I GB

IT500 Web Server

Manuale Utente
User Manual

ELKRON

Sul sito www.elkron.com potrebbero essere disponibili eventuali aggiornamenti della documentazione fornita a corredo del prodotto.

On the website www.elkron.com, you may find updated information relating to the documentation provided with the product.

DS80IT27-002C **LBT80826**

Le informazioni contenute in questo documento sono state raccolte e controllate con cura, tuttavia la società non può essere ritenuta responsabile per eventuali errori od omissioni.
La società si riserva il diritto di apportare in qualsiasi momento e senza preavviso miglioramenti o modifiche ai prodotti descritti nel manuale.

È inoltre possibile che questo manuale contenga riferimenti o informazioni di prodotti (hardware o software) o servizi non ancora commercializzati. Tali riferimenti o informazioni non significano in nessun modo che la società intenda commercializzare tali prodotti o servizi.

Elkron è un marchio commerciale di URMET S.p.A.
Tutti i marchi citati nel documento appartengono ai rispettivi proprietari.

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

The information contained in this manual was gathered and checked with care but the manufacturer cannot be held liable for errors or omissions.
The manufacturer reserves the right to implement improvements or changes to the products described in this manual without prior notice.

This manual may contain references or information on products (hardware or software) or services which are not yet on the market. These references and information do not imply that the manufacturer will market such products or services in the future.

Elkron is a trademark of URMET S.p.A.
All trademarks mentioned in this document are the property of their respective owners.

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

ITALIANO

Indice (V2.0.0-11)

Browser compatibili

Il Web Server è compatibile coi seguenti browser:

- **Google Chrome**, dalla versione 36.0.1985.125 m
- **Firefox**, dalla versione 30
- **Microsoft IE**, dalla versione 9
- **Safari**, dalla versione 5.1.7

Primo accesso

ATTENZIONE! Se nel sistema ci sono settori configurati con il blocco attivazione non è possibile effettuare il login e appare il messaggio “C’è almeno un settore in blocco attivazione; controllare la configurazione”.

Per accedere per la prima volta al Web Server utilizzare le credenziali di accesso predefinite (username = **admin**, password = **WebServer1**) con la procedura di Accesso.

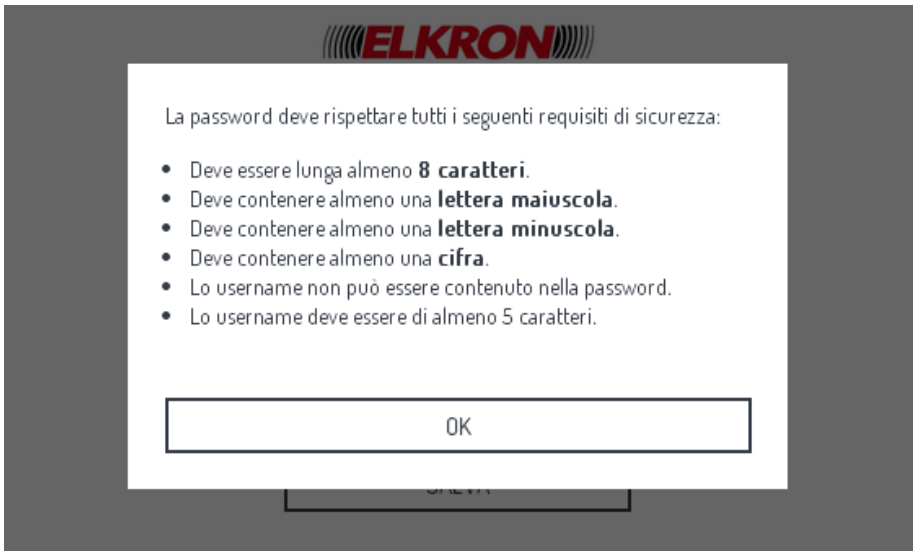
Appena effettuato l’accesso è obbligatorio cambiare username e password.
Se non si modificano le credenziali di accesso non sarà possibile interagire sul sistema di allarme tramite Web Server.

Dopo aver effettuato il login, appare un pop-up che chiede di modificare le credenziali di accesso.

Premere il pulsante **PROCEDI** per modificare le credenziali.
Si apre la pagina per inserire i nuovi dati.

Username e password devono rispettare determinate Caratteristiche obbligatorie di username e password.

Premendo il pulsante [i] un pop-up mostra i requisiti di sicurezza della password.



Dopo la modifica, le credenziali di accesso di fabbrica non saranno più valide.

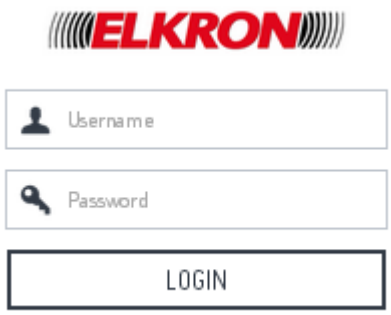
Se successivamente si cerca di effettuare il login con le credenziali di accesso di fabbrica si viene sempre riportati alla pagina di login e viene visualizzato il messaggio “Autenticazione fallita”.

Accesso

ATTENZIONE! Se nel sistema ci sono settori configurati con il blocco attivazione non è possibile effettuare il login e appare il messaggio “C’è almeno un settore in blocco attivazione; controllare la configurazione”.

Per accedere al sistema di allarme tramite Web Server fare quanto segue:

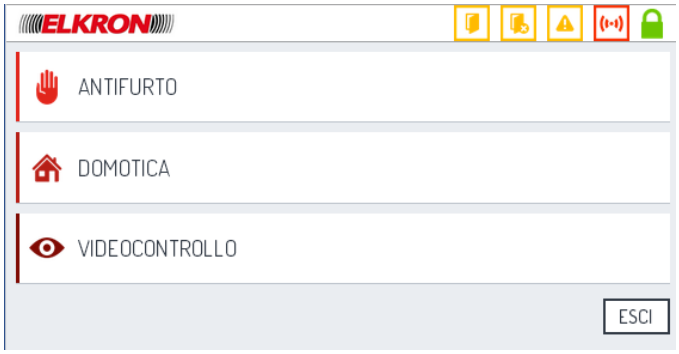
1. Collegarsi tramite computer, tablet o Smartphone all’indirizzo internet fornito dal tecnico. Viene creata una rete VPN e appare la schermata di login.



2. Inserire le credenziali di accesso (Username e Password). Le credenziali sono memorizzate localmente nel Web Server e sono univoche per tutti gli utenti del Web Server.
   ATTENZIONE! Non è possibile avere più accessi contemporanei. Se qualcuno ha già effettuato un accesso, indipendentemente dal dispositivo utilizzato (smartphone, tablet, PC), non sarà possibile accedere al Web Server fino all’uscita o alla scadenza della sessione attiva.
3. Premere il pulsante **LOGIN**.
4. Se il Web Server riconosce come valide le credenziali di accesso appare la Homepage.

Se le credenziali di accesso sono errate riappare la schermata di login e viene mostrato un messaggio di errore sulle credenziali inserite.

Homepage



Per accedere alla HOMEPAGE (Accedi) occorre autenticarsi con delle credenziali di accesso corrette. La Homepage è la pagina principale da cui si può accedere alle sezioni di gestione del sistema:

- **ANTIFURTO**, che consente di attivare e disattivare il sistema di allarme, verificare il suo stato, abilitare e disabilitare utenti ed effettuare configurazioni.
- **DOMOTICA**, che consente di attivare le uscite domotiche presenti sulla centrale antintrusione, eseguire degli scenari che attivino o sollecitino le uscite configurate.
- **VIDEOCONTROLLO**, che consente di interagire con l'eventuale sistema di videosorveglianza installato.

Inoltre nella HOMEPAGE viene visualizzato in forma sintetica, tramite icone, lo stato del sistema. Le icone appaiono solo quando c'è qualcosa da segnalare.

	Sistema allarme antintrusione attivo. Appare quando l'intero sistema di allarme antintrusione è attivo.
	Settori attivi. Appare quando uno o più settori, ma non l'intero sistema di allarme antintrusione, sono attivi.
	Ingresso isolato. Appare quando c'è almeno un ingresso isolato. Facendo clic sull'icona appare l'elenco di tutti gli ingressi isolati. L'icona di segnalazione sparisce appena non ci sono più ingressi isolati.
	Ingresso aperto. Appare quando c'è almeno un ingresso aperto. Facendo clic sull'icona appare l'elenco di tutti gli ingressi aperti. L'icona di segnalazione sparisce appena non ci sono più ingressi aperti.
	Allarme o manomissione. Appare quando c'è stato, o è in corso, almeno un allarme o una manomissione. Facendo clic sull'icona appare l'elenco di tutti gli allarmi e manomissioni memorizzati. Per far sparire l'icona, occorre effettuare la cancellazione della memoria allarmi tramite web server o tastiera, mentre, se sono presenti delle manomissioni, solo da tastiera e solo dal Tecnico o Responsabile tecnico. *ATTENZIONE*! Se non sono state eliminate tutte le cause di allarme l'icona di segnalazione continua ad essere presente.
	Anomalia o guasto. Appare quando nel sistema è stata rivelata un'anomalia o un guasto. Facendo clic sull'icona appare l'elenco di tutte le anomalie e i guasti memorizzati. Per far sparire l'icona di segnalazione occorre effettuare la cancellazione delle memorie guasti, tramite web server o tastiera. Alcune memorie guasti devono essere cancellate solo dal Tecnico o Responsabile tecnico da tastiera.

Premendo il pulsante **ESCI** ci si disconnette dal sistema e si torna alla schermata di login.

Per riaprire la **HOMEPAGE** occorrerà effettuare un nuovo accesso.

Antifurto

Alla sezione ANTIFURTO si accede dalla Homepage. Per espandere la sezione fare clic su ANTIFURTO.

La sezione è divisa in tre parti:

- Accedi, che consente di autenticarsi e accedere alla pagina di Gestione del sistema di allarme per attivare e disattivare il sistema di allarme intrusione e di esaminare i dettagli di eventuali segnalazioni (allarme, manomissione o guasto) degli ingressi.
- Stato, che consente di esaminare lo stato dell'intero sistema.
- Comandi rapidi, che consente di attivare e disattivare l'intero sistema di allarme intrusione, con un solo comando, o di eseguire due comandi rapidi programmati.

Le icone in alto mostrano, in forma sintetica, lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Facendo nuovamente clic su ANTIFURTO si richiude la sezione.

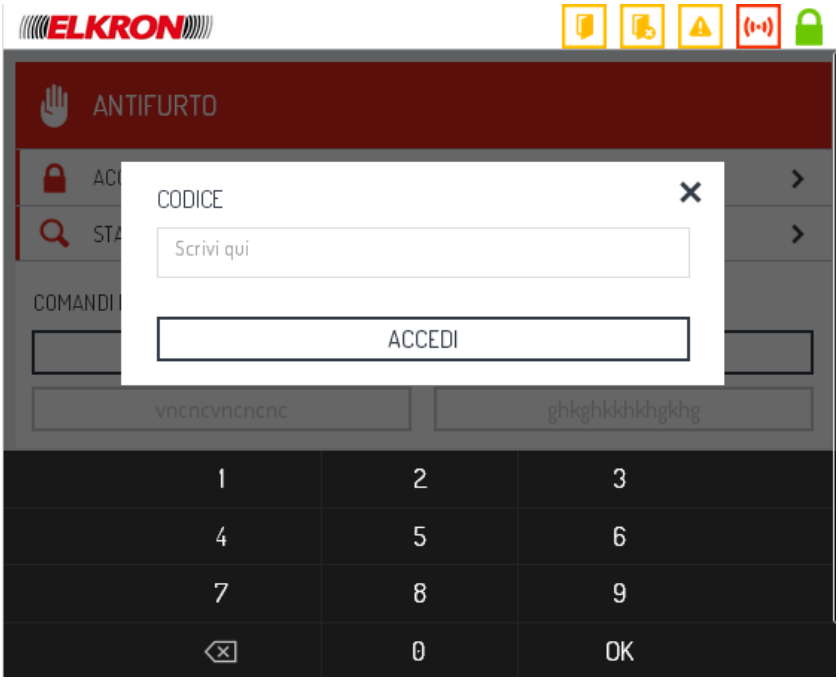
Accedi

Alla procedura ACCEDI si entra dalla sezione Antifurto.

Attraverso questa procedura è possibile accedere direttamente alla centrale antintrusione, se l'accesso non è ancora stato effettuato dalla sezione Domotica.

Autenticazione dell'accesso

Quando si entra alla procedura ACCEDI appare un pop-up per autenticarsi, se l'accesso non è ancora stato effettuato dalla sezione Domotica.



Digitare un codice di accesso valido e premere il pulsante **ACCEDI**. Il codice di accesso è il codice numerico a 6 cifre usato per accedere al sistema d'allarme tramite le tastiere fisiche, non la password usata per accedere al Web Server. *ATTENZIONE!* Se i codici di accesso configurati in centrale sono lunghi meno di 6 cifre occorre prima riconfigurarli a 6 cifre per poter accedere alla centrale tramite Web Server.

Il tasto ⌫ cancella solo l'ultima cifra inserita e il tasto **OK** equivale al tasto ACCEDI, inviando il codice inserito alla centrale per la validazione.
Le operazioni che si possono compiere dopo l'accesso al sistema dipendono dai privilegi posseduti dal codice di accesso inserito.

Per chiudere la finestra di pop-up, senza tentare di accedere al sistema, fare clic fuori dalla tastiera virtuale e dal pop-up oppure premere l'icona **X** del pop-up. Così facendo, anche se è stato inserito un codice, esso viene scartato e non controllato, non modificando pertanto il contatore dei tentativi di accesso errati.

Se il codice inserito è corretto appare la pagina di gestione (Gestione del sistema di allarme) del sistema di allarme antintrusione.

Se il codice inserito è errato, o non si è inserito nessun codice prima di premere il pulsante **ACCEDI**, viene visualizzato un messaggio di errore. Il contatore dei tentativi di accesso errati viene incrementato di 1.

Il numero massimo di tentativi di accesso errati è 21 (il limite è definito dalla centrale antintrusione e non è modificabile). Se viene inserito per più di 21 volte consecutive un codice di accesso errato, la centrale genera un allarme "falso codice".

Gestione del sistema di allarme

Alla pagina di gestione del sistema di allarme si accede dalla procedura Accedi.
Questa pagina consente di accedere alle funzioni per gestire il sistema di allarme antintrusione.

La pagina mostra:

- **Nome e stato delle aree** (nell'immagine di esempio sono CASA e BOX). L'icona indica che l'area è parzialmente attiva, l'icona che è totalmente attiva. Se non c'è nessuna icona vuol dire che l'area non è attiva. Il nome dell'area è quello che è stato configurato nella centrale.
- **Nome e stato dei settori**. L'elenco viene espanso o ridotto facendo clic sul nome dell'area di appartenenza o sul raggruppamento Settori.
  Accanto al nome del settore appaiono le icone di allarme intrusione o manomissione ( ), ingresso aperto ( ), ingresso isolato ( ).
  Se le icone sono grigie significa che non ci sono, ripettivamente, allarmi, ingressi aperti o ingressi isolati.
  Se la relativa icona è accesa (colorata) significa che è in corso o c'è stato un allarme, che uno o più ingressi sono aperti, che uno o più ingressi sono isolati. Facendo clic su di essa, il settore si espande e mostra l'elenco degli Ingressi associati al settore che hanno causato la o le segnalazioni.
  Se tutte le icone sono grige il settore non si espande.
- Lo stato del sistema, attraverso le icone in alto. Il loro significato e comportamento è uguale a quelle della Homepage.

L'icona consente di accedere alla pagina Impostazioni in cui è possibile configurare diverse funzioni e parametri del sistema. L'icona è attiva solo se il sistema di allarme è completamente disattivato.

Per attivare o disattivare aree o settori selezionare le aree o settori interessati facendo clic sul riquadro di selezione e premere il pulsante **DISATTIVA** o **ATTIVA** secondo necessità. L'azione scelta verrà effettuata solo sulle aree o settori selezionati.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Attivazione del sistema di allarme

Il sistema di allarme può essere attivato totalmente o parzialmente.

Il numero di aree e settori attivabili dipendono dalle credenziali d'accesso dell'utente. L'utente Master può sempre attivare tutte le aree e tutti i settori.

Per attivare tutto il sistema di allarme

In HOMEPAGE premere il pulsante ATTIVAZIONE TOTALE.

In alternativa, nella sezione ANTIFURTO selezionare tutte le aree e/o tutti i settori e premere il pulsante ATTIVA.

Per attivare parzialmente il sistema di allarme

In HOMEPAGE premere il relativo pulsante di comando rapido, se è stato configurato e abilitato per attivare parzialmente il sistema di allarme.

In alternativa, nella sezione ANTIFURTO selezionare i settori o le aree da attivare e premere il pulsante ATTIVA.

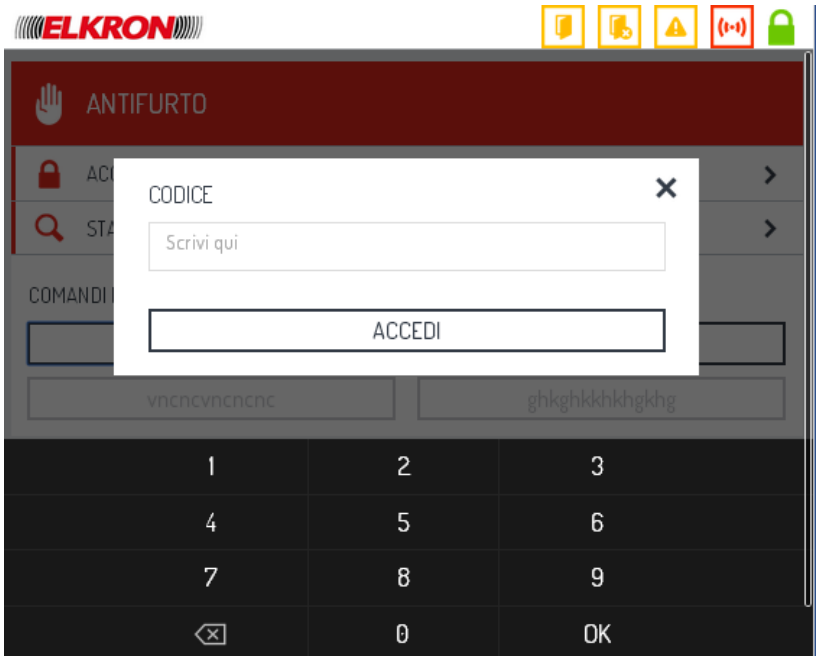
Disattivazione del sistema di allarme

Il sistema di allarme può essere disattivato totalmente o parzialmente da remoto purché sia stata abilitata la disattivazione da remoto. Il numero di aree e settori disattivabili dipende dalle credenziali d'accesso dell'utente. L'utente Master può sempre disattivare tutte le aree e tutti i settori.

Per disattivare tutto il sistema di allarme

In HOMEPAGE premere il pulsante DISATTIVAZIONE TOTALE.

Viene quindi richiesto il codice Utente (Autenticazione dell'accesso) per confermare l'operazione.



ATTENZIONE! Il comando di disinserimento totale disinserisce solo le aree e i settori che sono associati all'utente che inserisce il codice.

In alternativa, nella pagina ANTIFURTO selezionare tutte le aree e/o tutti i settori e premere il pulsante DISATTIVA.

Per disattivare parzialmente il sistema di allarme

Nella pagina ANTIFURTO selezionare i settori o le aree da disattivare e premere il pulsante DISATTIVA.

Ingressi associati al settore

Per vedere gli ingressi associati a un settore:

- nella pagina STATO espandere il settore facendo clic sul suo nome, oppure
- nella pagina ANTIFURTO espandere il settore facendo clic sul suo nome. Se il settore non ha ingressi con segnalazioni non si espande, a differenza di ciò che accade nella pagina STATO.

Viene mostrato l'elenco degli ingressi associati al settore e per ognuno di essi:

- se l'ingresso è aperto (icona );
- se l'ingresso è stato isolato manualmente o automaticamente (autoinibizione) (icona );
- se l'ingresso ha segnalato o sta segnalando un allarme oppure se è o è stato manomesso (icona ).

Se l'icona è grigia significa che per l'ingresso non vale la condizione associata all'icona stessa.

Facendo nuovamente clic sul nome del settore si chiude l'elenco.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Ingresso aperto

Alla pagina INGRESSI APERTI si accede facendo clic sull'icona . L'icona è visibile solo se c'è almeno un ingresso aperto.

Nella pagina sono elencati tutti gli ingressi aperti, raggruppati gerarchicamente per aree (se esistono) e settori. Se un settore non appartiene a nessuna area, esso viene visualizzato dopo le aree nel raggruppamento Settori.
Se un ingresso appartiene a più settori, esso viene elencato all'interno di ciascun settore.
Gli ingressi chiusi non vengono elencati.

La pagina viene aggiornata in tempo reale. Se nel sistema avvengono cambiamenti quando la pagina è aperta, indipendentemente dallo stato del sistema di allarme (attivo o disattivo), essi sono immediatamente visualizzati. Un ingresso che viene aperto sarà subito visualizzato nell'elenco, mostrando anche il settore ed eventuale area di appartenenza. Un ingresso che viene chiuso sarà immediatamente cancellato dall'elenco insieme al settore ed eventuale area di appartenenza, se non più necessari.

Per ogni ingresso sono visualizzate la sua denominazione e, tramite le icone accese (colorate), gli altri eventuali stati che lo caratterizzano: isolamento ( ) e allarme ( ).

Le icone in alto mostrano, in forma sintetica, lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **X** in alto a destra nella barra del titolo.

Ingresso isolato

Alla pagina INGRESSI ISOLATI si accede facendo clic sulla relativa icona . L'icona è visibile solo se il sistema ha degli ingressi isolati.

Nella pagina sono elencati tutti gli ingressi isolati, raggruppati gerarchicamente per aree (se esistono) e settori. Se un settore non appartiene a nessuna area, esso viene visualizzato dopo le aree nel raggruppamento Settori.

Se un ingresso appartiene a più settori, esso viene elencato all'interno di ciascun settore.
Gli ingressi non isolati non vengono elencati.

La pagina viene aggiornata in tempo reale. Se a sistema disattivo avvengono cambiamenti quando la pagina è aperta, essi sono immediatamente visualizzati. Un ingresso che viene isolato sarà subito visualizzato nell'elenco, mostrando anche il settore ed eventuale area di appartenenza.

Se l'ingresso viene incluso, cioè non è più isolato, esso sarà immediatamente cancellato dall'elenco e la pagina aggiornata immediatamente. Se il settore e l'eventuale area di appartenenza non contengono altri ingressi isolati, anche essi vengono cancellati.
Gli ingressi possono essere isolati e inclusi nuovamente tramite la pagina Isolamento ingressi del Web Server.

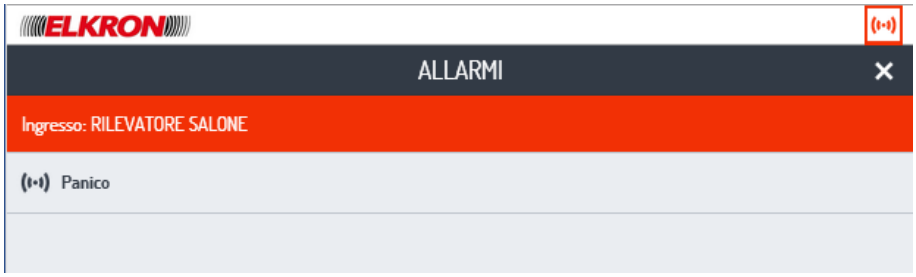
Per ogni ingresso sono visualizzate la sua denominazione e, tramite le icone accese (colorate), gli altri eventuali stati che lo caratterizzano: aperto ( ) e allarme ( ).

Le icone in alto mostrano, in forma sintetica, lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **X** in alto a destra nella barra del titolo.

Allarmi e manomissioni

Alla pagina ALLARMI si accede facendo clic sulla relativa icona .



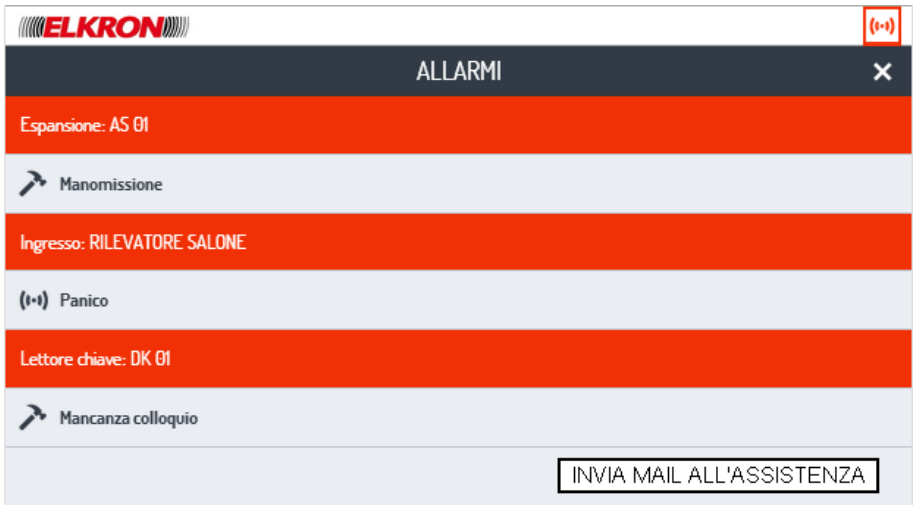
Nella pagina sono elencati tutti gli allarmi e le manomissioni presenti nella memoria allarme e nella memoria manomissione. Ciò significa che sono mostrati anche gli allarmi meno recenti, finché essi non vengono cancellati dalle memorie.

Allarmi e manomissioni sono raggruppati gerarchicamente per dispositivi. Ogni dispositivo è identificato dal suo tipo e dalla sua denominazione e sono elencati gli allarmi e manomissioni che lo interessano.
Allarmi e manomissioni sono contraddistinti anche da icone (= allarme, = manomissione).

All'apertura, la pagina mostra gli allarmi presenti in memoria. Se nel sistema avvengono cambiamenti quando la pagina è aperta, essi vengono immediatamente visualizzati aggiornando la pagina.

Le icone in alto mostrano, in forma sintetica, lo stato del sistema Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **X** in alto a destra nella barra del titolo.



Nel caso sia segnalata almeno una manomissione, in fondo alla pagina appare il pulsante “Invia mail all’assistenza”. Facendo clic su questo pulsante viene inviata una e-mail al primo indirizzo e-mail, memorizzato tra i contatti, e agli indirizzi e-mail dei contatti tecnici configurate. L’oggetto dell’e-mail inviata sarà “Richiesta di assistenza dell’impianto: ” seguito dal nome dell’impianto impostato in fase di configurazione.

Nell’e-mail vengono specificati i seguenti dati dell’impianto:

- “Impianto: ”, cioè il nome dell’impianto impostato in fase di configurazione.
- “Modello centrale: ”, identificato con marca e modello.
- “Versione centrale: ”, cioè la versione del firmware della centrale.
- “Codice impianto: ”, cioè il codice identificativo dell’impianto.

Se non è disponibile il modello della centrale, la versione firmware o il codice di impianto, al posto del dato appare il messaggio “Informazioni sull’impianto non disponibili”.

Di seguito, nella e-mail, vengono elencate tutte le manomissioni presenti al momento dell’invio, indicando per ognuna di esse:

- “Tipo dispositivo: ”, cioè il tipo di dispositivo guasto (ad esempio, espansione, lettore chiave, etc.).
- “Nome dispositivo: ”, cioè il nome attribuito al dispositivo in fase di configurazione (ad esempio AS01, DK01 etc.)
- “Segnalazione: ”, cioè il tipo di manomissione riscontrato (ad esempio Manomissione, Mancanza colloquio, etc.).
- “Data: ”, cioè la data in cui si è verificata la manomissione.
- “Ora: ” , cioè l’ora in cui si è verificata la manomissione.

Se non è disponibile la data o l’ora, al posto del dato appare il messaggio “Data e ora non disponibili”.

Segnalazioni di allarme e manomissione

Le segnalazioni di allarme o manomissione possono essere generate dai seguenti dispositivi:

- Centrale
- Espansione
- Espansione radio
- Ingresso filare
- Contatto magnetico radio
- Rivelatore IR radio
- Tastiera
- Uscita sirena radio
- Alimentazione supplementare AS500

Inoltre una segnalazione di allarme può essere generata anche dall'utente, tramite ingresso di allarme, tastiera o telecomando.

Le possibili segnalazioni sono:

Dispositivo	Sabotaggio	Mancanza colloquio	Jamming	Super visione radio	Allarme
Centrale	■				
Espansione	■	■			
Espansione radio		■	■	■	
Ingresso filare	■				Intrusione Preallarme Incendio Panico Soccorso Tecnologico tipo 1, 2, 3 Panico silenzioso Coercizione Reset incendio Prova
Contatto magnetico radio			■	■	
Rivelatore IR radio			■	■	
Tastiera		■			Panico silenzioso Soccorso Incendio
Telecomando					Panico Panico silenzioso Soccorso Incendio
Uscita sirena radio			■	■	
Alimentazione supplementare AS500	■	■			

Notifica dell’allarme via e-mail

Ogni evento di allarme intrusione, manomissione e ON/OFF aree o settori genera una e-mail istantanea, che viene inviata agli indirizzi configurati.

Il campo Oggetto della e-mail inviata viene compilato come: “Impianto ” + codice impianto + “Evento ” + identificativo univoco dell’evento + tipo di evento.

Nell’e-mail vengono specificate le seguenti informazioni sull’allarme:

- “Aree: ”, cioè le aree a cui è associato l’ingresso che ha segnalato l’allarme.
- “Settori: ”, cioè i settori a cui è associato l’ingresso che ha segnalato l’allarme.
- “Tipo di dispositivo: ”, cioè il tipo di dispositivo che ha segnalato l’allarme.
- “Nome del dispositivo: ”, cioè il nome attribuito in fase di configurazione al dispositivo che ha segnalato l’allarme. Se non è stato attribuito nessun nome appare il nome creato di default dal sistema in fase di installazione (ad esempio KB01).
- “Segnalazione: ”, cioè il tipo di allarme generato.
- Data e ora.

Se l’allarme è di tipo intrusione e all’ingresso interessato è associata una telecamera, viene generata una registrazione dell’evento. La registrazione contiene 15 immagini a bassa risoluzione (5 prima e 10 dopo l’allarme) o 8 ad alta risoluzione (4 prima e 4 dopo l’allarme). Tutte le immagini vengono catturate a distanza di un secondo una dall’altra.

Al termine della registrazione viene inviata una seconda e-mail, con allegata la prima immagine memorizzata dopo l’attivazione dell’allarme.

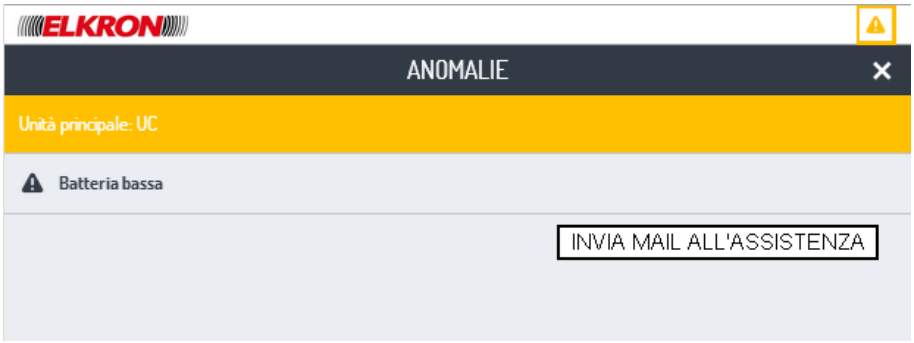
Il campo Oggetto della seconda e-mail inviata viene compilato come: “Impianto “ + codice impianto + “Evento” + identificativo univoco dell’evento, che è lo stesso utilizzato nella prima e-mail + tipo di evento.

Il testo della seconda e-mail sarà “È disponibile una registrazione dalla telecamera”, seguito dal nome attribuito alla telecamera in fase di configurazione. Nel caso la telecamera fosse fuori servizio, il testo sarà: “Registrazione dalla telecamera non disponibile”, seguito dal nome attribuito alla telecamera.

Se all’ingresso che segnala l’allarme sono associate più telecamere, vengono inviate e-mail di notifica separate, una per telecamera.

Anomalie

Alla pagina ANOMALIE si accede facendo clic sulla relativa icona , che appare quando è presente o memorizzato almeno un guasto o anomalia.



Attraverso questa pagina è possibile esaminare tutti i guasti e le anomalie presenti o memorizzate nello storico della centrale.

Guasti e anomalie sono raggruppati per dispositivi. Ogni dispositivo è identificato dai suoi tipo e denominazione.

All'apertura, la pagina mostra gli allarmi presenti in memoria. Se nel sistema avvengono cambiamenti quando la pagina è aperta, essi vengono immediatamente visualizzati.

Ogni tipo di evento viene evidenziato da un'icona e viene visualizzato il dettaglio dell'anomalia rivelata.

In fondo alla pagina appare il pulsante "Invia mail all'assistenza". Facendo clic su questo pulsante viene inviata una e-mail al primo indirizzo e-mail, memorizzato tra i contatti, e agli indirizzi e-mail configurati dei contatti tecnici. L'oggetto dell'e-mail inviata sarà "Richiesta di assistenza dell'impianto: " seguito dal nome dell'impianto impostato in fase di configurazione.

Nell'e-mail vengono specificati i seguenti dati dell'impianto:

- "Impianto: ", cioè il nome dell'impianto impostato in fase di configurazione.
- "Modello centrale: ", identificato con marca e modello.
- "Versione centrale: ", cioè la versione del firmware della centrale.
- "Codice impianto: ", cioè il codice identificativo dell'impianto.

Se non è disponibile il modello della centrale, la versione firmware o il codice di impianto, al posto del dato appare il messaggio "Informazioni sull'impianto non disponibili".

Di seguito, nella e-mail, vengono elencati tutti i guasti presenti al momento dell'invio, indicando per ognuno di essi:

- "Tipo dispositivo: ", cioè il tipo di dispositivo guasto (ad esempio, espansione, lettore chiave, etc.).
- "Nome dispositivo: ", cioè il nome attribuito al dispositivo in fase di configurazione (ad esempio AS01, DK01 etc.)
- "Segnalazione: ", cioè il tipo di guasto riscontrato (ad esempio Batteria bassa, Guasto alimentazione, Accecamento, etc.).
- "Data: ", cioè la data in cui si è verificato il guasto.
- "Ora: ", cioè l'ora in cui si è verificato il guasto.

Se non è disponibile la data o l'ora, al posto del dato appare il messaggio "Data e ora non disponibili".

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Anomalie rivelate

Il tipo di dispositivo determina le anomalie che possono essere segnalate, come mostrano gli elenchi che seguono.

Centrale

- Mancanza Rete: l'alimentazione di rete (230 V) della centrale è interrotta.
- Batteria bassa: la batteria tampone non è sufficientemente carica.
- Guasto PSTN: non funziona il collegamento telefonico filare.
- Guasto GSM: non funziona il collegamento telefonico cellulare.
- Guasto LAN: non funziona il collegamento alla rete Internet.
- Fuse V1: fusibile autoripristinante.
- Fuse V2: fusibile autoripristinante.

Espansione di centrale

- Guasto alimentazione: l'espansione non è alimentata correttamente.

Rivelatore

- Batteria bassa (rivelatore radio): la pila del rivelatore radio non è sufficientemente carica.
- Guasto: il rivelatore non funziona correttamente.

Ingresso filare

- Guasto: guasto generico dell'ingresso.
- Guasto rivelatore: il rivelatore non funziona correttamente.
- Guasto comunicatore: guasto del comunicatore esterno.
- Accecamento: c'è un tentativo di accecamento dei rivelatori.
- Guasto sirene: le sirene non funzionano correttamente.

Sirene radio

- Batteria bassa: la pila della sirena radio non è sufficientemente carica.

Tastiera

- Guasto alimentazione: la tastiera non è alimentata correttamente.

Lettore di chiave elettronica o di prossimità

- Guasto alimentazione: il lettore non è alimentato correttamente.

Telecomando

- Batteria bassa: la pila del telecomando non è sufficientemente carica.

Impostazioni

Alla pagina IMPOSTAZIONI si accede facendo clic sull'icona .

Questa pagina consente accedere alle funzioni per abilitare utenti e chiavi, configurare parametri e funzioni, modificare le credenziali di accesso, visionare lo storico, configurare gli scenari domotici e altro ancora.

ATTENZIONE! L'icona può essere cliccata e quindi la pagina visualizzata solo se il sistema di allarme è completamente disattivo.

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Le voci visualizzate sono dinamiche, ossia dipendono dal tipo di utente che ha effettuato l'accesso.

Funzioni disponibili

- **Abilitazioni**. Consente di abilitare utenti e chiavi. Abilita l'accessibilità da remoto e la disattivazione da remoto. È disponibile solo per l'utente Master.
- **Recapiti**. Consente di inserire, modificare e cancellare numeri di telefono ed e-mail nel sistema. È disponibile solo per l'utente Master.
- **Procedura di modifica** di username e password**.** Consente di modificare le username e password di accesso al solo Web Server. È disponibile solo per l'utente Master.
  IMPORTANTE: Per accedere al Web Server le credenziali sono uniche e uguali per tutti gli utenti. Le username e password qui definite servono soltanto ad accedere al Web Server, non a interagire con il sistema di allarme, che richiede di autenticarsi usando lo stesso codice usato con le tastiere.
- **Orologio**. Modifica data e ora memorizzate in centrale. È disponibile solo per l'utente Master.
- **Storico Eventi**. Mostra l'elenco delle attività eseguite direttamente sul sistema o tramite il Web Server. È disponibile per tutti gli utenti.
- **Isolamento ingressi**. Consente di isolare o includere nuovamente degli ingressi. È disponibile per tutti gli utenti. Se nessuno degli ingressi associati all'utente tramite i settori è isolabile, facendo clic su ISOLAMENTO INGRESSI appare un pop-up con il messaggio "Nessun ingresso isolabile".
- **Comandi rapidi**. Consente di configurare e abilitare le attivazioni rapide (quelle che appaiono nella sezione ANTIFURTO della HOMEPAGE) e gli scenari (quelli che appaiono nella sezione DOMOTICA della HOMEPAGE). È disponibile solo per l'utente Master.
- **Informazioni .** Mostra le informazioni tecniche generali del sistema. È disponibile per tutti gli utenti.

Il tasto **CANCELLA MEMORIA ALLARMI** è disponibile per tutti gli utenti.

Premendolo si cancellano tutte le segnalazioni di allarme della centrale per i settori di competenza dell'utente. Ciò significa che se un utente può operare solo su alcuni dei settori, determinate in base al codice di accesso numerico alla centrale, egli sarà in grado di cancellare solo gli allarmi degli ingressi che appartengono a quei settori, non la totalità degli allarmi. Vengono inoltre cancellate le segnalazioni di guasto rete.

Il pulsante non cancella, in ogni caso, le segnalazioni di guasti e manomissioni.

Quando si preme il pulsante **CANCELLA MEMORIA ALLARMI** appare un pop-up che conferma l'avvenuta cancellazione o segnala che essa non è avvenuta.

Abilitazioni

Alla pagina ABILITAZIONI si accede dalla pagina Impostazioni. La pagina è visibile solo all'utente Master.

Attraverso questa pagina è possibile abilitare e disabilitare chiavi, utenti, accessibilità e disattivazione da remoto.

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Le sezioni della pagina sono:

- **CHIAVI**. Facendo clic su CHIAVI la voce si espande e viene mostrato l'elenco di tutte le chiavi elettroniche e di prossimità acquisite dal sistema. Le chiavi vengono individuate come *numero <nomina chiave>*, dove *<nomina chiave>* è l'eventuale nome attribuito alla chiave in fase di programmazione del sistema. L'icona ✓ indica che la chiave è abilitata. Per richiudere l'elenco fare nuovamente clic su CHIAVI.
- **UTENTI**. Facendo clic su UTENTI la voce si espande e viene mostrato l'elenco di tutti gli utenti memorizzati nel sistema. Gli utenti vengono individuati come *numero <nomina utente>*, dove *<nomina utente>* è il nome attribuito all'utente in fase di programmazione del sistema. L'icona ✓ indica che l'utente è abilitato. Per richiudere l'elenco fare nuovamente clic su UTENTI.
- **ACCESSIBILITÀ DA REMOTO**. Serve a consentire l'accesso da remoto al sistema, ad esempio per operazioni di manutenzione, compreso l'accesso del Web Server. L'icona ✓ indica che l'accessibilità da remoto è abilitata.
- **DISATTIVAZIONE DA REMOTO**. Abilita la disattivazione del sistema da remoto tramite linea telefonica e comandi DTMF. L'icona ✓ indica che la disattivazione da remoto è abilitata.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Abilitare e disabilitare

Per abilitare o disabilitare una chiave, un utente, l'accessibilità da remoto o la disattivazione da remoto fare quanto segue:

1. Selezionare la voce su cui si vuole operare, facendo clic sul pulsante circolare di selezione. Si può selezionare solo una voce alla volta.
2. Premere il pulsante **ABILITA** o **DISABILITA**, secondo necessità. La voce selezionata verrà abilitata o disabilitata secondo il pulsante premuto.

Lo stato dei vari parametri viene aggiornato in tempo reale, cioè accanto al nome del parametro comparirà o scomparirà l'icona di abilitazione ✓ secondo il suo nuovo stato.

Le abilitazioni e disabilitazioni sono memorizzate nella centrale.

L'immagine di esempio sopra mostra che l'utente Franca è stata selezionata per essere disabilitata.

Recapiti

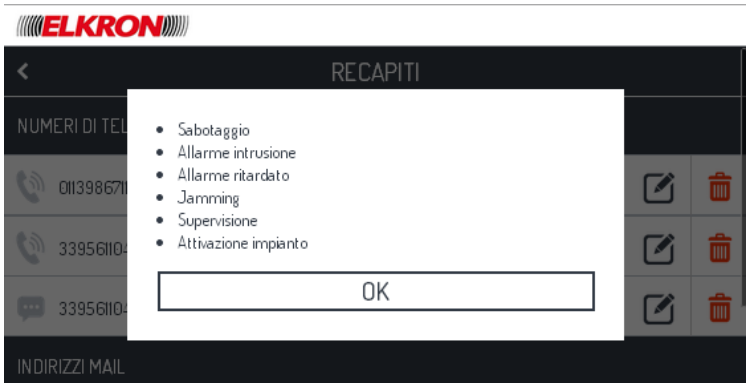
Alla pagina RECAPITI si accede dalla pagina Impostazioni. La pagina è visibile solo all'utente Master. Attraverso questa pagina è possibile modificare alcuni dei numeri di telefono già programmati in centrale, modificare e cancellare gli indirizzi e-mail che ricevono le segnalazioni di allarme generate dalla centrale. Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

La pagina mostra due sezioni, Numeri di telefono e Indirizzi mail, che possono essere espanse facendo clic su di esse. Per condensarle nuovamente fare clic sul loro titolo.

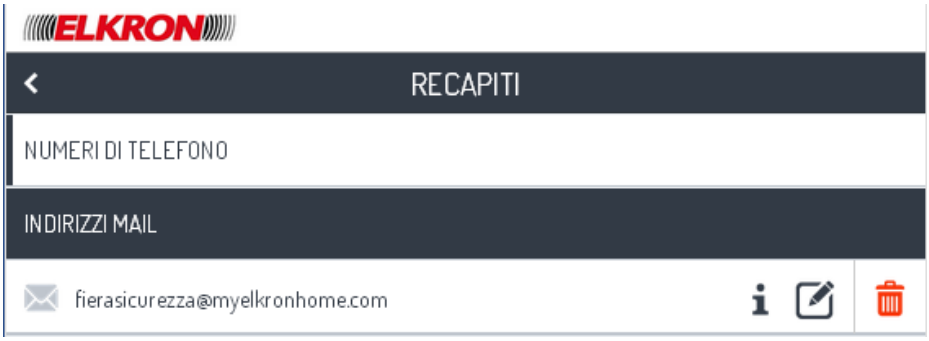
La sezione **Numeri di telefono** elenca tutti i numeri di telefono con specializzazione vocale o SMS configurati nella centrale. Se il numero di telefono che occupa la 12ª posizione di memoria in centrale è stato configurato come SMS, a quel numero vengono inviati gli SMS di rete.

La specializzazione viene indicata da un'icona posta accanto al numero di telefono (= vocale, = SMS). Facendo clic sull'icona viene aperta una finestra di pop-up che elenca tutti gli eventi associati a quel numero di telefono. I possibili eventi associati sono elencati in Allarmi notificati con messaggio vocale e Allarmi notificati via SMS.

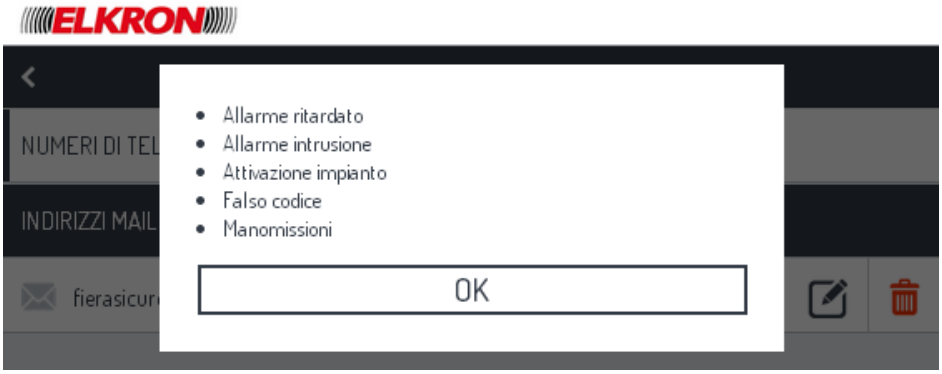


Numeri di telefono con specializzazione diversa da vocale o SMS, oppure numeri di telefono non configurati, non vengono elencati. La centrale contiene al massimo 12 numeri di telefono.

La sezione **Indirizzi mail** elenca gli indirizzi e-mail configurati.



Accanto all'indirizzo e-mail è posta l'icona . Facendo clic sull'icona viene aperta una finestra di pop-up che elenca tutti gli eventi associati a quella e-mail. I possibili eventi associati sono elencati in Allarmi notificati via e-mail.



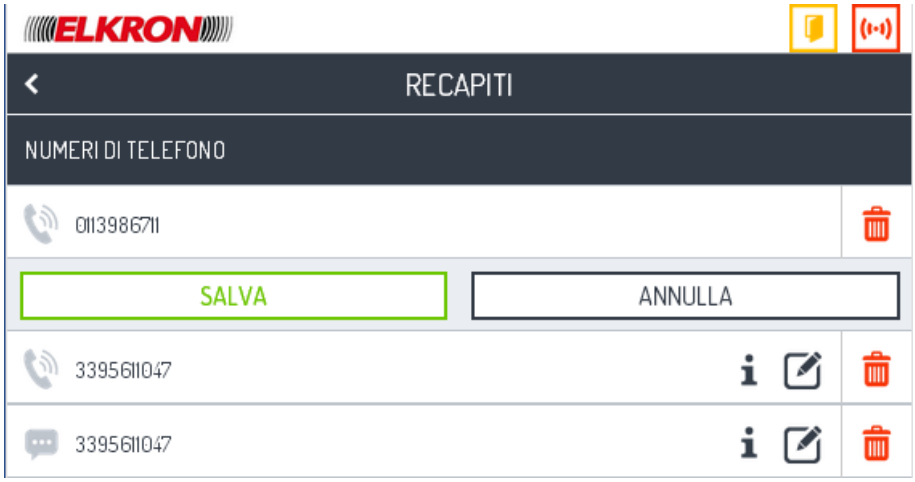
Il primo contatto e-mail riceve copia delle e-mail inviate al tecnico, quando si fa clic sul pulsante INVIA MAIL ALL'ASSISTENZA nelle pagine ANOMALIE e ALLARMI.

