Password Policy Manager for WordPress

Getting Started Guide & User Manual for the Plugin

This plugin is developed by WP White Security, the developers of the most comprehensive WordPress activity log plugin WP Security Audit Log, and Website File Changes Monitor, a file integrity monitor plugin for WordPress that does not report false alarms.

Manual version 1.4
Last updated: 4th June 2019.

Introduction

The main culprit of WordPress hack attacks are weak passwords. Unless policies are enforced, users use weak passwords. The plugin **Password Policy Manage for WordPress** was developed with this problem in mind. It helps WordPress website owners and administrators ensure their users use strong passwords.

Password Policy Manager for WordPress is a plugin that allows you to configure password policies users must adhere to, ensuring they use strong passwords that cannot be guessed during brute force attacks. It only takes a few seconds to configure strong WordPress passwords policies.

You do not have to familiarize yourself with a new system and interface. The **Password Policy Manager for WordPress** integrates seamlessly within your WordPress login page and uses the standard WordPress UI.

Note: This plugin does not work on WordPress multisite networks yet.

Benefits highlight

- Enforce strong password policies within seconds
- Out of the box support for WooCommerce
- Enforce use of lower & upper-case letters, numbers & special characters in passwords
- Set passwords to expire, ensuring users do not use the same password for very long
- Ensure password history checks so users do not use the same password often
- Reset all users' password with a click of a button
- Configure different policies for different user roles

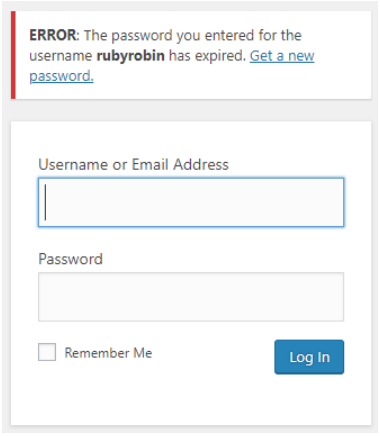
How does the plugin work?

When a user's password expires the user is either instantly logged out, or he can continue with the session and is forced to change the password the next time he tries to log back in to the site. This depends on how you configure the setting **Instantly terminate session on password expire or reset** which is explained in page of 11 this manual.

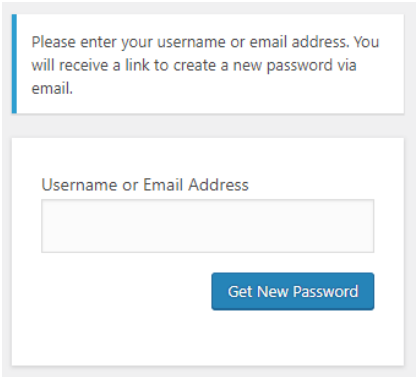
This section explains how users are notified that their password expired and how they can reset it.

Notification & password reset

1. Once the user with an expired password tries to login he is prompted about the expired password, as shown in the below screenshot.



2. Upon clicking on the **Get a new password** link the user is asked for the email address or username, as shown in the below screenshot.



3. If the user specifies a correct username or email they are sent an email with a link to reset the password. A copy of the email is shown in the below screenshot.

[WP White Security Dot Net] Password Reset Inbox ×

WordPress wordpress@wpwhitesecurity.net via wpwhitesecurity.com
to info

Someone has requested a password reset for the following account:

Site Name: WP White Security Dot Net

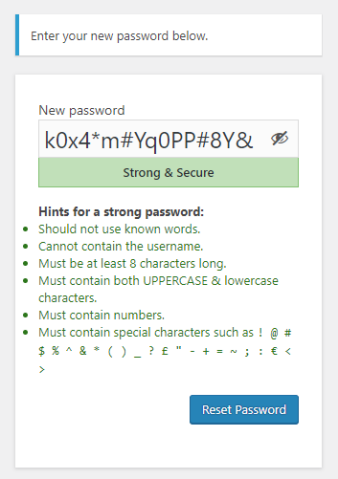
Username: rubyrobin

If this was a mistake, just ignore this email and nothing will happen.

