cPanel - Sicurezza

- Modifica Password account cPanel
- Attivare e Disattivare ModSecurity
- ImunifyAV - cPanel
- Attivare utenze secondarie di cPanel

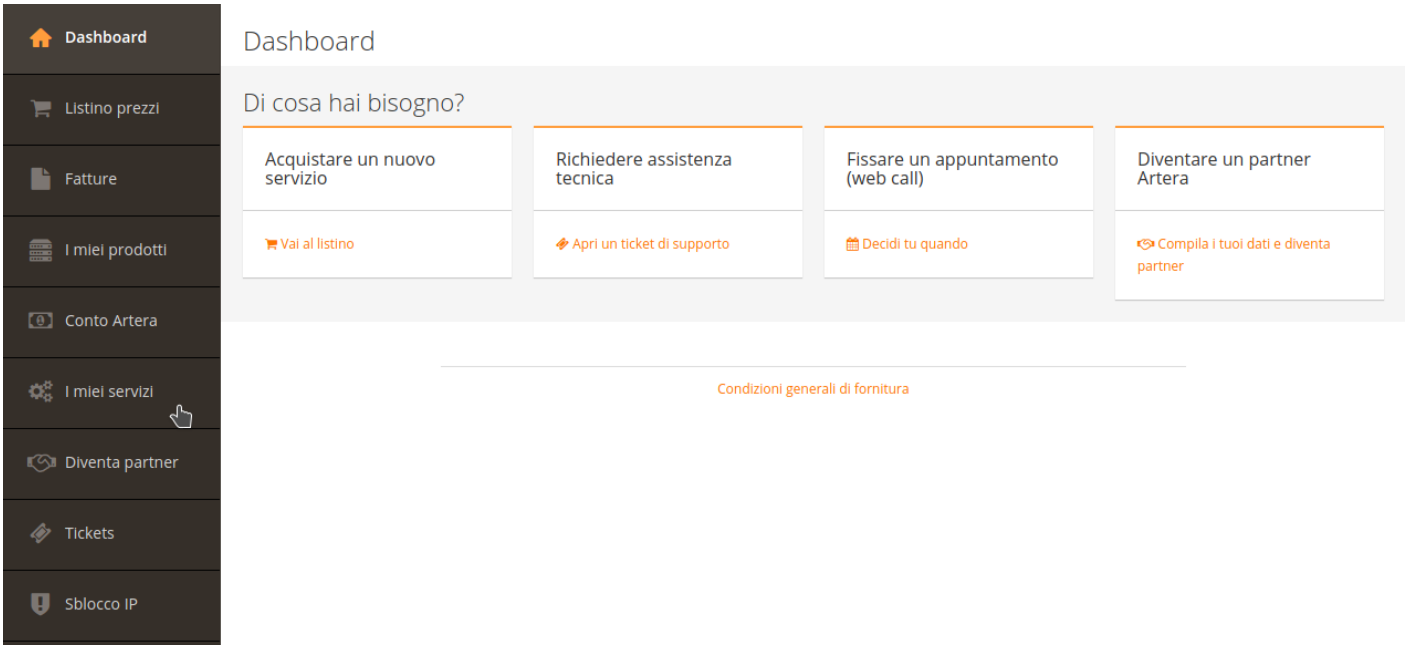
Modifica Password account cPanel

In questa guida illustreremo come modificare la password del proprio account cPanel, sia attraverso la propria area riservata, sia dal pannello di controllo.

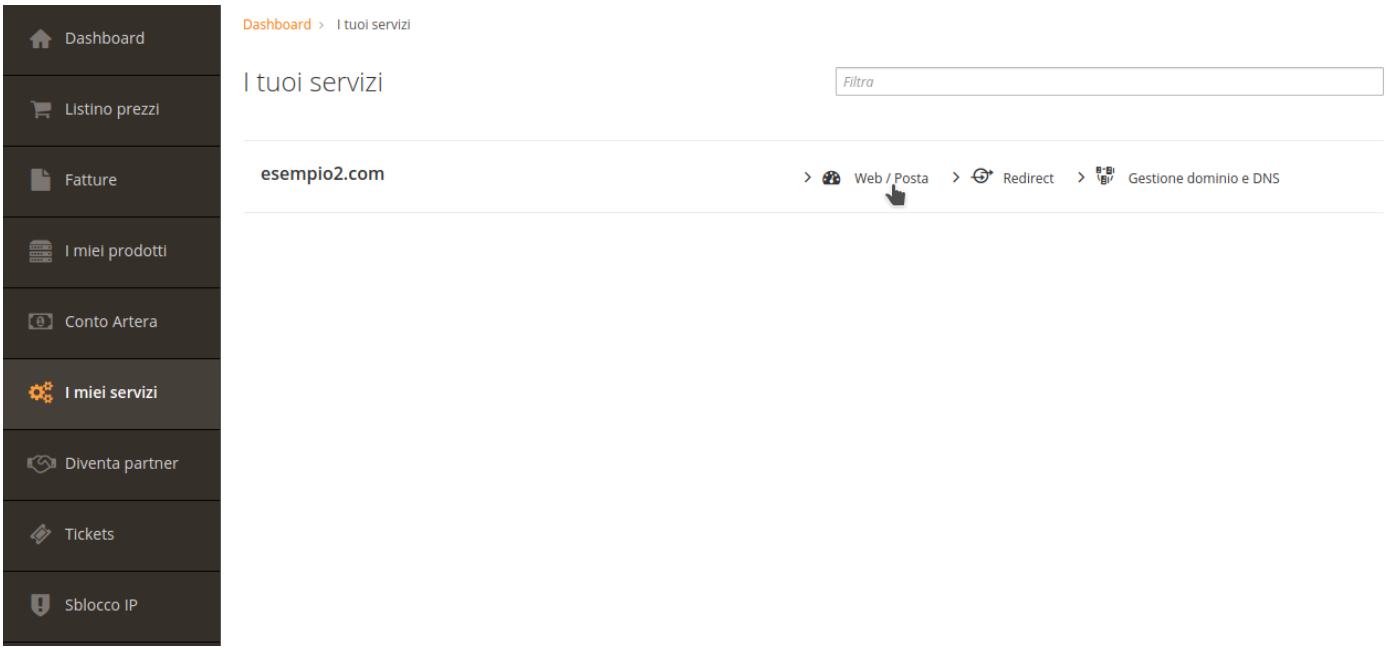
> L'utente cPanel e la sua password sono validi anche per collegarsi con client FTP o da SSH: la modifica della password influenzerà anche questi accessi.

