

Addendum per firmware v.8.x

**Centrali multifunzionali in configurazione
ibrida per antintrusione
serie **GW10931****



AVVERTENZE

PER L'INSTALLATORE:

Attenersi scrupolosamente alle norme vigenti sulla realizzazione di impianti elettrici e sistemi di sicurezza, oltre che alle prescrizioni del costruttore riportate nella manualistica a corredo dei prodotti.

Fornire all'utilizzatore tutte le indicazioni sull'uso e sulle limitazioni del sistema installato, specificando che esistono norme specifiche e diversi livelli di prestazioni di sicurezza che devono essere commisurati alle esigenze dell'utilizzatore.

Far prendere visione all'utilizzatore delle avvertenze riportate in questo documento.

PER L'UTILIZZATORE:

Verificare periodicamente e scrupolosamente la funzionalità dell'impianto accertandosi della correttezza dell'esecuzione delle manovre di inserimento e disinserimento.

Curare la manutenzione periodica dell'impianto affidandola a personale specializzato in possesso dei requisiti prescritti dalle norme vigenti.

Provvedere a richiedere al proprio installatore la verifica dell'adeguatezza dell'impianto al mutare delle condizioni operative (es. variazioni delle aree da proteggere per estensione, cambiamento delle metodiche di accesso ecc...).

Questo dispositivo è stato progettato, costruito e collaudato con la massima cura, adottando procedure di controllo in conformità alle normative vigenti. La piena rispondenza delle caratteristiche funzionali è conseguita solo nel caso di un suo utilizzo esclusivamente limitato alla funzione per la quale è stato realizzato, e cioè:

Centrali multifunzionali in configurazione ibrida per antintrusione

Qualunque utilizzo al di fuori di questo ambito non è previsto e quindi non è possibile garantire la sua corretta operatività, e pertanto è fatto espresso divieto al detentore del presente manuale di utilizzarlo per ragioni diverse da quelle per le quali è stato redatto, ovvero esplicative delle caratteristiche tecniche del prodotto e delle modalità d'uso.

I processi produttivi sono sorvegliati attentamente per prevenire difettosità e malfunzionamenti; purtroppo la componentistica adottata è soggetta a guasti in percentuali estremamente modeste, come d'altra parte avviene per ogni manufatto elettronico o meccanico. Vista la destinazione di questo articolo (protezione di beni e persone) invitiamo l'utilizzatore a commisurare il livello di protezione offerto dal sistema all'effettiva situazione di rischio (valutando la possibilità che detto sistema si trovi ad operare in modalità degradata a causa di situazioni di guasti od altro), ricordando che esistono norme precise per la progettazione e la realizzazione degli impianti destinati a questo tipo di applicazioni.

Richiamiamo l'attenzione dell'utilizzatore (conduttore dell'impianto) sulla necessità di provvedere regolarmente ad una manutenzione periodica del sistema almeno secondo quanto previsto dalle norme in vigore oltre che ad effettuare, con frequenza adeguata alla condizione di rischio, verifiche sulla corretta funzionalità del sistema stesso segnatamente alla centrale, sensori, avvisatori acustici, combinatore/i telefonico/i ed ogni altro dispositivo collegato. Al termine del periodico controllo l'utilizzatore deve informare tempestivamente l'installatore sulla funzionalità riscontrata.

La progettazione, l'installazione e la manutenzione di sistemi incorporanti questo prodotto sono riservate a personale in possesso dei requisiti e delle conoscenze necessarie ad operare in condizioni sicure ai fini della prevenzione infortunistica. È indispensabile che la loro installazione sia effettuata in ottemperanza alle norme vigenti. Le parti interne di alcune apparecchiature sono collegate alla rete elettrica e quindi sussiste il rischio di folgorazione nel caso in cui si effettuino operazioni di manutenzione al loro interno prima di aver disconnesso l'alimentazione primaria e di emergenza. Alcuni prodotti incorporano batterie ricaricabili o meno per l'alimentazione di emergenza. Errori nel loro collegamento possono causare danni al prodotto, danni a cose e pericolo per l'incolumità dell'operatore (scoppio ed incendio).

DICHIARAZIONE DI CONFORMITÀ UE

Prodotto conforme alle vigenti direttive europee EMC e LVD. Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: iessonline.com (previa semplice registrazione).

AVVERTENZE PER LO SMALTIMENTO - INFORMAZIONI AGLI UTENTI



Ai sensi della Direttiva 2012/19/UE, relativa allo smaltimento dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE), si precisa che il dispositivo AEE è immesso sul mercato dopo il 13 agosto 2005 con divieto di conferimento all'ordinario servizio di raccolta dei rifiuti urbani.