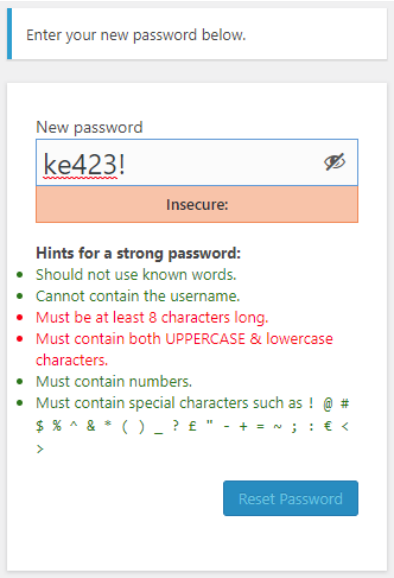
To reset your password, visit the following address:

<https://www.wpwhitesecurity.net/wp-login.php?action=rp&key=gvHprpf7ExPE7AMkoP2b&login=rubyrobin>

4. By clicking on the link the user is redirected to the password reset page. A new password is automatically recommended.

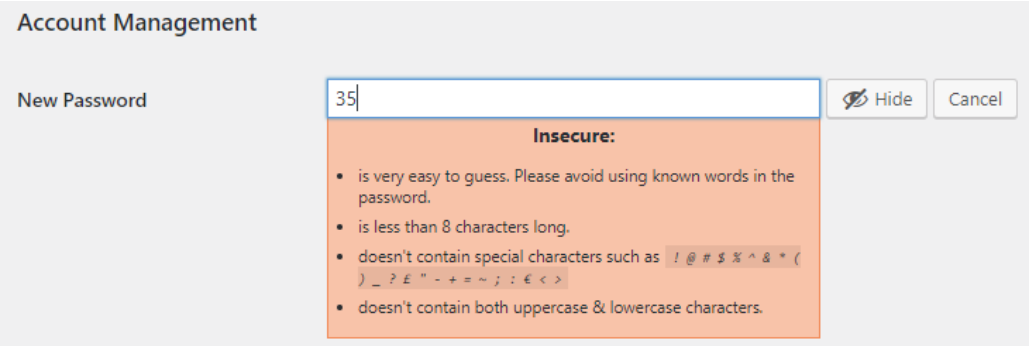


5. The user can use the recommended password or can specify a new one. If the user tries to use a password that does not match the policies, they are not allowed to reset it. Also, the policies which the password does not meet are highlighted in red, so the user is guided on what makes a strong password.



Resetting passwords in the user page

The policies also apply for password changes in the user profile page. As seen in the below screenshot, the user is shown which of the policies the password needs to meet to be reset.



Installing the plugin

WordPress dashboard

There is no need to unzip the plugin to install it from the WordPress dashboard. Just follow the below procedure:

1. Login to your WordPress admin pages using an administrator user.
2. Navigate to **Plugins** and click the **Add New** button.
3. Click the **Upload** button.
4. Click **Choose File** and navigate to the **password_policy_manager_wordpress.zip** file.
5. Select the file and click **Install Now**.

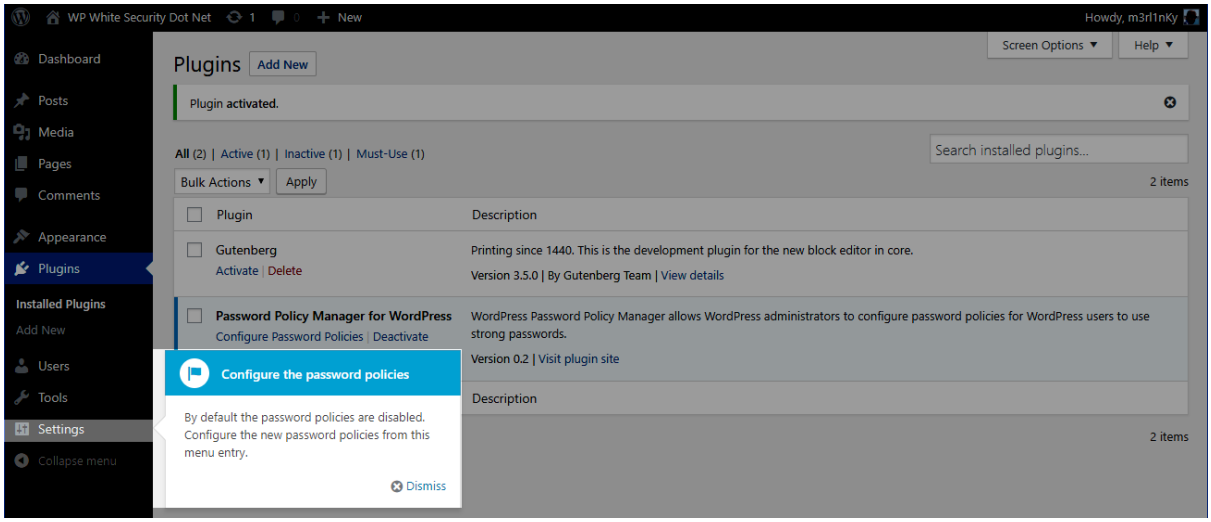
FTP

You can also install the plugin via FTP as explained in this procedure. If you are not familiar with FTP refer to how to Upload Files with FTP to WordPress.

