Creating Security Solutions. *With Care.*

RISCO Cloud

Applicazione di Gestione Remota

Manuale Installatore

Per maggiori informazioni sulle circa le centrali sono supportate dal RISCO CLOUD fare riferimento al nostro sito web: www.riscogroup.it

Contenuti

Introduzione

Questa guida fornisce informazioni riguardanti L'applicazione di Gestione Remota del RISCO Cloud per l'installatore e le istruzioni su come utilizzare l'applicazione. I destinatari di questa guida sono il personale incaricato per le installazioni e l'amministratore delle centrali e del sistema VUpoint. Lo scopo principale di questa guida è quello di fornire all'installatore le informazioni necessarie per gestire le centrali installate ed effettuare l'integrazione con il video VUpoint.

Documenti Correlati

I manuali di installazione di Agility ™ 3 e LightSYS ™ 2 forniscono ulteriori informazioni su alcuni dei temi affrontati in questa guida. Il Manuale del sistema VUpoint fornisce informazioni sulla connessione delle telecamere IP al Cloud RISCO

Abbreviazioni

Abbrev.	Descrizione
CP	Centrale antintrusione.
CPNS	Servizio di notifica centrale antintrusione
CPWS	Web Service centrale antintrusione
CSR	Ricevitore della società di ricezione eventi
Proxy	Server Proxy RISCO
GPRS	General Packet Radio Service (comunicazioni GPRS)
GPRS Proxy	Server parte della configurazione del Cloud RISCO preposto alla gestione delle comunicazioni GPRS con le centrali antintrusione.
IIS	Internet Information services
ISP	Internet Service Provider
RISCO Cloud/Proxy	Applicazione/Server Proxy RISCO
RISCO Cloud	Applicazione RISCO Server

Abbrev.	Descrizione
PSTN	Public Switched Telephone Network (Linea telefonica commutata)
RP	Applicazione di Programmazione Remota (per programmare le centrali antintrusione)
SIA	Protocollo di comunicazione eventi
SP	Service Provider – fa riferimento alle società di ricezione eventi supportate dal RISCO Cloud
WAApp	Applicazione di amministrazione Web (Accesso Area di Administrazione di RISCO Cloud)
WIApp	Applicazione Web Installatore (Accesso Installatore al RISCO Cloud)
WUApp	Applicazione Web Utente (Accesso Utente al RISCO Cloud)

Panoramica

L'area Installatore del Cloud RISCO è una componente importante basata sulla piattaforma web del servizio RISCO Cloud. Implementando una connettività di rete TCP/IP sicura, il Cloud RISCO fornisce connettività ad alta velocità tramite un'interfaccia a banda larga. Il ruolo predominante del Cloud RISCO è quello di gestire le comunicazioni tra i sistemi di sicurezza installati nelle case/aziende e, se richiesto, interfacciare questi sistemi con le apparecchiature delle società di ricezione eventi. Oltre alla segnalazione degli eventi, il Cloud RISCO permette al sistema di sicurezza di essere programmato e controllato mediante Client dedicati, applicazioni Web e applicazioni per Smartphone destinate all'utente finale.

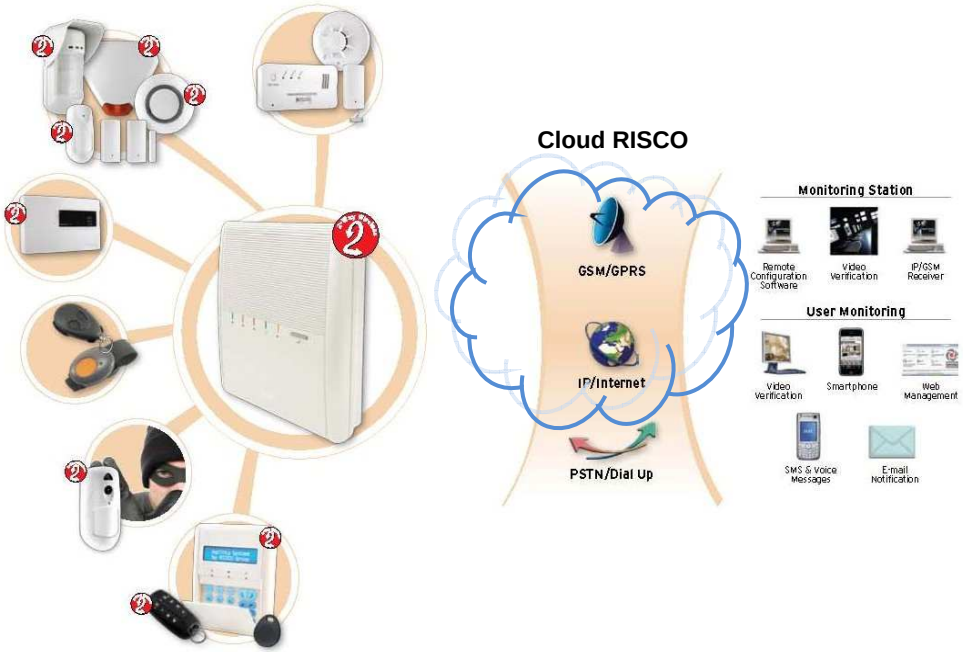

Figura 1 Architettura del sistema

I componenti principali del sistema sono:

- RISCO Cloud / Proxy - applicazione server / proxy che consente il collegamento tra le centrali gli utenti finali e i fornitori di servizi di ricezione eventi.
- Centrali RISCO – Centrali antintrusione fornite di moduli di comunicazione GSM / GPRS, IP o PSTN.

Registrazione Installatore

L'applicazione di Gestione dell'Area Installatore è una delle tante componenti del Cloud RISCO e richiede all'installatore una registrazione per ottenere l'accesso a questo servizio.

Registrazione all'area Installatore

1. Inserire l'indirizzo www.riscocloud.com/ELAS/WAAPP/Login.aspx nel browser e premere OK. Viene visualizzata la pagina di login.

Figura 2 Pagina di Login per l'Installatore

NOTE – Se ci si è già registrati ma non si ricordano più le credenziali di accesso, fare clic su Password Recovery per richiedere una password temporanea che verrà inviata al proprio indirizzo di posta elettronica precedentemente inserito.

Clic su Sign Up …. per visualizzare la pagina di Registrazione per l'installatore.

Figura 3 Pagina registrazione Installatore

2. Immettere i seguenti dati di registrazione negli appositi campi:

Campo	Descrizione
First/Last Name	Immettere il proprio nome e cognome
Email (Login Name)	Immettere la propria mail per il Login
Company Name	Immettere il nome della propria società
Password Confirm	Immettere la password scelta (2 volte)
Panel ID	Immettere il numero ID di una centrale. **Per la registrazione installatore è richiesta una centrale da connettere al cloud per la quale non sia già stata fatta la registrazione utente.**
Anti-Spam Code	Immettere il codice anti-spam visualizzato

3. Fare clic su Registra. Il processo di registrazione invierà una mail di conferma al vostro indirizzo di posta elettronica specificato.
4. Dalla mail ricevuta, cliccare sul link evidenziato per confermare la registrazione. La pagina di accesso viene visualizzata ed è ora è possibile accedere all'Area Installatore di gestione del cloud RISCO.

Login nell'applicazione dell'Area Installatore

Per accedere all'area installatore è necessario effettuare il Login.

