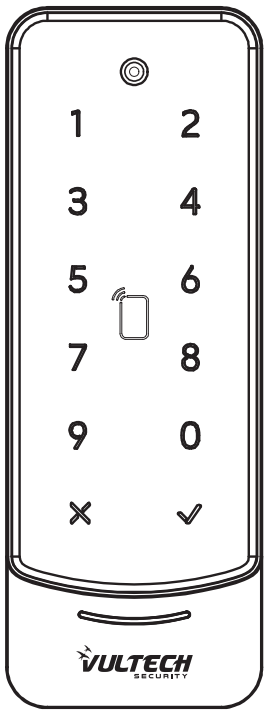
CONTROLLO ACCESSI
MODELLO

VS-CA501FRT



GUIDA

Aggiornamento Firmware
al 2026/01/9

NOTA

Si prega di seguire il manuale utente per una corretta installazione dei prodotti. In caso di dubbi, consultare il sito www.vultechsecurity.it o contattare l'assistenza tecnica.

L'illustrazione mostrata qui è puramente a scopo illustrativo. I nostri prodotti sono costantemente soggetti ad aggiornamenti, pertanto potrebbero risultare differenti per estetica o avere versioni firmware aggiornate. Non vi sarà alcun preavviso da parte nostra circa eventuali aggiornamenti. Ciò nonostante, le specifiche tecniche resteranno invariate.

Il prodotto e le batterie devono essere smaltiti separatamente dai rifiuti domestici. Al termine della sua funzione, contattare gli uffici amministrativi locali per ricevere corrette indicazioni sulle modalità di smaltimento. In questo modo si salvaguarderà l'ambiente e la salute umana.
L'azienda è da sempre impegnata a seguire una condotta green e sostenibile e incoraggiamo il riciclo e il riutilizzo delle risorse per salvaguardare l'ambiente.

PARAMETRI DISPOSITIVO

- Indirizzo IP di fabbrica: 192.168.1.200
- Nome utente: admin
- Password: 123456

CONTENUTI

Contenuto della confezione.....1
Immagine del prodotto.....2
Configurazione sistema.....3
Schema di collegamento.....4
Installazione.....7
Impostazioni da web.....13
Risoluzione dei problemi comuni.....31
Istruzioni di sicurezza.....32

CONTENUTO DELLA CONFEZIONE

Assicurarsi che la confezione contenga i seguenti articoli:

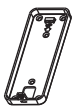
VS-CA501FRT

Set di viti

Cacciavite Torx

Tappo

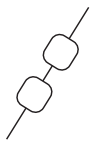
Copertura del cablaggio



Copertura posteriore

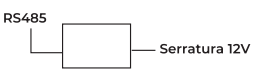
Chiave di prossimità

Manuale Rapido



Diodo

ACCESSORI

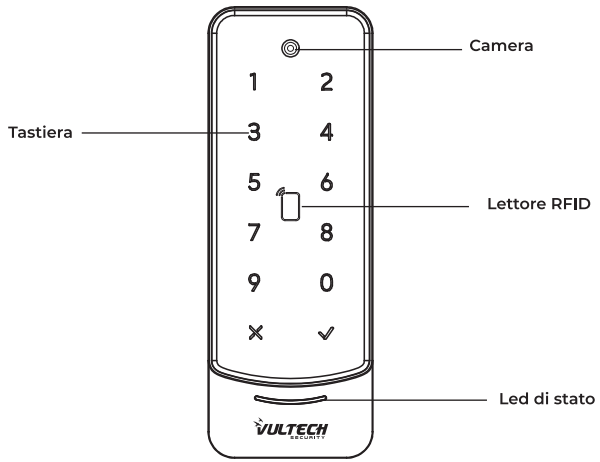


Modulo aggiuntivo RS485 per apertura serrature (VS-LOCKPLUS)

VS-CICA (Opzionale)

IMMAGINE DEL PRODOTTO

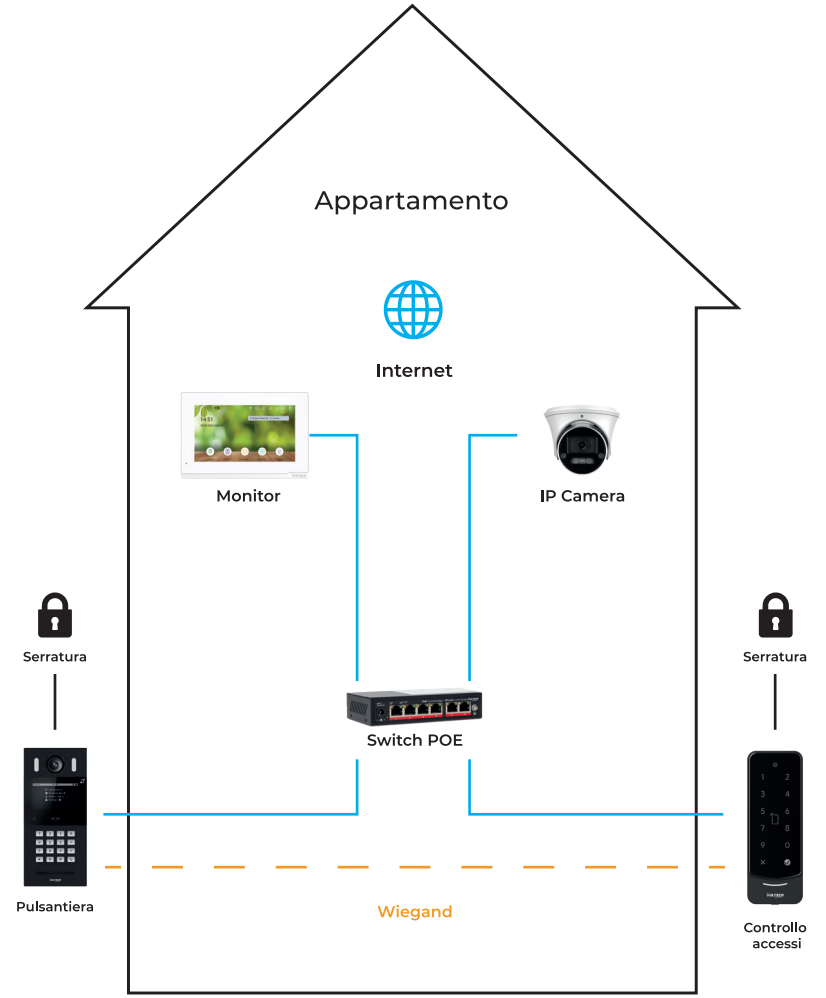
Modello: **VS-CA501FRT**



Caratteristiche:

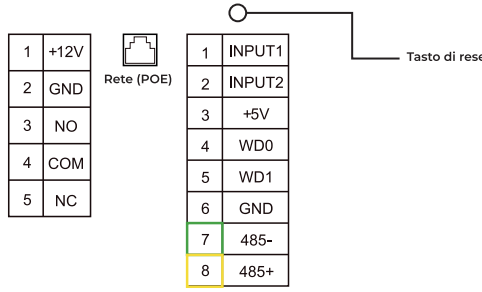
- Sistema: Linux
- Camera 2 MP
- Grado di protezione: IP 65 / IK08
- Alimentazione: 12V 2A / PoE IEEE802.3af
- 1 uscita a Relè
- Allarme Tamper
- Lettore RFID: 13.56MHz and 125kHz
- Tastiera numerica
- RS485: supportato
- Wiegand: Supporta ingresso e uscita
- Bluetooth: 5.3
- Montaggio a parete o a incasso
- Dimensioni prodotto: 137 x 50 x 27 mm

CONFIGURAZIONE SISTEMA



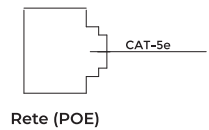
Lo schema illustra la configurazione tipo di un impianto che prevede il videocitofono con il controllo accessi integrato.
Da notare che il dispositivo per il controllo accessi può essere configurato anche in stand-alone, indipendentemente da un impianto di videocitofonia.

