefinita.

Fase 3. Selezione **DHCP** o **Static** per LAN Type. Se si seleziona **Static**, si può proseguire con l'inserimento manuale delle restanti informazioni di rete. Se si seleziona "**DHCP**", non sarà possibile modificare le altre informazioni di rete.

Fase 4. Dopo aver inserito una nuova impostazione, cliccare su **OK** per confermare. Se nome utente e password sono corretti, una finestra visualizza il messaggio seguente: **Status: Configure success!!** (Stato: Configurazione riuscita!)

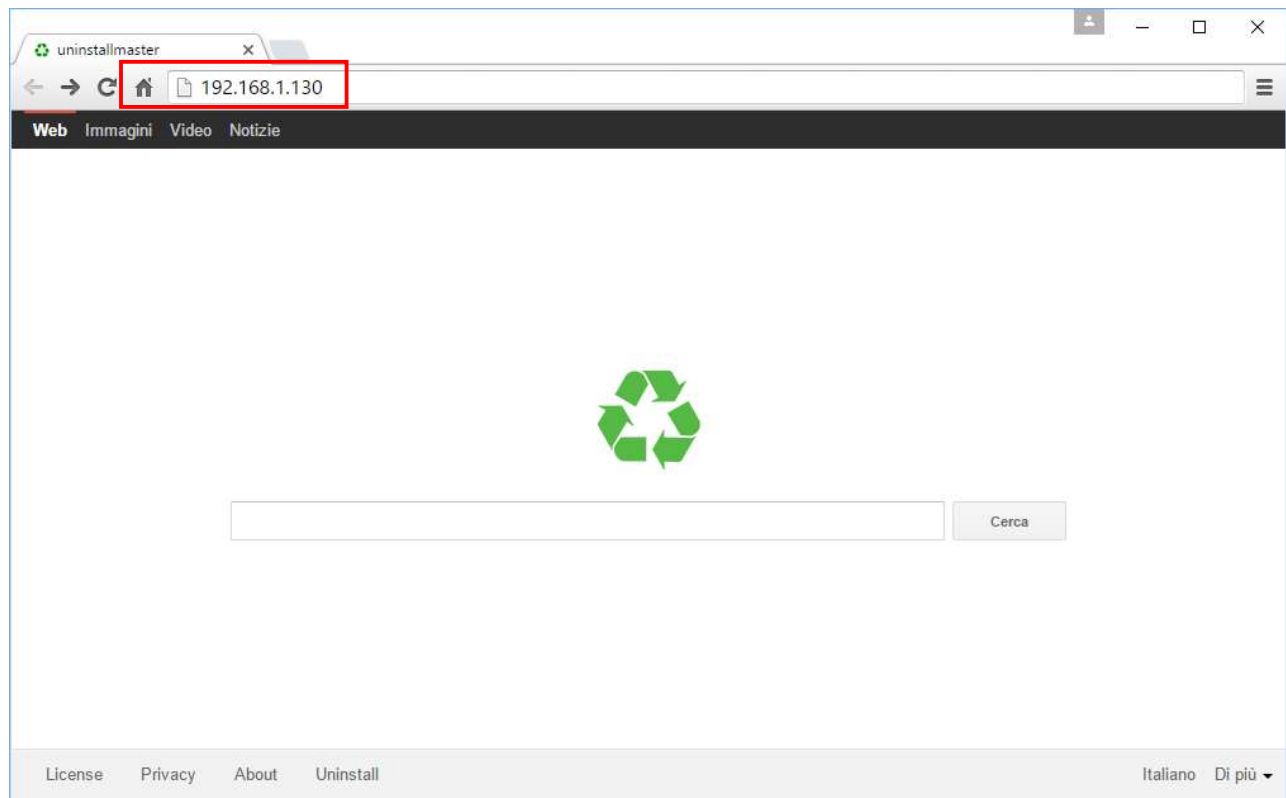
<NOTA>

L'opzione "Go to add sensor" non è disponibile nella presente versione.

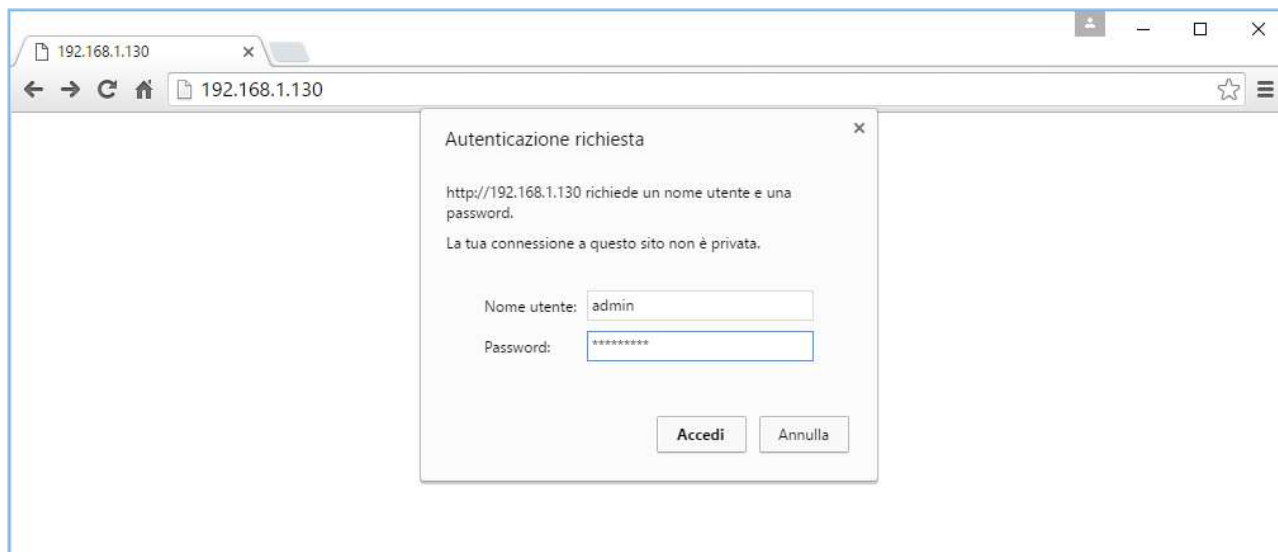
4. ACCESSO AL PANNELLO DI CONTROLLO DELLA CENTRALE

Fase 1. Selezionare la centrale nel software Finder e cliccare su "Open Webpage" per collegarsi al Pannello di controllo.

In alternativa, utilizzare un browser digitando l'indirizzo IP della centrale visualizzato dal software Finder nella barra degli indirizzi.



Fase 2. Nella finestra di richiesta delle credenziali di accesso, inserire il nome utente e la password e premere "**Accedi**".



Nome Utente di default: **admin** Password di default: **cX+HsA*7F1**

ATTENZIONE! per ottemperare a recenti disposizioni anti-hackeraggio, la Centrale adotta il seguente meccanismo per la generazione della password. Dopo il primo inserimento della password predefinita **cX+HsA*7F1** il sistema richiede, al primo accesso di modificarla inserendo la propria. Se questo non avviene entro un'ora, il sistema impedisce l'accesso e sarà necessario disalimentare completamente e rialimentare la centrale per eseguire l'operazione completa.

NOTA BENE: in seguito a spegnimento o Reset o aggiornamento FW, la centrale riadotta la password predefinita.

Fase 3. La sottostante videata visualizza l'Accesso del Pannello di Controllo Locale con le informazioni relative alla centrale.



- [Accesso](#)
- [Home Page](#)
- [Storico Eventi](#)
- [Report Eventi](#)
- [Impostazioni Centrale](#)
- [Dati Utente](#)
- [Cattura Eventi](#)
- [Trasmissione Eventi](#)
- [Storico Dispositivi HA](#)
- [Gestione Dispositivi](#)
- [Gestione Rete](#)
- [Gestione Sistema](#)
- [Uscita](#)

Informazioni Generali

Versione Firmware:	MR-PRO 0.0.2.27L BG_U-ITR-F1-BD_BLA30.20201225
Versione Firmware/RF:	BG_U-ITR-F1-BD_BLA30.20201225
Versione ZigBee:	
Versione Z-wave:	
Versione GSM:	Quectel EC21EFAR06A03M4G
Indirizzo IP Pubblico:	5.90.2.154
Indirizzo IP Privato:	192.168.0.99
MAC Address:	00:10:94:01:12:24

© 2021 Elkron

5. GESTIONE DEI DISPOSITIVI

Nel presente capitolo vengono illustrate le modalità per apprendere, modificare, eliminare e controllare i vari dispositivi che possono comporre il sistema Egon. È possibile acquisire fino a **80** dispositivi e un totale massimo di **6** rivelatori con fotocamera o videocamera e un totale di **4** telecamere IP TEL600 (INT o EXT).

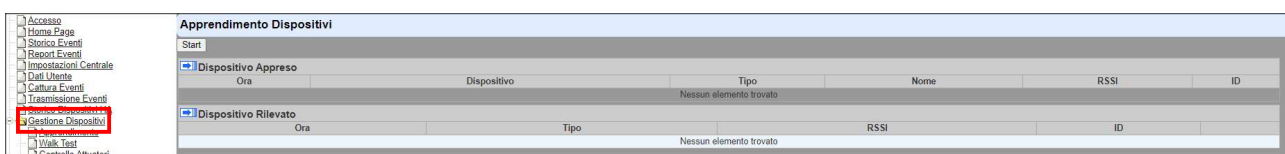
Per essere utilizzati, i seguenti dispositivi Zigbee:

- Rivelatori con fotocamera o videocamera: IR600FC, IR600VC, EIR600FC, IR600 FC/N
- Ripetitore Zigbee ZB600RPT
- LED di Stato LS600
- Dispositivi per la Home Automation

necessitano che sia installato il dispositivo USB/ZIGBEE (Dongle Zigbee opzionale).
La centrale può prevedere un massimo di 40 dispositivi Zigbee.

5.1. Apprendimento

Fase 1. Con la centrale in stato **Disattivo**, selezionare il sottomenu “**Apprendimento**” del menu “**Gestione Dispositivi**”.



Premere il tasto “**Start**”: la centrale entra nella fase di apprendimento, il LED 1 inizia a lampeggiare in verde e si attiverà un time out di 20 minuti per effettuare l'apprendimento dei dispositivi. Al termine del tempo, la centrale uscirà automaticamente dalla modalità apprendimento: il LED 1 della centrale ritornerà acceso fisso verde.

Fase 2. Premere il pulsante di apprendimento sul dispositivo. Per alcuni dispositivi (vedere manuali istruzioni dei singoli prodotti) tenere premuto il pulsante di apprendimento per circa 10 secondi per trasmettere un codice di apprendimento (per maggiori dettagli, consultare il manuale del dispositivo).

Fase 3. Se la centrale riceve il codice di apprendimento, emette 2 brevi ‘bip’ e visualizza le informazioni del dispositivo nella videata. Se invece la centrale emette 1 ‘bip’ lungo, vuol dire che il dispositivo è stato già acquisito dalla centrale.



<NOTA>

☞ Se il dispositivo da apprendere è già stato appreso in precedenza, questo comparirà nella sezione dei **Dispositivi Appresi**.

Fase 4. Premere “**Aggiungi**” per includere il dispositivo nella centrale. Il dispositivo è appreso nel sistema.

<NOTA>

La centrale è in grado di effettuare il test di Supervisione sui dispositivi solo se il Test Supervisione è stato in precedenza attivato nel sottomenu “**Impostazioni Centrale/Supervisione**”. Se invece i dispositivi vengono appresi con il test Supervisione disattivato, non sarà possibile abilitarlo in seguito, ma si dovrà eliminare e riapprendere i dispositivi che si vogliono sottoporre al Test Supervisione.

Fase 5. Effettuare la procedura dalla Fase 2 alla Fase 4 per acquisire altri dispositivi. Per uscire dalla modalità di apprendimento della centrale e riportarla al normale funzionamento, clicare sul pulsante “**Stop**”.

Fase 6. Selezionando il menu “**Home**” vengono visualizzati tutti i dispositivi precedentemente acquisiti.

Lista Dispositivi									
Dispositivo	Tipo	Nome	Condizione	Batteria	Tamper	Esclusione	RSSI	Stato	
1	Telecomando	Piero	■	■ Batteria bassa	■	No	Forte, 8		Modifica Elimina Escludi
4	IR	Sala	■	■	■	No	Forte, 9		Modifica Elimina Escludi
5	IR c/Camera	Ingresso	■	■	■	No	Forte, 9		Modifica Elimina Escludi Identifica

Significato delle colonne:

- **Dispositivo:** numero di inserimento del dispositivo
- **Tipo:** tipologia dispositivo
- **Nome:** nome che si può assegnare al dispositivo all'interno del sistema
- **Condizione:** stato di servizio del dispositivo (viene per esempio indicato se Fuori Servizio)
- **Batteria:** stato della batteria (viene indicato se la carica è bassa)
- **Tamper:** stato di manomissione (tamper) del dispositivo
- **Esclusione:** visualizza lo stato di disabilitazione permanente o temporanea del dispositivo
- **RSSI:** livello del segnale radio, misurato da 1 a 9. Con un livello inferiore a 3 la comunicazione è ancora garantita ma si consiglia di cercare una posizione che garantisca una maggiore portata
- **Stato:** informazioni sullo stato del dispositivo

Significato dei comandi:

- **Modifica:** permette di configurare il comportamento dei Dispositivi (vedi oltre)
- **Elimina:** permette di eliminare il dispositivo
- **Escludi:** permette di escludere il dispositivo (vedere descrizione nel capitolo relativo alla Home page)
- **Identifica:** permette di identificare alcuni tipi di dispositivi (vedere descrizione nel capitolo relativo alla Home page)

APPRENDIMENTO LOCALE TRAMITE TASTO DEDICATO A BORDO DELLA CENTRALE

La funzione di apprendimento locale della centrale serve per acquisire il dispositivo senza utilizzare il Pannello di controllo sul PC.