Login

Per accedere all'applicazione:

1. Inserire User Name e Password.
2. Cliccare su Login e viene visualizzata la pagina principale.

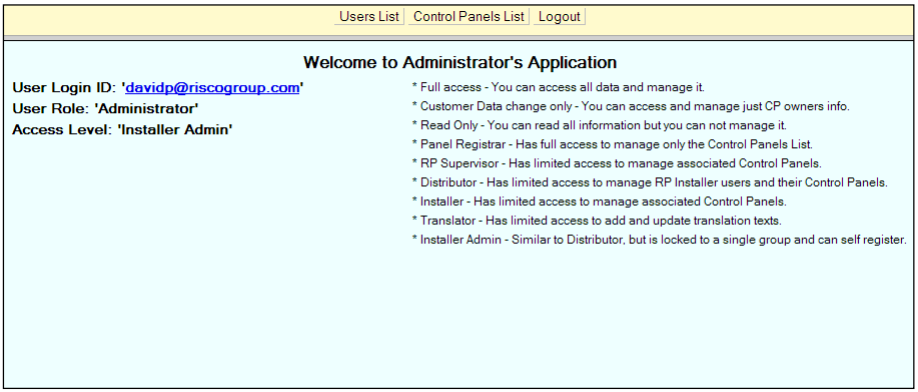

Figura 4 Pagina principale

La pagina principale visualizza i dettagli dell'utente corrente. Nella parte superiore della pagina ci sono dei menu per i collegamenti alle varie pagine dell'applicazione.

Logout

Per terminare la sessione fare click su Logout e automaticamente si ritorna alla pagina di Login.

Area Installatore - Gestione Utenti/Installatori

Nella pagina **User List** (Elenco utenti), è possibile visualizzare l'elenco degli utenti / installatori che sono stati creati e autorizzati dall'installatore amministratore ad entrare nell'area installatore limitata per alcune funzioni. In questa area è quindi possibile creare altri utenti/installatori per la gestione delle.

Figura 5 Pagina Lista Utenti/Operatori

Colonna	Descrizione
Login ID	Il nome utente immesso quando si fa il Login
Role	Il tipo di utente. Il tipo può essere solo programmatore remoto (utente RP).
Access Level	Il livello di autorizzazione dell'utente. Il livello di accesso può essere solo Installatore
First/Middle/Last Name	I dati personali dell'utente.
Phone	Il numero di telefono dell'utente.
Last Update	La data in cui i dati dell'utente sono stati modificati l'ultima volta.
Updated By	L'operatore RISCO Cloud che ha aggiornato per ultimo i dati dell'utente. (Se bianco significa che l'utente Administrator è stato cancellato dal database del Cloud RISCO)
Display List Filtering	L'elenco di visualizzazione degli utenti può essere filtrato selezionando dalla finestra in basso a destra il numero massimo di utenti visualizzati per pagina.

Aggiungere un nuovo Utente/Installatore

Per aggiungere un nuovo Utente/Installatore:

1. Nella pagina Elenco Utenti, scegliere **New User** (Nuovo utente) ; viene visualizzata la pagina Aggiornamento utente.

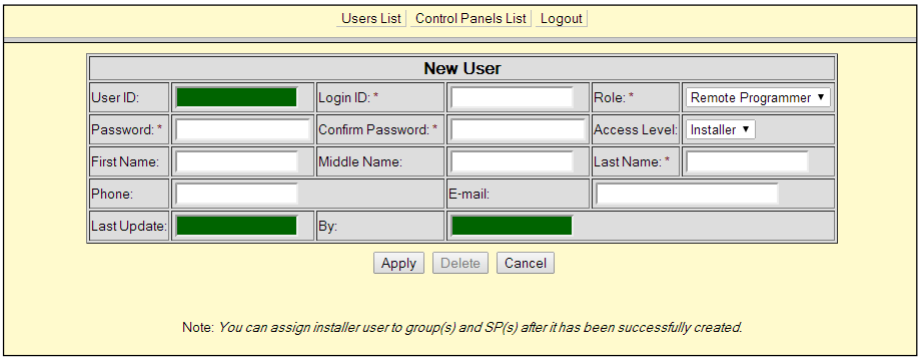

Figura 6 Pagina Nuovo Utente

NOTA – I campi obbligatori sono contrassegnati da un asterisco (*).

2. Inserire la login ID di accesso del nuovo utente, password (due volte) e dati personali negli appositi campi.

NOTA – La User ID utente viene assegnata automaticamente una volta che il nuovo utente viene salvato nel sistema.

Editare un Utente/Installatore esistente

Per editare i dettagli di un Utente/Installatore esistente:

1. Nella pagina Elenco Utenti, fare clic sull' ID dell' Utente / installatore che si desidera modificare (colorata in blu); viene visualizzata la pagina
2. Modificare i dati dell' Utente/Installatore.
3. Cliccare OK per salvare.

Cancellare un Utente/Installatore

Per cancellare un Utente/Installatore:

1. Nella pagina Elenco Utenti, fare clic sull' ID dell'utente/installatore si desidera cancellare; viene visualizzata la pagina.
2. Click Delete (cancella) e poi OK; l'utente viene cancellato.

Lista delle Centrali

La Lista delle centrali è un elenco di tutte le centrali abbinate all'Installatore. Una centrale deve comparire nella lista per essere riconosciuta come connessa al Cloud RISCO.

Per visualizzare l'elenco delle centrali:

1. Aprire la pagina **control panel list** (Lista delle centrali).
2. Scegliere gli opportuni filtri di ricerca per le centrali che si desidera visualizzare e fare clic su Trova; vengono visualizzate nella schermata le voci richieste.

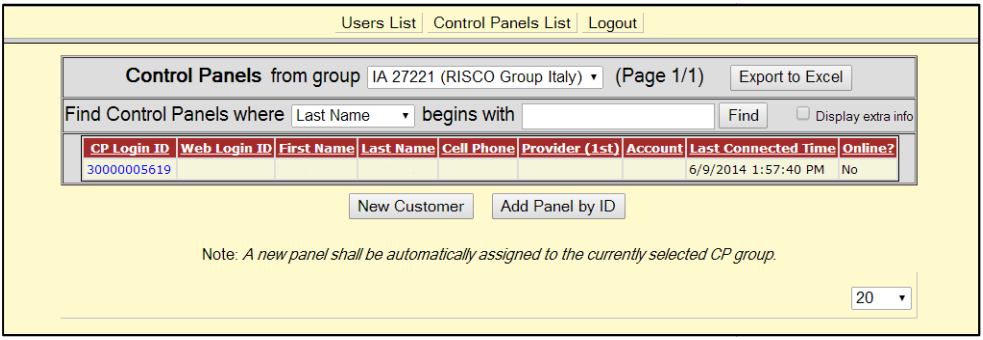

Figura 7 Pagina Lista delle Centrali

Aggiungere una nuova Centrale

Questa funzione permette di aggiungere una centrale appena connessa per la quale non si è ancora fatta la registrazione utente al Cloud RISCO. In pratica questa funzione viene usata per la centrale che si sta installando.

Per aggiungere una nuova Centrale:

Nella pagina Lista delle Centrali, fare clic su **New Customer** (Nuovo Cliente); viene visualizzata la pagina Nuova Centrale.

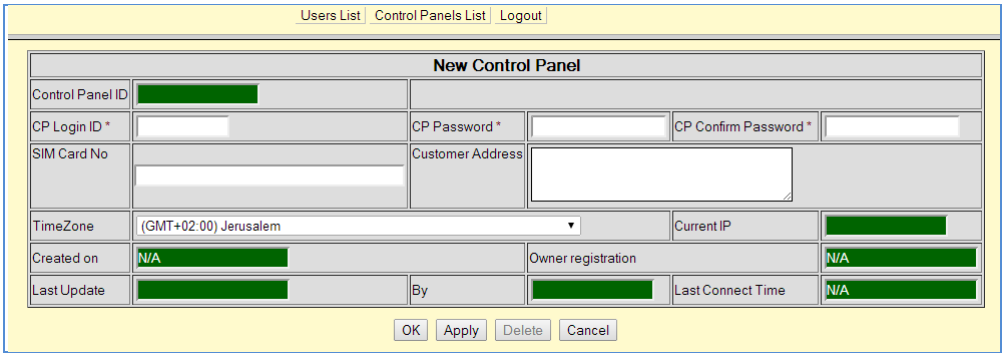

Figura 8 Pagina Nuova Centrale

1. Inserire i dettagli della nuova centrale nei campi appropriati. I campi disponibili sono descritti nella seguente tabella.