Modifica di un numero di telefono

Si può modificare un solo numero di telefono alla volta.

Per modificare un numero di telefono:

1. Fare clic sull'icona del numero di telefono da modificare. Appare il menu di modifica.



2. Digitare il nuovo numero di telefono.
   Se il numero di telefono è specializzato vocale si possono inserire cifre (0…9) e la lettera "P", che serve a inserire una pausa di 2 secondi nella composizione, ad esempio se è richiesta da un eventuale centralino. La lunghezza massima del numero di telefono è 28 caratteri, tra cifre e lettere "P".
   Se il numero di telefono è specializzato SMS si possono inserire solo cifre (0…9). La lunghezza massima del numero di telefono è 10 cifre.
3. Premere il pulsante **SALVA** per memorizzare le modifiche, **ANNULLA** per uscire dalla procedura senza effettuare modifiche.

ATTENZIONE! Il Web Server effettua un controllo formale sulla correttezza del numero di telefono, non sulla sua esistenza o sul suo funzionamento.

ATTENZIONE! La procedura di modifica del numero di telefono non consente di modificare gli altri suoi parametri (ad esempio le associazioni agli allarmi). Per modificare gli altri parametri del numero di telefono chiedere l'intervento del tecnico.

Cancellazione di un numero di telefono

Si può cancellare un solo numero di telefono alla volta.

Per cancellare un numero di telefono fare clic sulla sua icona . Il numero di telefono di riferimento viene cancellato ma gli altri parametri configurati rimangono memorizzati.

Sarà quindi possibile, in un secondo tempo, assegnare un nuovo numero di telefono di riferimento alla stessa posizione di memoria.

Modifica di un indirizzo e-mail

Si può modificare un solo indirizzo e-mail alla volta.

Per modificare un indirizzo e-mail:

1. Fare clic sull'icona dell'indirizzo e-mail da modificare. Appare il menu di modifica.
2. Digitare il nuovo indirizzo e-mail.
3. Premere il pulsante **SALVA** per memorizzare la modifica, **ANNULLA** per uscire dalla procedura senza effettuare modifiche.

ATTENZIONE! Il Web Server effettua un controllo formale sulla correttezza dell'indirizzo e-mail, che deve essere nel formato *nome@dominio.estensione*, non sulla sua esistenza o sul suo funzionamento.

ATTENZIONE! La procedura di modifica dell'indirizzo e-mail non consente di modificare gli altri suoi parametri (ad esempio le associazioni agli allarmi).

Cancellazione di un indirizzo e-mail

Si può cancellare un solo indirizzo e-mail alla volta.

Per cancellare un indirizzo e-mail fare clic sulla sua icona . L'indirizzo e-mail viene cancellato ma gli altri parametri configurati rimangono memorizzati. Sarà quindi possibile, in un secondo tempo, assegnare un nuovo indirizzo e-mail alla stessa posizione di memoria.

Allarmi notificati con messaggio vocale

Se sono stati attivati dei numeri di telefono per invio vocale a essi vengono inviate le notifiche per:

- Allarme intrusione
- Allarme tecnologico Tipo1
- Allarme tecnologico Tipo2
- Allarme tecnologico Tipo3
- Allarme incendio
- Panico
- Panico Silenzioso
- Soccorso
- Allarme coercizione
- On/Off Settori/Sistema
- Manomissione
- Rete 230V
- Batteria bassa
- Guasti
- Scadenza SIM

Ogni numero di telefono può ricevere più tipi di notifica e le notifiche possono essere diverse per ogni numero di telefono.

Allarmi notificati via SMS

Se sono stati attivati dei numeri di telefono per invio SMS a essi vengono inviate le notifiche per:

- Allarme intrusione
- Allarme tecnologico Tipo1
- Allarme tecnologico Tipo2
- Allarme tecnologico Tipo3
- Allarme incendio
- On/Off Settori/Sistema
- Manomissione
- Scadenza SIM

Ogni numero di telefono può ricevere più tipi di notifica e le notifiche possono essere diverse per ogni numero di telefono.

Allarmi notificati via e-mail

Se sono stati attivati degli indirizzi e-mail a essi vengono inviate le notifiche per:

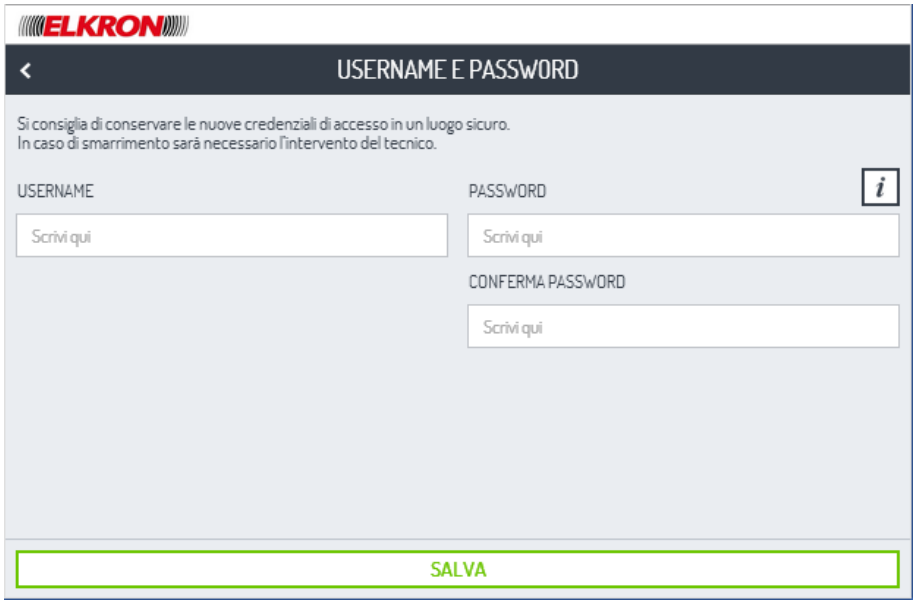
- Allarme intrusione
- Allarme ritardato
- ON/OFF Settori/Sistema
- Falso codice
- Manomissione

Ogni e-mail può ricevere più tipi di notifica e le notifiche possono essere diverse per ogni e-mail.

Il primo contatto e-mail riceve copia delle e-mail inviate al tecnico, quando si fa clic sul pulsante INVIA MAIL ALL'ASSISTENZA nelle pagine ANOMALIE e ALLARMI.

Username e Password

Alla pagina USERNAME E PASSWORD si accede dalla pagina Impostazioni. La pagina è visibile solo all'utente Master.



Attraverso questa pagina è possibile modificare le credenziali di accesso al Web Server (username e password). Si possono modificare una o entrambe le credenziali, secondo necessità.

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Caratteristiche obbligatorie di username e password

USERNAME

- Lunghezza minima 5 caratteri.
- Lunghezza max 15 caratteri.
- Caratteri ammessi: a…z, A…Z, 0…9 e i caratteri \ | !;" $ % & / ( ) = ? ^ + * @ # , ; . : - _ < > [ ] ` { } ~

PASSWORD

- Lunghezza minima 8 caratteri.
- Lunghezza max 15 caratteri.
- La password deve contenere almeno una lettera maiuscola, una lettera minuscola e una cifra.
- Caratteri ammessi: a…z, A…Z, 0…9 e i caratteri \ | !;" $ % & / ( ) = ? ^ + * @ # , ; . : - _ < > [ ] ` { } ~
- La username non può essere contenuta nella password.

Procedura di modifica di username e password

La procedura consente di modificare le credenziali di accesso. Per effettuare le modifiche:

1. Inserire la nuova username (il testo inserito è visibile).
2. Inserire la nuova password (il testo inserito viene mascherato da asterischi).
3. Inserire nuovamente la password per conferma (il testo inserito viene mascherato da asterischi).
4. Premere il pulsante **SALVA** per salvare le nuove credenziali di accesso.

ATTENZIONE! Bisogna inserire entrambe le credenziali di accesso (username e password), anche quella che non si vuole cambiare, perché la procedura di modifica non conserva in memoria i valori non variati.

Facendo clic sull'icona [i] appare un pop-up che elenca le caratteristiche obbligatorie della password.

Se username o password non rispettano le caratteristiche obbligatorie richieste (Caratteristiche obbligatorie di username e password) appare un pop-up che segnala che almeno un criterio non è stato rispettato. Modificare username o password e provare a salvare nuovamente. Non è possibile inserire username e password di fabbrica.

Se *Nuova password* e *Conferma password* non sono uguali appare il messaggio di errore "Le password inserite non coincidono". Reinserire *Nuova password* e *Conferma password* e provare a salvare nuovamente.

Quando username e password sono validi esse vengono memorizzate nel Web Server e riappare la pagina di login, dove occorre autenticarsi nuovamente con le nuove username e password prima di procedere.

ATTENZIONE! Conservare in un luogo sicuro il nuovo nome utente e la nuova password.

Nel caso si smarriscano le credenziali di accesso occorre contattare il tecnico, che provvederà a ripristinare il valore di fabbrica delle credenziali di accesso.
Le credenziali di accesso vengono riportate al valore di fabbrica anche dopo il reset hardware del Web Server.
Se le credenziali di accesso vengono riportate al valore di fabbrica occorre effettuare un nuovo primo accesso e modificarle.

Orologio

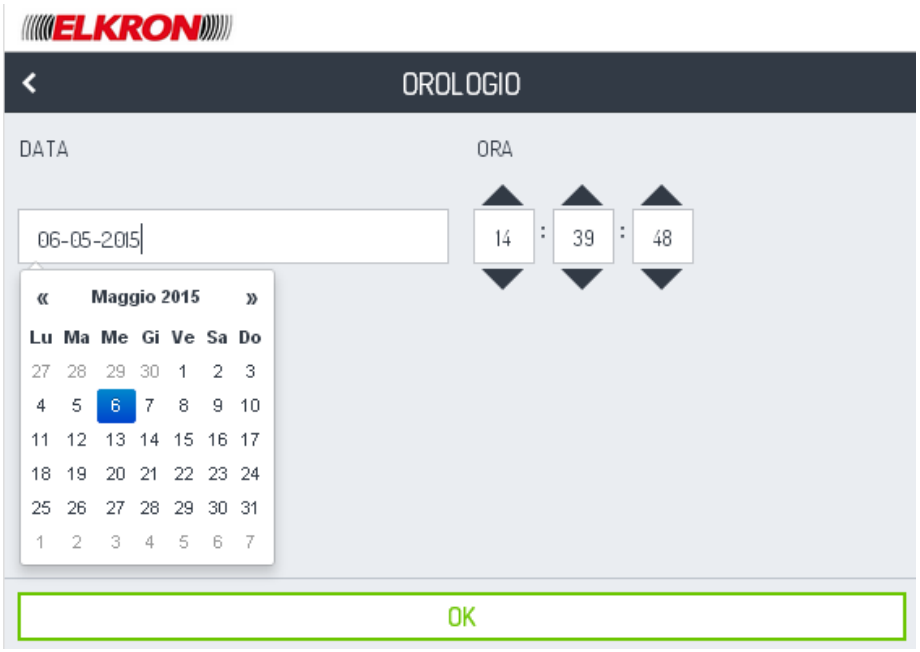
Alla pagina OROLOGIO si accede dalla pagina Impostazioni. La pagina è visibile solo all'utente Master.
Attraverso questa pagina è possibile visualizzare e quindi modificare la data e l'ora usata dalla centrale.

La data e l'ora mostrate sono quelle della centrale.
Cliccando sul pulsante **MODIFICA**, è possibile cambiare le impostazioni di data ed ora.

Le icone in alto mostrano lo stato del sistema Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

ATTENZIONE! Data e ora vengono usate dalla centrale nella memorizzazione degli eventi e allarmi nello storico e per la gestione del programmatore orario. Inserire una data o un orario non corretti può creare disservizi.



Per modificare la data:

- Fare clic sul campo data.
- Nel calendario che appare selezionare giorno, mese e anno.

Per modificare ora, minuti e secondi:

- Fare clic sulle frecce ▲ o ▼ per il campo ora, minuti o secondi da modificare fino alla visualizzazione del valore desiderato.

Al termine premere il pulsante **OK** per memorizzare la nuova data e il nuovo orario in centrale.

Storico Eventi

Alla pagina STORICO EVENTI si accede dalla pagina Impostazioni. La pagina è visibile a tutti gli utenti.

Attraverso questa pagina è possibile esaminare tutti gli eventi (attivazioni, disattivazioni, allarmi etc.) memorizzati nello storico eventi della centrale.

All'apertura della pagina vengono visualizzati tutti gli eventi più recenti accaduti l'ultimo giorno. Durante lo scaricamento dei dati il Web Server non è operativo. Per ogni tipo di evento elencato vengono specificate la data e l'ora in cui è accaduto.

L'ordine di presentazione degli eventi è dal più recente al più vecchio.
Si può allargare o restringere l'elenco degli eventi utilizzando la funzione filtro (Filtrare gli eventi).

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Filtrare gli eventi

È possibile filtrare gli eventi per restringere l'elenco dei risultati utilizzando il FILTRO DATA, che circoscrive il periodo di tempo analizzato.

Le possibili opzioni sono:

- Ultimo giorno (default)
- Ultima settimana
- Ultimo mese
- Ultimi 3 mesi
- Ultimo anno

Di ogni evento elencato si possono esaminare i dettagli (Esaminare i dettagli degli eventi).

Esaminare i dettagli degli eventi

Per visualizzare un evento in dettaglio fare clic sulla riga dello STORICO che lo elenca. Per nascondere i dettagli fare nuovamente clic sulla riga.

Le informazioni disponibili dipendono dal tipo di evento, come mostra la tabella che segue.

EVENTO	**INFORMAZIONI**
Allarme intrusione	ID e nomina dell'ingresso Numero logico dell'ingresso
Preallarme	ID e nomina dell'ingresso Numero logico dell'ingresso
Allarme tecnologico tipo 1/2/3	ID e nomina dell'ingresso Numero logico dell'ingresso
Allarme incendio	ID e nomina della sorgente da cui è partito l'allarme Numero logico dell'ingresso
Panico	ID e nomina della sorgente da cui è partito l'allarme Numero logico dell'ingresso
Panico silenzioso	ID e nomina della sorgente da cui è partito l'allarme Numero logico dell'ingresso
Soccorso	ID e nomina della sorgente da cui è partito l'allarme Numero logico dell'ingresso
Allarme coercizione	ID del dispositivo da cui è partito l'allarme sensore allarmato
ON/OFF Settori/Sistema	ID del dispositivo (KP = tastiera; MODEM = Hi-Connect; WS = Web Server,…) ID e nomina utente che ha inserito il codice ID e nomina di tutti i settori che sono stati attivati/disattivati

Inizio Manutenzione	ID del dispositivo (KP= tastiera) ID del tecnico
Fine Manutenzione	ID del dispositivo (KP= tastiera) ID del tecnico
Inizio Isolamento ingressi	ID e nomina dell'ingresso ID dell'utente
Fine isolamento ingressi	ID e nomina dell'ingresso ID dell'utente
Evento Assenza rete istantanea	Nomina della centrale SISTEMA
Evento fine assenza rete	Nomina della centrale SISTEMA
Inizio guasto	ID e nomina dell'ingresso L'uscita che è stata attivata
Evento fine guasto	ID e nomina dell'ingresso L'uscita che è stata attivata
Falso Codice	Nessuna informazione
Scadenza SIM	Nomina della centrale ID del tecnico
Evento reset incendio	

Isolamento ingressi

Alla pagina ISOLAMENTO INGRESSI si accede dalla pagina Impostazioni. La pagina è visibile a tutti gli utenti.

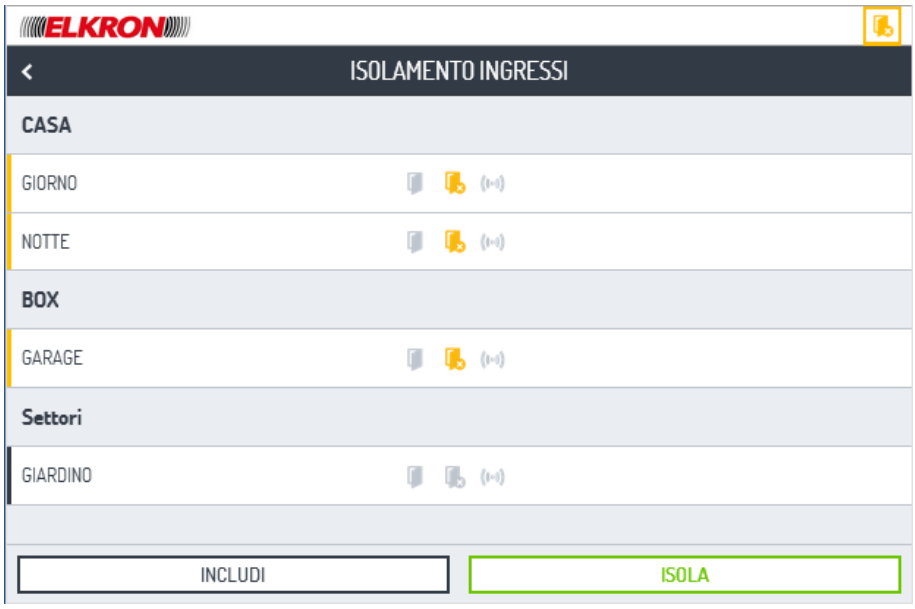
Attraverso questa pagina è possibile isolare o includere nuovamente degli ingressi del sistema di allarme antintrusione.

Un ingresso può dover essere isolato quando presenta qualche anomalia, per poter comunque attivare il sistema di allarme.

ATTENZIONE! Isolare un ingresso è una misura temporanea di emergenza, che riduce l'efficacia del sistema di allarme antintrusione. Appena possibile bisogna eliminare l'anomalia che ha richiesto l'isolamento dell'ingresso.

Le icone in alto mostrano lo stato del sistema Il loro significato e comportamento è spiegato nella descrizione della Homepage.

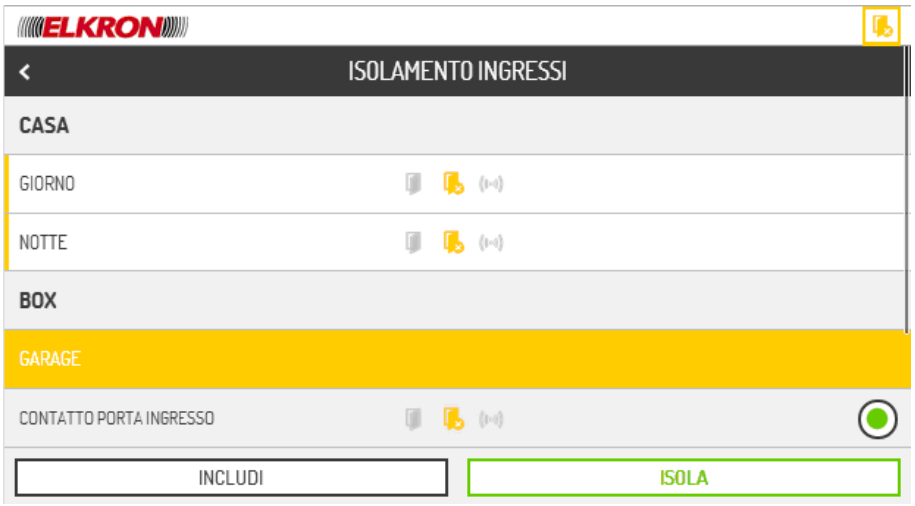
Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.



Vengono visualizzati solo le aree o i settori di competenza dell'utente che ha effettuato il login e che hanno ingressi isolabili.

Un ingresso è isolabile quando è stato così definito in fase di programmazione del sistema. Non tutti gli ingressi sono isolabili.

Se l'utente non ha competenza sugli ingressi isolabili esistenti, appare una finestra di pop-up con il messaggio "Nessun ingresso isolabile". Premendo il pulsante **INDIETRO** si chiude il pop-up.



Facendo clic su un settore si espande l'elenco degli ingressi isolabili ad esso associati (eventuali altri ingressi non isolabili, appartenenti al settore, non vengono mostrati).
Facendo nuovamente clic sul nome del settore l'elenco scompare.

Per ogni ingresso sono visualizzate la sua denominazione e, tramite le icone accese (colorate), gli altri eventuali stati che lo caratterizzano: ingresso aperto ( ) e allarme ( ).

Lo stato di aree, settori e ingressi viene letto al momento dell'apertura della pagina e aggiornato in tempo reale. Ciò significa che le icone possono cambiare anche a pagina aperta.

Isolamento e inclusione degli ingressi

Si può isolare o includere solo un ingresso alla volta.

Per isolare o includere nuovamente un ingresso isolabile:

1. Selezionare con un clic il pulsante di selezione circolare posto a destra dell'ingresso che interessa.
2. Premere il pulsante **ISOLA** per isolare l'ingresso selezionato, premere il pulsante **INCLUDI** per includere nuovamente l'ingresso selezionato.
3. L'icona di stato dell'ingresso su cui si è operato si aggiorna automaticamente.

Comandi rapidi

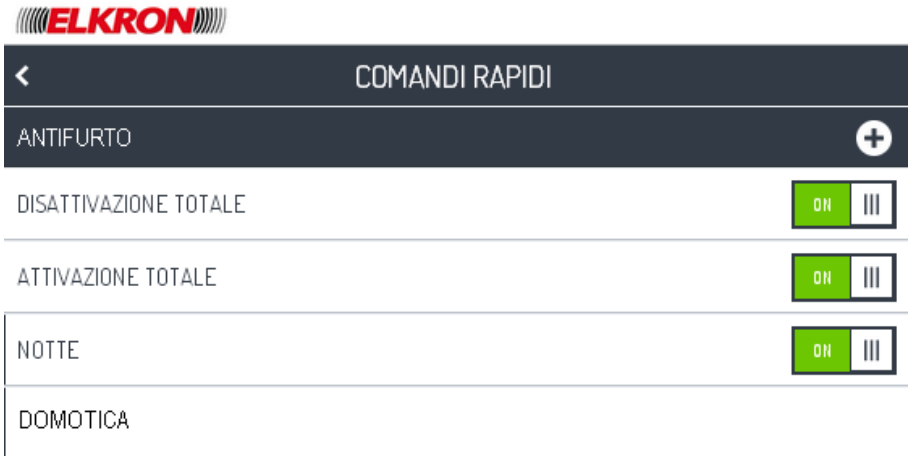
Alla pagina COMANDI RAPIDI si accede dalla pagina Impostazioni. La pagina è visibile solo all'utente Master.

Attraverso questa pagina è possibile configurare i tasti di attivazione rapida che appaiono nella Homepage.

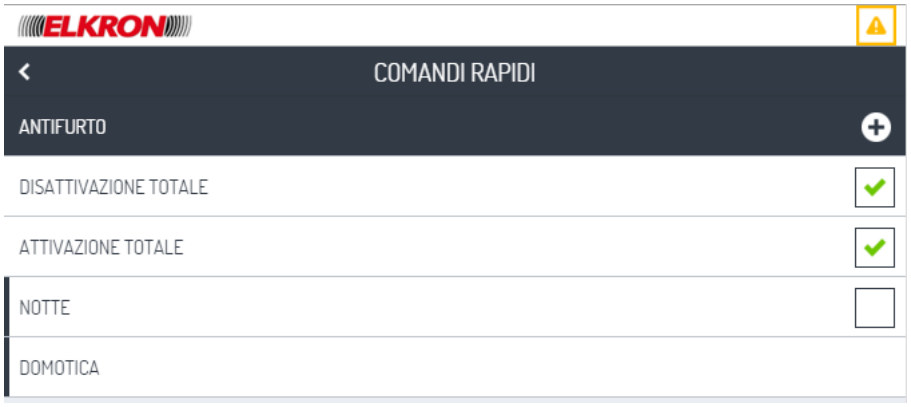
La pagina mostra due sezioni, Antifurto e Domotica, che possono essere espanse facendo clic su di esse. Per comprimerle nuovamente fare clic sul loro titolo.

Antifurto

ATTENZIONE! Videata antecedente la versione 1.3.0-X



ATTENZIONE! Videata presente dalla versione 1.3.0-X



È possibile programmare 4 comandi rapidi. Due sono già predefiniti (ATTIVAZIONE TOTALE e DISATTIVAZIONE TOTALE) e non è possibile cancellarli o modificarli.

ATTIVAZIONE TOTALE e DISATTIVAZIONE TOTALE escono di fabbrica disabilitati ed occorre abilitarli prima di poterli usare.

Per abilitare o disabilitare un comando rapido basta fare clic sull'icona dell'interruttore a slitta che si trova a destra del suo nome: con ON il comando rapido viene abilitato nella HOMEPAGE, con OFF rimane visibile ma è disabilitato (non può essere cliccato).

I comandi rapidi predefiniti (ATTIVAZIONE TOTALE e DISATTIVAZIONE TOTALE) quando sono disabilitati cambiano semplicemente colore (grigio invece di nero).

NOTA: qualora venisse cambiato il codice MASTER, occorre accedere ai comandi rapidi, disabilitarli tutti e successivamente riabilitarli.

Per una descrizione più dettagliata del funzionamento dei comandi rapidi vedere Come funzionano i comandi rapidi.

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Configurazione di un nuovo comando rapido

I comandi rapidi possono essere creati solo dall'utente Master.

Per creare un nuovo comando rapido:

1. Fare clic sull'icona ⊕ in alto a destra della sezione ANTIFURTO della pagina COMANDI RAPIDI. Appare la pagina NUOVO COMANDO RAPIDO. L'icona ⊕ è visibile solo se è possibile inserire ancora un comando rapido.

2. Inserire obbligatoriamente un nome descrittivo per il nuovo comando rapido nel campo "Etichetta". La lunghezza massima è 24 caratteri.
   Il nome inserito deve essere diverso dai nomi di comandi rapidi già presenti. Un eventuale errore viene segnalato dal messaggio "Etichetta comando rapido già presente. Inserire un nome differente".
3. Selezionare, facendo clic sul riquadro di selezione, le aree e i settori che fanno parte del nuovo comando rapido. Aree e settori possono essere scelti nella combinazione che si vuole.
   Se si sceglie un'area vengono automaticamente selezionati tutti i suoi settori, se si selezionano tutti i settori di un'area viene automaticamente selezionata anche l'area stessa.
4. Premere il pulsante **SALVA** per creare il nuovo comando rapido. Se non è stato selezionato almeno un settore o un'area compare il messaggio di errore "Selezionare almeno un settore da attivare".
   Facendo clic sull'icona **X** in alto a destra è possibile chiudere la pagina senza memorizzare le impostazioni effettuate.
5. Il nuovo comando rapido creato è disabilitato di default e occorre abilitarlo per poterlo usare.

Modifica di un comando rapido

I comandi rapidi possono essere modificati solo dall'utente Master. Non è possibile modificare ATTIVAZIONE TOTALE e DISATTIVAZIONE TOTALE.

Per modificare un comando rapido:

1. Fare clic sul nome del comando rapido: vengono elencate le aree attivate e appaiono i tasti ELIMINA e MODIFICA.
2. Premere il pulsante **MODIFICA**. Riappare la pagina utilizzata per creare un nuovo comando rapido.
3. Modificare il nome del comando rapido e aggiungere o rimuovere aree e settori dal comando rapido, secondo necessità. Le modifiche devono rispettare le stesse regole della Configurazione di un nuovo comando rapido.
4. Premere il pulsante **SALVA** per memorizzare e rendere effettive le modifiche effettuate.

Cancellazione di un comando rapido

I comandi rapidi possono essere cancellati solo dall'utente Master. Non è possibile cancellare ATTIVAZIONE TOTALE e DISATTIVAZIONE TOTALE.

Per cancellare un comando rapido:

1. Fare clic sul nome del comando rapido: vengono elencate le aree attivate e appaiono i tasti ELIMINA e MODIFICA.
2. Premere il pulsante **ELIMINA**.
3. Appare un pop-up con il messaggio "Attenzione. Cliccando su "Elimina" verrà cancellato il comando rapido. Si desidera procedere?". Premere nuovamente il tasto **ELIMINA** per chiudere il pop-up e cancellare il comando rapido, oppure premere il tasto **ANNULLA** per chiudere il pop-up senza cancellare il comando rapido.

CONSIGLIO: Se un comando rapido non serve più non occorre cancellarlo, basta disabilitarlo. In questo modo, se successivamente si cambiasse idea, non sarà necessario ricrearlo da zero, ma basterà abilitarlo di nuovo.

Come funzionano i comandi rapidi

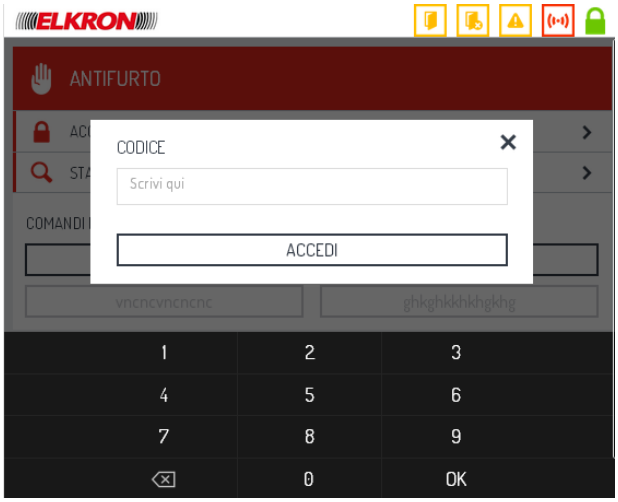
I comandi rapidi sono disponibili nella sezione ANTIFURTO della HOMEPAGE.

I pulsanti dei comandi rapidi possono essere neri, per indicare che il comando è abilitato, oppure grigi, per indicare che il comando è disabilitato. Per attivare il sistema di allarme basta premere il pulsante ATTIVAZIONE TOTALE. Non viene richiesto il codice utente.

IMPORTANTE! Con i pulsanti di comando rapido tutti gli utenti possono attivare i settori associati al pulsante, anche quelli che non sono di loro competenza. Ciò significa che, in determinate condizioni, un utente potrebbe attivare settori che non sarà più in grado di disattivare.

Se si preme il tasto DISATTIVAZIONE TOTALE appare un pop-up dove deve essere inserito un codice valido di 6 cifre (Master o Utente). Inserire il codice e premere il pulsante ACCEDI. Il comportamento del pop-up di inserimento del codice è uguale a quello della procedura Accedi.

I settori disattivati sono solo quelli di competenza dell'utente che ha inserito il codice.

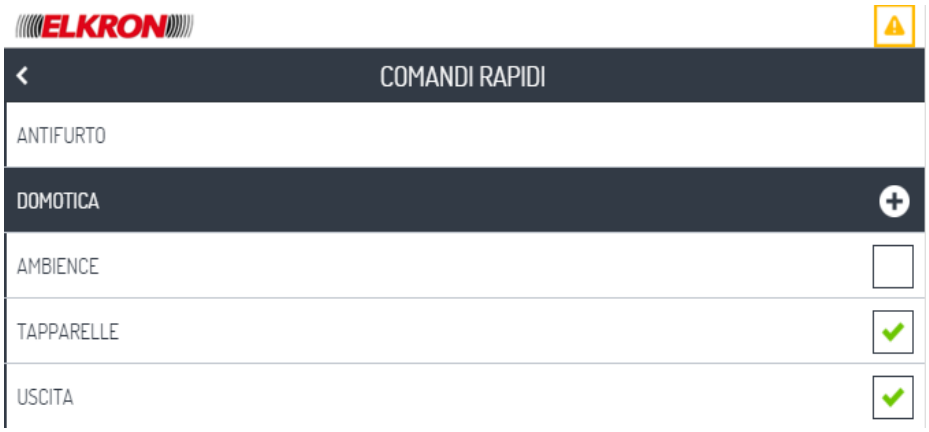


Per ulteriori informazioni sui comandi rapidi (come abilitarli, disabilitarli, crearli, modificarli e cancellarli) vedere la sezione Antifurto dei Comandi rapidi.

Domotica

ATTENZIONE! Videata antecedente la versione 1.3.0-X

ATTENZIONE! Videata presente dalla versione 1.3.0-X



È possibile programmare 4 scenari.

Per abilitare o disabilitare uno scenario basta fare clic sull'icona dell'interruttore a slitta che si trova a destra del suo nome: con ON lo scenario viene abilitato nella HOMEPAGE, con OFF rimane visibile ma è disabilitato (non può essere cliccato).
Gli scenari quando sono disabilitati cambiano semplicemente colore (grigio invece di nero).

NOTA: qualora venisse cambiato il codice MASTER, occorre accedere agli scenari, disabilitarli tutti e successivamente riabilitarli.

Per una descrizione più dettagliata del funzionamento degli scenari vedere Come funzionano gli scenari.

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona < in alto a sinistra nella barra del titolo.

Configurazione di un nuovo scenario

Gli scenari possono essere creati solo dall'utente Master.

Per creare un nuovo comando rapido:

1. Fare clic sull'icona ⊕ in alto a destra della sezione DOMOTICA della pagina COMANDI RAPIDI. Appare la pagina NUOVO SCENARIO. L'icona ⊕ è visibile solo se è possibile inserire ancora uno scenario.

2. Inserire obbligatoriamente un nome descrittivo per il nuovo comando rapido nel campo "Etichetta". La lunghezza massima è 24 caratteri. Finché non viene inserito nessun carattere il campo **SALVA** è disabilitato. Il nome inserito deve essere diverso dai nomi di scenari già presenti. Un eventuale errore viene segnalato dal messaggio "Etichetta scenario già presente. Inserire un nome differente".
3. Selezionare, facendo clic sul riquadro di selezione, le uscite che si vuole vengano azionate con l'esecuzione dello scenario. Per le uscite di tipo comandabile è possibile selezionare se si vuole che siano attivate o disattivate durante l'esecuzione dello scenario.
4. Premere il pulsante **SALVA** per creare il nuovo scenario. Se non è stata selezionata almeno un'uscita compare il messaggio di errore "Selezionare almeno una voce". Facendo clic sull'icona **X** in alto a destra è possibile chiudere la pagina senza memorizzare le impostazioni effettuate.
5. Il nuovo scenario creato è disabilitato di default e occorre abilitarlo per poterlo usare.

Modifica di uno scenario

Gli scenari possono essere modificati solo dall'utente Master.

Per modificare uno scenario:

1. Fare clic sul nome dello scenario: vengono elencate le uscite selezionate e appaiono i tasti **ELIMINA** e **MODIFICA**.
2. Premere il pulsante **MODIFICA**. Riappare la pagina utilizzata per creare un nuovo scenario.
3. Modificare il nome dello scenario e selezionare le uscite con relativa configurazione che dovranno essere attivate/disattivate o sollecitate all'esecuzione dello scenario. Le modifiche devono rispettare le stesse regole della Configurazione di un nuovo scenario.
4. Premere il pulsante **SALVA** per memorizzare e rendere effettive le modifiche effettuate.

Cancellazione di uno scenario

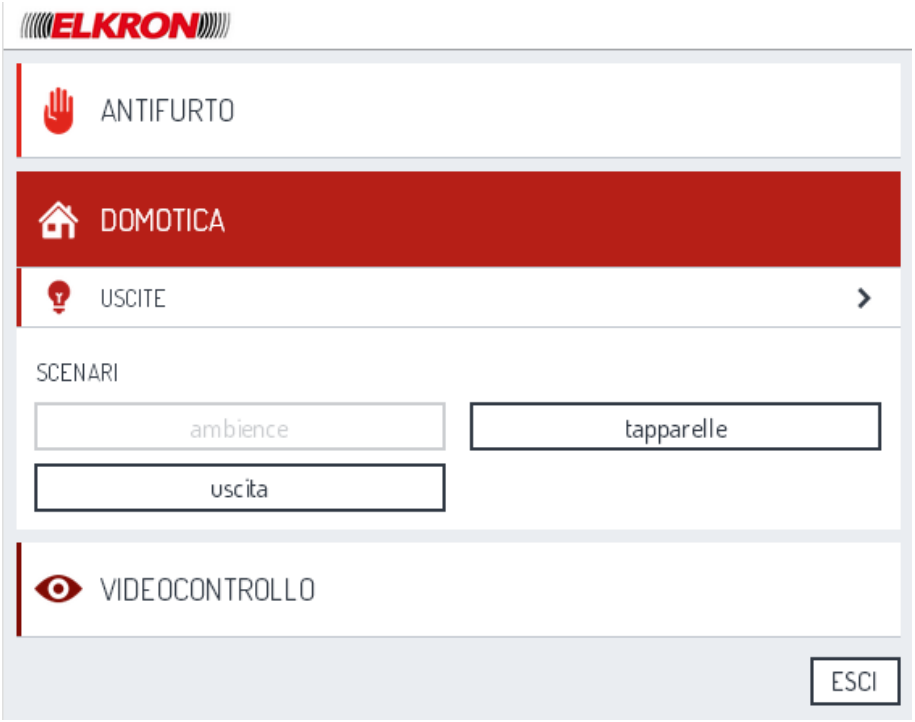
Gli scenari possono essere cancellati solo dall'utente Master.

Per cancellare uno scenario:

1. Fare clic sul nome dello scenario: vengono elencate le uscite selezionate e appaiono i tasti **ELIMINA** e **MODIFICA**.
2. Premere il pulsante **ELIMINA**.
3. Appare un pop-up con il messaggio "Attenzione. Cliccando su "Elimina" verrà cancellato lo scenario. Si desidera procedere?". Premere nuovamente il tasto **ELIMINA** per chiudere il pop-up e cancellare lo scenario, oppure premere il tasto **ANNULLA** per chiudere il pop-up senza cancellarlo.

Come funzionano gli scenari

Gli scenari disponibili nella HOMEPAGE, sotto la sezione DOMOTICA.



I pulsanti degli scenari possono essere neri, per indicare che è abilitato, oppure grigi, per indicare che lo scenario è disabilitato.

Per eseguire uno scenario è sufficiente cliccare sul pulsante corrispondente. Non viene richiesto il codice utente.

Per ulteriori informazioni sugli scenari (come abilitarli, disabilitarli, crearli, modificarli e cancellarli) vedere la sezione Domotica dei Comandi rapidi.

Informazioni

Alla pagina INFORMAZIONI si accede dalla pagina Impostazioni. La pagina è visibile a tutti gli utenti. Attraverso questa pagina è possibile conoscere le informazioni tecniche generali del sistema.

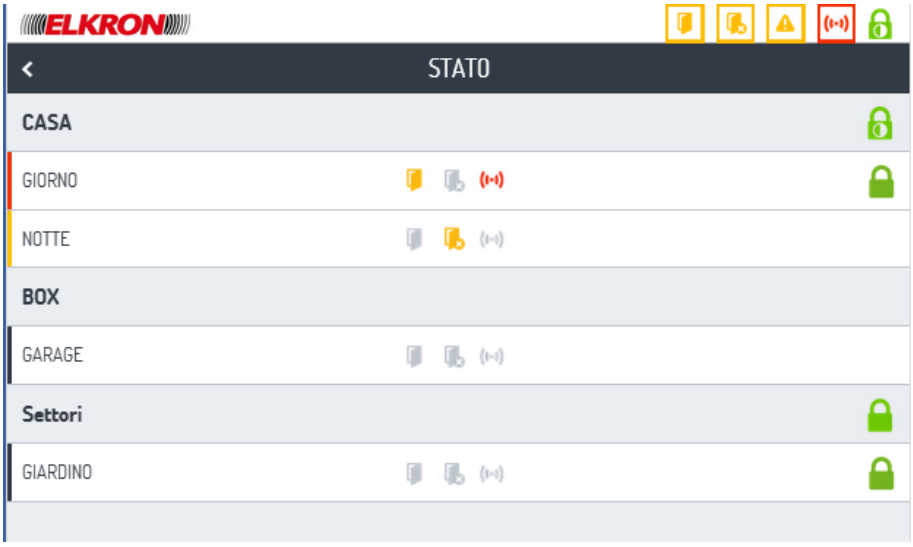
Le informazioni disponibili sono:

- **Mac address**: indirizzo MAC del Web Server.
- **Codice ID**: codice di identificazione del Web Server.
- **Nomina dispositivo**: Elkron.
- **Versione Web Server**: versione del firmware del Web Server.
- **Tipo centrale**: modello della centrale d'allarme a cui è collegato il Web Server.
- **Versione centrale**: versione del firmware della centrale d'allarme.
- **Indirizzo IP**: indirizzo IP del Web Server.
- **Subnet mask**: subnet mask usata dal Web Server.
- **Gateway predefinito:** indirizzo del gateway
- **Server DNS**: indirizzo IP del server che fornisce il servizio DNS.
- **Velocità**: le velocità di trasmissione della LAN.

Premendo il pulsante "Test connessione" verranno effettuati in automatico alcuni test per verificare il corretto funzionamento della rete e l'invio delle e-mail agli indirizzi configurati.

Stato

Alla pagina STATO si accede dalla sezione Antifurto.



Attraverso questa pagina è possibile verificare lo stato corrente del sistema di allarme intrusione.
Vengono visualizzate le aree e i settori dell'intero sistema. Se non ci sono segnalazione per un settore, le relative icone sono grigie.

Facendo clic sul nome di un settore, questo viene espanso e mostra l'elenco completo di tutti gli ingressi a esso associati. Per ogni ingresso le icone relative indicano il suo stato: allarme, aperto, isolato.

IMPORTANTE! A differenza di altre pagine del Web Server che mostrano informazioni simili, la pagina STATO ha delle caratteristiche molto interessanti:

- Può essere visualizzata senza dover effettuare un accesso autenticato.
- Elenca tutti gli ingressi e settori, non solo quelli per cui ci sono delle segnalazioni.

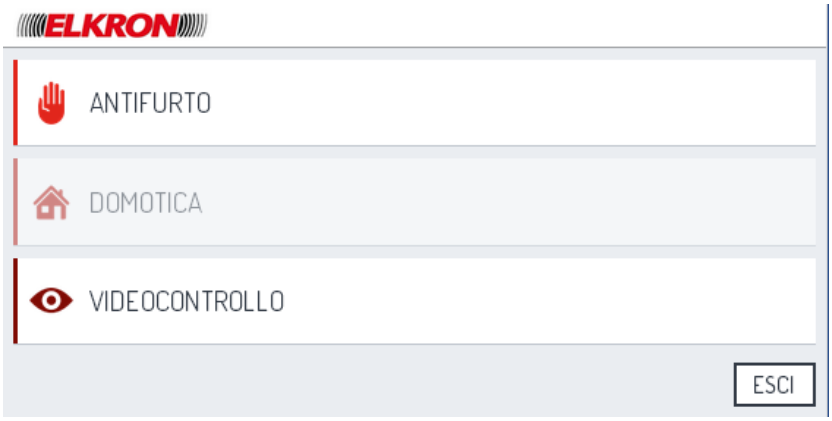
Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

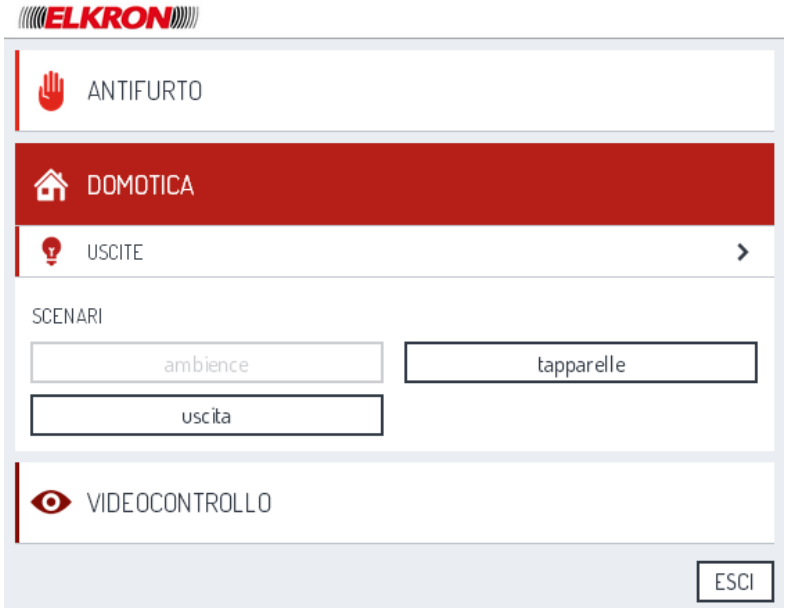
Domotica

Alla sezione DOMOTICA si accede dalla Homepage. Per espandere la sezione fare clic su DOMOTICA.

Se il pulsante DOMOTICA è grigio significa che non ci sono uscite domotiche configurate sulla centrale e non è possibile espandere la sezione.



Se invece è stata configurata sulla centrale almeno un'uscita di tipo domotico il pulsante DOMOTICA è abilitato ed è possibile espandere la sezione.



La sezione è divisa in due parti:

- Uscite, che consente di autenticarsi e accedere alla pagina di Gestione delle uscite domotiche per attivare e disattivare le uscite o per sollecitarle.
- Scenari, che consente di eseguire gli scenari configurati. Al click di uno scenario viene visualizzato un pop-up informativo sull'esito dell'invio del comando (dalla versione 1.3.0.-X e successive).

Le icone in alto mostrano, in forma sintetica, lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Facendo nuovamente clic su DOMOTICA si richiude la sezione.

Cliccando sul pulsante **ESCI**, si verrà disconnessi dal sistema, tornando alla schermata di login.

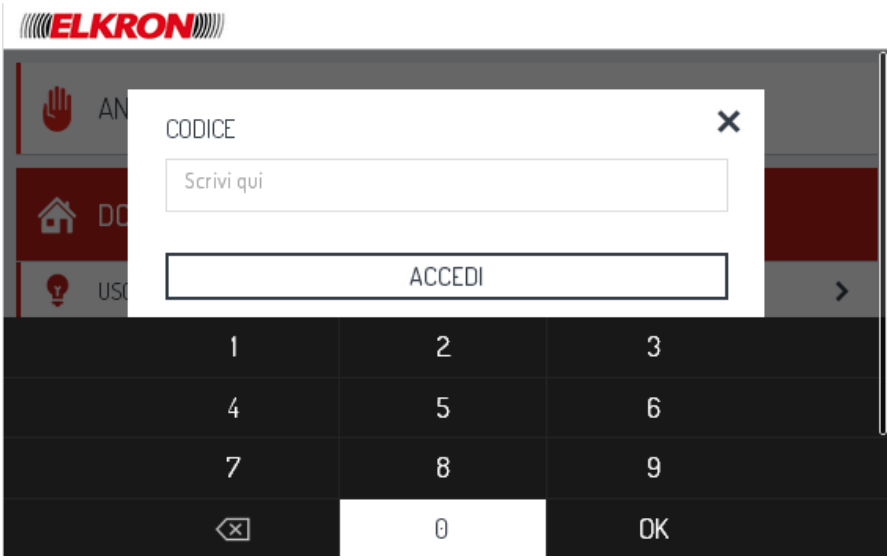
Uscite

Alla procedura ACCEDI si entra dalla sezione Domotica.

Attraverso questa procedura è possibile accedere direttamente alle uscite domotiche presenti nella centrale antintrusione, se l'accesso non è ancora stato effettuato dalla sezione Antifurto.

Autenticazione dell'accesso

Quando si entra alla procedura ACCEDI appare un pop-up per autenticarsi, se l'accesso non è ancora stato effettuato dalla sezione Antifurto.



Digitare un codice di accesso valido e premere il pulsante **ACCEDI**. Il codice di accesso è il codice numerico a 6 cifre usato per accedere al sistema d'allarme tramite le tastiere fisiche, non la password usata per accedere al Web Server. *ATTENZIONE*! Se i codici di accesso configurati in centrale sono lunghi meno di 6 cifre occorre prima riconfigurarli a 6 cifre per poter accedere alla centrale tramite Web Server.

Il tasto  cancella solo l'ultima cifra inserita e il tasto **OK** equivale al tasto **ACCEDI**, inviando il codice inserito alla centrale per la validazione.
Le operazioni che si possono compiere dopo l'accesso al sistema dipendono dai privilegi posseduti dal codice di accesso inserito.