Fase 1. Tenere premuto il tasto di apprendimento locale/reset sul retro della centrale CR600WF per 10 secondi e rilasciarlo quando si sente un bip. Il LED 1 inizia a lampeggiare in verde per indicare che la centrale è in modalità di apprendimento.

Fase 2. Premere il tasto di apprendimento sui dispositivi per trasmettere un codice di apprendimento. Se la centrale riceve il codice di apprendimento, la centrale lo indica emettendo due bip.

Fase 3. Per uscire dalla modalità di apprendimento, premere il pulsante di reset fino a quando il led verde smette di lampeggiare e la centrale emette due bip

Fase 4. Continuare con la modifica delle impostazioni dei dispositivi nel Pannello di controllo locale.

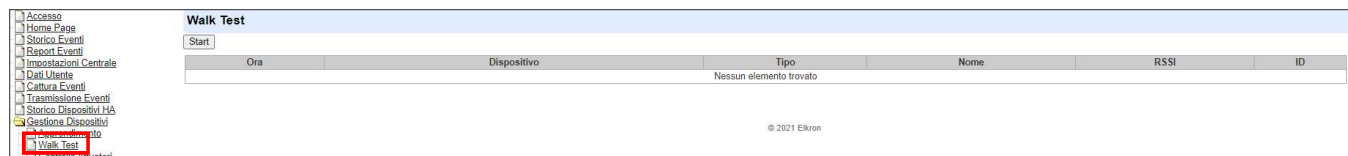
5.2. Walk Test

Il Walk Test deve essere utilizzato per verificare la presenza dei dispositivi, la loro portata radio e la corretta generazione degli allarmi.

<NOTA>

Per i test di copertura dei rivelatori di movimento fare riferimento ai relativi manuali istruzioni.

Fase 1. Selezionare il sottomenu **"Walk Test"** del menu **"Gestione Dispositivi"**. Durante il Walk test il LED 1 sulla centrale rimarrà spento per tutta la durata del Walk Test.



Premere il tasto **"Start"**: la centrale entra nella fase di Test, il LED 1 si spegne e si attiverà un time out di 20 minuti per effettuare il test dei dispositivi. Al termine del tempo, la centrale uscirà automaticamente dalla modalità apprendimento: il LED 1 della centrale ritornerà acceso fisso verde.

Fase 2. Premere il pulsante di apprendimento sul dispositivo per trasmettere un codice di test (per maggiori dettagli,

consultare il manuale del dispositivo) oppure generare un allarme.

Fase 3. Se la centrale riceve il codice di test, emette un 'bip lungo' e visualizza le informazioni del dispositivo nella videata; tra queste occorre in particolare verificare il livello di portata del dispositivo (colonna RSSI).

Walk Test						
Stop						
Ora	Dispositivo	Tipo	Nome	RSSI	ID	
18:12:22	13	Telecomando	Piero	9	RF:03d03500	

Fase 4. Per terminare il Walk Test e riportare la centrale al normale funzionamento, cliccare sul pulsante **"Stop"**. Il LED 1 torna verde fisso.

NOTA: il valore di segnale radio (RSSI) della telecamera IP TEL600 non è significativo perché la connessione con la telecamera è di tipo IP.

5.3. Modifica dei Dispositivi

Dopo aver acquisito un dispositivo nel sistema, nella videata "Home" si può procedere alla modifica delle sue impostazioni.

Fase 1. cliccare su **Modifica**, in corrispondenza del dispositivo che si vuole programmare.

Lista Dispositivi									
Dispositivo	Tipo	Nome	Condizione	Batteria	Tamper	Esclusione	RSSI	Stato	
1	Contatto Magnetico	Garage EEA				No	Buono, 5	Porta chiusa	Modifica Elimina Escludi

Fase 2. le impostazioni di Rivelatori, Telecomandi, Tastiere, Dispositivi Foto/Video e Sirene sono descritte nelle pagine seguenti. Cliccare sul pulsante **Salva** dopo aver inserito le impostazioni o le informazioni desiderate.

5.3.1 Rivelatori

Modifica Dispositivo

Contatto Magnetico

ID: RF:f0242210

Versione:

Riservato:

Nome:

Tag:

Dispositivo:

Attributo: ☐ Esclusione Permanente

Attributo: ☒ Memorizzato

Attributo: ☐ Attiva/Disattiva:

Attributo: ☐ 24 H:

Disattivo -:

Attivo Totale -:

Attivo Parziale A -:

Attivo Parziale B -:

Attivo Parziale C -:

Attivazione Trigger:

Fine Trigger:

Allarmi in Uscita: ☒ Disabilitati

Significato dei campi

- **ID:** identificativo del dispositivo, campo non modificabile.
- **Versione:** non disponibile. Per usi futuri.
- **Nome:** inserire un nome per il dispositivo. È consentito un massimo di 27 caratteri.
- **Tag:** non disponibile. Per usi futuri.
- **Dispositivo:** numero del dispositivo, normalmente non è necessario modificarlo, cambiarlo solo per necessità particolari.

- **Attributo: Disabilitazione permanente (esclusione):** questa opzione disattiva (esclude) il dispositivo selezionato finché non si deselezioni l'opzione. I segnali di batteria scarica e di manomissione inviati dal dispositivo verranno comunque segnalati. Per eliminare completamente le segnalazioni occorre eliminare il dispositivo.

ATTENZIONE! La Disabilitazione Permanente non disattiva:

- *le sirene, di cui esclude soltanto l'invio dei report delle segnalazioni di anomalie relative alle sirene*
- *i dispositivi di Home Automation, di cui esclude soltanto i messaggi di Supervisione.*
- *l'allarme sonoro e visivo sul rivelatore fumo*

Per la funzione di "Disabilitazione temporanea" del dispositivo, consultare il paragrafo **6.2. Funzione "Esclusione Dispositivo"**.

- **Attributo: Memorizzato:** questa opzione è utilizzata solo per i telecomandi e per i contatti porta utilizzati per attivare il sistema. Permette di stabilire se gli eventi relativi a questo dispositivo devono essere memorizzati tra gli eventi di sistema. Si consiglia di lasciare questa opzione abilitata
- **Attributo: Attiva/Disattiva:** questa opzione permette di utilizzare i contatti porta per attivare e disattivare il sistema. Se viene selezionato "**Normalmente aperto**", il contatto porta è a riposo quando è aperto. Quando il contatto porta si chiude, il sistema viene attivato totalmente. Se viene selezionato "**Normalmente chiuso**", il Contatto porta è a riposo quando è chiuso. Quando il contatto porta si apre, il sistema viene attivato totalmente.

ATTENZIONE! L'attivazione totale del sistema tramite questo attributo associato a un contatto magnetico avviene direttamente, senza tenere in considerazione eventuali anomalie presenti nel sistema e senza attivare il tempo di uscita.

- **24H:** se selezionato, l'allarme verrà sempre generato, a prescindere dallo stato di attivazione del sistema. E' possibile selezionare il tipo di allarme generato. Se viene selezionato questo attributo, non sarà possibile determinare gli attributi per gli altri stati
- **Disattivo:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del sistema in stato Disattivo. Se per esempio viene selezionato l'attributo Campanello, la centrale emetterà un suono in stato Disattivo ogni volta che il rivelatore sarà andato in allarme. In stato Disattivo non è possibile prevedere allarmi ritardati.
- **Attivo Totale:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del sistema in stato Attivo Totale. Se per esempio viene selezionato l'attributo Furto Istantaneo, la centrale genererà un allarme istantaneo ogni volta che il rivelatore sarà andato in allarme.
- **Attivo Parziale A:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del sistema in stato Attivo Parziale nella Zona A. Se per esempio viene selezionato l'attributo Ritardato Tempo 1, la centrale genererà un allarme Ritardato ogni volta che il rivelatore sarà andato in allarme.
- **Attivo Parziale B:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del sistema in stato Attivo Parziale nella Zona B. Se per esempio viene selezionato l'attributo Allarme Silenzioso, la centrale genererà un allarme Silenzioso ogni volta che il rivelatore sarà andato in allarme.
- **Attivo Parziale C:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del sistema in stato Attivo Parziale nella Zona C. Se per esempio viene selezionato l'attributo Nessuno, la centrale NON genererà nessun allarme quando il rivelatore sarà andato in allarme.
- **Trigger:** parametro per la gestione della Home Automation (vedere Guida dedicata).
- **Trigger ripristinato:** parametro per la gestione della Home Automation (vedere Guida dedicata).
- **Allarmi in Uscita:** se selezionato, non saranno generati allarmi durante il Tempo di Uscita.

Elenco degli attributi dei rivelatori

La tabella seguente mostra gli attributi associabili ai rivelatori Egon. Ogni attributo determina il comportamento del sistema in caso di allarme nei diversi stati (sistema disattivo, attivo totale, attivo parziale).

SE L'ATTRIBUTO DEL RIVELATORE È:	QUANDO IL RIVELATORE VA IN ALLARME IL COMPORTAMENTO DEL SISTEMA E' IL SEGUENTE:
NESSUNO	Non viene generato nessun allarme
CAMPANELLO	La centrale emette un suono di avvertimento
FURTO ISTANTANEO	Viene generato un allarme istantaneo
RITARDATO TEMPO 1	Viene generato un allarme al termine del Tempo di Ritardo 1 se il sistema non viene disattivato prima
RITARDATO TEMPO 2	Viene generato un allarme al termine del Tempo di Ritardo 2 se il sistema non viene disattivato prima
FURTO PERCORSO	Se il sensore va in allarme in stato Attivo Totale o Parziale, viene generato un allarme istantaneo Se il sensore va in allarme durante il tempo di ingresso, viene generato un allarme al termine del Tempo di Ritardo se il sistema non viene disattivato prima.
FURTO ESTERNO	Viene generato un allarme istantaneo identificato come Esterno
FURTO SILENZIOSO	Viene generato un allarme istantaneo silenzioso, cioè senza l'attivazione di allarmi acustici (sirena interna e esterna)

5.3.2 Telecomandi RC600 e Tastiere KP600

Significato dei campi

Modifica Dispositivo

Telecomando

ID: RF:04384600

Versione:

Riservato:

Nome:

Tag:

Dispositivo: 12 ▼

Attributo: ☐ Esclusione Permanente

Attributo: ☒ Memorizzato

Attributo: Pulsante Panico: Allarme Panico ▼

Attributo: Pulsante Totale: Default ▼

Attributo: Pulsante Parziale: Default ▼

Attributo: Pulsante Disattiva: Default ▼

Attributo: Selezione Zona: Parziale A ▼

[Cancella](#)

- **ID:** identificativo del dispositivo, campo non modificabile.
- **Versione:** non disponibile. Per usi futuri.
- **Nome:** inserire un nome per il dispositivo. È consentito un massimo di 27 caratteri.
- **Tag:** non disponibile. Per usi futuri
- **Dispositivo:** numero del dispositivo, normalmente non è necessario modificarlo, cambiarlo solo per necessità particolari.
- **Attributo: Disabilitazione permanente (esclusione):** questa opzione disattiva (esclude) il dispositivo selezionato finché non si deselezioni la funzione. I segnali di batteria scarica e di manomissione inviati dal dispositivo verranno comunque segnalati. Per eliminare completamente le segnalazioni occorre eliminare il dispositivo.
- **Attributo: Memorizzato:** questa opzione permette di stabilire se gli eventi relativi a questo dispositivo devono essere memorizzati tra gli eventi di sistema. Si consiglia di lasciare questa opzione abilitata
- **Attributo: Pulsante Panico:** l'impostazione dell'attributo (vedi oltre) determina il comportamento del tasto Panico del telecomando o della tastiera remota. Se per esempio viene selezionato l'attributo Allarme Panico Silenzioso, la pressione di esso genererà un allarme Panico senza l'attivazione delle sirene.
- **Attributo: Pulsante Totale:** modificare l'impostazione di fabbrica (default) solo per applicazioni di Home Automation (vedere Guida dedicata).
- **Attributo: Pulsante Parziale:** modificare l'impostazione di fabbrica (default) solo per applicazioni di Home Automation (vedere Guida dedicata).
- **Attributo: Pulsante Disattiva:** modificare l'impostazione di fabbrica (default) solo per applicazioni di Home Automation (vedere Guida dedicata).
- **Attributo: Selezione Zona:** questa opzione permette di stabilire quale Zona A, B o C attivare tramite il Pulsante Parziale.

Elenco degli attributi del tasto Panico dei telecomandi e delle tastiere

La tabella seguente mostra gli attributi associabili al tasto Panico dei telecomandi e delle tastiere Egon. Ogni attributo determina il comportamento del sistema in caso di pressione del tasto.