IT08100000005590

1. INTRODUZIONE

Con il firmware v.8.x la centrale della serie GW10931 viene dotata di interessanti caratteristiche funzionali alla cui descrizione è dedicato questo documento che va ad integrare la documentazione standard delle centrali.

Le novità sono:

Gestione del modulo MDWIFI (*) - Utilizzo evoluto dei telecomandi

Per la programmazione delle centrali è necessario installare il BrowserGW v.3.0.29 o sup. ed i moduli specifici v. 8.0.xx o sup. per i vari modelli di centrale. Nel caso di installazione di software di precedente versione potrà essere utile aggiornarli direttamente accedendo alla funzione di "Aggiornamento Software" disponibile nel menu "Strumenti".

2. MODALITA' DI FUNZIONAMENTO CON BROWSERGW

Il software di gestione consente di scegliere tra due modalità di funzionamento selezionabili in alternativa ovvero come **modalità base** oppure **modalità avanzata**. La prima volta che viene caricato un modulo che supporta la doppia modalità, BrowserGW chiede di scegliere la modalità di funzionamento; tale scelta può essere variata in qualsiasi momento agendo sull'apposito pulsante nella barra degli strumenti di BrowserGW.

- **Modalità Base:** la modalità base consente esclusivamente la configurazione delle opzioni principali ed è adatta agli utilizzatori che desiderano una programmazione semplificata della centrale.
- **Modalità Avanzata:** la modalità avanzata consente la configurazione di tutte le funzioni della centrale ed è adatta ad utenti esperti.

3. GESTIONE DEL MODULO MDWIFI (*)

Il modulo MDWIFI (*) consente la gestione tramite Metronet (*) di una centrale **GW10931** o sfruttando una connessione alla rete locale tramite WiFi. Il modulo è dotato di antenna integrata e di piccole dimensioni e di rapida installazione e configurazione.

Il modulo MDWIFI (*) fornisce un solo canale di comunicazione ed è utilizzabile SOLO per la connessione Metronet anche per sessioni di teleassistenza.

È necessario però considerare che i tempi di risposta risentono dei tempi di latenza dei sistemi trasmissivi utilizzati. Questi ritardi si manifestano anche durante la visualizzazione della pagina Metronet (*) dal PC o dal cellulare dell'utente.

La presenza del modulo MDWIFI (*) preclude l'utilizzo del connettore MINIDIN per comunicazione seriale.

Sia con il BrowserGW che da tastiera è possibile verificare lo stato del modulo e impostare i parametri della connessione Wi-Fi.

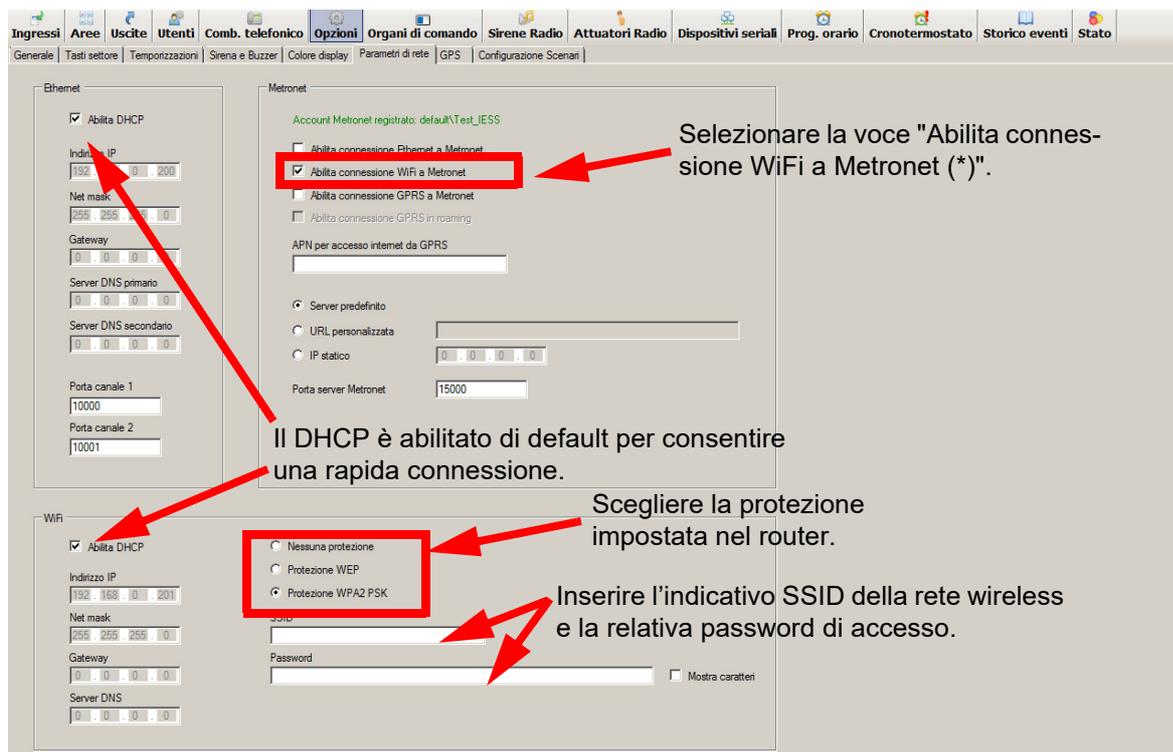
3.1 Configurazione della centrale e del modulo MDWIFI (*)

