

## AGGIORNAMENTO CENTRALE SECURLAN FEBBRAIO 2019

### SECURLINK PRO CLOUD VERSIONE 6.4.0 e PLUGIN VERSIONE 5.0

- 1) Rivisitazione grafica del software Securlink Pro Cloud (versione 6.4.0 ) ma mantenimento della risoluzione Video a 1024x768 pixel per compatibilità dell'adattamento dei contenuti con ambiente web ( <http://cloudfree.securlan.it> ).
- 2) Rilascio della versione WEB pubblica e gratuita del software Securlink Pro Cloud all'indirizzo <http://cloudfree.securlan.it>. La versione pubblica ha limitazione a tempo di utilizzo di max 20 minuti e non salva nessuna dato sul server web. Al termine della programmazione via WEB della vostra centrale, i dati dell'impianto modificato possono essere inviati ad una Vostra email e in seguito importato come nuovo Impianto nel nuovo Securlink Pro Cloud 6.4.0.
- 3) Dopo l'installazione Securlink richiede la registrazione dei dati dell'utente Amministratore. L'utente che accede al nuovo Securlink ora deve avere sia Username che Password. Di default la Username del primo utente è Amministratore e la Password è a Vostra discrezione programmabile al primo avvio del programma, prima di entrare in programmazione. L'amministratore può creare altri Utenti (max 16) ognuno dei quali può avere opzioni di controllo sui parametri del software e associazione profilo di centrale a totale discrezione dell'amministratore. Ogni Nuovo Utente avrà la sua Username e la sua Password di login al programma.
- 4) Securlink Pro Cloud (sia su PC che su Web) è ora utilizzabile con connessione :
  - 1) Cloud (senza aperture porte nel router lato centrale),
  - 2) DDNS CLOUD utilizzando il servizio Cloud di Cwebforce per raggiungere la centrale (necessario apertura porta di programmazione nel router lato centrale).
  - 3) TCP/IP (indirizzo statico) e DDNS su servizi ddns di terze parti.
- 5) Modificata la procedura di creazione tabelle SMS, C.ID ed EMAIL. Ogni sezione ha ora la sua tabella di configurazione ed associazione all'evento totalmente indipendente. SMS ed EMAIL sono adesso (come per il C.ID) associabili al singolo evento di centrale (es. Zona 1 Allarme) ed è possibile salvare e richiamare infinite tabelle pre-programmate per ogni tipologia di gruppo SMS, EMAIL e C.ID. Le tabelle sono richiamabili dalla pagina principale di Securlink o dall'interno delle relative sezioni di utilizzo.
- 6) In pannello Programmazione sono stati modificati i Gruppi di accesso ai dati di programmazione. Sono stati divisi in 6 sezioni, ognuna con un suo tasto di accesso :
  - CENTRALE : Attivatori, Moduli, Ingressi/Uscite, Sistema
  - TCP/GSM : Network, GSM/GPRS, Descrizioni Estese, E-Mail, Utenti Web, C.ID/SIA-IP, Trigger, Video Verifica , Tools e Monitoraggio
  - CWEB : Configurazione e controllo Cloud Cwebforce
  - AUDIO : Text To Speech per Messaggi di Evento, Aree, Zone, Uscite ed anche Guida Vocale
  - CHIAMATE : Comunicazione, Numeri di telefono, Messaggi di canale, C.ID e tabelle SMS e C.ID
  - EVENTI : Lettura Memoria Eventi di centrale con supplemento FILTRO DI RICERCA per dettaglio ricerca evento ( tipo di evento, data; ora ).In Memoria Eventi è ora possibile avere descrizione dettagliate degli elementi programmati in centrale ed in particolare è ora mostrata la descrizione del Nome assegnato al Tag (prima era mostrato solo l'utente assegnato al tag).

