

Sitelok Password Security Plugin



V1.6

Sitelok Password Security Plugin

Copyright 2012-2021 Vibralogix. All rights reserved.

This document is provided by Vibralogix for informational purposes only to licensed users of the Sitelok product and is provided on an 'as is' basis without any warranties expressed or implied.

Information in this document is subject to change without notice and does not represent a commitment on the part of Vibralogix. The software described in this document is provided under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software except as specifically allowed in the license.

It is the users responsibility to ensure the suitability of the product before using it. In no circumstances will Vibralogix be responsible for any loss or damage of data or programs as a result of using the product. Your use of the product implies acceptance of these terms.

Contents

Chapter 1 Introduction	4
What is the Sitelok Password Security plugin?	4
Chapter 2 Installation	5
Installing for the first time or upgrading	5
Disabling the Plugin	5
Uninstalling the plugin	5
Chapter 3 Using the plugin	6
Password Format	6
Valid characters	6
Minimum length	6
Maximum length	7
Required lowercase characters	7
Required uppercase characters	7
Required numbers	7
Required other characters	7
Override password mask	7
Invalid password message	7
Incorrect password action	8
Incorrect entries allowed	8
Attempts left message	8
Account locked message	9
User email template	9
Admin email template	9
Password Renewal	9
Password reuse	10
Reused password message	10
Force password renewal after	10
Change password on first login	10
Change non user password	11
Password change page	11
Translating English text	11
Chapter 4 Support	12

Chapter 1 Introduction

What is the Siteelok Password Security plugin?

The Password Security plugin adds a number of options for controlling the type and use of passwords within Siteelok. Features include

- Control over the characters allowed in the password
- Setting of minimum and maximum password length
- Setting password format such as requiring a minimum of character types (uppercase, lowercase, numeric or other symbols).
- The ability to lock an account for a fixed period or permanently (for admin review) after an incorrect password is entered a certain number of times.
- Stop the reuse of previously used passwords
- Force users to renew password after a period of time

Chapter 2 Installation

Installing for the first time or upgrading

- 1) Extract the contents of the zip file to your PC.
- 2) Upload the plugin_pwsec folder to your existing Sitelok slpw folder using FTP. There are no special permissions required on most servers.
- 3) Login to the Sitelok control panel.
- 4) Open the following URL in the browser

http://www.yoursite.com/slpw/plugin_pwsec/install.php

which will start the installation process. If all is well you will be taken to the plugin preferences page where you will see the plugin listed.

If you have any problems with installation please let us know so that we can help you.

Disabling the Plugin

To disable the Password Security plugin select **Plugin Preferences** in the **Plugin** menu option of Sitelok. Uncheck the enable box for the plugin and click the **Save** button. You can enable it again in the same way.

Uninstalling the plugin

To permanently remove the plugin and its settings follow these steps.

- 1) Disable the plugin as above.
- 2) Click the delete icon next the plugin in the disabled plugins section.
- 3) Confirm the action in the alert box.

If the plugin is uninstalled successfully you will be returned to the plugin preferences page.

Chapter 3 Using the plugin

Click the Password Security option in the Plugins menu to display the settings page. This is split into three sections. Remember to click the **Save** button at the bottom of the page to save any changes.

Password Format

This section allows you to define the format of passwords. This includes the length valid characters and also whether the password should contain a minimum number of certain character types (lowercase, uppercase, numbers or symbols).

Password Format

This section allows you to define the minimum requirements for the password. This includes the minimum length and types of characters required in the password. There is also an option to force the global random password mask to match the settings here too.

Valid characters

Minimum length

Maximum length

Required lowercase letters

Required uppercase letters

Required numbers

Required other characters required number of non alphanumeric characters from the valid list

Override password mask? if checked then random passwords generated by Sitelok will also use the above format

Invalid password message

Valid characters

This lists the characters that you wish to allow in passwords. You can include any of the following.

0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
WXYZ!@#\$%^&*()-_+=:;,./<>{}|~`?

Minimum length

This sets the minimum length for passwords. Sitelok has a global minimum of 5 characters so you can set between 5 and 50.

Maximum length

This is the maximum length for passwords between 5 and 50 characters.

Required lowercase characters

Sets the minimum number of lowercase characters required in the password.

Required uppercase characters

Sets the minimum number of uppercase characters required in the password.

Required numbers

Sets the minimum number of numeric characters required in the password.

Required other characters

Sets the minimum number of other characters required in the password.

Override password mask

If you check this setting then the random passwords generated by Sitelok will use the format defined above (excluding other characters) instead of being based on the global mask set in the main Sitelok configuration.

Invalid password message

This is the message that is displayed to users if a chosen password does not meet any of the conditions set.

Incorrect password action

This section defines what action to take if a user enters an incorrect password during login. You can choose to ignore this, block access to the account for a fixed period of time or lock the account for admin review.