Per la corretta configurazione ed uso del modulo MDWIFI (*) l'installatore deve operare come segue:

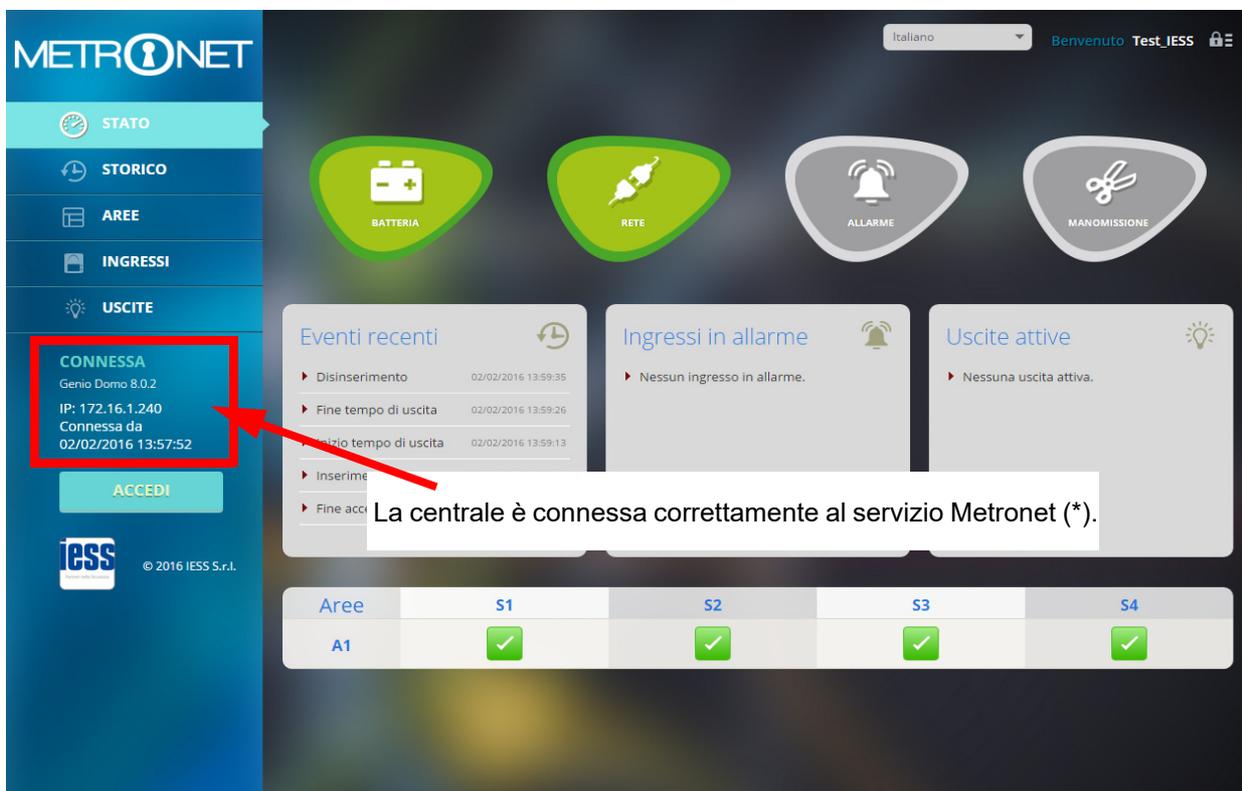
- Registrare il modulo andando nel menu REGISTRAZIONE MODULI / Modulo WiFi e premendo il tasto 1.
- Raggiungere successivamente il menu PARAMETRI DI RETE e premere "Ok", se il modulo è l'unico installato si potrà vedere l'intensità del segnale radio ricevuto dal router localmente disponibile e il MAC ADDRESS.
- L'intensità del segnale radio RSSI è visualizzata con ???? (segnale assente), con ##### (massimo segnale).
- Connettere via USB la centrale al BrowserGW v.3.0.29 o superiore e modulo compatibile v.8.x.
- Leggere la configurazione della centrale e impostare i parametri di rete disponibili nelle sezioni Metronet (*) e Wi-Fi della finestra "Opzioni". Un esempio può essere quello dell'immagine che segue.