1. Decompress (unzip) the plugin file **password_policy_manager_wordpress.zip**.
2. Connect to your WordPress website using a FTP client.
3. Upload the directory password_policy_manager_wordpress to the site's */wp-content/plugins/* directory.
4. Login to your WordPress dashboard and navigate to the **Plugins** page.
5. Click the Activate link under the **Password Policy Manager for WordPress**.

Getting started

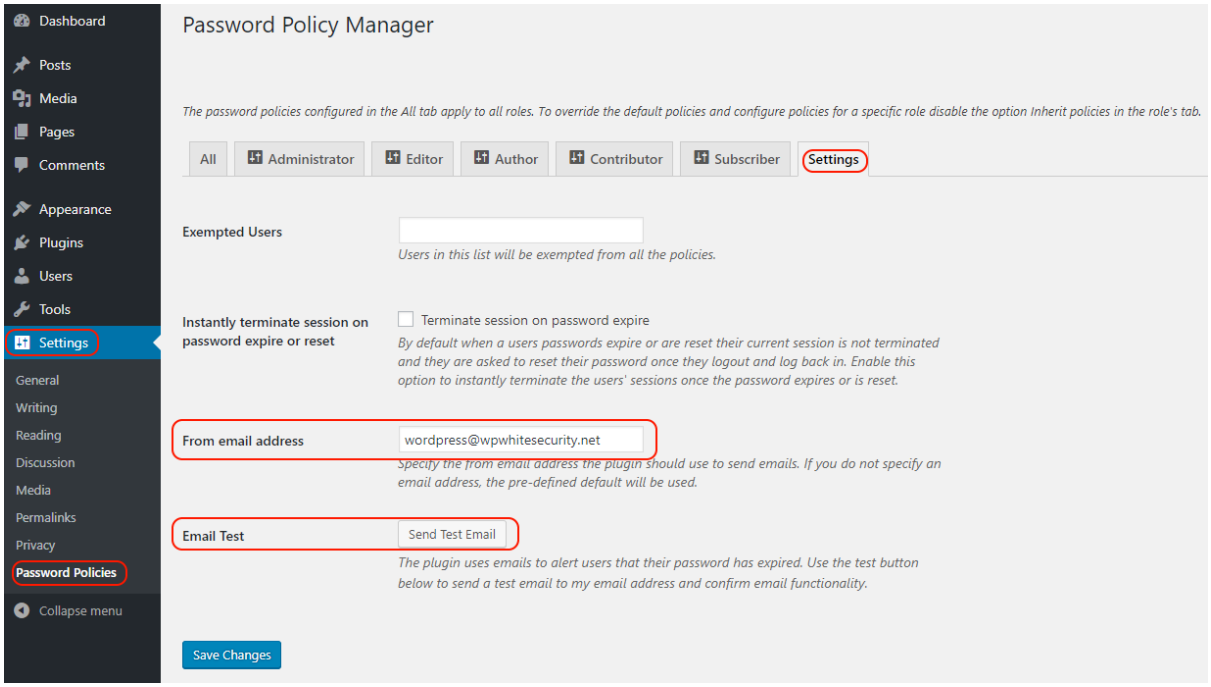
The first time you install the plugin a dialogue pops up highlighting from where you can configure the password policies.



Dismiss the notification and click on **Settings** and **Password Policies** to configure the policies. By default, all the password policies are disabled.

Before anything else - test the setup

Password reset notifications are sent over email. So before you configure any policies confirm that the plugin can send emails.

