AIRSECURITY & HOTSPOT SECURITY

SICUREZZA SU BRANDMEISTER

Breve guida per attivare la funzione AirSecurity & Hotspot Security

Con questa breve guida voglio segnalare la modalità di attivazione della sicurezza (AirSecurity) per il prorio ID (o tutti gli ID che si hanno registrati in DMR) sul network BrandMeister.

Come prima cosa (se non si è già registrati) bisogna registrarsi sul sito del network BrandMeister a questo indirizzo:

https://brandmeister.network/?page=register

Compilare tutti i campi richiesti e attendere la mail di conferma di avvenuta attivazione del proprio account su BrandMeister per poi procedere a fare il login e gestire il proprio account stesso.

Successivamente scaricare un'applicazione per il proprio smartphone che gestisce password temporanee (TOTP) disponibili sia per Android che per iPhone.

Esempio per Android:

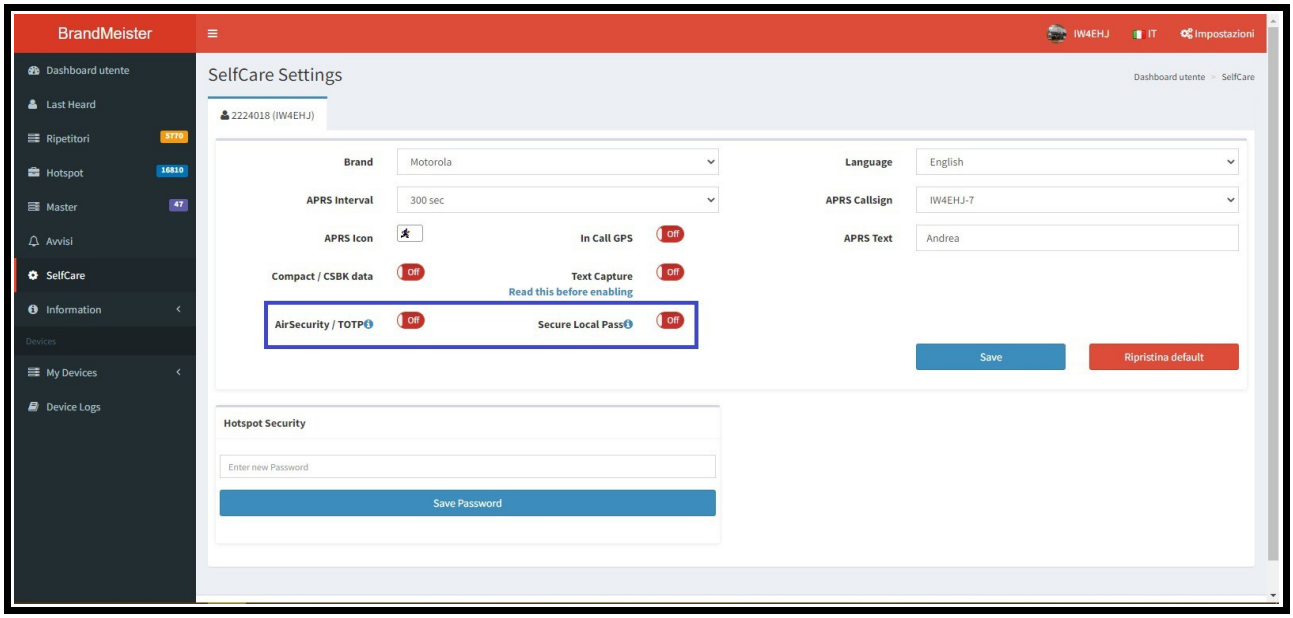
https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp
https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=it