Modifica password dall'area riservata

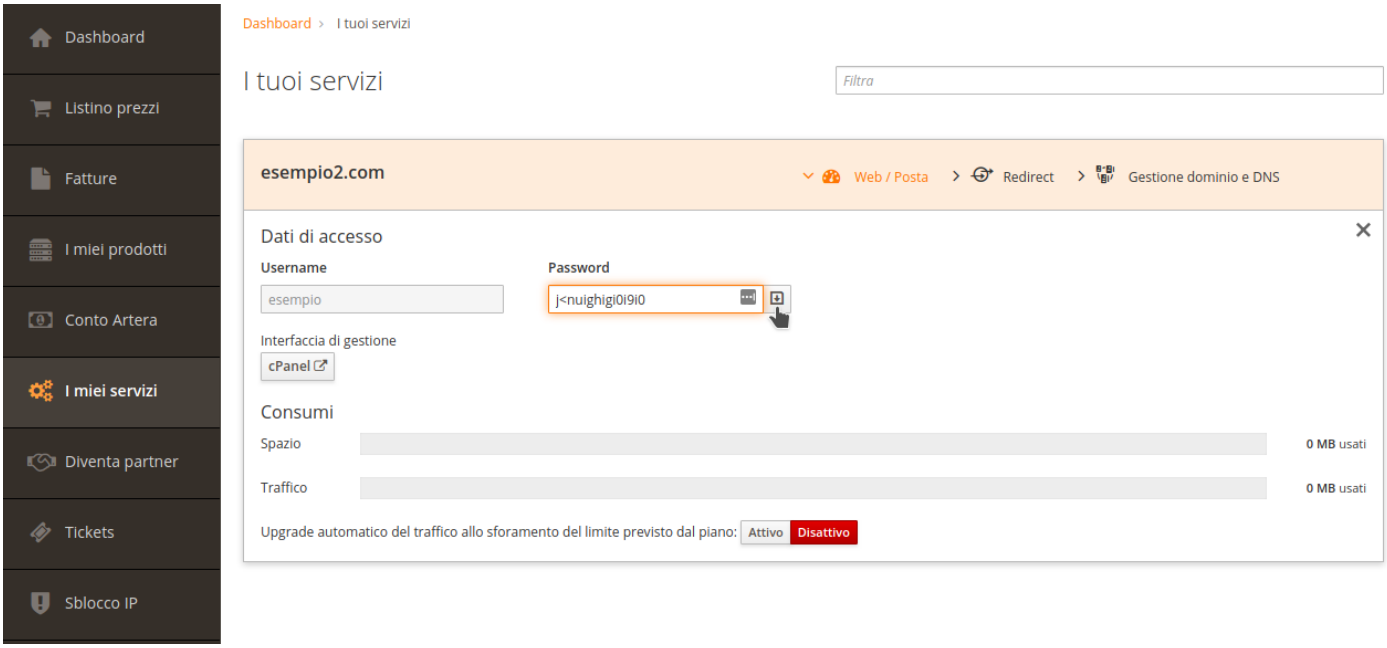
Prima di tutto è necessario accedere alla propria area riservata (admin.artera.net) ed entrare nella sezione "I miei servizi", che trovate nel menù laterale.



In questa sezione troverete tutti i servizi attivati per i vostri domini. Per modificare la password di cPanel è necessario aprire "Web/Posta".



A questo punto è sufficiente inserire la nuova password nel campo "Password" e cliccare sul tasto salva a lato (icona di una freccia rivolta verso il basso all'interno di un quadrato) per confermare la nuova password.

