

---

# **WP fail2ban Blocklist**

**Charles Lecklider**

**Jun 15, 2022**



# CONTENTS

- 1 Configuration 3**
  - 1.1 fail2ban . . . . . 3
    - 1.1.1 Standard Filters . . . . . 3
- 2 *define()* Constants 5**
  - 2.1 All . . . . . 5
    - 2.1.1 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_CUSTOM\_JAIL . . . . . 5
    - 2.1.2 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_IGNORE\_IPS . . . . . 5
    - 2.1.3 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_LOG . . . . . 6



WP fail2ban Blocklist is a collaborative preemptive blocklist for ClassicPress and WordPress.



## CONFIGURATION

### 1.1 fail2ban

#### 1.1.1 Standard Filters

The filter files included should not be edited; there are no user-serviceable parts inside.

#### Typical Settings

If you are using the typical settings for *WPf2b* the Blocklist add-on will work without further configuration.

#### Custom Jail

1. Copy `wpf2b-blocklist-hard.conf` to your `fail2ban/filters.d` directory
2. Create a new file in `fail2ban/jail.d` called `wpf2b-blocklist.conf`

```
[wpf2b-blocklist-hard]
enabled = true
filter = wpf2b-blocklist-hard
logpath = /var/log/auth.log
maxretry = 1
port = http,https
```

---

**Note:** Make sure you change `logpath` to the correct log for your OS. If your OS uses *systemd* it may be simpler and/or easier to install a real syslog service first.

---

2. Reload or restart `fail2ban`





## *DEFINE()* CONSTANTS

### 2.1 All

#### 2.1.1 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_CUSTOM\_JAIL

New in version 1.0.0.

Changes the log format to match entries in `wpf2b-blocklist-hard.conf` instead of `wordpress-hard.conf`.

If you cannot set `maxretry = 1` in your `wordpress-hard` jail you must set this and create a custom `fail2ban` jail.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_CUSTOM_JAIL', true);
```

**Default:** `false`

#### 2.1.2 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_IGNORE\_IPS

New in version 1.0.0.

Changed in version 2.0.0: Entries can include IPv6 addresses.

A list of IP addresses to ignore if they appear in a Blocklist update.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_IGNORE_IPS', [  
    '1.2.3.4',  
    '2.3.4.5/24'  
]);
```

**Default:** `[]` (*empty list*)

Commonly used when accessing a site via shared access (e.g. Campus proxy, 3rd-party VPN, etc.).

---

**Note:** IPv6 addresses require *WP fail2ban* version 5 or later.

---

---

**Tip:** If you have whitelisted IPs in `fail2ban` because of shared access you should also add them here.

---

**See also:**

`WP_FAIL2BAN_PROXIES` has the same syntax.

### 2.1.3 WP\_FAIL2BAN\_ADDON\_BLOCKLIST\_LOG

New in version 1.0.0.

---

The syslog facility to use for a custom jail.

```
define('WP_FAIL2BAN_ADDON_BLOCKLIST_LOG', LOG_LOCAL7);
```

**Default:** LOG\_AUTH *or* LOG\_AUTHPRIV

**See also:**

- [\*WP\\_FAIL2BAN\\_ADDON\\_BLOCKLIST\\_CUSTOM\\_JAIL\*](#)
- [\*WP\\_FAIL2BAN\\_USE\\_AUTHPRIV\*](#)