SCHEMA DI COLLEGAMENTO

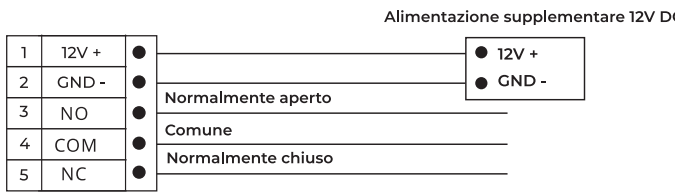


1.Rete / POE / RJ45

L'interfaccia RJ45 standard serve per la connessione con uno switch PoE o un altro switch di rete. Il PSE deve essere conforme allo standard IEEE 802.3af (PoE) e la sua potenza di uscita non deve essere inferiore a 15,4 W e la sua tensione di uscita non deve essere inferiore a 50V.



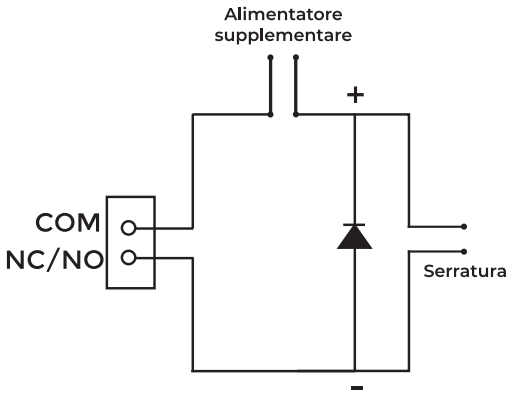
2. Alimentazione / Relè



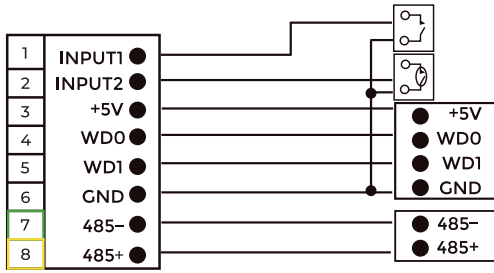
ATTENZIONE

1. Quando si effettua un collegamento a un dispositivo di carico induttivo come un relè o una serratura elettromagnetica, si consiglia di utilizzare un diodo 1A / 400 V (incluso negli accessori) in parallelo al dispositivo di carico per assorbire i picchi di tensione del carico induttivo. In questo modo il controllo accessi sarà protetto.

2. La corrente di carico del relè non può essere superiore a 1A.



3. Ingressi / Wiegand / RS485



Interfaccia di configurazione di input personalizzata / Wiegand / RS485

• L'interfaccia di input può essere configurata per eseguire diverse funzioni, come ad esempio comandare un pulsante di uscita, un sensore porta o un sensore di fumo.

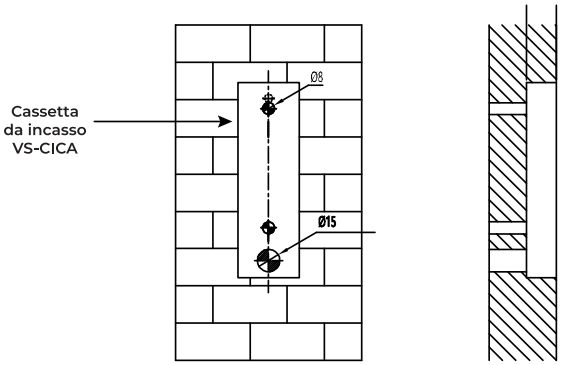
• Il protocollo Wiegand può permettere la connessione ad un altro dispositivo compatibile con lo stesso protocollo, come può essere ad esempio la pulsantiera esterna VS-PE210IP-LCD (si rimanda allo schema a pag. 3)

• L'uscita +5V è in grado di alimentare un dispositivo che supporti il protocollo Wiegand, purché esso non superi i 100mA.

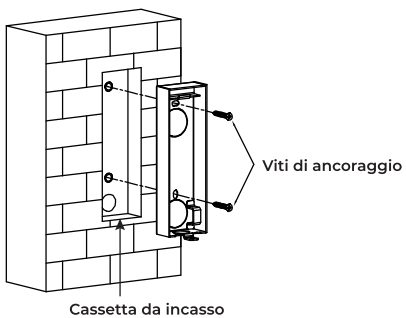
• L'uscita RS485 abilita la connessione al VS-LOCKPLUS. Da notare che in tal caso l'alimentazione 12V dovrà essere prevista come supplementare.

INSTALLAZIONE

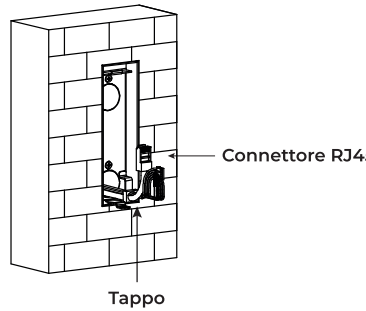
Montaggio ad incasso



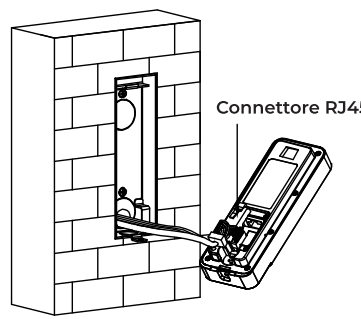
1.Incassare la cassetta a filo muro.



2. Fissare la base del controllo accessi alla cassetta appena incassata a filo muro.

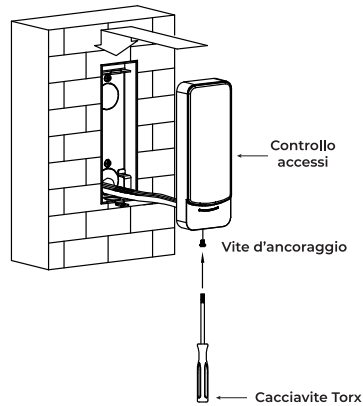


3. Far passare i cavi attraverso il foro predisposto e, successivamente, applicare il connettore RJ45.



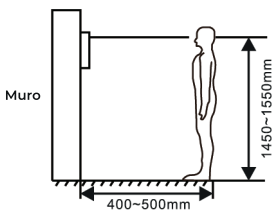
4. Collegare il connettore RJ45 al dispositivo di controllo accessi.