- 7) Spostato tasto MONITOR IMPIANTO dalla lista tendina menu Impianto alla posizione fissa a sinistra, sotto pannello elementi da programmare.  
Molto più semplice e veloce ora aprire il Monitoraggio della centrale.
- 8) Sono stati rimossi dal pannello principale i tasti COPIA DATI ELEMENTO, COPIA DATI BLOCCO e COPIA DATI TOTALE che consentivano, dopo una lettura dalla centrale, di fissare sul profilo a video i dati letti. Ora a default i tasti COPIA sono disabilitati e, dopo una lettura di centrale, gli elementi letti vengono automaticamente applicati al profilo aperto (non è necessario confermare la Copia).  
Se si desidera tornare alla modalità dei tasti COPIA manuale è disponibile una opzione, in pannello UTILITY, definita COPIA AUTOMATICA DATI DI CENTRALE che deve essere disattivata.  
La funzione attiva nasconde automaticamente i tasti COPIA.
- 9) In UTILITY vengono ora rese visibili le impostazioni di comunicazione relative al tipo di Comunicazione selezionata ( vedi punto 10 ) ed è stata aggiunta la selezione COPIA AUTOMATICA DATI DI CENTRALE (vedi punto 8) e la selezione ABILITA TAB GUIDA VOCALE IN PANNELLO AUDIO.  
Questa ultima selezione determina, se spuntata, la presenza del Tab Guida Vocale in Pannello Audio (text to speech) e consente la totale riprogrammazione dei messaggi della Guida Vocale interattiva. Questo allo scopo di consentirvi di adattare la voce della Guida Vocale interattiva alle diverse Lingue (non Italiano) o a diversi modi di intendere il comando DTMF della Guida Vocale per come la stessa è concepita di fabbrica.
- 10) In COMUNICAZIONE sono state aggiunte le modalità di connessione alla centrale CLOUD e DDNS CLOUD. Dopo avere selezionato la modalità di Comunicazione desiderata, entrando in Utility viene mostrata solo la programmazione inerente la modalità definita (scelta interattiva).
- 11) Le modalità CLOUD e DDNS CLOUD funzionano solo se la centrale è stata connessa al Cloud Cwebforce, se si è in possesso del Codice Impianto Cweb e si hanno le credenziali Tecnico al Cloud (Username e Password del Tecnico). A tale scopo è prevista la procedura che l'utente Privato, registrato sul portale [www.securlan.it](http://www.securlan.it), ha a disposizione per invitarvi ad essere il Tecnico del suo impianto di allarme Securlan e fornirvi le credenziali di accesso.  
La modalità CLOUD non necessita di aperture porte nel router. La modalità DDNS CLOUD utilizza il Cloud Cwebforce per risolvere l'indirizzo pubblico ma necessita di apertura porta sul router.  
Le modalità TCP/IP e DDNS rimangono funzionanti come nella precedente versione di Securlink.  
E' stata mantenuta anche la compatibilità con il precedente modulo plugin TCP/IP DIGI.  
Il tipo di comunicazione selezionato verrà mostrato all'interno del tasto di connessione.
- 12) E' stata aggiunta la configurazione del modulo plugin WI-FI dal Securlink. Il plugin WI-FI è totalmente programmabile da pagina web. Tramite la programmazione da Securlink sarà possibile impostare il plugin WI-FI senza aprire la sezione Web da browser.  
La funzionalità dipende dal tipo di firmware a bordo del plugin WI-FI (da versione firmware 3.0).
- 13) Sulla parte basse a sinistra del cruscotto dei comandi appaiono ora solo i tasti INVIA ELEMENTO, INVIA e LEGGI ELEMENTO, LEGGI.  
INVIA ELEMENTO e LEGGI ELEMENTO agiscono in modo diretto sull'elemento selezionato relativo alla sezione aperta. INVIA e LEGGI aprono invece un popup da cui è possibile Leggere od Inviare solo la sezione aperta, TUTTO o le sezioni a scelta spuntando i singoli checkbox dentro il popup.
- 14) In Pannello TCP/IP sezione PORTE è stata introdotta una porta dedicata in modo esclusivo alla connessione criptata con la nuova App Securlan. La porta in questione è definita di tipo CODIFICATO. Di default la porta 3 è programmata come CODIFICATA ( descritta come Porta App default ) ma anche le porte 1 e 2 possono essere ridefinite allo scopo. SOLO la porta di tipo Codificato supporta la

connessione con aa nuova App Securlan ed è dedicata al nuovo protocollo che identifica anche l'Utente Web di centrale autorizzato ai comandi (vedi punto 17).