Per chiudere la finestra di pop-up, senza tentare di accedere al sistema, fare clic fuori dalla tastiera virtuale e dal pop-up oppure premere l'icona X del pop-up. Così facendo, anche se è stato inserito un codice, esso viene scartato e non controllato, non modificando pertanto il contatore dei tentativi di accesso errati.

Se il codice inserito è corretto appare la pagina di gestione (Gestione delle uscite domotiche) delle uscite domotiche della centrale antifurto.

Se il codice inserito è errato, o non si è inserito nessun codice prima di premere il pulsante **ACCEDI**, viene visualizzato un messaggio di errore. Il contatore dei tentativi di accesso errati viene incrementato di 1.

Il numero massimo di tentativi di accesso errati è 21 (il limite è definito dalla centrale antintrusione e non è modificabile). Se viene inserito per più di 21 volte consecutive un codice di accesso errato, la centrale genera un allarme "falso codice".

Gestione delle uscite domotiche

Alla pagina di gestione delle uscite domotiche si accede dalla procedura Accedi.

Questa pagina consente di accedere alle funzioni per gestire ogni singola uscita domotica.

La pagina mostra:

- **Id e nome di ogni uscita comandabile** nell'immagine di esempio sono USCITA 3- Luce giardino e USCITA 4 - Irrigazione. Il pulsante a slitta 

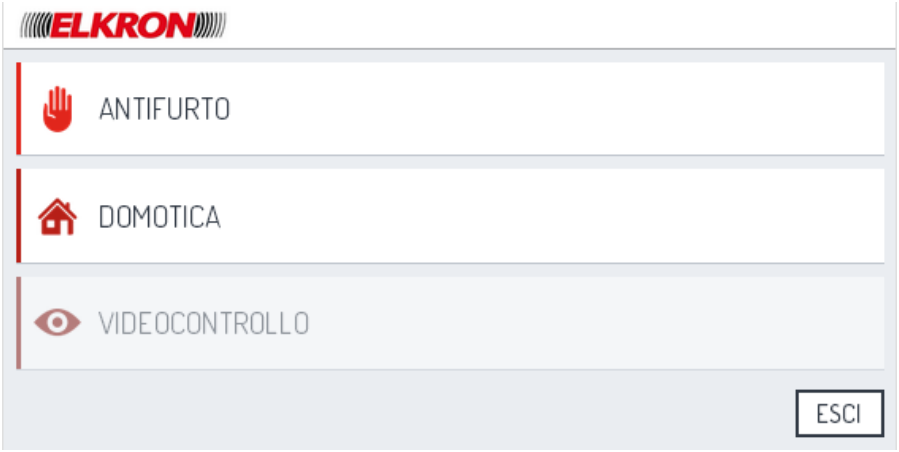
indica che è possibile attivare o disattivare l'uscita.
  Id e nome di ogni uscita comandabile impulsiva nell'immagine di esempio sono USCITA 5 – Ingresso pedonale e USCITA 6 – Ingresso carraio. Il pulsante esegui indica che è possibile dare un singolo impulso che solleciti l'uscita.
- Lo stato del sistema, attraverso le icone in alto. Il loro significato e comportamento è uguale a quelle della Homepage.

Per tornare alla pagina precedente fare clic sull'icona < in alto a sinistra nella barra del titolo.

Videocontrollo

Alla sezione VIDEOCONTROLLO si accede dalla Homepage.

Se il pulsante VIDEOCONTROLLO è disabilitato significa che non ci sono telecamere configurate e non è possibile espandere la sezione.



Se invece c'è almeno una telecamera configurata, facendo clic sul pulsante VIDEONTROLLO è possibile espandere la sezione.

Appaiono i pulsanti:

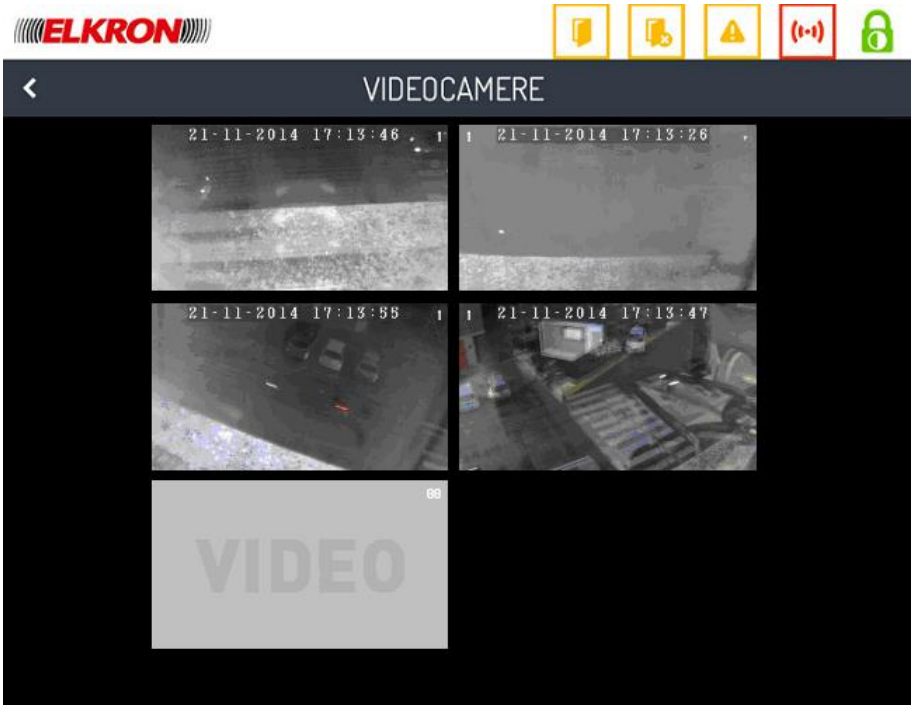
- Videocamere, che consente di visualizzare in tempo reale le immagini riprese dalle telecamere.
- Storico che consente di visualizzare, inviare via mail e salvare le immagini delle telecamere memorizzate in seguito a un evento di allarme.

Le icone in alto mostrano lo stato del sistema Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Premendo il pulsante **ESCI** ci si disconnette dal sistema e si torna alla schermata di login.

Videocamere

Alla pagina VIDEOCAMERE si accede col pulsante VIDEOCAMERE della sezione Videocontrollo.



In questa pagina è possibile gestire le anteprime delle telecamere acquisite e associate (max 8). A ogni riquadro di anteprima è associata una sola telecamera.

Le anteprime vengono aggiornate sfalsate tra di loro, con l'intervallo di 1 secondo tra una telecamera e l'altra (ad esempio, se ci sono 3 telecamere l'immagine della singola telecamera verrà aggiornata ogni 3 secondi).

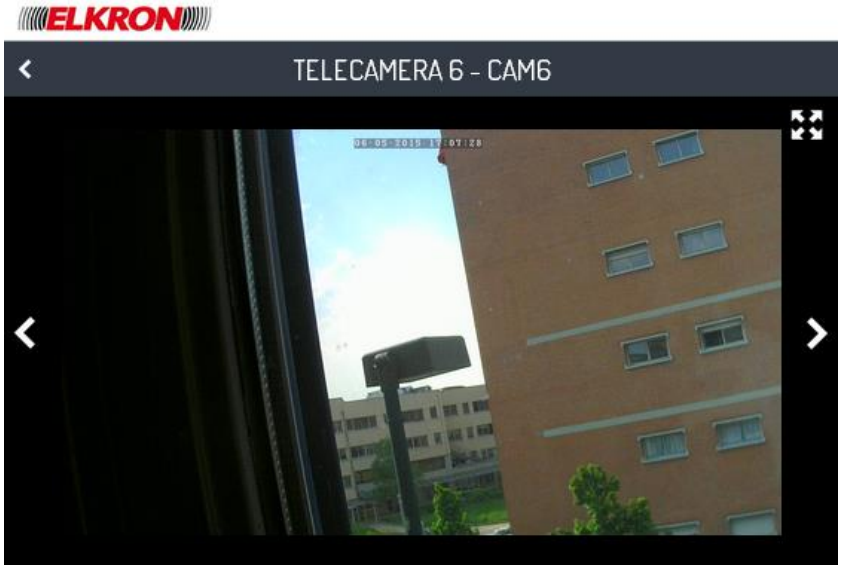
Se l'immagine della telecamera non è disponibile viene mostrato un riquadro grigio con la scritta VIDEO.

Facendo clic su un'anteprima si apre la Pagina di dettaglio della telecamera.

Le icone in alto mostrano lo stato del sistema Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Pagina di dettaglio della telecamera

Alla pagina di dettaglio della telecamera si accede facendo clic sul suo riquadro di anteprima nella pagina Videocamere.



L'immagine video viene aggiornata una volta al secondo. Sovraimpresse all'immagine, in alto ci sono data e ora. Il titolo della pagina mostra, invece, il nome attribuito alla telecamera in fase di configurazione.

Se nel sistema sono state acquisite e associate più telecamere appaiono i pulsanti di navigazione **<** e **>** per passare da una telecamera all'altra.

Cliccando sull'icona l'immagine viene mostrata a schermo intero.

È possibile ritornare alla visualizzazione a schermo normale cliccando sull'icona .

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona **<** in alto a sinistra nella barra del titolo.

Storico

Allo Storico del videocontrollo si accede col pulsante STORICO della sezione Videocontrollo.

All'apertura della pagina vengono visualizzati cronologicamente tutti gli eventi. Ogni evento è identificato dal nome della telecamera e dalla data e ora in cui è accaduto.

Facendo clic su un evento esso si espande e vengono mostrati:

- La denominazione dell'ingresso che ha segnalato l'allarme;
- Il nome del settore a cui è associato l'ingresso che ha segnalato l'allarme e fatto scattare la registrazione video;
- Il pulsante **ELIMINA**, che consente di cancellare manualmente l'evento e le immagini relative;
- Il pulsante **BLOCCA**, che consente di bloccare l'evento e prevenire la sua cancellazione automatica.
  ATTENZIONE! Bloccando gli eventi si riduce la memoria disponibile per memorizzare nuovi eventi. Un evento dovrebbe essere bloccato solo finché le immagini registrate non siano state scaricate e memorizzate su altro supporto.
- Il pulsante **VISUALIZZA**, per visionare e salvare le immagini.
- Il pulsante **INVIA MAIL**, che invia tutte le immagini dell'evento a tutti i contatti che ricevono segnalazioni per gli eventi di intrusione.

Facendo nuovamente clic sul nome dell'evento i dettagli vengono nascosti.

Se un evento è stato bloccato, nell'elenco degli eventi viene visualizzata l'icona e al posto del pulsante BLOCCA appare il pulsante **SBLOCCA**.

Quando si fa clic sul **VISUALIZZA** appare una nuova finestra:

La barra del titolo riporta il nome dell'evento. Il pulsante **<** della barra del titolo riporta alla pagina precedente.

Il pulsante  invia l'immagine corrente a tutti i tutti i contatti che ricevono segnalazioni per gli eventi di intrusione.

Tramite il PC con browser Chrome e Firefox, nelle versioni supportate (vedere il capitolo Browser compatibili), è possibile scaricare l'immagine corrente utilizzando il pulsante  .

Il pulsante fa partire lo scorrimento automatico delle immagini in modalità filmato, che può essere interrotto cliccando sul pulsante .

I pulsanti e permettono di navigare manualmente tra le immagini, ogni volta che si visualizza un'immagine differente viene aggiornato l'indicatore dell'immagine corrente (ad esempio 9 / 15) e viene incrementata la barra di progressione rossa.

Cliccando sul pulsante l'immagine viene mostrata a schermo intero.

É possibile ritornare alla visualizzazione a schermo normale cliccando sull'icona .

Le icone in alto mostrano lo stato del sistema. Il loro significato e comportamento è spiegato nella descrizione della Homepage.

Per tornare alla pagina precedente fare clic sull'icona < in alto a sinistra nella barra del titolo.

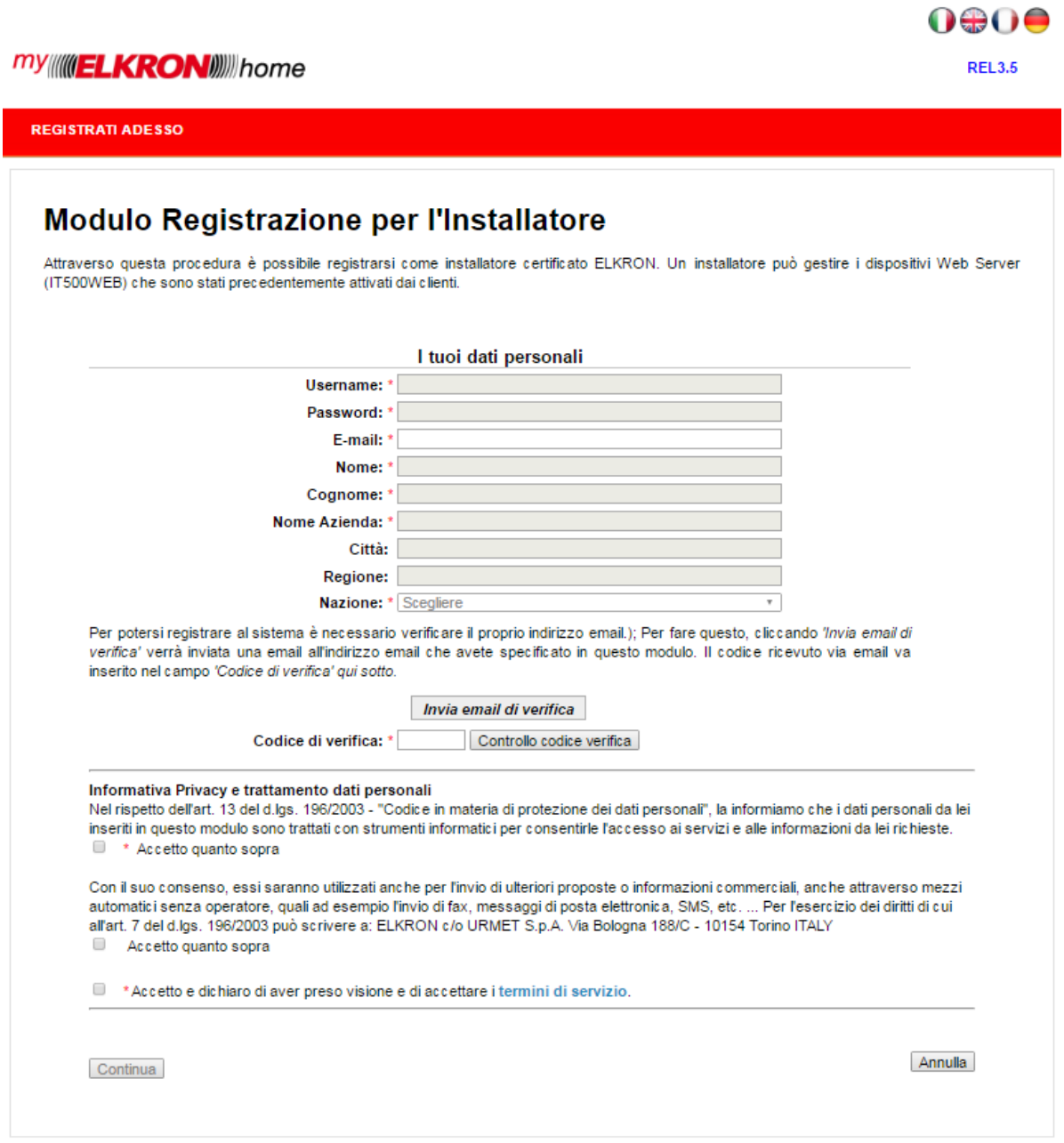
Registrazione del server

Per l'utilizzo del Web Server da remoto è necessario registrare il dispositivo sul portale www.myelkronhome.com.

Il dispositivo può essere registrato solo dall'installatore, è necessario pertanto che l'installatore disponga di un account (si veda la sezione "Registrazione Installatore" per ulteriori dettagli).

Registrazione Installatore

Per registrare un account installatore, accedere al portale www.myelkronhome.com e selezionare la voce "REGISTRATI ADESSO". Si aprirà la seguente schermata:



Inserire un indirizzo email valido dell'installatore nel campo "E-mail" e cliccare "Invia email di verifica". Inserire nel campo "Codice di verifica" il codice ricevuto via email (se la mail non arriva entro pochi minuti, controllare la cartella della posta indesiderata) e cliccare "Controllo codice verifica". A questo punto si abiliteranno tutti gli altri campi. Inserire almeno tutti i dati obbligatori (contrassegnati da un asterisco) e spuntare almeno le caselle relative alla privacy e al trattamento dei dati personali (contrassegnate anch'esse da un asterisco).

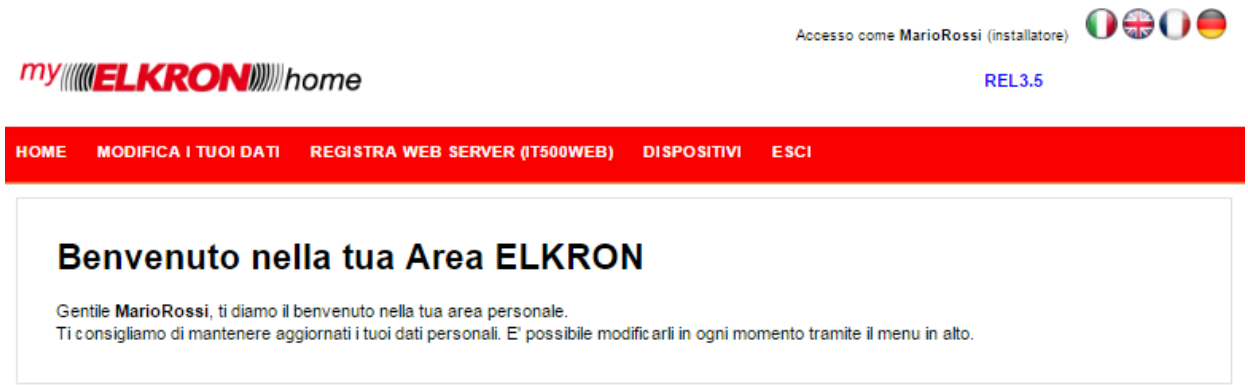
La password deve rispettare i seguenti criteri di sicurezza:

- Deve essere lunga almeno 8 caratteri.
- Deve contenere almeno una lettera maiuscola.
- Deve contenere almeno una lettera minuscola.
- Deve contenere almeno un carattere speciale.
- Deve contenere almeno una cifra.
- Lo username non può essere contenuto nella password.

Premere "Continua" per terminare la procedura di registrazione o "Annulla" per annullare.
Al termine della procedura si riceverà una mail di conferma registrazione avvenuta.

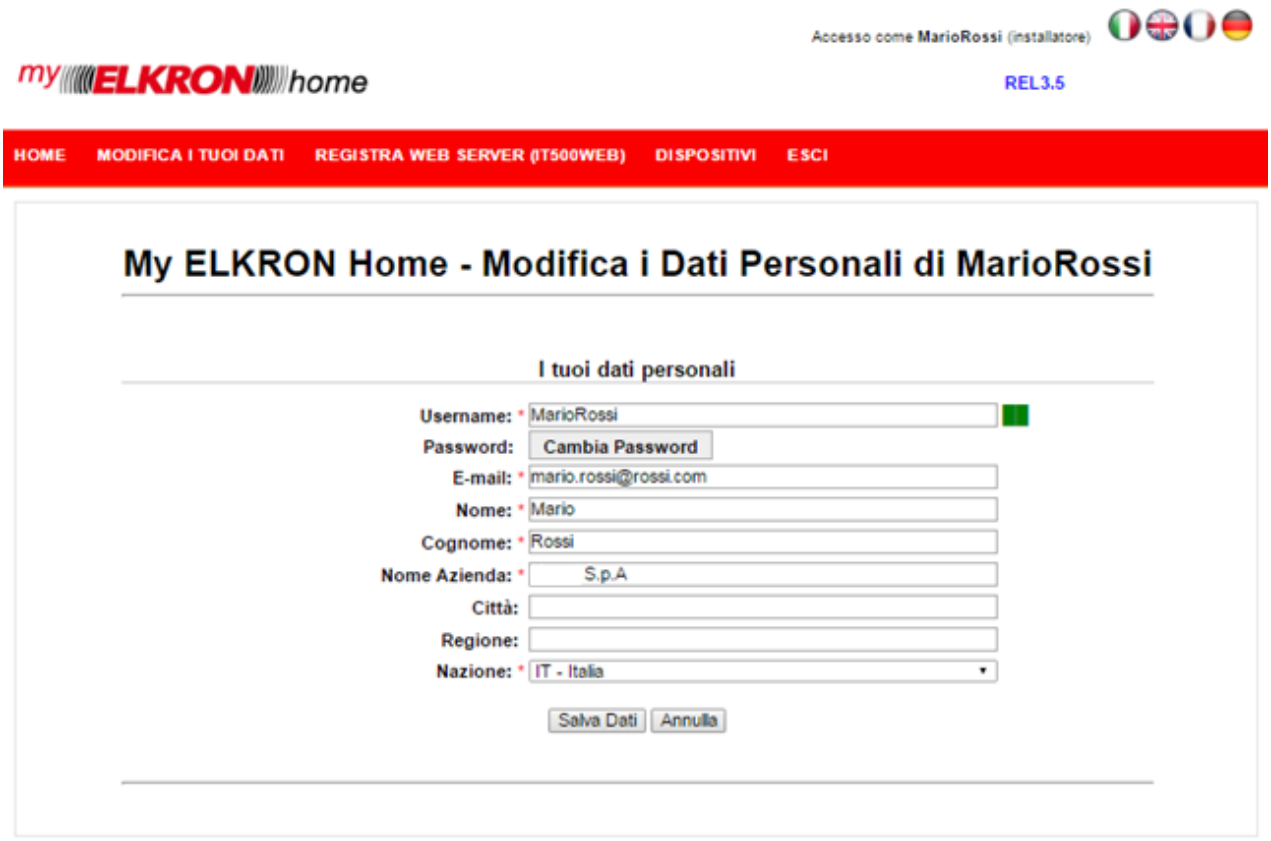
Accesso Installatore

Sezione Home



Dopo aver effettuato il login, l'installatore viene reindirizzato alla sua Home.
Da qui può accedere alla sezione per gestire i propri dati ("MODIFICA I TUOI DATI"), può effettuare la registrazione di un nuovo Web Server ("REGISTRA WEB SERVER (IT500WEB)"), può gestire i suoi dispositivi e quelli dei suoi clienti ("DISPOSITIVI") o può effettuare un logout ("ESCI").

Sezione Modifica i tuoi dati

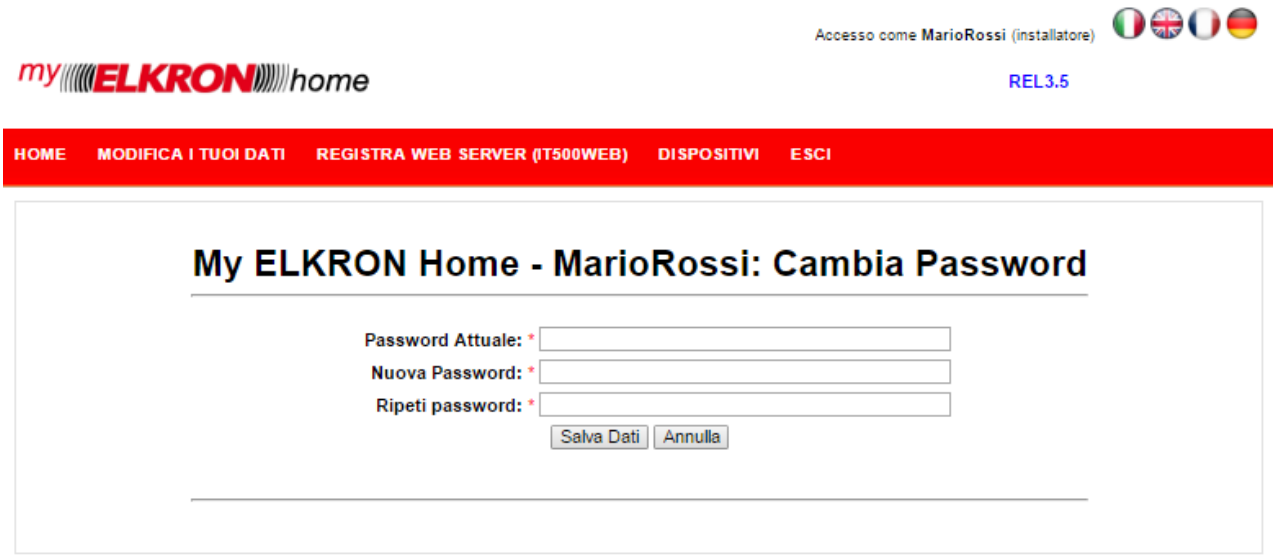


In questa pagina l'installatore può aggiornare i suoi dati personali.

Lo username deve rispettare i seguenti criteri di sicurezza:

- Deve essere lungo almeno 6 caratteri.
- Deve essere lungo al massimo 30 caratteri
- Sono ammessi, ma non obbligatori, i seguenti e solo questi caratteri speciali: - _ & @ .
- Non sono ammessi nomi utente che inizino con w00_1E_E0_

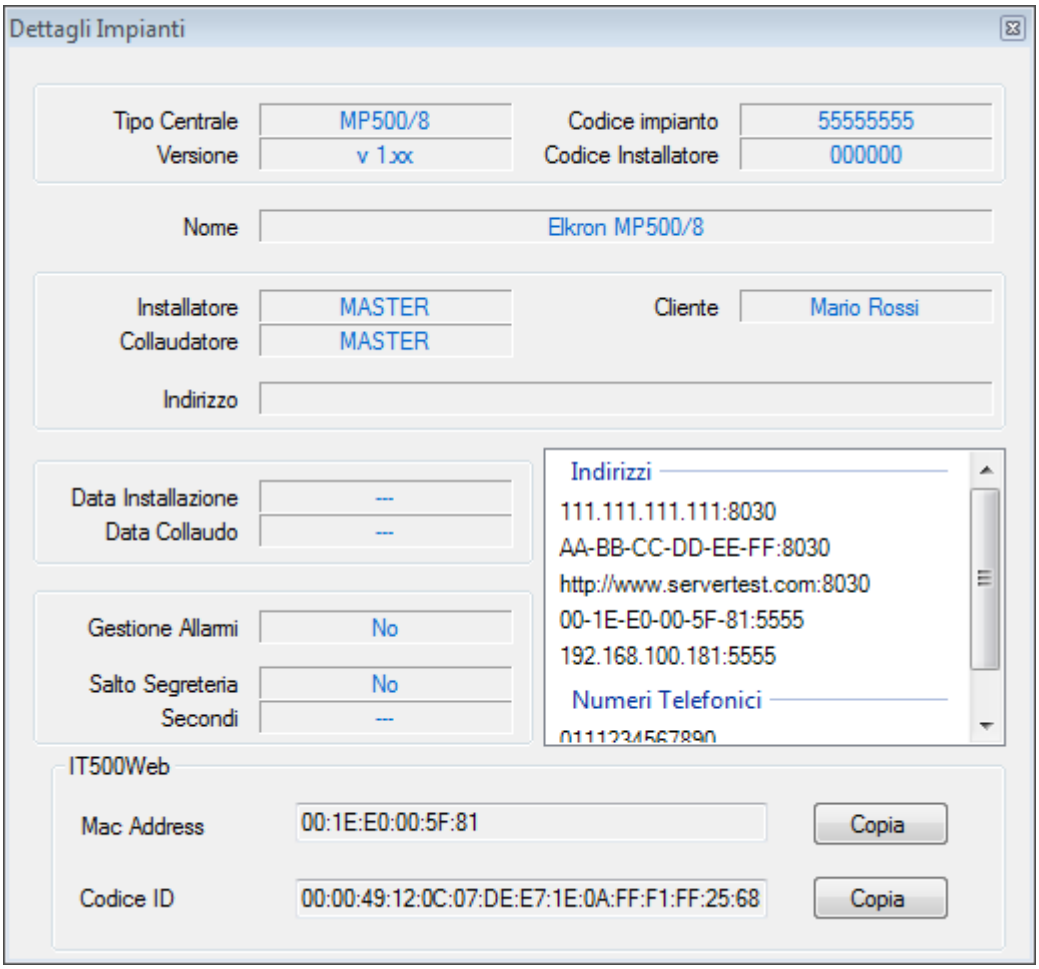
Per cambiare la password è necessario cliccare il tasto “Cambia password”, mentre tutti gli altri dati sono editabili da qui. Per confermare le eventuali modifiche cliccare il tasto “Salva Dati”.



Per cambiare la password è necessario inserire la password attualmente in uso, la nuova password e la conferma della nuova password. Cliccare “Salva Dati” per confermare la modifica.

Sezione Registra Web Server (IT500WEB)

In questa sezione vanno inseriti i dati relativi al dispositivo da registrare. Verranno richiesti i seguenti dati: Mac Address, Codice ID e indirizzo web ed indirizzo email del cliente.
I primi due possono essere reperiti nella pagina “Dettagli Impianti” di Hi-Connect.



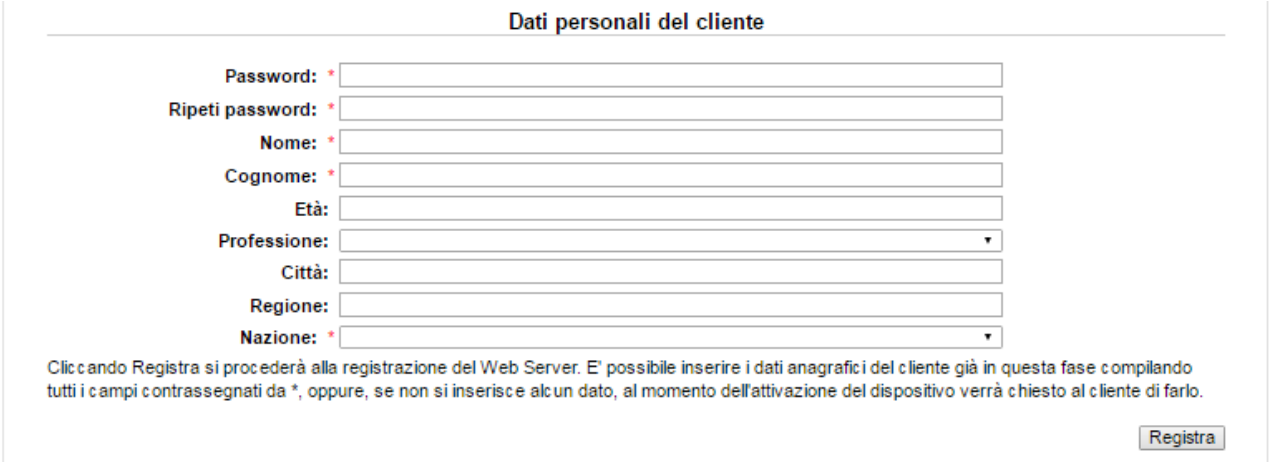
L’indirizzo web deve essere scelto dall’utente e sarà utilizzato in futuro per accedere all’impianto tramite rete esterna. Ad esempio, se si sceglie come indirizzo “webserver”, si potrà accedere al proprio impianto digitando nel browser http://webserver.myelkronhome.com.

Inserire tutti i dati richiesti e cliccare “Verifica”.

⚠ **ATTENZIONE!** E' importante inserire l'indirizzo email valido e attivo del cliente, al fine di evitare malfunzionamenti nel sistema.
Cliccare "Verifica". Se i dati inseriti sono corretti, comparirà un form da compilare con i dati anagrafici del cliente. E' possibile compilare almeno tutti i campi obbligatori (contrassegnati da un *) o lasciare tutto in bianco e procedere con la registrazione. Verrà creato automaticamente un account utente ed una email di riepilogo verrà inviata all'indirizzo indicato. Per attivare il Web Server è necessario che il cliente clicchi sul link ricevuto via email. Si veda la sezione "Accesso CLIENTE" per ulteriori informazioni.

⚠ **ATTENZIONE!** Qualora l'indirizzo email indicato risultasse già presente nel sistema, i dati anagrafici del cliente saranno visualizzati per riepilogo e non saranno modificabili. In questo caso non verrà creato un nuovo account utente e il Web Server appena registrato verrà associato all'utente già presente nel sistema. Sarà in ogni caso necessario cliccare il link ricevuto via email per attivare il dispositivo.

⚠ **ATTENZIONE!** Qualora si indicasse l'indirizzo email dell'installatore, il Web Server sarà automaticamente considerato come di sua proprietà e non saranno inviate email di conferma. Il dispositivo sarà attivato automaticamente.



Cliccare "Registra" per completare la procedura di registrazione.

Sezione Dispositivi

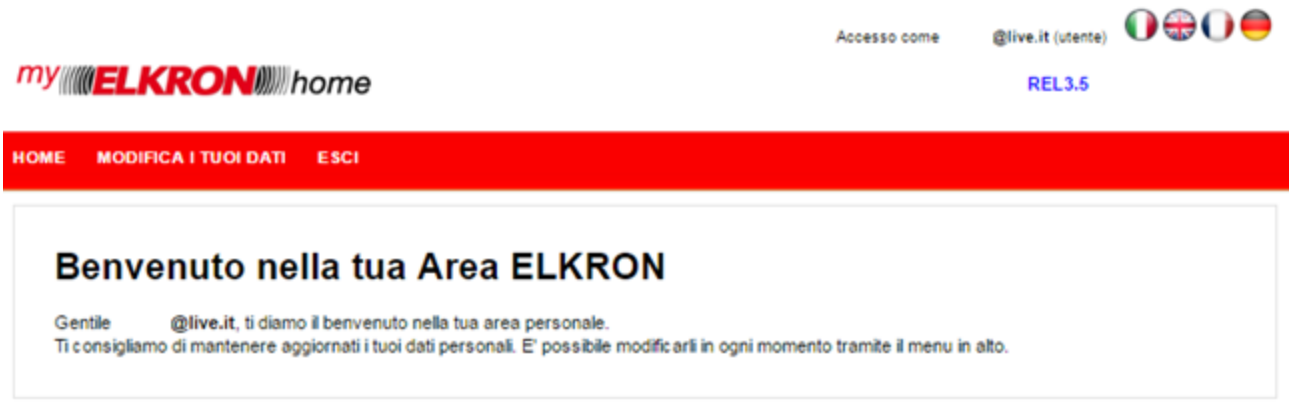
La pagina “DISPOSITIVI” è divisa in due sezioni: nella prima sono elencati i Web Server di proprietà dell’installatore, per i quali quindi lui stesso è il cliente finale / utilizzatore, nella seconda sono elencati i dispositivi dei suoi clienti ma che l’installatore è abilitato a telegestire. Da questa è possibile:

- Richiedere un nuovo invio della mail contenente il link da cliccare per attivare il Web Server subito dopo la sua registrazione (utile qualora l’utente non riceva la mail o la cancelli per errore prima di cliccare il link). Il tasto “Reinvia e-mail di attivazione” è disponibile solo per i dispositivi non ancora attivati. Una volta cliccato il link, il pulsante non sarà più visualizzato.
- Richiedere la cancellazione della registrazione di un impianto tramite il pulsante elimina (icona a forma di cestino). Per confermare la cancellazione di un Web Server, il cliente dovrà cliccare un link ricevuto via mail.
- Richiedere un nuovo invio della mail contenente il link da cliccare per confermare la cancellazione del Web server. Il tasto “Reinvia e-mail di conferma” è disponibile solo per i dispositivi per i quali è stata chiesta la cancellazione e solo finchè il cliente non confermi l’operazione cliccando il link ricevuto tramite email.

⚠ **ATTENZIONE!** Qualora il Web Server da cancellare fosse dell’installatore, quindi elencato nella prima sezione, non sarà inviata una email con un link da cliccare per confermare, e la cancellazione sarà confermata automaticamente.

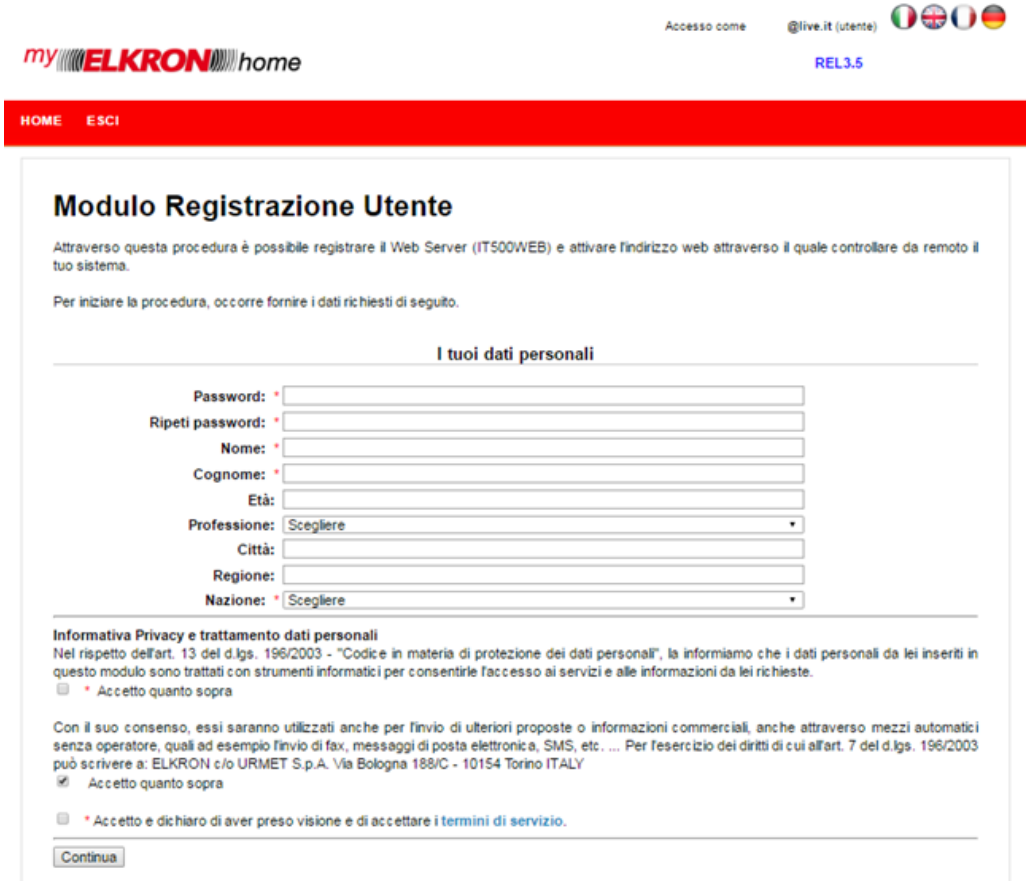
Accesso Cliente

Sezione Home

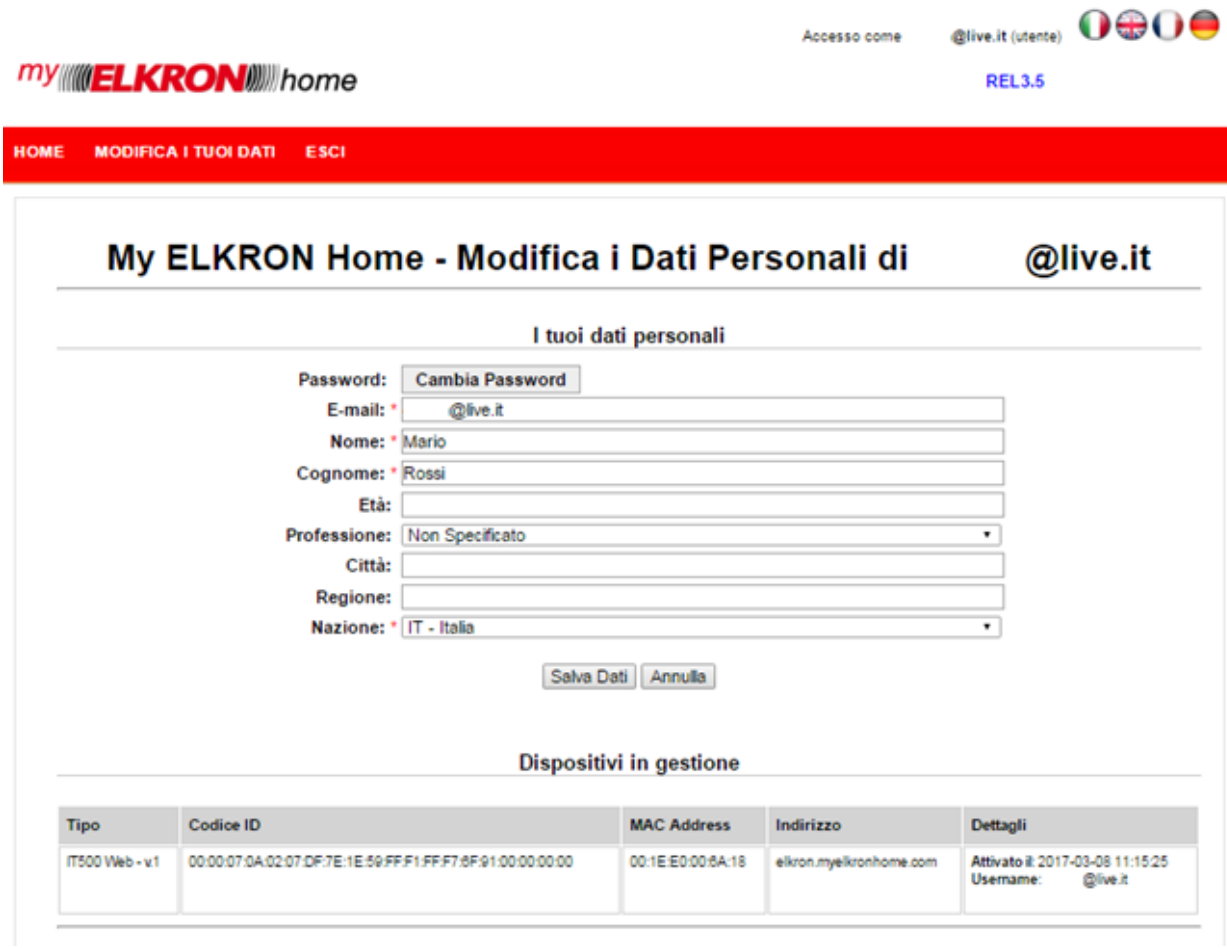


Dopo aver effettuato il login, il cliente viene reindirizzato alla sua Home. Da qui può accedere alla sezione per gestire i propri dati (“Modifica i tuoi dati”) o può effettuare un logout (“Esci”).

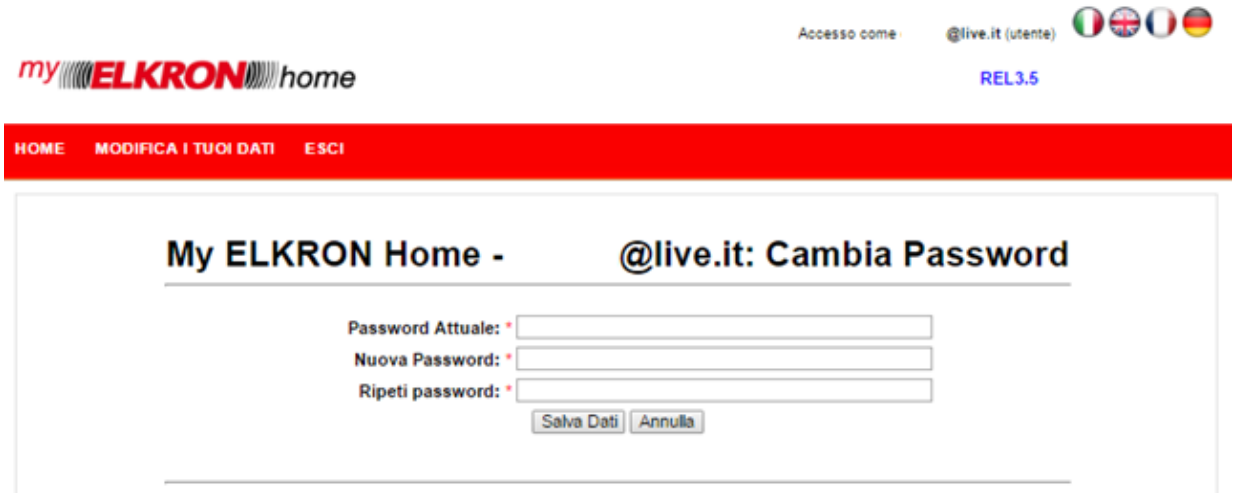
Al primo accesso, verrà chiesto di confermare i dati inseriti dall’installatore in fase di registrazione del Web Server (IT500WEB) o di inserirli qualora l’installatore non l’abbia già fatto. Se ci sono operazioni in corso, quali la conferma di registrazione o cancellazione, queste verranno automaticamente confermate a seguito dell’accesso fatto tramite il link ricevuto via email e dopo aver eventualmente confermato i dati in caso di primo accesso.



Sezione Modifica i tuoi dati



In questa pagina il cliente può visualizzare il dettaglio del proprio dispositivo IT500WEB e aggiornare i dati personali.
Per cambiare la password è necessario cliccare il tasto “Cambia password”, mentre tutti gli altri dati sono editabili da qui. Per confermare le eventuali modifiche cliccare il tasto “Salva Dati”.



Per cambiare la password è necessario inserire la password attualmente in uso, la nuova password e la conferma della nuova password. Cliccare “Salva Dati” per confermare la modifica.

Schemi centrali Elkron per applicazioni Domotica

La domotica integrata (Yokis/Elkron) permette di tenere sotto controllo la casa a distanza tramite telefono, Smartphone, tablet o computer e consente di inviare messaggi di emergenza.

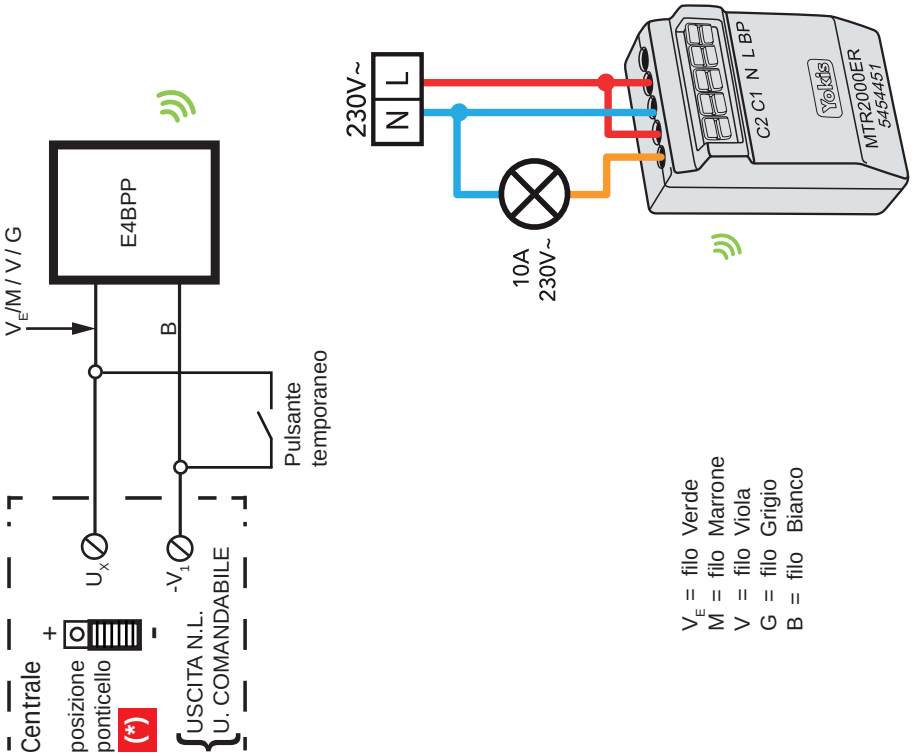
L'automazione, permette di migliorare e di effettuare un controllo ed un monitoraggio intelligente ed efficiente con la centralizzazione dei comandi.

Questi impianti, espandibili nel tempo, permettono la gestione di carichi:

- Controllo accensioni, temporizzazioni, spegnimento e scenari illuminazione delle luci;
- Gestione tapparelle, motorizzazioni (apertura e chiusura);
- Centralizzazione di comandi;
- Efficienza nell'impiego dell'energia elettrica e nei consumi elettrici.