Esempio per iPhone:

https://apps.apple.com/it/app/freeotp-authenticator/id872559395

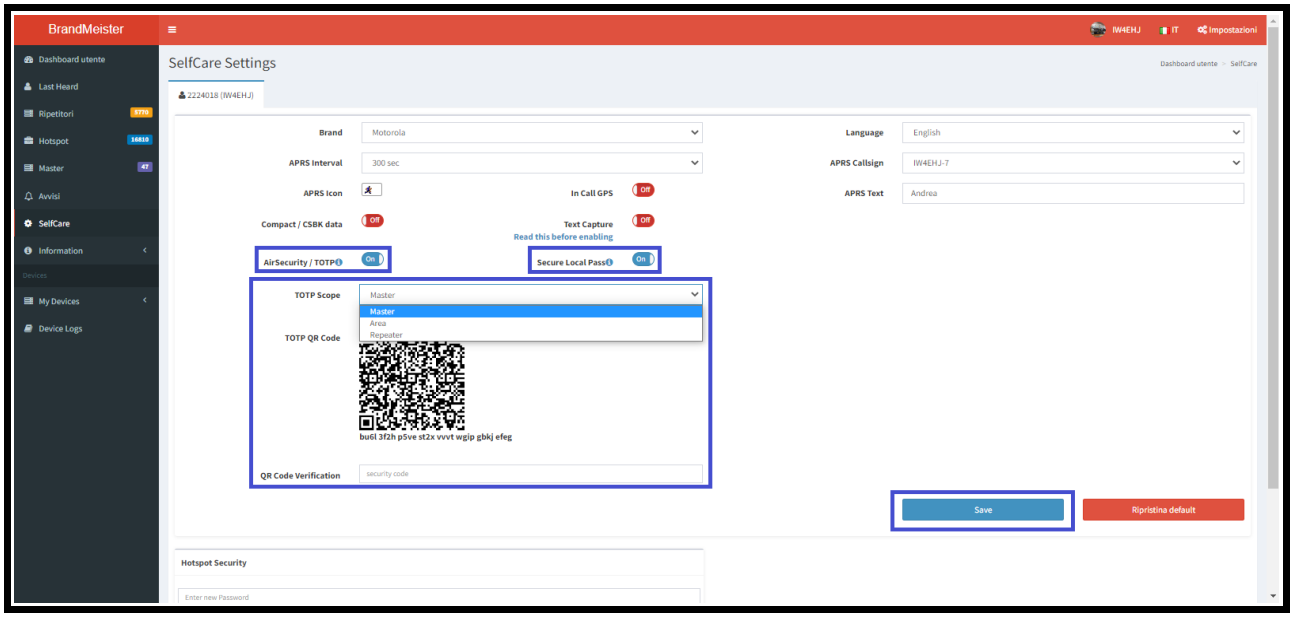
Una volta registrati e scaricata l'applicazione entrare nel proprio account BrandMeister e nella sezione selfcare troverete le due funzioni "AirSecurity/TOTP" e "Secure Local Pass" che sono settate su OFF come nella foto sucessiva.

La prima voce "AirSecurity/TOTP" attiverà la sicurezza del proprio ID mentre la seconda voce "Secure Local Pass" servirà per poter utilizzare il proprio ID tramite i nostri accessi privati (hotspot, applicazioni, server DVSwitch ed altro già protetti da Hotspot Security che vediamo dopo) mentre sul resto della rete il nostro ID rimarrà bloccato.



A questo punto attivate entrambe le due voci come nella prossima foto.

Una volta attivate le due voci si presenta un QR Code con un menù a tendina con le tre scelte, la prima scelta "Master" serve a bloccare il proprio ID sulla rete come avveniva in precedenza e ti darà la possibilità di essere sbloccati da radio o da selfcare (poi vediamo come) mentre la seconda scelta "Area" sarà implementata prossimamente (probabilmente si riferirà ad una certa area selezionabile) e la terza scelta "Repeater" che ti blocca sulla rete e ti permette di sbloccare il proprio ID solo sul ripetitore usato per effettuare la procedura di sblocco mentre come detto il pulsante "Secure Local Pass" permette di bypassare il blocco se si utilizza un accesso alla rete tramite un proprio hotspot, applicazione o server DVSwitch realizzato con il nostro ID a 7 cifre più eventuale ESSID.