5. Fissare la copertura di cablaggio sul retro del dispositivo.



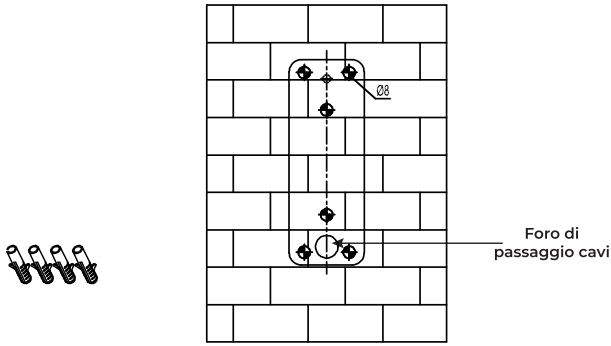
6. Alloggiare il dispositivo di controllo accessi nella base e fissarlo con l'apposita vite di ancoraggio.

Istruzioni per l'installazione

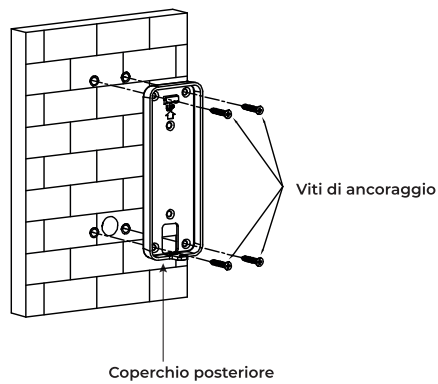


(Suggerimento): La telecamera deve trovarsi a 145 - 155 cm da terra. La pulsantiera installata a questa altezza può catturare perfettamente il volto umano.

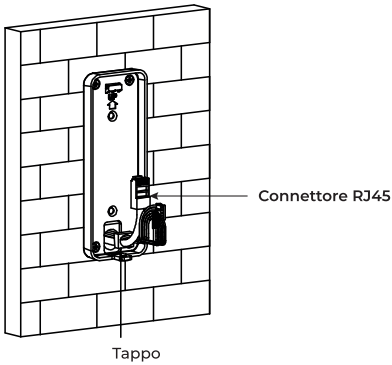
Installazione a parete



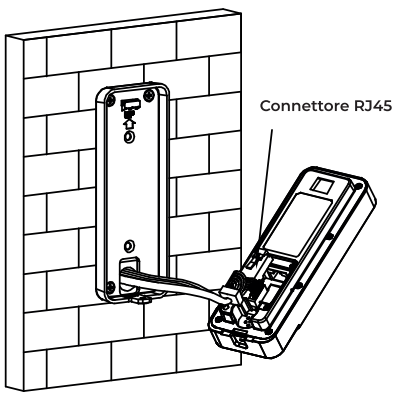
1. Segnare sul muro i fori da praticare per il fissaggio e il passaggio dei cavi.



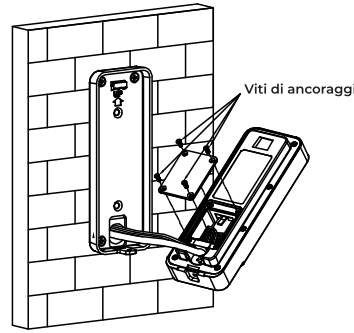
2. Fissare la base del controllo accessi al muro.



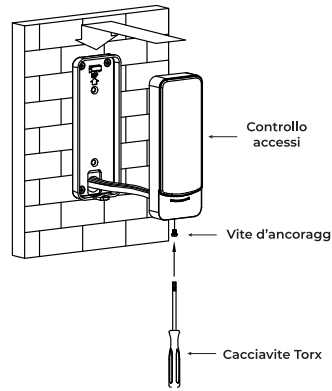
3. Far passare i cavi attraverso il foro predisposto e, successivamente, applicare il connettore RJ45.



4. Collegare il connettore RJ45 al dispositivo di controllo accessi.

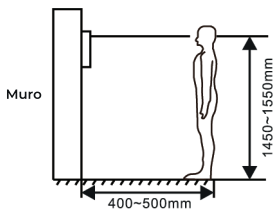


5. Fissare la copertura di cablaggio sul retro del dispositivo.



6. Alloggiare il dispositivo di controllo accessi nella base e fissarlo con l'apposita vite di ancoraggio.

Istruzioni per l'installazione

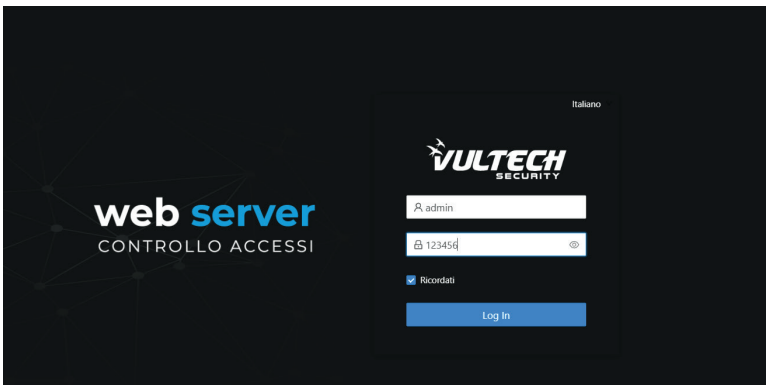


(Suggerimento): La telecamera deve trovarsi a 145 - 155 cm da terra. La pulsantiera installata a questa altezza può catturare perfettamente il volto umano.

IMPOSTAZIONI DA WEB

Questo manuale spiegherà in dettaglio i procedimenti per configurare correttamente il dispositivo utilizzando l'interfaccia web.
Collegare il dispositivo e il PC a uno switch di rete per metterli in comunicazione nella stessa rete LAN.
Per avviare il collegamento inserire il seguente indirizzo IP sulla barra del browser web: 192.168.1.200
Si raggiungerà così una pagina di login. Inserire i seguenti dati di accesso:
• Username: admin
• Password: 123456

Ora è possibile iniziare con la procedura di configurazione del dispositivo.
Nota bene: In qualsiasi caso, soprattutto per interventi tecnici su impianti preesistenti, è possibile risalire all'indirizzo IP tramite il software scaricabile dal sito vultechsecurity.it (per il download: visitare la pagina web del prodotto e fare clic su "Supporto").