SE L'ATTRIBUTO DEL TASTO È:	QUANDO PREMUTO IL COMPORTAMENTO DEL SISTEMA E' IL SEGUENTE:
ALLARME FURTO	Viene generato un allarme istantaneo
ALLARME FUMO	Viene generato un allarme fumo
ALLARME PANICO SILENZIOSO	Viene generato un allarme senza l'attivazione delle sirene in caso di richiesta di attivazione sotto minaccia
ALLARME PANICO	Viene generato un allarme con l'attivazione delle sirene in caso di aggressione

NOTA BENE: gli attributi selezionabili ma non descritti nella tabella non sono operativi

Anche il telecomando è un dispositivo con comunicazione bidirezionale: quando il suo comando viene riconosciuto dalla centrale, conferma il riconoscimento facendo lampeggiare velocemente il suo LED (lampeggio verde). In caso di mancato riconoscimento il led lampeggia lentamente tre volte (lampeggio rosso). In questo ultimo caso controllare la sua programmazione e la sua portata.

Se si vuole attivare l'antifurto con il telecomando, anche in presenza di anomalie nel sistema, occorre premere due volte il tasto dedicato. L'inizio del conteggio da parte della centrale, se previsto, conferma l'avvenuta attivazione del sistema. Porre attenzione al suono del conteggio per essere certi di aver attivato il sistema, ed eventualmente regolare il volume nel menu **"Impostazioni Centrale"**.

5.3.3 Dispositivi foto/video

I rivelatori con fotocamera o videocamera e le telecamere IP possono essere gestiti e configurati nel sottomenu “**Dispositivi Video**” del menu “**Gestione Dispositivi**”.



Dispositivo	Tipo	Nome	Modifica	Elimina	Vedi	Programmazione
1	IP Camera		Modifica	Elimina	Vedi	Programmazione
Richiesta foto/video						

Significato delle colonne e dei comandi

Dispositivo	Tipo	Nome	Modifica	Elimina	Vedi	Programmazione
8	IR c/Camera	Esterno 868 F1	Modifica	Elimina		
			Richiesta foto/video	Richiesta foto/video (No Flash)		
10	IR c/Camera Esterno	Garage EIR	Modifica	Elimina		
			Richiesta foto/video	Richiesta foto/video (No Flash)		
15	IP Camera	IP camera TEST	Modifica	Elimina	Vedi	Programmazione
			Richiesta foto/video			

- **Dispositivo:** numero di inserimento del dispositivo
- **Tipo:** tipologia dispositivo
- **Nome:** nome che si può assegnare al dispositivo all'interno del sistema
- **Modifica:** permette di modificare i parametri e gli attributi del dispositivo, che sono gli stessi dei Rivelatori IR
- **Elimina:** permette di eliminare il dispositivo
- **Programmazione** (solo per Telecamera IP): permette di accedere ai menu di programmazione della telecamera IP
- **Richiesta foto/video:** permette di far scattare una foto al dispositivo per poter controllare le immagini riprese. Il rivelatore con fotocamera acquisisce 1 immagine, che può essere visionata nel menu “**Cattura Eventi**”.
- **Richiesta foto/video (no Flash):** le foto vengono eseguite senza l'ausilio del flash automatico (per non consumare le batterie del dispositivo)

Nel caso venga selezionata la telecamera IP, i video registrati saranno visibili su Portale, APP e interfaccia locale di programmazione della telecamera dopo qualche istante. Non saranno però visibili nella videata “**Cattura Eventi**”.

Elenco degli attributi delle telecamere IP

Modifica Dispositivo

IP Camera

ID: XF:001d940c666a

Versione:

Riservato:

Nome:

Tag:

Dispositivo: 1

Attributo: ☐ Esclusione Permanente

Attributo: Trigger da Dispos.: Tutti Disabilitato Disabilitato Disabilitato

Attributo: ☒ 24 H: Allarme Furto

Disattivo -: No Risposta

Attivo Totale -: Furto Istantaneo

Attivo Parziale A -: No Risposta

Attivo Parziale B -: No Risposta

Attivo Parziale C -: No Risposta

Attivazione Trigger: Nessuna

Fine Trigger: Nessuna

Allarmi in Uscita: ☒ Disabilitati

OK Default Reset Cancell

- **ID:** identificativo del dispositivo, campo non modificabile.
- **Versione:** non disponibile. Per usi futuri.
- **Nome:** inserire un nome per il dispositivo. È consentito un massimo di 27 caratteri.
- **Tag:** non disponibile. Per usi futuri.
- **Dispositivo:** normalmente non è necessario modificare il numero del dispositivo, cambiarlo solo per necessità particolari.
- **Attributo: Disabilitazione permanente (esclusione):** questa opzione disattiva (esclude) il dispositivo selezionato finché non si deselezioni la funzione.
- **Attributo: Trigger da dispositivo:** tramite queste 4 opzioni è possibile associare la registrazione di un video ad un allarme generato da 4 diversi rivelatori oppure da qualunque rivelatore presente nell'impianto (opzione Tutti). Selezionare il numero del rivelatore da associare rilevandolo nella tabella dei Dispositivi oppure selezionare Tutti. Oltre ai rivelatori, è possibile associare un telecomando: in questo caso il video verrà inviato in caso di allarme Panico.
- **Attributo: 24H:** se selezionato, sarà sempre possibile visualizzare la telecamera da remoto.

Nel caso si desideri che la telecamera IP possa essere visualizzata solo in determinati stati (disattivo, parziale A, B o C, attivo totale) occorre deselezionare l'opzione **24H** e selezionare l'attributo FURTO ISTANTANEO negli stati prescelti. Gli altri attributi in questo caso non sono significativi.

Se per esempio viene utilizzata la seguente configurazione:

Attributo: ☐ 24 H: Allarme Furto

Disattivo -: No Risposta

Attivo Totale -: Furto Istantaneo

Attivo Parziale A -: No Risposta

Attivo Parziale B -: Furto Istantaneo

Attivo Parziale C -: No Risposta

la telecamera sarà visibile con il sistema attivo nella zona B o attivo totalmente, mentre non sarà visibile negli altri stati disattivo e attivato nelle zone A e C.

5.3.4 Sirene

Le sirene possono essere gestite e configurate nel sottomenu “**Gestione Sirene**” del menu “**Gestione Dispositivi**”.

Significato delle colonne e dei comandi



- **Dispositivo:** numero di inserimento del dispositivo
- **Tipo:** tipologia dispositivo
- **Nome:** nome che si può assegnare al dispositivo all'interno del sistema
- **Tamper On:** questa opzione serve per abilitare la protezione antimanomissione della sirena.
- **Tamper Off:** questa opzione serve per disabilitare la protezione antimanomissione della sirena.
- **Suono Conferma On:** con questa opzione è possibile decidere di far emettere un bip di avviso alla sirena quando il sistema viene attivato o disattivato.
- **Suono Conferma Off:** con questa opzione il bip di avviso viene disabilitato.
- **Suono Ingresso On:** con questa opzione è possibile decidere di far emettere un bip di avviso alla sirena durante il conteggio del tempo di entrata.
- **Suono Ingresso Off:** con questa opzione il bip di avviso viene disabilitato.

<NOTE>

- ☞ Le modifiche sull'impostazione della Sirena saranno effettuate contemporaneamente su tutte quelle presenti nel sistema, ma NON su quella interna alla centrale.
- ☞ Per evitare un allarme di manomissione accidentale quando si cambiano le batterie della sirena o si cambia la sua posizione di installazione, è necessario dapprima disattivare il Tamper della sirena, selezionando "Tamper Sirena OFF" nella videata di modifica.
- ☞ Se si dimentica di riabilitare il Tamper, dopo un'ora la rilevazione tornerà comunque attiva.

6. IMPOSTAZIONI DEL SISTEMA

In questo capitolo sono analizzate i menu per la configurazione di base del sistema.

Si consiglia di procedere con la configurazione del sistema rispettando la sequenza delle videate presentata in questo capitolo.

6.1. Accesso – Informazioni generali

In questa pagina è possibile visualizzare i dati della centrale, in particolare la versione firmware e il Mac Address.

Informazioni Generali

Versione Firmware:

MR-PRO 0.0.2.27G BG_U-ITR-F1-BD_BL A30 20201225

Versione Firmware/RF:

BG_U-ITR-F1-BD_BL A30 20201225

Versione ZigBee:

Versione Z-wave:

Versione GSM:

Quectel EC21EFAR06A03M4G

Indirizzo IP Pubblico:

37.103.154.201

Indirizzo IP Privato:

192.168.1.13

MAC Address:

00:1D:94:01:12:23

6.2. Home page

In questa pagina sono presenti gli stati e i comandi più importanti dell'impianto.

Home Page

Report Eventi

Impostazioni Centrale

Quali Utente

Cattura Eventi

Trasmissione Eventi

Storico Dispositivi HA

Gestione Dispositivi

Gestione Rete

Gestione Sistema

Uscita

Centrale

Stato Attivazione: Attivo Parziale A

Stato

Batteria	Tamper	ZigBee dongle	Interferenza	Rete Elettrica	Segnale GSM	Rumore RF
Batteria mancante/scarica	Normale	N/D	Normale	Normale	N/D	1

Stato Anomalia

Anomalia	Disabilitazione Segnalazione
SIM Non Inserita	<input type="checkbox"/> Azzerà
Nessun segnale GSM	<input type="checkbox"/> Azzerà
Batteria centrale mancante/scarica	<input type="checkbox"/> Azzerà
Disconnessione WIFI	<input type="checkbox"/> Azzerà
Numero5 Batteria bassa	<input type="checkbox"/> Azzerà
Zone3 Not Found	<input type="checkbox"/> Azzerà
Zone17(Ingresso) Not Found	<input type="checkbox"/> Azzerà
Zone10(Garage EIR) Not Found	<input type="checkbox"/> Azzerà
Zone8(Esterno 868 F1) Not Found	<input type="checkbox"/> Azzerà
Zone2(CASA Soggiorno) Not Found	<input type="checkbox"/> Azzerà
Zone6(CASAPortone 2) Not Found	<input type="checkbox"/> Azzerà
Zone16 Not Found	<input type="checkbox"/> Azzerà

OK Reset

Ricarica

Lista Dispositivi

Dispositivo	Tipo	Nome	Condizione	Batteria	Tamper	Esclusione	RSSI	Stato	Modifica	Elimina	Escludi
1	Contatto Magnetico	Garage EEA				No	Buono, 5	Porta chiusa			
2	IR	CASA Soggiorno	Fuori Servizio			No	N/D		Modifica	Elimina	Escludi
3	Sirena					No			Modifica	Elimina	Escludi
4	Contatto Magnetico	Porta retro	Fuori Servizio			No	Forti, 9	Porta chiusa	Modifica	Elimina	Escludi
5	Telecomando			Batteria bassa		No	Forti, 9		Modifica	Elimina	Escludi

- **Stato attivazione:** stato di attivazione del sistema (attivo/disattivo/parzializzato)

Centrale

Stato Attivazione: Disattivo

- **Stato Centrale:** in quest'area vengono visualizzati gli stati della centrale relativi:

Stato

Batteria	Tamper	ZigBee dongle	Interferenza	Rete Elettrica	Segnale GSM	Rumore RF
Normale	Normale	Normale	Normale	Normale	N/D	1

- alla presenza o allo stato di carica della batteria di backup interna
- alla corretta chiusura dell' contenitore (tamper)
- alla presenza del Dongle Zigbee USB/ZIGBEE. NOTA BENE: se nell'impianto sono presenti dispositivi Zigbee, la manomissione del dispositivo genera un allarme di sabotaggio di tipo Tamper
- alla presenza di tentativi di accecamento radio della centrale (interferenza jamming)
- allo stato di alimentazione da rete elettrica
- alla presenza di una connessione GSM
- alla presenza di rumore radio nell'ambiente. Un valore 0 significa nessuna interferenza, un valore 9 significa massima interferenza. Il valore deve perciò rimanere basso per garantire la massima affidabilità del sistema

- **Stato Anomalie:** in quest'area vengono elencate le anomalie eventualmente presenti nel sistema. Dal momento che il sistema richiede una doppia conferma per l'attivazione del sistema in caso di presenza di anomalie, in questa videata è anche possibile decidere se ignorare quelle selezionate e attivare il sistema direttamente senza la necessità di una doppia conferma (codice reinserito o comando di attivazione forzato sulle tastiere o tasto attivazione ripremuto sul telecomando). Selezionando **"Azzera"** e premendo il tasto **"OK"** si stabilisce di ignorare l'anomalia.