Le porte mantengono la programmabilità per compatibilità alle App già in uso (Securkeypad) funzionanti in modalità criptaggio Tastiera/Monitor o Completo.

Rimane il vincolo di una porta di programmazione per collegamento con software Securlink (TCP/DDNS e DDNS CLOUD) che di default è la 2105.

15) In Pannello TCP/IP è stata aggiunta la sezione FIREWALL. In Firewall è possibile programmare fino a 3 indirizzi IP Autorizzati a collegarsi alla centrale ( white list ). E' inoltre possibile definire una finestra temporale (giorni e orari in cui gli indirizzi autorizzati possono essere accettati dalla centrale alla connessione). Se solo un indirizzo IP è programmato in lista il blocco viene attivata e solo l'indirizzo programmato avrà accesso alla centrale.

16) In Pannello GSM-GPRS sono stati aggiunti :

- 1) **GSM-CID** – controllo Jamming su modulo GSM con selezione dell'uscita su cui inviare l'interferenza rilevata o l'acceccamento subito. E' possibile programmare il Tempo di permanenza del disturbo prima che venga considerato Interferenza o Acceccamento.
- 2) **RISPOSTA CLI ESCLUSIVA** – se spuntata consente, alle chiamate telefoniche inviate ai numeri CLI, di evitare i 2 squilli e chiudere la chiamata per ottenere il riconoscimento del numero del chiamante. Se non spuntata ( come attualmente in uso ) le chiamate ai numeri CLI devono essere chiuse prima del terzo squillo ( al terzo risponde la Guida Vocale ) per ottenere il riconoscimento del numero chiamante e l'azione sulla uscita. Con l'opzione spuntata NON sarà possibile utilizzare un numero CLI chiamante per entrare in Guida Vocale, in quanto il comunicatore chiuderà la telefonata al primo squillo dopo il riconoscimento del numero chiamante.
- 3) **ABILITA RICEZIONE DTMF DOPO LA RISPOSTA** – se spuntata abilita la funzionalità di ricezione dei segnali di controllo dei ricevitori digitali verso il plugin SOLO dopo la risposta e la connessione. Funzione necessaria in alcuni casi dove i Ricevitori Digitali (Contact ID) hanno problemi a sincronizzare i comandi di controllo verso il dispositivo che invia loro il dato digitale in DTMF.
- 4) **SMS PER TRIGGER** – aggiunta lista di 8 numeri invio SMS da abbinare al nuovo evento Trigger
- 5) **GPRS** – aggiunto sezione impostazioni GPRS. In centrale è stata abilitata la connettività GPRS che consente di utilizzare la SIM dati per connessione della centrale alla rete Internet.

La connettività GPRS può essere utilizzata in modalità:

- **SERVER** (Sim con IP Statico) che rende la centrale raggiungibile solo a chi conosce l'indirizzo IP assegnato alla Sim dati (APP, Securlink e Monitoraggio) e consente alla centrale di inviare segnalazioni sulla rete dati (SIA IP, Protocollo proprietario ed altre info).
- **CLOUD con GPRS** in backup su rete LAN/ADSL con connettività della centrale a Cloud Cwebforce e utilizzo dei servizio P2P e DDNS CLOUD, per raggiungere la centrale da App e Securlink.
- **CLOUD con LAN/ADSL** in backup su rete GPRS con connettività della centrale a Cloud Cwebforce e utilizzo dei servizio P2P e DDNS CLOUD, per raggiungere la centrale da App e Securlink.
- Preimpostati gli APN più utilizzati e programmabilità di APN Custom
- Porta di connessione a GPRS (default 3001), tipo di criptaggio, codice di sicurezza centrale (dedicato a connessione GPRS) e selezione se utilizzare il canale GPRS per Programmazione, Monitoraggio o entrambi ( limitazione dei controlli verso la centrale su canale GPRS ).