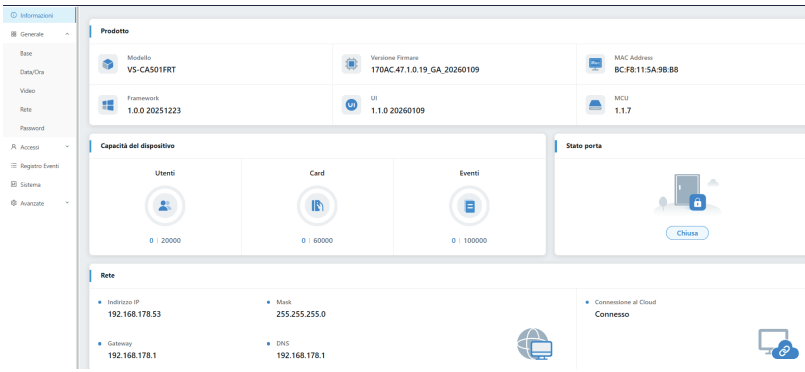


1.Generale

Questo è il primo punto che s'incontra nel pannello di configurazione.
In esso è possibile recuperare informazioni generali del dispositivo. Di seguito verranno illustrate le varie sezioni in dettaglio.

1.1. Generale > Informazioni

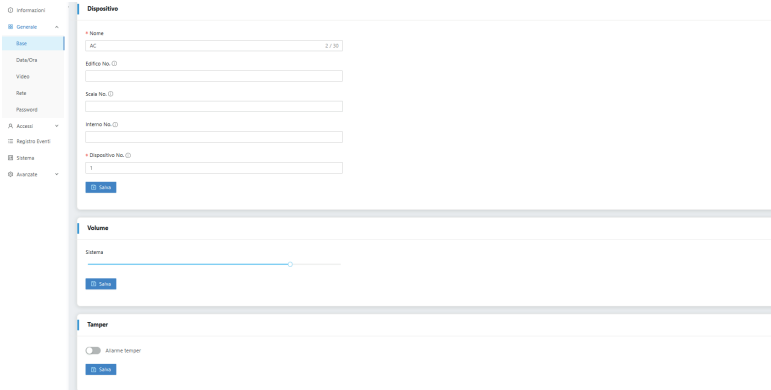
Le informazioni di base del prodotto appaiono quando si accede per la prima volta all'interfaccia web.



Modello	Modello del dispositivo
Versione Firmware	Versione firmware del dispositivo
MAC Address	Indirizzo MAC del dispositivo
Framework	Struttura del dispositivo
UI	Interfaccia utente del dispositivo
MCU	Micro Controller Unit per gestire accessi fisici
Utenti	Indicatore degli utenti registrati (max. 20000)
Card	Indicatore delle card registrate (max. 60000)
Eventi	Indicatore degli eventi verificati (max. 100000)
Stato porta	Indicatore dello stato della porta
Indirizzo IP	Indirizzo IP attuale del dispositivo
Mask	Maschera di sottorete del dispositivo
Gateway	Gateway del dispositivo
DNS	Domain Name Server del dispositivo
Connessione al Cloud	Stato della connessione al Cloud

1.2. Generale > Base

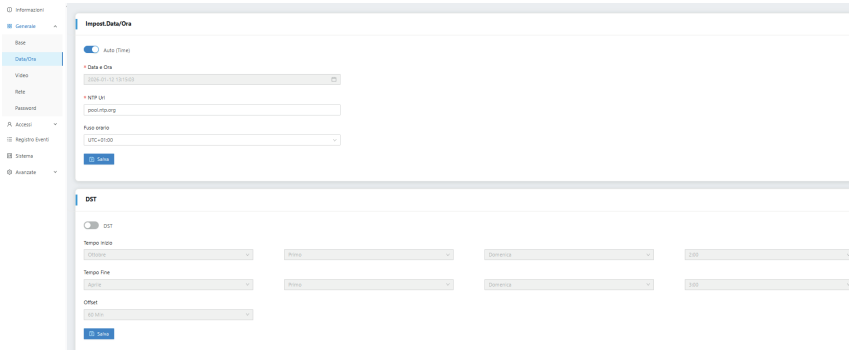
In questa colonna è possibile configurare alcune impostazioni di base del dispositivo come la collocazione, i livelli di volume e il tamper.



Dispositivo	Sezione dove sono indicate le informazioni di collocazione del dispositivo (nome del dispositivo, edificio, scala, interno, numero del dispositivo).
Volume	Impostazioni del volume di sistema.
Tamper	Abilitazione del tamper di manomissione.

1.3 Generale > Impost. Data/Ora

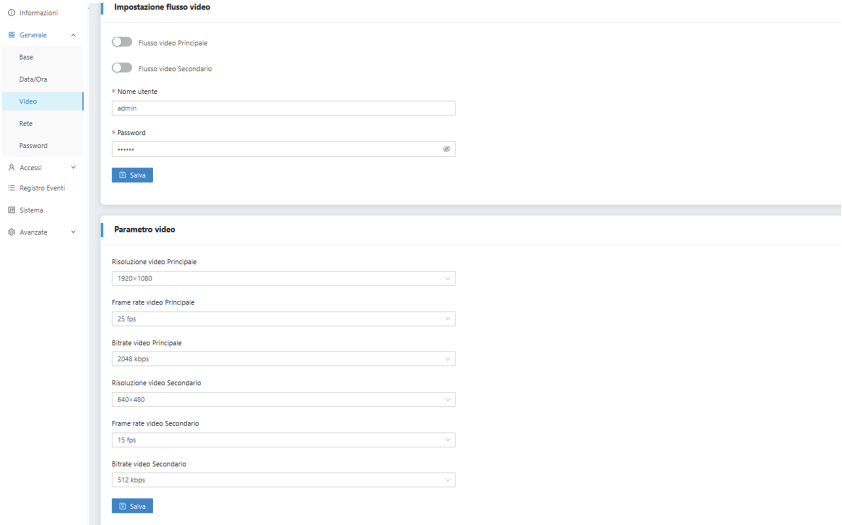
Qui è possibile configurare l'ora del dispositivo e impostare l'ora legale.



Auto (Time)	Abilita la sincronizzazione dell'ora con quella del web.
Data e ora	Impostazione di data e ora.
NTP URL	È un protocollo utilizzato per sincronizzare l'ora NTP (Network Time Protocol).
Fuso orario	Impostazione relativa al fuso orario di appartenenza.
DST	Abilitare per impostare l'ora legale.
Tempo inizio	Impostare l'inizio dell'ora legale.
Tempo fine	Impostare la fine dell'ora legale.
Offset	Il valore predefinito è 60 minuti.