Campo	Descrizione
Control Panel ID	Un numero che viene assegnato automaticamente dal Cloud quando si crea il cliente.
CP Login ID	Questo è il numero univoco "Panel ID" (ID Centrale) che identifica ogni centrale. Questo numero deve essere uguale a quello riportato sulla etichetta della centrale visibile anche da tastiera tramite menù di visualizzazione delle informazioni e/o in diagnostica. Questo numero viene utilizzato dalla centrale per l'identificazione durante la connessione a RISCO Cloud. Per modificare questo campo, fare clic sul pulsante **change** (Modifica) a destra del campo quindi fare clic su OK nella finestra di conferma. Il numero massimo di caratteri che si può inserire l'ID CP è 16 (le centrali RISCO ne utilizzano 11/15)
CP Password/ CP Confirm Password	Utilizzato dalla centrale per l'autenticazione quando si connette a RISCO Cloud. Questo parametro deve essere identico a quello programmato in centrale. Il numero massimo di caratteri si può inserire per il CP password è 16.(Sulle centrali RISCO il default è AAAAAA)
SIM Card No.	Numero di riferimento scheda sim del modulo di comunicazione GPRS della centrale.
Customer Address	Dettagli dell'indirizzo del cliente.
Time Zone	Il fuso orario in cui si trova la centrale RISCO.

Campo	Descrizione
Current IP	Indirizzo IP attuale della centrale (questo parametro viene visualizzato dopo il primo collegamento tra la centrale e il RISCO Cloud).
Last Update/By	L'ultima volta che le informazioni della centrale sono stati aggiornati dall'utente/installatore e colui che ha eseguito le modifiche.
Last Connect Time	L'ultima volta che la centrale si è collegata al RISCO Cloud.

Aggiungere una Centrale esistenze già registrata come Utente sul Cloud e non associata a nessun installatore.

Questa funzione permette di aggiungere una centrale per la quale è già stata fatta una registrazione utente e non è ancora associata ad alcun installatore. Per aggiungere una centrale con queste caratteristiche è necessario possedere le 15 cifre del numero ID centrale (Panel ID). In pratica questa funzione viene usata per aggiungere opzioni come il VUpoint ad una centrale che è già stata installata in precedenza.

Per associare al proprio gruppo una centrale esistente procedere come segue:
Nella pagina Lista delle Centrali, fare clic su **Add Panel by ID** (Aggiungi centrale tramite numero ID centrale); viene visualizzata la pagina seguente.

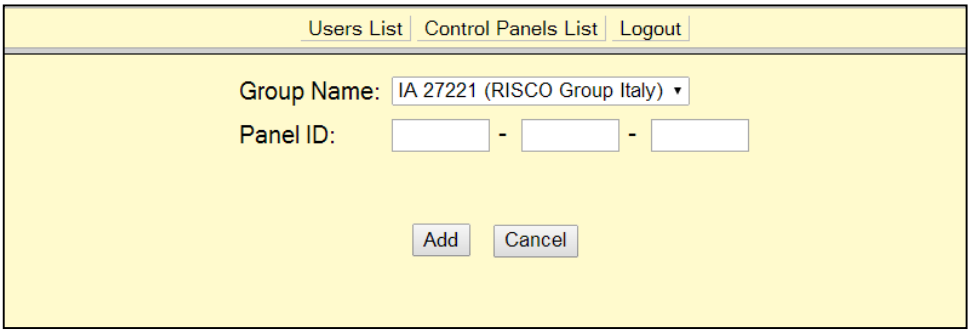

Figura 9 Pagina Aggiunta centrale esistente

1. Inserire il numero ID centrale (Panel ID) della centrale da associare al proprio gruppo e premere il tasto **ADD** (Aggiungi).

   La centrale verrà aggiunta alla lista delle centrali associate al proprio gruppo installatore.

Editare una centrale esistente

Per editare una centrale esistente:

1. Nella pagina Lista delle Centrali, fare clic sul CP Login ID del cliente che si desidera modificare; viene visualizzata la pagina **Control Panel Update**
2. Inserire i dettagli della centrale come richiesto.
3. Cliccare OK per salvare.

Cancellare una centrale

Per cancellare una centrale:

1. Nella pagina Lista delle Centrali, fare clic sul CP ID della centrale che si desidera eliminare; viene visualizzata la pagina **Control Panel Update** .
2. Cliccare su **Delete** (cancella) e poi OK; La centrale viene cancellata.

Opzioni Aggiuntive per le Centrali

Aprendo la pagina **Control Panel Update**, la colonna sulla sinistra offre una serie di opzioni di programmazione aggiuntive per la centrale selezionata.
Di seguito la descrizione di ognuna di queste opzioni.

Event Forwards – consente all'installatore di attivare o disattivare le categorie di eventi che l'utente potrà selezionare per le notifiche trasmesse via e-mail dal cloud.

Service Providers – consente all'installatore di definire i dati delle Società di Ricezione Eventi (Vigilanze) a cui vengono inoltrati gli eventi di allarme.

Network Cameras – consente all'installatore di definire ed integrare le telecamere IP con la centrale.

Web Users – permette all'installatore di aggiungere sub-utenti (subusers) Web abilitati alla gestione della centrale. In ogni caso qualsiasi accesso alla centrale viene garantito e abilitato solo digitando il codice utente della centrale stessa.

Group Membership – al momento non disponibile per l'installatore.

Devices Descriptors – al momento non disponibile per l'installatore.

User Video Events – in questa pagina l'installatore può definire i parametri per la cancellazione dei video/immagini dal Cloud e può visualizzare un log delle immagini/video cancellati dall'utente.

CP Statistics – consente all'installatore di visualizzare le statistiche riferite alla centrale selezionata (es.: inserimenti, disinserimenti, ultimo collegamento, ecc.)

Smartphone List – consente all'installatore di visualizzare l'elenco degli Smartphone registrati associati alla centrale.

Di seguito la spiegazione dettagliata delle opzioni elencate.

Event Forwards – (Inoltro degli Eventi)

La notifica degli eventi è una funzione che consente l'inoltro di eventi occorsi tramite e-mail o SMS (ad oggi gli SMS non sono supportati). L'elenco delle opzioni di inoltro eventi viene visualizzato nella pagina Notifiche Eventi situata all'interno dell'area Web Utente. Questa opzione nell'area di Amministrazione Installatore è utilizzata per abilitare o disabilitare le categorie di eventi disponibili per le notifiche. I contatti (indirizzi e-mail) per l'inoltro degli eventi, sono però definiti dal cliente nella propria area.

Per editare l'inoltro degli Eventi:

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento **Event Forwards** (Inoltro Eventi) nella colonna di sinistra; viene visualizzata la tabella inoltro eventi.

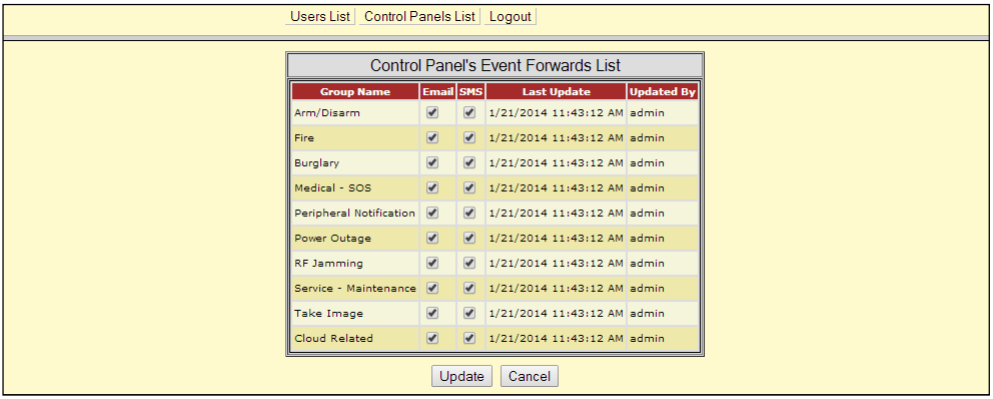

Figura 10 Tabella inoltro Eventi

3. Utilizzando le caselle di controllo che compaiono nelle colonne E-mail e SMS abilitare o disabilitare l'inoltro di eventi per ogni gruppo.
4. Cliccare Update per salvare.