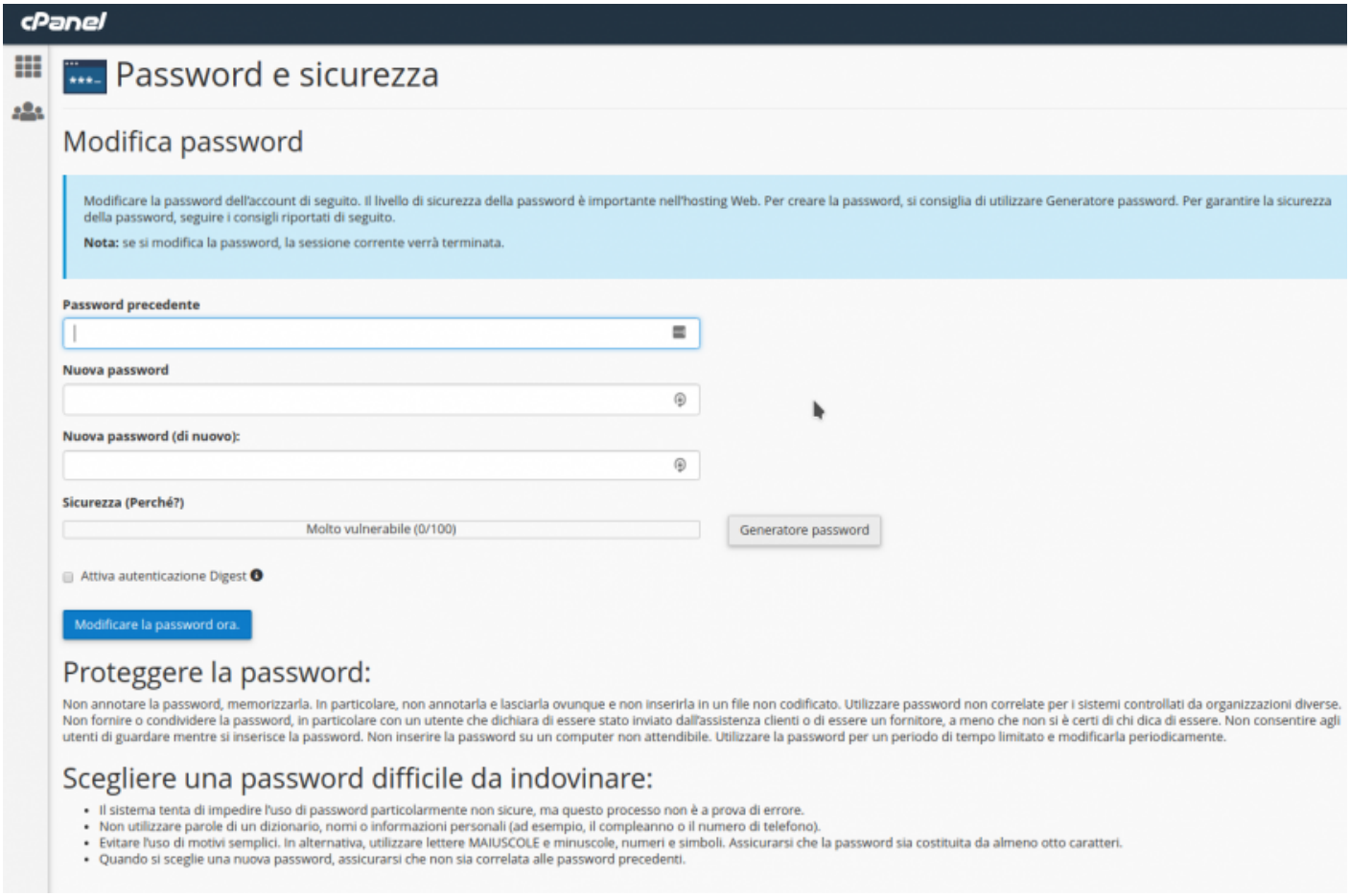


Modifica password dal pannello cPanel

Prima di tutto è necessario accedere al proprio pannello di controllo visitando l'indirizzo https://mail.DOMINIO:2083 con proprio browser internet, sostituendo a DOMINIO il dominio del vostro sito internet senza www, ed entrare nella sezione "Password e sicurezza" che trovate nel blocco "Preferenze".

> Potete aiutarvi utilizzando il filtro di cPanel, che trovate in cima a tutte le sue sezioni appena eseguito l'accesso.

La pagina visualizzata richiederà l'inserimento della vecchia password e di quella nuova, che andrà confermata inserendola nell'apposito campo di verifica "Nuova password (di nuovo)".



Potete generare la password personalmente o utilizzare il "Generatore password" di cPanel, che offre diverse opzioni per creare quella più sicura possibile.

> La nuova password deve raggiungere un livello di sicurezza minimo di 65, per poter essere utilizzata.

Attivare e Disattivare ModSecurity

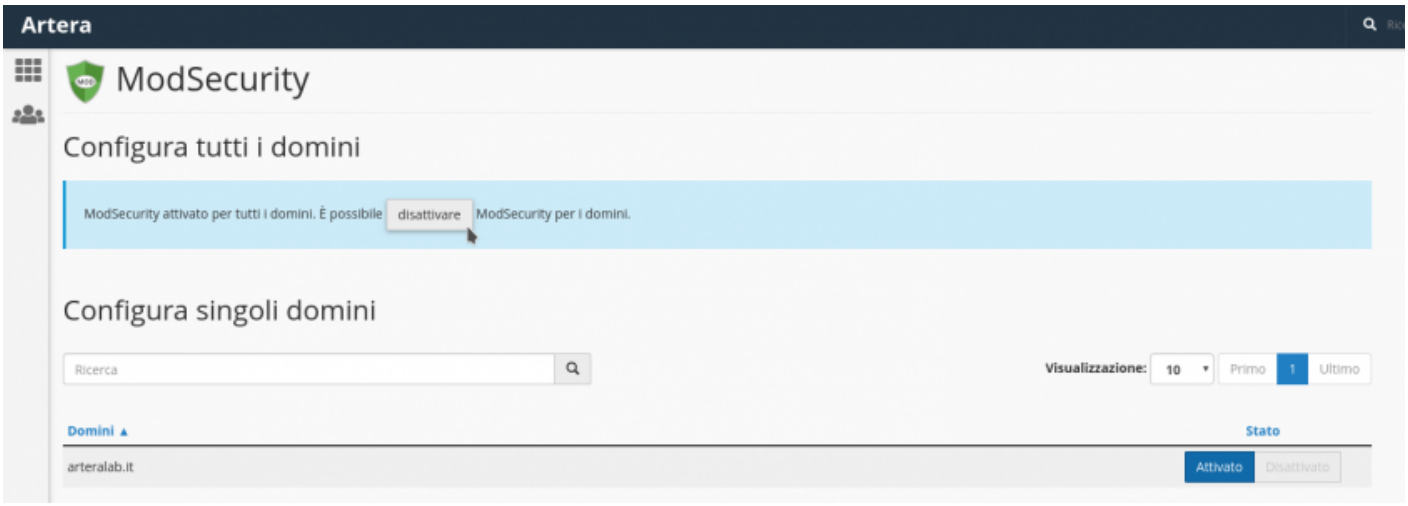
Per eseguire alcune modifiche sul vostro sito potrebbe essere necessario dover disattivare temporaneamente ModSecurity, in questa guida illustreremo come procedere tramite il pannello di controllo cPanel.