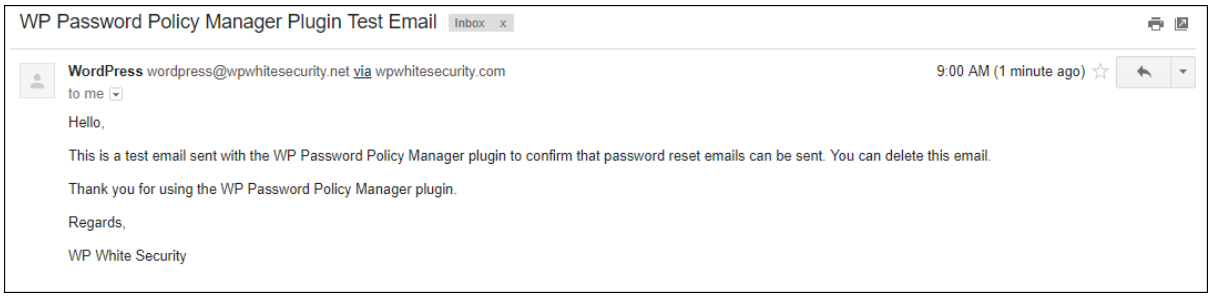


To confirm the plugin can send emails:

1. Navigate to the **Settings** tab
2. Confirm that the **From email address** is correct. This is the email address the plugin will use as a from address.

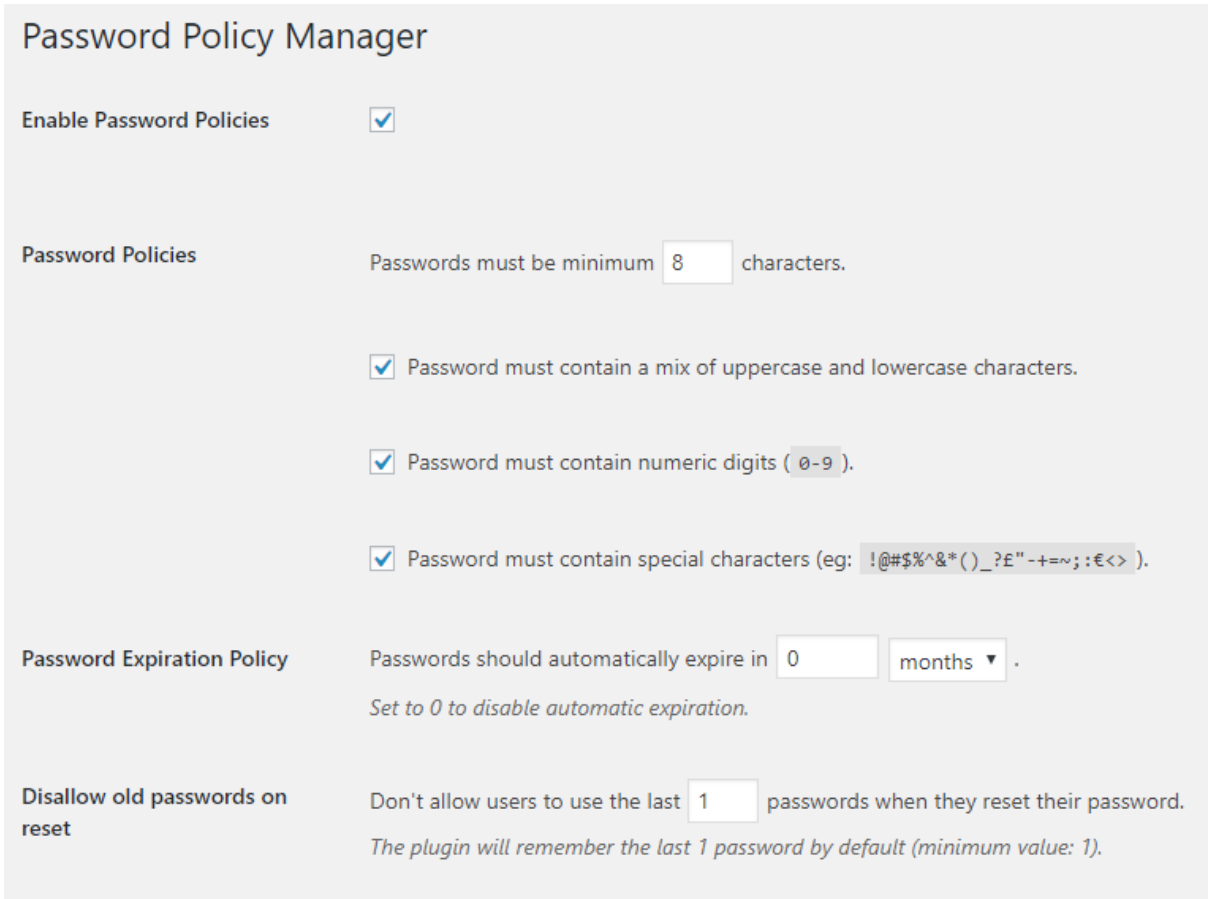
3. Click **Send Test Email**

The test email will be sent to the email address configured for your logged in user. So if you are logged in as user *rubyrobin* and your email address is *support@wpwhitesecurity.com* the test email will be sent to *support@wpwhitesecurity.com.*



Configuring the password policies

To enable and configure the password policies navigate to the **All** tab, tick the setting **Enable Password Policies** and check the check box next to the policy you'd like to enable. If need be also specify a value. Below is an explanation of the different password policies you can configure and their default values.



