

cPanel - Sicurezza

- [Modifica Password account cPanel](#)
- [Attivare e Disattivare ModSecurity](#)
- [Imunify360 - cPanel](#)
- [Attivare utenze secondarie di cPanel](#)

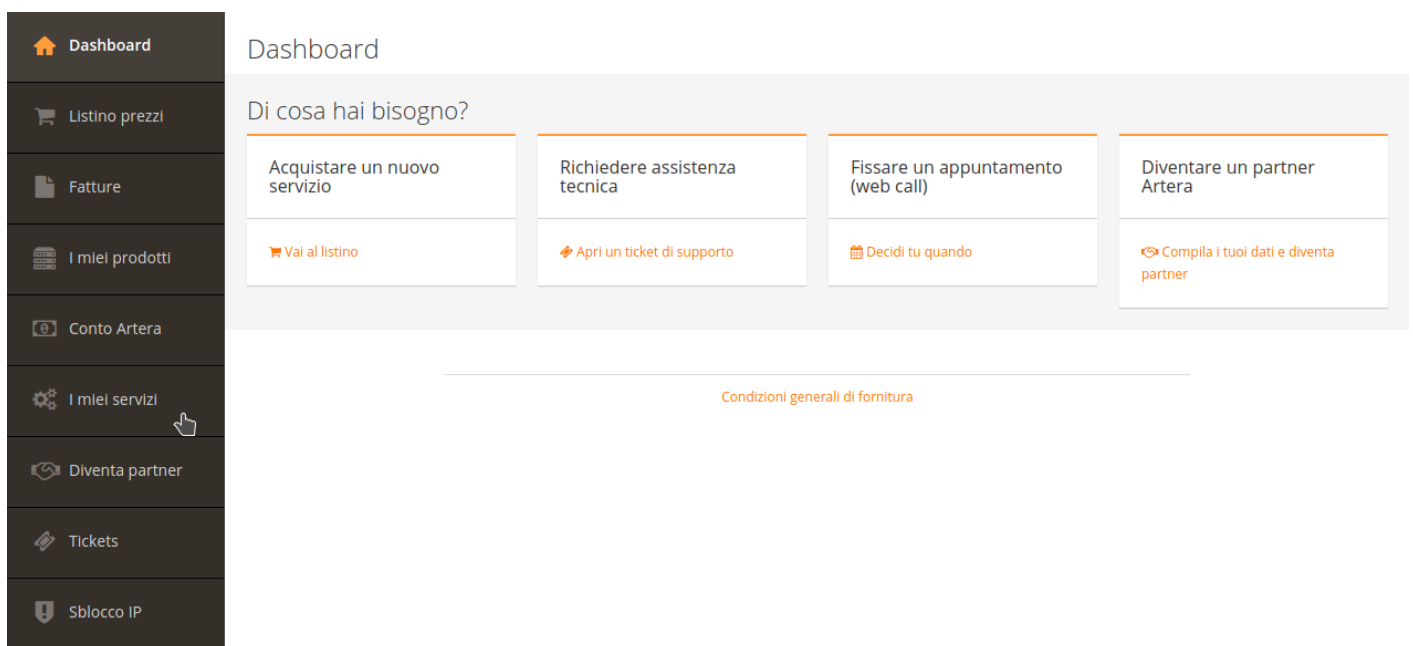
Modifica Password account cPanel

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

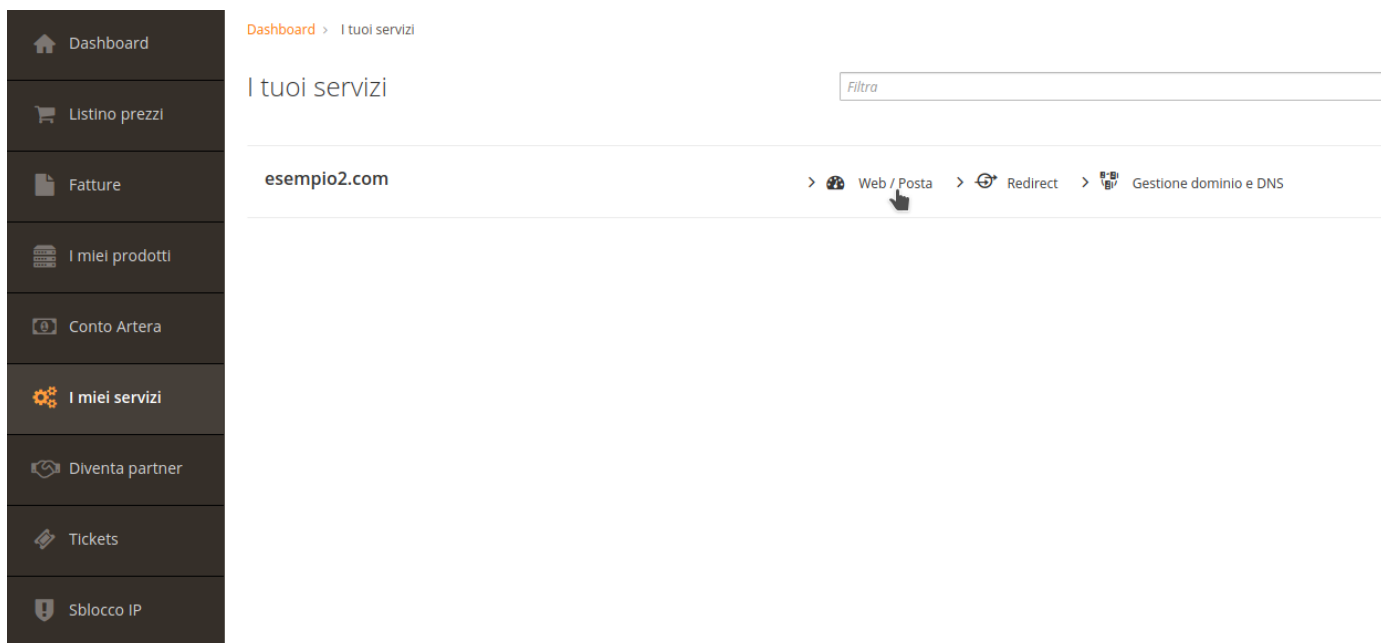
L'utente cPanel e la sua password sono validi anche per collegarsi con client FTP o da SSH: la modifica della password influenzerà anche questi accessi.