Stato Anomalie	
Anomalia	Disabilitazione Segnalazione
Tamper centrale	<input type="checkbox"/> Azzera
SIM Non Inserita	<input type="checkbox"/> Azzera
Nessun segnale GSM	<input type="checkbox"/> Azzera
Disconnessione WiFi	<input type="checkbox"/> Azzera
Batteria centrale mancante/scarica	<input type="checkbox"/> Azzera

- **Lista Dispositivi:** in quest'area vengono elencati i dispositivi presenti nel sistema e le loro caratteristiche. Vengono inoltre resi disponibili i comandi di Modifica, Eliminazione, Esclusione e Identificazione:

Lista Dispositivi									
Dispositivo	Tipo	Nome	Condizione	Batteria	Tamper	Esclusione	RSSI	Stato	
1	Telecomando	Piero		Batteria bassa		No	Forte, 8		Modifica Elimina Escludi
4	IR	Sala				No	Forte, 9		Modifica Elimina Escludi
5	IR c/Camera	Ingresso				No	Forte, 9		Modifica Elimina Escludi Identifica

- **Dispositivo:** numero di inserimento del dispositivo
- **Tipo:** tipologia dispositivo
- **Nome:** nome che si può assegnare al dispositivo all'interno del sistema
- **Condizione:** stato di servizio del dispositivo (viene per esempio indicato se Fuori Servizio)
- **Batteria:** stato della batteria (viene indicato se la carica è bassa)
- **Tamper:** stato di manomissione (tamper) del dispositivo
- **Esclusione:** visualizza lo stato di disabilitazione permanente o temporanea del dispositivo
- **RSSI:** livello del segnale radio, misurato da 1 a 9. Con un livello inferiore a 3 la comunicazione è ancora garantita ma si consiglia di cercare una posizione che garantisca una maggiore portata
- **Stato:** informazioni sullo stato del dispositivo (per esempio lo stato di apertura di un Contatto)
- **Modifica:** permette di modificare i parametri d'uso dei dispositivi (vedi paragrafo 5.3 **Modifica delle impostazioni del dispositivo**)
- **Elimina:** permette di eliminare i dispositivi (vedi oltre)
- **Escludi:** permette di escludere i dispositivi (vedi oltre)
- **Identifica:** permette di identificare alcuni tipi di dispositivi (vedi oltre)

Selezionando **"Ricarica"** si aggiorna lo stato dei dispositivi in tempo reale.

Eliminazione di un dispositivo

Per rimuovere un dispositivo dalla centrale, selezionare la relativa casella e cliccare su **"Elimina"**: il dispositivo selezionato sarà rimosso.

ATTENZIONE! Per ragioni di sicurezza, la funzione "Elimina" non disattiva le sirene anche se le esclude dalla lista dei dispositivi e dai report delle segnalazioni di anomalie.

Per disattivare le sirene occorre disalimentarle o fare un reset di fabbrica (vedere manuale del dispositivo).

<NOTA>

Se un dispositivo rimane disconnesso dalla centrale, il suo consumo risulterà maggiore.

Per eliminare i dispositivi Zigbee IR600FC, IR600VC, IR600 FC/N, EIR600FC, ZB600RPT, LS600 e per tutti i dispositivi di Home Automation non è necessario eseguire il comando di Eliminazione ma è sufficiente il loro Reset ai valori di fabbrica

Esclusione di un dispositivo

I dispositivi possono essere temporaneamente esclusi selezionando la casella relativa e cliccando su “**Escludi**”. Nel caso dei Contatti Magnetici, la prima intrusione verrà ignorata dal sistema durante la prima attivazione, tutte le successive intrusioni genereranno invece l'allarme. Nel caso dei Rivelatori IR, non saranno generati allarmi per tutto il periodo di attivazione. Durante tale periodo, il dispositivo segnalerà comunque eventuali situazioni di batteria scarica e di manomissioni.

È possibile utilizzare questa funzione per evitare allarmi di manomissione accidentali quando si cambiano le batterie di un dispositivo o si cambia la sua posizione.

ATTENZIONE! La Disabilitazione Temporanea non disattiva la telecamera IP e i dispositivi di Home Automation. Per le sirene, la disabilitazione temporanea impedisce soltanto l'invio dei report delle segnalazioni di anomalie. Per i dispositivi di Home Automation, impedisce le segnalazioni di mancate supervisioni. Per i rivelatori di fumo disabilita la segnalazione di allarme sulla centrale ma non quello sul dispositivo stesso

Identificazione di un dispositivo

La funzione di identificazione, nella videata di Gestione dei dispositivi, è disponibile solo per i dispositivi IR600FC, IR600VC, IR600 FC/N, EIR600FC, ZB600RPT, LS600 e per tutti i dispositivi di Home Automation e può essere utilizzata per individuare questi dispositivi dopo l'apprendimento.

La funzione di identificazione NON deve essere utilizzata entro 1 minuto dalla pressione del pulsante del dispositivo o entro 3 minuti dall'apprendimento del dispositivo. In questi casi il dispositivo potrebbe non ricevere correttamente i segnali dalla centrale.

Fase 1. Selezionare la casella con il numero del dispositivo e cliccare su “Identifica” sotto la lista.

Fase 2. Se il dispositivo riceve correttamente il segnale, il relativo led di segnalazione lampeggia 10 volte per conferma. Se il led del dispositivo non lampeggia, vuol dire che il dispositivo non riceve il segnale dalla centrale.

- **Note:** area in cui è possibile inserire delle proprie note promemoria tramite il comando “**Modifica**”

Note			
No.	Tipo	Descrizione	
#1			Modifica
#2			Modifica

Il comando **Reset Centrale** permette di resettare la centrale riavviandola senza modificare nessuna delle programmazioni fatte.

Il comando **Reset ZigBee** permette di resettare il Dongle Zigbee in caso di problemi.

6.3. Storico Eventi

In questo menu è disponibile lo storico degli eventi della centrale tra i quali sono compresi:

- ✓ Tutti gli eventi di allarme
- ✓ Tutti gli eventi di anomalie
- ✓ Tutti gli eventi di attivazione e disattivazione da telecomando o tastiera con l'utente
- ✓ Tutti gli eventi di attivazione e disattivazione da remoto.

Storico Eventi			
Ricarica			
Ora	Dispositivo	Utente	Evento
2022-01-24 18:05:36			Report OK
2022-01-24 18:05:34	Zona13(Pieno)		Disattivazione
2022-01-24 18:05:28			Report OK
2022-01-24 18:05:26	Zona4(Porta retro)		Furto (Volumetrico)
2022-01-24 18:05:05	Zona4(Porta retro)		Tempo Ingresso 1
2022-01-24 18:05:01			Report OK
2022-01-24 18:04:50	Zona13(Pieno)		Parcializzazione A
2022-01-24 18:04:35			Report OK
2022-01-24 18:04:33	Zona13(Pieno)		Disattivazione
2022-01-24 18:04:18			Report OK
2022-01-24 18:04:15	Zona4(Porta retro)		Allarme Furto
2022-01-24 18:04:11			Report OK

- **Data e ora:** data e ora in cui si è verificato l'evento.
- **Dispositivo:** dispositivo che ha provocato l'evento.
- **Utente:** utente che ha eseguito l'azione relativa all'evento.
- **Evento:** descrizione dell'evento.

<NOTA>: GLI EVENTI RELATIVI ALLE TELECAMERE IP TEL600 NON SONO DISPONIBILI IN QUESTA VIDEATA.____

6.4. Report Eventi

Questo menu riporta dati che non sono destinati all'utente ma al servizio di assistenza e potranno essere richiesti per eseguire delle diagnosi sull'impianto

6.5. Impostazioni Centrale

In questo menu è possibile configurare alcune impostazioni relative alla centrale ed al sistema.

- **Tempo assenza rete elettrica:** in questo campo, specificare il tempo di attesa per la centrale prima di generare una segnalazione in seguito al rilevamento dell'assenza di alimentazione elettrica. L'impostazione di fabbrica è **5 minuti**.
- **Tempo ritardo risparmio energia:** in caso di assenza di rete elettrica la centrale va in modalità di risparmio energia (vedi paragrafo 2.4, uso della Batteria ricaricabile). Questo tempo stabilisce quanto viene ritardata l'avvio della modalità L'impostazione di fabbrica è **5 secondi**.
- **Abilitazione Jamming:** in questo campo, indicare se la centrale deve rilevare le interferenze a radiofrequenza e generare una segnalazione in caso positivo. Se la centrale rileva un disturbo radio in grado di accecarne le comunicazioni con i dispositivi per oltre 1 o 2 minuti, segnalerà l'evento tramite i report previsti. L'allarme scompare se il disturbo viene a mancare per oltre 1 o 2 minuti. L'impostazione di fabbrica è **1 minuto**
- **Test Periodico:** questa funzione permette di configurare i test periodici della centrale, interni e di reportistica. L'impostazione di fabbrica è **24 ore**
- **Offset Test Periodico:** il tempo di Offset permette di stabilire dopo quanto tempo viene inviato il primo report a partire dall'accensione della centrale. L'impostazione di fabbrica è **1 ora**
- **Risoluzioni Immagini di Allarme:** con questa funzione è possibile modificare l'impostazione di cattura delle immagini di allarme dei rivelatori con fotocamera. Le opzioni disponibili sono:
 - ☞ **640 x 480 x 3:** il rivelatore con fotocamera acquisisce 3 immagini con risoluzione 640 x 480 quando rileva un'intrusione.
 - ☞ **320 x 240 x 6:** il rivelatore con fotocamera acquisisce 6 immagini con risoluzione 320 x 240 quando rileva un'intrusione.
 - ☞ **320 x 240 x 3:** il rivelatore con fotocamera acquisisce 3 immagini con risoluzione 320 x 240 quando rileva un'intrusione (**Impostazione di fabbrica**)
- **Immagini in scala di grigi per esterni:** consente di stabilire se le immagini di allarme vanno riprese in bianco/nero, per ottenere una migliore resa video in particolari condizioni. L'impostazione di fabbrica è **Disabilitate**
- **Sirena interna:** se abilitata, la sirena integrata nella centrale viene attivata ed emette un suono di allarme quando viene generato un allarme. L'impostazione di fabbrica è **Abilitata**
- **Ignorare guasto IP/4G:** consente di decidere se si vuole ignorare o meno eventi di errore relativi alla funzione Ethernet o 4G. Gli eventi di errore ignorati non saranno visualizzati nel pannello di controllo locale.
 - ☞ **Disattivo:** Se si seleziona Disattivo, nessun evento viene ignorato (**Impostazione di fabbrica**)
 - ☞ **IP:** Se si seleziona IP, gli eventi relativi alla funzione Ethernet vengono ignorati.
 - ☞ **4G:** Se si seleziona 4G, gli eventi relativi alla trasmissione dati 4G vengono ignorati.
 - ☞ **IP+4G:** Se si seleziona IP+4G, tutti gli eventi relativi alla connessione Internet vengono ignorati.
- **NOTA BENE:** l'esclusione disabilita anche le possibilità di connessioni IP e GSM
- **Lingua:** permette di selezionare la lingua d'uso

Dopo avere completato le impostazioni precedenti, premere il pulsante **"OK"** per confermare le modifiche.

Altre Impostazioni:

- **Ultima uscita:**

☞ **Ultima uscita On:** quando il sistema viene **Attivato Totalmente** e un contatto magnetico impostato con un attributo **Ritardato** da aperto si chiude, il sistema si attiva senza attendere la fine del ritardo di uscita.

☞ **Ultima uscita Off:** la funzione descritta sopra non è attiva. L'impostazione di fabbrica è **Ultima uscita Off**.

- **Attivare con anomalie:**

☞ **Conferma:** con questa impostazione, se si tenta l'attivazione in presenza di un'anomalia, viene richiesta una doppia conferma per l'attivazione del sistema (codice reinserito o comando di attivazione forzato sulle tastiere o tasto attivazione ripremuto sul telecomando). L'impostazione di fabbrica è **Conferma**.

☞ **Attivazione diretta:** con questa impostazione l'attivazione del sistema in presenza di un'anomalia avviene direttamente senza la necessità di una doppia conferma.

- **Tamper:**

☞ **Totale.** Gli allarmi antimanomissione (Allarmi Tamper) vengono generati solo in stato di attivazione totale (l'evento di manomissione viene comunque segnalato anche in stato di attivazione parziale o di disattivazione). L'impostazione di fabbrica è **Totale**.

☞ **Sempre.** L'allarme antimanomissione viene generato in qualsiasi stato del sistema.

- **Supervisione:** abilita/disabilita la supervisione per i dispositivi accessori. Se non viene ricevuto alcun segnale di supervisione entro il periodo impostato per un determinato dispositivo, la centrale segnerà un allarme di supervisione, che verrà notificato all'utente. L'impostazione di fabbrica è **On**.

***ATTENZIONE.** Per avvalersi della modalità di Supervisione e del relativo allarme in caso di mancata ricezione del segnale di un dispositivo da parte della centrale, il dispositivo deve essere appreso con il Test Supervisione abilitato.*

Impostazione Tempi:

- **Timer Supervisione:** imposta il timer di supervisione per i dispositivi accessori. L'impostazione di fabbrica è **12 ore**.
- **Ritardo ingresso 1 Totale:** stabilisce il tempo che viene lasciato all'utente per disattivare il sistema attivo Totale quando vengono generati allarmi dai rivelatori che prevedono i ritardi di ingresso 1. (Per maggiori informazioni, consultare il paragrafo 5.3. **Modifica delle impostazioni del dispositivo**). L'impostazione di fabbrica è **20 secondi**.
- **Ritardo ingresso 2 Totale:** stabilisce il tempo che viene lasciato all'utente per disattivare il sistema attivo Totale quando vengono generati allarmi dai rivelatori che prevedono i ritardi di ingresso 2. (Per maggiori informazioni, consultare il paragrafo 5.3. **Modifica delle impostazioni del dispositivo**). L'impostazione di fabbrica è **20 secondi**.
- **Ritardo uscita Totale:** stabilisce il tempo necessario all'attivazione del sistema attivo Totale. L'impostazione di fabbrica è **30 secondi**.
- **Ritardo ingresso 1 Parziale:** stabilisce il tempo che viene lasciato all'utente per disattivare il sistema attivo Parziale quando vengono generati allarmi dai rivelatori che prevedono i ritardi di ingresso 1. (Per maggiori informazioni, consultare il paragrafo 5.3. **Modifica delle impostazioni del dispositivo**). L'impostazione di fabbrica è **20 secondi**.
- **Ritardo ingresso 2 Parziale:** stabilisce il tempo che viene lasciato all'utente per disattivare il sistema attivo Parziale quando vengono generati allarmi dai rivelatori che prevedono i ritardi di ingresso 2. (Per maggiori informazioni, consultare il paragrafo 5.3. **Modifica delle impostazioni del dispositivo**). L'impostazione di fabbrica è **20 secondi**.
- **Ritardo uscita Parziale:** stabilisce il tempo necessario all'attivazione del sistema attivo Parziale. L'impostazione di fabbrica è **30 secondi**.
- **Durata attivazione allarme:** quando viene attivato un allarme, sia la sirena della centrale sia la sirena esterna emettono un allarme in base all'impostazione della durata dell'allarme definita in questo campo. L'impostazione di fabbrica è **3 minuti**.