Minimum password length: use this setting to specify the least number of characters a WordPress password should have. Default value is *8*.

Upper and lower-case policy: enable this option to enforce users to use both lower and UPPER-case letters in their passwords.

Numeric digits policy: enable this option to enforce users to use numeric digits in their passwords.

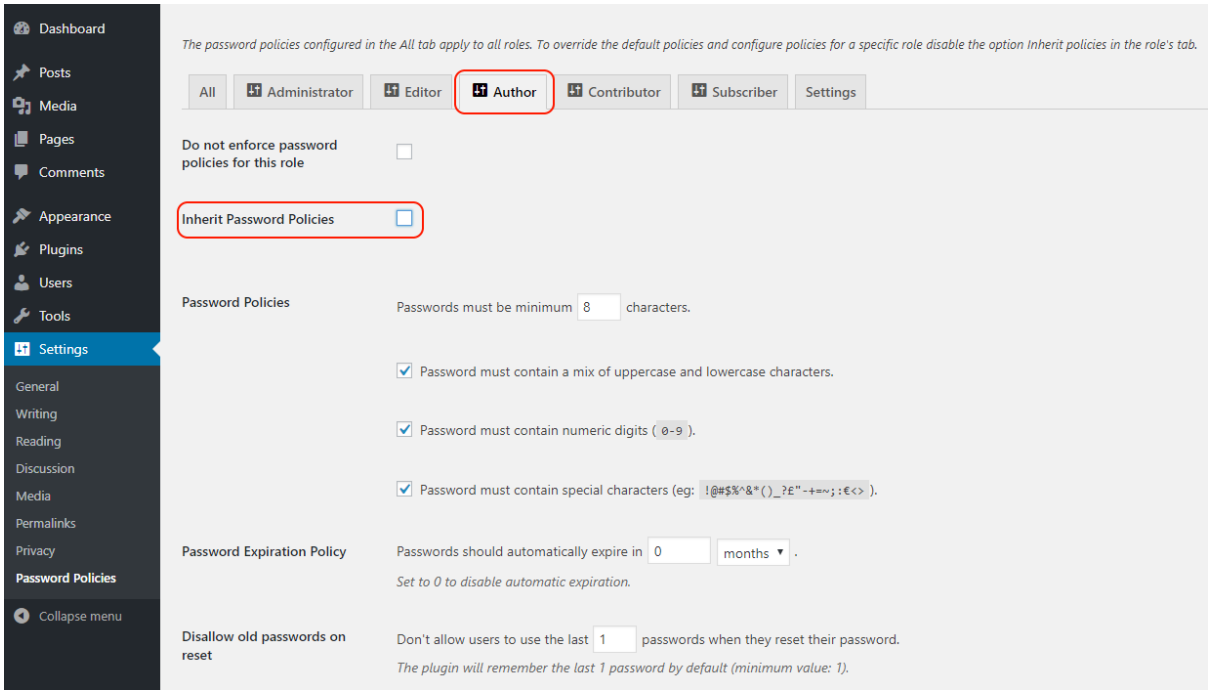
Special characters policy: enable this option to enforce users to use special characters in their passwords.

Password expiration policy: use this option to specify the lifetime of a password in days, weeks or months. When the password expires the user must change it. Default value is *0*, which means passwords won't expire.

Old passwords policy: use this option to specify how many passwords the plugin remembers so users do not use the same password. Default value is *1*, which means the user cannot use the same password he had last.

NOTE: Always click the **Save Changes** button at the bottom to save any configuration changes.