Modifica password dall'area riservata

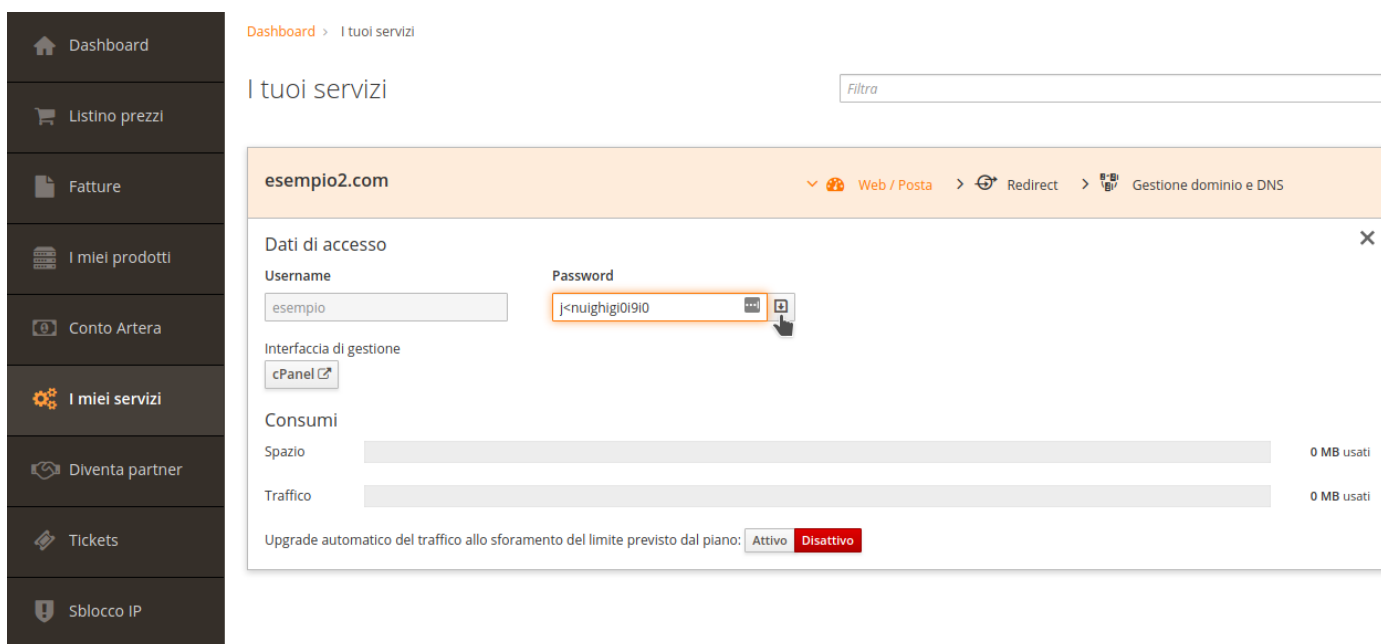
Prima di tutto è necessario accedere alla propria area riservata (admin.artera.net) ed entrare nella sezione "I miei servizi", che trovate nel menù laterale.



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)".

cPanel

Password e sicurezza

Modifica password

Modificare la password dell'account di seguito. Il livello di sicurezza della password è importante nell'hosting Web. Per creare la password, si consiglia di utilizzare Generatore password. Per garantire la sicurezza della password, seguire i consigli riportati di seguito.

Nota: se si modifica la password, la sessione corrente verrà terminata.

Password precedente

Nuova password

Nuova password (di nuovo):

Sicurezza (Perché?)

Molto vulnerabile (0/100)

Generatore password

☐ Attiva autenticazione Digest

[Modificare la password ora.](#)

Proteggere la password:

Non annotare la password, memorizzarla. In particolare, non annotarla e lasciarla ovunque e non inserirla in un file non codificato. Utilizzare password non correlate per i sistemi controllati da organizzazioni diverse. Non fornire o condividere la password, in particolare con un utente che dichiara di essere stato inviato dall'assistenza clienti o di essere un fornitore, a meno che non si è certi di chi dica di essere. Non consentire agli utenti di guardare mentre si inserisce la password. Non inserire la password su un computer non attendibile. Utilizzare la password per un periodo di tempo limitato e modificarla periodicamente.

Scegliere una password difficile da indovinare:

- Il sistema tenta di impedire l'uso di password particolarmente non sicure, ma questo processo non è a prova di errore.
- Non utilizzare parole di un dizionario, nomi o informazioni personali (ad esempio, il compleanno o il numero di telefono).
- Evitare l'uso di motivi semplici. In alternativa, utilizzare lettere MAIUSCOLE e minuscole, numeri e simboli. Assicurarsi che la password sia costituita da almeno otto caratteri.
- Quando si sceglie una nuova password, assicurarsi che non sia correlata alle password precedenti.

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.

Artera

ModSecurity

Configura tutti i domini

ModSecurity attivato per tutti i domini. È possibile [disattivare](#) ModSecurity per i domini.