<NOTA>

Verificare contestualmente la configurazione di Durata Allarme della sirena esterna. Se sono state impostate tempistiche diverse tra il Pannello di Controllo locale e la sirena, prevale la tempistica più breve.

I suoni generati dalla centrale a fronte degli eventi che seguono possono essere disabilitati (**Off**), emessi con un volume **Basso** o con un volume **Alto**:

- ☞ **Campanello:** se abilitato, la centrale emette un breve suono quando viene generato un allarme su un rivelatore con la funzione Campanello con il sistema in stato disattivo. (Per maggiori informazioni, consultare il paragrafo 5.3 **Modifica delle impostazioni del dispositivo**.)
- ☞ **Ingresso totale:** se abilitato, la centrale in stato di attivazione totale emette dei 'bip' durante il tempo di ingresso.
- ☞ **Uscita totale:** se abilitato, la centrale emette dei 'bip' durante il tempo di uscita per l'attivazione totale.
- ☞ **Ingresso parziale:** se abilitato, la centrale in stato di attivazione parziale emette dei 'bip' durante il tempo di ingresso.
- ☞ **Uscita parziale:** se abilitato, la centrale emette dei 'bip' durante il tempo di uscita per l'attivazione parziale.
- ☞ **Conferma Attivazione/Disattivazione:** se abilitato, la centrale emette un suono nel momento della Attivazione e della Disattivazione.
- ☞ **Avvertimento:** se abilitato, la centrale emette dei 'bip' ogni 30 secondi se nel sistema è presente un'anomalia.
- ☞ **Durata suoni tempi Ingresso/Uscita:** è possibile stabilire per quanti secondi la centrale emette dei 'bip' durante la Attivazioni e le Disattivazioni

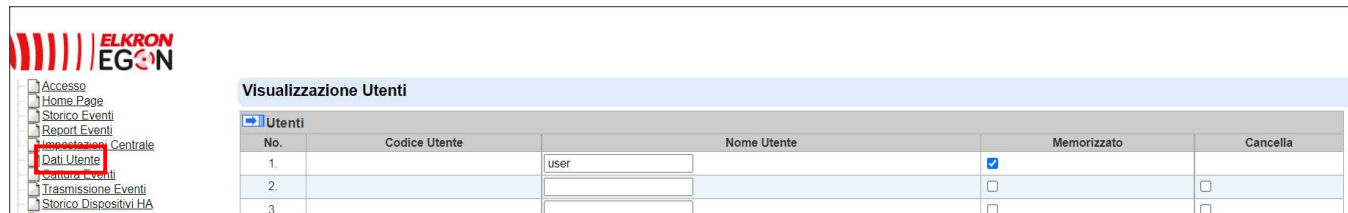
<NOTA>

Le sirene, attivate in caso di allarme incendio generato da un rivelatore di fumo, hanno un suono diverso dall'allarme intrusione, di tipo intermittente

Dopo avere completato le impostazioni precedenti, premere il pulsante "**OK**" per confermare le modifiche.

6.6. Dati Utenti

In questa videata vengono visualizzati i nominativi degli utenti abilitati a utilizzare il sistema, inseriti tramite l'APP o il portale. In questa pagina non è possibile inserire nuovi utenti ma solo visualizzarli.



The screenshot displays the 'Visualizzazione Utenti' (User Visualization) screen. On the left, a sidebar menu includes options like 'Accesso', 'Home Page', 'Storico Eventi', 'Report Eventi', 'Impostazioni Centrale', 'Dati Utenti' (highlighted with a red box), 'Scambio Eventi', 'Trasmissione Eventi', and 'Storico Dispositivi HA'. The main area shows a table with the following data:

No.	Codice Utente	Nome Utente	Memorizzato	Cancella
1.		user	<input checked="" type="checkbox"/>	
2.			<input type="checkbox"/>	<input type="checkbox"/>
3.			<input type="checkbox"/>	<input type="checkbox"/>

Per motivi di sicurezza, i codici personali degli utenti non vengono visualizzati. Il codice di fabbrica per l'utente 1 è **1234**.

Il campo "**Memorizzato**" viene utilizzato per stabilire se le operazioni di attivazione e disattivazione dell'utente vengono riportate nella lista degli eventi. La spunta del campo abilita la registrazione degli eventi.

Il campo "**Cancella**" permette di cancellare eventuali codici supplementari.

6.7. Cattura Eventi

In questa videata vengono visualizzati immagini e video acquisiti dai rivelatori con fotocamera e videocamera. Vengono memorizzati solo immagini e video degli ultimi eventi.

Ora	Num.	Tipo	Stato	Media	Commenti	
2021-12-09 15:49:20	1	Allarme	Fatto		No Packet Lost, No Packet Lost, No Packet Lost,	Elimina
2021-12-09 15:43:04	1	Allarme	Fatto		No Packet Lost, No Packet Lost, No Packet Lost, No Packet Lost, No Packet Lost, No Packet Lost,	Elimina
2021-12-09 15:35:11	1	Allarme	Fatto		No Packet Lost, No Packet Lost, No Packet Lost,	Elimina

- **Ora:** data e ora di acquisizione dell'immagine/video.
- **Dispositivo:** numero identificativo del rivelatore che ha fornito l'immagine o il video.
- **Tipo:** tipo di immagine o video memorizzati, in seguito ad allarme o su richiesta.
- **Stato:** lo stato dell'evento acquisito può assumere i valori seguenti:
 - **In attesa file media:** il rivelatore con fotocamera o videocamera ha acquisito e invierà l'immagine/il video alla centrale non appena il file sarà pronto. Per le immagini/video di allarme, se si disattiva la centrale in questo stato, l'immagine e il video acquisiti saranno cancellati e non verranno inviati.
 - **In attesa di cattura:** il rivelatore con fotocamera o videocamera sta inviando l'immagine/il video acquisito alla centrale. Per immagini/video di allarme, se si disattiva la centrale in questo stato, l'immagine e il video acquisiti saranno cancellati e non verranno inviati.
 - **Caricato:** il rivelatore con fotocamera o videocamera ha terminato l'invio dell'immagine/del video alla centrale. La centrale sta ora caricando l'immagine/il video sulla destinazione programmata.
 - **Disponibile:** La centrale ha terminato di caricare l'immagine/il video.
 - **Fallito:** il rivelatore con fotocamera o videocamera non è riuscito a inviare l'immagine/il video alla centrale. Verificare che la fotocamera/videocamera non sia guasta o che la sua batteria non sia scarica (foto e filmati richiedono molta energia) e poi eseguire un Walk Test per controllare l'intensità del segnale.
 - **Timeout:** il rivelatore con fotocamera o videocamera non ha risposto alla richiesta della centrale. Verificare che la fotocamera/videocamera non sia guasta o che la sua batteria non sia scarica (foto e filmati richiedono molta energia) e poi eseguire un Walk Test per controllare l'intensità del segnale.
- **Media:** visualizzazione dei video e delle foto memorizzate. Cliccare sull'immagine o sul Download del video per visualizzare il file.
- **Commenti:** stato delle trasmissioni dati
- **Elimina:** elimina il video o la foto dalla memoria interna della centrale


<NOTE>

☞ Se un allarme di un rivelatore con fotocamera o videocamera viene generato mentre il sistema è attivo, non disattivare il sistema di allarme prima che venga visualizzato lo stato "Caricato" o "Disponibile." In caso contrario, l'immagine/il video saranno cancellati e non verranno inviati alla centrale e al Server di sistema.

☞ I video registrati dalle telecamere IP TEL600 non sono disponibili in questa videata

6.8. Trasmissione Eventi (menu per utenti specializzati)

In questo menu vengono elencati tutti gli eventi che si sono succeduti durante il normale funzionamento della centrale e che sono stati inviati al server di sistema:

						
Trasmissione Eventi						
Ricarica						
<div>Accesso Home Page Storico Eventi Report Eventi Impostazioni Centrale Dati Utente Cattura Eventi Trasmissione Eventi Stato Dispositivi HA Gestione Dispositivi Gestione Rete Gestione Sistema Uscita</div>						
Ora	Zona/Utente	Trigger / Ripristino	Evento CID	Note	Stato Trasmissioni	
2022-01-05 11:07:50	1	Restore	721	Attivo Parziale B	Fatto	
2022-01-05 11:07:17	1	Trigger	401	Disattivazione Remota	Fatto	
2022-01-05 11:06:16	4	Trigger	132	Furto (Volumetrico)	Fatto	
2022-01-05 11:05:34	1	Restore	720	Attivo Parziale A	Fatto	
2022-01-05 11:04:04	1	Trigger	400	Disattivazione da Telecomando	Fatto	
2022-01-05 11:03:01	7	Trigger	130	Furto	Fatto	
2022-01-05 11:01:47	1	Restore	400	Attivazione da Telecomando	Fatto	
2022-01-05 11:01:22	1	Trigger	400	Disattivazione da Telecomando	Fatto	
2022-01-05 11:00:23	1	Restore	400	Attivazione da Telecomando	Fatto	
2022-01-05 10:57:30	7	Restore	383	Tamper Ripristinato	Fatto	
2022-01-05 10:56:34	7	Trigger	383	Tamper	Fatto	
2022-01-05 09:03:34	0	Trigger	602	Test Periodico	Fatto	

La centrale registra un totale di 250 eventi segnalati con le informazioni descritte di seguito:

- **Ora:** data e ora dell'evento.
- **Dispositivo/Utente:** viene visualizzato il numero del dispositivo relativo all'evento.
- **Trigger/Ripristino:** definisce il tipo di evento
- **Evento CID:**
 - Il codice CID Evento viene registrato in un formato di 4 cifre costituito da **"Prefisso + Codice evento"**
 - Prefisso: **"1"** rappresenta gli eventi che stanno avvenendo. **"3"** rappresenta il ripristino degli eventi.
 - Codice evento: Codice CID Evento di 3 cifre. Per esempio: **"1302"** vuol dire "Batteria scarica" e **"3302"** vuol dire "Ripristino da batteria scarica".
- **Descrizione:** descrizione dell'evento
- **Stato:** visualizza l'avvenuta trasmissione dell'evento.

<NOTA>

Gli eventi relativi alle telecamere IP non sono disponibili in questa videata.

6.9. Storico Dispositivi HA

In questo menu è disponibile lo storico degli eventi della centrale relativi alla Home Automation

7. GESTIONE RETE

Nei sottomenu del menu **Gestione Rete** è possibile configurare le connessioni di rete.

7.1. GSM

In questo menu è possibile controllare lo stato del GSM e configurare le impostazioni della rete 4G.

The screenshot shows the ELKRON EGO N web interface. On the left is a sidebar menu with options like 'Accesso', 'Home Page', 'Storico Eventi', 'Report Eventi', 'Impostazioni Centrale', 'Dati Utente', 'Cattura Eventi', 'Trasmissione Eventi', 'Storico Dispositivi HA', 'Gestione Dispositivi', 'Apprendimento', 'Walk Test', 'Controllo Attuatori', 'Dispositivi Video', 'Gestione Sirene', 'Gestione Rete', 'LAN', 'Wireless', and 'Gestione Sistema'. The 'Gestione Rete' menu item is highlighted with a red box. The main content area is divided into two sections: 'GSM' and '4G'. The 'GSM' section shows the status: 'Stato: Inserisci SIM, IMEI: 867962049753315, IMSI: ...'. Below this is the 'Limitazione di Connessione' section with a dropdown menu set to '1 hr' and buttons for 'OK' and 'Reset'. The '4G' section has input fields for 'APN', 'Utente', and 'Password', with 'OK' and 'Reset' buttons below them. At the bottom of the 4G section are links for 'Invio SMS...' and 'GSM Reset'.

- **Stato:** in questo campo viene visualizzato lo stato del modulo 4G (presenza SIM e copertura del campo).
- **IMEI:** in questo campo viene visualizzato il codice IMEI del modulo 4G.
- **Limitazione di Connessione:** nel caso in cui la rete IP LAN o WiFi risulti disconnessa e la centrale sia connessa solo in 4G, è possibile stabilire per quanto tempo la connessione rimanga in 4G prima di riprovare a connettersi in LAN o WiFi. Cliccare sul pulsante **“OK”** per aggiornare l'impostazione inserita
NOTA BENE: il valore **“Nessun limite”** va usato solo se l'unica connessione disponibile è la 4G (no LAN e no WiFi).
- **4G:** al fine di poter utilizzare la connessione 4G come connessione di back-up, è necessario programmare questa sezione per garantire le comunicazioni con i dispositivi remoti.