Questo modulo protegge dagli attacchi più diffusi e filtra tutte le richieste in entrata. Per una maggiore sicurezza, le intercetta e verifica prima ancora che vengano gestite dagli script.

Per prima cosa è necessario accedere al proprio pannello di controllo visitando l'indirizzo https://mail.DOMINIO:2083 con proprio browser internet, sostituendo a "DOMINIO" il dominio del vostro sito internet senza www.

Nel gruppo SICUREZZA, cliccare su ModSecurity.

Verrà aperta la pagina di gestione dove sarà possibile disattivare e attivare ModSecurity.



Disattivare ModSecurity rende vulnerabile il vostro sito, è quindi consigliato disabilitarlo solo se è necessario e riattivarlo una volta completate le modifiche.

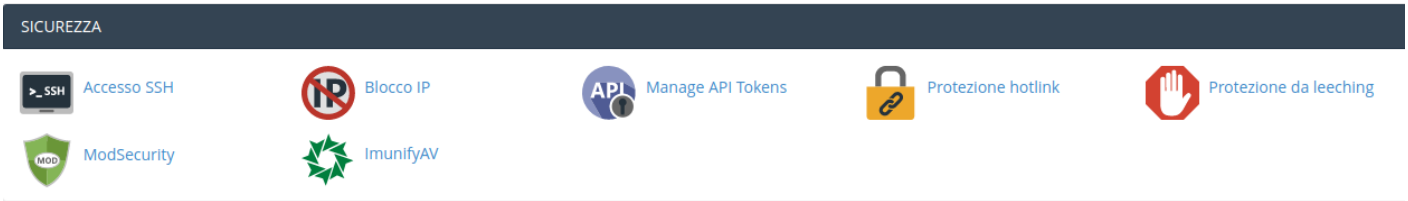
ImunifyAV - cPanel

ImunifyAV è uno scanner antimalware che rileva tutti i file dannosi, compresi backdoor, web-shell, virus, scripts, phishing e molti altri.

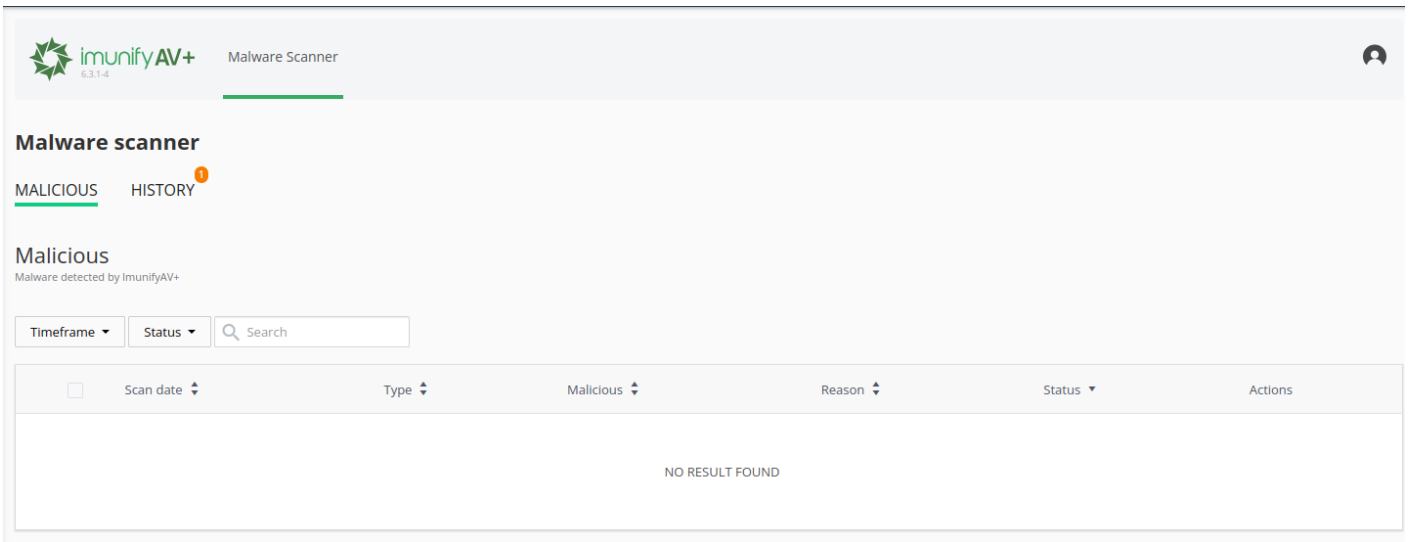
E' installato su tutti i server WHM di Artera e permette di gestire direttamente da cPanel i file che sono stati rilevati come dannosi.

In questa guida illustreremo come poter utilizzare le funzioni che il plugin ImunifyAV mette a disposizione.

Prima di tutto è necessario accedere al proprio pannello di controllo visitando l'indirizzo https://mail.DOMINIO:2083 con proprio browser internet, sostituendo a DOMINIO il dominio del vostro sito internet senza www, ed entrare nella sezione "ImunifyAV".



Una volta entrati il pannello mostrerà lo stato dei file contenuti nell'hosting a seguito dell'ultima scansione effettuata dal sistema. Nel caso in cui non sia stato rilevato del malware non verrà riportato nulla nella sezione Malicious.