Configura singoli domini

Ricerca

Visualizzazione: 10 Primo 1 Ultimo

Domini ▲	Stato
arteralab.it	Attivato Disattivato

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

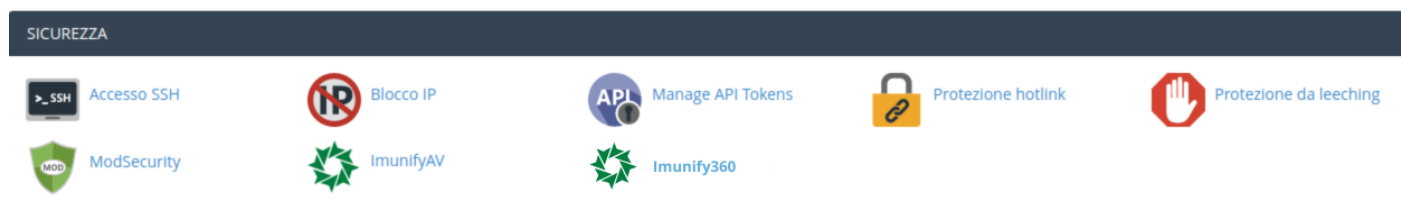
Imunify360 - cPanel

Imunify360 è uno scanner antimalware che rileva tutti i file dannosi, compresi backdoor, web-shell, virus, scripts, phishing e molti altri.

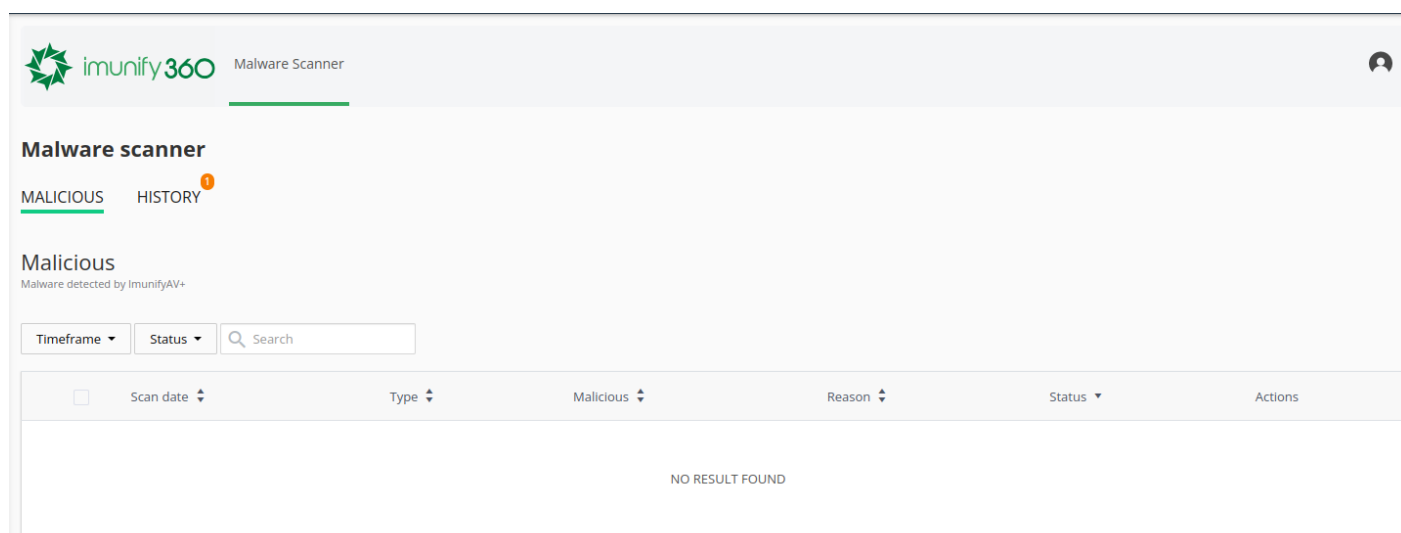
E' installato su tutti i server WHM di Artera e permette di gestire direttamente da cPanel i file che sono stati rilevati come dannosi.