☞ **Nome APN (punto di accesso).** Il nome di un punto di accesso per il GPRS. Il nome APN deve essere richiesto al fornitore del servizio telefonico. Si citano gli APN degli operatori più comuni:

- **TIM:** wap.tim.it
- **Vodafone:** mobile.vodafone.it; web.omnitel.it; m2m.vodafone.bis
- **Vodafone HO:** web.ho-mobile.it
- **Wind:** internet.wind; internet.wind.biz
- **Fastweb:** apn.fastweb.it

Una volta impostato il nome APN, il sistema può connettersi a Internet.

☞ **Utente:** Il nome di accesso da inserire prima di accedere alle funzionalità 4G. Questa informazione, se necessaria, deve essere richiesta al fornitore del servizio telefonico.

☞ **Password:** La password dell'utente da inserire prima di accedere alle funzionalità 4G. Questa informazione, se necessaria, deve essere richiesta al fornitore del servizio telefonico.

- **Invio SMS:** il comando permette di inviare un SMS di prova.

Dopo avere inserito tutte le informazioni, cliccare sul pulsante **“OK”** per aggiornare le impostazioni inserite.

- **Reset GSM.** Questo pulsante serve a resettare il modulo 4G presente nella centrale.

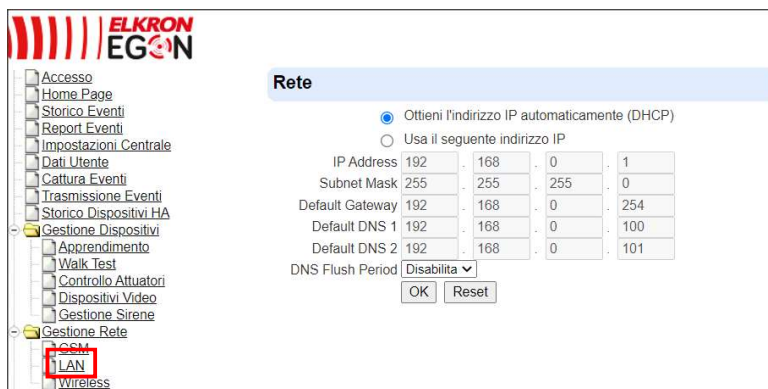
<NOTE>

1. Eliminare la richiesta del Codice PIN dalla SIM card (servirsi di un telefono cellulare).
2. Utilizzare SIM card con attivazione dati e fonia, verificandone la data di scadenza.

3. Dal momento che si tratta di un impianto di sicurezza, per la SIM card si consiglia di utilizzare un contratto in abbonamento che non corra il rischio di rimanere senza credito residuo
4. Nel caso vengano utilizzate SIM card prepagate, controllare periodicamente che la SIM abbia un buon margine di credito per assicurare l'operabilità del modulo GSM.
5. Si consiglia di attivare una SIM card prepagata o a contratto che preveda un traffico dati non inferiore a 100MB/mese. I consumi medi per connessioni ADSL e 4G sono i seguenti:
 - 50MB/mese per una connessione al Server "Always ON" (24 ore al giorno per ogni giorno del mese)
 - 90-140KB per ogni video
 - 25KB per ogni foto alla massima risoluzione

La ELKRON declina ogni responsabilità relativa alla non disponibilità, temporanea o permanente, della rete trasmissiva cellulare GSM che possa condizionare l'invio delle informazioni programmate.

7.2. LAN



In questo menu è possibile configurare i parametri della connessione LAN

● DHCP:

☞ **On.** se DHCP è impostato su On, la centrale ottiene automaticamente l'indirizzo IP dal server DHCP di rete. Pertanto, non occorre effettuare alcuna impostazione..

☞ **Off:** Se DHCP è impostato su Off, si devono inserire manualmente le informazioni per Indirizzo IP, Subnet mask, Gateway, DNS. Verificare preventivamente di essere in possesso di tutti i dati necessari relativi al proprio ambiente di rete. Per ulteriori informazioni, rivolgersi al gestore della rete locale.

7.3. WiFi

In questo menu è possibile configurare i parametri della connessione WiFi al Router

Programmazione WiFi

Rilevazione assenza:

SSID:

Autenticazione:

Password:

Encryption:

Stato: Disconnesso , Segnale: 0

☒ Ottieni l'indirizzo IP automaticamente (DHCP)

☐ Usa il seguente indirizzo IP

Indirizzo IP:

Subnet Mask:

Default Gateway:

Default DNS 1:

Default DNS 2:

- **Rilevazione assenza:** se si desidera che un'eventuale disconnessione del WiFi venga segnalata negli stati ed eventi del sistema, Selezionare “**Abilita**”
- **SSID:** nome della rete selezionata
- **Autenticazione:** metodo di autenticazione utilizzato per la connessione al router
- **Password:** password del router
- **Encryption:** tipo di crittografia utilizzato dal router

Premere sul tasto “**Scan WiFi AP**” per cercare la rete **WiFi** alla quale ci si vuole connettere. Dalla lista delle reti **WiFi** disponibili (vedere sotto un esempio), selezionare la rete che interessa premendo il tasto “**Setta**” al fondo della riga. Cliccando sul tasto “**X**” di WiFi Aps si cancella la tabella delle reti WiFi.

WiFi Aps	SSID	MAC	Autenticazione	Encryption	Livello Segnale	Canale	
	CasaPerra 2	f8:44:e3:d6:b1:a9	WPA2PSK	TKIP	100	1	Setta
	ALHN-5140-EXT	4c:6e:6e:52:f1:4f	WPA2PSK	AES	100	11	Setta
	ALHN-5140	68:d4:82:87:94:99	WPA2PSK	TKIP	74	11	Setta
	FASTWEB-86AA0C	a4:91:b1:86:aa:0c	WPA2PSK	AES	70	1	Setta
	FASTWEB-GNC1KC	e8:d1:1b:c3:3a:6d	WPA2PSK	AES	62	1	Setta

Premere il tasto “**OK**” per confermare i dati inseriti. Dopo aver aggiornato la pagina del browser, l'avvenuta connessione potrà essere verificata sulla riga **Stato**.

In alternativa è possibile inserire i dati manualmente utilizzando l'indirizzamento con IP statico.

Una volta configurata la connessione, per utilizzare la connessione wireless rimuovere il cavo di rete l'alimentazione dalla centrale. Rialimentare e verificare lo stato di connessione (terzo LED verde) dopo circa un minuto.

La stessa procedura deve essere utilizzata nel caso che il router WiFi venga sostituito da un altro dispositivo.

Se invece si preferisce instaurare nuovamente una connessione via cavo, disalimentare, collegare il cavo di rete e rialimentare.

ATTENZIONE: utilizzare sempre e solo un tipo di connessione, o con cavo o con WiFi

8. GESTIONE SISTEMA

Nei sottomenu del menu **Gestione Sistema** è possibile configurare i parametri di sistema.

8.1. Cambio Password

In questo menu è possibile specificare nome utente e password per accedere al Pannello di controllo della centrale.

☞ **Nome Utente:** è il nome utente da utilizzare quando si accede al Pannello di controllo locale. Il nome predefinito è “admin”. Se si desidera modificare il nome utente, inserire un nuovo nome nel campo. Il numero massimo di caratteri è 20.

☞ **Nuova Password:** se si desidera modificare la password, inserire in questo campo la nuova password. Il numero massimo di caratteri è 20.

☞ **Ripeti Password:** digitare di nuovo la password in questo campo.

8.2. Home Automation

Vedere Guida dedicata.

8.3. Scenari

Vedere Guida dedicata.

8.4. Report

In questo menu è possibile impostare la destinazione della reportistica. Sono disponibili fino a 8 destinazioni per la trasmissione delle informazioni.



● Tipo di report:

La centrale CR600WF supporta i seguenti tipi di report:

☞ **Report IP/GPRS in formato CID/SIA DC09:**

Formato di destinazione del report: ip://account@xxx.xxx.xxx.xxx:port/CID_SIA/SES

Per esempio: ip://account@59.124.123.22:8765/CID_SIA/SES

ip://	6543	59.124.123.23	:8765	/CID_SIA
Tipo di report	Account	Indirizzo IP del server	Numero di porta	Formato del report

☞ **Report IP/GPRS in formato CID:**

Formato di destinazione del report: ip://Account@Server IP:Porta/CID

Per esempio: ip://6543@59.124.123.22:8765/CID

ip://	6543	@59.124.123.23	:8765	/CID
Tipo di report	Account (4-8 cifre)	Indirizzo IP del server	Numero di porta	Formato del report

☞ **Report IP/GPRS in formato SIA:**

Formato di destinazione del report: ip://Account@Server IP:Porta/SIA

Per esempio: ip://6543@59.124.123.22:8765/SIA

ip://	6543	@59.124.123.23	:8765	/SIA
Tipo di report	Account (4-8 cifre)	Indirizzo IP del server	Numero di porta	Formato del report

☞ Report Chiamata Voce:

Formato di destinazione del report: voce://Numero tel.

Per esempio: voce://00391234567890

voce://	0039	1234567890
Tipo di report	Prefisso internazionale	Numero di telefono

<Note>

☞ L'indirizzo 1 viene configurato automaticamente alla prima connessione con il Server

ATTENZIONE! I parametri dell'intera riga non vanno mai modificati!

Nel caso di interventi di manutenzione o di modifica accidentale di questo parametro, occorre utilizzare la procedura di Invio Configurazione dal Portale Egon (si veda la Guida dedicata).

☞ Il tipo di report deve essere inserito in lettere minuscole

☞ I cambi di stato non possono essere comunicati tramite Chiamate Voce

☞ L'invio delle e-mail può essere impostato solo sul Portale o sull'APP

● Filtro:

Tramite la selezione del filtro, è possibile definire segnalazioni di eventi differenti:

☞ Tutti gli eventi: la centrale segnala ai destinatari del report gli eventi relativi ad allarmi, anomalie e cambi di stato del sistema.

☞ Eventi di allarme e cambi di stato: la centrale segnala ai destinatari del report gli eventi relativi agli allarmi e ai cambi di stato.

☞ Eventi di allarme senza cambi di stato: la centrale segnala ai destinatari del report solo gli eventi relativi agli allarmi.

☞ Eventi di stato: La centrale segnala ai destinatari del report solo gli eventi relativi ai cambi di stato. Si sconsiglia l'uso di questo filtro, soprattutto sull'indirizzo 1, perchè inibisce la segnalazione degli allarmi ai dispositivi remoti.

NOTA: la gestione della reportistica tramite Notifiche su telefono cellulare può essere definita indipendentemente sulle APP

● Gruppo:

È possibile assegnare le destinazioni dei report a diversi gruppi. I gruppi di report operano secondo le seguenti regole:

☞ La priorità di invio dei report viene definita dal numero assegnato al Gruppo. Il Gruppo 1 è prioritario rispetto ai numeri successivi. Da Gruppo 1 → Gruppo 2 → Gruppo 3 →ecc.

☞ Se a un gruppo sono assegnate più destinazioni di report, quando un report viene inviato con successo a una delle destinazioni, il sistema arresta l'invio del report alle restanti destinazioni del gruppo e passa al report per il gruppo successivo.

Se la centrale non riesce a inviare il report alla prima destinazione di un gruppo, passa alla destinazione successiva. Se non riesce a inviare il report ad alcuna destinazione del gruppo, la centrale riprova l'invio per 2 volte prima di passare al gruppo successivo.

Se non riesce a inviare il report ad alcun gruppo, la centrale ricomincia l'invio del report dal Gruppo 1 finché almeno un gruppo non riceva il report.

◆ Per i report "VOCE", se la chiamata non riesce, la centrale ricompile ciascun numero di telefono per 3 volte, fino a un massimo di 9 tentativi totali.

☞ Esempio. Per ricevere sia le notifiche su cellulare (relative sempre al Report di riga 1) che le chiamate vocali telefoniche in caso di allarme, utilizzare due gruppi distinti, uno per ogni tipo di segnalazione. Se invece si desidera ricevere un solo tipo di segnalazione, utilizzare lo stesso numero di gruppo per chiamate vocali e notifiche. In quest'ultimo caso la chiamata vocale sarà ricevuta solo se la notifica su cellulare non sarà andata a buon fine.

ESEMPI

Esempio	Configurazione	Comportamento
A	1) Notifica IP -> Gruppo 1 2) Invio Chiamata -> Gruppo 1	La centrale invierà soltanto una notifica su smartphone se questa sarà correttamente ricevuta. Invierà invece la chiamata vocale se la notifica non sarà ricevuta (per es. per mancanza di rete dati presso la centrale o lo smartphone).
B	1) Notifica IP -> Gruppo 1 2) Invio Chiamata -> Gruppo 2	La centrale invierà sempre sia notifica che chiamata vocale telefonica.
C	1) Notifica IP -> Gruppo 1 2) Invio Chiamata -> Gruppo 2 3) Invio Report digitale -> Gruppo 2	La centrale invierà sempre sia notifica che chiamata telefonica. Se la chiamata telefonica non andrà a buon fine, invierà anche un segnalazione tramite protocollo digitale (per es. a una Centrale di Sorveglianza)
D	1) Notifica IP -> Gruppo 1 2) Invio Report digitale -> Gruppo 2 3) Invio chiamata telefonica -> Gruppo 2	La centrale invierà sempre sia notifica che il Report digitale. Se il Report digitale non andrà a buon fine, invierà anche una chiamata telefonica.