Comando ON/OFF di un MTR2000ER via radio, da un canale E4BPP

Cablaggio di un E4BPP alla centrale con uscita elettrica



(*) ATTENZIONE: CONFIGURAZIONE HW CENTRALE

IMPORTANTE
Nel caso di utilizzo di un'uscita elettrica di Centrale è indispensabile spostare il ponticello corrispondente in posizione "-" prima di collegare il trasmettitore. In caso contrario quest'ultimo si danneggerà irreparabilmente.

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COMANDABILE

COLLEGAMENTO DIRETTO

Sul pulsante temporaneo collegato al trasmettitore, fare 5 pressioni brevi. Il led del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.

Mentre il led del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "connect" dell'MTR2000ER, situato nella parte posteriore.
Il led del trasmettitore smetterà di lampeggiare.

Attenzione! È indispensabile che il ricevitore sia alimentato.

CONFIGURAZIONE DELLA MODALITÀ ISTANTANEA (=ON/OFF)

Sul pulsante temporaneo collegato al trasmettitore, fare 10 pressioni brevi per entrare nel Menu di Configurazione: il led del trasmettitore lampeggerà velocemente.

Mentre il led lampeggia, esercitare 17 pressioni brevi sul pulsante: risposta 7 lampeggi del led del trasmettitore.

Da questo momento la luce collegata all'MTR2000ER sarà correttamente pilotata dalla centrale o dall'espansione in modalità ON/OFF.

SD541-9000

Comando ON/OFF di un MTR2000ER via radio, da un canale E4BPP

Cablaggio di un E4BPP alla centrale/espansione con uscita relè

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COMANDABILE

COLLEGAMENTO DIRETTO

Sul pulsante temporaneo collegato al trasmettitore, fare 5 pressioni brevi. Il led del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.

Mentre il led del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "connect" dell'MTR2000ER, situato nella parte posteriore.
Il led del trasmettitore smetterà di lampeggiare.

Attenzione! È indispensabile che il ricevitore sia alimentato.

CONFIGURAZIONE DELLA MODALITÀ ISTANTANEA (=ON/OFF)

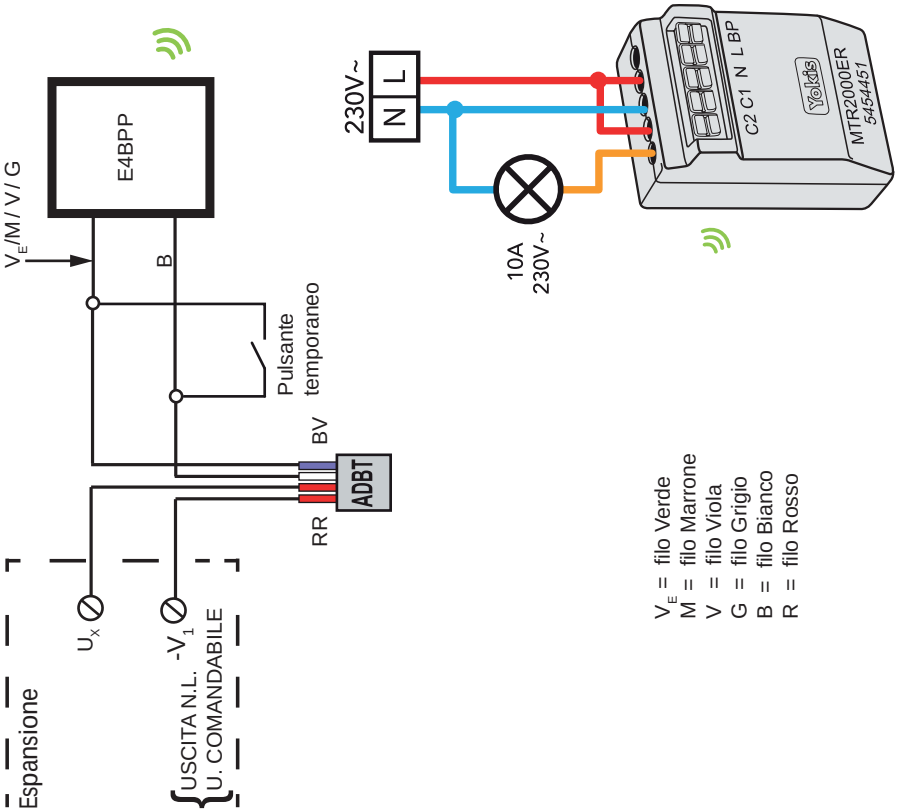
Sul pulsante temporaneo collegato al trasmettitore, fare 10 pressioni brevi per entrare nel Menu di Configurazione: il led del trasmettitore lampeggerà velocemente.

Mentre il led lampeggia, esercitare 17 pressioni brevi sul pulsante: risposta 7 lampeggi del led del trasmettitore.

Da questo momento la luce collegata all'MTR2000ER sarà correttamente pilotata dalla centrale o dall'espansione in modalità ON/OFF.

Comando ON/OFF di un MTR2000ER via radio, da un canale E4BPP

Cablaggio di un E4BPP all'espansione con uscita elettrica



CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COMANDABILE

COLLEGAMENTO DIRETTO

Sul pulsante temporaneo collegato al trasmettitore, fare 5 pressioni brevi. Il led del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.

Mentre il led del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "connect" dell'MTR2000ER, situato nella parte posteriore.
Il led del trasmettitore smetterà di lampeggiare.

Attenzione! È indispensabile che il ricevitore sia alimentato.

CONFIGURAZIONE DELLA MODALITÀ ISTANTANEA (=ON/OFF)

Sul pulsante temporaneo collegato al trasmettitore, fare 10 pressioni brevi per entrare nel Menu di Configurazione: il led del trasmettitore lampeggerà velocemente.

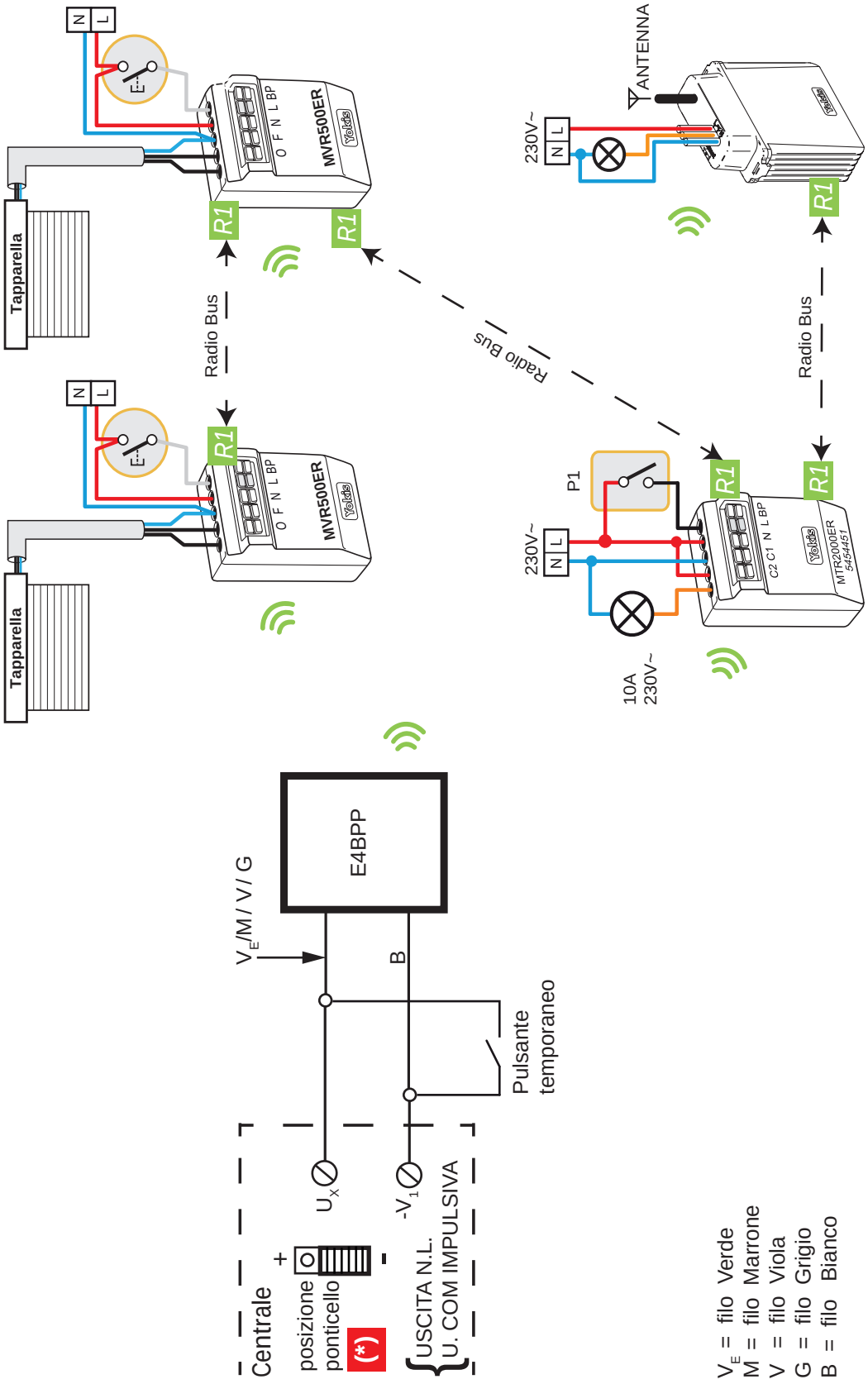
Mentre il led lampeggia, esercitare 17 pressioni brevi sul pulsante: risposta 7 lampeggi del led del trasmettitore.

Da questo momento la luce collegata all'MTR2000ER sarà correttamente pilotata dalla centrale o dall'espansione in modalità ON/OFF.

SD541-9002

Comando centralizzato di apertura o chiusura di luci e/o tapparelle

Cablaggio di un E4BPP alla centrale con uscita elettrica



SD541-9003 (Foglio 1/2)

(*) ATTENZIONE: CONFIGURAZIONE HW CENTRALE

IMPORTANTE
Nel caso di utilizzo di un'uscita elettrica di Centrale è indispensabile spostare il ponticello corrispondente in posizione " - " prima di collegare il trasmettitore. In caso contrario quest'ultimo si danneggerà irreparabilmente.

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

R1-R1 - Definire il Bus Radio collegando i ricevitori tra di loro

Esercitare una pressione rapida su "Connect" del ricevitore 1. Il suo LED inzia a lampeggiare (R1).
Mentre il LED lampeggia, premere su "Connect" sul ricevitore 2 (R1). Per confermare il collegamente, il LED del ricevitore 2 lampeggia una sola volta e il LED del ricevitore 1 smette di lampeggiare; a collegamento avvenuto, entrambi i moduli reagiscono (lampeggio dei moduli di illuminazione oppure breve movimento della tapparella).

E5 - Collegare il trasmettitore al ricevitore più vicino

Esercitare 5 pressioni rapide sul pulsante temporaneo connesso al trasmettitore (E5).
Il LED del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.
Mentre il LED del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "Connect" del ricevitore più vicino.
il LED del trasmettitore smetterà di lampeggiare. La luce connessa al modulo lampeggierà oppure la tapparella farà un breve movimento.

Attenzione! È indispensabile che il ricevitore sia alimentato.

M6 - Configurare il trasmettitore all'invio di un comando centralizzato

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazione (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare 6 pressioni rapide sul pulsante temporaneo (6).
Il LED lampeggia 6 volte per confermare la modalità centralizzata.

M10/M11/M20 - Definire se il comando è per luci, tapparelle o entrambe

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per LUCI: 10 pressioni rapide sul pulsante temporaneo (10) (default).
- Per TAPPARELLE: 11 pressioni rapide sul pulsante temporaneo (11).
- Per LUCE e TAPPARELLE: 20 pressioni rapide sul pulsante temporaneo (20).

Il LED lampeggia per confermare. Rispettivamente: 10, 1, 10 volte.

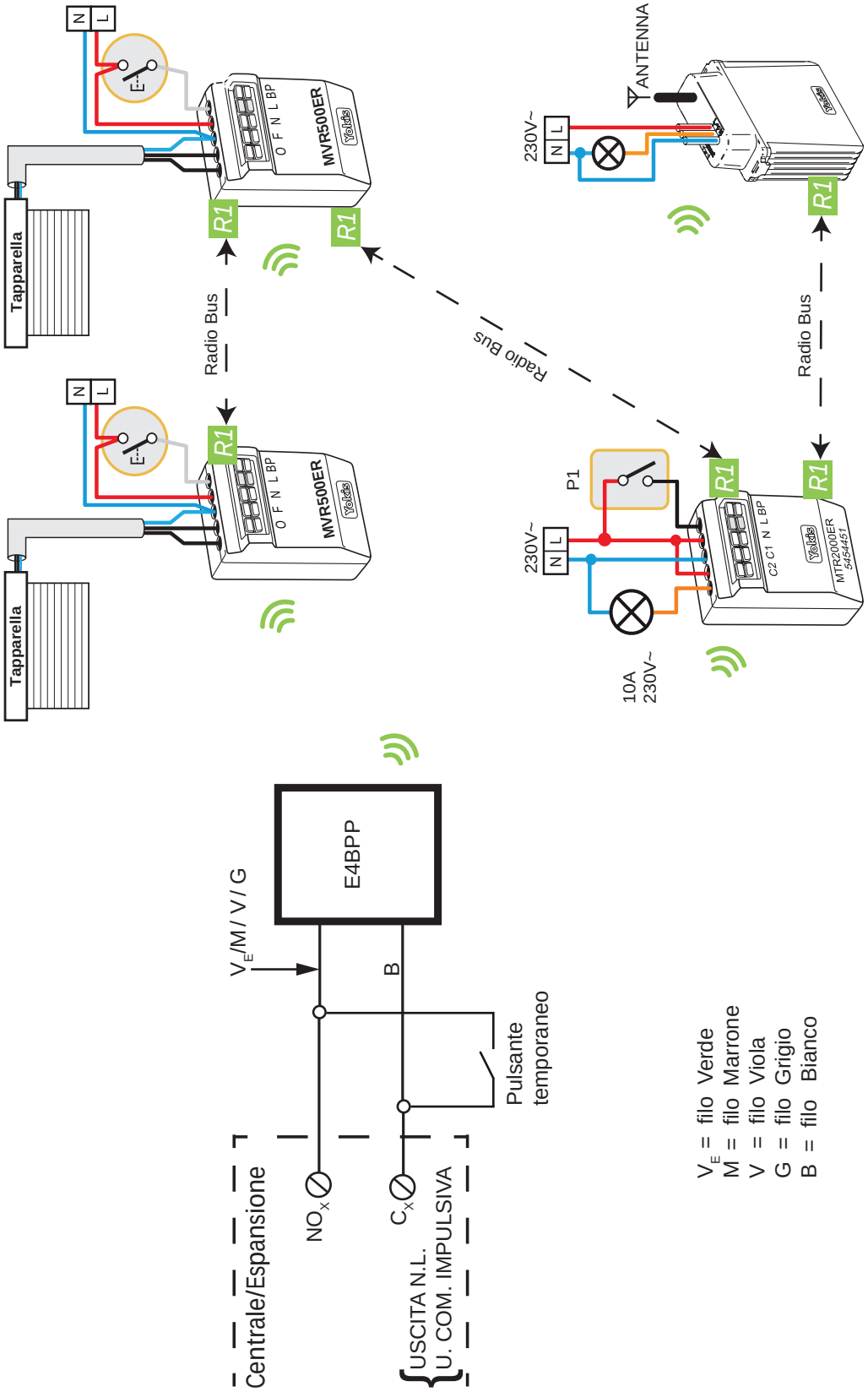
M3/M4 - Definire l'azione: Accensione o Salita / Spegnimento o Discesa

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per Accensione (o Salita tapparelle): 3 pressioni rapide sul pulsante temporaneo (3)
- Per Spegnimento (o Discesa tapparelle): 4 pressioni rapide sul pulsante temporaneo (4)

Il LED lampeggia per confermare : 3 o 4 volte

Comando centralizzato di apertura o chiusura di luci e/o tapparelle

Cablaggio di un E4BPP alla centrale/espansione con uscita relè



SD541-9004 (Foglio 1/2)

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

R1-R1 - Definire il Bus Radio collegando i ricevitori tra di loro

Esercitare una pressione rapida su "Connect" del ricevitore 1. Il suo LED inzia a lampeggiare (R1).
Mentre il LED lampeggia, premere su "Connect" sul ricevitore 2 (R1). Per confermare il collegamente, il LED del ricevitore 2 lampeggia una sola volta e il LED del ricevitore 1 smette di lampeggiare; a collegamento avvenuto, entrambi i moduli reagiscono (lampeggio dei moduli di illuminazione oppure breve movimento della tapparella).

E5 - Collegare il trasmettitore al ricevitore più vicino

Esercitare 5 pressioni rapide sul pulsante temporaneo connesso al trasmettitore (E5).
Il LED del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.
Mentre il LED del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "Connect" del ricevitore più vicino.
il LED del trasmettitore smetterà di lampeggiare. La luce connessa al modulo lampeggierà oppure la tapparella farà un breve movimento.

Attenzione! È indispensabile che il ricevitore sia alimentato.

M6 - Configurare il trasmettitore all'invio di un comando centralizzato

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazione (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare 6 pressioni rapide sul pulsante temporaneo (6).
Il LED lampeggia 6 volte per confermare la modalità centralizzata.

M10/M11/M20 - Definire se il comando è per luci, tapparelle o entrambe

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per LUCI: 10 pressioni rapide sul pulsante temporaneo (10) (default).
- Per TAPPARELLE: 11 pressioni rapide sul pulsante temporaneo (11).
- Per LUCE e TAPPARELLE: 20 pressioni rapide sul pulsante temporaneo (20).

Il LED lampeggia per confermare. Rispettivamente: 10, 1, 10 volte.

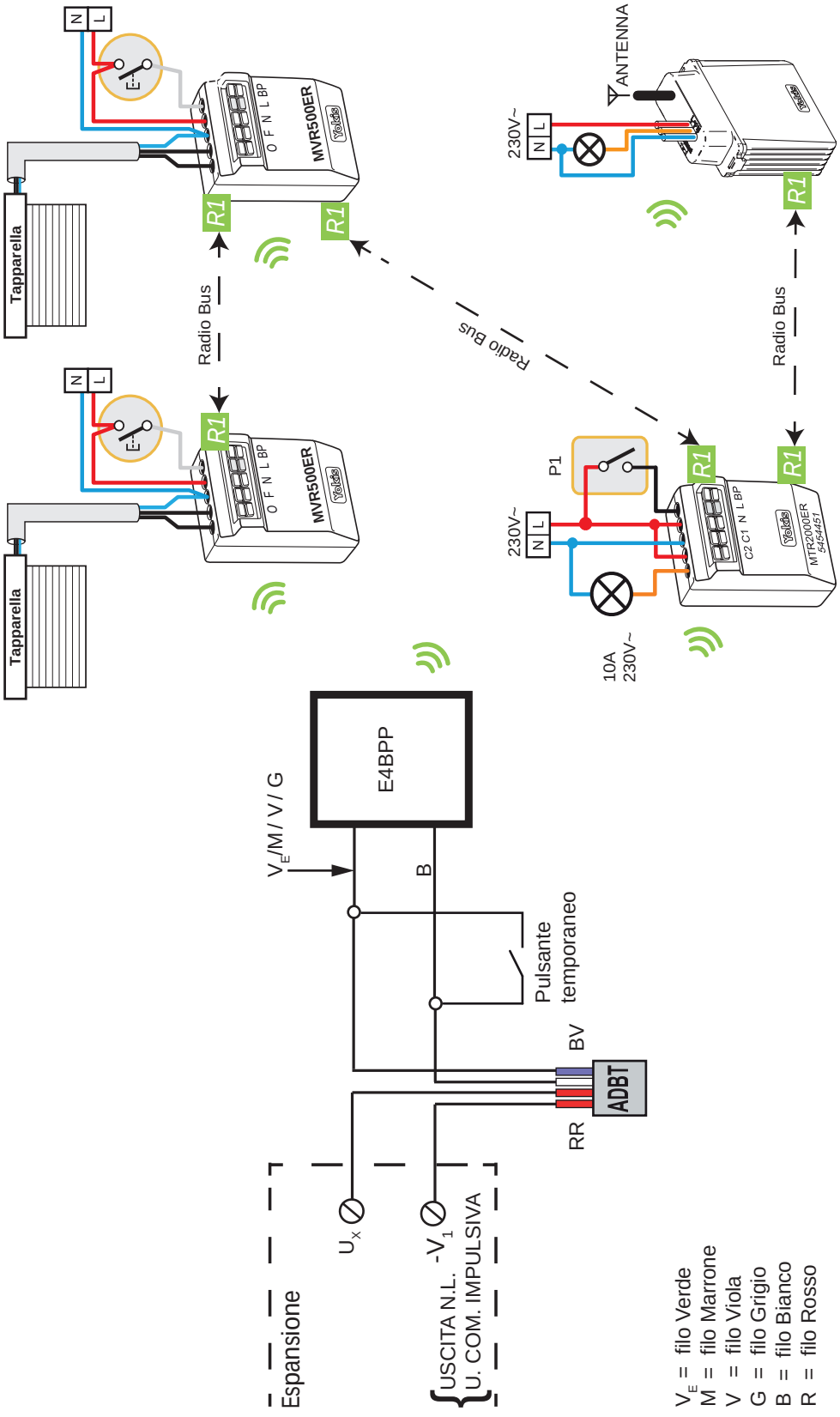
M3/M4 - Definire l'azione: Accensione o Salita / Spegnimento o Discesa

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per Accensione (o Salita tapparelle): 3 pressioni rapide sul pulsante temporaneo (3)
- Per Spegnimento (o Discesa tapparelle): 4 pressioni rapide sul pulsante temporaneo (4)

Il LED lampeggia per confermare : 3 o 4 volte

Comando centralizzato di apertura o chiusura di luci e/o tapparelle

Cablaggio di un E4BPP all'espansione con uscita elettrica



SD541-9005 (Foglio 1/2)

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

R1-R1 - Definire il Bus Radio collegando i ricevitori tra di loro

Esercitare una pressione rapida su "Connect" del ricevitore 1. Il suo LED inzia a lampeggiare (R1).
Mentre il LED lampeggia, premere su "Connect" sul ricevitore 2 (R1). Per confermare il collegamente, il LED del ricevitore 2 lampeggia una sola volta e il LED del ricevitore 1 smette di lampeggiare; a collegamento avvenuto, entrambi i moduli reagiscono (lampeggio dei moduli di illuminazione oppure breve movimento della tapparella).

E5 - Collegare il trasmettitore al ricevitore più vicino

Esercitare 5 pressioni rapide sul pulsante temporaneo connesso al trasmettitore (E5).
Il LED del trasmettitore inizierà a lampeggiare, per 30 secondi, indicando così l'attesa di una connessione.
Mentre il LED del trasmettitore lampeggia, fare una breve pressione con la punta di una matita nel foro "Connect" del ricevitore più vicino.
il LED del trasmettitore smetterà di lampeggiare. La luce connessa al modulo lampeggierà oppure la tapparella farà un breve movimento.

Attenzione! È indispensabile che il ricevitore sia alimentato.

M6 - Configurare il trasmettitore all'invio di un comando centralizzato

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazione (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare 6 pressioni rapide sul pulsante temporaneo (6).
Il LED lampeggia 6 volte per confermare la modalità centralizzata.

M10/M11/M20 - Definire se il comando è per luci, tapparelle o entrambe

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per LUCI: 10 pressioni rapide sul pulsante temporaneo (10) (default).
- Per TAPPARELLE: 11 pressioni rapide sul pulsante temporaneo (11).
- Per LUCE e TAPPARELLE: 20 pressioni rapide sul pulsante temporaneo (20).

Il LED lampeggia per confermare. Rispettivamente: 10, 1, 10 volte.

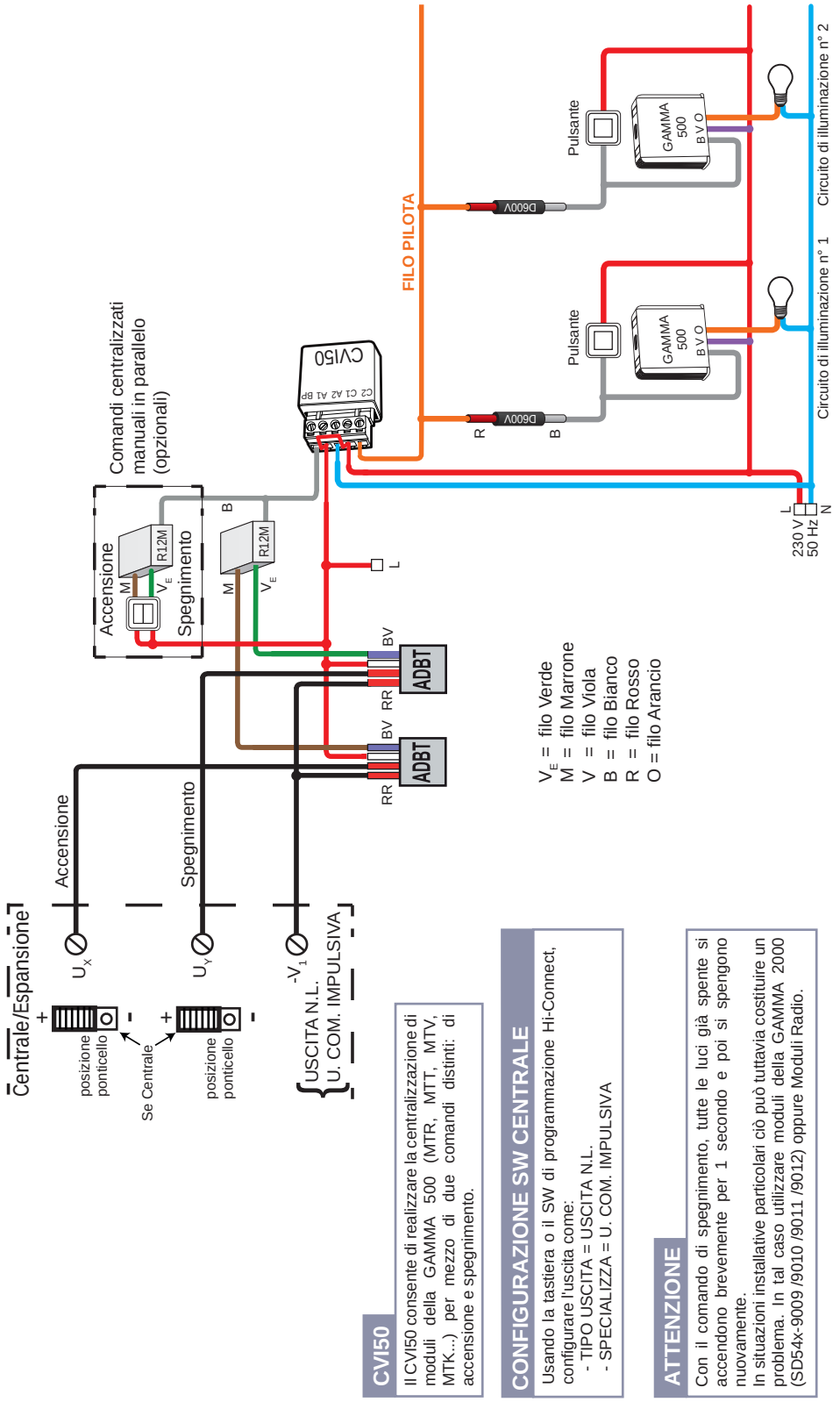
M3/M4 - Definire l'azione: Accensione o Salita / Spegnimento o Discesa

Esercitare 10 pressioni rapide sul pulsante temporaneo del trasmettitore (Menu configurazioni (M)).
Il LED del trasmettitore lampeggierà velocemente.
Mentre il LED lampeggia, esercitare:
- Per Accensione (o Salita tapparelle): 3 pressioni rapide sul pulsante temporaneo (3)
- Per Spegnimento (o Discesa tapparelle): 4 pressioni rapide sul pulsante temporaneo (4)

Il LED lampeggia per confermare : 3 o 4 volte

Centralizzazione di moduli della GAMMA 500 per mezzo di CVI50 e di due ADBT su centrale/espansione ELKRON

Comando centralizzato di accensione /spegnimento via CVI50 su centrale/espansione con uscite elettriche



CVI50

Il CVI50 consente di realizzare la centralizzazione di moduli della GAMMA 500 (MTR, MTT, MTV, MTK...) per mezzo di due comandi distinti: di accensione e spegnimento.

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

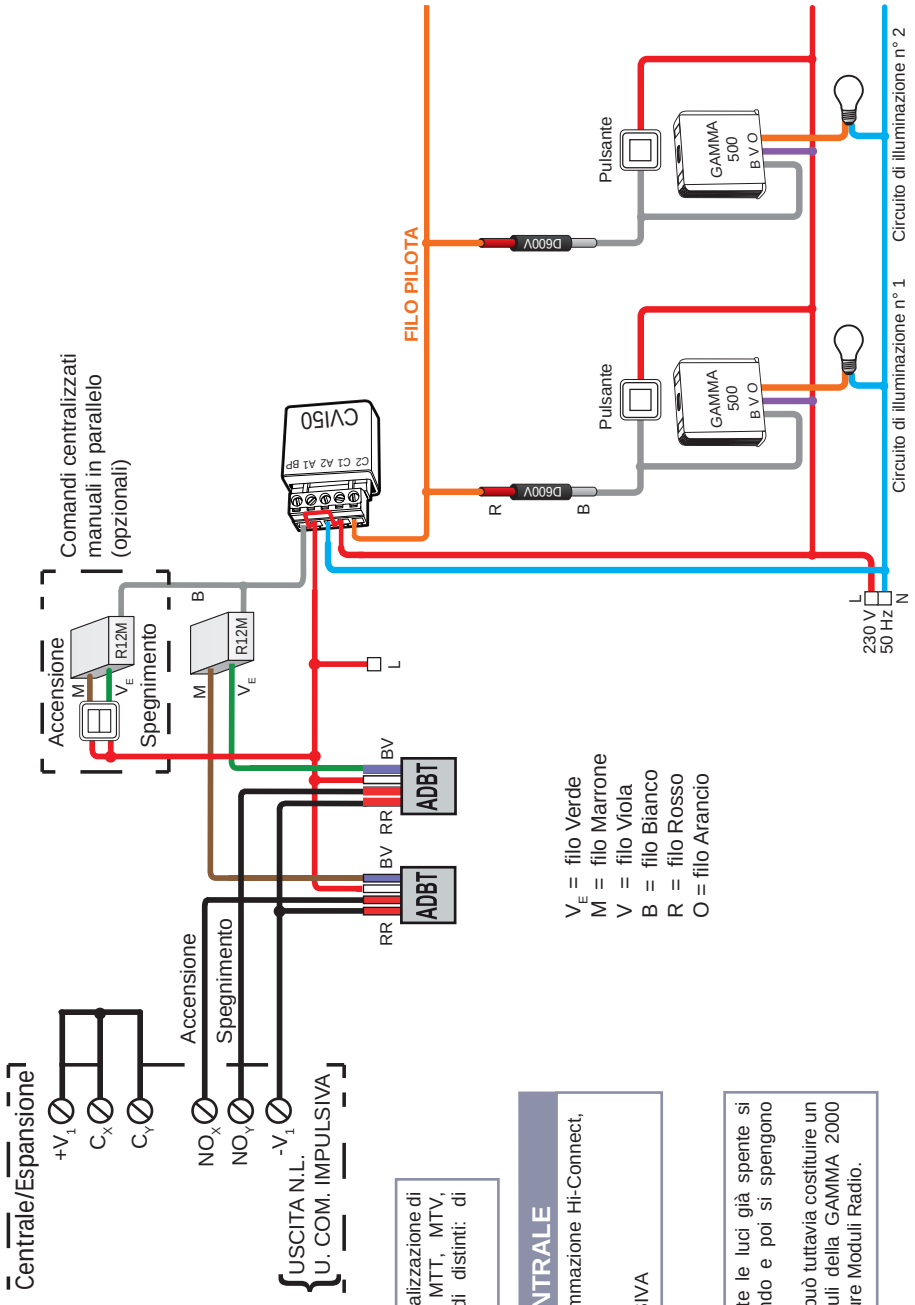
ATTENZIONE

Con il comando di spegnimento, tutte le luci già spente si accendono brevemente per 1 secondo e poi si spengono nuovamente.
In situazioni installative particolari ciò può tuttavia costituire un problema. In tal caso utilizzare moduli della GAMMA 2000 (SD54x-9009 /9010 /9011 /9012) oppure Moduli Radio.

SD541-9006

Centralizzazione di moduli della GAMMA 500 per mezzo di CVI50 e di due ADBT su centrale/espansione ELKRON

Comando centralizzato di accensione /spegnimento via CVI50 su centrale/espansione con uscite a relè



CVI50

Il CVI50 consente di realizzare la centralizzazione di moduli della GAMMA 500 (MTR, MTT, MTV, MTK...) per mezzo di due comandi distinti: di accensione e spegnimento.

CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

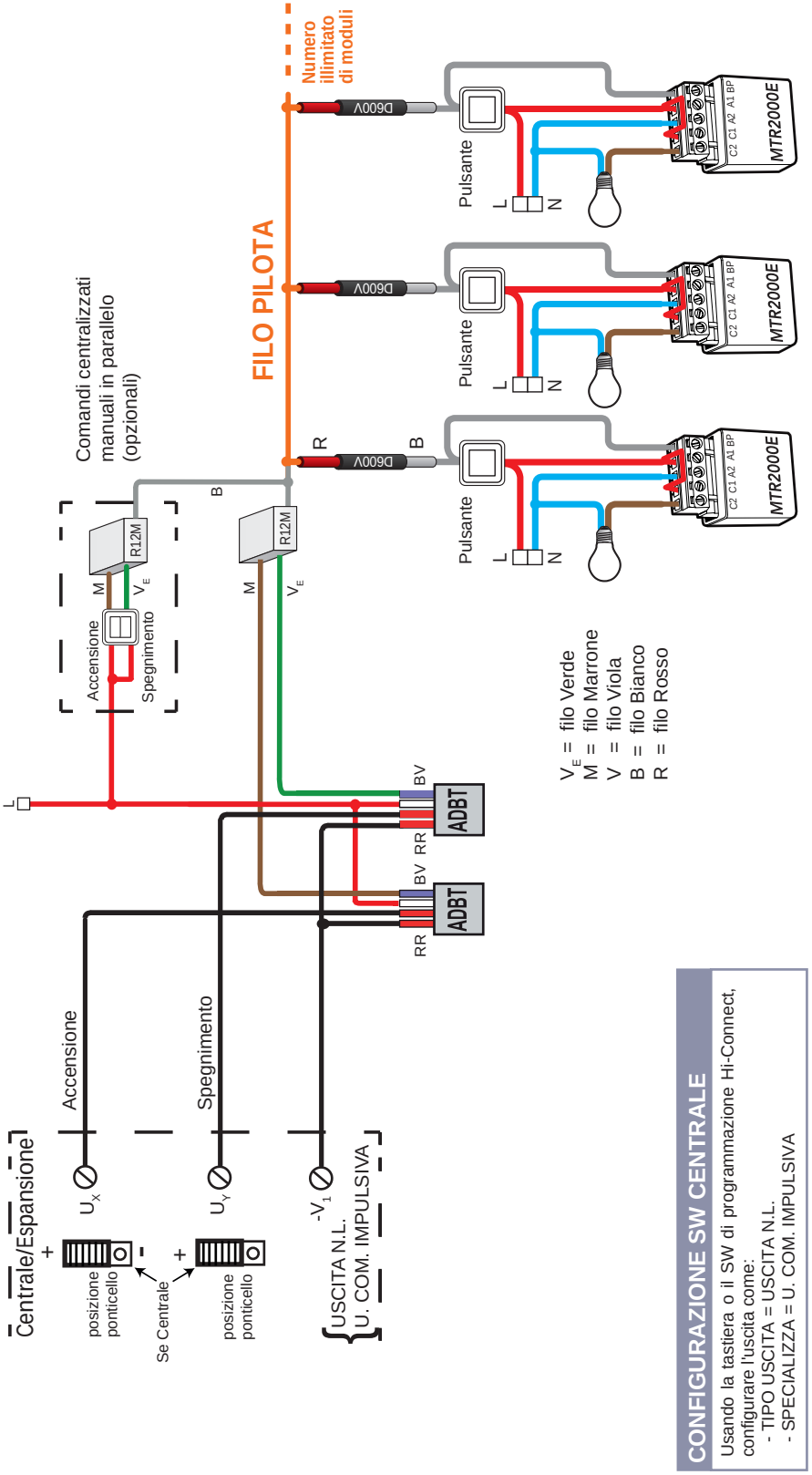
ATTENZIONE

Con il comando di spegnimento, tutte le luci già spente si accendono brevemente per 1 secondo e poi si spengono nuovamente.
In situazioni installative particolari ciò può tuttavia costituire un problema. In tal caso utilizzare moduli della GAMMA 2000 (SD54x-9009 /9010 /9011 /9012) oppure Moduli Radio.

SD541-9007

Cablaggio per la centralizzazione dell'illuminazione con relè MTR2000E da centrale/espansione ELKRON

Cablaggio a 4 fili con comune pulsanti alla fase centrale/espansione con uscite elettriche



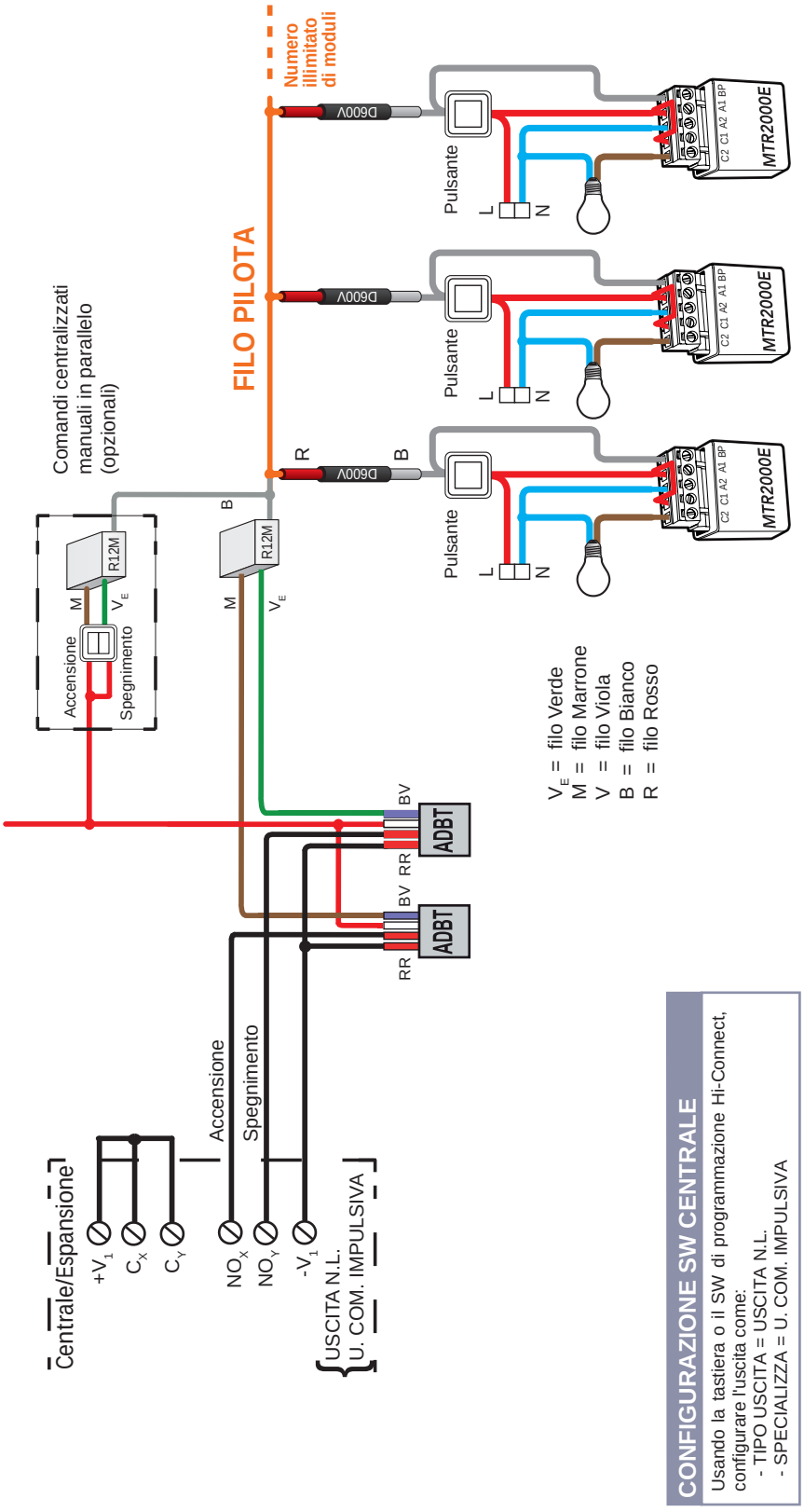
CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

SD541-9008

Cablaggio per la centralizzazione dell'illuminazione con relè MTR2000E da centrale/espansione ELKRON

Cablaggio a 4 fili con comune pulsanti alla fase centrale/espansione con uscite a relè



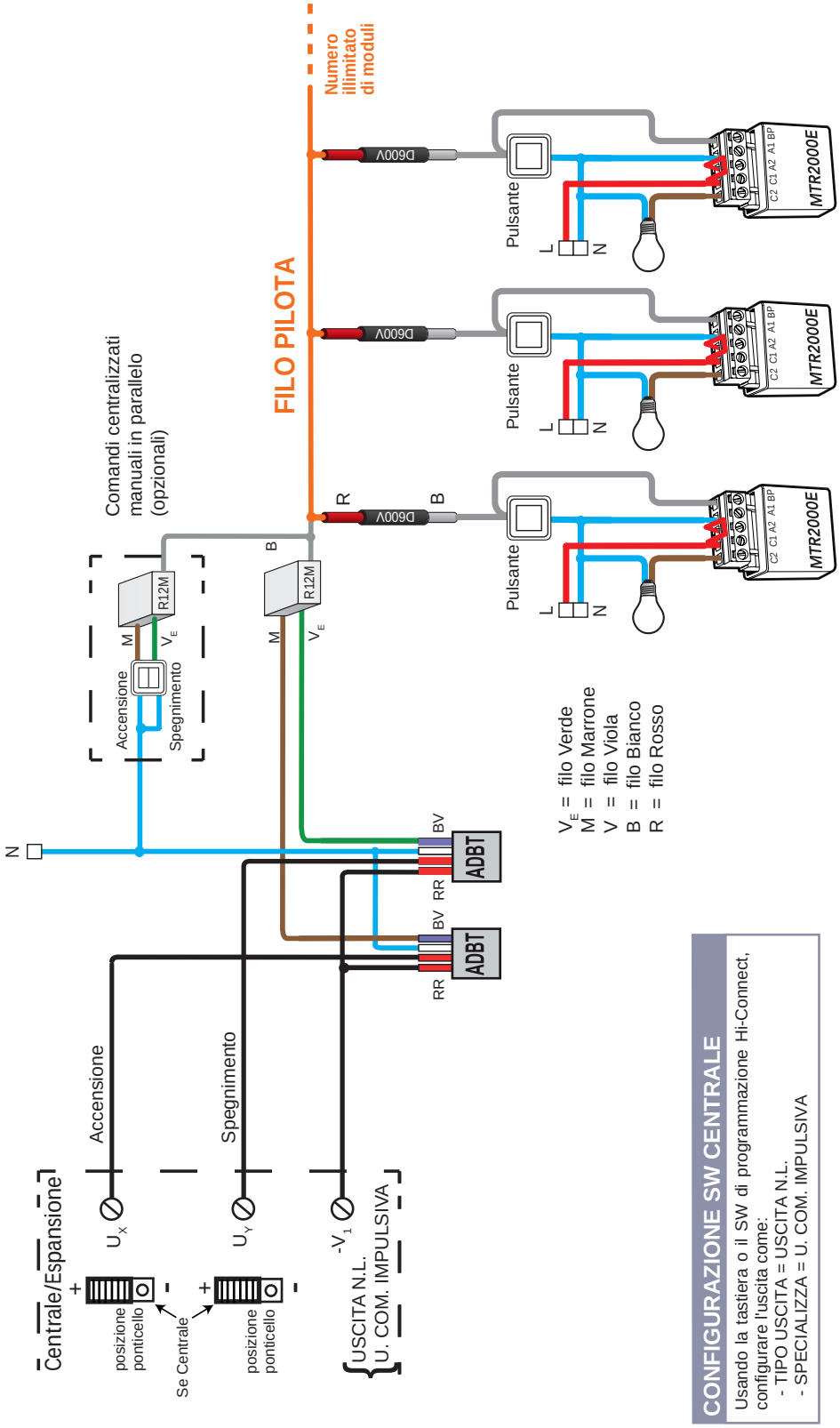
CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

SD541-9009

Cablaggio per la centralizzazione dell'illuminazione con relè MTR2000E da centrale/espansione ELKRON

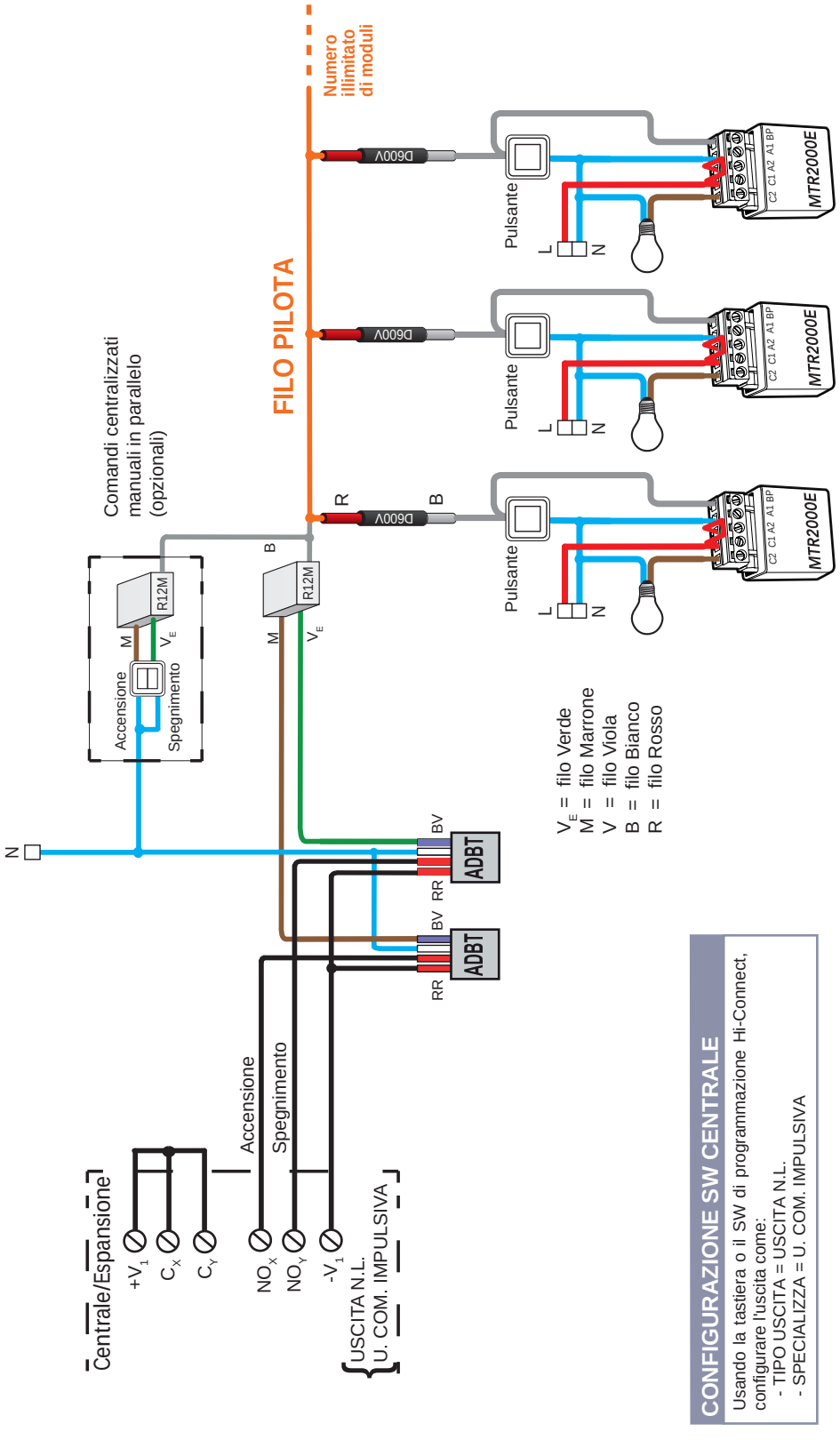
Cablaggio a 3 fili con comune pulsanti al neutro centrale/espansione con uscite elettriche