In questa guida illustreremo come poter utilizzare le funzioni che il plugin Imunify360 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 "Imunify360".



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.

E' possibile eseguire due azioni sui malware rilevati:

- [View /home/esempiocom/public_html/b.php](http://View/home/esempiocom/public_html/b.php)

VJA1L3hzT3ZzZ1jEbkpsa1h6aVh1NVJHOTBaSm1SWVET1ZDQ3hSSkhhemhzWmdRcEpnRFdQYnJ3Rmd3NHlWOXP0G0S0uKWVWM2R4RlBBdTyzWldmbUtoOeWQ1bJaxc3BMNmJmJclDd2b1lveWzTeHNBV1Bdy9aNUJqbHrVM1ZsbkRVSG1wN2dBZmlvZ3c4dmgwbdHjJWA1M2lxVVRWR0hBtXRBUjllYwI1VfkrNkixMzgyZU5UemM2bWbHnWU5UR5U029B2dHp3MwdrTVFyL1krTWwrT9VaVjuZGd5VfRWMldZemNQVY9BZVpqVWR1T59HukQZu1cxdQj3L1F0S21TUVa3UzJMSDjTE15N0M3.blAXZzhL0UixaytBM25yn3G8Z256tUzPbTEr1dvTndweTVYvYdwXfMeDuXQVZtNGXvDNXu2RYaVhyaUkxSVJw9S9jTNSXSS0pTzcEvcUxWbHplRIdaRjdtVfVSNU3G5eUeWnK1ZoYVWMSExYbhd5CvM7Zr3YmwybKXbVlgyJTK3dva2hNkXGd5M3abv2NETZfMcnlyQv00VBfVEVj3MkNZhJlTLEWkdr1dBdSKZRbkdUdUYrU0t2NTBORmlaoXVuRHVYkVBzNukvVVMvcDlvMVl6K1VySmM5WURSeFVRZtBUQ1ZZYnInRGQRNu93cVl5YWFV1JlaDMrRFBhMlhWtWw5MWZaWDhInWdpQTG5GbnYrV9GrcwVtOsrNmZd3Y2kMksa3dwdFV51RtXedIdERSty1krEzEBELMJIWJ0S2drTnrbhW5L1BrCdZtUQXpQXkOZGTCv1WHU5NFY0NVNqpd7K3pKqXBUbsmwb5b1F50jClTpB2tF35kNldWZ1QllexRmnpdHhXrVYwZDWSEVHZUuLz0NtHlWtK5Y3FXUE9XEQvdXkb13havjYvc13M5NvaMvDYnYvVlVCY2RZPK1NsVm1mNU9jRnJ5cVlYjYk1ZanAwOHhGc21a1MxM01hWGdQJTJBMvndUeG5jYmFWSzcZv21mZllWbIBVUmpOclRoenpuNzjCQnMvdGU2c3o3dzNRmNlzenN2dzc1cWw2NTZnWmluOvDnb21DrNl6eG5QWwBHRM1Juf