1.4 Generale > Impostazione flusso video

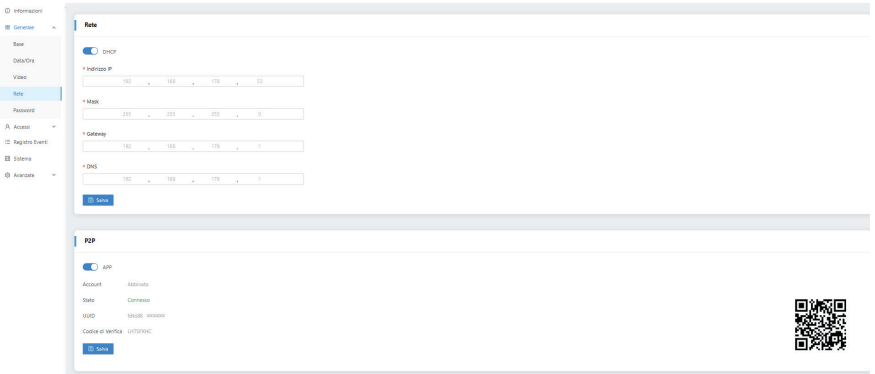
Qui è possibile abilitare i flussi video e i relativi parametri.



Flusso video principale	Abilita il flusso video principale
Flusso video secondario	Abilita il flusso video secondario
Nome utente	Indica il nome utente
Password	Indica la password impostata
Risoluzione video Principale	Imposta la risoluzione video principale
Frame rate video Principale	Imposta il frame rate video principale
Bitrate video Principale	Imposta il bitrate video principale
Risoluzione video Secondario	Imposta la risoluzione video secondario
Frame rate video Secondario	Imposta il frame rate video secondario
Bitrate video Secondario	Imposta il bitrate video secondario

1.5 Generale > Rete

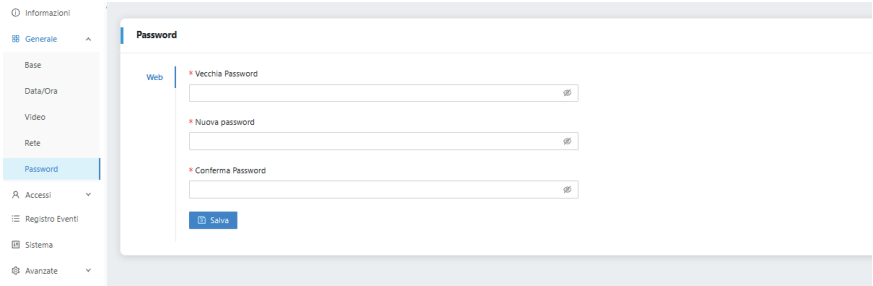
La rete del dispositivo può essere impostata su DHCP o su un indirizzo IP statico. Possibilità di impostare, inoltre, l'accesso al cloud da app V-Guardian EVO.



DHCP	Abilitare DHCP (Dynamic Host Configuration Protocol) per distribuire dinamicamente i parametri di configurazione della rete.
Indirizzo IP	Configurare l'indirizzo IP statico per distribuire manualmente i parametri di configurazione della rete.
Mask	Maschera di sottorete.
Gateway	Un componente che fa parte di due reti, che utilizzano protocolli diversi.
DNS	Domain Name Server del dispositivo.
App	Genera il codice QR per raggiungere il cloud tramite app.
Account	Indica lo stato dell'account.
Stato	Indica il corretto stato di connessione con il cloud.
UUID	Codice identificativo univoco del dispositivo.
Codice di Verifica	Codice a doppio fattore di protezione.

1.6 Generale > Password

In questa sezione è possibile modificare e personalizzare la propria password web. La password web è utile all'amministratore per accedere alle impostazioni del dispositivo. La password predefinita è 123456.



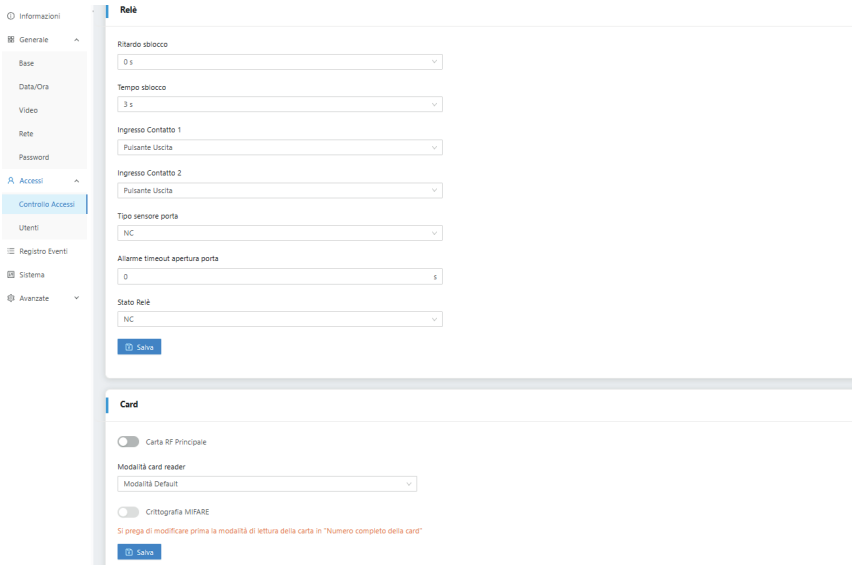
Vecchia Password	Inserire la password attuale.
Nuova Password	Inserire la nuova password.
Conferma Password	Confermare la nuova password reinserendola.

2. Accessi

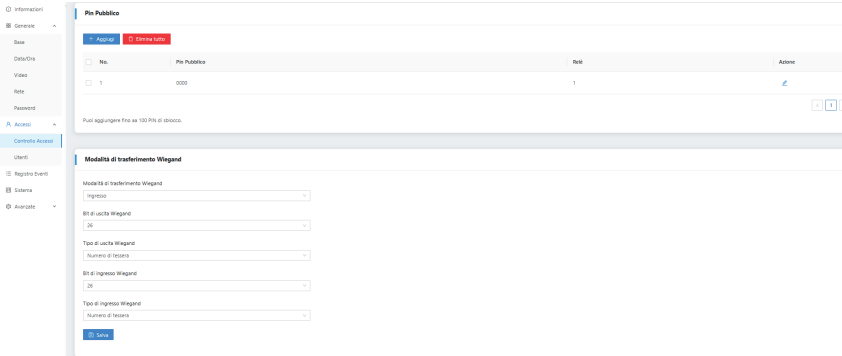
Qui è possibile gestire i parametri per configurare gli ingressi e l'uscita del controllo accessi e impostare i parametri.

2.1 Accessi > Controllo accessi

In questa sezione è possibile inserire i parametri per il controllo degli accessi e delle card.

