Per-User Login Email Limit

Magic Login Pro · https://handyplugins.co/docs/per-user-login-email-limit/

Magic Login includes a built-in safeguard that limits how many login emails can be sent to the same user within a rolling one-hour window.

This helps reduce repeated login email abuse, mail flooding against individual accounts, and excessive token churn for the same user.

How It Works

When a login email is requested, Magic Login keeps track of how many login emails have already been sent to that user during the last hour.

If the configured limit is reached, no additional login email will be sent until earlier requests fall outside the one-hour window.

Default Behavior

By default, Magic Login allows up to `60` login emails per user within one hour.

This default is intentionally generous so that normal usage is not affected, while still providing a safety guard against repeated abuse targeting the same account.

Important Notes

This safeguard is designed as a lightweight abuse protection layer.

It is not a replacement for:

- full request throttling
- CAPTCHA or bot protection
- WAF or edge-level rate limiting
- SMTP or mail provider delivery controls

If you need stronger request-level protection, additional controls at the site or infrastructure level are still recommended.

Configuration

You can override the default limit in `wp-config.php` using the following constant:

```
define( 'MAGIC_LOGIN_REQUEST_FAILSAFE_LIMIT', 50 );
```

Disable the Limit

To disable this safeguard entirely, set the limit to 0:

```
define( 'MAGIC_LOGIN_REQUEST_FAILSAFE_LIMIT', 0 );
```

Filter Override

Developers can also override the limit programmatically using the magic_login_request_failsafe_limit filter.

Example:

```
add_filter( 'magic_login_request_failsafe_limit', function( $limit, $user ) {
	return 50;
}, 10, 2 );
```