3d6d3pY2MzNR3hGeU9CUlOcFRkYb0lkaGoOYTU2KlXUQ5XL2NMTztnRTNHWtAYU0Y0T1ZyWkVwWlRM0fQEOE9aSanBoZnSLXNBNmRmY5mt3QWZb0ZhZmFlnmhOtfIveCtZdQc254MjRfYkN1jXtXuch1V4VUrIetWlXgJl1hWaTjL2U4VdFRTN2VnhlMIdioWtNmEFqJtRBMWUQJTN3C9NSXsmbWlKRfRdJlJWwQrCk21dUhxURoajFVJMxMdtdKOENSKvRnJdaV1YlzcvcTByRloyRTWdUpU0ztcht1h0LytnD9PRcWp6R0yQ0ZSej3V1ZHXUcXV1A3efJYbFkxeWNlEFeVZUDJMa2ZOEOjvTUYRmjMcFqJvURub0F5dzhjNGFFWtRfAhcvYUzEg4MFVC5NWNhWlN2VG1Cb5WMSm2d6Y2UWsmXmEg1dVJZaEzVZmpkbl1NkaxkERwZF3hYmVWGVUFZMvZ0jtUkx55d2oa2dBv29VQJ1ZaWPNZG0uZ0Z5X9LQ2p6M0dzak560StBmm04eWx3bFFWOC8u53C2TZR9mEj2VJZRM9hQZCxbLUUdJRGEEZwF3KjDwcmorMnpGMjVcxzQwQZRPfLWV949nERZV8uA5X839a4p3pmsyUuV5MnNBtmtdNqW8wTFJQaUxodmFFNNVR1clvKRfDlVUQ2MDJ2aHp4YkFvN0g1dJnQwVvg1Y0lHek5Cd3RvU1g4OHZ0TtDJZfZgM1I3M0k3MEdkamFHY28rc0kwajZBdUlfUEU5L0ctbVdVGH9h03VNZGhuenVlKZ5UdU2TFVM0C1NFZxbtdVmfVIZ9YdZ8zL040WvYdWVgwdtVZSExp050R3p3dYktrQTvtajZQndXmM21UR1c5UBoem9plbVE4N2RUtXNcG90dHNCMTlVEX21VXF0RkPlUuWdH0F4bjjoJNdVbK6Z9Z0FUNL2anp0WFbZjNmS521E2kxkdlUhdKnptQROGRhUfTwcBLDlU9aamQ5NnRnjdtFVYQXVq3bPrYkRSUuXtOFTNQUxxbPfdFRUQjW3GjJmW4c4cnRVu3FkcmUtlzFGZlX5Wxh2ZjZdGZG0Yj3Nz2QWUoreTgra3I4WgtFUDVFaGd4FpCb1VBZGvmL1N4TzRyYkI5V2joUGxra0pkT1B4RG5XeE4A05HhcxClEdUxxvMq3Q0WEZdXBINyPwKrUd1pxdD0CglJazBoZTQJlIUU5MCW9FVhWtAZaVheJENKZGK21qadZlRfAd2d5QmRlcGjYjYzUxU5URVRC3pWYtYL3aVudmhmgU5SutaNURGdyVJOGPN5G83UXNkE2uXk65pcEYzeFsczRoK5XQ1FPYlJZNUEvenFvCtJ1qad1ZTErEnt2m9wNtBuN1YnUNkRlcEjUVRVY1M5Mtu5U5tR2c253BuZnYQZ5YwchCl2d2lYU14L1T21NIZVFZ3hdc0FzNoRfBZ2RlanBFPQWbNbeKy