Una volta effettuata la scelta desiderata nella tendina apriamo la nostra applicazione per la gestione degli OTP e aggiungiamo un nuovo elemento (la procedura cambia a seconda di quale applicazione si andrà ad usare) inquadrando il QR Code.

Può essere fatta anche manualmente se l'applicazione permette di inserire il codice manuale che trovate sotto il QR Code stesso.

Una volta terminata la procedura nella vostra applicazione si attiverà il collegamento con BM quindi per confermare dovete inserire nel campo "QR Code Verification" il numero che vi appare sullo smartphone cliccando appunto sul collegamento appena creato e successivamente salvando cliccando su "Save".

Consiglio se si vuole utilizzare più di un dispositivo (smartphone e tablet) prima di salvare si può inserire in tutti i dispositivi che abbiamo il collegamento a BM inquadrando il QR Code, così facendo in questo modo tutti i vostri dispositivi sono in grado di generare il codice TOTP per effettuare lo sblocco temporaneo.

In alternativa se non si vuole usare il QR Code per Google Authenticator si può utilizzare la stringa che trovate sotto al QR Code stesso in modo da effettuare la procedura direttamente da smartphone sensa utilizzare un PC e confermando sempre inserendo il "QR Code Verification" e facendo poi "Save".

Questa procedura va effettuata per tutti gli ID singolarmanente che abbiamo regisrati sulla rete DMR (creando appunto per ogni ID un collegamento nell'applicazione), nel selfcare abbiamo i nostri ID separati e quindi configurabili tramite la linguetta posta in alto che indica i nostri ID attivi sulla rete DMR.

Ora che la funzione "AirSecurity/TOTP" è attiva ogni passaggio sulla rete BrandMeister verrà automaticamente rifiutato con un messaggio vocale di "Accesso Negato" ma non sui nostri hotspot o varie applicazioni che utilizziamo perchè abbiamo attivato la voce "Secure Local Pass".

Ora veniamo invece all'utilizzo dello sblocco tramite TOTP per poter nuovamente trasmettere sulla rete temporaneamente e quindi per un tempo limitato ai trenta minuti standard non modificabili.

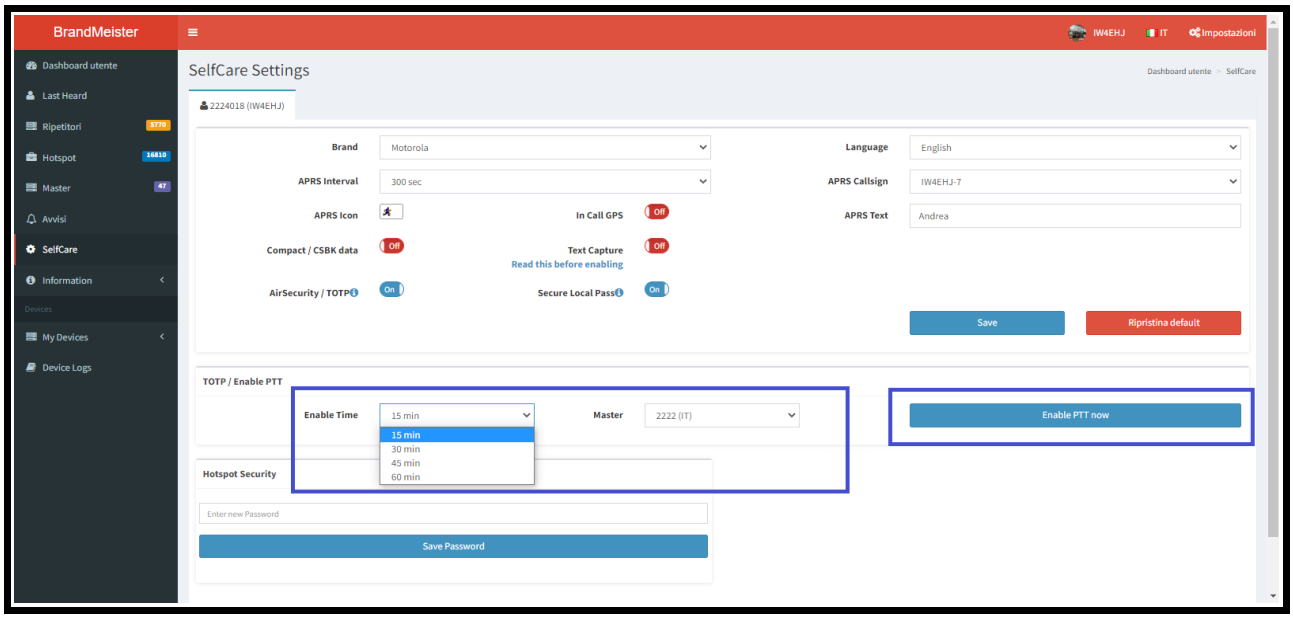
Per poter riabilitare temporaneamente il nostro ID dobbiamo aprire la nostra applicazione e preparare la radio a trasmettere un chimata privata.