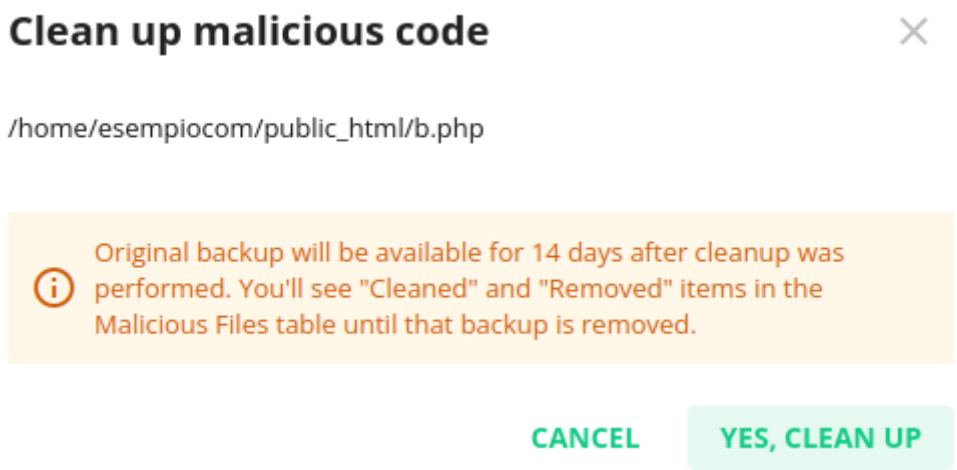
Se invece sono presenti malware sotto la sezione Malicious troverete tutti i file che sono stati rilevati come infetti.

Scan date	Type	Username	Malicious	Reason	Status	Actions
April 25, 2022 8:00 AM		esempiocom	/home/esempiocom/public_html/b.php	SMW-SA-04961-php.bkdr.wshll-10	Infected	

E' possibile eseguire due azioni sui malware rilevati:

- Con il tasto riportante l'icona "occhio" è possibile visualizzare il contenuto del file.

- Con il tasto riportante l'icona "scopa" è possibile ripulire il file infetto.



> Come indicato nel popup che compare procedendo con la pulizia del malware, il backup del file originale rimarrà disponibile e recuperabile per 14 giorni, dopodiché sarà rimosso.

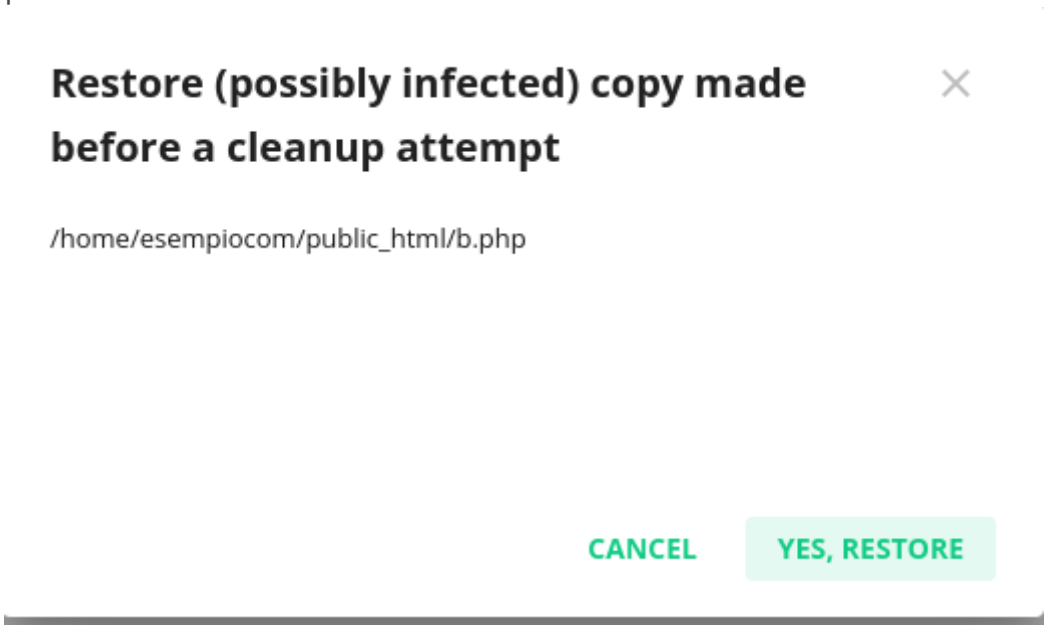
Una volta ripulito il file verrà visualizzato come segue.

Scan date	Type	Username	Malicious	Reason	Status	Actions
April 25, 2022 8:00 AM		esempiocom	/home/esempiocom/public_html/b.php	SMW-SA-04961-php.bkdr.wshll-10	Content removed	

A questo punto sarà possibile eseguire due operazioni su di esso:

- con il tasto riportante l'icona "occhio" sarà sempre possibile visualizzare il contenuto del file, ma in questo risulterà ripulito dal codice malevolo

- con il tasto riportante l'icona "orologio" sarà, invece, possibile ripristinare il file originale, operazione necessaria nel caso il sistema dovesse rimuovere anche del codice essenziale per il corretto funzionamento del sito.



Sotto la sezione History sarà possibile visualizzare lo storico delle operazioni effettuate sui file malevoli.

imunify AV+ 6.3.1-4 Malware Scanner

Malware scanner

MALICIOUS HISTORY

History

Search

Date	Type	Path	Cause	Initiator	Event
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Restored original
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Cleanup removed content
April 28, 2022 11:08 AM		/home/esempiocom/public_html/b.php	manual	root	Restored original
April 28, 2022 10:53 AM		/home/esempiocom/public_html/b.php	manual	root	Cleanup removed content
April 25, 2022 8:00 AM		/home/esempiocom/public_html/b.php	background	root	Detected as malicious
April 20, 2022 4:37 PM		/home/esempiocom/public_html/b.php	user	root	Detected as malicious