17) E-MAIL – aggiunta tabella programmazione e-mail per singolo evento o evento multiplo verso la singola email.

18) UTENTI WEB – l'aggiornamento del plugin alla versione 5.0 comporta una TOTALE rivisitazione del modo di connessione tra APP e Centrale. Con il plugin aggiornato alla versione 5.0 (o successivi) è possibile utilizzare la nuova APP Securlan ed il Cloud [www.cwebforce.it/ev](http://www.cwebforce.it/ev) a condizione che l'utente che chiede la connessione alla centrale ( **Utente Web** ) sia stato autorizzato dalla programmazione eseguita in questa sezione. Ciò comporta un alto standard di sicurezza sulla connessione che (a parte i criptaggi previsti nel protocollo) necessita non più del solo Codice di Sicurezza di centrale (6 cifre) per validare la connessione ma anche dell'identità di chi chiede la connessione (Utente Web) con Username e Password e del quale si confrontano in line le autorizzazioni sulla centrale. A tale scopo viene utilizzata la sezione UTENTI WEB. Fino a 32 diversi Utenti Web possono essere programmati, attivati ed abbinati agli Utenti di centrale. L'Utente Web di tipo **CONDIZIONATO** segue esattamente gli attributi del Codice di centrale a cui viene abbinato. Di default (modalità utente web condizionato) se abbiniamo l'Utente Web 1 al Codice Utente di centrale 1 (Supervisore) otteniamo che la Username dell'Utente Web sarà **Codice 1** e la password **1234**. Se vario il nome descrizione dell'utente 1 di centrale e modifico la sua password, le stesse diventeranno la nuova Username e la nuova Password dell'Utente Web 1.

L'Utente Web di tipo CONDIZIONATO prende in automatico le caratteristiche e gli attributi dell'Utente di centrale a cui viene abbinato, ma è comunque possibile RIDURRE (se necessario) gli attributi dell'Utente Web rispetto all'Utente di centrale. La parte bassa del cruscotto sezione Utente Web mostra tutti gli attributi assegnabili all'Utente Web e ne consente la modifica.

Se l'Utente Web viene definito di tipo **NON CONDIZIONATO** automaticamente la sua Username, la sua Password e i suoi attributi vengono svincolati dall'Utente di centrale a cui viene abbinato.

Tutti gli attributi ed i privilegi dell'Utente Web NON CONDIZIONATO saranno disponibili per caratterizzare e definire l'autorità dei comandi dello stesso verso la centrale.

La Username e la Password dell'Utente Web di tipo NON CONDIZIONATO hanno dei vincoli di creazione per numero minimo di caratteri (8 cifre minimo per Username) e elementi della password (8 caratteri minimo tra numeri ed una maiuscola, una minuscola ed un carattere speciale).

L'Utente Web definito (username, password ed attributi) verrà poi richiesto nella creazione del profilo di connessione con l'App Securlan o all'interno del portale Web Cwebforce.

L'Utente Web NON ha niente a che vedere con l'utente Tecnico utilizzato in Securlink o nella App per connessione in modalità Tecnico. L'Utente Tecnico DEVE essere creato ed attivato dal Privato.

L'Utente Web riconosciuto alla connessione con la centrale verrà automaticamente LIMITATO alle sue autorizzazioni (Aree, Zone, Uscite e d altro) e riconosciuto in Memoria Eventi quando agisce, sia da App che da Cwebforce.