Una volta entrati in modalità chiamata privata digitare sulla radio il 9 seguito dal codice TOTP che ci viene proposto dall'applicazione, chiaramente il tutto deve essere fatto senza far scadere il tempo a disposizione (30 secondi) altrimenti il codice TOTP cambia (essendo un codice a tempo) e bisogna quindi usare il nuovo codice fornito, la procedura di sblocco è fattibile anche tramite applicazione (DroidStar o DVSwitch Mobile) e non solo da radio in caso "Secure Local Pass" sia impostata su OFF.

Esempio se cliccando sull'applicazione ci appare il codice 506789 la nostra chiama privata deve essere 9506789 quindi a questo punto sentiremo un messaggio vocale di "Codice Di Accesso Accettato" e possiamo tranquillamente trasmettere per un tempo impostato fisso dal server di trenta minuti, una volta trascorso il tempo il nostro ID torna ad essere bloccato e necessita di essere nuovamene sbloccato tramite procedura mentre se il codice viene sbagliato si ottiene un messaggio vocale con "Codice Di Accesso Rifiutato".

Questa procedura è valida anche se nella fase di attivazione della funzione "AirSecurity/TOTP" abbiamo scelto "Repeater" ma in questo caso viene sbloccato il proprio ID solo sul ponte usato per la procedura di sblocco ma rimane bloccato su tutta la rete tranne sempre per gli hotspot e accessi vari per via della funzione "Secure Local Pass" attiva.

Se in fase di attivazione abbiamo scelto "Master" oltre al metodo classico via radio abbiamo la possibilità di sbloccare temporaneamente il nostro ID in autonomia sul nostro selfcare utilizzando il menù dedicato che abbiamo a disposizione come indicato in foto.