NOTA

I dispositivi qui identificati con il simbolo (*) sono articoli integrativi presenti nell'offerta IESS. Maggiori informazioni possono essere reperite sul sito www.iessonline.com.



- Scrivere i parametri in centrale.
- Creare nel servizio Metronet (*) l'account per l'utente, verrà generata una chiave di registrazione del modulo inviata dal servizio all'indirizzo e-mail di registrazione dell'utente.
- Leggere la chiave ed inserirla nel menu della centrale "ACCOUNT INTERNET", premere OK ed attendere la registrazione. Per eventuali errori di registrazione leggere il capitolo "Errori" in questo manuale.
- Utilizzare il browser di internet o uno smartphone per controllare l'effettivo accesso alla pagina della centrale dell'utente.



NOTA
I dispositivi qui identificati con il simbolo (*) sono articoli integrativi presenti nell'offerta IESS. Maggiori informazioni possono essere reperite sul sito www.lessonline.com.

4. CONNESSIONE AL SERVIZIO METRONET (*)

Come già spiegato nella documentazione del servizio Metronet (*) si espone un esempio della procedura di registrazione. Dalla mail di registrazione ricevuta si dovrà copiare il codice di registrazione a 9 cifre escludendo i trattini. Per effettuare la registrazione della centrale utilizzare l'apposito menu in tastiera a disposizione solo del manutentore:

1	Login installatore da centrale disinserita	5	Registrare l'account premendo il tasto 1 ed inserire il codice di registrazione e premere Ok.
2	Ok	6	Attendere qualche secondo per il completamento dell'operazione.
3	Navigazione nei menu fino a "Account Internet"	7	Un beep di conferma avviserà se la procedura di registrazione è avvenuta con successo ed apparirà la scritta "REGISTRATO".
4	Ok	8	Uscire dal menu di programmazione.

4.1 Errori durante la registrazione al servizio Metronet (*)

Descrizione dei codici generici di errore:

Errore 1: errore di risoluzione DNS o apertura connessione.

- Solo per connessione GPRS: verificare la correttezza dell'APN di accesso a Internet, verificare che il piano tariffario della SIM preveda traffico internet, verificare il credito residuo nella SIM.
- Se utilizzata URL personalizzata per il server Metronet (*), verificare correttezza dell'URL inserita.
- Solo per connessione Ethernet: se non è utilizzato un IP statico, verificare impostazione dei server DNS, verificare la correttezza degli indirizzi IP dei server DNS dal menu "Parametri di rete" della centrale.
- Se utilizzato IP statico per il server Metronet (*), verificare correttezza dell'IP inserito.
- Solo per connessione Ethernet: se utilizzato IP statico, verificare l'impostazione del gateway di accesso a internet, verificare la correttezza dell'indirizzo IP del gateway dal menu "Parametri di rete" della centrale.

Errore 3: errore di scambio dati con il server Metronet (*).

- Solo per connessione GPRS: verificare la correttezza dell'APN di accesso a internet, verificare che il piano tariffario della SIM preveda traffico internet, verificare il credito residuo nella SIM.
- Verificare l'operatività del server Metronet (*) tramite connessione all'interfaccia Web <https://metronet.iessononline.com>.

Errore 2: errore di apertura connessione.

- Solo per connessione GPRS: verificare la correttezza dell'APN di accesso a internet, verificare che il piano tariffario della SIM preveda traffico internet, verificare il credito residuo nella SIM.
- Se utilizzato IP statico per il server Metronet (*), verificare correttezza dell'IP inserito.
- Solo per connessione Ethernet: se utilizzato IP statico, verificare l'impostazione del gateway di accesso a internet, verificare la correttezza dell'indirizzo IP del gateway dal menu "Parametri di rete" della centrale.
- Solo per connessione Ethernet: verificare che la porta 15000 sia aperta in uscita sull'eventuale proxy/firewall.
- Verificare l'operatività del server Metronet (*) tramite connessione all'interfaccia Web <https://metronet.iessononline.com>.

Errore 4: codice di registrazione non valido.

- Generare un nuovo codice di registrazione e ripetere la procedura con il nuovo codice.

4.2 Avviso importante sulla sicurezza per l'utilizzo in INTERNET

L'utilizzo di INTERNET per la connessione a sistemi di sicurezza espone le apparecchiature al rischio di attacchi informatici, generalmente perpetrati da hackers, che diventano sempre più sofisticati e potenzialmente destabilizzanti per il buon funzionamento dell'apparato. Il funzionamento sicuro in Internet di componenti destinati all'uso in sistemi di sicurezza richiede l'adozione di misure volte a proteggere questi apparati da attacchi intenzionali.