Sia nella App Securlan che in Cwebforce le credenziali dell'Utente Web possono essere, a discrezione, salvate nel profilo (ed utilizzate in automatico alla connessione) o NON salvate nel profilo ed immesse ogni volta manualmente prima di avviare la connessione. E' anche possibile salvare solo una delle 2 parti (Username e/o Password nel profilo) e richiamare in manuale solo la parte non salvata. Basterà ad esempio salvare la Username ed alla richiesta di connessione verrà richiesta solo la Password.

19) C.ID OVER IP – è il protocollo di comunicazione con ricevitori digitali di nuova generazione, tramite segnali digitali in rete dati (ADSL o GPRS). La centrale connessa alla rete dati (ADSL, GPRS o entrambi) invia ai ricevitori programmati (indirizzo IP e porta) il dato di riconoscimento dell'evento di centrale. Gli eventi inviati dal protocollo C.ID OVER IP sono gli stessi della tabella del C.ID ed i parametri della sezione Comunicatore – CENTRO SERVIZI. Fino a 3 diversi indirizzi IP possono essere programmati.

Il protocollo C.ID OVER IP può funzionare anche promiscuamente al protocollo C.ID (dtmf).

Nella spunta TIPO PROTOCOLLO è possibile selezionare SIA (protocollo ufficiale dei ricevitori digitali over IP) oppure PROPRIETARIO che abilita un protocollo di proprietario (Securlan) per comunicazione con software di ricezione allarmi da noi sviluppati.

20) TRIGGER – i Trigger sono insieme alla Video Verifica una delle più importanti novità dell'aggiornamento alla versione firmware 5.0 del plugin TCP/IP/GPRS. Fino a 48 Trigger possono essere programmati ed ogni Trigger ha assegnato una sua destinazione, un suo ritardo all'attivazione, una sua inattività per filtro alla ripetizione del trigger ed un modo di riarmo (anche una sua descrizione). La SORGENTE che scatena il Trigger è definibile in una tabella che può associare fino a 4 eventi diversi, in modalità OR o AND tra di loro. La sorgente del Trigger può avere una diversa scelta di Condizione di attivazione e può in alcune programmazioni richiamare lo stato di una Uscita o la dipendenza da una Area. Definita la sorgente che scatenerà il Trigger andrà programmata l'AZIONE che il Trigger ha come scopo. L'azione può coinvolgere solo una NOTIFICA ( email o sms ) o una Uscita o una azione di cattura Video (snapshot e/o filmato) o (solo nel caso di prodotti Dahua) cambiare lo stato di un ingresso del DVR/NVR (senza collegare fili) e/o muovere l'Uscita di un DVR/NVR.

A breve verrà introdotto anche un PROGRAMMATORE ORARIO annuale perpetuo che agirà insieme ai Trigger per azioni soggette a periodi temporali annuali, con festività, straordinario ed eccezioni.

21) VIDEO – la sezione Video lavora solo se con la centrale di allarme sono presenti anche gli elementi hardware video (dvr/nvr e/o telecamere IP). Nella versione firmware 5.0 sono stati testati i prodotti video a marchio Dahua ed Hikvision, da cui è possibile catturare snapshot (fotogrammi).

Sui DVR/NVR a marchio Dahua è anche possibile interagire via network per variare lo stato di un ingresso (causare evento allarme), muovere una Uscita sul dispositivo Video, leggere lo stato di Motion del singolo canale o lo stato Diagnostico del DVR/NVR ( maggiori dettagli a richiesta ).

Per catturare fotogrammi è **NECESSARIO INSTALLARE una SD CARD** nel Plugin TCP/IP/GPRS.