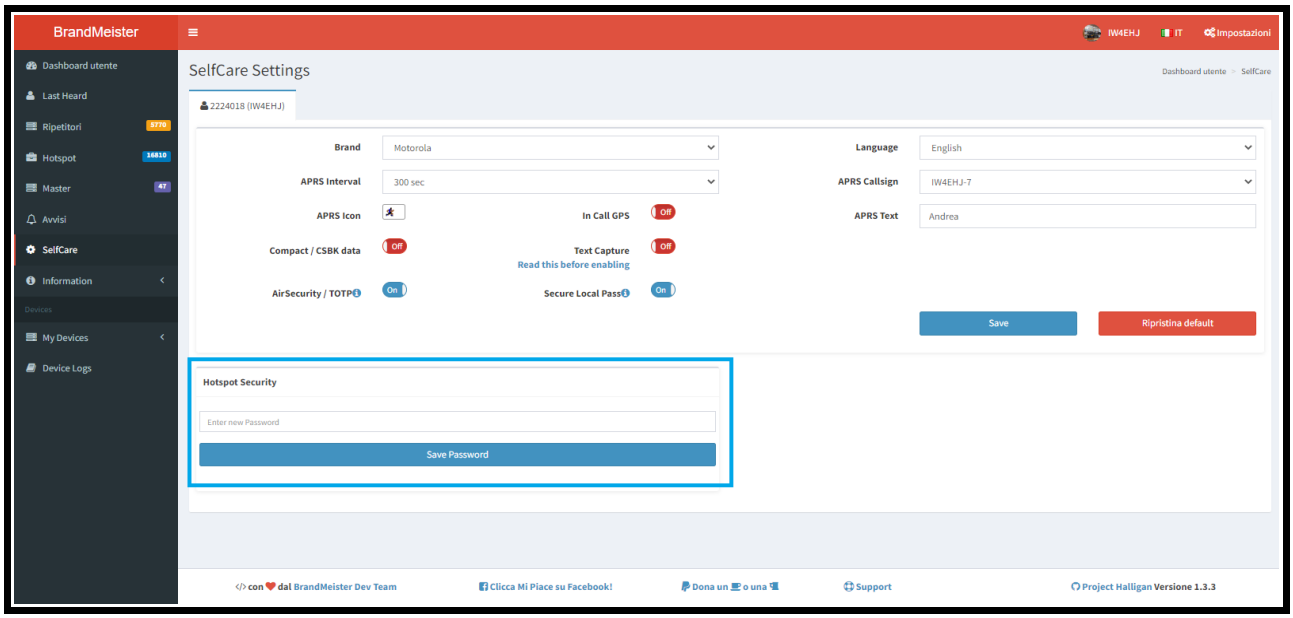
Qui dobbiamo selezionare il tempo che vogliamo nella tendina "Enable Time" (15, 30, 45 o 60 minuti) e il master di riferimento nella tendina "Master" e premere "Enable PTT now" in questo modo il nostro ID sarà attivo per il tempo selezionato e sul master selezionato (dove il ponte che usiamo è collegato) senza dover disattivare la funzione completamente.

Una volta che la funzione di "AirSecurity/TOTP" viene disattivata portando su OFF la linguetta e la si vuole riattivare bisogna rifare tutta la procedura e cancellare sull'applicazione del dispositivo o dei vari dispositivi il collegamento a BM perchè chiaramente non sarà più valido.

Attualmente il blocco tramite "AirSecurity/TOTP" funziona solo con la fonia e non per la messaggistica.

Naturalmente se non si attiva la funzione "Secure Local Pass" le regole di blocco sono valide anche per i nostri hotspot e applicazioni varie e quindi soggette al blocco del nostro ID al passaggio dai nostri dispositivi personali o server DVSwitch ecc.

Veniamo ora alla funzione "Hotspot Security", che è obbligatorio fare se si vuole utilizzare un sistema hotspot o eventualmente le varie applicazioni disponibili su smartphone, bisogna entrare sempre nel proprio selfcare ed impostare una password personale (che sarà poi da impostare su qualsiasi hotspot in nostro possesso o applicazione), in modo da impedire a chiunque di creare un accesso sulla rete utilizzando il nostro ID (come già successo).



Come vediamo in foto nel campo "Hotspot Security" dovete inserire la vostra password personale e poi cliccare su "Save Password" per confermare, una volta salvato il campo torna bianco ma non vi preoccupate la password è stata salvata correttamente e la potrete usare su tutti gli hotspot e applicazioni, anche qui vale la regola se avete più ID potete fare la password per ogni ID singolarmanente tramite la linguetta superiore nel proprio selfcare, potete cambiare password quando e quante volte senza problemi in caso non la ricordiate più, poi andrà impostata su tutti i vostri dispositivi utilizzati.

Con questo è tutto.

73' da Andrea IW4EHJ

E-mail:iw4ehj@alice.it

QRZ: https://www.qrz.com/db/IW4EHJ

(Revisione 2 del 11-04-2023)