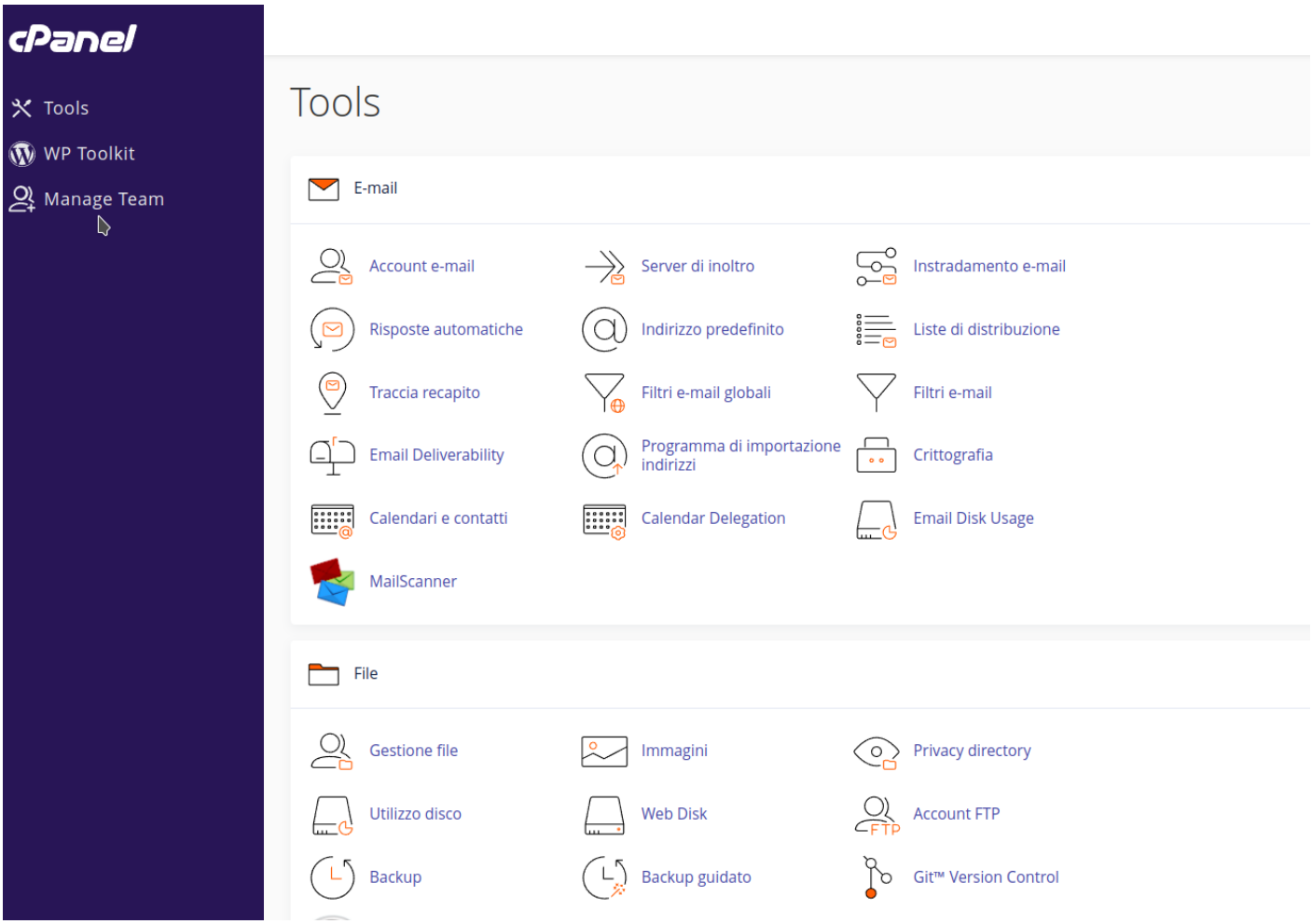
Items per page: 25

Attivare utenze secondarie di cPanel

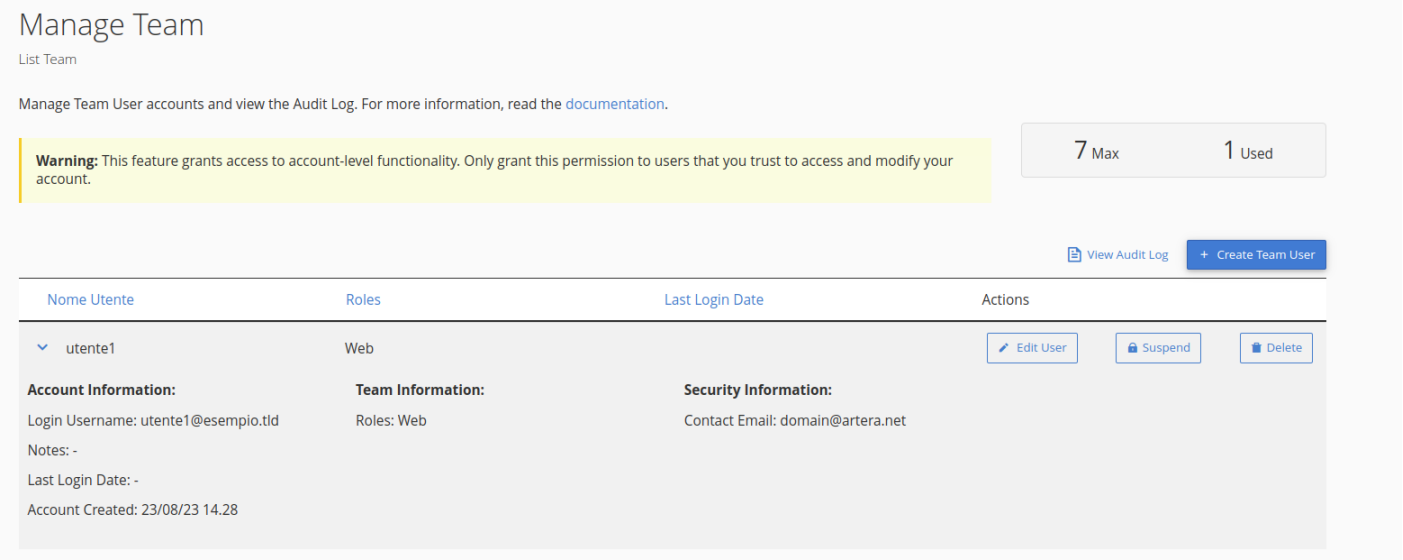
Il "Manage Team" è uno strumento molto utile messo a disposizione da cPanel, che permette di abilitare utenti supplementari limitandone, eventualmente, le funzionalità accessibili: a seconda dei ruoli definiti, infatti, un utente potrà gestire i servizi di posta, i servizi web, o il database. Di seguito vediamo come fare.