Le soluzioni che possono essere adottate sono diverse; tra le varie suggeriamo tre possibilità:

1. L'interporre tra l'apparato ed Internet un dispositivo Firewall fisico ed effettuare una appropriata programmazione del Router per abilitare solo i MAC ADDRESS dei dispositivi connessi al router.
2. Preferire la chiave di protezione WPA2-PSK al posto di una chiave WEP. È altamente sconsigliato non impostare alcuna chiave protezione.
3. Modificare periodicamente la password di protezione per l'accesso al router. Questa soluzione richiede l'intervento del manutentore, eventualmente da ipotizzare in sede di manutenzione periodica dell'impianto.

Nota per le chiavi WEP: le chiavi WEP utilizzabili sono a 64bit (5 caratteri ascii) o a 128 bit (13 caratteri ascii).

La mancata adozione di misure preventive espone il dispositivo a possibili attacchi le cui conseguenze non sono ipotizzabili e prevedibili.

NOTA

I dispositivi qui identificati con il simbolo (*) sono articoli integrativi presenti nell'offerta IESS. Maggiori informazioni possono essere reperite sul sito www.iessononline.com.

Ingressi		Aree		Uscite		Utenti		Comb. telefonico		Opzioni		Organi di comando		Sirene Radio		Attuatori Radio		Dispositivi seriali		Prog. ora			
	Nome utente	Settori permessi Area 1		Settori proposti Area 1		Settori permessi Area 2		Settori proposti Area 2		Settori permessi Area 3		Settori proposti Area 3											
▶ 01	Utente 1	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
02	Utente 2	1	2	3	4	1	2	3	4	---	---	---	---	---	---	---	---	---	---	---	---	---	---
03	Utente 3	1	2	3	4	1	2	3	4	---	---	---	---	---	---	---	---	---	---	---	---	---	---
04	Utente 4	1	2	3	4	1	2	3	4	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Generali | **Settori permessi/proposti** | Azione telecomando (1) | Azione telecomando (2)

 Impostare i settori permessi/proposti ad ogni utente facendo click con il mouse sulla relativa casella della griglia.

 Se abilitato, l'inserimento veloce è attivo su tutti i settori associati ad almeno un utente. Rimuovere i settori dagli utenti non attivi per impedire l'inserimento veloce di settori indesiderati.

Elimina settori degli utenti non attivi

6. AGGIORNAMENTO FIRMWARE DI CENTRALE 8.4.1 - FUNZIONI AGGIUNTIVE

6.1 Visualizzazione degli ingressi in allarme nei periodi di inattività della tastiera

Aggiornando BrowserGW alla versione 3.7.1 o superiore e utilizzando un modulo Genio 8.7.2 o superiore, alla pagina **Opzioni > Generale**, pannello **Opzioni Generali**, viene resa disponibile la funzione **Visualizza ingressi in allarme durante inattività tastiere**.

Se selezionata, in condizione di inattività la tastiera visualizza su schermo i nomi degli ingressi che si trovano in stato di allarme. I nomi verranno mostrati uno dopo l'altro ciclicamente; nel ciclo di visualizzazione verranno mostrati anche il nome dell'area o il messaggio di benvenuto.

La funzione è valida solo per la tastiera di bordo e per i primi 8 organi di comando.

Default: funzione non attiva.

7. AGGIORNAMENTO FIRMWARE DI CENTRALE 8.4.2 - FUNZIONI AGGIUNTIVE

7.1 Aggiunta Opzioni EN50131

A partire dalla versione firmware di centrale 8.4.2, versione di BrowserGW 3.7.8 o superiore, modulo Genio 8.8.6 o superiore, vengono introdotte nella pagina **Opzioni > Generale > Opzioni EN50131** le seguenti opzioni:

- **Necessaria autorizzazione installatore per inserimento con guasti/manomissioni:** la funzione è necessaria per soddisfare le prescrizioni al Grado 3 della norma EN50131 ed è disponibile solo se è attivata la funzione "Attiva blocco inserimento". Default: funzione non attiva.
- **Abilita preavviso inserimento da prog. orario:** se spuntata, le tastiere emetteranno segnalazioni acustiche un minuto prima dell'attivazione del programmatore orario.
- **Cancellazione memorie guasto/manomissione solo da installatore:** se attivata, solo l'installatore potrà cancellare le memorie di guasto o manomissione. Default: funzione non attiva.
- **Esclusione ingressi solo da installatore:** se attivata, solo l'installatore potrà escludere gli ingressi della centrale. Questo procedimento aumenta il grado di sicurezza dell'impianto. Default: funzione non attiva.