SD541-9010

Cablaggio per la centralizzazione dell'illuminazione con relè MTR2000E da centrale/espansione ELKRON

Cablaggio a 3 fili con comune pulsanti al neutro centrale/espansione con uscite a relè



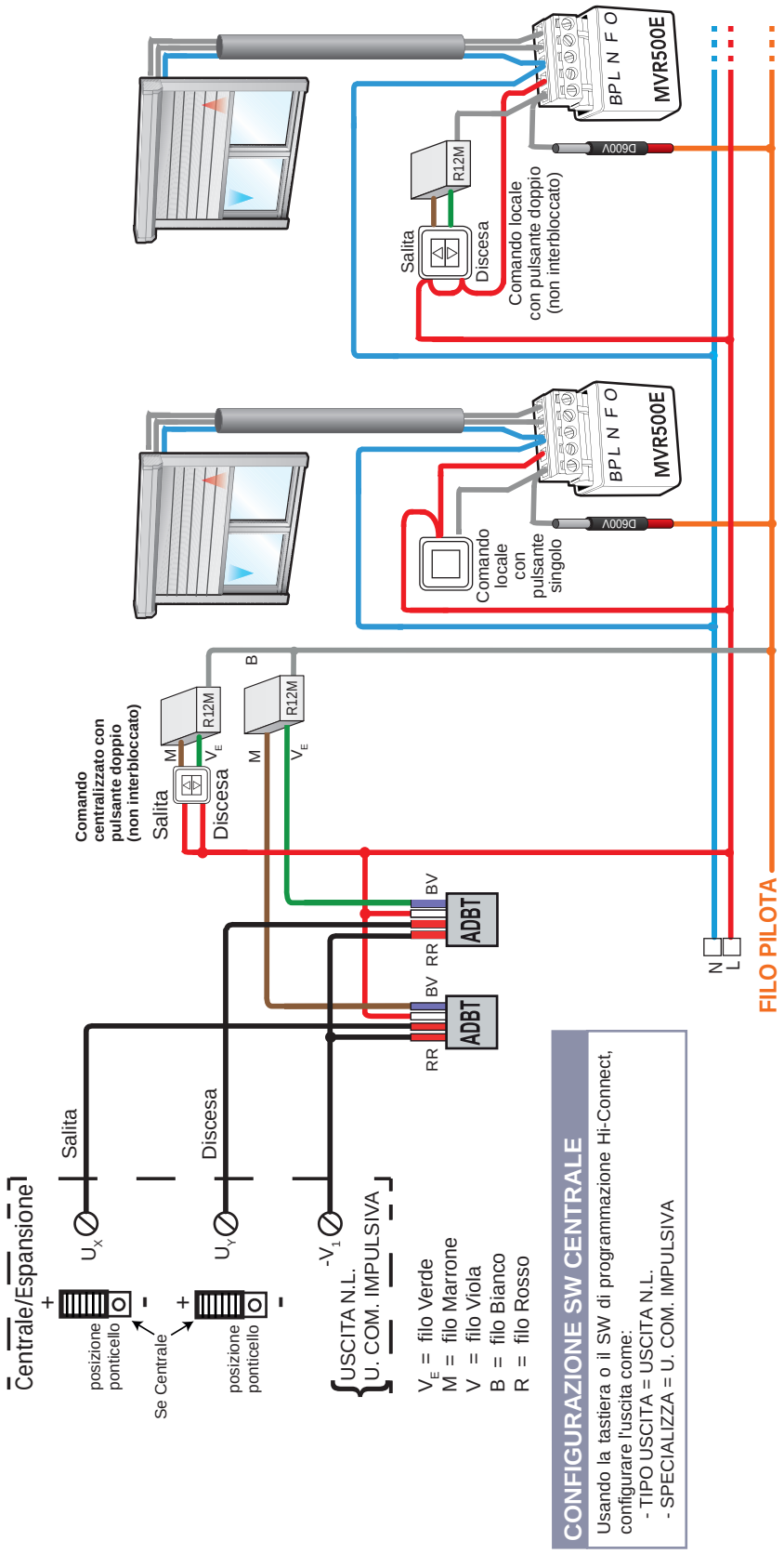
CONFIGURAZIONE SW CENTRALE

Usando la tastiera o il SW di programmazione Hi-Connect, configurare l'uscita come:
- TIPO USCITA = USCITA N.L.
- SPECIALIZZA = U. COM. IMPULSIVA

SD541-9011

Centralizzazione di tapparelle su pulsanti e centrale/espansione ELKRON

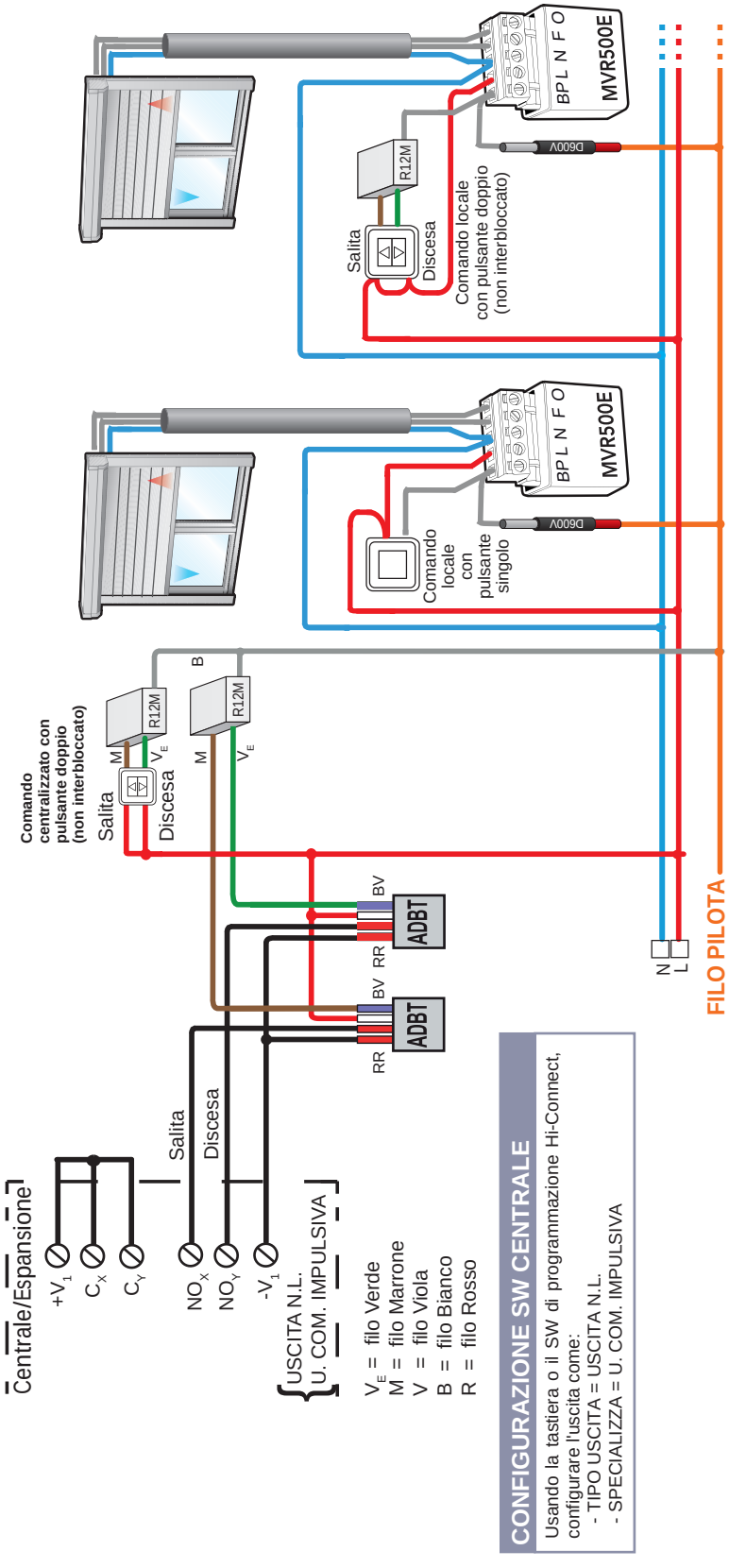
Centrale/espansione con uscite elettriche



SD541-9012

Centralizzazione di tapparelle su pulsanti e centrale/espansione ELKRON

Centrale/espansione con uscite a relè



SD541-9013

ENGLISH

Index (V2.0.0-11)

Compatible browsers

The Web Server is compatible with the following browsers:

- **Google Chrome**, from version 36.0.1985.125 m
- **Firefox**, from version 30
- **Microsoft IE**, from version 9
- **Safari**, from version 5.1.7

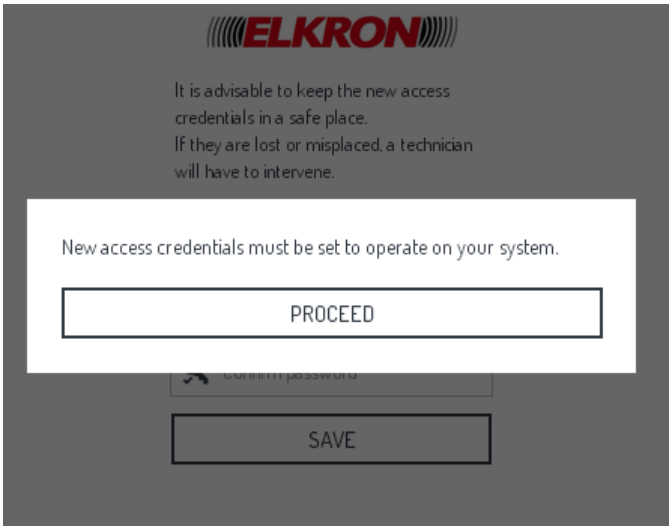
First access

WARNING: If the system has partitions configured with the block arming, it is not possible to log in and the following message will appear: “There is at least one partition with block arming: check the configuration”.

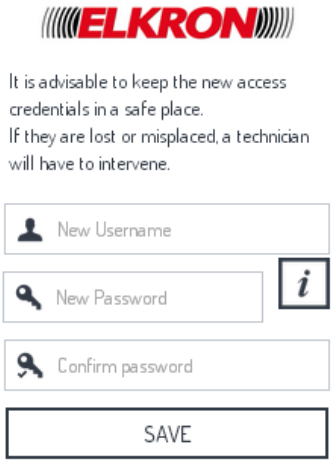
To access the Web Server for the first time, use the default access credentials (username = **admin**, password = **WebServer1**) with the procedure of How to log on.

Once you have logged in, it is necessary to change the username and password.
If you do not change the access credentials, it will not be possible to interact on the alarm system via Web Server.

After completing the login, a pop-up appears and asks to change the access credentials.

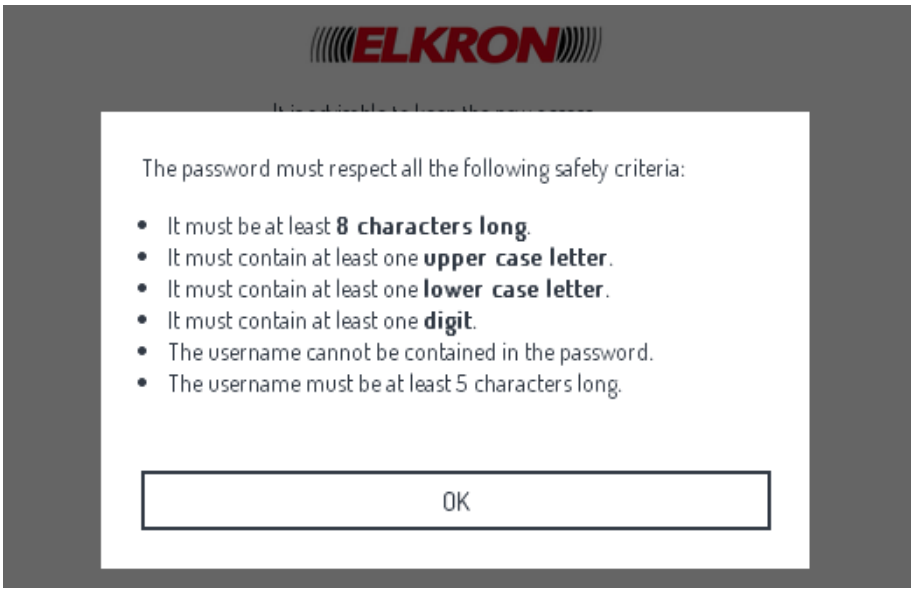


Push the **PROCEED** button to change the credentials. The page where you must insert the new information opens.



Username and password must conform with specific characteristics (Username and password requirements).

Press the [i] button and a pop-up will appear to specify the password security requirements.



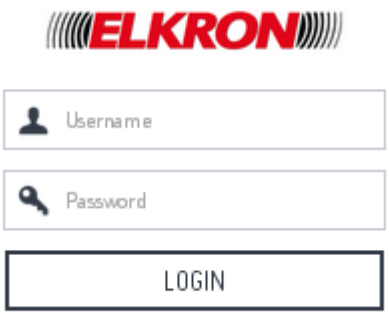
After changing access information, the default credentials will no longer be valid. If login is later attempted with the default credentials, the login page will continue to appear with the message “Authentication failed”.

How to log on

WARNING: If the system has partitions configured with the block arming, it is not possible to log in and the following message will appear: “There is at least one partition with block arming: check the configuration”.

To access the alarm system via Web Server, follow the instructions below:

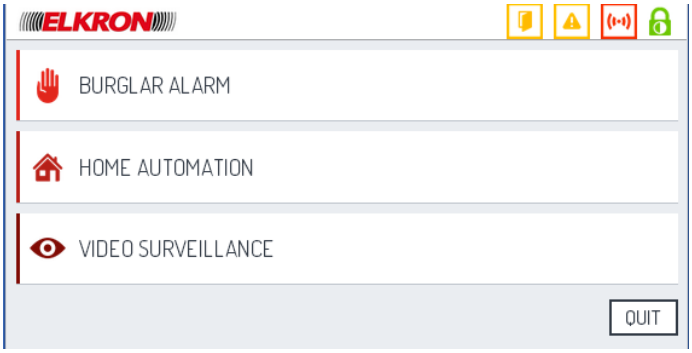
1. Connect via computer, tablet or Smartphone to the Internet address provided by the technician. A VPN network is created and the login screen appears.



2. Insert the access credentials (Username and Password). The credentials are memorised locally in the Web Server and are the same for all the Web Server users. **ATTENTION!** It is not possible to have more than one access at the same time. If someone has already logged in, no matter what device was used (Smartphone, tablet, PC), it will not be possible to access the Web Server until that user logs out or the current session expires.
3. Push the **LOGIN** button.
4. If the Web Server recognises the validity of the access credentials, the Homepage will appear.

If the access credentials are wrong, the login screen will reappear and an error message will appear on the credentials inserted.

Homepage



To access the HOMEPAGE (Access) it is necessary to log in with the correct access credentials. The Homepage is the main page from which all the system management sections may be accessed:

- **BURGLAR ALARM**, which makes it possible to arm and disarm the alarm system, verify its status, enable and disable users and make configurations.
- **HOME AUTOMATION,** it allows user activate home automation output, configured in burglar alarm system, execute scenarios to activate or stimulate extis.
- **VIDEO SURVEILLANCE**, which makes it possible to interact with the video surveillance system, if installed.

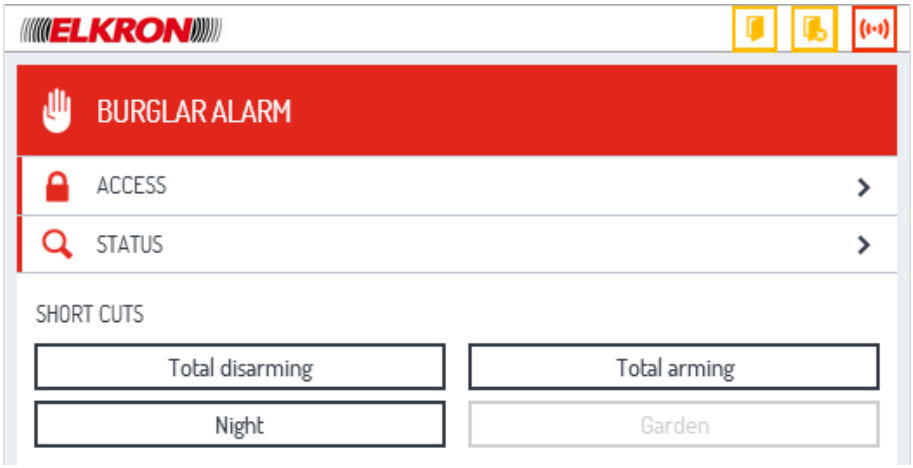
The HOMEPAGE also contains a summary of the system status represented with icons. The icons appear only when there is something to signal.

	**Burglar alarm system armed**. This appears when the entire burglar alarm system is armed.
	**Partitions armed**. This appears when one or more partitions, but not the entire burglar alarm system, are armed.
	**Isolated input**. This appears when there is at least one isolated input. If you click on the icon, a list of all the isolated inputs will appear. The signalling icon disappears as soon as there are no more isolated inputs.
	**Open input**. This appears when there is at least one open input. If you click on the icon, a list of all the open inputs appears. The signalling icon disappears as soon as there are no more open inputs.
	**Alarm or tampering**. This appears when there is or was at least one alarm or tampering. If you click on the icon, a list of all the alarms and tampering events memorised appears. To eliminate the icon, it is necessary to delete the alarm memory via the web server or keypad. However, in case of tampering this can be done only by the Technician or Technical Manager via the keypad only. *WARNING*: If not all the causes of the alarm icons are eliminated, the icon signal will continue to be present.
	**Problems and breakdown**. This appears when a malfunction or breakdown has been detected in the system. If you click on the icon, a list of all the malfunctions and breakdowns memorised will appear. To eliminate the icon, it is necessary to delete the breakdowns from the memory via the web server or keypad. Some breakdown memories must be deleted only by the Technician or Technical Manager by means of the keypad.

If you click the **QUIT** button, you will be disconnected from the system and return to the login screen. To reopen the **HOMEPAGE**, you must log in again.

Burglar Alarm

Access the BURGLAR ALARM section from the Homepage. To expand the section, click on BURGLAR ALARM.



The section is divided into three parts:

- Access, which allows you to log in and access the Alarm system management page to arm and disarm the burglar alarm system and examine the potential signal details (alarm, tampering, or breakdown) of the inputs
- Status, which makes it possible to examine the status of the entire system.
- Short cuts, which makes it possible to arm and disarm the entire burglar alarm system with just one command, or to carry out two programmed short cuts.

The icons above illustrate a summary of the system status. The meaning and behaviour is explained in the description of the Homepage.

Click again on the BURGLAR ALARM to close the section.

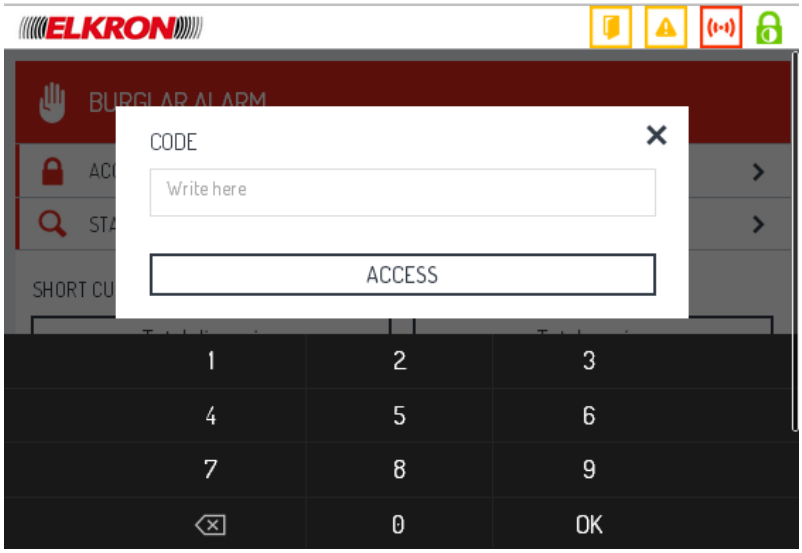
Access

The ACCESS procedure can be accessed from the Burglar Alarm section.

Use this procedure to access the burglar alarm control panel directly, if access not already performed from Home automation section.

Authentication of access

When you start the ACCESS procedure, a pop-up appears so you can authenticate who you are, if not already done in Home automation section.



Digit a valid access code and press the **ACCESS** button. The access code is the 6-digit numerical code used to access the alarm system via the physical keypad, not the password used to access the Web Server.

WARNING: If the access codes configured in the control panel are less than 6 digits long, it must first be reconfigured as a 6-digit number in order to access the control panel via the Web Server.

The ⌫ key cancels only the last digit and **OK** button is the same as **ACCESS**, it sends the code to the system.

The operations that can be carried out after entering the system depend on the privileges possessed by the access code inserted.

To close the pop-up window without attempting to access the system, click outside of the virtual keypad and the pop-up or press the **X** icon on the pop-up. In this way, even if a code has been inserted, it is eliminated and not checked, and the counter of incorrect access attempts remains unchanged.

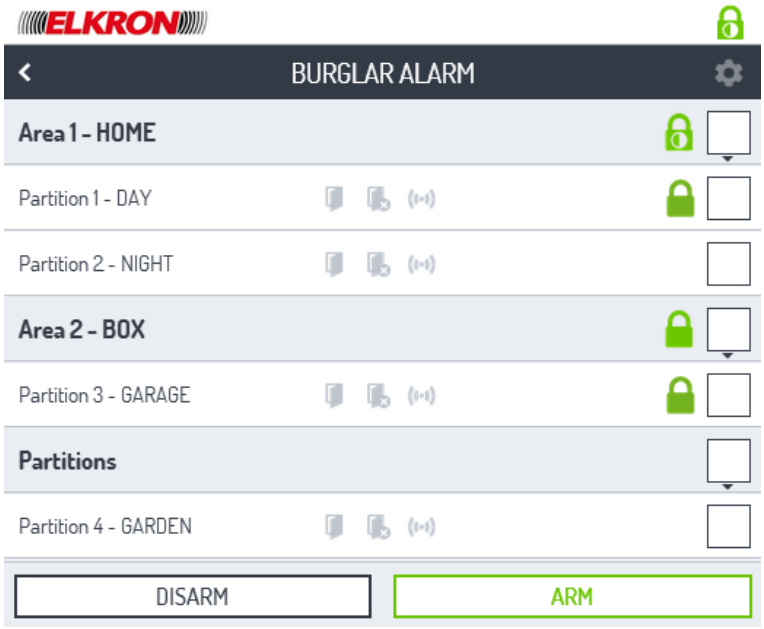
If the code inserted is correct, the management page (Alarm system management) of the burglar alarm system appears.

If the code inserted is wrong, or no code is inserted before pushing the **ACCESS** button, an error message appears. The counter of the failed access attempts is increased by 1.

The maximum number of failed access attempts is 21 (the limit is set by the burglar alarm control panel and cannot be changed). If an incorrect access code is inserted for more than 21 consecutive times, the control panel generates a “wrong code” alarm.

Alarm system management

The alarm system management page can be accessed with the Access procedure.
This page allows access to the functions for managing the burglar alarm system.



The page includes:

- **Name and status of the areas** (in the example they are HOME and BOX). The icon indicates that the area is partially armed, the icon that is totally armed. If there is no icon, it means that the area is not armed. The name of the area is the one that was configured in the control panel.
- **Partition name and status**. The list can be expanded or reduced by clicking on the name of the area of belonging or on the Partitions grouping.
  Next to the partition name are the icons of the burglar alarm or tampering (), open input (), isolated input (). If the icons are grey, it means that there are not, repeatedly, alarms, open inputs, or isolated inputs.
  If the relative icon is on (coloured), it means there was an alarm, that one or more inputs are open, that one or more inputs are isolated. When you click on this, the partition will expand and show the list of the Inputs associated with the partition that have caused signal or signals.
  If all the icons are grey, the partition will not expand.
- The system status, via the icons at the top. The meaning and behaviour is the same as those on the Homepage.

The icon makes it possible to access the Settings page, where it is possible to configure different system functions and parameters. The icon is enabled only if the alarm system is completely disarmed.

To arm or disarm areas or partitions, select the areas or partitions desired by clicking on the selection panel and pressing the **DISARM** or **ARM** button as required.
The action selected will be executed only on the areas or partitions selected.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

Arming the alarm system

The alarm system can be armed totally or partially.

The number of areas or partitions armed depends on the user's access credentials.

The Master user can always arm all the areas and all the partitions.

Arming the entire alarm system

On the HOMEPAGE press the TOTAL ARMING.

Another alternative, in the BURGLAR ALARM section, is to select all the areas and/or all the partitions and press the ARM button.

Partially arming the alarm system

On the HOMEPAGE, press the short cut button, if it has been configured and enabled to partially arm the alarm system.

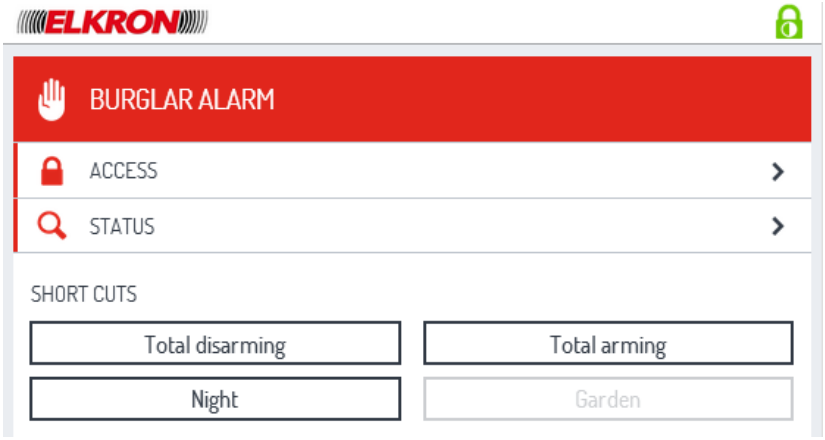
Another alternative, in the BURGLAR ALARM section, is to select the partitions or the areas to be armed and press the ARM button.

Disarming the alarm system

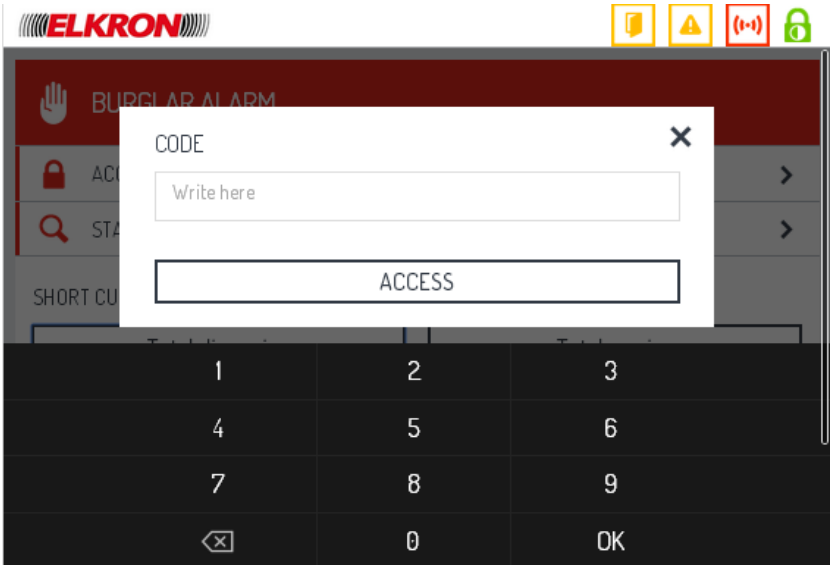
The alarm system can be totally or partially disarmed remotely provided that the disarming via remote has been enabled. The number of areas or partitions that can be disarmed depends on the user's access credentials. The Master user can always disarm all the areas and all the partitions.

Disarming the entire alarm system

On the HOMEPAGE, press the TOTAL DISARMING.



A request will be made for the User code (Authentication of access) to confirm the operation.



WARNING: The command for total disarming disarms only the areas and partitions that are associated with the user who inserts the code.

Otherwise, in the INTRUSION ALARM page, select all the areas and/or all the partitions and press the DISARM button.

Partially disarming the alarm system

On the BURGLAR ALARM page, select the partitions or areas to be disarmed and press the DISARM button.

Inputs associated with the partition

To see the inputs associated with a sector:

- on the STATUS page, expand the partition by clicking on its name, or
- on the BURGLAR ALARM page, expand the partition by clicking on its name. If the partition does not have any inputs with signals, it will not expand; the opposite is true for the STATUS page.

The list of inputs associated with the partition and for each of them will appear:

- if the input is open (icon );
- if the input was isolated manually or automatically (auto-inhibition) (icon );
- if the input has signalled or is signalling an alarm or if it was or has been tampered with (icon ).

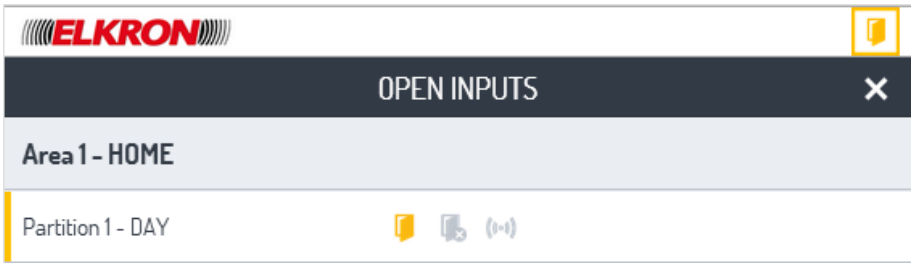
If the icon is grey, it means that the conditions associated with the icon itself are not valid.

Clicking again on the partition name closes the list.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

Open input

The user can access the OPEN INPUTS page by clicking on the icon . The icon is visible only if there is at least one input open.



The page contains a list of all the open inputs group hierarchically by area (if they exist) and partitions. If a sector does not belong to any area, it is visualised after the areas in the Partitions grouping.
If an input belong to more than one sector, it is listed inside each partition.
The closed inputs are not listed.

The page is updated in real time. If changes occur in the system when the page is open, regardless of the alarm system status (armed or disarmed), they are immediately visualized. An input that is opened will immediately be visualized in the list, including its partition and potential area of belonging. An input that is closed will be immediately deleted from the list, together with the partition and potential area of belonging, if no longer necessary.

The name of each input is visualized; other potential status is visualized via the activated icons (coloured): isolation ( ) and alarm ( ).

The icons above illustrate a summary of the system status. The meaning and behaviour is explained in the description on the Homepage.

To return to the previous page, click on the **X** icon at the top right in the title.

Isolated input

The ISOLATED INPUTS page can be accessed by clicking on the relative icon . The icon is visible only if the system has isolated inputs.

The page contains a list of all the isolated inputs grouped hierarchically by areas (if they exist) and partitions. If a sector does not belong to any area, it is visualised after the areas in the Partitions groupings.

If an input belongs to more than one sector, it is listed inside each partition.
Inputs that are not isolated are not listed.

The page is updated in real time. If changes are made while the system is disarmed and the page is open, they are visualized immediately. An input that is isolated will be visualized immediately in the list, together with the partition and any potential area of belonging.

If the input is included, or is no longer isolated, it will be immediately deleted from the list and the page will be updated immediately. If the partition and the potential area of belonging do not contain other isolated inputs, they will also be deleted.

The inputs can be isolated and included again via the Isolated input page of the Web Server.

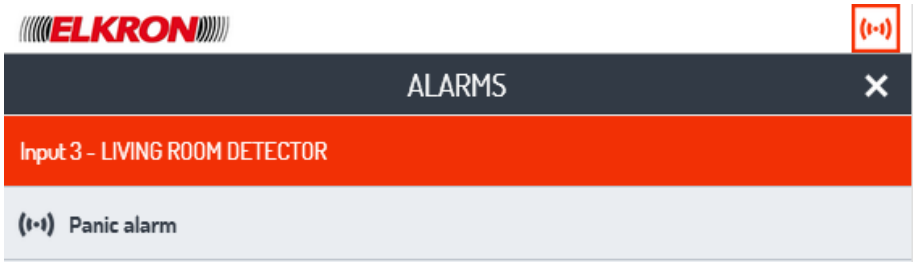
The name of each input is visualized; other potential status is visualized via the activated icons (coloured): open ( ) and alarm ( ).

The icons above illustrate a summary of the system status. The meaning and behaviour is explained in the description on the Homepage.

To return to the previous page, click on the **X** icon at the top right in the title.

Alarms and tampering

The ALARMS page can be accessed by clicking on the relative icon .



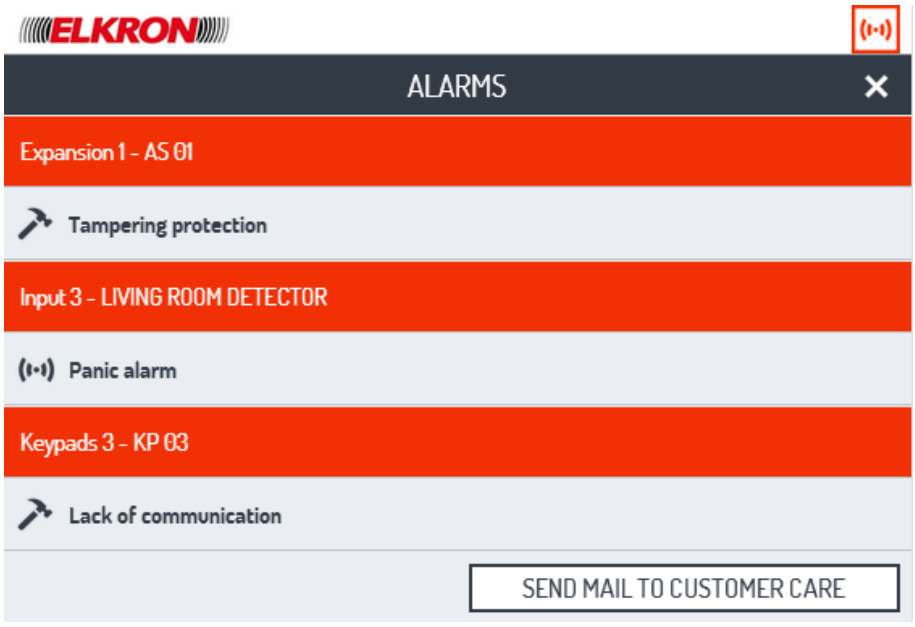
The page lists of all the alarms and tampering events present in the alarm memory and tampering memory. Less recent alarms continue to be included until they are deleted from the memories.

Alarms and tampering are grouped hierarchically by devices. Each device is identified by its type and name and its corresponding alarms and tampering are listed.
Alarms and tampering are also marked by icons (= alarm, = tampering).

Upon opening the page, all the alarms in the memory are displayed. If changes are made to the system while the page is open, they will be visualized immediately when the page is reloaded.

The icons at the top summarise the system status. Their meaning and behaviour is explained in the description on the Homepage.

To return to the previous page, click on the **X** icon at the top right in the title.



If at least one tampering is signalled, at the bottom of the page there will be a button saying "Send mail to Customer Care". Clicking on this button will send an e-mail to the first e-mail address memorized among the contacts and to the e-mail addresses of the technical contacts as configured. The subject of the mail sent will be “Request for system assistance: “ followed by the name of the system as set during the configuration.

In the e-mail, the following information about the system will be specified:

- “System:” , or the name of the system as set during the configuration.
- “Control panel model:” , identified with brand and model.
- “Control panel version: ”, or the version of the firmware installed on the control panel.
- “System code: ” , the identification code of the system.

If the control panel model, the firmware version or the system code is not available, the message “Information on the system not available” will appear in place of the information.

Following this information in the mail, there will be a list of all the tampering events present at the time the e-mail is sent, indicating for each of them:

- “Type of device: ”, or the type of device that has broken down (for example, expansion, key reader, etc.).
- “Device name: ” or the name attributed to the device during the configuration (for example, AS01, DK01 etc.)
- “Signal: ”, or the type of tampering detected (for example, Tampering, Lack of dialogue, etc.).
- “Date: ”, or the date on which the tampering was verified.
- “Time: ”, or the time at which the tampering was verified.

If the date and time are not available, the message “Date and time not available” will appear.

Signalling alarms and tampering

The signalling of alarms and tampering can be generated by the following devices:

- Control panel
- Expansion
- Radio expansion module
- Wired input
- Magnetic contact radio
- IR radio detector
- Keypads
- Radio siren output
- Supplementary power source AS500

Moreover, an alarm signal can also be generated by the user via the alarm, keypad or remote control.

The possible signals are:

Device	Sabotage	Lack of dialogue	Jamming	Radio supervision	Alarm
Control panel	■				
Expansion	■	■			
Radio expansion module		■	■	■	
Wired input	■				Burglar Pre-alarm Fire Panic Emergency Technological type 1, 2, 3 Silent panic Hold-up Reset fire alarm Test
Magnetic contact radio			■	■	
IR radio detector			■	■	
Keypads		■			Silent panic Emergency Fire
Remote control					Panic Silent panic Emergency Fire
Radio siren output			■	■	
Supplementary power source AS500	■	■			

Notification of the alarm via e-mail

Every burglar alarm event, tampering, and ON/OFF areas or partitions instantaneously generates an e-mail that is sent to the addresses configured.

The subject line of the mail sent is completed as: “System” + system code + “Event” + univocal ID of the event + type of event.
The e-mail specifies the following information about the alarm:

- “Areas: ”, or the areas where the input that signalled the alarm is associated.
- “Partitions: ”, or the partitions where the input that signalled the alarm is associated.
- “Type of device: ”, or the type of device that signalled the alarm.
- “Name of the device: ”, or the name attributed to the device, which signalled the alarm, during configuration If no name was attributed, the default name created by the system during installation will appear (for example, KB01).
- “Signalling: ”, or the type of alarm generated.
- Date and time.

If the alarm is an burglar alarm and the input involved is associated with a video camera, a recording of the event is generated. The recording contains 15 low resolution images (5 before and 10 after the alarm) or 8 high resolution images (4 before and 4 after the alarm). All the images are captured at an interval of one second between them.

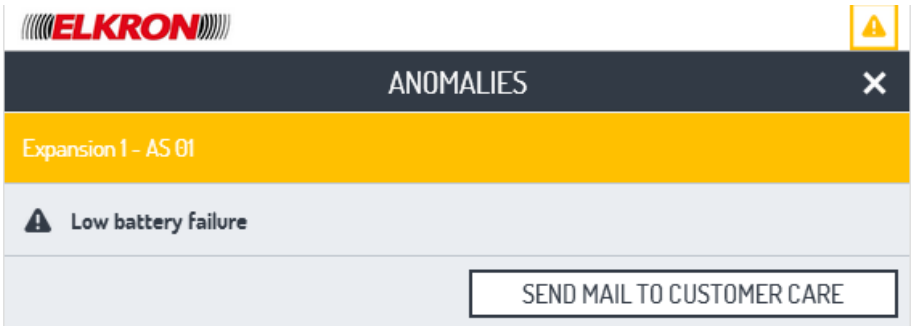
When the recording is completed, a second e-mail is sent with the first image memorized after the activation of the alarm attached.
The subject of the second e-mail sent is completed as: “System” + system code + “Event” + univocal ID of the event, which is the same used in the first e-mail + type of event.

The text of the second e-mail will be “A recording from the video camera is available”, followed by the name attributed to the camera during configuration. If the video camera was not working, the text will read: “Recording from the video camera not available”, followed by the name attributed to the video camera.

If there is more than one video camera associated with the input that signals the alarm, separate e-mails are sent, one for each camera.

Anomalies

The ANOMALIES page can be accessed by clicking on the relative icon , which appears when at least one fault or anomaly is present or memorized.



On this page the user can examine all the faults and anomalies present or memorized in the control panel log.

Faults and anomalies are grouped by device. Each device is identified by its type and name.

Upon opening the page, all the alarms in the memory are displayed. If changes are made to the system while the page is open, they are visualized immediately.

Each type of event is highlighted by an icon and the details of the anomaly detected are visualized.

The “Send mail to Customer Care” button appears at the bottom of the page. Clicking on this button will send an e-mail to the first e-mail address memorised among the contacts and to the technician contact e-mails configured in the system. The subject of the mail sent will be “Request for system assistance: “ followed by the name of the system as set during the configuration.

In the e-mail, the following information about the system will be specified:

- “System: ”, or the name of the system as set during the configuration.
- “Control panel model: ”, identified with brand and model.
- “Control panel version: ”, or the version of the firmware installed on the control panel.
- “System code: ”, the identification code of the system.

If the control panel model, the firmware version or the system code is not available, the message “Information on the system not available” will appear in place of the information.

Following this in the e-mail, there will be a list of all the faults present at the time of sending, indicating for each of them:

- “Type of device: ”, or the type of device that has broken down (for example, expansion, key reader, etc.).
- “Device name: ” , or the name attributed to the device during the configuration (for example, AS01, DK01 etc.)
- “Signalling: ”, or the type of fault detected (for example, Battery low, Power supply failure, Jamming, etc.).
- “Date: ”, or the date on which the failure occurred.
- “Time: ”, or the time at which the failure occurred.

If the date and time are not available, the message “Date and time not available" will appear.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

Anomalies detected

The type of device determines the anomalies that can be signalled, as illustrated in the lists that follow.

Control panel

- Lack of Power: the power supply (230 V) of the control panel is interrupted.
- Low Battery: the back-up battery is not charged sufficiently.
- PSTN failure: the wired telephone connection does not work.
- GSM failure: the cell phone connection does not work.
- LAN failure: the Internet connection does not work.
- Fuse V1: self-resetting fuse.
- Fuse V2: self-resetting fuse.

Expansion of the control panel

- Power supply failure: the expansion is not powered correctly.

Detector

- Low Battery (radio detector): the battery of the radio detector is not charged sufficiently
- Failure: the detector does not function correctly.

Wired input

- Failure: generic input failure.
- Detector failure: the detector does not function correctly.
- Communicator failure: failure of the external communicator.
- Jamming: there is an attempt to jam the detectors.
- Siren failure: the sirens do not function correctly.

Radio siren

- Low Battery: the battery of the radio siren is not charged sufficiently.

Keypad

- Power supply failure: the keypad is not powered correctly.

The electronic or proximity key reader

- Power supply failure: the reader is not powered correctly.

Remote control

- Low Battery: the remote control battery is not charged sufficiently.

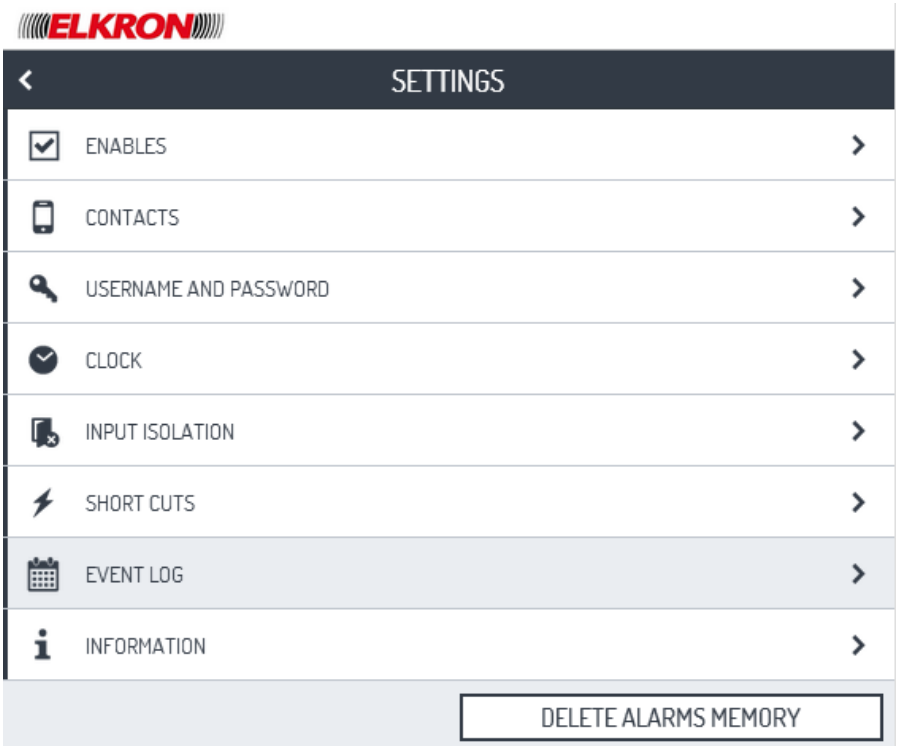
Settings

The SETTINGS page can be accessed by clicking on the icon .

This page allows the user to access functions to enable users and keys, configure parameters and functions, modify access credentials, view the log, set Home automation scenarios and more.

WARNING: The icon can be clicked and so the page can be seen only if the alarm system is completely disarmed.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.



The items visualized are dynamic, in that they depend on the type of user has gained access.

Functions available

- **Enables.** Makes it possible to enable users and keys. Enables accessibility and disarming via remote. It is available only to the Master user.
- **Contacts**. Makes it possible to insert, modify, and delete telephone numbers and e-mail addresses found in the system. It is available only to the Master user.
- **Procedure to change the username and password**. This makes it possible to modify the usernames and passwords only for access to the Web Server. It is available only to the Master user.
  IMPORTANT: To access the Web Server, the credentials are unique and the same for all users. The usernames and passwords defined here are used only to access the Web Server, not to interact with the alarm system, which requires the user to log in using the same code used with the keypads.
- **Clock**. This changes the date and time memorized in the control panel. It is available only to the Master user.
- **Event Log**. This shows the list of activities carried out directly on the system or via the Web Server. It is available to all users.
- **Input isolation**. This makes it possible to isolate inputs or include them again. It is available to all users. If none of the inputs associated with the user via the partitions can be isolated, clicking on INPUTS ISOLATION will trigger a pop-up with the message “No input can be isolated”.
- **Short cuts**. This allows the user to configure and enable the short cuts (those that appear in the BURGLAR ALARM section of the HOMEPAGE) and scenarios (that appears in HOME AUTOMATION section in HOMEPAGE). It is available only to the Master user.
- **Information.** This shows the general technical information about the system. It is available to all users.

The **DELETE ALARM MEMORY** key is available to all users.

Press this key to delete all the alarm signals of the control panel for the partitions to which the user has access. This means that if a user can operate only on some partitions, determined according to the numerical access code of the control panel, he will be capable of cancelling only the input alarms that belong to those partitions, and not all of the alarms.

The lack of power supply signals are also deleted.