<NOTA>

La destinazione di invio della reportistica relativa alle telecamere IP TEL600 deve essere programmata sulla interfaccia locale della telecamera stessa (fare riferimento al suo manuale).

● Essenziale/Opzionale

Essenziale: la centrale invierà le segnalazioni a tutti i gruppi configurati come “**Essenziali**”. La centrale continuerà a provare l’invio delle segnalazioni sino a che almeno una di esse sia andata a buon fine. Il Gruppo 1 è sempre Essenziale.

Opzionali: la centrale invierà le segnalazioni al gruppo configurato come “**Opzionale**” solo se le segnalazioni del gruppo precedente non saranno andate a buon fine. Per esempio: se il Gruppo 3 è Opzionale, la centrale invierà le segnalazioni di questo gruppo solo se quelle del Gruppo 2 non saranno andate a buon fine.

● 1 Retry/ 3 Retry/ 5 Retry/ 10 Retry/ 99 Retry:

Se le segnalazioni di un Gruppo non vanno a buon fine, la centrale ritenterà la trasmissione per il numero di volte definito con questo parametro.

8.5. Report SMS

In questo menu è possibile impostare l'uso degli SMS inviati dalla centrale.

Report SMS	
Indirizzo Report	Filtro
1	Tutti gli eventi
2	Tutti gli eventi
3	Tutti gli eventi
4	Tutti gli eventi
5	Tutti gli eventi

Note: 1. SMS in formato CID, es: sms://account@n.telefono
2. SMS in formato testo, es: sms://n.telefono/TEXT

OK Reset

☞ Report SMS in formato Testo (solo se la centrale dispone di scheda SIM):

Formato di destinazione del report: sms://numero di cellulare/TEXT

Per esempio: sms://00393476064587/TEXT

0sms://	00393476064587	/TEXT
Tipo di report	Numero di cellulare	Formato del report

<NOTA>

Se gli SMS vengono definiti in questo menu, saranno sempre inviati.

Nel caso si voglia gestire le priorità dei messaggi SMS con i criteri dei Gruppi definiti nel menu precedente, inserire la stessa stringa definita per questo menu nelle righe dei Report della tabella del menu precedente invece che in questo menu.

8.6. Upload Video

Questo menu consente di impostare la destinazione di invio di immagini/video acquisiti dai rivelatori con fotocamera o videocamera.

Server Upload Foto/Video

URL 1:

URL 2:

URL 3:

URL 4:

URL 5:

Prefix:

☐ Cancella gli eventi dopo averli inviati

Note: 1. IP (Ethernet o 4G) in protocollo FTP, es: ftp://user:password@server/path
2. IP (Ethernet o 4G) in protocollo HTTP, es: http://server/path
3.
4.

OK Reset

- **Indirizzo 1:** indirizzo configurato automaticamente alla prima connessione con il Server.

ATTENZIONE! Questo parametro non va mai modificato!

Nel caso di interventi di manutenzione o di modifica accidentale di questo parametro, reinserire il seguente:

Indirizzo 1: http://www.egon.elkron.com:8080/up-post.php

- **Indirizzi 2~5:** inserire indirizzi FTP.

☞ Formato FTP: **Errore. Riferimento a collegamento ipertestuale non valido.**

- **Prefix:** identificativo di accesso della centrale

<NOTA>

La destinazione di invio di immagini/video acquisiti dalle telecamere IP TEL600 deve essere programmata sulla interfaccia locale della telecamera stessa (fare riferimento al suo manuale).

8.7. XMPP

Questo menu riporta dati che non sono destinati all'utente ma al servizio di assistenza e potranno essere richiesti per eseguire delle diagnosi sull'impianto

ATTENZIONE! Questi parametri non vanno mai modificati!

Nel caso di interventi di manutenzione o di modifica accidentale di questi parametri, reinserire i seguenti:

- **XMPP:** xmpp://www.egon.elkron.com:5222
- **Dominio:** elkron-home-portal
- **Amministrazione:** security_admin

8.8. Data & Ora

Questo menu consente di impostare data e ora a bordo della centrale.

The screenshot shows the 'Data & Ora' configuration page. On the left is a sidebar menu with items like 'Accesso', 'Home Page', 'Storico Eventi', 'Report Eventi', 'Impostazioni Centrale', 'Dati Utente', 'Cattura Eventi', 'Trasmissione Eventi', 'Storico Dispositivi HA', 'Gestione Dispositivi', 'Gestione Rete', 'Gestione Sistema', 'Cambio Password', 'Home Automation', 'Scenari', 'Report', 'Report SMS', 'Upload Video', 'XMPP', 'Data & Ora' (highlighted), and 'Firmware'. The main area contains three sections: 'Data & Ora' with 'Data' set to 2022/01/14 and 'Ora' set to 15:53, both with 'OK' and 'Reset' buttons; 'Fuso Orario' with a dropdown menu showing '(GMT+01:00) Brussels, Copenhagen, Madrid, Paris' and 'OK'/'Reset' buttons; and 'Orologio Universale' with a checkbox for 'Sincronizza automaticamente con orologio universale su Server NTP' and a 'Server' dropdown set to 'pool.ntp.org' with 'OK'/'Reset' buttons.

- **Data & Ora:** consente di impostare data e ora correnti.
- **Fuso Orario:** consente di impostare il fuso orario locale.
- **Orologio Universale:** selezionando la sincronizzazione automatica, la centrale sincronizzerà il proprio orologio interno con il servizio offerto da Internet tramite un Server NTP, selezionabile. Si consiglia di non variare questo parametro.

8.9. Firmware & Firmware RF

In questi menu è possibile aggiornare i firmware della centrale per la gestione dei dati e dei dispositivi RF.



Fase 1. Selezionare il file del firmware nel computer.

Fase 2. Cliccare su “**Applica**” per caricare il file del firmware sulla centrale.

Fase 3. Servono pochi minuti per completare il caricamento: **NON** spegnere la centrale durante l’operazione. Nella fase di aggiornamento, sulla centrale si accendono contemporaneamente i 3 led e al termine dell’aggiornamento la centrale emette 2 bip sonori e torna nel suo stato originale

Fase 4. Terminata l’operazione, cliccare sul pulsante di “Accesso” e verificare la presenza della nuova versione FW.

8.10. Reset di Fabbrica

Questo menu consente di cancellare tutte le informazioni e le impostazioni memorizzate nella centrale e riportare le impostazioni ai valori di fabbrica. Una volta eseguito, al termine del tempo alla rovescia, attendere il riavvio della centrale per circa 30 secondi.



È possibile:

- non variare i parametri di rete selezionando le casella “**Mantenere impostazioni di rete**”
- non perdere la configurazione dei dispositivi già appresi selezionando le casella “**Mantenere impostazioni dispositivo**”.

<NOTA>

Per il reset di fabbrica è anche possibile utilizzare il pulsante all'interno della centrale, che cancellerà anche le impostazioni di rete e dei dispositivi.

NOTA BENE! *A differenza del reset effettuato da menu, questo reset effettuato tramite pulsante reinizializza la centrale con un indirizzo IP di tipo STATICO.*

Per effettuare il reset procedere nel seguente modo:

- disconnettere l'alimentazione di rete e spostare l'interruttore della batteria su OFF.
- mantenendo premuto il pulsante di Apprendimento/Reset, riconnettere l'alimentazione di rete tenendo premuto il pulsante fino a quando i tre led lampeggeranno contemporaneamente; a questo punto i tre led si spegneranno.
- a questo punto è possibile rilasciare il pulsante e spostare nuovamente l'interruttore della batteria su ON. Attendere il riavvio della centrale per circa 30 secondi.

ATTENZIONE! *Dopo aver effettuato il reset di fabbrica, la centrale non è più in grado di gestire l'upload e i report, in quanto viene cancellato anche l'indirizzo del server. È indispensabile ripristinarlo e riattivare queste funzionalità. Per far ciò si utilizza la procedura di Invio Configurazione dal Portale Egon (si veda la Guida dedicata).*

8.11. Backup & Ripristina

Questo menu permette di eseguire il salvataggio e il ripristino dei dati di configurazione della centrale. Questa operazione deve essere eseguita dopo aver consultato il servizio di assistenza.

8.12. Log Sistema

Questo menu riporta dati che non sono destinati all'utente ma al servizio di assistenza e potranno essere richiesti per eseguire delle diagnosi sull'impianto

9. CARATTERISTICHE TECNICHE DELLA CENTRALE

Prestazioni principali:

- Comunicazioni bidirezionali in radiofrequenza con tutti i dispositivi
- Connessione in radiofrequenza fino a 80 dispositivi
- Connessione fino a 6 rivelatori IR con fotocamera o videocamera per la video-verifica degli allarmi
- Connessione fino a 4 telecamere IP
- Gestione 3 zone di parzializzazione + totale
- Massimo 20 utenti configurabili (codici e telecomandi)
- Massimo 20 codici di attivazione/disattivazione/parzializzazione configurabili
- Capacità di memorizzare fino a 200 eventi
- Registrazione di 3 o 6 foto e 10 secondi di video ad ogni allarme. Registrazione di 30 secondi di video nel caso della telecamera IP, con possibilità di ottenere anche la registrazione video prima dell'evento di allarme.
- Attivazioni/disattivazioni da telecomandi, tastiere, PC, Smart Phone, Contatti configurati per le attivazioni/disattivazioni e Scenari/Regole di Home Automation
- Connessione al Router tramite cavo Ethernet o WiFi (alternativi)
- Invio allarmi/immagini/video su server HTTP/FTP, email, chiamate telefoniche ed SMS (solo se la centrale dispone di scheda SIM), notifiche Push, protocolli CID e SIA
- Ascolto ambientale tramite telecamera IP
- Trasmissione allarmi tramite:
 - CID/ SIA over TCP/IP (DC09), su Ethernet o 4G (solo se la centrale dispone di scheda SIM)
 - SMS su GSM (solo se la centrale dispone di scheda SIM)
 - Video e immagini su Email/ FTP over Ethernet o 4G (solo se la centrale dispone di scheda SIM)
- Controllo remoto tramite portale WEB o APP (iOS e Android)
- Misura Presenza segnali wireless e 4G
- Supervisione di tutti i dispositivi eccetto il telecomando e la tastiera
- Rilevazione interferenze in radiofrequenza (anti Jamming)
- Sirena integrata
- Conforme alle certificazioni EN 50131 Grado 2, Classe II

Specifiche:

- GSM quad band 900/1800/850/1900 MHz
- Connessioni wireless in:
 - 4G
 - ZigBee HA 1.2
 - 868 MHz narrow band
 - WiFi
- Connessione in rete Ethernet 10/100 Mbit
- Alimentazione interna da 9V 1A
- Massimo consumo: 30 mA@ 230VAC
- Batteria interna di backup ricaricabile: 4,8V Ni-Mh, 1100 mAh
- Autonomia della batteria di backup: 15 ore medie senza Zigbee USB, 5 ore con Zigbee USB, dipendenti dal comportamento avvenuto
- Banda radiofrequenza: 868,600-868.700MHz
- Potenza radio massima trasmessa: +15dBm
- Livello sonoro della sirena interna: 95dB @ 1m
- Temperatura di funzionamento: da -10° a +45°C
- Dimensioni: 260 X 176 X 30 mm
- Peso: 600 g

10. STRUMENTI DI GESTIONE REMOTA

Il sistema Elkron EGON può essere gestito da remoto tramite smartphone e pc. Elkron mette a disposizione una App dedicata e un portale web multi-browser, entrambi accessibili con credenziali riservate scelte dall'utente.

Il portale è raggiungibile al seguente indirizzo: <https://www.egon.elkron.com/home>. La prima attività da effettuare è di **registrarsi come Nuovo Utente** (una procedura guidata indicherà le operazioni da fare).

Una volta registrati, dal portale è possibile:

- Attivare/parzializzare/disattivare l'impianto
- Visualizzare lo stato dei dispositivi presenti nel sistema
- Visualizzare gli ultimi 200 eventi, video e foto
- Configurare nuovi utenti e nuovi codici; visualizzare quelli già presenti in qualità di master
- Visualizzare le informazioni di base del sistema
- Configurare alcuni parametri dei dispositivi (tra cui l'esclusione dei rivelatori in modo permanente)
- Cambiare la password principale
- Configurare le email e le notifiche push a cui inviare i report
- Generare il codice per l'accesso all'installatore
- Visualizzare le immagini riprese dalle telecamere IP TEL600 in tempo reale

Il manuale di utilizzo del portale è disponibile nell'area riservata del sito Elkron, sezione *Prodotti e Soluzioni*.