- **Attiva blocco inserimento:** aggiornando il firmware alla versione 8.4.2, il blocco inserimento viene attivato anche in caso di batteria scarica di telecomandi. Con il telecomando, in caso di blocco inserimento, è comunque possibile inserire l'impianto con una doppia pressione del tasto: alla prima pressione il telecomando notifica l'inserimento rifiutato (emissione di un beep e accensione del LED rosso), alla seconda pressione inserisce l'impianto.

7.2 Visualizzazione dello stato di sospensione degli utenti

Nella pagina **Utenti > Generale**, pannello **Opzioni Utente**, è presente la funzione "Abilita gestione autorizzazione utenti". La selezione di questa funzione consente a un utente di gestire gli attributi di attività concessi agli utenti attivi e a se stesso.

L'attivazione della funzione fa apparire il relativo menu "GESTIONE UTENTI" in tastiera, visibile navigando tra i menu a disposizione dell'utente specifico dopo l'accesso con codice (login).

Gli attributi di attività si potranno attivare solo da tastiera utilizzando i tasti:

Ok = per editare cambiare gli attributi - Totale - Solo inserimento - Solo disinserimento - Sospeso.

1 = per cambiare velocemente l'attributo utente in Totale.

= per sospendere velocemente un utente.

Stop = uscita dal menu con memorizzazione.

A partire dalla versione firmware di centrale 8.4.2, versione di BrowserGW 3.7.8 o superiore, modulo Genio 8.8.6 o superiore, se un utente viene sospeso da un altro utente abilitato alla gestione delle autorizzazioni, si accende la spia "Anomalie Utenti" nella pagina **Stato > Stato Aree**. Premere sulla spia per accedere ai dettagli della pagina Stato Utenti.

7.3 Memoria di anomalia

A partire dalla versione firmware di centrale 8.4.2, versione di BrowserGW 3.7.8 o superiore, modulo Genio 8.8.6 o superiore, viene mantenuta la memoria della condizione di anomalia.

7.4 Ritardo segnalazione "Verificare programmazione uscite"

Sul display della centrale viene visualizzato un avviso di verifica programmazione (VERIFICARE, PROGRAMM. USCITE) se viene rilevata almeno una movimentazione uscita ogni 8 secondi per 3 minuti continuativi.

A partire dalla versione firmware di centrale 8.4.2, questo tempo viene aumentato da 3 minuti a 30 minuti.

7.5 Controllo delle uscite

Funzioni disponibili nella pagina **Uscite**, in corrispondenza di ciascuna singola uscita.

Controllo manuale uscita

Funzione disponibile solo se il Modo dell'uscita non è impostato a "Stato" o "Stato negato".

Se selezionato, consente di comandare manualmente anche le uscite la cui funzione di uscita non è impostata a "Controllo manuale".

Esempio: l'utilizzo è pensato per comandare le uscite anche da Metronet (*).

Attivabile senza autenticazione

Se selezionato, questa uscita può essere attivata senza che venga richiesto il codice utente.

Se deselezionato, verrà richiesta l'autenticazione per attivare questa uscita.

7.6 Opzioni combinatore

Funzioni disponibili nella pagina **Comb. telefonico > Combinatore GSM**.

Disattiva telecontrollo via SMS

Se spuntata, il telecontrollo via SMS non può essere effettuato.

Tecnologia di accesso radio per modulo 4G (*)

Seleziona la tecnologia di accesso alla rete mobile per il modulo 4G eventualmente installato. Sono disponibili varie opzioni, singole (solo 4G / solo 3G / solo 2G) o combinate.

NOTA

I dispositivi qui identificati con il simbolo (*) sono articoli integrativi presenti nell'offerta IESS. Maggiori informazioni possono essere reperite sul sito www.iessonline.com.

8. AGGIORNAMENTO FIRMWARE DI CENTRALE 8.6.5: GESTIONE PROTOCOLLO SIA DC-09

A partire dalla versione firmware di centrale 8.6.5, il combinatore è in grado di trasmettere eventi via IP secondo lo standard SIA IP Reporting (TCP-2007) tramite il protocollo supportato ADM-CID.

I parametri della comunicazione si possono impostare tramite la sotto-pagina **SIA DC-09**, disponibile a partire dalla versione di BrowserGW 3.11.8 e utilizzando versioni dei moduli Genio superiori o uguali alla 8.10.13.