> Attenzione questi utenti saranno in grado di effettuare operazioni sensibili, consigliamo quindi di fornire questi accessi solo a persone fidate.

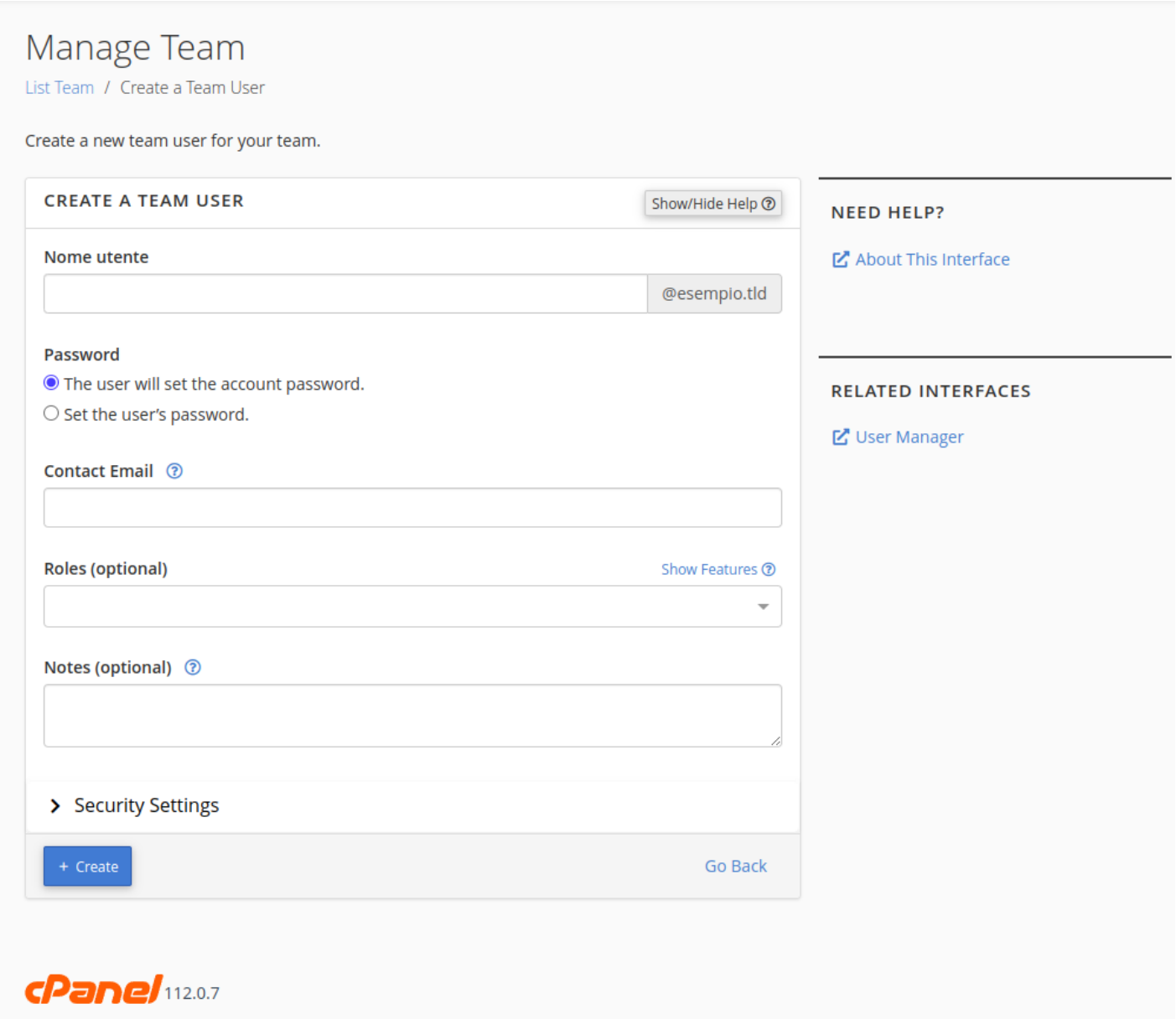
Prima di tutto è necessario accedere al proprio pannello di controllo cPanel visitando l'indirizzo https://mail.DOMINIO:2083 con proprio browser internet, sostituendo a DOMINIO il dominio del vostro sito internet senza www, ed entrare nella sezione "Manage Team". Sulla barra di sinistra sarà disponibile una scorciatoia.



Una volta eseguito l'accesso a "Manage Team" sarà possibile gestire le utenze attive o attivarne di nuove , se necessario. Il sistema permetterà inoltre di visualizzare i dettagli di ogni account attivo, di modificarli, sospenderli o cancellarli.



Per attivare un nuovo account è necessario cliccare sul bottone blu "Create Team User", reperibile in alto a destra, con il quale il sistema aprirà il form di creazione dell'utente.



Il riquadro "**Nome utente**" dovrà essere compilato col nome dell'utente che si ha intenzione di attivare, tenendo in cosiderazione che il nome completo sarà comprensivo di @dominio, dove "dominio" è il nome dominio per cui è stato attivato il pannello di controllo.