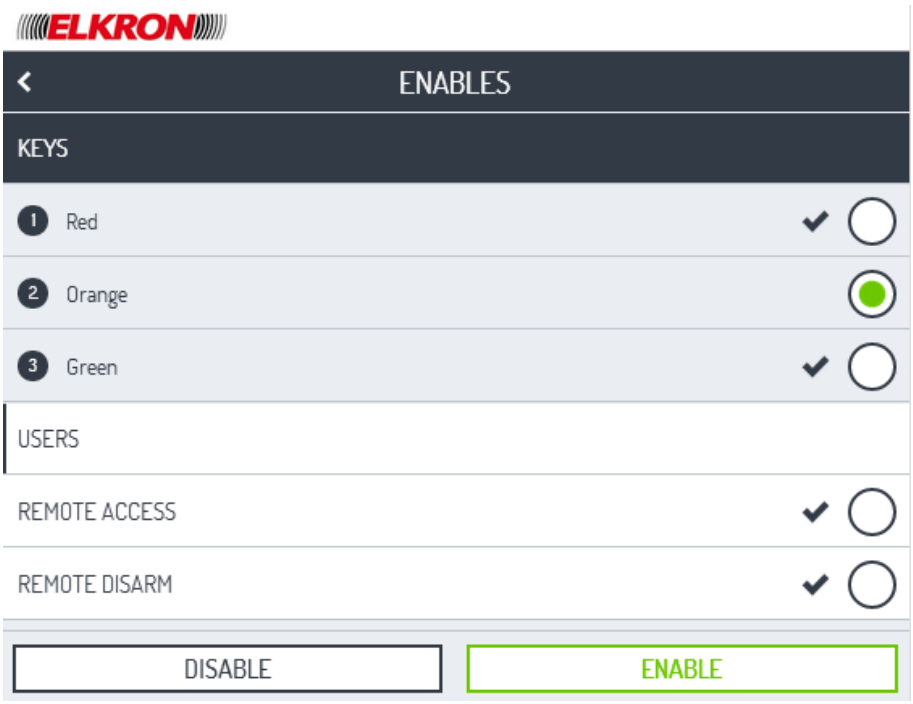
In any case, the button does not delete fault and tampering signals.

When the user presses the **DELETE ALARMS MEMORY**, a pop-up appears to confirm if the data has been deleted successfully or not.

Enables

The ENABLES page can be accessed from the Settings page. This page is visible only to the Master user.
From this page it is possible to enable and disable keys, users, accessibility and disarming from remote.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.



The sections of the page are:

- **KEYS**. When KEYS is clicked the item expands and the list of all the electronic and proximity keys acquired by the system is displayed. The keys are identified by *number* <*key name*>, where <*key name*> is the potential name attributed to the key during system programming. The icon ✓ indicates that the key is enabled. Click on KEYS again to close the list.
- **USERS**. By clicking on USERS, the item expands and the list of all the users memorised in the system is displayed. The users are identified by *number* <*user name*>, where <*user name*> is the name attributed to the user during system programming. The icon ✓ indicates that the user is enabled. Click on USERS again to close the list.
- **ACCESSIBILITY VIA REMOTE**. This can be used for remote access to the system, for example, for maintenance operations, including access to the Web Server. The icon ✓ indicates that accessibility via remote is enabled.
- **DISARMING VIA REMOTE**. This enables disarming of the system via remote control through the telephone line and DTMF commands. The icon ✓ indicates that the disarming via remote is enabled.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

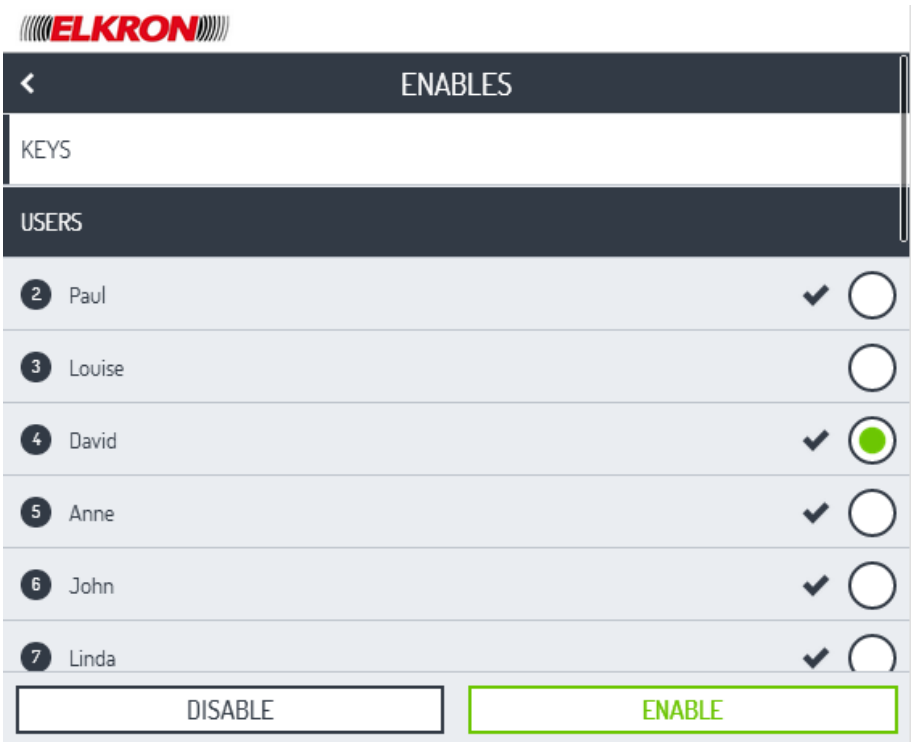
Enabling and disabling

To enable or disable a key, a user, remote accessibility or remote disabling, follow the instructions below:

1. Select the item on which you would like to operate by clicking on the circular selection button. Only one item may be selected at a time.
2. Press the **ENABLE** or **DISABLE** button, as needed. The item selected will be enabled or disabled according to the button pushed.

The status of the various parameters is updated in real time, so next to the name of the parameter the enabled icon will appear or disappear, ✓ according to the new status.

The enabling and disabling are memorised in the control panel.

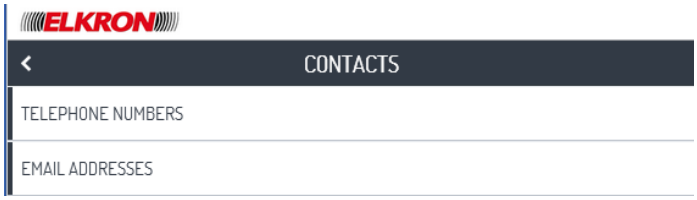


The image in the example above illustrates that the user Franca was selected to be disabled.

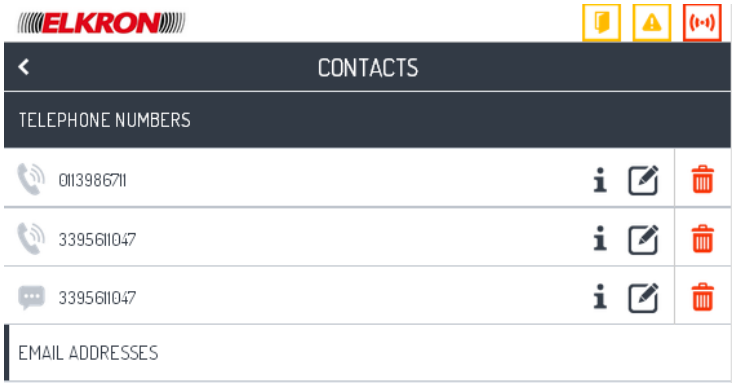
Contacts

The CONTACTS page can be accessed from the Settings page. This page is visible only to the Master user. This page can be used to modify some of the telephone numbers already programmed in the control panel, modify and delete the e-mail addresses that receive the alarm signals generated by the control panel. The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

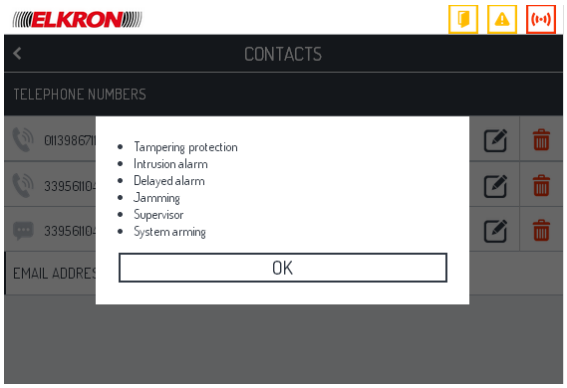
To return to the previous page, click on the icon **<** on the upper left of the title bar.



The page is divided into two sections, Telephone numbers and e-mail addresses, that can be expanded by clicking on them. To reduce the menu again, click on their title. The **Telephone number** section lists all the telephone numbers with vocal specialisation or SMS configured in the control panel. If the telephone number that occupies the 12th position of memory in the control panel was configured as an SMS, the network SMS are sent to that number.

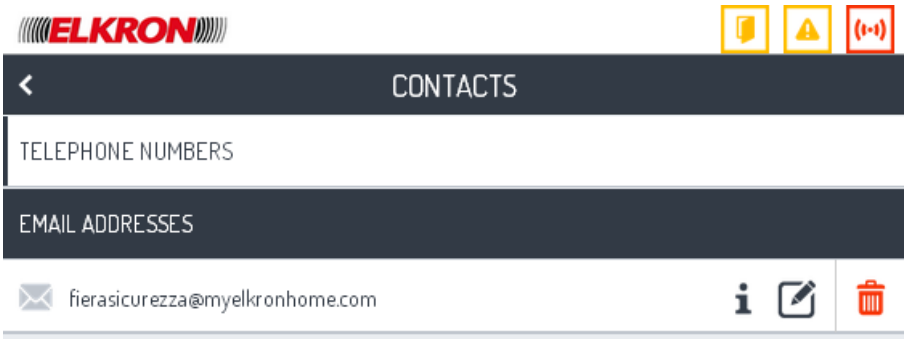


The specialization is indicated by an icon next to the telephone number (= vocal, = SMS). Click on the icon to open a pop-up window that lists all the events associated with that telephone number. The events possibly associated are listed in Alarms notified with vocal message and Alarms notified via SMS.

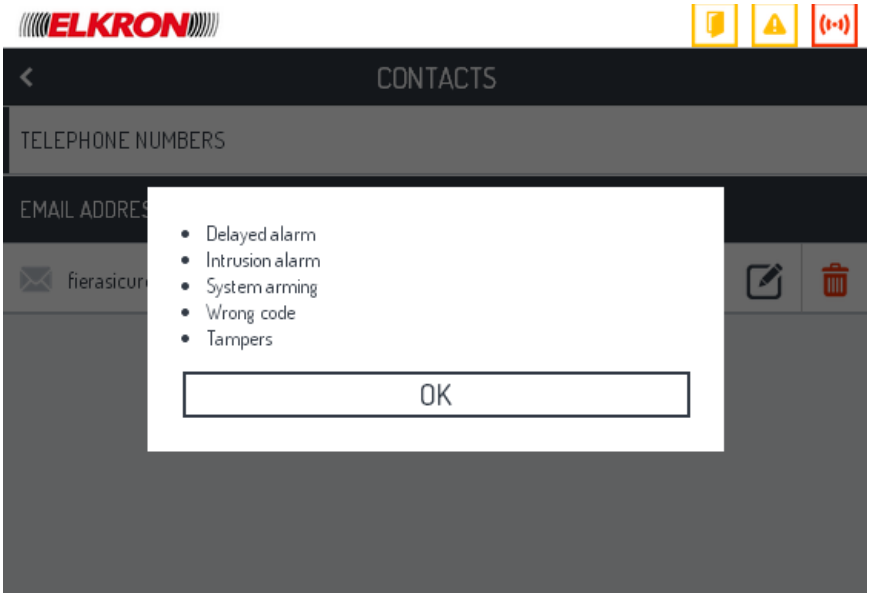


Telephone numbers with specialisations other than vocal or SMS, or telephone numbers not configured, are not listed. The control panel contains a maximum of 12 telephone numbers.

The **E-mail address** section lists the configured e-mail addresses.



Next to the e-mail address is an icon ℹ. Click on the icon to open a pop-up window that lists all the events associated with that e-mail. The events possibly associated are listed in Alarms notified via e-mail.



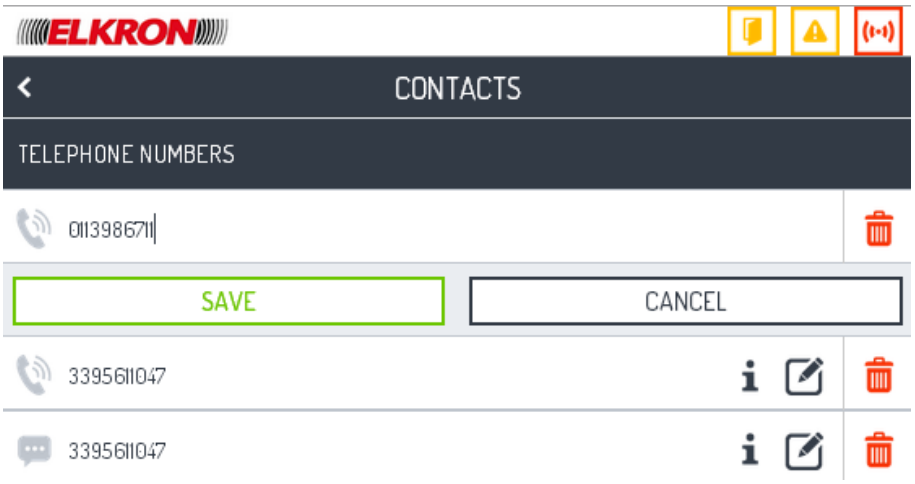
The first e-mail contact receives a copy of the e-mails sent to the technician when the operator clicks on the SEND MAIL TO CUSTOMER CARE button on the ANOMALIES and ALARMS pages.

Changing a telephone number

Only one telephone number can be changed at a time.

To change a telephone number.

1. Click on the icon of the telephone number to be changed. The change number menu will appear.



2. Type the new telephone number.
   If the telephone number is specialised vocal, digits (0…9) and the letter “P” can be inserted, which can be used to insert a 2-second pause in the composition, for example, if it should be requested by a switchboard. The maximum length of the telephone number is 28 characters, between digits and letters “P”.
   if the telephone number is specialised SMS, only digits (0…9) can be inserted. The maximum length of the telephone number is 10 digits.
3. Press the **SAVE** button to memorise the modifications made, **CANCEL** to exit from the procedure without making any changes.

WARNING: The Web Server carries out a formal control on the correctness of the telephone number, not on its existence or functioning.

WARNING: The telephone number modification procedure does not allow the user to modify others of his parameters (for example, the associations with alarms). To modify the other parameters of the telephone number, ask for technical intervention.

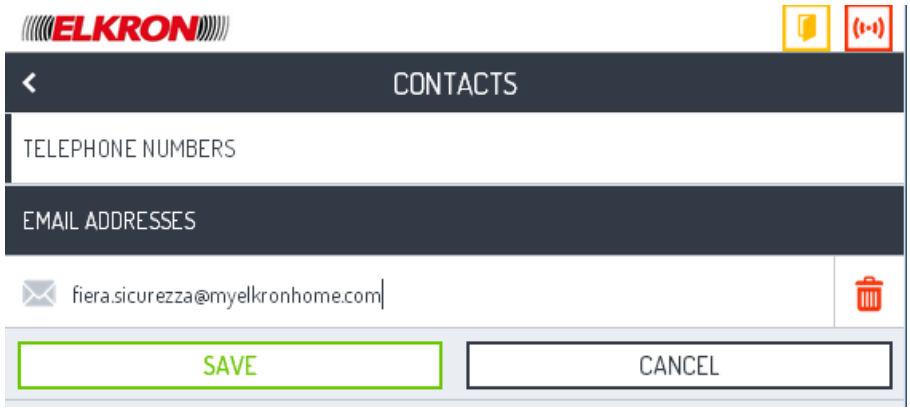
Deleting a telephone number

Only one number can be deleted at a time.

To delete a telephone number, click on its icon . The number of the telephone of reference is deleted but the other parameters configured remain memorised.
It will then be possible to assign a new telephone number of reference to the same memory position.

Changing an e-mail address

Only one-e-mail address can be changed at a time.



To change an e-mail address:

1. Click on the icon of the e-mail address to be changed. The change menu will appear.
2. Type in the new e-mail address.
3. Press the **SAVE** button to memorise the change, **CANCEL** to exit from the procedure without making any changes.

WARNING: The Web Server carries out a formal control on the correctness of the e-mail addresses, which must be in the format *name@dominion.extension*, but not on its existence or correct functioning.

WARNING: The change e-mail procedure does not allow changes to be made to its other parameters (for example, associations with alarms).

Deleting an e-mail address

Only one e-mail address can be deleted at a time.

To delete an e-mail address, click on its icon . The e-mail address will be deleted but the other parameters configured remain memorised. It will then be possible, at a later time, to assign a new address to the same memory position.

Alarms notified with vocal message

If telephone numbers for sending vocal messages have been enabled, they are sent notices for:

- Burglar alarm
- Technological alarm Type 1
- Technological alarm Type 2
- Technological alarm Type 3
- Fire alarm
- Panic
- Silent panic
- Emergency
- Hold-up alarm
- On/Off Partitions/System
- Tamper
- Power 230V
- Low battery
- Faults
- SIM Card Expiry

Each telephone number can receive different types of notifications and the notifications can be different for each telephone number

Alarms notified via SMS

If telephone numbers are enabled for sending SMS, they will be sent notifications for:

- Burglar alarm
- Technological alarm Type 1
- Technological alarm Type 2
- Technological alarm Type 3
- Fire alarm
- On/Off Partitions/System
- Tamper
- SIM Card Expiry

Each telephone number can receive different types of notifications and the notifications can be different for each telephone number.

Alarms notified via e-mail

If there are e-mail addresses enabled, they will be sent notifications for:

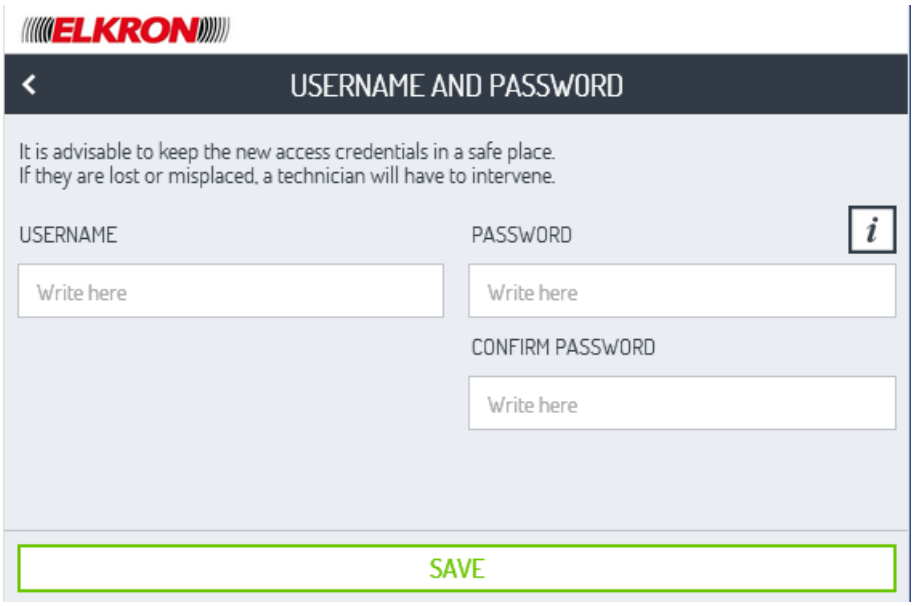
- Burglar alarm
- Delayed alarm
- ON/OFF Partitions/System
- Wrong code
- Tamper

Each e-mail can receive more than one type of notice and the notifications can be different for each e-mail.

The first e-mail contact receives a copy of the e-mails sent to the technician when the operator clicks on the SEND MAIL TO CUSTOMER CARE button on the ANOMALIES and ALARMS pages.

Username and password

The USERNAME AND PASSWORD page can be accessed from the Settings page. This page is visible only to the Master user.



On this page the user can modify the access credentials to the Web Server (username and password). One or both credentials can be changed, as needed.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

Username and password requirements

USERNAME

- Minimum length of 5 characters.
- Maximum length of 15 characters.
- Characters allowed: a…z, A…Z, 0…9 and characters \ | !;" $ % & / ( ) = ? ^ + * @ # , ; . : - _ < > [ ] ` { } ~

PASSWORD

- Minimum length of 8 characters.
- Maximum length of 15 characters.
- The password must contain at least one upper-case letter, one lower-case letter, and one number.
- Characters allowed: a…z, A…Z, 0…9 and characters \ | !;" $ % & / ( ) = ? ^ + * @ # , ; . : - _ < > [ ] ` { } ~
- The username cannot be contained in the password.

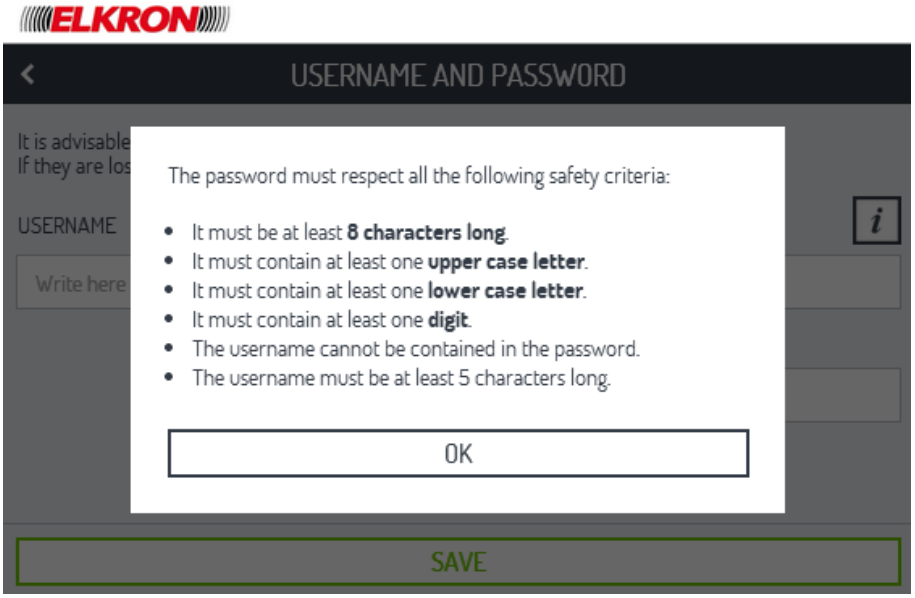
Procedure to change the username and password

The procedure allows the modification of access credentials. To make such changes:

1. Insert the new username (the text inserted is visible).
2. Insert the new password (the text inserted will be masked by asterisks).
3. Insert the new password again to confirm it (the text inserted will be masked by asterisks).
4. Press the **SAVE** button to save the new access credentials.

WARNING: It is necessary to insert both access credentials (username and password), even if one is not to be changed, because the procedure does not save the unchanged values in the memory.

Click on the icon [i] and a pop-up window will appear and list the required characteristics of the password.



If the username or password do not respect these obligatory characteristics (Username and password requirements)a pop-up window will appear to signal that at least one of the criteria was not respected. Change the username or password and try saving again. It is not possible to insert the default username and password set by the manufacturer.

If the *New password* and *Confirm password* are not the same, the error message “The passwords inserted do not match" will appear. Reinsert *New password* and *Confirm password* and try saving again.

When the username and password are valid, they are memorised in the Web Server and the login page reappears, where it is necessary to log in again with the new username and password before continuing.

WARNING: Keep the new user name and password in a safe place.

It you should lose your access credentials, contact the technician, who will reset the default values of the access credentials.
The access credential are restored to the default settings also after the Web Server hardware is reset.
If the access credentials are reset to default, it is necessary to carry out the first access again and then modify them.

Clock

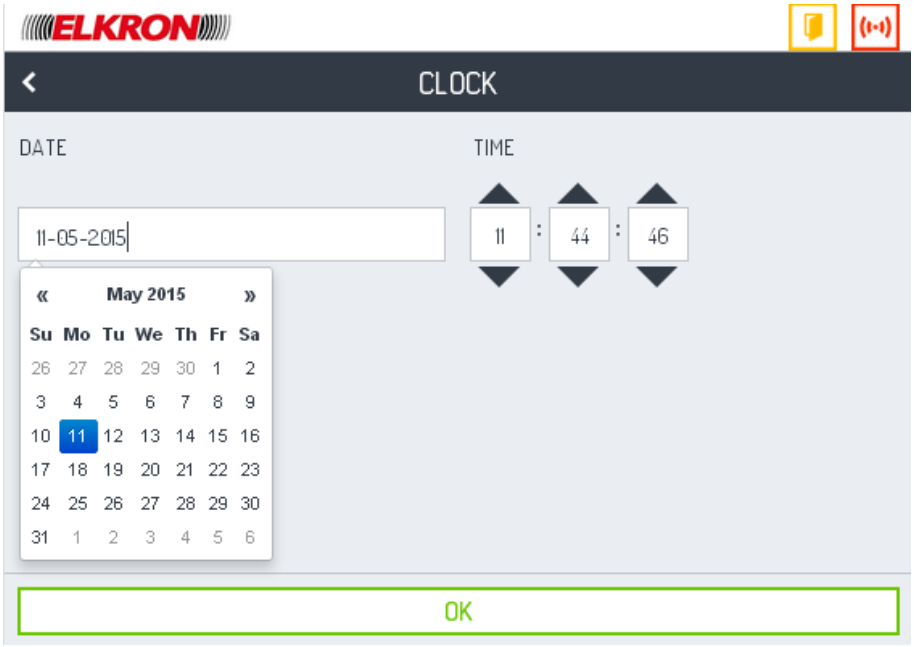
The CLOCK page can be accessed from the Settings page. This page is visible only to the Master user.
On this page the user can view and modify the date and time used by the control panel.

The date and time are those of the control panel.
Clicking on EDIT button, is possible to change date and hours settings.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

WARNING: Date and time are used by the control panel in memorising the events and alarms in the log and for the management of the schedule programmer. Inserting an incorrect date or time may create malfunctions.



To change the date:

- Click on the date field.
- In the calendar that appears, select a day, month, and year.

To change the hour, minutes, and seconds:

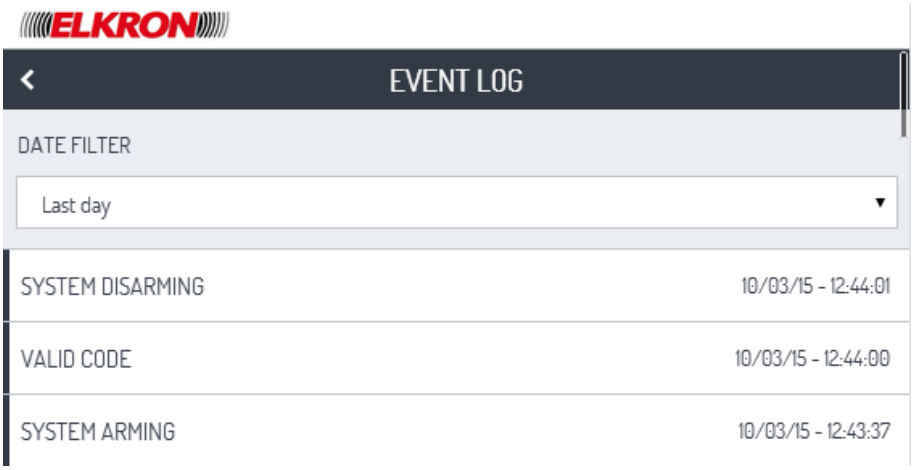
- Click repeatedly on arrow ▲ or ▼ in each field to modify hour, minute and second till desired values.

When finished, press the **OK** button to memorise the new date and time in the control panel.

Event Log

The EVENT LOG page can be accessed from the Settings page. This page is visible to all users.

On this page the user can examine all the events (armings, disarmings, alarms, etc.) memorised in the events log of the control panel.



When the page is opened, all the most recent events that occurred in the last day are visualized. During the downloading of the data, the Web Server is not operative. For every type of event listed, the date and time in which it occurred are specified.

The events are presented in reverse chronological order, from the most recent to the oldest. This list of events can be lengthened or shortened by using the filter function (Filtering the events).

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

Filtering the events

It is possible to filter the events to reduce the list of the results thanks to the DATA FILTER that limits the period of time being analysed.

The possible options are:

- Last day (default)
- Last week
- Last month
- Last 3 months
- Last year

For each event listed, the user can examine the details (Examining the details of the events).

Examining the details of the events

To visualize an event in detail, click on the line of the LOG that lists it. To hide the details, click on the line again.

The information available depends on the type of event, as illustrated in the table that follows.

EVENT	INFO
Burglar alarm	ID and input name Logic number of input
Pre-alarm	ID and input name Logic number of input
Technological alarm type 1/2/3	ID and input name Logic number of input
Fire alarm	ID and source name from which the alarm was triggered Logic number of input
Panic	ID and source name from which the alarm was triggered Logic number of input
Silent panic	ID and source name from which the alarm was triggered Logic number of input
Emergency	ID and source name from which the alarm was triggered Logic number of input
Hold-up alarm	ID of the device from which the alarm was triggered alarm sensor
ON/OFF Partitions/System	ID of the device (KP = keypad; MODEM = Hi-Connect; WS = Web Server,…) ID and username that inserted the code ID and name of all partitions that were armed/disarmed
Start Maintenance	ID of the device (KP= keypad) ID of the installer

End Maintenance	ID of the device (KP= keypad) ID of the installer
Start input isolation	ID and input name ID of user
End input isolation	ID and input name ID of user
Instantaneous no mains power event	name of control panel SYSTEM
Event end lack of power	name of control panel SYSTEM
Start failure	ID and input name output that was armed
Event end failure	ID and input name output that was armed
Wrong Code	No information
SIM Card Expiry	name of control panel ID of the installer
Reset fire alarm event	

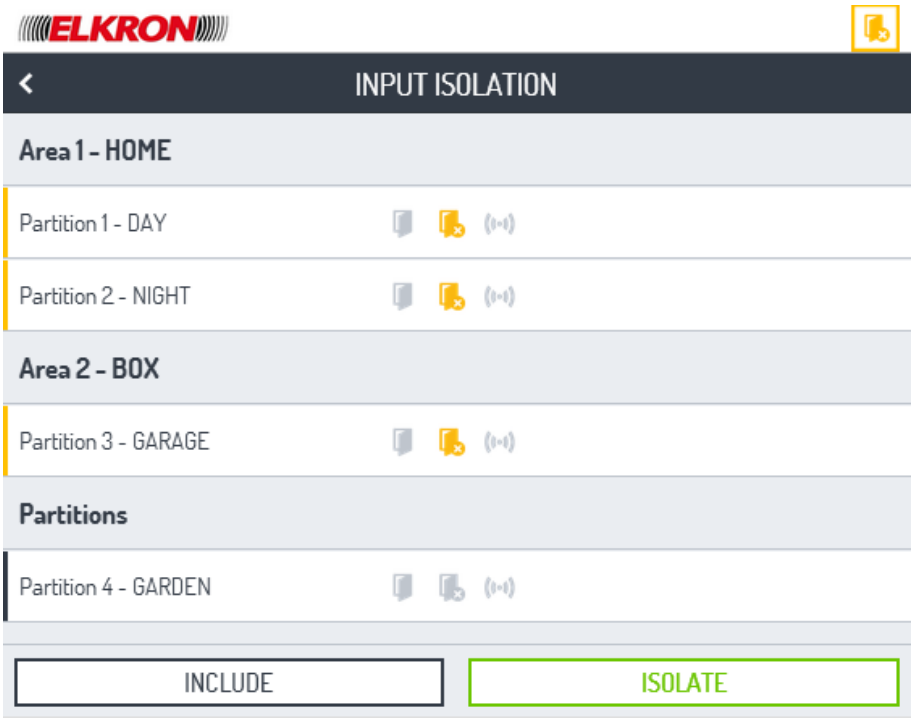
Input isolation

The INPUT ISOLATION page can be accessed from the Settings page. This page is visible to all users
On this page the user can isolate inputs of the burglar alarm or include them again.
An input must sometimes be isolated when it presents some anomaly, in order to arm the alarm system in any case.

WARNING: Isolating an input is a temporary emergency measure that reduces the effectiveness of the burglar alarm system. It is necessary to eliminate the anomaly that made the input isolation necessary as soon as possible.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

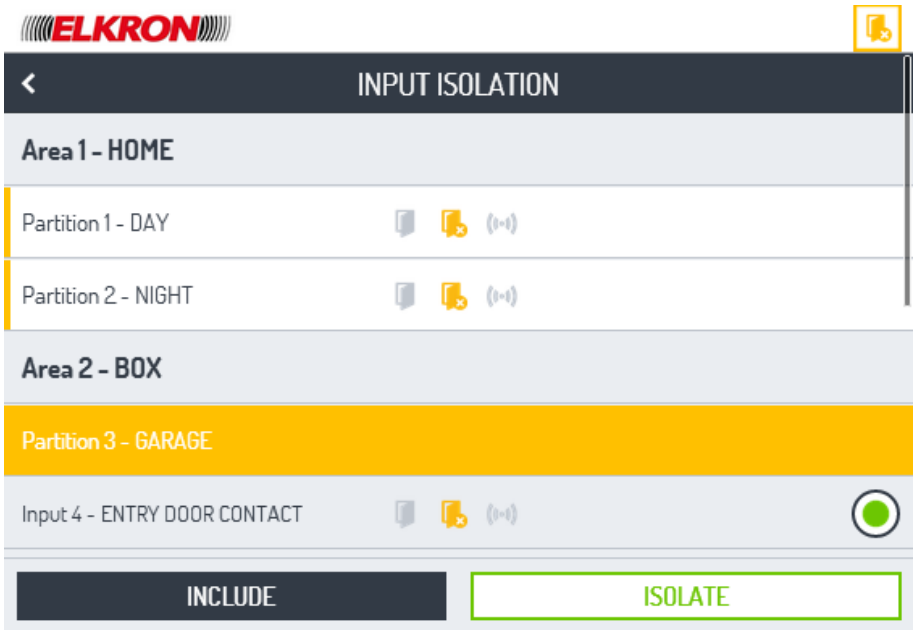
To return to the previous page, click on the icon **<** on the upper left of the title bar.



The user who logged in will visualize only the areas and partitions he is qualified to work on and have inputs that can be isolated.

An input can be isolated when it was defined as such during the system programming. Not all inputs can be isolated.

If the user is not qualified to work on the existing inputs that can be isolated, a pop-up window will appear with the message “No input can be isolated”. Press the **BACK** button to close the pop-up window.



Click on a partition to expand the list of inputs that can be isolated associated with it (any other inputs that cannot be isolated, belonging to the partition, will not be shown).
Click again on the name of the partition and the list will disappear.

The name of each input is visualized; other potential status is visualized via the activated icons (coloured): input open ( ) and alarms ( ).

The status of the areas, partitions, and inputs is read at the time the page is opened and updated in real time. This means that the icons can change also while the page is open.

Isolating and including inputs

Only one input can be isolated or included at a time.

To isolate an input or include it again:

1. Click on the circular selection button at the right of the input in question.
2. Press the **ISOLATE** button to isolate the input selected; press the **INCLUDE** button to include the input selected again.
3. The status icon of the input isolated or included will be updated automatically.

Short cuts

The SHORT CUTS page can be accessed from the Settings. This page is visible only to the Master user.

On this page the user can configure the short cut keys that appear on the Homepage.

The page shows two sections, Burglar alarm and Home automation that can be expanded clicking on them. To compress is enough re-click again on the title.

Burglar alarm

WARNING! Screen before version 1.3.0-X

WARNING! Actual screen from version 1.3.0-X

It is possible to program 4 short cuts. Two are already set by default (TOTAL ARMING and TOTAL DISARMING) and cannot be deleted or changed.

TOTAL ARMING and TOTAL DISARMING are disabled as default and must be enabled before they can be used.

To enable or disable a short cut, just click on the icon of the sliding switch to the right of its name: with ON the short cut will be enabled on the HOMEPAGE; with OFF it remains visible but is disabled (it cannot be clicked). When the default short cuts (TOTAL ARM and TOTAL DISARM) are disabled, they simply change colour (grey instead of black).

NOTE: if the MASTER code is changed, you will need access to shortcuts, disable them all and then rehabilitate them.

For a more detailed description of how short cuts work, see How short cuts work.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

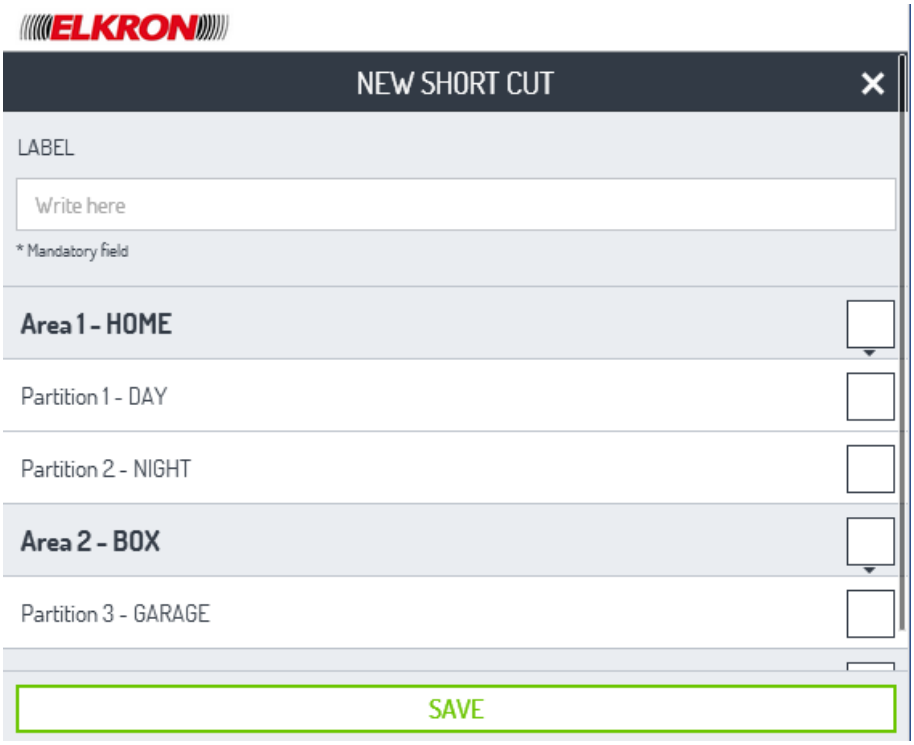
To return to the previous page, click on the icon **<** on the upper left of the title bar.

Configuring a new short cut

Short cuts can be created only by the Master user.

To create a new short cut:

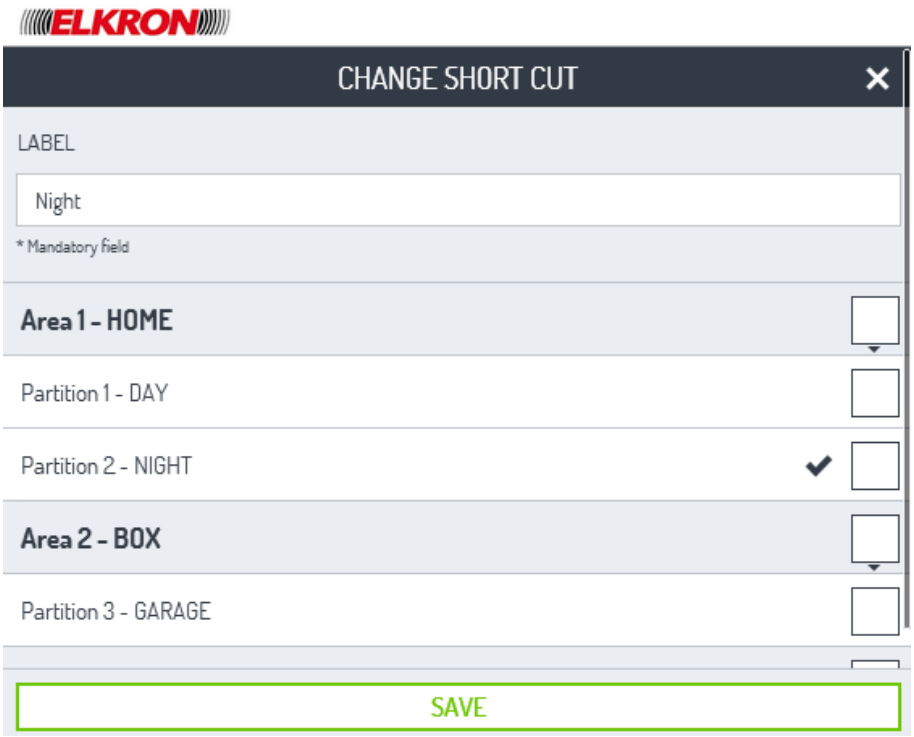
1. Click on the icon ⊕ at the top right of the BURGLAR ALARM section in SHORT CUTS page. The NEW SHORT CUT page will appear. The icon ⊕ is visible only if it is still possible to insert a short cut.



2. It is necessary to insert a descriptive name for the new short cut in the “Label” field. The maximum length is 24 characters.
   The name inserted must be different from the short cut names already present. Any error will be signalled by the message “Short cut label already present. Insert a different name”.
3. Select by clicking on the selection square, the areas and partitions that are part of the new short cut. Areas and partitions can be selected in the combination desired. If an area is selected, all its partitions are automatically selected; if all the partitions of an area are selected, the area itself is automatically selected.
4. Press the **SAVE** button to create the new short cut. If at least one partition or one area is not selected, the error message “Select at least one partition to arm” will appear. Clicking on **X** icon, is possible to close the page discarding selections done.
5. The new short cut created is disabled by default and must be enabled in order to use it.

Changing a short cut

Short cuts can be changed only by the Master user. It is not possible to change TOTAL ARMING and TOTAL DISARMING.



To change a short cut:

1. Click on the name of the short cut: a list of the areas armed will appear with the DELETE and CHANGE keys.
2. Press the **CHANGE** button. The page used to create a new short cut will reappear.
3. Change the name of the short cut and add or remove areas and partitions from the short cut as needed. The changes must comply with the same rules for Configuring a new short cut.
4. Press the **SAVE** button to memorise and confirm the changes made.

Deleting a short cut

The short cuts can be deleted only by the Master user. It is not possible to delete TOTAL ARMING and TOTAL DISARMING.

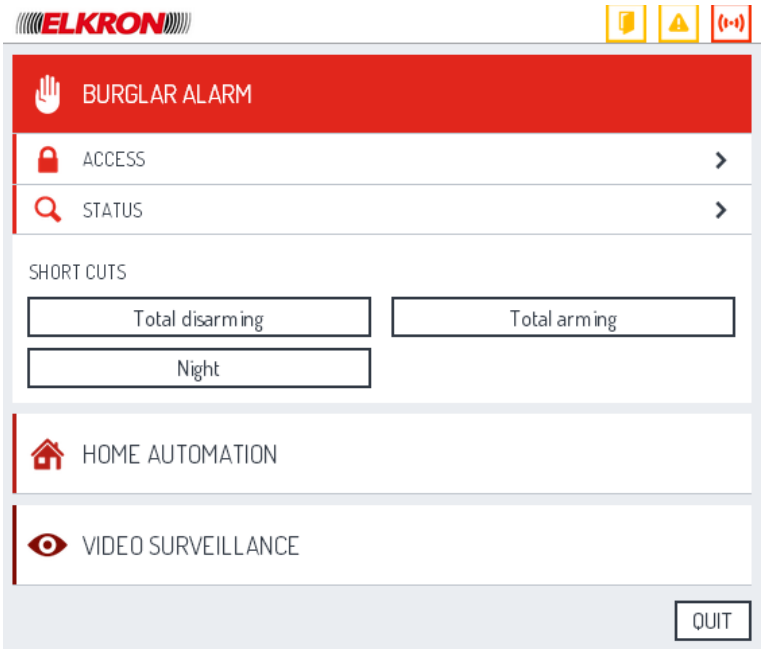
To delete a short cut:

1. Click on the name of the short cut: a list of the areas armed will appear with the DELETE and CHANGE keys.
2. Press the **DELETE** key.
3. A pop-up will appear with the message “Attention. Clicking on “Delete” will eliminate the short cut. Are you sure?”. Press the **DELETE** key again to close the pop-up and delete the short cut, or press the **CANCEL** key to close the pop-up without deleting the short cut.

ADVICE: If a short cut is no longer needed, it is not necessary to delete it; it can simply be disabled. In this way, if you should change your mind, it will not be necessary to recreate it from scratch. It can simply be enabled again.

How short cuts work

Short cuts are available on the BURGLAR ALARM section in the HOMEPAGE.



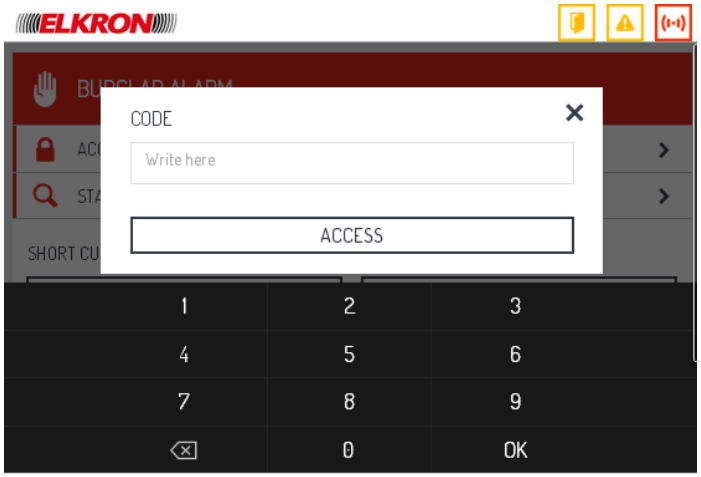
Short cut buttons can be black to indicate that the command is enabled, or grey, to indicate that the command is disabled.

To arm the alarm system, just press the TOTAL ARM button. No user code is required.

IMPORTANT! With the short cut buttons, all the users can arm the partitions associated with the button, even if they are not authorised to do so. This means that, under certain conditions, a user could arm partitions he will not be able to disarm.

If the TOTAL DISARM key is pressed, a pop-up appears where a valid 6-digit code must be inserted (Master or User). Insert the code and press the ACCESS button. The pop-up button for inserting the code works like the Access procedure.

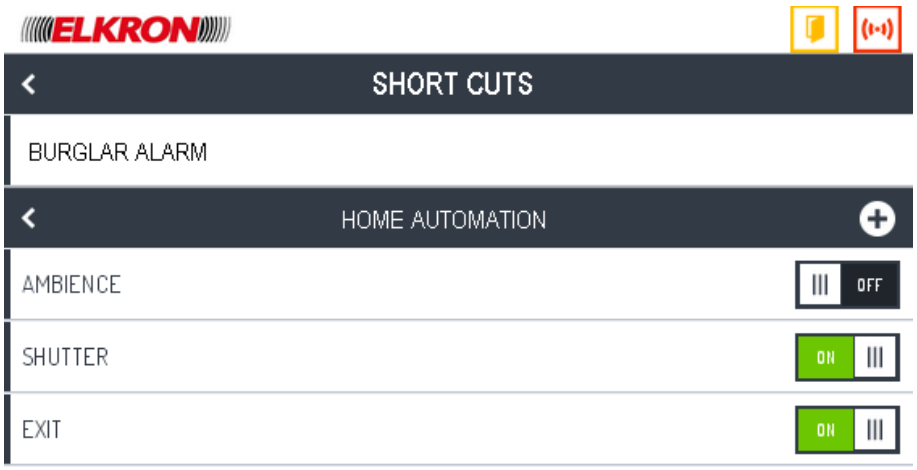
The partitions disarmed are only those assigned to the user who inserted the code.



For more information about short cuts (like how to enable, disable, create, modify, and delete them) see Burglar alarm section in Short cuts.

Home automation

WARNING! Screen before version 1.3.0-X



WARNING! Actual screen from version 1.3.0-X

It's possible to configure 4 scenarios.

To enable or disable a short cut, just click on the icon of the sliding switch to the right of its name: with ON the short cut will be enabled on the HOMEPAGE; with OFF it remains visible but is disabled (it cannot be clicked). When the scenarios are disabled, they simply change colour (grey instead of black).

NOTE: if the MASTER code is changed, you will need access to shortcuts, disable them all and then rehabilitate them.