Allo scatenarsi del Trigger, il plugin si collega al dvr/nvr/telecamera IP programmata e può catturare fino a 4 fotogrammi. A seguire posiziona i fotogrammi nella SD card e li trasferisce al Cloud Cweb. Dalla APP Securlan e o dal portale Cwebforce è possibile consultare gli eventi che hanno annesso un elemento di Video Verifica. Sul portale Cwebforce gli eventi Video permangono disponibili per max 48 ore e poi vengono cancellati. E' comunque possibile scaricare gli eventi Video (fotogrammi e/o filmati) mentre sti stanno consultando, sia da portale Cweb che da App e portarli offline (su PC e/o telefono). Gli eventi video scaricati sulla App Securlan vengono in automatico salvati in cartelle interne al telefono e permangono fino alla loro cancellazione manuale (vedi istruzioni App Securlan su <http://www.evoforce.it/securlan/app-manuale/> ). Rimangono, dopo averli scaricati, visibili fino alla massima capacità delle cartelle del telefono destinate alla archiviazione di fotogrammi e/o filmati. Sia sul portale Cwebforce che nella App è presente un Player per mostrare le foto e/o i video catturati dal trigger di centrale.

**NOTA : il servizio di Video Verifica è soggetto a sottoscrizione abbonamento.**

Per ottenere fotogrammi su evento Trigger è sufficiente equipaggiare la scheda Plugin TCP/IP/GPRS con una scheda SD Card di buona qualità (supporto schede fino a 32GB). Per ottenere filmati ( fino a 10 secondi prima e 10 secondi dopo l'evento trigger ) è necessario installare la scheda VIDEO BOX.

La scheda Video Box è posizionabile in centrale o indifferentemente sulla rete Lan. Si alimenta 12Vcc ed ha a bordo una porta di rete Lan RJ45. Il software Securlink è in grado di trovare la scheda Video Box sulla rete e programmarla per ottenere, su evento Trigger, la cattura di filmato fino per max 20 secondi (10 secondi prima e max 10 secondi dopo il trigger) relativo alla scena della sorgente video catturata. La scheda Video Box può attualmente controllare fino a 8 sorgenti/flussi video

(DVR/NVR/Telecamera IP) e gestirli in attesa dell'evento trigger che determina la creazione di un filmato. Dato che la scheda Video Box ha un buffer di 30 secondi di memoria, quando il trigger determina la richiesta del filmato si possono richiamare fino a 10 secondi prima e fino a 10 secondi dopo l'evento (max 20 secondi in totale). Comunque per questione di praticità, portabilità e velocità di realizzazione del filmato, il periodo di Pre e Post allarme può anche essere programmato a 5 secondi. In sezione VIDEO di Securlink fino a 32 sorgenti Video possono essere definite per la cattura di fotogrammi. La sorgente Video 1 è ad esclusivo utilizzo della Video Box.

- 22) MONITORAGGIO – è stata aggiunta la sezione VIDEO sotto pannello Monitoraggio. Video mostra il comportamento dei canali video abilitati alla cattura di filmati e/o foto e ne monitora lo stato per un check visivo della corretta programmazione ed attività.
- 23) In Lista Impianti è stato aggiunto il controllo ESPORTAZIONE WEB. Il comando Esportazione Web avvia l'esportazione del profilo di centrale programmato e ne consente l'invio tramite email a destinatario a vostra discrezione. Il file generato dall'esportazione web può essere in seguito importato in Securlink ( V.6.4.0.) da comando Importa e ricreare la programmazione del profilo di centrale da cui è stato esportato. E' una funzione molto utile nella versione Securlink Cloud Free Web ( <http://cloudfree.securlan.it> ) dove la programmazione NON viene salvata in locale ma può solo essere esportata con questo comando.
- 24) All'indirizzo <http://cloudfree.securlan.it> è disponibile una versione TOTALMENTE web (browser internet) del software Securlink Pro Cloud a disposizione di chiunque voglia raggiungere una centrale Securlan di cui conosce le credenziali di connessione. Nessun software sul vostro PC è necessario allo scopo ma è sufficiente aprire un browser Internet (si suggerisce Chrome o Firefox e si sconsiglia Internet Explorer). La compatibilità grafica all'uso del Securlink in pagina web può scalare a Tablet e/o Smartphone con adeguate dimensioni dello schermo. Nessuna limitazione del sistema Operativo da cui esegue la connessione via browser (Windows, Mac, Linux) e nessun software installato sul vostro PC.