Incorrect password action

Here you can set a limit on the number of password attempts a user can make before getting their account blocked for a period of time or for admin review. Both the user and admin can be emailed when an account is blocked.

Incorrect entries allowed	<input type="text" value="No limit"/>	Allows you to block access if the password is entered incorrectly
Attempts left message	<input type="text" value="Incorrect password. You have !!!attemptsleft!!! left"/>	Wrong password message for user. Use !!!attemptsleft!!! to display number of attempts left.
Action to take	<input type="text" value="Block access for 10 minutes"/>	If you set anything apart from No Limit you can choose to either block access permanently or for a period of time.
Account locked message	<input type="text" value="Your account is locked for !!!lockedtime!!!"/>	Account locked message for user. Use !!!lockedtime!!! to display locked time left if required.
User email template	<input type="text" value="Don't email the user"/>	Email template to send to the user if their account is blocked
Admin email template	<input type="text" value="Don't email admin"/>	Email template to send to the admin when an account is blocked

Incorrect entries allowed

This sets the number of incorrect password entries before action is taken. You can set this to between **1** and **5** attempts or **No Limit** to disable it.


Attempts left message

This is the message displayed to the user when they enter an incorrect password. If you wish to include the number of attempts left in the message then use **!!!attemptsleft!!!** in the text as a place holder. For example

Incorrect password. You have !!!attemptsleft!!! attempts left

You can use simple html in the message but please use ' instead of " if needed.

Action to take

This defines what action to take after the user has entered the password incorrectly the set number of times. You can either lock the account for a period between 3 minutes and 24 hours or permanently requiring the admin to unlock the account. If a user is locked the admin can unlock them at any time fro the Sitelok control panel. Just login and click the  icon next to the user. This will display a page where you can see the time left (for temporary locking) and check a checkbox to unlock the account immediately.

Account locked message

This is the message a user sees when their account has been locked. If you have used a temporary lock you can include the time left in the text by using `!!!lockedtime!!!` as a placeholder. For example

Your account is locked for `!!!lockedtime!!!`

You can use simple html in the message but please use ' instead of " if needed.

User email template

You can if you wish select an email template to be sent to the user when their account is locked. This is useful to warn the user of possible attempts by a third party to access the account.

Admin email template

You can if you wish select an email template to be sent to the admin when a users account is locked.

Password Renewal

This section allows you to force users to change their password after a set period and also controls the reuse of previous passwords. Only a secure seeded hash of the users previous passwords are stored in the database for security.

Chapter 3 - Using the plugin

Password Renewal

For added security it is a good idea to stop users from using the same password all of the time. You can force the user to use a new password after a period of time and also stop them reusing old passwords.

Password reuse Previous passwords can be used

Reused password message

Force password renewal after

Change password on first login? If checked then a new user is forced to change the password the first time they login

Change non user password? If checked then a user is forced to change the password if it has been set via password reset or admin etc

Password change page

This should be the absolute path such as /members/updated.php. Don't include the http://www.yoursite.com part.

Password reuse

This setting determines whether a user can reuse an old password again or not. If you are going to force users to renew their passwords you should at least stop them reusing the current password.

Reused password message

This is the message displayed to the user when they enter a new password that has been used before.

You can use simple html in the message but please use ' instead of " if needed.

Force password renewal after

You can set the maximum period a user is allowed to use a password before being forced to change it. If a user has not changed their password for longer than this period they will be redirected to a designated page after login where they can change the password. No other pages will be accessible until the password is changed.

Change password on first login

If checked this will force users to change their password the first time they login. This feature is only active if you have also enabled a forced password change renewal period.

Change non user password

If checked this will force users to change their password whenever they have been changed by the admin, password reset process or other times where the user did not directly enter their own new password. This feature is only active if you have also enabled a forced password change renewal period.

Password change page

This is the page users will be redirected to after they login when they are forced to change their password. It should be the path to the page without the `http://yoursite.com` part of the URL For example

[/members/update.php](#)

No other page will be accessible until they have changed the password.

Normally you would use an update profile form on this page allowing the user to change their password.

You can optionally set the thankyou page for the form in the designer to this special variable to have the user return to the last page accessed.

`!!!pwseclastpage!!!`

Translating English text

If you want to change or translate the English text seen by users then you can do so by adding these lines to your `slconfig.php`. Other text can be changed in the plugin settings.

```
define("MSG_PWSTOKEN_DAYS", "days");
define("MSG_PWSTOKEN_HOURS", "hours");
define("MSG_PWSTOKEN_MINUTES", "minutes");
define("MSG_PWSTOKEN_SECONDS", "seconds");
```

Chapter 4 Support

Hopefully if you have followed this manual carefully everything will be working fine. However sometimes things don't go quite so smoothly so if you have any questions or problems then please check the FAQ on the support page or email us.

Support area: <http://www.vibralogix.com/support/>

Email: support@vibralogix.com