Service Provider

I fornitori di servizi, Service Provider, possono essere identificati nelle Società di Ricezione Eventi (Vigilanze) alle quali il Cloud RISCO inoltra, tramite specifici protocolli, gli eventi occorsi presso gli impianti installati e controllati dai sistemi di sicurezza RISCO. Questa sezione spiega come abbinare una centrale ad una società di ricezione eventi. L'elenco dei provider disponibili per l'assegnazione di una centrale è determinato preventivamente dall'amministratore del Cloud RISCO.

Ogni centrale può essere abbinata a più società di ricezione eventi via Proxy o SIA IP. Questa funzione assicura che la società di monitoraggio con il quale il cliente finale ha sottoscritto un accordo, riceverà i messaggi relativi alla centrale del cliente. Gli Eventi saranno filtrati dal Forwarding come spiegato sopra.

Per assegnare un fornitore di servizi alla centrale

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento **Service Provider** (società di monitoraggio) nella colonna di sinistra; viene visualizzata la tabella dei Fornitori di Servizi.

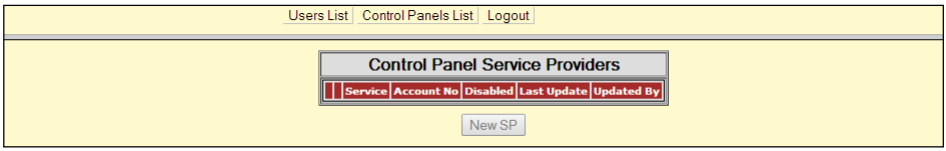

Figura 9 Tabella assegnazione Service Provider

3. Fare clic sul pulsante Nuovo SP scegliere un provider di servizi disponibile.
4. Inserire il numero di Account (Codice Impianto) nel campo di testo.

NOTA – Questo numero account verrà inviato insieme agli eventi al Service Provider, (società di ricezione eventi), indipendentemente dal numero di account inserito in centrale ed utilizzato con altri vettori di comunicazione.

5. Cliccare su Update.

Editare un Service Provider per la centrale

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Cliccare sul collegamento **Service Provider** (società di monitoraggio), la tabella dei provider disponibili viene visualizzata.
3. Cliccare sul Service Provider abbinato alla centrale.
4. Inserire i dettagli come richiesto.

NOTE – Se si desidera disattivare il fornitore del servizio senza eliminarlo dal registro del pannello di controllo, selezionare la casella di controllo Disabled (Disattivato)

5. Cliccare su Update.

Cancellare un Service Provider

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento **Service Provider** (società di monitoraggio) nella colonna di sinistra; viene visualizzata la tabella Fornitori di Servizi.
3. Fai clic sul link Delete (Elimina) accanto al Service Provider della centrale; il Service Provider viene eliminato.

NOTA – Questa procedura elimina solo il Service Provider in abbinamento alla centrale e non lo elimina dal DataBase del RISCO Cloud.

Network Cameras

L'area di Amministratore Installatore di RISCO Cloud fornisce un'interfaccia utilizzabile da remoto tramite il web che consente di aggiungere telecamere IP associate alla centrale di allarme, definirne le impostazioni e configurare gli eventi di allarme per l'attivazione.

IMPORTANTE – Per accedere alle telecamere IP e definirne le impostazioni una centrale intrusione deve essere stata precedentemente programmata e connessa al Cloud RISCO. Per maggiori informazioni consultare il manuale della centrale.

Definizione dei parametri della telecamera IP

Dopo aver collegato la telecamera IP alla rete (vedi, Collegamento della telecamera IP alla rete) è possibile definirne i parametri.

Per definire le impostazioni della telecamera IP:

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento Network Cameras (Telecamere IP) nella colonna di sinistra; viene visualizzato l'elenco delle telecamere IP (l'elenco sarà vuoto se non sono state definite telecamere IP) .

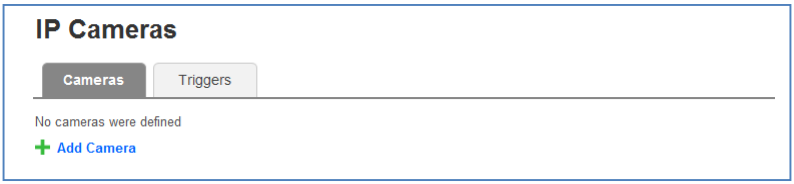

Figura 12 Lista Telecamere IP

3. Cliccare su a **Add Camera**, viene visualizzata la finestra "**Add Camera**.

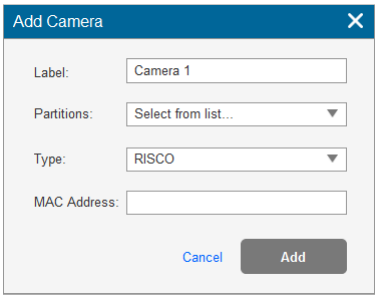

Figura 13 Aggiungi Telecamera

4. Definire i seguenti campi nella finestra "**Add Camera**".

Campo	Descrizione	Tipo Telecamera
Label	Nome della Telecamera	RISCO, ONVIF & Generic IP cameras
Partitions	Selezionare la partizione/i dalla lista di quelle disponibili	RISCO, ONVIF & Generic IP cameras
Type	Scegliere il tipo di telecamera RISCO (per ONVIF o impostazioni telecamera generici, fare riferimento al manuale Cloud Application Installer))	RISCO, ONVIF & Generic IP cameras

Campi aggiuntivi vengono visualizzati nella finestra di dialogo Aggiungi telecamera a seconda del tipo di telecamera che si è selezionata (vedi esempi qui sotto per ONVIF e telecamere IP generico).