For a more detailed description of how short cuts work, see How scenarios work.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

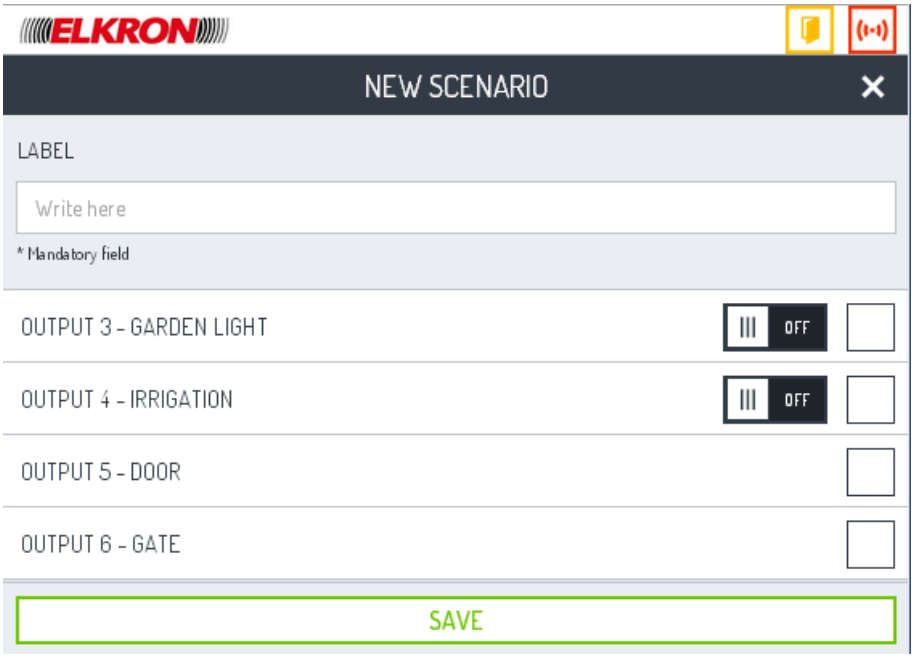
To return to the previous page, click on the icon **<** on the upper left of the title bar.

Configuring a new scenario

Short cuts can be created only by the Master user.

To create a new short cut:

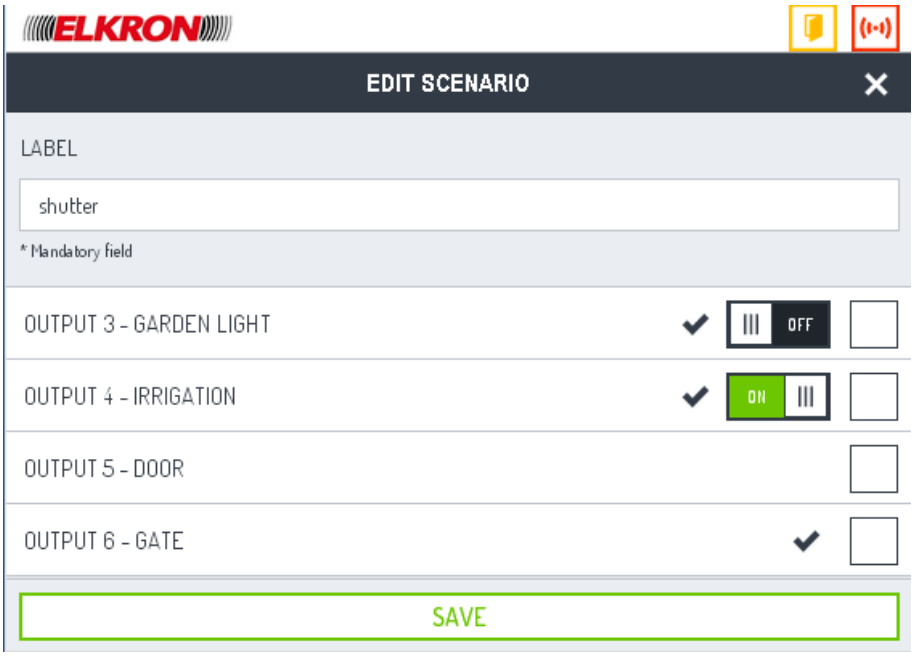
1. Click on the icon ⊕ at the top right of the HOME AUTOMATION section in SHORT CUTS page. The NEW SCENARIO page will appear. The icon ⊕ is visible only if it is still possible to insert a scenario.



2. It is necessary to insert a descriptive name for the new short cut in the “Label” field. The maximum length is 24 characters. **SAVE** button is disabled until at least a character is entered in Label field.
   The name inserted must be different from the short cut names already present. Any error will be signalled by the message “Short cut label already present. Insert a different name”.
3. Select by clicking on the selection square, the output to be activated or stimulated executing the scenario. For on-off output, it’s possible to define if they’ve to be activated or disactivated during scenarion execution.
4. Press the **SAVE** button to create the new scenario. If at least one output is not selected, the error message “Select at least one” will appear. Clicking on **X** icon, is possible to close the page discarding selections done.
5. The new scenario created is disabled by default and must be enabled in order to use it.

Changing a scenario

Scenarios can be changed only by the Master user.



To change a scenario:

1. Click on the name of the scenario: a list of the selected output and their configuration will appear with the DELETE and CHANGE keys.
2. Press the **CHANGE** button. The page used to create a new scenario will reappear.
3. Change the name of the scenario and add or remove output or change their configuration as needed. The changes must comply with the same rules for Configuring a new scenario.
4. Press the **SAVE** button to memorise and confirm the changes made.

Deleting a scenario

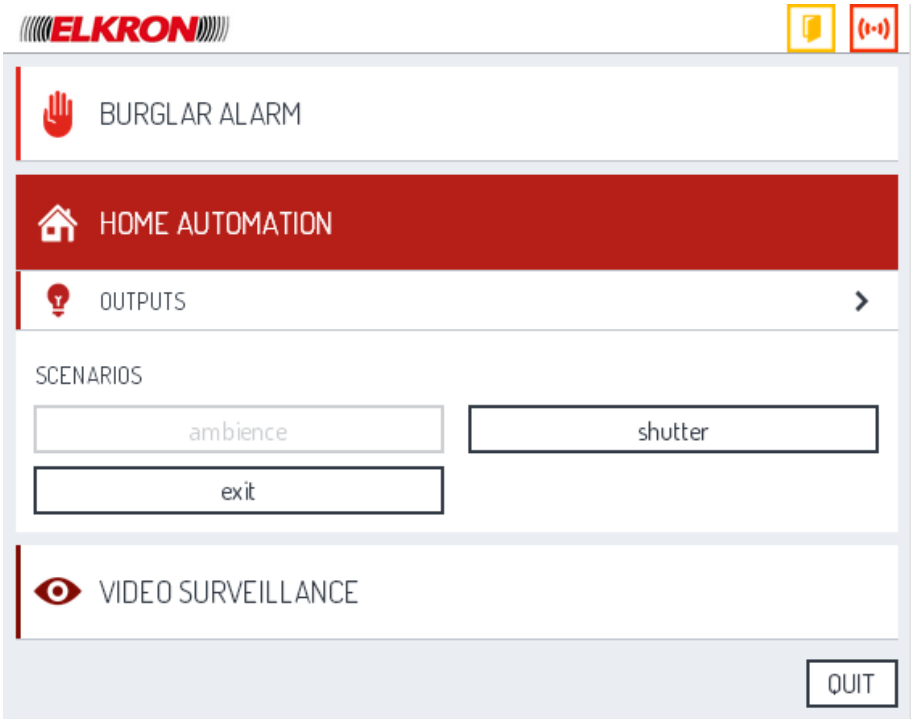
The scenario can be deleted only by the Master user.

To delete a scenario:

1. Click on the name of the scenario: a list of the selected output and their configuration will appear with the DELETE and CHANGE keys.
2. Press the **DELETE** key.
3. A pop-up will appear with the message “Attention. Clicking on “Delete” will eliminate the scenario. Are you sure?”. Press the **DELETE** key again to close the pop-up and delete the scenario, or press the **CANCEL** key to close the pop-up without deleting it.

How scenarios work

Scenarios are available in HOMEPAGE, under HOME AUTOMATION section.



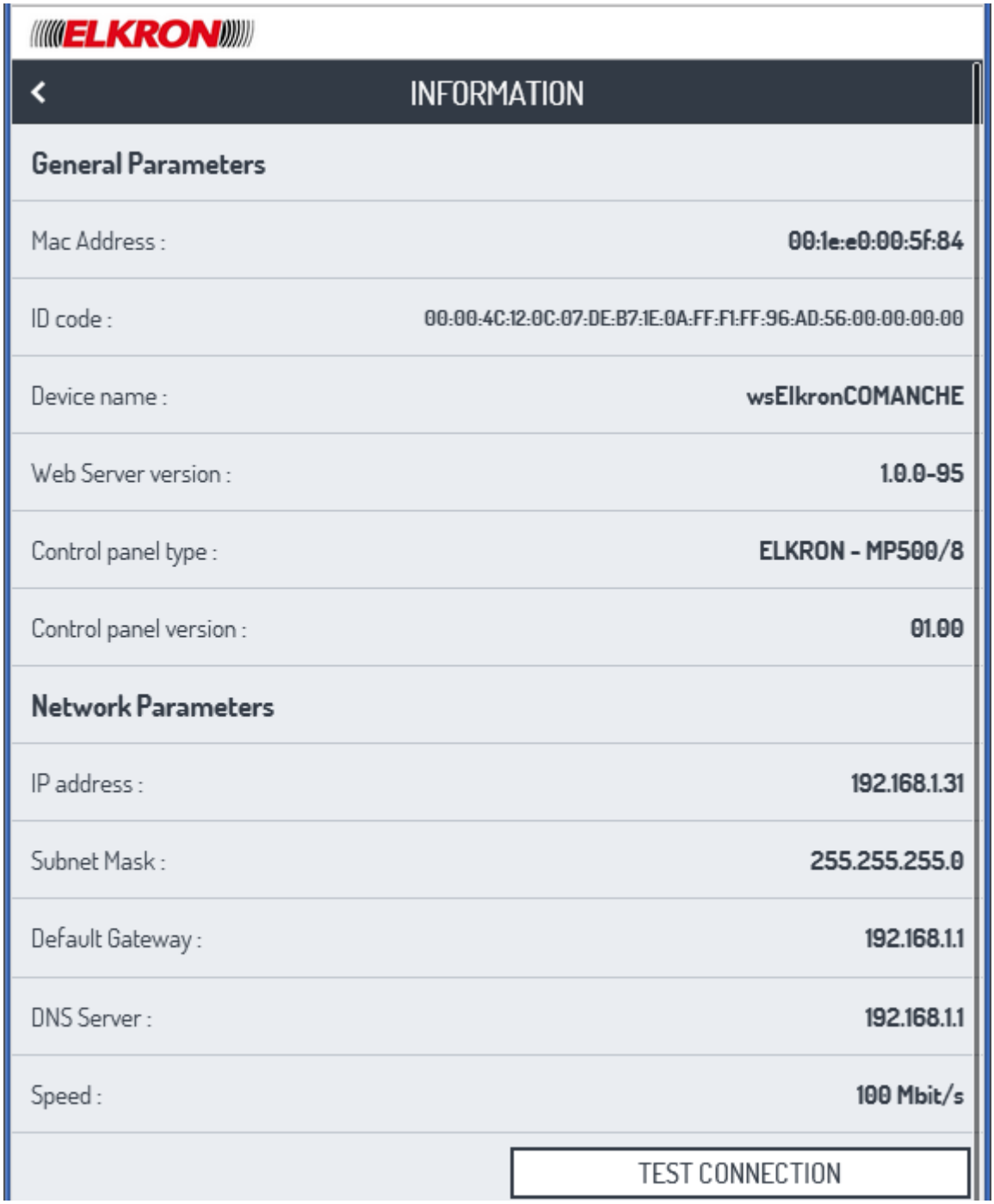
Short cut buttons can be black to indicate that the command is enabled, or grey, to indicate that the command is disabled.

To execute a scenario, just click on the button. No user code is required.

For more information on scenarios (how to enable, disable, create, edit or delete) please check Home automation section in Short cut page.

Information

The INFORMATION page can be accessed from the Settings page. This page is visible to all users. On this page the user can find the general technical information about the system.



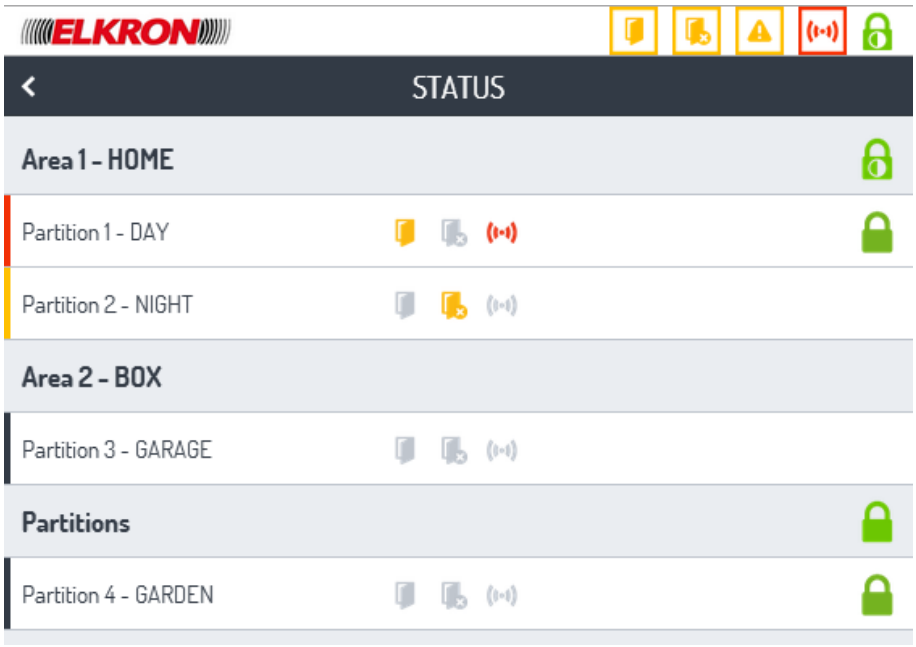
The information available is:

- **Mac address**: MAC address of the Web Server.
- **ID Code**: ID code of the Web Server.
- **Description**: Elkron.
- **Web Server Version**: version of the Web Server firmware.
- **Type of control panel**: model of the alarm control panel to which the Web Server is connected.
- **Control Panel Version**: version of the alarm control panel firmware.
- **IP Address**: IP address of the Web Server.
- **Subnet mask**: subnet mask used by the Web Server.
- **Default Gateway:** gateway address
- **DNS Server**: IP address of the server that provides the DNS server.
- **Speed**: the LAN transmission speed.

Clicking the button “Connection test” some checks will be automatically performed to verify the network connection and the mail forwarding.

Status

The STATUS page can be accessed from the Burglar Alarm section.



On this page the user can verify the current status of the burglar alarm system.
The areas and partitions of the entire system are visualized. If there are no signals for a partition, the corresponding icons are grey.

Click on the name of a partition to expand it and show the complete list of all the inputs associated with it. For every input, the relative icons indicate its status: alarm, open, isolated.

IMPORTANT! Unlike the other pages of the Web Server that display similar information, the STATUS page has some very interesting features:

- It can be visualized without having to log in.
- It lists all the inputs and partitions, not only those for which there are signals.

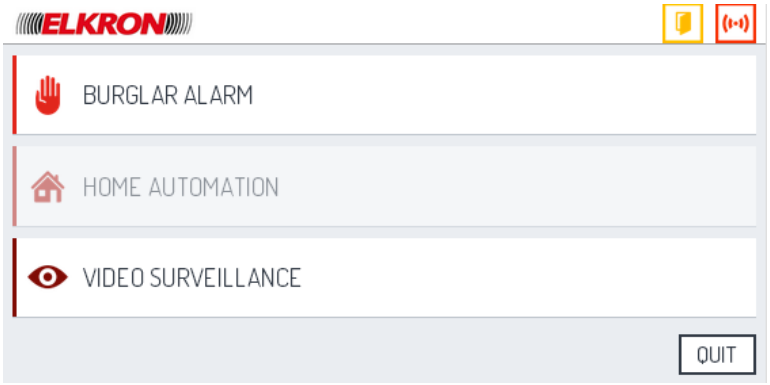
The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

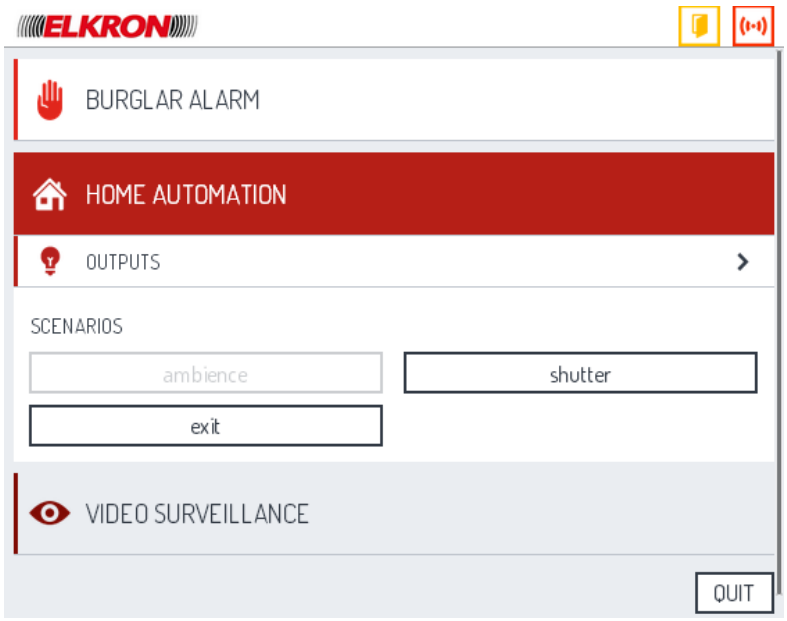
Home automation

The HOME AUTOMATION section can be accessed from the Homepage.

If the HOME AUTOMATION label is grey, it means that there are no home automation output configured in the burglar alarm plant and it is not possible to expand the section.



If at least a home automation output has been configured in the burglar alarm plant, the HOME AUTOMATION button is enable and it's possible to click to expand the section.



There are two sections:

- Outputs, allows authentication and access to page Home automation output management to activate/de-activate or stimulate outputs.
- Scenarios, to execute configured scenarios. Clicking on any scenario is displayed an information pop-up about command sending status (from 1.3.0-X version and subsequent).

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

Clicking again on Home automation, the section is collapsed.

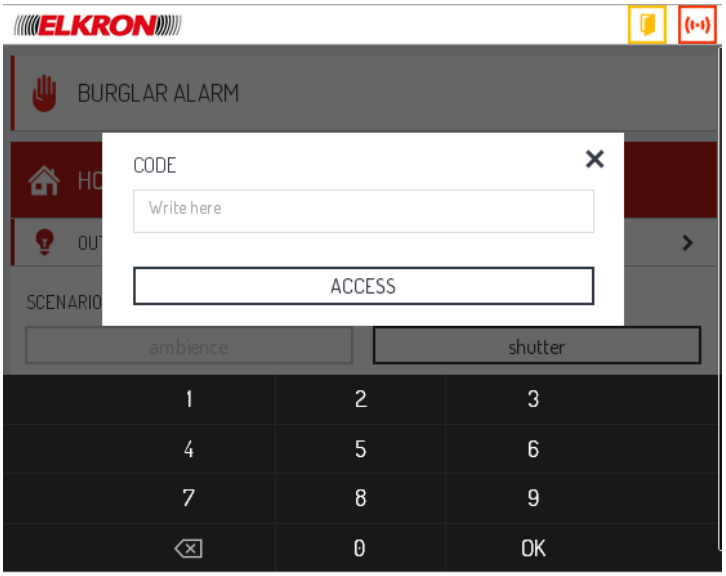
If you click the **QUIT** button, you will be disconnected from the system and return to the login screen.

Outputs

The ACCESS procedure can be accessed from the Home automation section.
Use this procedure to access the home automation outputs directly, if access not already performed from Burglar Alarm section.

Access authentication

When you start the ACCESS procedure, a pop-up appears so you can authenticate who you are if not already done in Burglar alarm section.



Digit a valid access code and press the **ACCESS** button. The access code is the 6-digit numerical code used to access the alarm system via the physical keypad, not the password used to access the Web Server.
WARNING: If the access codes configured in the control panel are less than 6 digits long, it must first be reconfigured as a 6-digit number in order to access the control panel via the Web Server.

The ⌫ key cancels only the last digit and OK button is the same as ACCESS, it sends the code to the system.
The operations that can be carried out after entering the system depend on the privileges possessed by the access code inserted.

To close the pop-up window without attempting to access the system, click outside of the virtual keypad and the pop-up or press the **X** icon on the pop-up. In this way, even if a code has been inserted, it is eliminated and not checked, and the counter of incorrect access attempts remains unchanged.

If the code inserted is correct, the management page (Home automation output management) of the home automation plant.

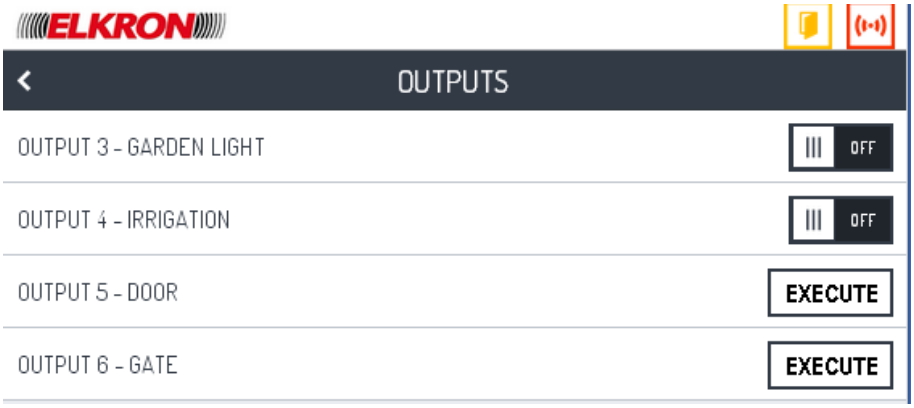
If the code inserted is wrong, or no code is inserted before pushing the **ACCESS** button, an error message appears. The counter of the failed access attempts is increased by 1.

The maximum number of failed access attempts is 21 (the limit is set by the burglar alarm control panel and cannot be changed). If an incorrect access code is inserted for more than 21 consecutive times, the control panel generates a “wrong code” alarm.

Home automation output management

It's possible to access to home automation outputs page from Access authentication procedure.

This page access to functions to manage each home automation output.



The page shows:

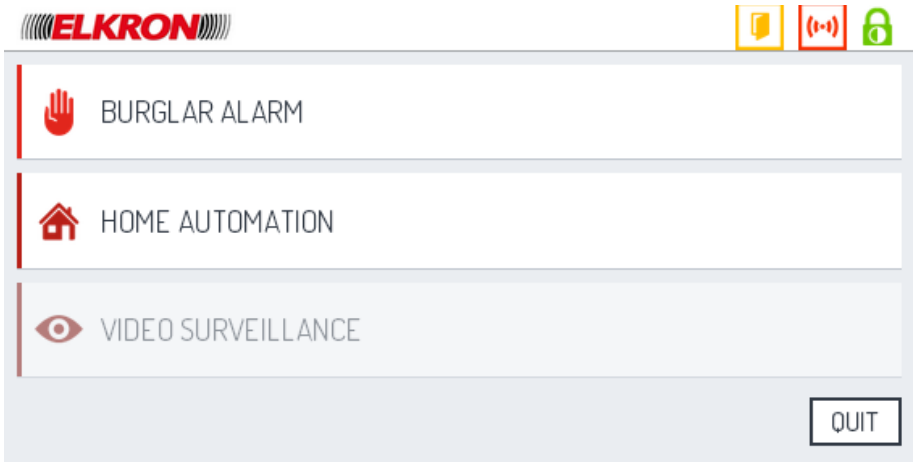
- **Id and name of each output to be activated** in the image above for example OUTPUT 3 – Garden light and OUTPUT 4 - Irrigation. The sliding button OFF indicate it's possible to activate or de-activate the output.
  Id and name of each toggle output in the image above for example OUTPUT 5 – Door and OUTPUT 6 – Gate. The execute button indicate it's possible to send a single impulse to toggle the output.
- The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon < on the upper left of the title bar.

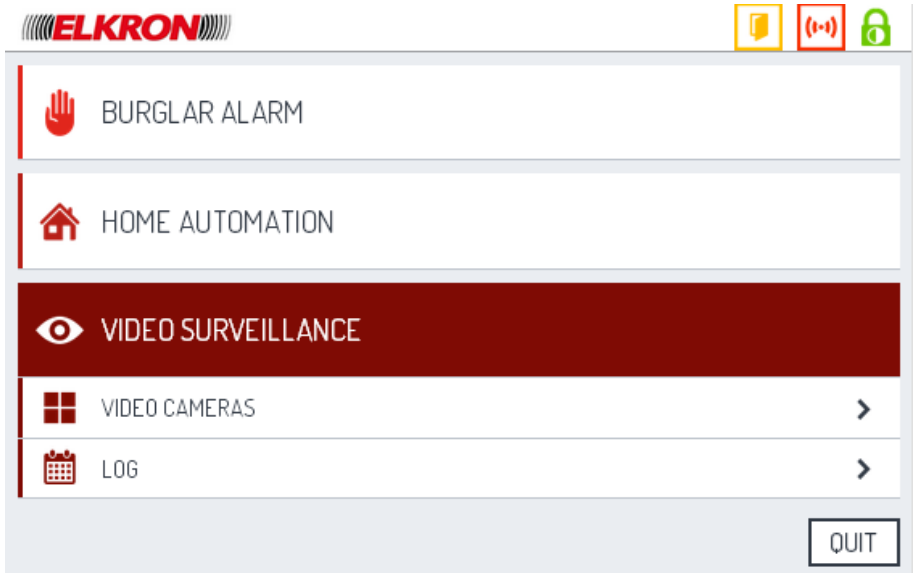
Video surveillance

The VIDEO SURVEILLANCE section can be accessed from the Homepage.

If the VIDEO SURVEILLANCE button is disabled, it means that there are no cameras configured and it is not possible to expand the section.



Instead, if there is at least one video camera configured, clicking on the VIDEO SURVEILLANCE button will expand the section.



The following buttons will appear:

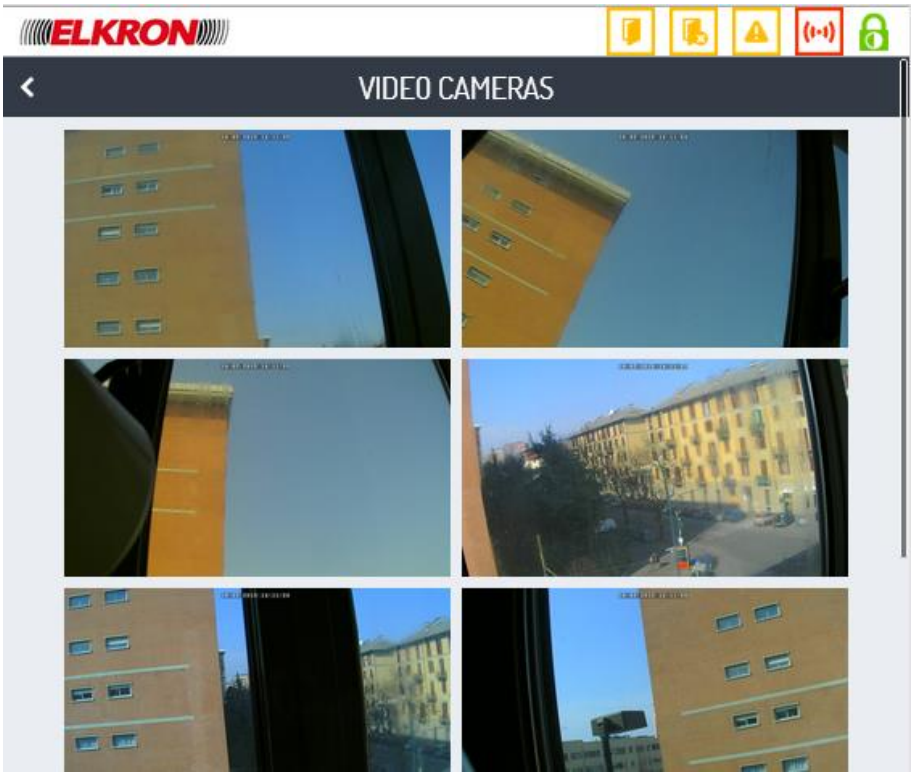
- Video cameras, that allow the user to see the images taken by the video cameras in real time.
- Log, which makes it possible to see, send by mail and save the images of the video cameras saved after an alarm event.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

If you click the **QUIT** button, you will be disconnected from the system and return to the login screen.

Video cameras

The VIDEO CAMERAS page can be accessed with the VIDEO CAMERAS button of the Video surveillance section.



On this page the user can manage the previews of the video cameras acquired and associated (max 8). Each frame of the preview is associated with only one video camera.

The previews are updated alternately with an interval of 1 second between a video camera and another (for example, if there are 3 video cameras, the image of the individual camera will be updated every 3 seconds).

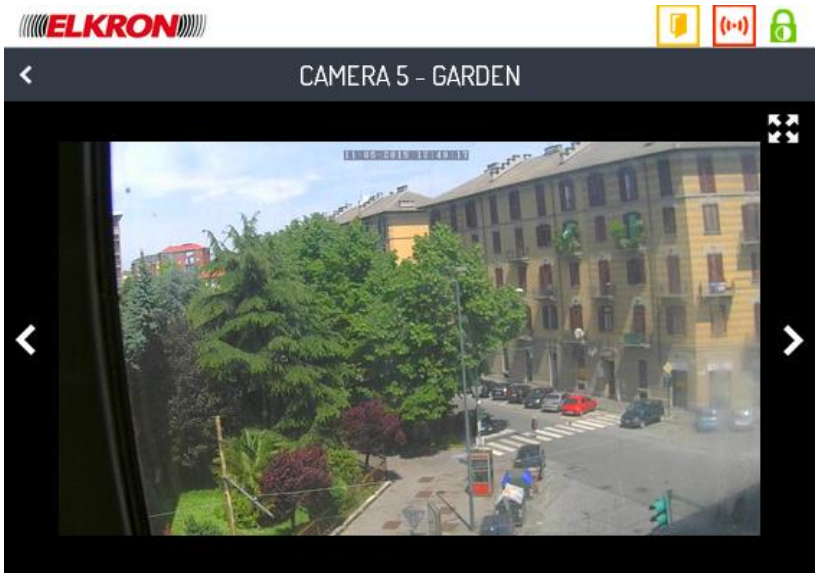
If the image of the video camera is not available, a grey frame with the word VIDEO on it will appear.

Click on the preview to open the Video camera detail page.

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

Video camera detail page

The video camera detail page can be accessed by clicking on its preview frame on the Video cameras page.



The video image is updated once every second. The date and time are superimposed on the upper part of the image. instead, the title of the page indicates the name attributed to the video camera during configuration.

If more than one video camera was acquired and associated, the navigation buttons **<** and **>** to move from one camera to another will appear.

Clicking on icon l the image is showed in full screen.

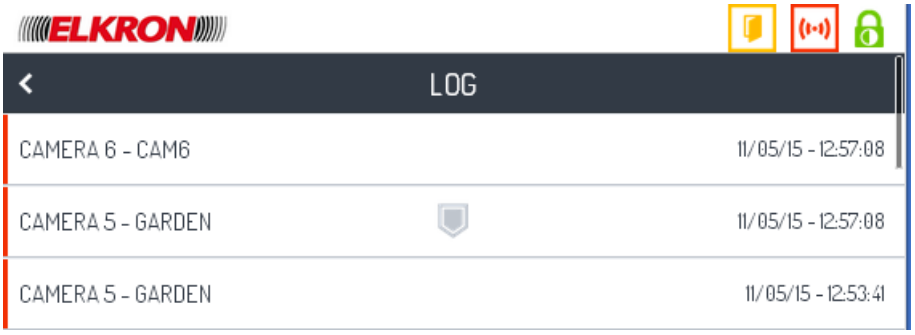
It's possible to go back to windows screen clicking on icon

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

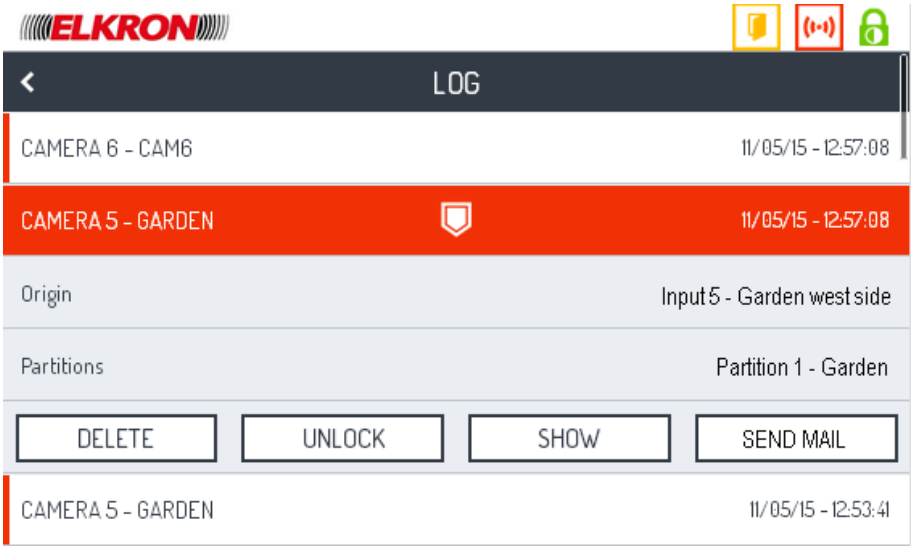
To return to the previous page, click on the icon **<** on the upper left of the title bar.

Log

The Video surveillance log can be accessed with the LOG button of the Video surveillance section.



When the page opens, all the events will appear in chronological order. Each event is identified by the name of the camera and by the date and time it occurred.



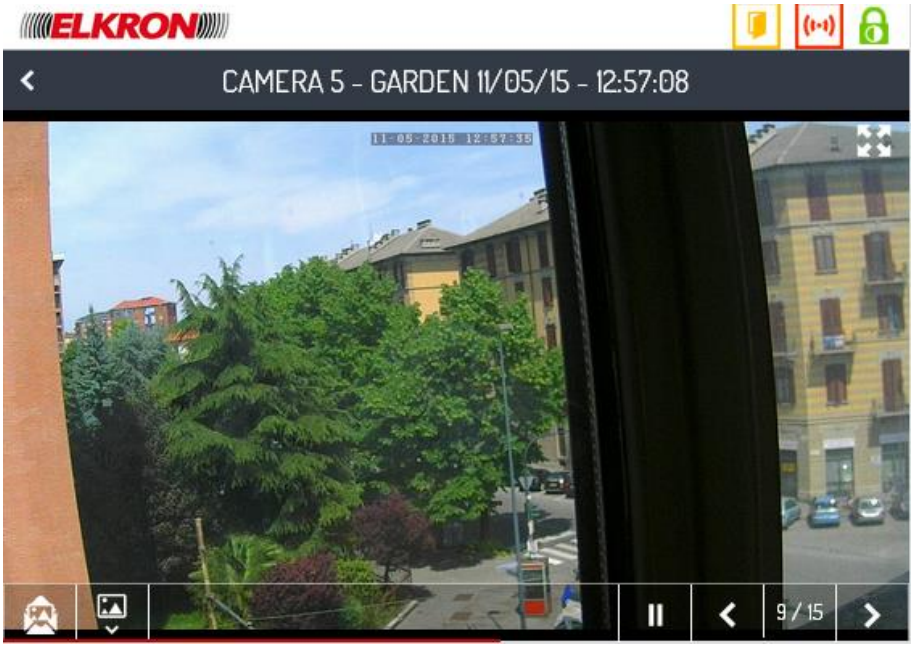
Click on an event to expand it and find:

- the name of the input that signalled the alarm;
- the name of the partition associated with the input that signalled the alarm and triggered the video recording;
- the **DELETE** button, that makes it possible to manually delete the event and the relative images;
- the **BLOCK** button, that makes it possible to block the event and prevents its automatic deletion.
  ATTENTION! Blocking events reduces the memory available to memorise new events. An event should be blocked only until the images recorded are downloaded and saved on another support.
- The **SHOW** button, to view and save the images.
- The **SEND MAIL**, button, to send all images of the event to all contacts configured for burglar alarm notification.

Clicking a second time on the name of the event, the details are hidden.

If an event was blocked, the list of the events will have an icon and instead of the BLOCK button, an **UNLOCK** button will appear.

When you click on **VIEW**, a new window appears:



The title bar will contain the name of the event. The **<** button on the title bar returns to the previous page.

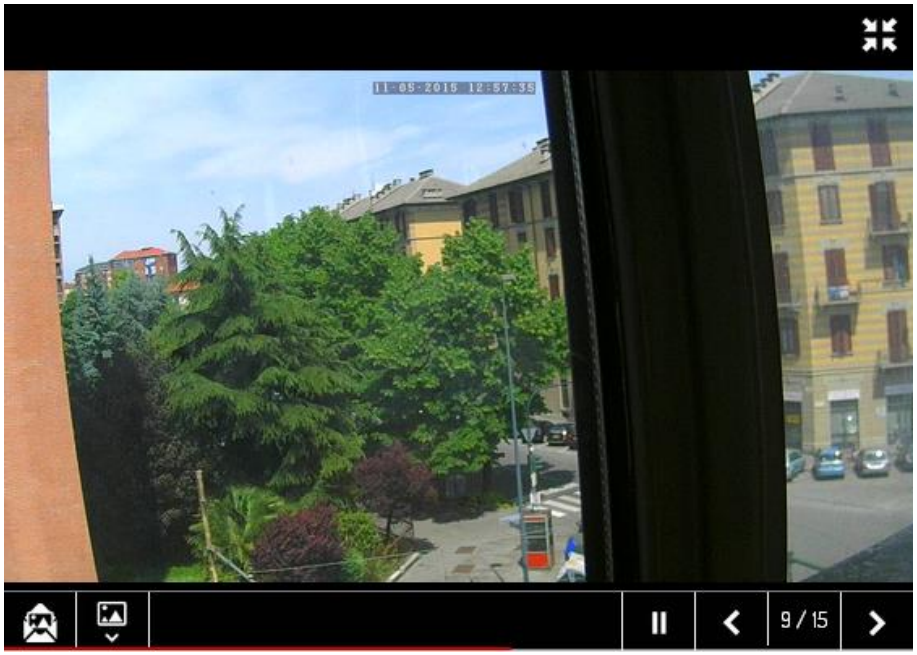
Button sends current image to all contacts configured for burglar alarm notification.

Using your PC with Chrome and Firefox browsers, versions supported (see chapter Compatible browsers), you can download the image using the button .

Button  starts playing the slide show of all images, it can be paused clicking on 

The two buttons  and  allow manual navigation back and forth among the images; the red bar, at the bottom of the page, shows slideshow progress such as the indication number (for example ).

Clicking on icon  the image is showed in full screen.



It's possible to go back to windows screen clicking on icon  .

The icons at the top indicate the system status. Their meaning and behaviour is explained in the description of the Homepage.

To return to the previous page, click on the icon **<** on the upper left of the title bar.

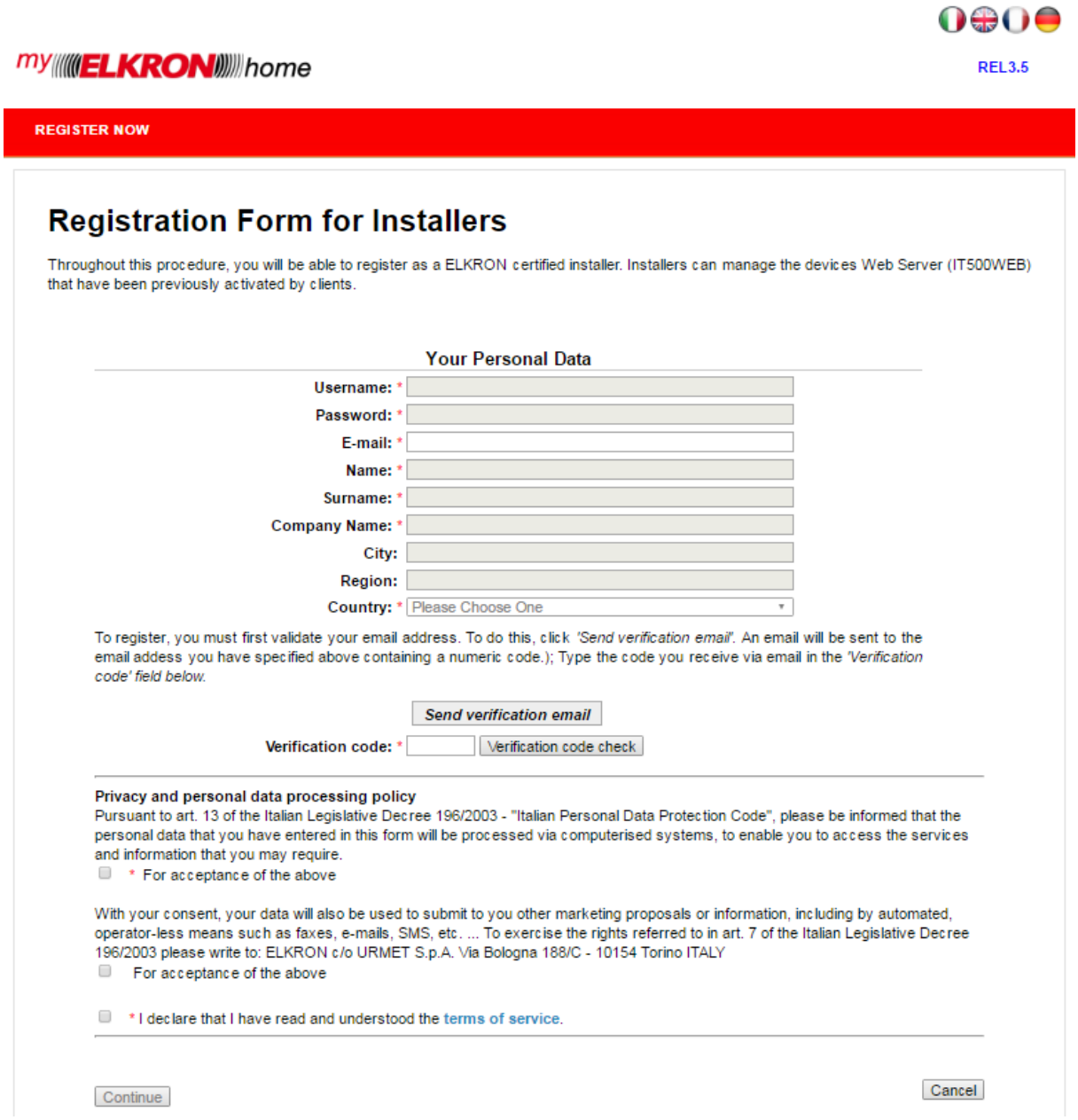
Server registration

The device must be registered on the www.myelkronhome.com portal in order to use the remote web server.

The device can only be registered by the installer. For this reason, the installer must have an account (see the “Installer registration” section for more details).

Installer registration

To record an installer account, go to the portal at www.myelkronhome.com and select “REGISTER NOW”. The following page will appear:



Enter the installer's valid email address in the ‘‘E-mail’’ field and click on ‘‘Send verification email’’. Enter the code you received by email in the ‘‘Verification code’’ field (check your spam inbox if you do not receive the email after a few minutes) and click on ‘‘Verification code check’’. All the other fields will be enabled at this point. Enter the mandatory data (marked with an asterisk) and tick the privacy and personal data processing policy boxes (also marked with asterisks).

The password must respect the following safety criteria:

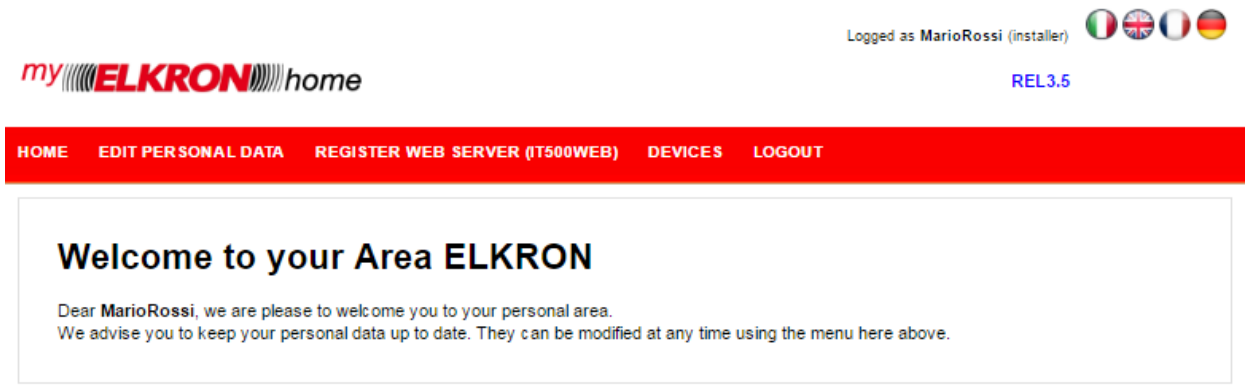
- It must be at least 8 characters long.
- It must contain at least one upper case letter.
- It must contain at least one lower case letter.
- It must be at least 1 special character.
- It must contain at least one digit.
- The username cannot be contained in the password.

Press “Continue” to end the registration procedure or “Cancel” to cancel it.

You will receive a confirmation email at the end of the registration procedure.

Installer access

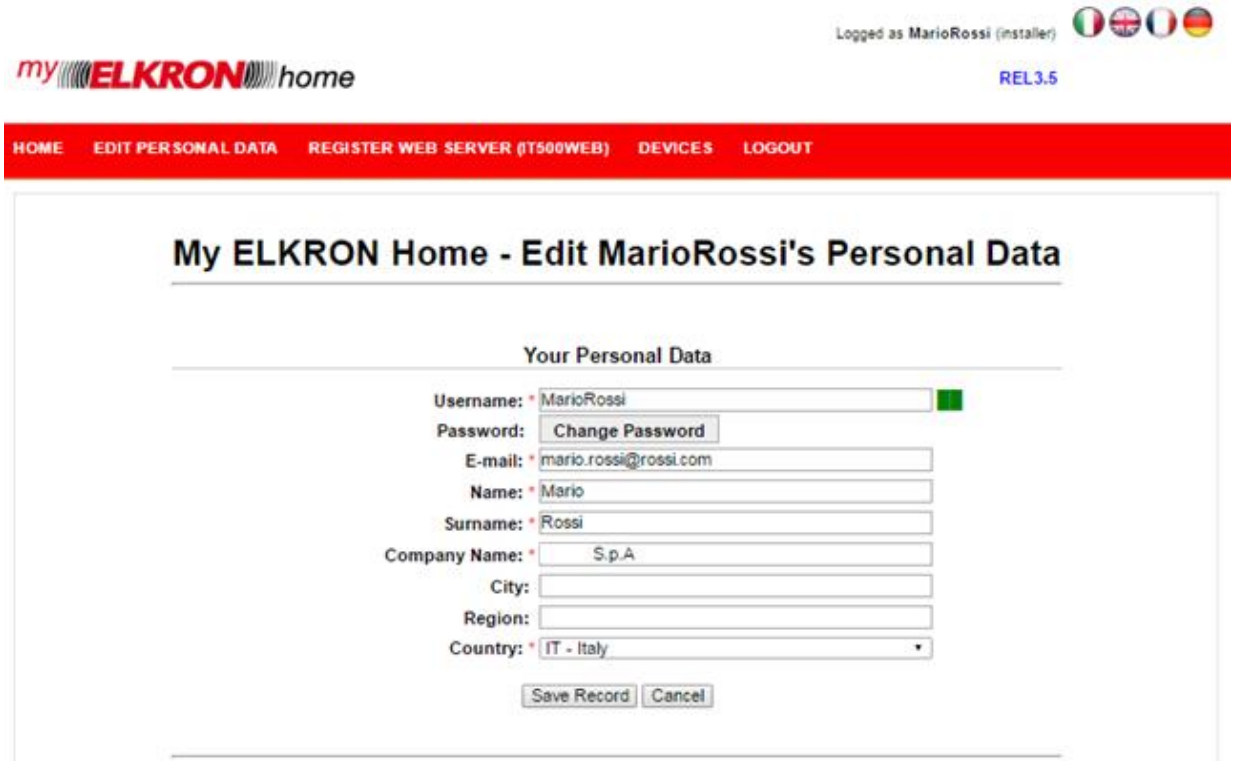
Home section



The installer will be routed to the respective Home page after logging in.