Le opzioni "**Password**" permettono di impostare la password manualmente o di inviare una email all'indirizzo di posta elettronica che verrà associato all'utente, in modo che possa generare la password in autonomia.
Spuntando la voce "Set the user's password." il sistema metterà a disposizione il riquadro con il quale inserire/generare manualmente la password.

In "**Contact Email**" è necessario inserire l'indirizzo di posta elettronica che dev'essere associato all'utente cPanel che si sta attivando. Nel caso si scegliesse l'opzione "The user will set the account password." è all'email inserita in questo riquadro che verrà inviato il messaggio con il link per generare la password.

Il menù "**Roles (optional)**" permette di definire eventuali limitazioni all'utente che si vuole attivare:

- Administrator: l'utente potrà accedere a qualsiasi funzionalità di cPanel;
- Database: l'utente potrà utilizzare solo gli strumenti relativi alla gestione dei database;
- Email: l'utente avrà accesso solo alle funzionalità relative al servizi di posta elettronica;
- Web: l'utente sarà in grado di usare solo gli strumenti per la gestione del sito, come ad esempio i backup, le statistiche, WP Toolkit e altro.

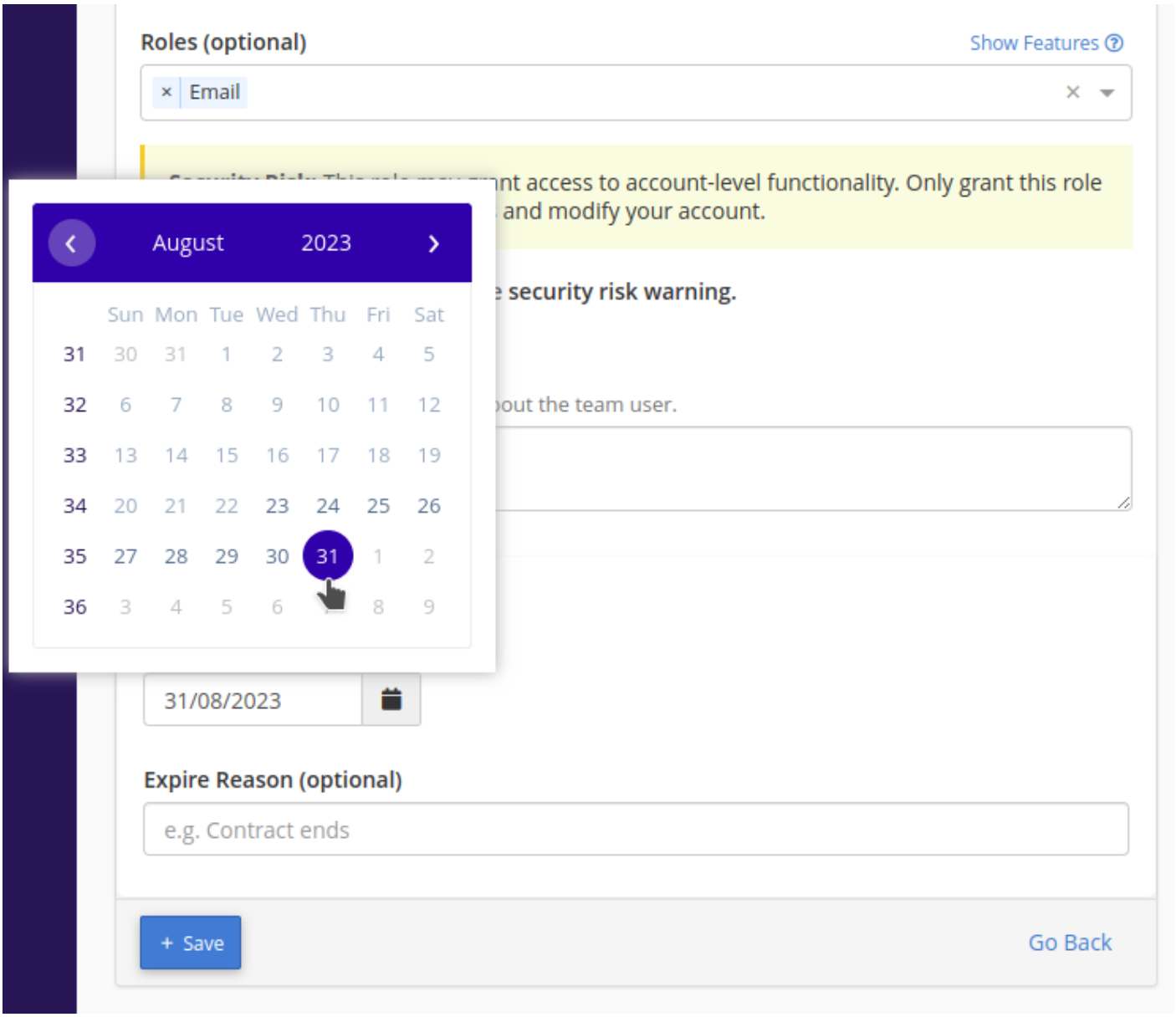
> La voce "Hide Features" pemette di visualizzare l'elenco degli strumenti accessibili per ogni ruolo.

> E' possibile abilitare più di un ruolo per ogni utente.

> Non definire un ruolo attiverà un utente con accesso solo alle informazioni di base.

Il riquadro "**Notes (optional)**" permette di inserire delle informazioni aggiuntive in merito all'utente che si vuole creare.

Cliccando su "**Security Settings**" il sistema permetterà di definire una data di scadenza, dopo la quale l'utente verrà automaticamente eliminato.



Il riquadro "**Expire Reason (optional)**" consente di inserire informazioni aggiuntive in merito alla scadenza dell'utente.

Una volta compilati tutti i paramteri sarà sufficiente cliccare sul tasto blu "Save" per attivare l'utenza.