La sotto-pagina è disponibile nella pagina **Combinatore telefonico**. Si compone dei seguenti pannelli contenenti le opzioni da impostare:

8.1 Opzioni generali

- **GMT Offset:** la validazione da parte del software ricevente è basata sull'ora, che deve tenere conto anche del fuso orario. Impostare in questo campo la distanza in ore dal meridiano fondamentale del Paese dove è installata la centrale (es. per l'Italia è impostato +1 di default).
- **Abilita trasmissione criptata su primario (secondario):** spuntare per proteggere i messaggi di evento con una password. Impostare la password nel campo **Chiave crittografica** del pannello **Server Primario (Secondario)**.
- **Timestamp su invii in chiaro a primario (secondario):** se spuntato, con messaggi non criptati verranno trasmesse al server primario (secondario) informazioni aggiuntive su data e ora.
- **Doppia notifica:** se spuntata, verranno inviati messaggi ogni volta su **entrambi** i server.
- **Attiva combinatore SIA DC-09 via...:** spuntare la casella corrispondente alla modalità di connessione (Ethernet, WiFi o GPRS). Se sono spuntate più opzioni, verrà data la priorità a quella più in alto nell'elenco (ad esempio, se sono spuntati WiFi e GPRS la priorità viene assegnata alla trasmissione in WiFi).
- **Protocollo digitale:** selezionare dal menu a tendina il formato del protocollo (decimale/esadecimale).

Nota: se la connessione avviene tramite GPRS e anche e-Connect utilizza questa modalità, la connessione fallita sul server potrebbe determinare una disconnessione temporanea del servizio e-Connect.

8.2 Server Primario

Impostare in questo pannello i parametri del server primario che riceverà le segnalazioni di evento.

- **Indirizzo IP e Porta TCP:** impostare l'indirizzo IP e la porta TCP del server primario.
- **Chiave crittografica:** impostare una password esadecimale per la criptazione dei messaggi. Il campo è abilitato solo se l'opzione **Abilita trasmissione criptata su primario** è spuntata nel pannello **Opzioni generali** di fianco.
- **Numero account:** numero identificativo dell'apparato.

8.3 Server Secondario

È possibile usufruire anche di un secondo server di backup: impostare in questo pannello i parametri del server secondario. I significati dei parametri sono analoghi a quelli relativi al server primario.

8.4 Configurazione Sia DC09

- **Carica configurazione SiaDC09:** cliccare per caricare un file di configurazione (.sdp) dei parametri SIA DC-09 salvato in precedenza.
- **Salva configurazione SiaDC09:** cliccare per salvare la configurazione dei parametri SIA DC-09 attuale su un file (.sdp) nel computer.

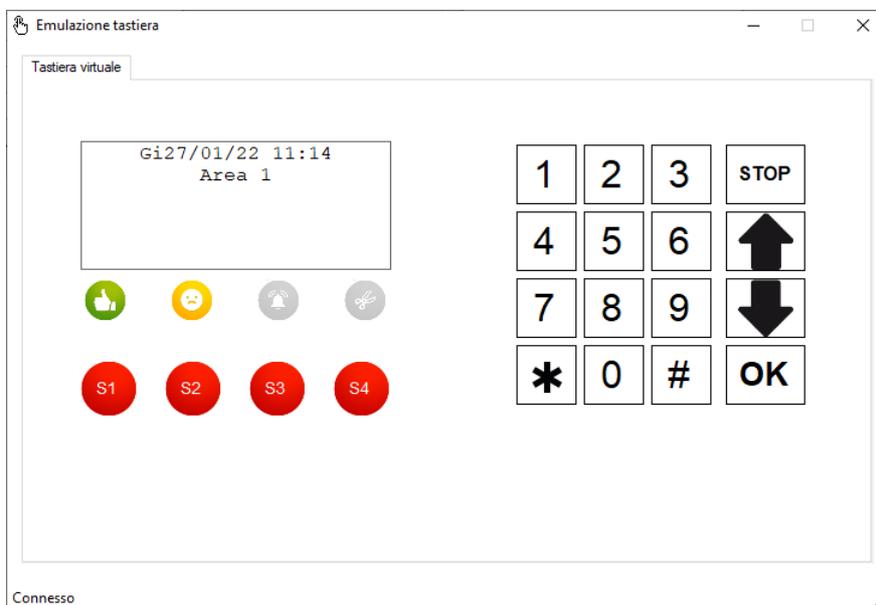
9. AGGIORNAMENTO FIRMWARE DI CENTRALE 8.8.8: EMULAZIONE TASTIERE

A partire dalla versione firmware di centrale 8.8.8 ed utilizzando BrowserGW 3.18.16 o superiore con modulo 8.17.4 o superiore, è disponibile uno strumento di emulazione della tastiera da remoto.

Questo strumento permette di emulare una specifica tastiera fisicamente presente nell'impianto, per impartire da remoto i relativi comandi senza utilizzare fisicamente la tastiera stessa.