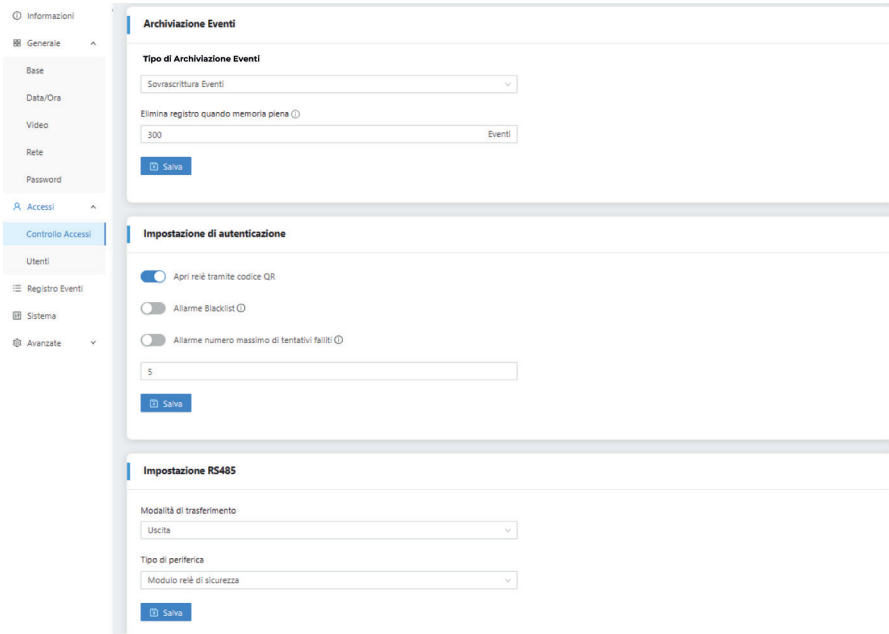


Ritardo sblocco	Imposta il tempo di ritardo sull'attivazione del relè.
Tempo sblocco	Imposta la durata di attivazione del relè.
Ingresso Contatto 1	Imposta la modalità di scelta dell'ingresso 1.
Ingresso Contatto 2	Imposta la modalità di scelta dell'ingresso 2.
Tipo sensore porta	Seleziona il tipo di sensore porta tra NC e NO.
Allarme timeout apertura porta	Imposta un tempo allo scadere del quale può attivarsi un allarme che genera un messaggio popup in app.
Stato relè	Seleziona la modalità del relè tra NC e NO.
Carta RF Principale	Abilita l'uso di una card principale.
Modalità card reader	Cambia il tipo di card.
Crittografia MIFARE	Crea una crittografia avanzata della card.



PIN Pubblico	Sezione dedicata all'aggiunta o all'eliminazione del PIN di sblocco del controllo accessi. Questo PIN è definito pubblico in quanto generico e non legato a nessun utente.
Modalità di trasferimento Wiegand*	Imposta la modalità di trasferimento/ricezione dati con protocollo Wiegand.
Bit di uscita Wiegand*	Imposta la modalità di Bit d'uscita Wiegand.
Tipo di uscita Wiegand*	Seleziona il tipo di uscita.
Bit di ingresso Wiegand*	Imposta la modalità di Bit d'ingresso Wiegand.
Tipo di ingresso Wiegand*	Seleziona il tipo di ingresso.

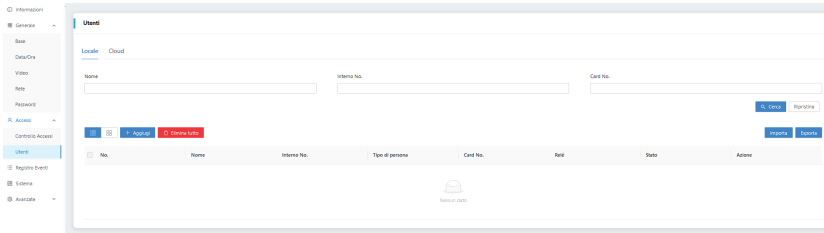
***Consultare il manuale dedicato al corretto uso del protocollo Wiegand.**



Tipo di archiviazione	Seleziona il tipo di archiviazione dei log.
Elimina registro quando memoria piena	Imposta il numero massimo di eventi da tenere in memoria. Superato il limite, i nuovi eventi sovrascriveranno i più vecchi.
Apri relà tramite codice QR	Abilita o disabilita l'opzione di aprire il relè tramite un codice QR.
Allarme Blacklist	Abilita l'invio di un allarme sonoro e di una notifica popup su app al verificarsi di un tentativo di accesso di un utente in blacklist.
Allarme numero massimo di tentativi falliti	Abilita l'invio di un allarme sonoro e di una notifica popup su app al verificarsi di un certo numero di tentativi di accesso (da impostare).
Modalità di trasferimento	Seleziona la modalità di trasferimento dati (Ingresso/Uscita) tramite protocollo RS485.
Tipo di periferica	Seleziona il tipo di periferica.

2.2 Accessi > Utenti

Questa sezione è dedicata alla creazione degli utenti per la gestione del dispositivo di controllo accessi. Una volta creato l'utente, sarà possibile personalizzarne le informazioni in una finestra che apparirà.



Nome / Interno No. / Card No.	Campi destinati alla ricerca di utenti già registrati.
Aggiungi	Usare questo comando per aprire la finestra utile ad aggiungere un nuovo utente.
Elimina tutto	Usare questo comando per eliminare gli utenti già precedentemente registrati.
Importa	Importa una nuova lista di utenti da registrare.
Esporta	Esporta la lista degli utenti registrati.

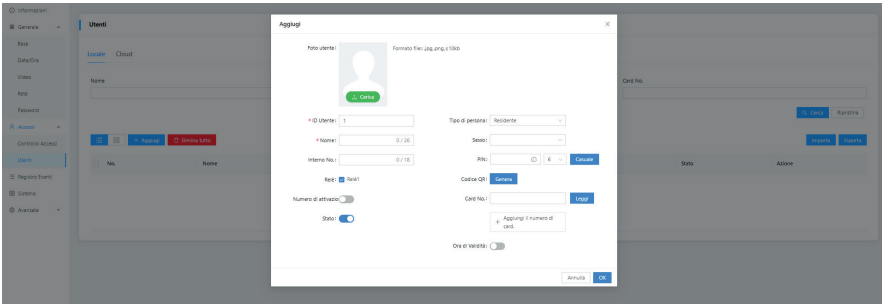
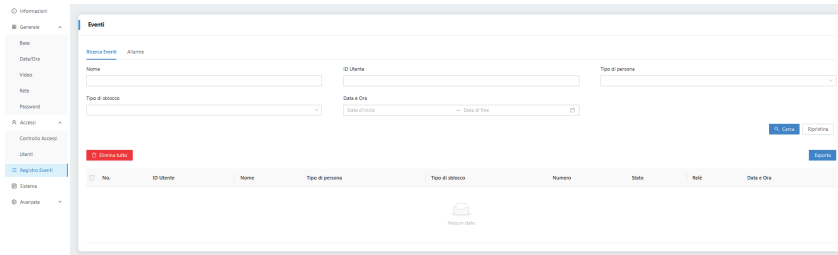


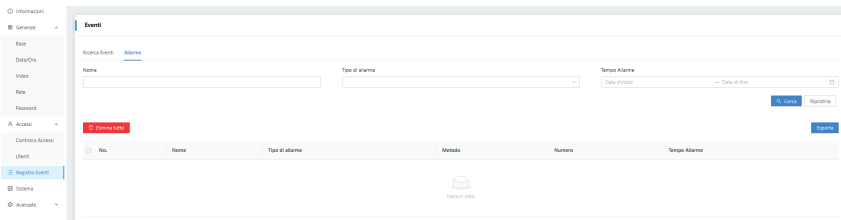
Foto utente	Permette di caricare una foto dell'utente.
ID Utente	Indica il numero identificativo.
Tipo di persona	Seleziona il tipo di utente.
Nome	Permette di personalizzare l'utenza aggiungendo un nome.
Sesso	Permette di specificare il tipo di sesso dell'utente.
Interno No.	Permette di indicare il numero di interno relativo all'utente.
PIN	Creazione di un PIN personalizzato, con possibilità di generazione automatica.
Relè	Abilita il relè.
Codice QR	Genera un codice QR di identificazione.
Numero di attivazioni	Se abilitato, permette di indicare il numero massimo di azioni consentite per l'utente.
Card No.	Permette di associare una o più card all'utente.
Stato	Attiva o disattiva l'utenza.
Ora di validità	Permette di indicare fasce orarie entro le quali l'utente è abilitato a utilizzare le funzioni del controllo accessi.