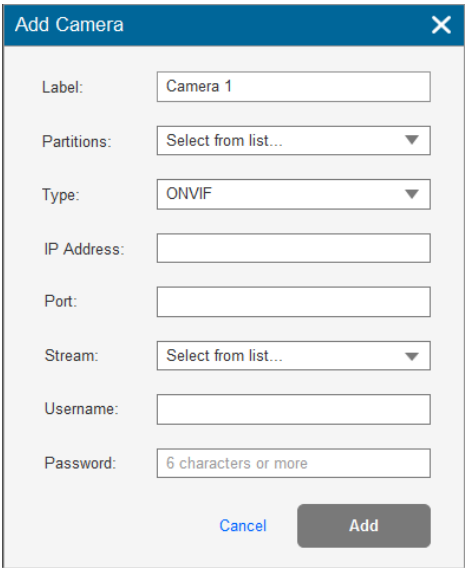

Figura 10 Nuova Telecamera ONVIF

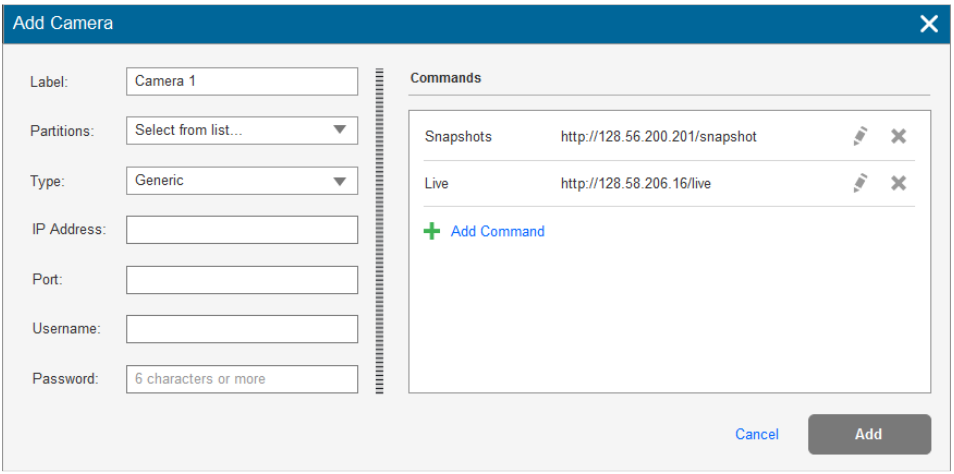

Figura 11 Nuova telecamera Generica IP

5. Definire i seguenti campi nella finestra Aggiungi telecamera a seconda del tipo di telecamera selezionata.

Campo	Descrizione	Tipo Telecamera
MAC Address	Inserire l'indirizzo MAC, così come riportato sulla scatola o sul coperchio posteriore della telecamera IP. L'indirizzo MAC (Media Access Control Address) è il codice che identifica univocamente la telecamera sulla rete. Nota: Il codice MAC va digitato esattamente come riportato sull'imballo o sulla telecamera (Maiuscole e Minuscole divisi dai 2 punti).	Solo telecamera RISCO IP
IP Address	Inserire l'IP (Internet Protocol address) della Access Point (switch/Router) a cui è collegata la telecamera. Questa è un indirizzo assegnato da ciascun Access Point per la comunicazione sulla rete.	Solo telecamera ONVIF & IP Generica
Port	Inserire il numero di porta utilizzato dalla telecamera.	Solo telecamera ONVIF & IP Generica
User Name and Password	Se utilizzate dalla telecamera per la connessione inserire User Name e Password	Solo telecamera ONVIF & IP Generica

6. Fare clic su "**Add**" se la telecamera è riconosciuta appare il seguente messaggio (La parte inerente al WIFI è valida solo per le telecamere RISCO).

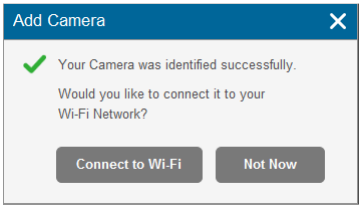

Figura 12 La telecamera è stata identificata correttamente

NOTA – Questo messaggio è rilevante solo per le telecamere IP che sono fisicamente connesse alla rete LAN tramite l'Access Point (switch/Router).

Notare che le telecamere con l'opzione WiFi vanno sempre comunque collegate al Cloud via cavo e solo successivamente abilitate in WiFi.

7. Selezionare una delle seguenti opzioni:

   Connect to Wi-Fi – per stabilire una connessione di rete wireless (passare al punto 9 per collegare la telecamera IP alla rete wireless).

   Not Now – per stabilire una connessione di rete LAN (saltare i passaggi 8, 9 e 10 - connessione di rete wireless - e collegare la telecamera IP alla rete LAN).

8. Se si è selezionata l'opzione "Connessione a Internet Wi-Fi", viene visualizzato un elenco delle reti wireless disponibili.

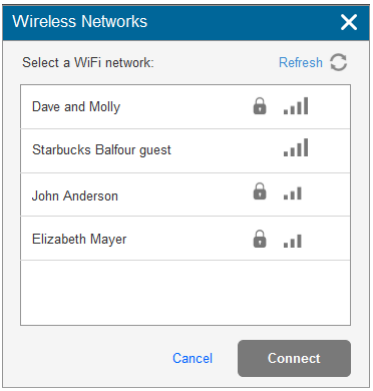

Figura 13 Lista delle reti WIFI disponibili

9. Selezionare una rete wireless dall'elenco e fare clic su Connect (Connetti).

NOTA – Se la rete è protetta da password, la password deve essere immessa nella apposita finestra.

10. Fare clic su OK per stabilire la connessione wireless (Consultare Connessione a una rete wireless utilizzando il RISCO Cloud).

IMPORTANTE – Una volta che è stata stabilita la connessione wireless, non dimenticare di scollegare la telecamera IP dall'Access Point (Switch/Router).

11. Una volta che la telecamera è pronta per l'uso verrà visualizzato un messaggio, fare clic su OK. La telecamera IP viene visualizzata nella pagina Telecamere.

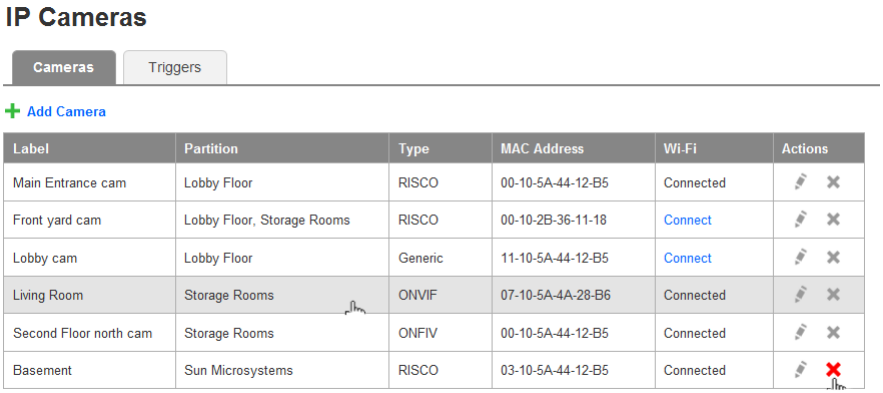

Figura 14 Lista Telecamere IP

NOTA – Esiste la possibilità di editare o cancellare la telecamera IP selezionata

Definizione dei parametri di attivazione della telecamera IP

Qualsiasi evento del seguente elenco può essere utilizzato per attivare una telecamera

Eventi di Partizione			
Allarme Incendio	Allarme Panico	Allarme Medico	Allarme Intrusione
Inserimento Totale	Inserimento Parziale	Disinserimento	Coercizione
Tamper	Allarme 24 HR	Allarme Allagamento	Allarme Gas
Allarme Ambientale	Allarme inattività	Bassa Temperatura	Allarme Uscita
Eventi di Zona			
Allarme	Zona Esclusa	Zona Re-inclusa	Tamper

Per definire i parametri di attivazione:

1. Dalla pagina di Controllo Centrale/Telecamere, fare clic sulla scheda **Trigger**.

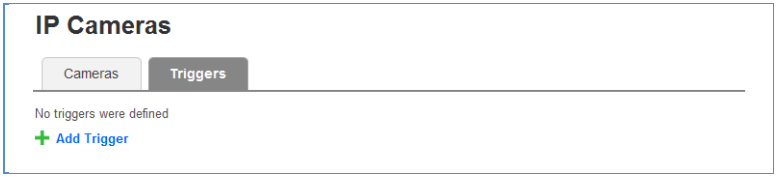

Figura 15 Lista Attivazioni Telecamere

2. Fare clic su **Add trigger (Aggiungi Comando)**; la finestra **Add Trigger** viene visualizzata.

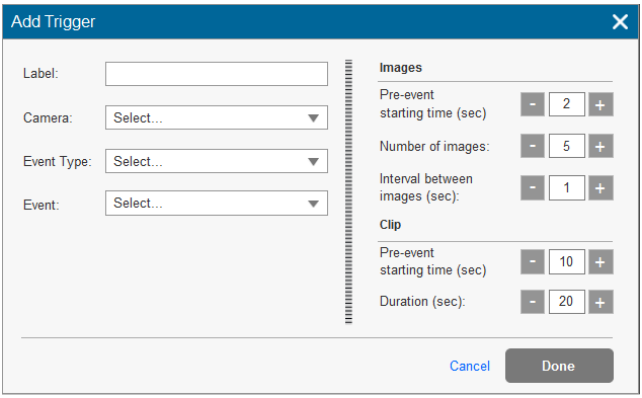

Figura 20 Aggiungi Comando

3. Definire i seguenti campi nella finestra **Add Trigger**.

Campo	Descrizione	Tipo Evento
Label	Descrizione associata al comando	Eventi per partizione/sensori
Camera	Scegliere la Telecamera dalla lista	Eventi per partizione/sensori
Event Type	Scegliere la tipologia di evento dalla lista	Eventi per partizione/sensori

Campi aggiuntivi possono essere visualizzati nella finestra di dialogo **Add trigger** in base al tipo di evento che si è selezionato (vedi esempi seguenti).