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

Clean up malicious code

/home/esempiocom/public_html/b.php

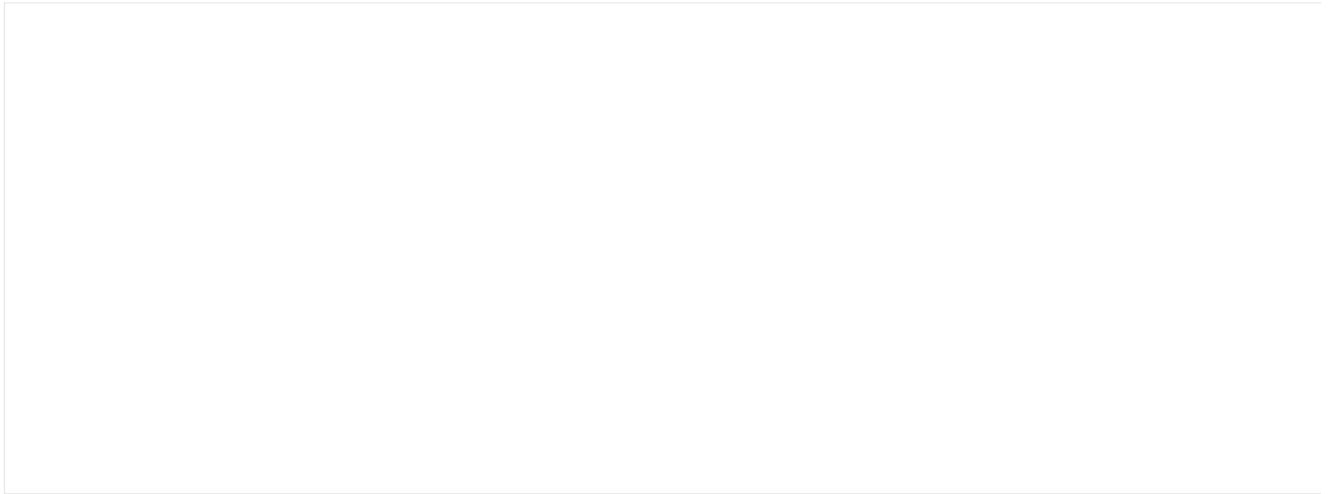
Come indicato nel popup che compare procedendo con la pulizia del malware, il backup del file originale rimarrà disponibile e recuperabile per 14 giorni, dopodiché sarà rimosso.

Una volta ripulito il file verrà visualizzato come segue.

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

View /home/esempiocom/public_html/b.php



CANCEL

- 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.