L'App UTENTE “**Elkron Egon**” può essere installata sul proprio smartphone collegandosi all'**App Store** (per iPhone) o **Google Play** (per Android). L'Applicazione permette di:

- Attivare/parzializzare/disattivare l'impianto
- Visualizzare lo stato dei dispositivi presenti nel sistema
- Visualizzare gli ultimi 200 eventi selezionandoli per tipo
- Visualizzare le informazioni di base del sistema
- Cambiare la password principale
- Configurare le email e le notifiche push a cui inviare i report
- Configurare notifiche per le APP e le email
- Eseguire la registrazione della centrale e dell'utente associato
- Generare il codice per l'accesso all'installatore
- Visualizzare le immagini riprese dalle telecamere IP TEL600 in tempo reale
- Gestire i dispositivi della Home Automation

<NOTE IMPORTANTI>

- L'Utente deve prevedere una connessione alla rete Internet tramite modem ADSL o SIM dati compatibile con i dispositivi del sistema e avere sottoscritto un abbonamento a Internet.
- L'accesso al Portale e all'Applicazione Egon e la ricezione di notifiche e email implicano che la centrale Egon sia costantemente connessa alla rete Internet.
- L'installazione e la configurazione degli apparecchi di telecomunicazione che consentono di accedere alla rete Internet sono realizzate sotto l'esclusiva responsabilità dell'Utente.
- L'Azienda mette in guardia l'Utente contro il potenziale rischio di interruzioni della connessione Internet, tali da compromettere, in tutto o in parte, l'accesso e il funzionamento del Portale e dell'Applicazione Egon e la ricezione di notifiche e email.
- L'Azienda declina qualsiasi responsabilità in caso di malfunzionamento o impossibilità di accedere al Portale e all'Applicazione Egon e della ricezione di notifiche e email a causa di un'interruzione della connessione Internet dell'Utente.
- Non è consentita la connessione di più di una sessione alla volta, sia da App che da portale. Una connessione esclude l'altra.
- Durante le fasi di installazione o successive manutenzioni tramite il Pannello di Controllo Locale, si sconsiglia l'uso contemporaneo di App e portale per eventuali test di sistema o per interagire con il sistema. Al termine delle operazioni di installazione e manutenzione scollegare il pc locale.
- In caso di mancata ricezione delle email, verificare le cartelle spam/posta indesiderata.
- Sia il Portale che l'App, per ragioni di sicurezza, hanno un limite massimo di tempo per la durata di una sessione.
- Si consiglia di utilizzare password per portale e App di almeno 8 caratteri.
- Una manomissione tamper con il sistema attivo viene registrata nello Storico di App e portale sia come manomissione tamper che come allarme intrusione

Sul link www.elkron.it/egon.aspx è presente una sezione interamente dedicata al sistema Egon. Qui è possibile conoscere le principali funzionalità del sistema e consultare gli aggiornamenti e le notizie che Elkron periodicamente pubblica.

11. APPENDICI

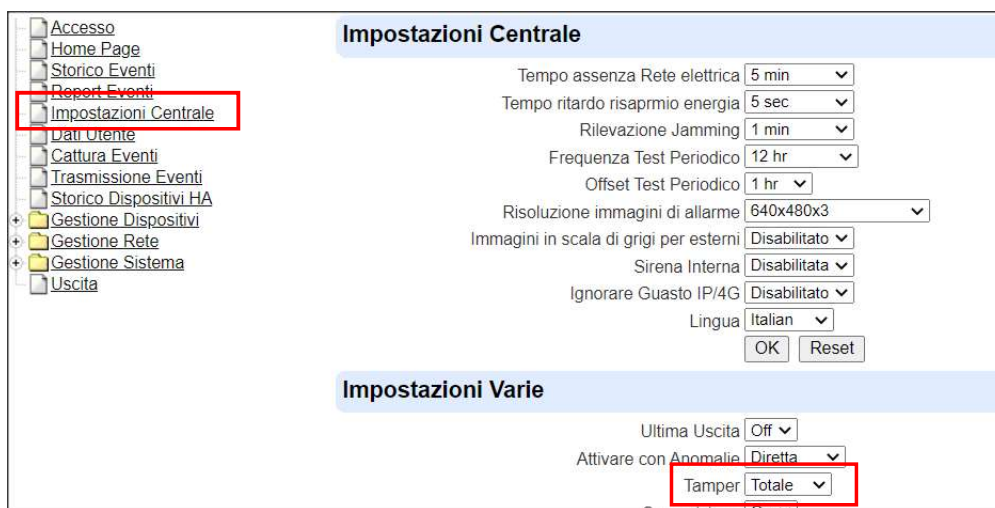
11.1. Tipologie di allarme ed eventi generati nel sistema

ALLARME INTRUSIONE	
Generato se	<ul style="list-style-type: none"> Si verifica un tentativo di intrusione
La centrale attiva	<ul style="list-style-type: none"> I dissuasori presenti nel sistema, cioè le sirene esterne e/o sirena interna alla centrale, tranne nel caso degli allarmi silenziosi per i quali si attivano solo le notifiche il pop-up "Nuovo Evento" sul portale se abilitato, l'invio di email con relativo messaggio di Allarme intrusione se abilitato, l'invio di SMS con relativo messaggio di Allarme intrusione tramite il modulo GSM/4G (solo se la centrale dispone di scheda SIM) se abilitata, la notifica con relativo messaggio di Allarme intrusione sull'APP dedicata se abilitato, l'invio di allarmi ai centri di vigilanza (CID, SIA ecc..)
L'allarme viene segnalato	<ul style="list-style-type: none"> sulla centrale tramite il lampeggio del led rosso (sistema in allarme) sulle tastiere (vedere dettagli sui relativi manuali)
L'allarme viene memorizzato	<ul style="list-style-type: none"> nella centrale, nel menu Storico nella APP utente e nel Portale, nel menu Eventi
L'allarme dura	<ul style="list-style-type: none"> per il Tempo di allarme intrusione programmato
L'allarme si interrompe con	<ul style="list-style-type: none"> l'introduzione di un codice valido sulla tastiera e il successivo comando di disattivazione l'introduzione di un codice valido su portale o APP e il successivo comando di disattivazione un comando di disattivazione da telecomando un cambio di stato dal contatto magnetico programmato come Attiva/Disattiva
Generato se	<ul style="list-style-type: none"> viene aperto un Tamper nel tentativo di manomettere un dispositivo del sistema (centrale, tastiere o dispositivi come DC, IR, Sirene). La rilevazione dipende dalla programmazione Tamper impostata nel menu "Impostazione Centrale" viene manomesso il Dongle Zigbee e nell'impianto sono presenti dispositivi Zigbee; in questo caso viene generato un allarme di sabotaggio di tipo Tamper. La rilevazione dipende dalla programmazione Tamper impostata nel menu "Impostazione Centrale".
Attiva	<ul style="list-style-type: none"> I dissuasori presenti nel sistema (sirene esterne e/o sirena interna alla centrale) il pop-up "Nuovo Evento" sul portale se abilitato, l'invio di email con relativo messaggio di Allarme Tamper se abilitato, l'invio di SMS con relativo messaggio di Allarme Tamper la notifica sull'APP dedicata con relativo messaggio di Allarme Tamper se abilitato, l'invio di allarmi ai centri di vigilanza (CID, SIA ecc..)
L'allarme viene segnalato	<ul style="list-style-type: none"> sulla centrale con il lampeggio del led rosso
L'allarme viene memorizzato	<ul style="list-style-type: none"> nel portale, nel menu Eventi nella APP utente, nel menu Eventi nella centrale, nel menu Storico, con la segnalazione di anomalia sul led giallo acceso
L'allarme dura	<ul style="list-style-type: none"> per il Tempo di allarme programmato
Si interrompe con	<ul style="list-style-type: none"> l'introduzione di un codice valido sulla tastiera e il successivo comando di disattivazione premendo il comando di disattivazione sul portale o sulla APP e digitando un codice valido il comando di disattivazione da telecomando un cambio di stato dal contatto magnetico programmato come Attiva/Disattiva

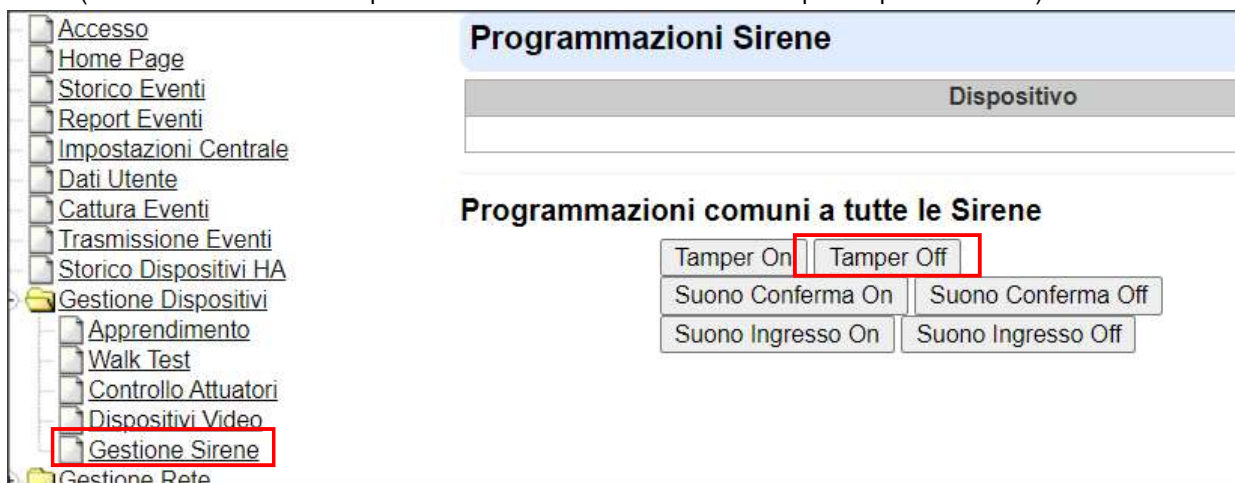
11.2. Istruzioni per sostituzione e smaltimento batterie

Procedura generale

1. Prima di sostituire le batterie di qualsiasi componente del sistema **Egon**, accertarsi che la centrale sia in stato disattivo.
2. Collegarsi al *Pannello di Controllo locale* della centrale o alla *App Installatore* per verificare la configurazione esistente ed eventualmente modificarla come descritto al punto 3 per i dispositivi e per la sirena.
3. Per i dispositivi accessori: all'interno del menu "**Impostazioni Centrale**", effettuare la selezione **Allarme Tamper** → **Totale**. In questo modo, l'apertura dei dispositivi per il cambio batterie non genererà allarme Intrusione.



Per la sirena: all'interno del menu *Dispositivi/Programmazione Sirena*, disabilitare la protezione antimanomissione della sirena, selezionando **Off** su "**Tamper Sirena**" e cliccando sul tasto per confermare la scelta (la sirena tornerà attiva dopo un'ora anche non riabilitando il Tamper in questa videata).



4. Seguire le procedure di cambio batterie per ogni singolo dispositivo e per la sirena descritte di seguito.
5. Dopo aver effettuato l'operazione di cambio batterie, verificare nella lista Eventi la chiusura del tamper

Procedura sui singoli dispositivi

Per la procedura sui singoli dispositivi, fare riferimento ai manuali a corredo di ciascun modello.



ATTENZIONE: dopo la sostituzione delle pile è necessario attendere almeno 40 minuti per assicurare l'operatività del sistema.

La durata delle batterie può risultare ridotta rispetto a quanto indicato nelle caratteristiche tecniche. I fattori che possono influenzare la durata delle batterie possono essere:

- frequenza di attivazione/disattivazione;
- frequenza di allarmi rilevati;
- difficoltà di comunicazione per scarsa portata e/o ambienti disturbati di uno o più dispositivi;
- richiesta di foto e video dai rivelatori con fotocamera e videocamera

Smaltimento delle batterie

Lo smaltimento delle batterie deve avvenire secondo la normativa vigente e servendosi di aziende di smaltimento o recupero autorizzate.

Si ricorda che le pile al litio sono a tutti gli effetti dei rifiuti speciali con codice di classificazione CER 160605 (E.W.C. 160605) e che il loro smaltimento, a fine ciclo vita, è regolamentato da precise disposizioni di legge. Questi prodotti incorporano pile al litio o ad alta capacità che, se gettate nel fuoco o inopportunamente manipolate od utilizzate possono anche causare esplosioni e/o incendi con grave pericolo per l'incolumità delle persone. Per ulteriori informazioni o chiarimenti, si prega di contattare direttamente ELKRON.

DICHIARAZIONE DI CONFORMITÀ UE SEMPLIFICATA

Il fabbricante, URMET S.p.A., dichiara che il tipo di apparecchiatura radio: CENTRALE ANTIFURTO CR600WF è conforme alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: www.elkron.com

DIRETTIVA 2012/19/UE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 4 luglio 2012 sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE).



Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

L'utente dovrà, pertanto, conferire l'apparecchiatura giunta a fine vita agli idonei centri comunali di raccolta differenziata dei rifiuti elettrotecnici ed elettronici. In alternativa alla gestione autonoma è possibile consegnare l'apparecchiatura che si desidera smaltire al rivenditore, al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente.

Presso i rivenditori di prodotti elettronici con superficie di vendita di almeno 400 m² è inoltre possibile consegnare gratuitamente, senza obbligo di acquisto, i prodotti elettronici da smaltire con dimensione massima inferiore a 25 cm.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.



ELKRON

Tel. +39 011.3986711 - Fax +39 011.3986703
www.elkron.com – mail to: info@elkron.it

ELKRON è un marchio commerciale di **URMET S.p.A.**

Via Bologna 188/C – 10154 Torino (TO) Italia
www.elkron.com