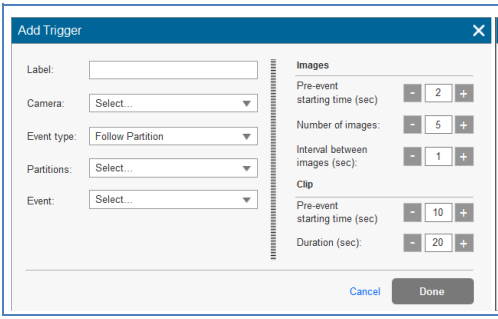

Figura 21 Aggiungi Attivazione per Partizione

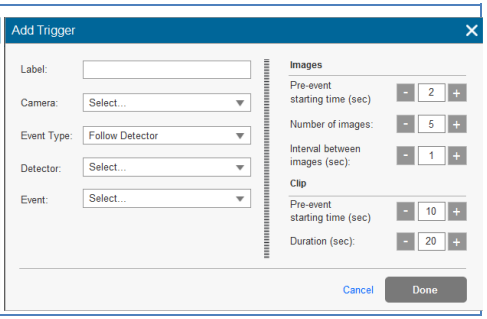

Figura 22 Aggiungi Attivazione per sensore

4. Definire i seguenti campi nella finestra di dialogo **Add trigger** in base al tipo di evento che si è selezionato.

Campo	Descrizione	Tipo Evento
Partitions	Selezionare la partizione(i) dalla lista. **NOTA** – Vengono visualizzate solo le partizioni programmate per la centrale di allarme.	Solo Eventi di Partizione
Detector	Selezionare dalla lista la zona desiderata	Solo Eventi di Zona
Event	Selezionare dalla lista l'evento desiderato	Eventi di Partizione/Zone

5. Definire le seguenti impostazioni per Images (Foto)/clip (video):

Campo	Descrizione
Images	**Pre-event starting time (sec)** – tempo antecedente l'evento dal quale far partire la sequenza di immagini (pre-allarme). **Number of images** – numero di immagini da trasmettere. **Interval between images (sec)** – intervallo tra le immagini.
Clip	**Pre-event starting time (sec)** – tempo antecedente l'evento dal quale far partire la clip video. **Duration (sec)** – Durata complessiva della clip video **Nota:** Questi campi sono attualmente bloccati ed i parametri di default non possono essere modificati

6. Una volta terminato, fare clic su **Done** (Fatto). Il comando della telecamera definita viene visualizzato nella pagina **Camera Triggers List** (Lista Comandi telecamera).

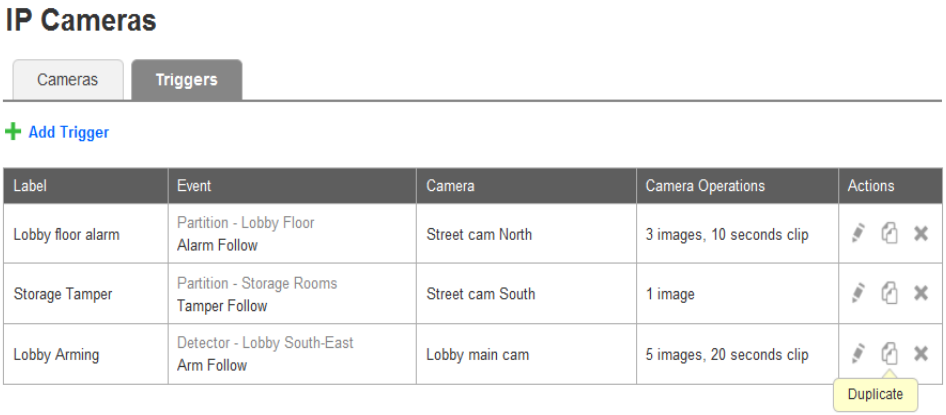

Figura 16 Elenco Comandi Telecamera

NOTA – Esiste la possibilità di editare , duplicare , o cancellare l'attivazione per la telecamera selezionata.

IMPORTANTE – Non possono essere definite due attivazioni uguali per la stessa telecamera. In questo caso almeno una delle due attivazioni o entrambi devono essere modificate.

WEB User (Utente finale)

Nella pagina Web Users, l'installatore amministratore RISCO Cloud può creare ulteriori utenti Web. Questi utenti aggiuntivi possono anche essere creati dall'utente Master registrato nella pagina Web di gestione utente della centrale.

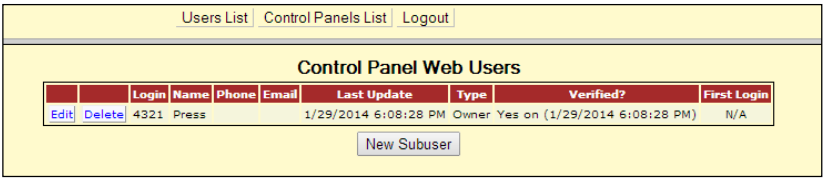

Figura 17 Nuovo Utente WEB

Per Creare un nuovo Utente che interagisce con la centrale:

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul link **User** (Utenti) nella colonna di sinistra, viene visualizzata la pagina Utenti Web.
3. Cliccare su **New Sub User** (Nuovo Sub Utente)

   Viene visualizzata la pagina degli utenti WEB come sotto riportato.

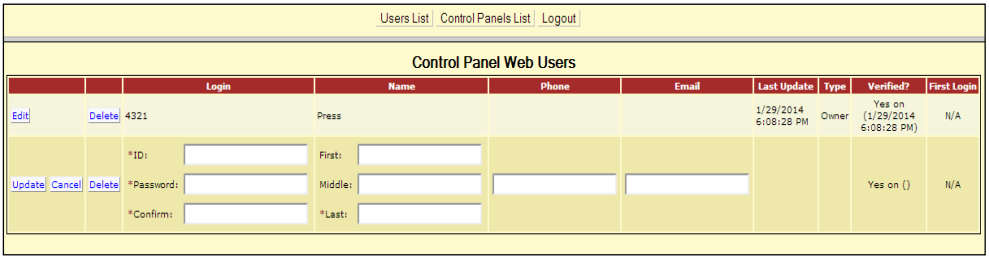

Figura 18 Creazione di un nuovo Utente WEB

Campo	Descrizione
Login ID	Nome di login del cliente che va inserito per l'applicazione WEB.
Login Password **Login Confirm**	La password del cliente che deve essere immessa quando accede all'applicazione Web. La lunghezza massima della password è 16 caratteri. La password deve iniziare con una lettera. (applicabile solo quando l'opzione di auto-registrazione è disabilitata). Campo di conferma Password (applicabile solo quando l'opzione di auto-registrazione è disabilitata).
First/Middle/ Last Name	I dati personali del Cliente.

Campo	Descrizione
Cell Phone/E-mail	Informazioni aggiuntive del Cliente. (applicabile solo quando l'opzione di auto-registrazione è disabilitata)
Last Update	L'ultima volta che i dati del Cliente sono stati modificati.

Group Membership

Questa opzione non è al momento disponibile per gli installatori.

Device Descriptors

Questa opzione non è al momento disponibile per gli installatori.

User Video Events

Nella pagina **User Video Events** (Eventi Video Utente) l'utente può definire i parametri per gli eventi video e visualizzare un registro dei video rimossi.

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul link **User Video Event** (Eventi Video Utente) nella colonna di sinistra, viene visualizzata la pagina User Video Events parameters.