In this section you can manage your data (“EDIT PERSONAL DATA”), register a new Web Server (“REGISTER NEW SERVER (IT500WEB)”), manage your devices and those of your customers (“DEVICES”) and logout (“Logout”).

Edit personal data section

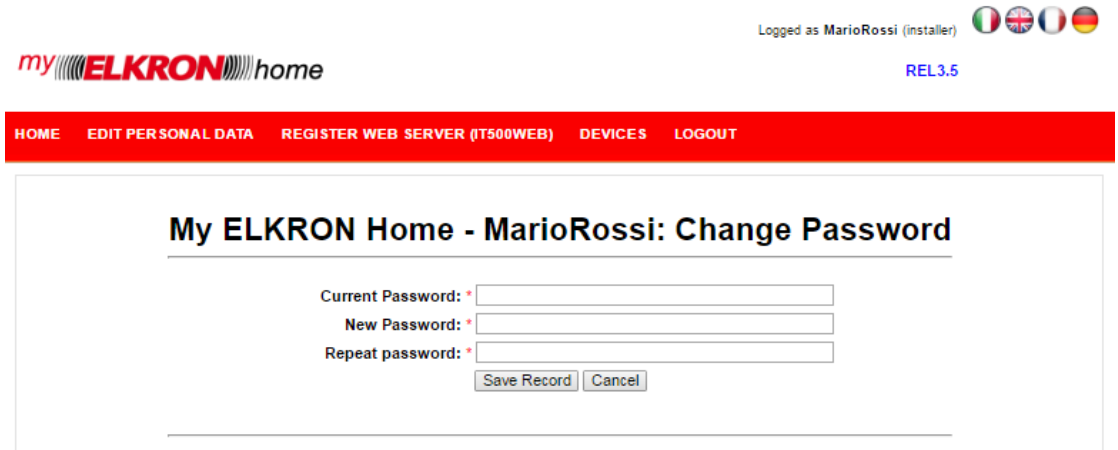


You can update your personal data on this page.

The username must respect the following safety criteria:

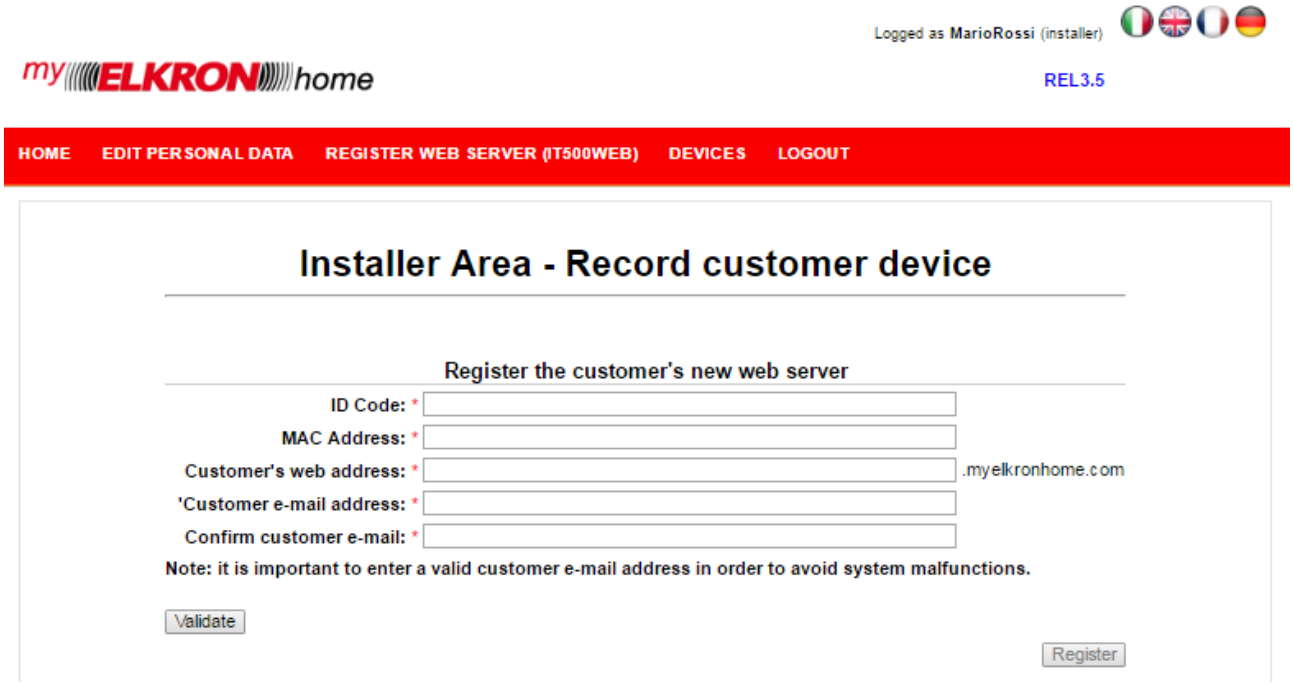
- It must be at least 6 characters long.
- It must be no more than 30 characters long.
- The following special characters are allowed but not mandatory (other special characters are not allowed): - _ & @ .
- User names starting with w00_1E_E0_ are not allowed.

To change your password, click on “Change password”. All other data can be edited directly on the page.
Click on “Save Record” to confirm any changes.

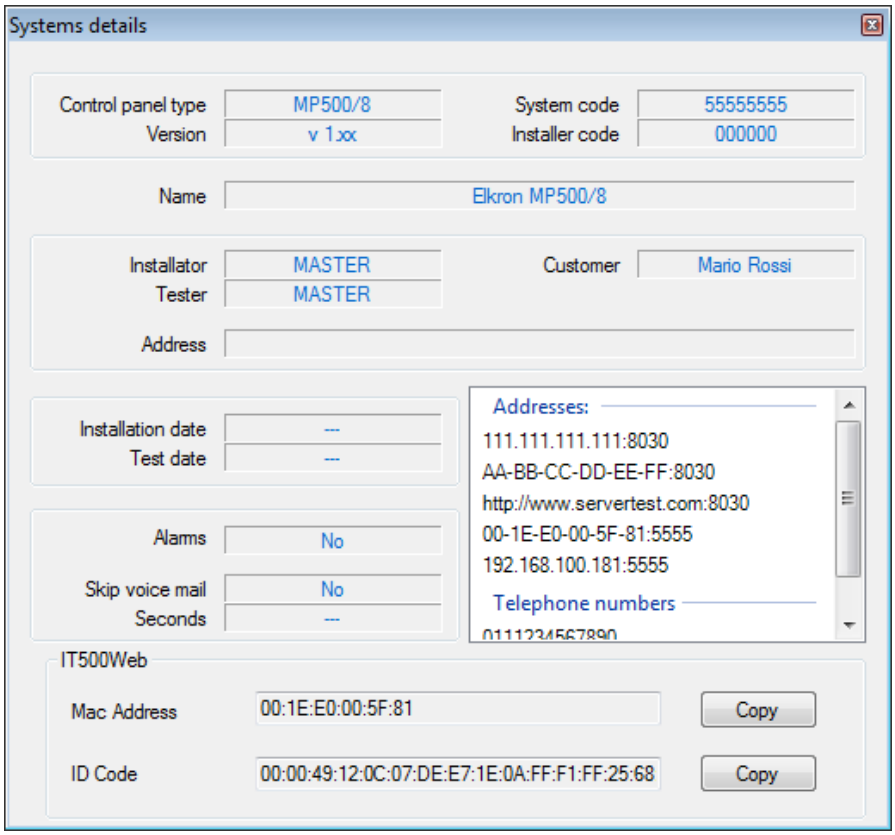


To change the password, enter the password currently in use and the new password. Then type in the new password again. Click on “Save Record” to confirm the change.

Register New Server section (IT500WEB)



Enter the data on the device to be registered in this section. The following data will be requested: Mac Address, ID Code, web address and the customer's email address. The first two can be retrieved on the “System details” page of Hi-Connect.



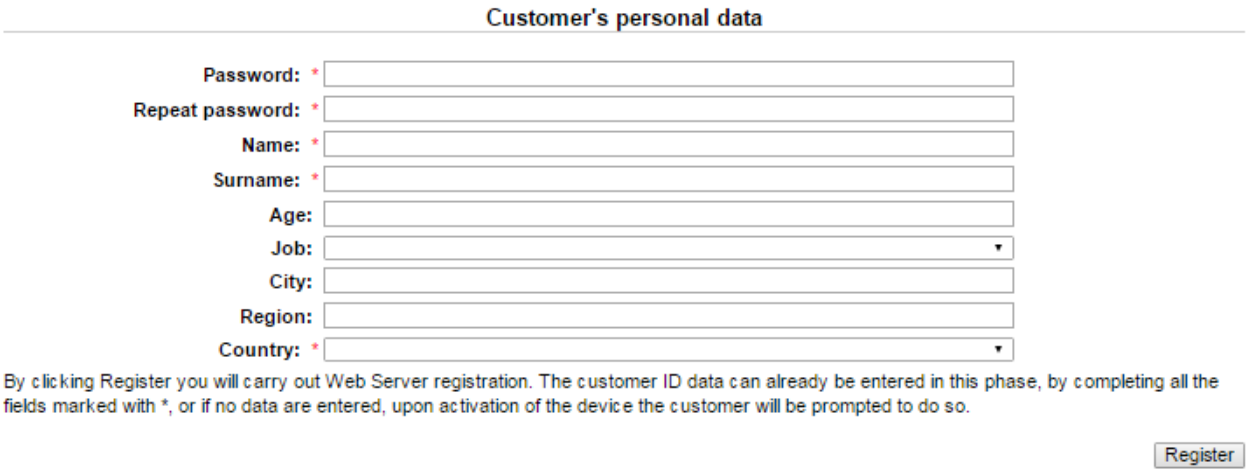
The web address must be chosen by the user and will be used in the future to access the system from an external network. For example, if the chosen address is “webserver”, enter http://webserver.myelkronhome.com in the browser to access your system.

Enter all the required data and click on "Validate".

WARNING! Importantly, the customer's email address must be valid and active to avoid system malfunctions.
Click on "Validate". A form to be filled in with the customer's details will appear if the entered data are correct. You can fill in all the fields marked with an asterisk (*) or leave all fields blank and proceed with the registration. A user account will be automatically created and an email containing a summary of the information will be sent the indicated address. The customer must click on the link received by email to activate the Web Server. See “Customer access” for more details.

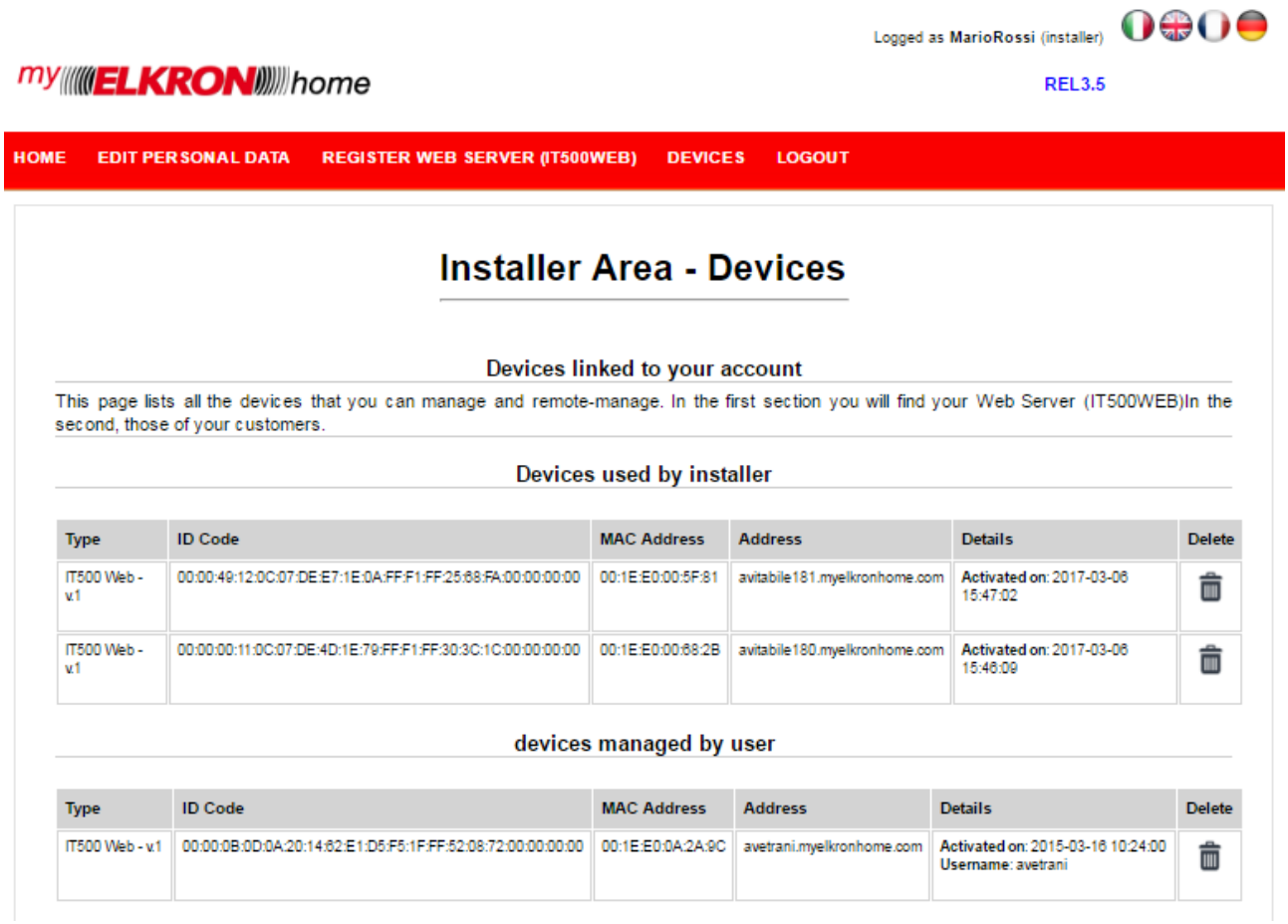
WARNING! If the indicated address is already included in the system, a summary of the customer's details will be shown and cannot be edited. In this case, a new user account will not be created and the newly registered Web Server will be associated with the user already present in the system. In all cases, activation is needed by clicking on the received email to activate the device.

WARNING! If the installer's email address is provided, the Web Server will be automatically considered as one of the installer's devices and no confirmation email will be sent. The device will be activated automatically.



Click on “Register” to complete the registration procedure.

Devices section



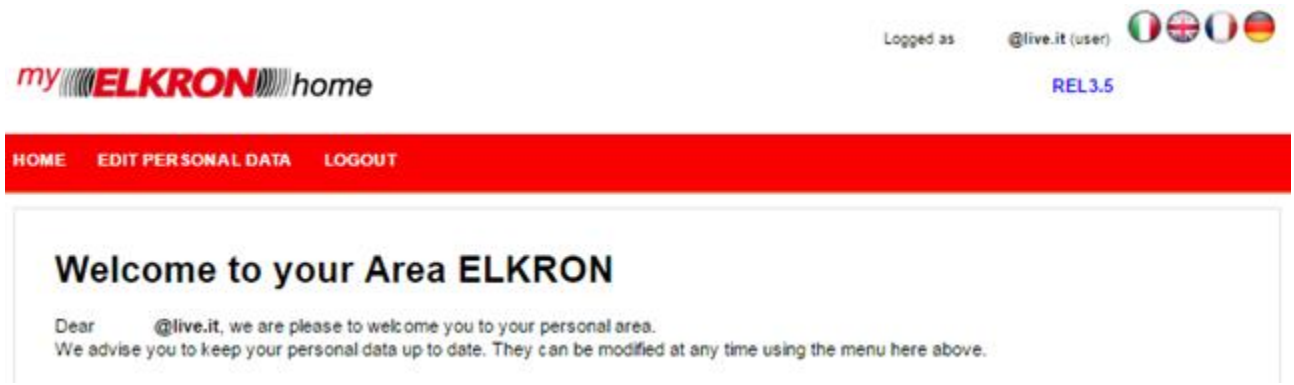
The “DEVICES” page is split into two sections: the installer's Web Servers, for which the installer is the end customer/user, are shown in the first section and the devices of the installer's customers that the installer can remotely manage are shown in the second section. From here you can:

- Ask to send a new email containing the link to be clicked on to activate the Web Server immediately after it was registered (useful if the user does not receive the email or deletes it by mistake before clicking on the link). The “Resend activation email” button will only be available for devices which have still not been activated. The button will no longer appear after the link has been clicked.
- Ask to delete the registration of a system by using the Delete button (trash can icon). To confirm deletion of a Web Server the customer must click on the email they will receive by email.
- Ask to send a new email containing the link to be click on to confirm Web Server deletion. The “Resend activation email” button is only available for the devices for which deletion was requested and only until the customer confirms the operation by clicking on the link received by email.

⚠ **WARNING!** If the Web Server to be deleted is one used by the installer, and therefore listed in the first section, no email containing a link to be clicked to confirm will be send and deletion will be confirmed automatically.

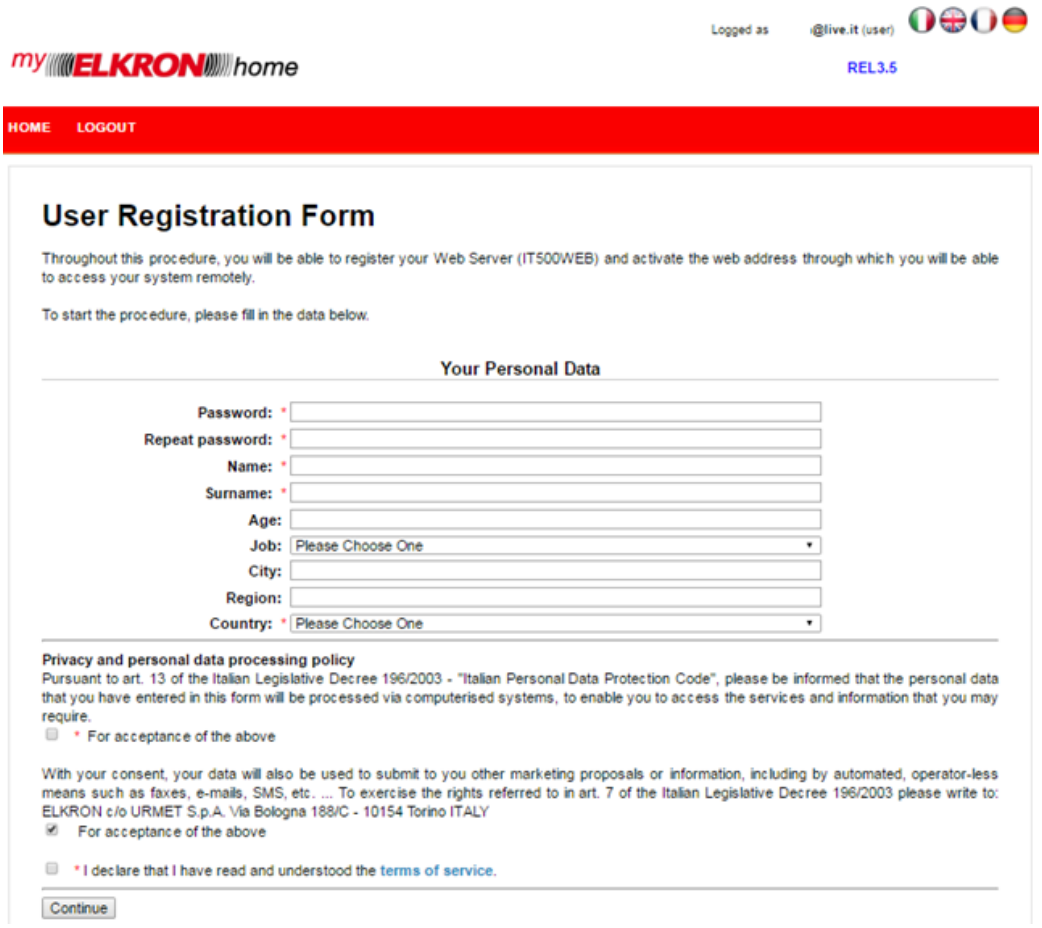
Customer access

Home section

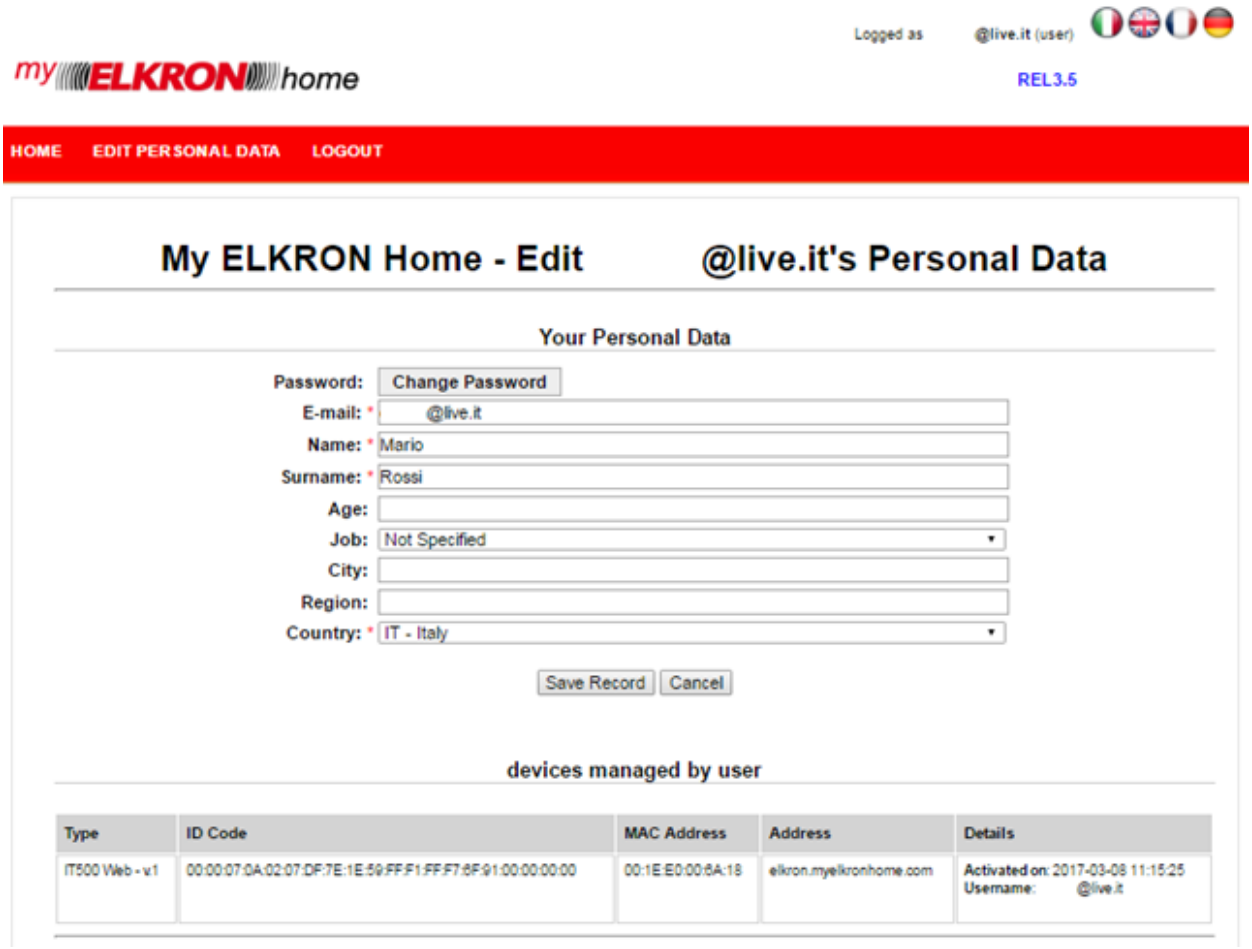


The customer will be routed to your Home after logging in.
From here, you can access the section for managing your data (“Edit personal data”) or logout (“Logout”).

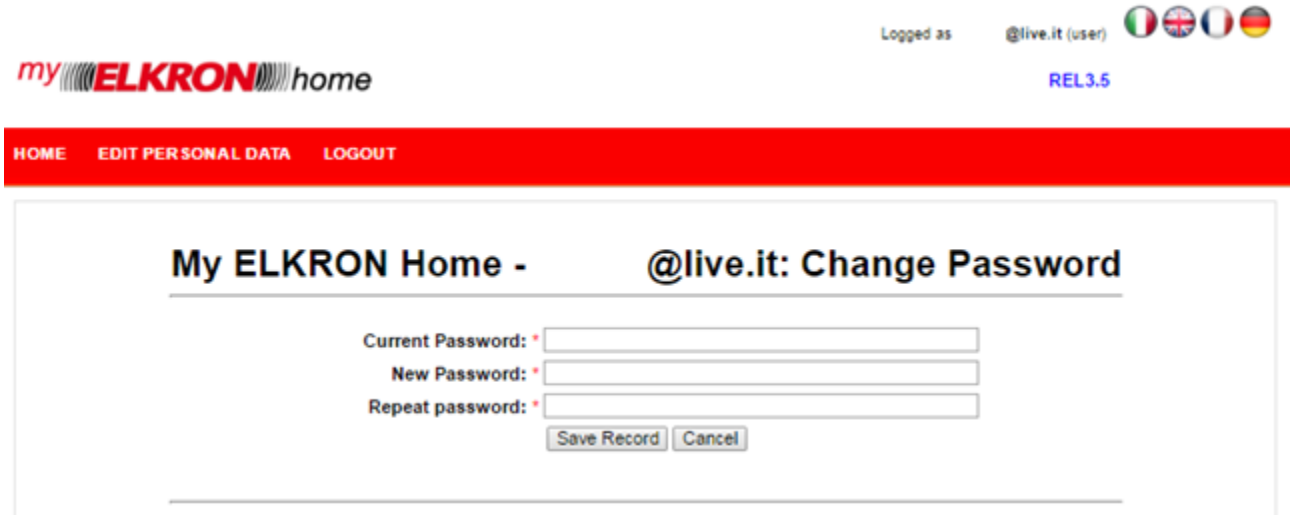
At the first access, you will be required to enter the data entered by the installer during Web Server (IT500WEB) registration or to enter them if the installer has not done so already. Any operations in progress, such as registration or deletion confirmation, will be automatically confirmed after accessing by means of the link received by email and after having confirmed the first access data.



Edit personal data section



On this page, the customer can see the details of their IT500WEB and update personal data. To change your password, click on “Change password”. All other data can be edited directly on the page. Click on “Save Record” to confirm any changes.



To change the password, enter the password currently in use and the new password. Then type in the new password again. Click on “Save Record” to confirm the change.

Elkron control unit diagrams for Home Automation applications

Integrated (Yokis/Elkron) Home Automation enables to fully monitor homes remotely by using a telephone, smartphone, tablet or computer, and also allowing for emergency message sending.

Automation helps improve clever and efficient home monitoring thanks to the centralising of controls.

Remotely controlled home automation systems can be expanded in time to manage:

- Lighting control, timers, light turning-off and lighting scenes
- Rolling shutter and motor drive control (opening and closing)
- Controls centralising
- Efficient electric power use and power consumption optimising

ON/OFF radio control of a MTR2000ER via an E4BPP channel

E4BPP wiring to the control panel with electrical output

(*) WARNING: CONTROL PANEL HW CONFIGURATION

IMPORTANT

If a Control panel electrical output is used, the corresponding jumper must be moved to the position "-" before connecting the transmitter. Otherwise, the transmitter will be irreparably damaged.

CONTROL PANEL SW CONFIGURATION

By using the keypad or the Hi-Connect programming software, configure the output as follows:
- OUTPUT TYPE = OUTPUT N.L.
- CUSTOMIZE = O. COMMANDABLE

DIRECT CONNECTION

Briefly press 5 times the temporary pushbutton connected to the transmitter. The transmitter LED will start flashing for 30 seconds to indicate that it is waiting for connection.

While the transmitter LED is flashing, shortly press the MTR2000ER "connect" hole located in the rear part with the tip of a pencil.
The transmitter LED will stop flashing.

Warning! The receiver must be powered on.

INSTANTANEOUS MODE CONFIGURATION (=ON/OFF)

Briefly press 10 times the temporary pushbutton connected to the transmitter to enter the Configuration Menu: the transmitter LED will start flashing rapidly.

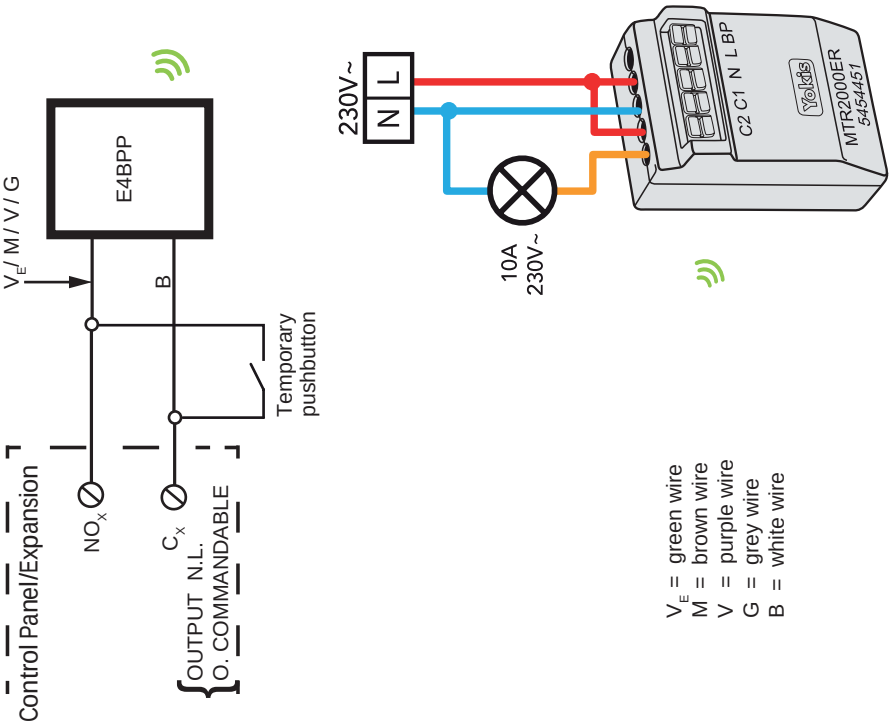
While the LED is flashing, briefly press the pushbutton 17 times: the transmitter LED will respond by flashing 7 times.

From now on, the light connected to MTR2000ER will be correctly piloted by the control panel or the expansion in the ON/OFF mode.

SD542-9000

ON/OFF radio control of a MTR2000ER via an E4BPP channel

E4BPP wiring to the control panel/expansion with relay output



CONTROL PANEL SW CONFIGURATION

By using the keypad or the Hi-Connect programming software, configure the output as follows:
- OUTPUT TYPE = OUTPUT N.L.
- CUSTOMIZE = O. COMMANDABLE

DIRECT CONNECTION

Briefly press 5 times the temporary pushbutton connected to the transmitter. The transmitter LED will start flashing for 30 seconds to indicate that it is waiting for connection.

While the transmitter LED is flashing, shortly press the MTR2000ER "connect" hole located in the rear part with the tip of a pencil.
The transmitter LED will stop flashing.

Warning! The receiver must be powered on.

INSTANTANEOUS MODE CONFIGURATION (=ON/OFF)

Briefly press 10 times the temporary pushbutton connected to the transmitter to enter the Configuration Menu: the transmitter LED will start flashing rapidly.

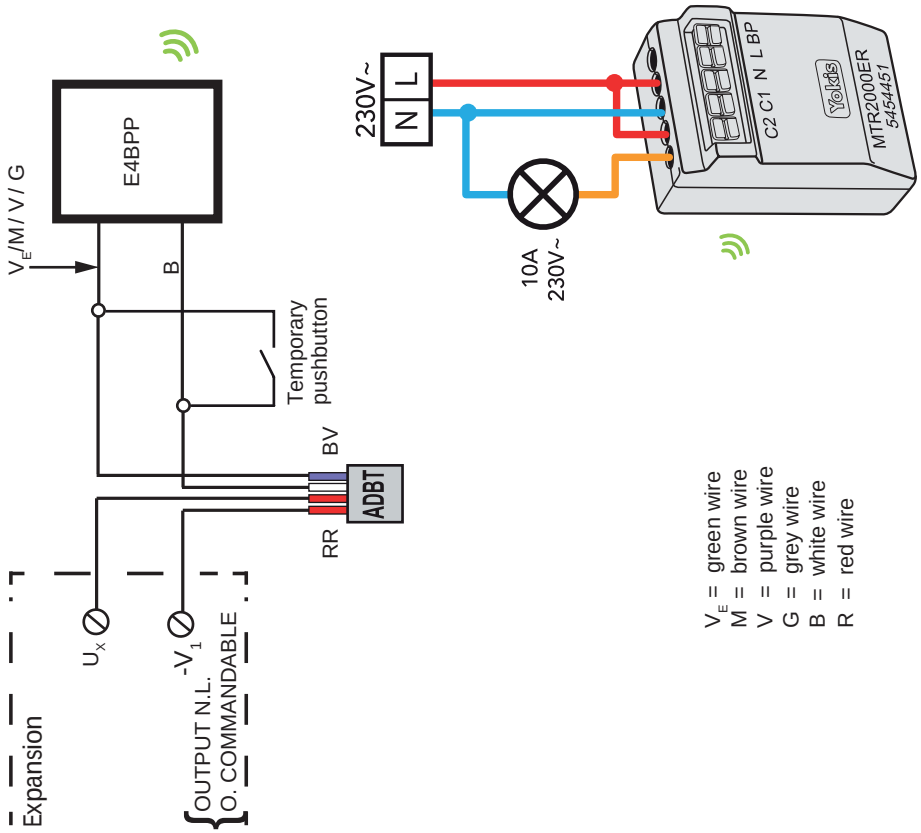
While the LED is flashing, briefly press the pushbutton 17 times: the transmitter LED will respond by flashing 7 times.

From now on, the light connected to MTR2000ER will be correctly piloted by the control panel or the expansion in the ON/OFF mode.

SD542-9001

ON/OFF radio control of a MTR2000ER via an E4BPP channel

E4BPP wiring to the expansion with electrical output



CONTROL PANEL SW CONFIGURATION

By using the keypad or the Hi-Connect programming software, configure the output as follows:
- OUTPUT TYPE = OUTPUT N.L.
- CUSTOMIZE = O. COMMANDABLE

DIRECT CONNECTION

Briefly press 5 times the temporary pushbutton connected to the transmitter. The transmitter LED will start flashing for 30 seconds to indicate that it is waiting for connection.

While the transmitter LED is flashing, shortly press the MTR2000ER "connect" hole located in the rear part with the tip of a pencil.
The transmitter LED will stop flashing.

Warning! The receiver must be powered on.

INSTANTANEOUS MODE CONFIGURATION (=ON/OFF)

Briefly press 10 times the temporary pushbutton connected to the transmitter to enter the Configuration Menu: the transmitter LED will start flashing rapidly.

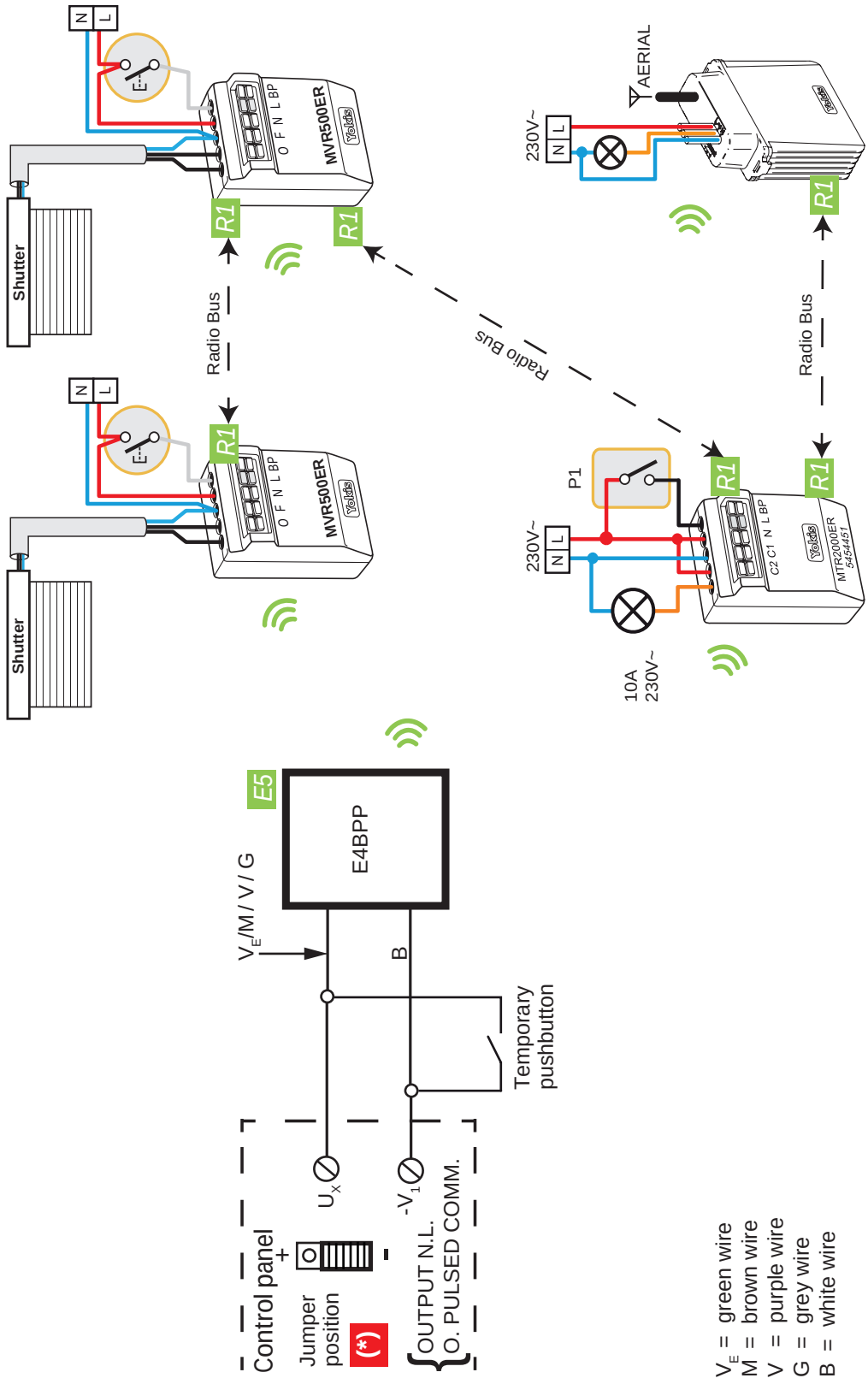
While the LED is flashing, briefly press the pushbutton 17 times: the transmitter LED will respond by flashing 7 times.

From now on, the light connected to MTR2000ER will be correctly piloted by the control panel or the expansion in the ON/OFF mode.

SD542-9002

Centralised on/off control for lights and/or opening/closing of shutters

E4BPP wiring to the control panel with electrical output



SD542-9003 (Page 1/2)

(*) WARNING: CONTROL PANEL HW CONFIGURATION

IMPORTANT
If a Control panel electrical output is used, the corresponding jumper must be moved to the position " - " before connecting the transmitter. Otherwise, the transmitter will be irreparably damaged.

CONTROL PANEL SW CONFIGURATION

By using the keypad or the Hi-Connect programming software, configure the output as follows:
- OUTPUT TYPE = OUTPUT N.L.
- CUSTOMIZE = O. PULSED COMM.

R1-R1 - Define the Radio Bus by connecting receivers one to the other

Apply a short press to "Connect" on receiver 1. Its LED will start flashing (R1).
While the LED is flashing, press "Connect" on receiver 2 (R1). To confirm the connection, the LED of receiver 2 will only flash once and the LED of receiver 1 will stop flashing; after establishing a connection, both modules will respond (the lighting modules will flash or the shutter will move briefly).

E5 - Connect the transmitter to the closest receiver

Briefly press 5 times the temporary pushbutton connected to the transmitter (E5). The transmitter LED will start flashing for 30 seconds, to indicate that it is waiting for connection.

While the transmitter LED is flashing, shortly press the "connect" hole of the closest receiver with the tip of a pencil.

The transmitter LED will stop flashing. The light connected to the module will flash or the shutter will move briefly.

Warning! The receiver must be powered on.

M6 - Configuring the transmitter for centralised control sending

Briefly press 10 times the transmitter temporary pushbutton (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, briefly press the temporary pushbutton (6) 6 times.
The LED will flash 6 times to confirm the centralised mode.

M10/M11/M20 - Define whether the control is for the lights, shutters or both

Briefly press the transmitter temporary pushbutton 10 times (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, apply:
- For the LIGHTS: a short press to the temporary pushbutton 10 times (10) (default).
- For the SHUTTERS: a short press to the temporary pushbutton 11 times (11).
- For the LIGHTS and SHUTTERS: a short press to the temporary pushbutton 20 times (20).

The LED will flash to confirm: 10, 1, 10 times – respectively.

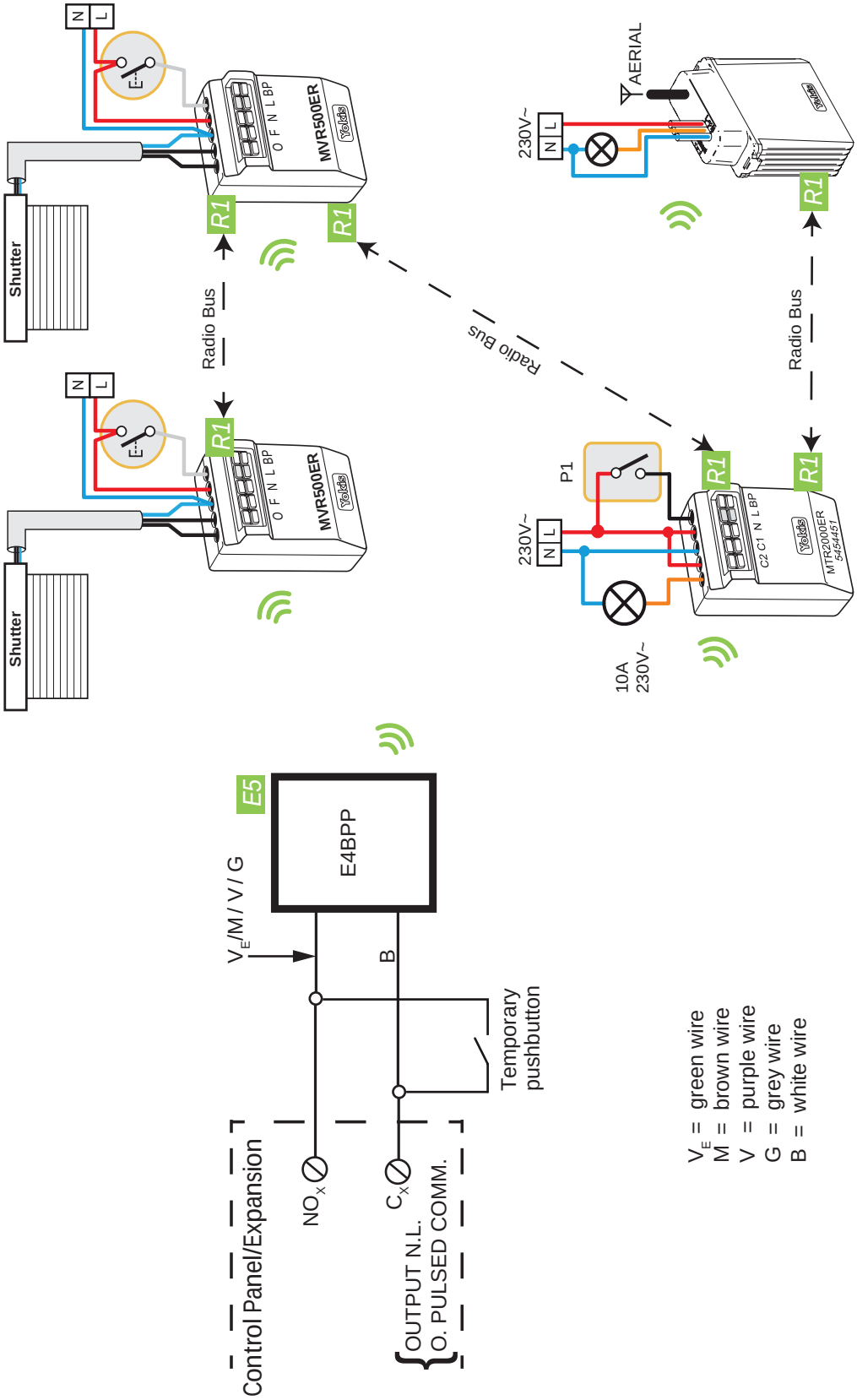
M3/M4 - Define the action: Turning On or Up movement / Turning Off or Down movement

Briefly press the transmitter temporary pushbutton 10 times (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, apply:
- For Turning On (or Shutters Up movement): 3 short presses to the temporary pushbutton (3).
- For Turning Off (or Shutters Down movement): 4 short presses to the temporary pushbutton (4).

The LED will flash to confirm: 3 or 4 times

Centralised on/off control for lights and/or opening/closing of shutters

E4BPP wiring to the control panel/expansion with relay output



SD542-9004 (Page 1/2)

CONTROL PANEL SW CONFIGURATION

By using the keypad or the Hi-Connect programming software, configure the output as follows:
- OUTPUT TYPE = OUTPUT N.L.
- CUSTOMIZE = O. PULSED COMM.

R1-R1 - Define the Radio Bus by connecting receivers one to the other

Apply a short press to "Connect" on receiver 1. Its LED will start flashing (R1).
While the LED is flashing, press "Connect" on receiver 2 (R1). To confirm the connection, the LED of receiver 2 will only flash once and the LED of receiver 1 will stop flashing; after establishing a connection, both modules will respond (the lighting modules will flash or the shutter will move briefly).

E5 - Connect the transmitter to the closest receiver

Briefly press 5 times the temporary pushbutton connected to the transmitter (E5). The transmitter LED will start flashing for 30 seconds, to indicate that it is waiting for connection.

While the transmitter LED is flashing, shortly press the "connect" hole of the closest receiver with the tip of a pencil.

The transmitter LED will stop flashing. The light connected to the module will flash or the shutter will move briefly.

Warning! The receiver must be powered on.

M6 - Configuring the transmitter for centralised control sending

Briefly press 10 times the transmitter temporary pushbutton (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, briefly press the temporary pushbutton (6) 6 times.
The LED will flash 6 times to confirm the centralised mode.

M10/M11/M20 - Define whether the control is for the lights, shutters or both

Briefly press the transmitter temporary pushbutton 10 times (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, apply:
- For the LIGHTS: a short press to the temporary pushbutton 10 times (10) (default).
- For the SHUTTERS: a short press to the temporary pushbutton 11 times (11).
- For the LIGHTS and SHUTTERS: a short press to the temporary pushbutton 20 times (20).

The LED will flash to confirm: 10, 1, 10 times – respectively.

M3/M4 - Define the action: Turning On or Up movement / Turning Off or Down movement

Briefly press the transmitter temporary pushbutton 10 times (Configuration Menu (M)).
The transmitter LED will flash rapidly.
While the LED is flashing, apply:
- For Turning On (or Shutters Up movement): 3 short presses to the temporary pushbutton (3).
- For Turning Off (or Shutters Down movement): 4 short presses to the temporary pushbutton (4).

The LED will flash to confirm: 3 or 4 times

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

Via Bologna, 188/C - 10154 Torino (TO) – Italy
www.urmet.com

MADE IN ITALY