Le limitazioni della versione Web Free di Securlink sono :

- 1) Max 20 minuti per sessione di programmazione dalla creazione del profilo
- 2) Nessun salvataggio dei dati sul Server (introduzione manuale dei dati di connessione ogni volta) e nessun salvataggio dei dati inviati alla centrale e/o ricevuti dalla centrale (perdita della programmazione effettuata salvo l'esportazione con invio della stessa in allegato tramite email).
- 3) Limitazione di alcuni comandi NON presenti nella versione Web Free Di Securlink.

E' comunque in fase avanzata di sviluppo una versione WEB di Securlink, totalmente identica alla versione su PC, con gli stessi requisiti e sincronizzabile tra PC e WEB. E' una versione a richiesta degli utenti Tecnici registrati sul portale [www.securlan.it](http://www.securlan.it) che sarà fornita in abbonamento. Sul portale [www.securlan.it](http://www.securlan.it) verranno a breve forniti altri servizi ai Tecnici registrati per consentire il Monitoraggio, la Programmazione, la Supervisione e delle centrali registrate al Cloud ed autorizzate dall'Utente Privato al vostro controllo. A seconda del tipo di abbonamento che andrete ad acquistare, avrete a disposizione una consolle con i comandi che Vi consentiranno una totale Supervisione delle centrali di allarme Securlan a cui siete stati autorizzati. Memoria Eventi, Monitoraggio, Programmazione, Diagnostica e delega a dipendenti e/o collaboratori a cui potete destinare lo stesso controllo o una serie di controlli con limitazioni da Voi definite. Il tutto con il semplice utilizzo di una connessione Internet, un PC, un Browser ed in piena libertà.

## NUOVA APP SECURLAN

A supporto dell'aggiornamento firmware del Plugin 5.0 nasce la nuova App chiamata SECURLAN. L'App sarà disponibile su APP STORE e PLAY STORE e verrà rilasciata anche per piattaforma Windows. Per piattaforma Windows si intende installabile ed avviabile da PC in ambiente Windows 10.

La grafica delle 3 versioni è stata unificata.

L'APP è compatibile SOLO con le centrali equipaggiate con Plugin su cui è installato firmware versione 5.0 o superiore. La nuova App consente la connettività standard TCP e DDNS ed anche la nuova connettività CLOUD e DDNS CLOUD (modalità compatibili solo con centrali registrate al Cloud Cwebforce – **registrazione Gratuita**).

L'App consente anche la creazione di profili di connessione diretti al portale Cwebforce in modalità web, sostituendo la necessità di utilizzare l'attuale App Cwebforce.

In pratica, con una sola App si può definire se la connessione avviene in modalità grafica o in modalità Web. A breve sarà integrata anche la creazione del profilo centrale per SMS, andando ad integrare anche l'attuale App SecurSMS. Una sola APP e diversi modi di connessione a vostra discrezione.

L'App può controllare illimitati profili di centrale e a connessione avvenuta (Cloud, Ddns Cloud, Ddns o IP statico) prende il totale controllo della centrale leggendone automaticamente i contenuti attivi e programmati (sincronizzazione). La connessione è soggetta al riconoscimento dell'Utente Web di centrale e l'App in automatico LIMITA i comandi verso la centrale confrontando le autorizzazioni dell'Utente Web con quelle programmate in centrale.

Totale controllo sulle AREE, sulle ZONE, sulle USCITE e icone immediate per visione diretta degli stati di ALLARME, NON PRONTO e GUASTO con ricerca istantanea dell'elemento interessato dallo stato (semplice tocco dell'icona).

Possibilità di creare GRUPPI di Uscite per comandi multipli con un solo tocco.