3. Registro Eventi

Questa è la sezione del registro degli eventi. Qui è possibile risalire al tipo di evento effettuando una ricerca.



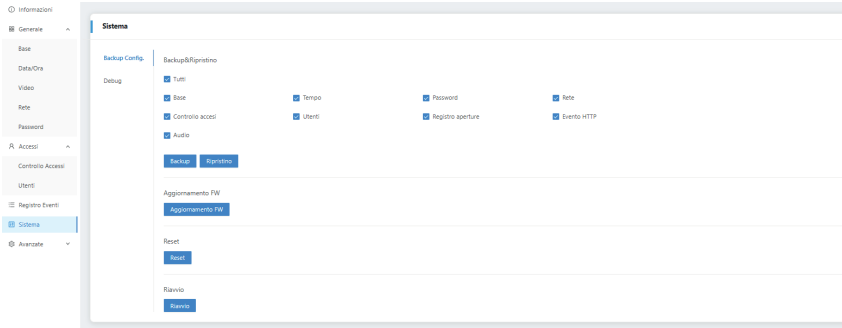
Ricerca Eventi	Possibilità di effettuare una ricerca di eventi registrati inserendo uno o più parametri tra: Nome, ID Utente, Tipo di persona, Tipo di sblocco, Data e Ora.
Elimina tutto	Elimina i risultati della ricerca.
Esporta	Esporta i risultati della ricerca.



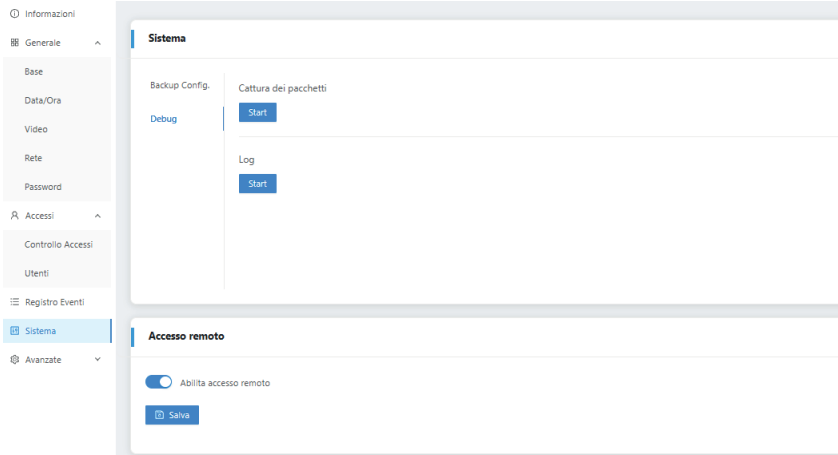
Allarme	Possibilità di effettuare una ricerca di allarmi registrati inserendo uno o più parametri tra: Nome, Tipo di allarme, Tempo allarme.
Elimina tutto	Elimina i risultati della ricerca.
Esporta	Esporta i risultati della ricerca.

4. Sistema

Questa è la sezione del menù nella quale è possibile ripristinare ed esportare la configurazione del dispositivo.
È inoltre possibile aggiornare il firmware, resettare o riavviare il dispositivo ed esportare un file di debug utile per analizzare eventuali anomalie di funzionamento.



Backup&Ripristino	Spuntare le voci per le quali si intende effettuare il backup o il ripristino di un dispositivo.
Aggiornamento FW	Comando che permette di aggiornare il firmware del dispositivo.
Reset	Riporta il dispositivo ai valori di fabbrica.
Riavvio	Effettua un riavvio del dispositivo.



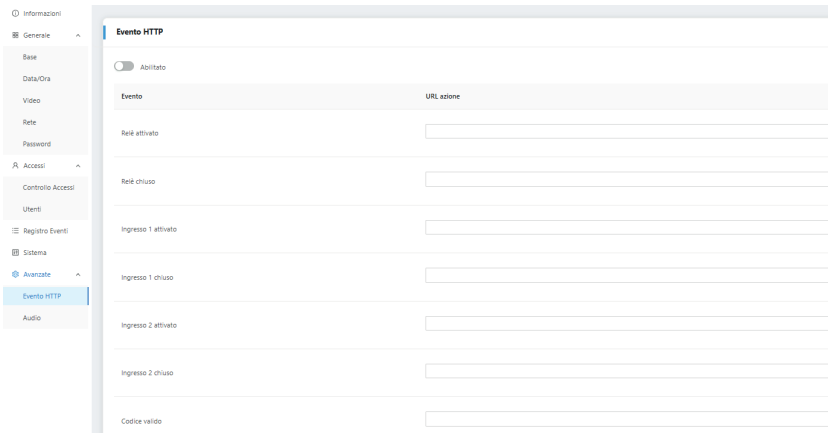
Cattura dei pacchetti	Crea pacchetti dati utili a individuare eventuali bug.
Log	Crea un registro degli eventi.
Abilita accesso remoto	Permette di abilitare la funzione di accesso da remoto al dispositivo.

5. Avanzate

In questo punto del menù è possibile abilitare funzioni avanzate relative agli eventi HTTP e all'audio.

5.1 Avanzate > Evento HTTP

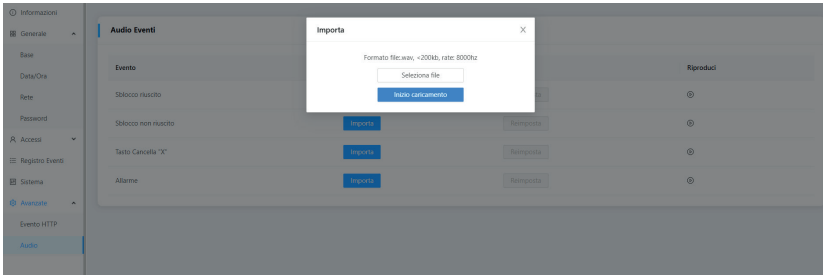
In questa sezione, abilitando la funzione evento HTTP, è possibile impostare un'azione inserendo una o più stringhe nei campi richiesti. È possibile, grazie a queste azioni, interfacciarsi con relè e centrali di allarme che gestiscono le stringhe HTTP.