Configuring different password policies for different user roles



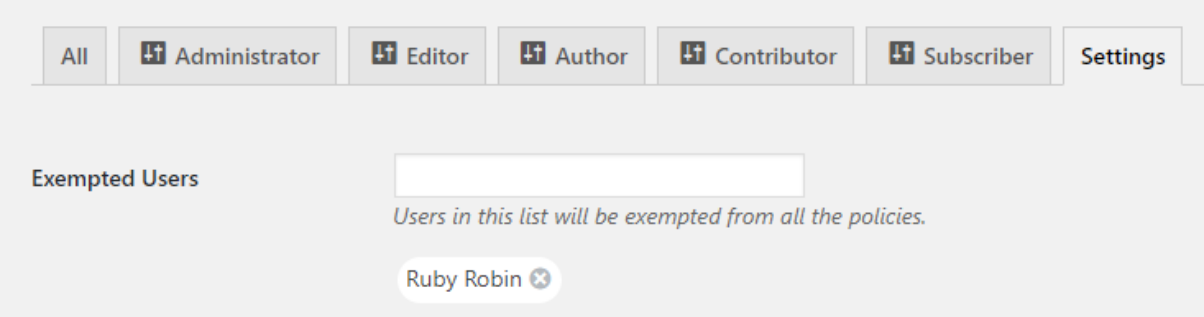
By default the password policies configured in the **All** tab apply to all the user roles. You can disable the inheritance of the *generic* policies and configure specific policies for a specific role by:

1. Navigating to the role's tab
2. Disable the option **Inherit Password Policies**
3. Proceed to configure the desired policies and save the changes.

Password policies settings

All the plugin settings are in the **Settings** tab.

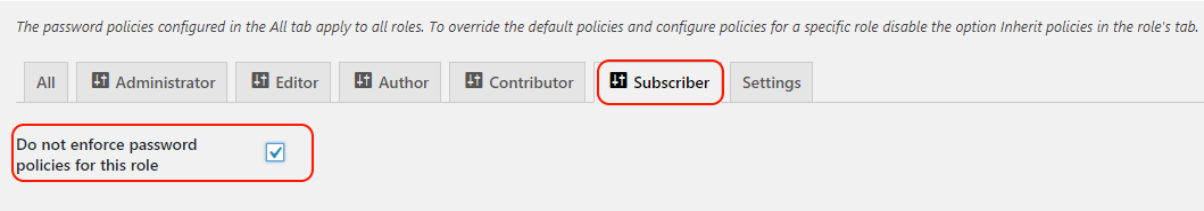
Exempting users from the policies



You can exempt users from the password policies by adding them in the setting **Exempted Users**. For example, in the screenshot above we are exempting the user *Rubyrobin.*

Click **Save Changes** to save the exemptions.

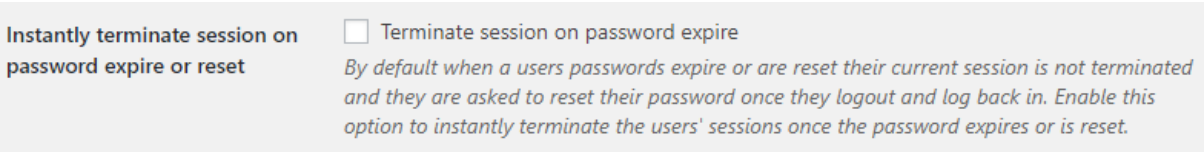
Exempting users with a specific role from the policies



You can also exempt all the users with a specific user role from the password policies. To do this:

1. Navigate to the role's tab
2. Enable the option **Do not enforce password policies for this role**.
3. Click **Save Changes** to save the new settings.

Controlling user sessions terminations on password expire



By default, when passwords expire users' session are not terminated instantly because this could result in unsaved work. The users are asked to reset their password the next time they login after they logout their existing session.

Though you can instantly terminate sessions upon password expiry by enabling the option **Terminate session on password expire** shown in the above screenshot.

NOTE: Always click the **Save Changes** button at the bottom to save any configuration changes.

Using a custom login page? Integrate the plugin

If you are using a custom login / password reset page on your WordPress website then you need to use a *hook* in our plugin to call our plugin so it displays and enforces the policies on your custom password reset and login page.

The Hook code example

Below is the code for the hook:

```
function example_ppm_enable_custom_form( $args ) {
        $args = array( 'element' => '#custom_password, #password',  );
        return $args;
}
add_filter( 'ppm_enable_custom_form', 'example_ppm_enable_custom_form' );
```

How to use the Hook

To integrate the hook simply add the above code to your site's *functions.php* file or to the custom password reset page.

Refer to the functions.php documentation for more information on this file.

Support and contact information

At WP White Security we pride ourselves of developing high quality plugins and provide excellent support.

In case of queries or if you require any assistance, you can contact us by sending us an email on support@wpwhitesecurity.com.

Password Policy Manager for WordPress is developed by WP White Security, the authors of the most comprehensive and widely used WordPress activity log plugin, WP Security Audit Log.