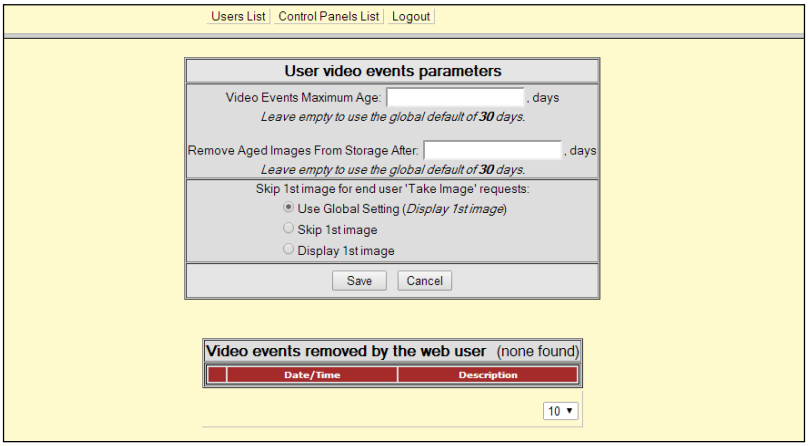

Figura 19 Pagina Eventi Video Utente

3. Definire i parametri richiesti.
4. Cliccare su **Save** (Salva) per salvare i cambiamenti.

Gli eventi video rimossi dal sistema da parte dell'utente web vengono visualizzati nella lista direttamente sotto i parametri. Su richiesta da parte dell'utente, l'opzione Ripristina consente all'amministratore di ripristinare eventuali eventi video cancellati dalla memoria.

CP Statistics

La pagina statistiche CP permette all'installatore di visualizzare informazioni statistiche generali sulla centrale selezionata.

Per visualizzare le statistiche:

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento **CP Statistic** (Statistiche Centrale) nella colonna di sinistra; viene visualizzata la pagina CP statistic.

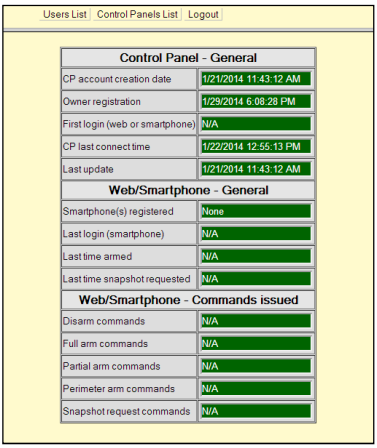

Figura 20 Statistiche centrale

Campo	Descrizione
CP account creation date	Quando la centrale è stata create.
Owner registration	La prima volta che il cliente ha registrato la propria centrale sul RISCO Cloud
First login (Web or Smartphone)	La prima volta che il cliente ha fatto un login al RISCO Cloud attraverso smartphone o web.
CP last connect time	L'ultima volta che la centrale si è connessa al RISCO Cloud
Last update	L'ultima volta che le informazioni del cliente sono state aggiornate.
Smartphone(s) registered	Il numero di smartphone registrati per la centrale selezionata.
Last login (Smartphone)	L'ultima volta che l'applicazione WEB o Smartphone è stata usata per effettuare il login al RISCO Cloud

Campo	Descrizione
Last time armed	L'ultima volta che il cliente usando l'applicazione attraverso WEB o Smartphone ha inserito il Sistema.
Last time snapshot requested	L'ultima volta che il cliente usando l'applicazione attraverso WEB o Smartphone ha fatto la richiesta di uno scatto (foto)
Disarm commands	L'ultima volta che il cliente usando l'applicazione attraverso WEB o Smrtphone ha disinserito il Sistema.
Full arm commands	Il numero di volte che utilizzando il WEB o l'applicazione smartphone il sistema è stato inserito in modo totale.
Partial arm commands	Il numero di volte che utilizzando il WEB o l'applicazione smartphone il Sistema è stato inserito in modo parziale.
Perimeter arm commands	Il numero di volte che utilizzando il WEB o l'applicazione smartphone il Sistema è stato inserito in modo perimetrale (non utilizzato con i sistemi risco).
Snapshot request commands	Il numero di volte che utilizzando il WEB o l'applicazione smartphone il cliente ha fatto la richiesta di uno scatto (foto)

Smartphone List

La pagina di Smartphone List consente all'utente di visualizzare l'elenco degli Smartphone registrati associati alla centrale.

Per visualizzare la lista degli smartphone:

1. Dalla schermata control panel list cliccare sulla centrale da modificare.
2. Fare clic sul collegamento **Smartphone List** (Lista Smartphone) nella colonna di sinistra per visualizzare la lista degli Smartphone.

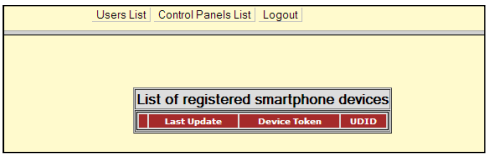

Figura 21 Lista Smartphone registrati

L'opzione Unregister (Cancella Registrazione) consente all'amministratore Installatore di annullare la registrazione di qualsiasi utente Smartphone dal sistema.

Appendix A: Tabella Eventi SIA e CONTACT ID

La seguente tabella illustra gli eventi che sono inclusi nella tabella degli eventi, sia per il protocollo SIA che per il Contact ID. Per ogni provider di servizi definito (centro di ricezione eventi), qualsiasi evento che appare nella tabella può essere attivato o disattivato (un evento abilitato è trasmesso al centro di ricezione quando lo stesso viene ricevuto da RISCO Cloud).

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
0	Fire Alarm	FA	1 110	Fire	Device Number
1	Panic Alarm	PA	1 120	Burglary	Device Number
2	Emergency Alarm	MA	1 150	Emergency	Device Number
3	Alarm	BA	1 130	Burglary	Device Number
4	Fire Restore	FR	3 110	Fire	Device Number
5	Panic Restore	PR	3 120	Burglary	Device Number
6	Medical Restore	MR	3 150	Medical - SOS	Device Number
7	Alarm Restore	BR	3 130	Burglary	Device Number
8	Trouble	BT	1 380	Peripherals	Device Number
9	Zone Bypassed	UB	1 570	Burglary	Device Number
10	Zone Unbypassed	UU	3 570	Burglary	Device Number
11	Zone Tamper	TA	1 137	Burglary	Device Number
12	Tamper Restore	TR	3 137	Burglary	Device Number
13	Full Arm	CL	3 401	Arm/Disarm	User Number
14	Part Arm	CG	3 456	Arm/Disarm	User Number
15	Perimeter Arm	CG	3 441	Arm/Disarm	User Number
16	Disarmed	OP	1 401	Arm/Disarm	User Number
17	Medical Alarm	MA	1 100	Medical - SOS	Device Number
18	Panic Alarm	PA	1 120	Burglary	Device Number
19	Fire Alarm	FA	1 110	Fire	Device Number
20	Edit User Code	JV	1 462	Service – Maintenance	User Number
21	Delete User Code	JX	3 462	Service – Maintenance	User Number
22	Duress	HA	1 121	Burglary	N.A.
23	Bell Cancel	BC	1 521	Burglary	User Number

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
24	Battery Low	YT	1 302	Power Outage	Device Number
25	Battery Restore	YR	3 302	Power Outage	Device Number
26	Battery Low	XT	1 384	Power Outage	Device Number
27	Battery Restore	XR	3 384	Power Outage	Device Number
28	AC Loss	AT	1 301	Power Outage	Device Number
29	AC Restore	AR	3 301	Power Outage	Device Number
30	Tamper	TA	1 137	Burglary	Device Number
31	Tamper Restore	TR	3 137	Burglary	Device Number
32	Communication Trouble	YC	1 350	Peripherals Notification	Device Number
33	Communication Restore	YK	3 350	Peripherals Notification	Device Number
34	Media Loss	LT	1 351	Peripherals Notification	Device Number
35	Media Restore	LR	3 351	Peripherals Notification	Device Number
36	Device Trouble	ET	1 330	Peripherals Notification	Device Number
37	Device Trouble Restore	ER	3 330	Peripherals Notification	Device Number
38	FM Jamming	XQ	1 344	RF Jamming	Device Number
39	FM Jamming Restore	XH	3 344	RF Jamming	NA
40	Programming Start	LB	1 627	Service – Maintenance	N.A.
41	Programming End	LX	1 628	Service – Maintenance	N.A.
42	Remote Programming Start	RB	1 412	Service – Maintenance	N.A.
43	Remote Programming End	RS	3412	Service – Maintenance	N.A.
44	Periodic Test	RP	1 602	Always Report	N.A.
45	Walk Test	TS	1 607	Service – Maintenance	User Number
46	End Walk Test	TE	3 607	Service – Maintenance	NA