5.2 Avanzate > Audio

In questa sezione è possibile personalizzare i messaggi audio relativi agli eventi indicati. Per procedere, sarà sufficiente selezionare il comando Importa e procedere con l'upload di un file audio (Formato file: .wav, <200kb, rate: 8000hz).

È inoltre possibile reimpostare l'audio di default per ogni singolo evento e ascoltarne un'anteprima tramite il comando Riproduci.



RISOLUZIONE DEI PROBLEMI COMUNI

1. Il controllo accessi non si avvia o si spegne.

- Controllare se c'è un'interruzione di corrente e, nel caso, ripristinare l'erogazione.

2. Il controllo accessi non ottiene un indirizzo IP.

- Controllare se il DHCP è abilitato sul controllo accessi.
- Controllare se il router può fornire l'indirizzo IP normalmente.

3. Non si avverte alcun suono di notifica.

- Controllare se il volume è impostato al minimo.

4. La carta Mifare non è riconosciuta dal dispositivo.

- Accedere dal web al pannello di gestione e controllare se la card è configurata come "Numero completo della card".

5. Il dispositivo emette un suono continuo.

- Verificare lo stato del sensore porta e il morsetto dedicato.

N.B. Si consiglia di verificare il corretto isolamento dei cavi a corredo del dispositivo

Informazioni generali di sicurezza

Per un corretto uso del prodotto leggere attentamente e conservare il seguente foglio illustrativo o il manuale d'istruzioni in dotazione o scaricabile gratuitamente sul sito web www.vultechsecurity.it nella pagina dedicata al prodotto.

Disposizioni per un utilizzo sicuro dei prodotti:

Importanti informazioni sulla sicurezza:

- PERICOLO DI SCOSSE ELETTRICHE
- Non utilizzare il dispositivo vicino all'acqua
- Pulire soltanto con un panno asciutto
- Eseguire l'installazione secondo le istruzioni del produttore
- Non installare vicino a fonti di calore quali termosifoni, stufe e altri apparecchi che producono calore, incluso gli amplificatori

AVVISO: PER RIDURRE IL RISCHIO DI SCOSSE ELETTRICHE, NON ESPORRE IL DISPOSITIVO A PIOGGIA O UMIDITA'.

Informazioni sullo smaltimento e tutela dell'ambiente
Rispettare le normative europee per lo smaltimento dei prodotti.

Smaltimento di apparecchiature elettriche ed elettroniche:

Il simbolo del cassonetto barrato riportato sull'apparecchiatura indica che il prodotto alla fine della sua vita utile deve essere raccolto separatamente dagli altri rifiuti. Per lo smaltimento sarà necessario portarlo in un apposito punto di raccolta per il riciclaggio di apparecchiature elettriche ed elettroniche oppure riconsegnarlo al rivenditore al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente, in ragione di uno a uno. Un corretto smaltimento di questi prodotti e delle relative batterie permette di salvaguardare l'ambiente e la salute delle persone evitando problemi di inquinamento, con conseguenti ripercussioni sulla salute umana, che potrebbero verificarsi in caso di smaltimento inadeguato. Per ulteriori informazioni sul corretto smaltimento dei prodotti consultare il servizio locale di smaltimento dei rifiuti.

Smaltimento delle batterie usate:

Il simbolo del cassonetto barrato indica che le batterie non devono essere gettate tra i rifiuti domestici generici. Se presenti, dovranno essere portate in un apposito punto di raccolta per il riciclaggio. Consultare il manuale d'istruzioni per conoscere la corretta procedura per la rimozione delle batterie.

Il prodotto o la sua confezione riporta il seguente marchio:

CE

Consultare la descrizione del prodotto sul sito web www.vultechsecurity.it per conoscere il marchio CE applicabile.

Con la presente, Giuliano Store S.r.l., dichiara che il prodotto è conforme ai requisiti essenziali e ad altre disposizioni pertinenti stabilite dalla direttiva EMC 2014/30/EU. Per prendere visione della dichiarazione di conformità visitare la scheda del prodotto sul sito web www.vultechsecurity.it

ATTENZIONE! Nel caso in cui il prodotto necessiti di batterie, prestare particolare attenzione all'installazione di quest'ultime. Le batterie non installate correttamente, infatti, possono danneggiarsi e perdere le sostanze al loro interno con il conseguente rischio di esplosioni ed eventuali danni a cose e persone. Evitare di manometterle, esporle a fonti di calore, all'umidità, a liquidi o a materiali conduttori.

ATTENZIONE! Nel caso in cui il prodotto sia alimentato da un alimentatore, questo deve essere utilizzato esclusivamente al chiuso. L'unico alimentatore che l'azienda garantisce è quello fornito con il prodotto. Evitare di manometterlo o cercare di ripararlo in caso di malfunzionamento. Evitare di esporlo a fonti di calore, all'umidità, a liquidi o a materiali conduttori

Garanzia limitata sull'hardware: VulTech Security® garantisce che il prodotto acquistato è privo di difetti di materiali e d è perfettamente funzionante per il periodo di 2 anni a decorrere della data di acquisto. Fatta eccezione per quanto proibito dalla legge in vigore, la presente garanzia non è trasferibile ed è limitata all'acquirente originale.

Condizioni Generali di Garanzia: VulTech Security® garantisce tutti i prodotti per un periodo di 2 anni a decorrere dalla data di acquisto del prodotto (**salvo differenti indicazioni**). Saranno accettati in garanzia solo prodotti accompagnati da uno scontrino fiscale o da fattura di acquisto. Ove necessario dovrà comparire in quest'ultima il codice seriale del prodotto in questione. La presente garanzia non copre problemi o danni causati da: 1) incidente, abuso, applicazione impropria, riparazione, modifica o smontaggio non autorizzato; 2) operazione impropria di manutenzione; 3) utilizzo di accessori non forniti da VulTech quali ad esempio batterie di ricambio. Prima di presentare una richiesta di garanzia, si raccomanda di visitare per ulteriori informazioni la sezione relativa all'assistenza tecnica sul sito web www.vultechsecurity.it

Esclusione di responsabilità: VULTECH SECURITY NON SARA' RESPONSABILE PER ALCUN DANNO SPECIALE, INDIRETTO, INCIDENTALE O CONSEQUENZIALE DI QUALSIASI GENERE, COMPRESE PERDITE DI PROFITTI INTROITI O DI DATI (SIA DIRETTAMENTE CHE INDIRETTAMENTE) O PERDITE COMMERCIALI PER LA VIOLAZIONE DI QUALCHE GARANZIA ESPLICITA O IMPLICITA SUL PRODOTTO ACQUISTATO

Indirizzo: GIULIANO STORE S.R.L - Strada consortile, consorzio IMPRE.CO, zona ASI, Carinaro (CE), 81032, Italia

VER.10.25

VULTECH SECURITY

CONTROLLO ACCESSI