Restore (possibly infected) copy made before a cleanup attempt



/home/esempiocom/public_html/b.php

CANCEL

YES, RESTORE


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



Malware scanner

MALICIOUS HISTORY

History

 Search

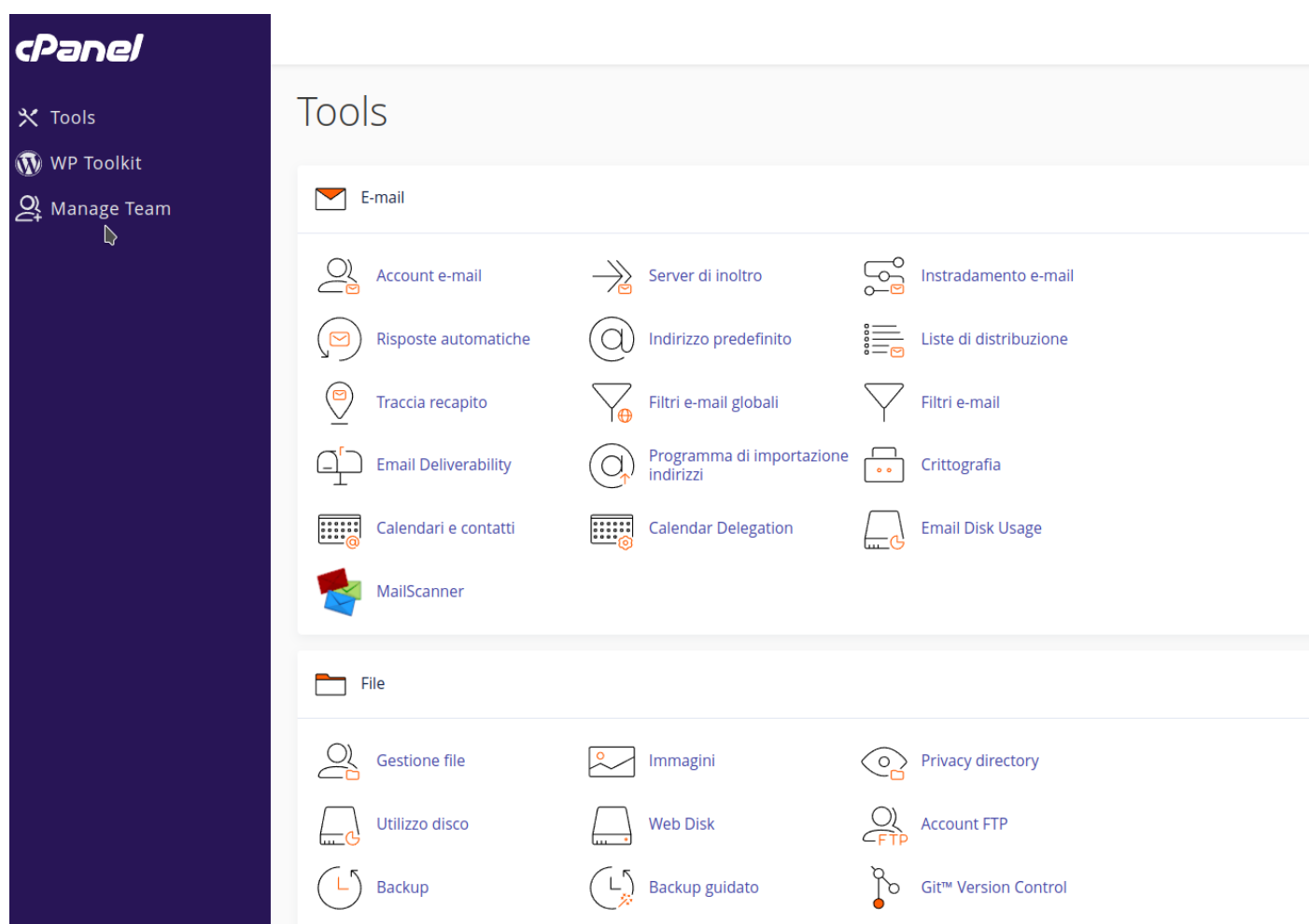
Date ▲	Type ▼	Path ▼	Cause ▼	Initiator ▼	Event
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Restored original
April 28, 2022 11:10 AM		/home/esempiocom/public_html/b.php	manual	root	Cleanup removed content
April 28, 2022 11:08 AM		/home/esempiocom/public_html/b.php	manual	root	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