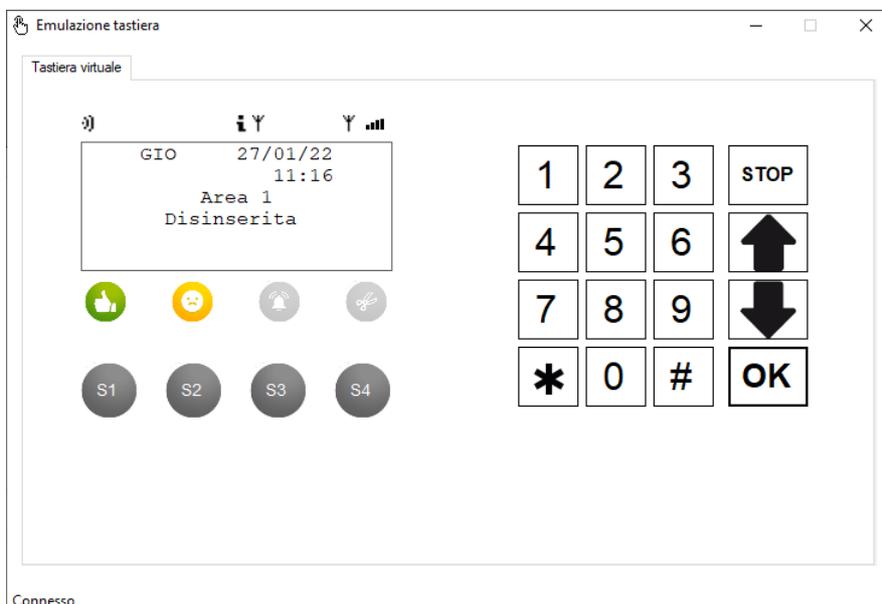
Per aprire lo strumento per una specifica tastiera:

- selezionare la tastiera dalla griglia superiore
- nella tab **Tastiere**, fare clic sul pulsante **Apri emulazione tastiera**



L'interfaccia riporta gli stessi tasti di cui è dotata la tastiera fisica e ne replica in tempo reale i messaggi riportati a display.

Lo stesso strumento di emulazione è disponibile anche per la tastiera di bordo: accedere alla pagina **Organi di comando > Tastiera di bordo** per utilizzarlo.



10. INDICE

1. INTRODUZIONE	3
2. MODALITA' DI FUNZIONAMENTO CON BrowserGW	3
3. GESTIONE DEL MODULO MDWIFI (*)	3
3.1. Configurazione della centrale e del modulo MDWIFI (*)	3
4. CONNESSIONE AL SERVIZIO Metronet (*)	5
4.1. Errori durante la registrazione al servizio Metronet (*)	5
4.2. Avviso importante sulla sicurezza per l'utilizzo in INTERNET	5
5. UTILIZZO EVOLUTO DEI TELECOMANDI	6
6. AGGIORNAMENTO firmware di centrale 8.4.1 - FUNZIONI AGGIUNTIVE	7
6.1. Visualizzazione degli ingressi in allarme nei periodi di inattività della tastiera	7
7. AGGIORNAMENTO firmware di centrale 8.4.2 - FUNZIONI AGGIUNTIVE	7
7.1. Aggiunta Opzioni EN50131	7
7.2. Visualizzazione dello stato di sospensione degli utenti	8
7.3. Memoria di anomalia	8
7.4. Ritardo segnalazione "Verificare programmazione uscite"	8
8. AGGIORNAMENTO firmware di centrale 8.6.5: gestione protocollo SIA DC-09	9
8.0.1. Opzioni generali	9
8.0.2. Server Primario	9
8.0.3. Server Secondario	9
9. AGGIORNAMENTO firmware di centrale 8.8.8: EMULAZIONE TASTIERE	10
10. INDICE	11

NOTA

I dispositivi qui identificati con il simbolo (*) sono articoli integrativi presenti nell'offerta IEES.
Maggiori informazioni possono essere reperite sul sito www.iessonline.com.

Punto di contatto indicato in adempimento ai fini delle direttive e regolamenti UE applicabili:
Contact details according to the relevant European Directives and Regulations:
GEWISS S.p.A. Via A.Volta, 1 IT-24069 Cenate Sotto (BG) Italy tel: +39 035 946 111 E-mail: qualitymarks@gewiss.com

According to applicable UK regulations, the company responsible for placing the goods in UK market is:
GEWISS UK LTD - Unity House, Compass Point Business Park, 9 Stocks Bridge Way, ST IVES
Cambridgeshire, PE27 5JL, United Kingdom tel: +44 1954 712757 E-mail: gewiss-uk@gewiss.com



+39 035 946 11

8:30 - 12:30 / 14:00 - 18:00
lunedì - venerdì / monday - friday



www.gewiss.com