Sono disponibili i controlli :

- 1) Tastiera Virtuale
- 2) Diagnostica
- 3) Memoria Eventi con filtro di ricerca
- 4) Video Verifica
- 5) Video Cattura
- 6) Video Live (apertura di porta RTSP lato router)
- 7) Notifiche Push con selezione della tipologia delle notifiche che si desidera ricevere
- 8) Connessione a portale Cwebforce

Sulla homepage del sito di registrazione [www.securlan.it](http://www.securlan.it) potete visionare le funzionalità della App Securlan e nel tempo altre funzioni verranno aggiunte ( Mappe Grafiche, Domotica, SMS ).

L'App Securlan è compatibile anche con Tablet ed iPad.

## PORTALE CWEBFORCE

Il portale Cwebforce è stato potenziato ed arricchito della funzionalità di Video Verifica. Con l'introduzione della versione 5.0 del firmware del Plugin, NON sarà più possibile utilizzare, in modo gratuito, i contenuti grafici di controllo di centrale che il portale mette a disposizione in modalità totalmente Web (responsive). La registrazione della centrale Securlan (firmware plugin 5.0 o superiori) al Cloud Cwebforce consentirà, **a titolo gratuito**, la connettività della App Securlan in modalità Cloud (no apertura porte nel router) e DDNS CLOUD (servizio ddns tramite Cloud con apertura porta nel router). I servizi di controllo grafico da pagina Web di Aree, Zone, Uscite, Memoria Eventi, Diagnostica e Setup avanzato, saranno dal 1 di Febbraio 2109 disponibili SOLO con abbonamento. Il servizio di Video Verifica è a complemento del servizio in Cloud della centrale ed è un servizio integrativo a pagamento.

Per i dettagli su servizi e relativi costi dei nuovi servizi consultate il sito [www.securlan.it](http://www.securlan.it).

La modalità GRATUITA offerta con la registrazione della centrale al Cloud consente anche l'utilizzo delle Notifiche Push verso l'App Securlan.

## PORTALE SECURLAN

Per consentire la registrazione delle centrali di allarme Securlan al servizio Cloud di Cwebforce è stato creato il portale di registrazione [www.securlan.it](http://www.securlan.it).

Per consentire l'attivazione in Cloud della centrale deve essere prima creato un Utente Privato.

Seguire la procedura di registrazione ed effettuare la Login al portale.

A seguire inizializzare la centrale alla registrazione in Cloud (con software Securlink da versione 6.4.0. o con SMS dedicato). La centrale invia una email in cui sono contenuti i dati di attivazione.

Dalla bacheca del Privato sarà possibile creare il profilo impianto relativo alla centrale che si sta inizializzando e al termine delle procedura (messaggio di conferma) la centrale sarà disponibile alla connettività da App ( Cloud, Ddns Cloud ). L'Utente Privato può a seguire creare ed un profilo Tecnico a supporto del suo impianto e creare le credenziali del Tecnico ( Username e Password ).

Fornite all'Utente Privato la Vostra email per consentirgli di inviarvi i dati con le Vostre credenziali di accesso alla centrale. Al termine della creazione del profilo del Tecnico una email vi verrà inviata in automatico con le credenziali che Vi consentiranno di utilizzare l'App Securlan (in modalità Tecnico) ed il software Securlink (in modalità Tecnico Cloud) per agire sulla centrale del Vostro cliente.

Registratevi come Tecnico utilizzando la stessa email che avete fornito all'Utente Privato.

Nella Vostra Bacheca troverete l'invito dell'Utente e la procedura di acquisizione dell'impianto sotto il Vostro controllo. Potete divenire Tecnico di illimitati profili impianto centrale e degli stessi ne sarete i supervisor. A tale scopo ogni Utente Privato, di cui siete il Tecnico, dovrà ripetere la procedura sopra esposta. Di tutti i profili impianto (centrali) di cui divenite Tecnico, sarete in tempi brevi in grado di effettuare Supervisione, Monitoraggio, Programmazione e Manutenzione.

Dal 1 di Febbraio 2019 una nuova avventura accompagnerà le centrali Securlan.

Benvenuti a bordo.

Evoforce srl

Nigretti Claudio