

Sitelok 2FA Plugin

for Google authenticator and Authy



V1.0

Sitelok 2FA Plugin

Copyright 2020 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 2FA plugin?	4
How does it work for users	4
Chapter 2 Installation	6
Installing for the first time or upgrading	6
Disabling the Plugin.....	6
Uninstalling the plugin	6
Setting up & using the plugin	7
Settings.....	7
Enable or disable 2FA for a user	9
Enable or disable 2FA for selected users	10
Allowing a user to enable or disable 2FA	10
Chapter 4 Support	11

Chapter 1 Introduction

What is the 2FA plugin?

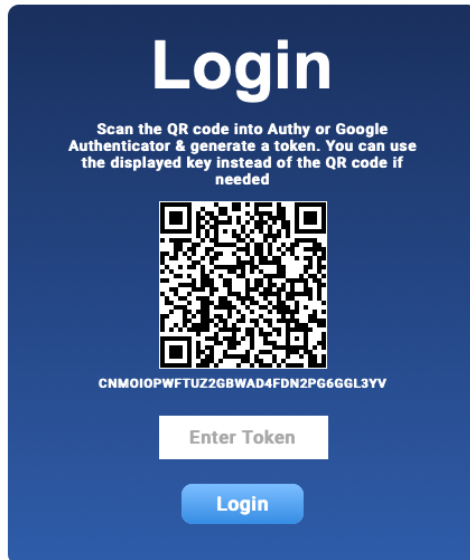
The 2FA plugin provides an extra login level after a user has entered their username and password. A 6 digit single use code is generated using Google Authenticator or Authy apps on the users smartphone (Authy also have versions for macOS, Windows and Linux as well).

Other apps that can generate TOTP 6 digit codes that change every 30 seconds may also be compatible.

The plugin can be setup to require 2FA login for specific usergroups or you can allow users to enable or disable 2FA as required.

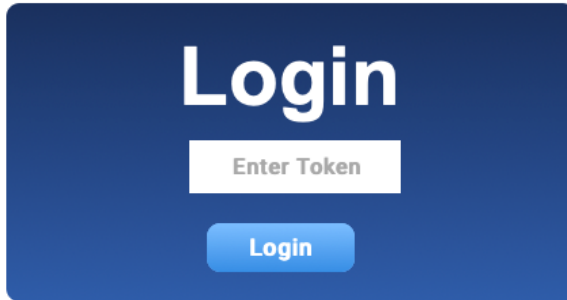
How does it work for users

When a user logs in for the first time they will enter their username and password as usual. After this they will see another login form similar to this one.



The user will need to scan the QR code (or manually enter the key) into Google Authenticator or Authy and enter the 6 digit token.

For subsequent logins the user will login with their username and password as usual and then see this login form where they enter the 6 digit code displayed in the app. Its easy and very secure.



A login form with a dark blue background. At the top, the word "Login" is written in large white font. Below it is a white rectangular input field with the text "Enter Token" in grey. At the bottom is a blue rounded rectangular button with the word "Login" in white.

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_2fa 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

https://www.yoursite.com/slpw/plugin_2fa/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 2FA 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 it's 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.

Setting up & using the plugin

Settings

You can access the plugin configuration by selecting **2FA** from the **Plugins** menu.

Settings

Incorrect entries allowed

Allows you to block access if the wrong token value is entered

Action to take

Send user an email when blocked (select template)

Send admin an email when user blocked (select template)

Help page URL (optional)

The help button on the new token login form will point to this page.

Incorrect entries allowed

Set how many times a user can enter an incorrect token before the login is blocked.

Action to take

Here you can set what action to take after the incorrect token entries. You can either block the login for a period of time or block the login permanently, requiring the site admin to unlock it.

Send user an email when blocked

You can optionally have an email sent to the user when their login is blocked. Check the box to enable this and select the email template to use.

Send admin an email when blocked

You can optionally have an email sent to the site admin when a user login is blocked. Check the box to enable this and select the email template to use.

Help page URL

You can enter an optional URL to a page where you explain further about the 2FA login process. The link is used on the 2FA login box the first time a user logs in (when the QR code is displayed).

Leave blank if you don't need this.

Apply to usergroups

In this section you can force the use of 2FA login for specific usergroups.

Set 'No usergroups' if you want to assign 2FA for specific users or if you want to allow users to choose to use it.

Apply to usergroups

Here you can force members of certain usergroups to use 2FA. Please note that only usergroups setup in the Usergroups section will work with 2FA. Any usergroups already linked to another login plugin will not be affected. You can override the usergroup setting for specific users.

Apply to usergroups

No usergroups. 2FA is assigned to specific users ▼

Select users

This section allows you to select users who have been specifically assigned the a login method. Please note that this will not select users which use 2FA based only on a usergroup requirement.

Select users

You can use the select button below to select users who have been **specifically** assigned a login method.

Please note that this will deselect any existing selected users.


Select users who have been specifically assigned the 2FA login method

Select users who have been specifically assigned the normal (user/pass) login method)

Select users who have been specifically assigned any login method

Select

Enable or disable 2FA for a user

You can manually change a users login method. To do this click the down arrow next to the user in the dashboard table and click  2FA.

Apply login method

- Use 2FA login method
- Use 2FA login method & reset any existing key (require new QR code)
- Use the login method defined by group membership
- Use the normal (user/pass) login

Use 2FA method

Select this option to force the user to use 2FA. If they have used it previously the same key will be used.

Use 2FA method & reset ny existing key

Select this option to force the user to use 2FA. If a user has already used 2FA before the key will be reset so that a new QR code is generated on the first login.

Use the login method defined by the group membership

Select this option so that the users uses the default login method assigned to the usergroup.


Use the normal (use/pass) login

Select this option to force the user house the standard non 2FA username and password login method.

Check box to unlock

When a user enters the wrong token too many times (as set) they will be locked out for a period of time or permanently. In this case you will see a checkbox to unlock the user.

Enable or disable 2FA for selected users

You can also select multiple users to set them to use 2FA. To do this select the users and click the More button above the dashboard table. Click the  2FA Selected option.

Allowing a user to enable or disable 2FA

Many sites may require users to use the 2FA login method but you may alternatively allow users to enable/disable 2FA themselves. This can be done using a link on a members page.

Enable 2FA

The link will automatically display 'Enable 2FA' or 'Disable 2FA' as appropriate. The code for this link is generated for you automatically and you can change the link text displayed etc. To access the snippet generator go to [Plugins - 2FA](#) - and click the [Snippets](#) button.

Adjust the settings as required and click the [Copy to Clipboard](#) button. You can then paste the snippet on your page.

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: <https://www.vibralogix.com/support/>

Email: support@vibralogix.com