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
47	Set Time	JT	1 625	Service – Maintenance	User Number
48	Set Date	JD	1 625	Service – Maintenance	User Number
49	Out of synchronization	UT	1 341	Do Not Report	Device Number
50	Resynchronization	UR	3 341	Do Not Report	Device Number
51	CP out of synchronization	UT	1 341	Peripherals Notification	Device Number
52	CP resynchronization	UR	3 341	Peripherals Notification	Device Number
53	Supervision Loss	US	1 381	Peripherals Notification	Device Number
54	Supervision Restore	UR	3 381	Peripherals Notification	Device Number
56	Clear Log	LB	1 621	Service – Maintenance	User Number
57	Stop Communication	OC	1 350	Do Not Report	User Number
58	Listen In Start	LF	1 606	Service – Maintenance	N.A.
59	Listen In End	LE	3 606	Service – Maintenance	N.A.
60	WDT Reset	RR	1 305	Service – Maintenance	Task
61	Power Up Reset	RR	3 301	Power Outage	Device Number
62	Net Disconnect	RA	1 350	Service – Maintenance	Device Number
63	Init Start	YD	1 551	Service – Maintenance	Device Number
64	Init End	YE	3 551	Service – Maintenance	Device Number
65	Message Queue Full	JO	1 624	Service – Maintenance	Device Number
66	Message Queue Restore	JL	3 621	Service – Maintenance	Device Number

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
67	Message Queue Disc.	YO	1 102	Service – Maintenance	Device Number
68	24 HR-X Alarm	TT	1 370	Burglary	Device Number
69	24 HR-X Restore	TR	3 370	Burglary	Device Number
70	Open After Alarm	OR	1 458	Burglary	User Number
71	GSM Signal Level	YY	1 605	Peripherals Notification	Signal Level (0-9)
72	No Arm Period Expire	CD	1 654	Service – Maintenance	N.A.
73	Trouble Restore	BJ	3 380	Peripherals Notification	Device Number
74	Water Alarm	WA	1 154	Burglary	Device Number
75	Water Restore	WH	3 154	Burglary	Device Number
76	Gas Alarm	GA	1 151	Fire	Device Number
77	Gas Restore	GH	3 151	Fire	Device Number
78	Environmental Alarm	UA	1 150	Burglary	Device Number
79	Environmental Restore	UH	3 150	Burglary	User Number
80	No Motion Alarm	NA	1 102	Medical - SOS	Device Number
81	Manual Test	RX	3 601	Burglary	User Number
82	Recent Closing	CR	1 459	Burglary	User Number
83	Exit Alarm	EA	1 454	Burglary	User Number
84	Exit Error	EE	1 457	Burglary	User Number
85	Alarm Canceled	OC	1 406	Burglary	User Number
86	Report Aborted	YO	1 466	Do Not Report	User Number
87	Swinger Trouble	BD	1 377	Service – Maintenance	Device Number
88	Cross Zoning Verification	BG	1 378	Service – Maintenance	Device Number
89	Daylight Change	YO	0 000	Do Not Report	NA
90	RF Comm Trouble	XQ	1 353	Service – Maintenance	Device Number
91	RF Comm Restore	XH	3 353	Service – Maintenance	Device Number

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
92	System Bell Fault	YA	1 321	Service – Maintenance	Device Number
93	System Bell Restore	YH	3 321	Service – Maintenance	Device Number
94	Web User Access Start	RB	1 412	Service – Maintenance	User Number
95	Web User Access End	RS	3 412	Service – Maintenance	User Number
96	No XML Proxy Connection	NC	1 350	Do Not Report	NA
97	No XML Proxy Connection Restore	NR	3 350	Do Not Report	NA
98	System Radio Jamming	XQ	1 344	RF Jamming	Device Number
99	External Battery Low	YT	1 302	Service – Maintenance	Device Number
100	External Battery Restore	YR	3 302	Service – Maintenance	Device Number
101	DHCP Fail	LT	1 351	Peripherals Notification	NA
102	DHCP Restore	LR	3 351	Peripherals Notification	NA
103	High Temperature	KA	1 158	Burglary	Device Number
104	High Temperature Restore	KH	3 158	Burglary	Device Number
105	Low Temperature	ZA	1 159	Burglary	Device Number
106	Low Temperature Restore	ZH	3 159	Burglary	Device Number
107	Partition 1 Armed	CG	3 400	Arm/Disarm	User Number, Address Number
108	Partition 2 Armed	OG	3 400	Arm/Disarm	User Number, Address Number
109	Partition 1 Disarmed	CG	1 400	Arm/Disarm	User Number, Address Number

ID	Event Name	SIA	Cont. ID	Event Group	Address Field
110	Partition 2 Disarmed	OG	1 400	Arm/Disarm	User Number, Address Number
111	Local Snapshot	XX	1 400	Do Not Report	User Number, Address Number
112	SMS Snapshot	XX	1 400	Do Not Report	User Number, Address Number
113	WEB Snapshot	XX	1 400	Do Not Report	User Number, Address Number
114	RP User Snapshot	XX	1 400	Do Not Report	User Number, Address Number
115	Sensor Snapshot	TW	1 139	Burglary	Device Number
116	RF Device WDT Reset	RR	1 305	Do Not Report	User Number, Address Number
117	Crash and Smash	UZ	1 777	Burglary	Device Number

Garanzia Limitata RISCO Group

RISCO Ltd. ,its subsidiaries and affiliates (the "Seller") warrants its products to be free from defects in materials and workmanship under normal use for 24 months from the date of production. Because the Seller does not install or connect the product, and because the product may be used in conjunction with products not manufactured by the Seller, the Seller cannot guarantee the performance of the security system which uses this product. The Seller's obligation and liability under this warranty is expressly limited to repairing and replacing, at the Seller's discretion, within a reasonable time after the date of delivery, any product not meeting these specifications. The Seller makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. Under no circumstances should the Seller be liable for any consequential or incidental damages for breach of this or any other warranty, expressed or implied, or upon any other basis of liability whatsoever. The Seller's obligation under this warranty shall not include any transportation charges or costs of installation or any liability for direct, indirect, or consequential damages or delay. The Seller does not warrant that the product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection. The buyer/customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an insurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof. Consequently the Seller shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning. However, if the Seller is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regardless of cause or origin, the Seller's maximum liability shall not exceed the purchase price of the product, which shall be a complete and exclusive remedy for the Seller. No employee or representative of the Seller is authorized to change this warranty in any way or grant any other warranty. Batteries installed in or used with the products are explicitly excluded from this or any other warranty. Seller gives no warranty whatsoever as to batteries and buyer's only remedy (if any) shall be in accordance with the warranty provided (if and to the extent provided) by the manufacturers of batteries.

WARNING: This product should be tested at least once a week.

CAUTION: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to local regulations.

Contattare RISCO Group

RISCO Group è impegnata sul fronte dell'assistenza alla clientela e al prodotto. Per contattarci visitare il nostro sito (www.riscogroup.it) o utilizzare i seguenti recapiti telefonici o email:

United Kingdom
Tel: +44-(0)-161-655-5500
support-uk@riscogroup.com

Belgium (Benelux)
Tel: +32-2522-7622
support-be@riscogroup.com

China (Shenzhen)
Tel: +86-755-82789285
support-cn@riscogroup.com

Italy
Tel: +39-02-66590054
support-it@riscogroup.com

USA
Tel: +1-631-719-4400
support-usa@riscogroup.com

Poland
Tel: +48-22-500-28-40
support-pl@riscogroup.com

Spain
Tel: +34-91-490-2133
support-es@riscogroup.com

Brazil
Tel: +55-11-3661-8767
support-br@riscogroup.com

Israel
Tel: +972-3-963-7777
support@riscogroup.com

France
Tel: +33-164-73-28-50
support-fr@riscogroup.com

China (Shanghai)
Tel: +86-21-52-39-0066
support-cn@riscogroup.com

Australia
Tel: +1800-991-542
support-au@riscogroup.com

5IN2188-IT