

Brute Force Manager

BFM (Brute Force Monitor) de DirectAdmin

Explicado para usuarios no técnicos

¿Qué es el BFM?

El **BFM** es el sistema de seguridad integrado en DirectAdmin que vigila, cuenta y bloquea intentos de acceso fallidos a:

- Panel de control (puerto 2222)
- Cuentas de correo (IMAP/POP/SMTP)
- FTP / SFTP
- SSH
- Aplicaciones web comunes (por ejemplo, WordPress)

Cuando detecta demasiados fallos desde una misma IP (o contra un mismo usuario) la bloquea automáticamente durante un tiempo, o la envía al cortafuegos para bloqueo permanente.

¿Cómo cuenta los intentos?

Parámetro	Lo que controla	Valor típico
<code>brutecount</code>	Máximo de intentos fallidos antes de bloquear la IP	20
<code>user_brutecount</code>	Máximo de intentos fallidos contra un mismo usuario	20
<code>brute_dos_count</code>	Peticiones repetidas a la página de login del panel (DoS)	100

Los límites se ajustan en **Admin Level** → **Admin Settings** → **pestaña Security**.

Picos frecuentes de intentos

- **Panel de control:** bots que prueban contraseñas de *admin*
- **Correo:** diccionarios contra cuentas populares (`info@`, `admin@`...)
- **WordPress:** ataques a `wp-login.php` (activar la opción *Scan for WordPress attacks* en BFM)

Qué pasa al superar el límite

1. La IP se añade a `/usr/local/directadmin/data/admin/ip_blacklist`.
2. (Opcional) Si está activado el enlace con CSF/LFD, la IP se bloquea a nivel de cortafuegos y no puede volver a conectarse.

Buenas prácticas recomendadas

- **Mantener** `brutecount` ≤ 20 para cortar diccionarios rápidos
- **Contraseñas fuertes:** el BFM bloquea, pero una clave robusta evita ataques exitosos
- **Revisar BFM a diario:** decide si alguna IP debe desbloquearse
- **Activar “Scan WordPress attacks”** si se usan sitios WordPress

Resumen

El BFM es un **vigilante automático**:

cuenta intentos, detecta patrones de ataque y bloquea al agresor antes de que entre.

Con límites bien ajustados y revisiones periódicas, mantenemos el servidor protegido sin afectar a los usuarios legítimos.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #2

Created 2025-06-19 08:27:17 UTC by Abkrim

Updated 2025-06-19 08:45:40 UTC by Abkrim