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.

Manage Team

List Team

Manage Team User accounts and view the Audit Log. For more information, read the [documentation](#).

Warning: This feature grants access to account-level functionality. Only grant this permission to users that you trust to access and modify your account.

7 Max

1 Used

View Audit Log

Create Team User

Nome Utente	Roles	Last Login Date	Actions
<div>utente1</div> <div>Account Information: Login Username: utente1@esempio.tld Notes: - Last Login Date: - Account Created: 23/08/23 14.28</div>	<div>Web</div> <div>Team Information: Roles: Web</div>	<div></div> <div>Security Information: Contact Email: domain@artera.net</div>	<div><div>Edit User</div><div>Suspend</div><div>Delete</div></div>

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.

Manage Team

[List Team](#) / [Create a Team User](#)

Create a new team user for your team.

CREATE A TEAM USER

Show/Hide Help ?

Nome utente

 @esempio.tld

Password

- ☒ The user will set the account password.
☐ Set the user's password.

Contact Email ?

Roles (optional)

Show Features ?

Notes (optional) ?

> Security Settings

+ Create

[Go Back](#)

NEED HELP?

[About This Interface](#)

RELATED INTERFACES

[User Manager](#)

cPanel 112.0.7

Il riquadro "**Nome utente**" dovrà essere compilato col nome dell'utente che si ha intenzione di attivare, tenendo in considerazione 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 ai 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" permette 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.

Roles (optional)

Show Features ?

×

Email

×

Security Risk: This role grants access to account-level functionality. Only grant this role and modify your account.

security risk warning.

about the team user.

<August2023>

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	30	31	1	2	3	4	5
32	6	7	8	9	10	11	12
33	13	14	15	16	17	18	19
34	20	21	22	23	24	25	26
35	27	28	29	30	31	1	2
36	3	4	5	6	7	8	9

31/08/2023

Expire Reason (optional)

e.g. Contract ends

+ Save

Go Back

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.