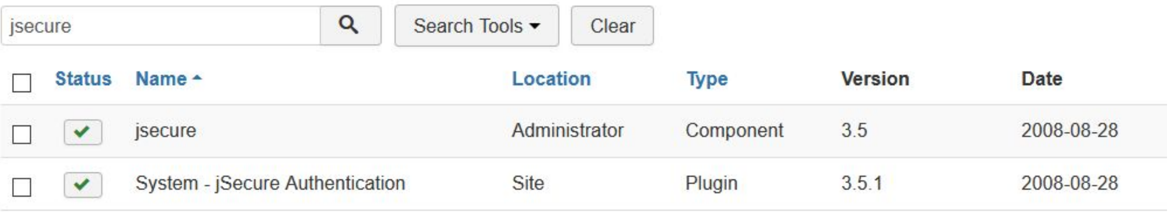
JSECURE AUTHENTICATION

Joomla! has one drawback, any web user can easily know the site is created in Joomla! by typing the URL to access the administration area (i.e. www.sitename.com/administrator). This makes hackers hack the site easily once they crack the id and password for Joomla!

INSTALLATION

1. Unzip the package file Unzip first which contains different zip packages for different Joomla! versions.
2. Navigate to extensions > manage > install and then open the upload package file tab
3. Choose the zip package file present in Unzip first according to Joomla! version from the browse button.
4. Then it will start installation of jsecure on your website. The plugin is automatically enabled upon installation but still you can verify if the plugin is enabled by navigating to extensions > manage and search for jsecure. You should see a screen as below.



□	Status	Name ▴	Location	Type	Version	Date
□	✓	jsecure	Administrator	Component	3.5	2008-08-28
□	✓	System - jSecure Authentication	Site	Plugin	3.5.1	2008-08-28

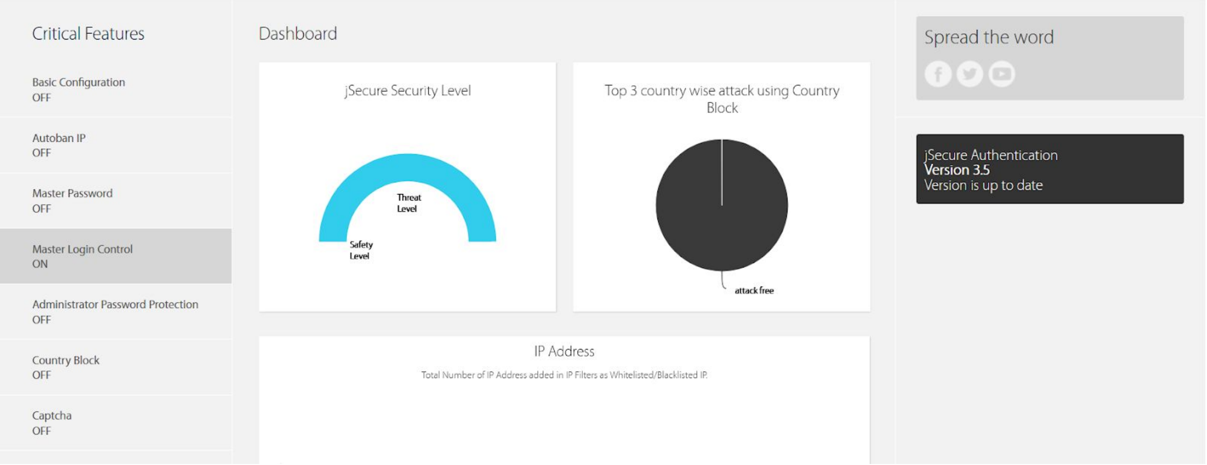
UNINSTALLATION

1. To uninstall the extension you need to navigate to extensions->manage.
2. Search for jsecure then you will find a plugin and a component. Select both and click on uninstall this will uninstall the extension from the system.

USAGE

To configure the plugin you have to use the jsecure component which you can find by navigating to components > jsecure authentication. Here is the dashboard of the plugin which gives you analysis of your website security

JSECURE AUTHENTICATION



Critical Features

Basic Configuration
OFF

Autoban IP
OFF

Master Password
OFF

Master Login Control
ON

Administrator Password Protection
OFF

Country Block
OFF

Captcha
OFF

Dashboard

jSecure Security Level

Top 3 country wise attack using Country Block

IP Address

Total Number of IP Address added in IP Filters as Whitelisted/Blacklisted IP.

Spread the word

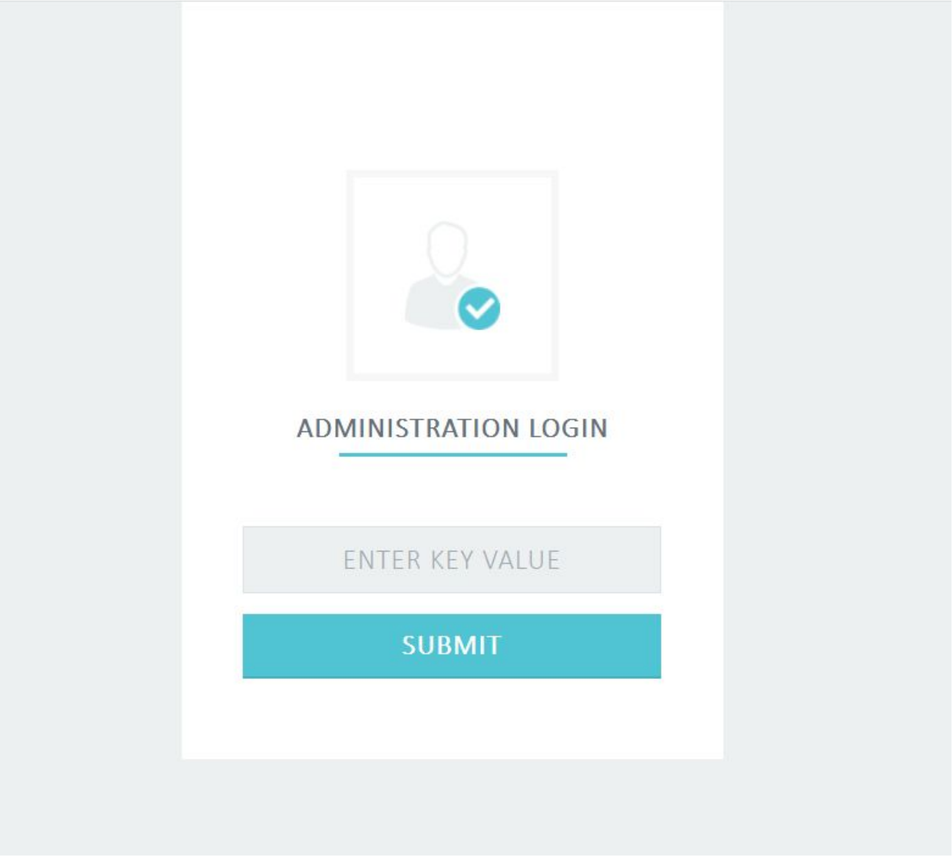
jSecure Authentication
Version 3.5
Version is up to date

We will now understand the features of this plugin and how you can configure this in detail.

Basic configuration

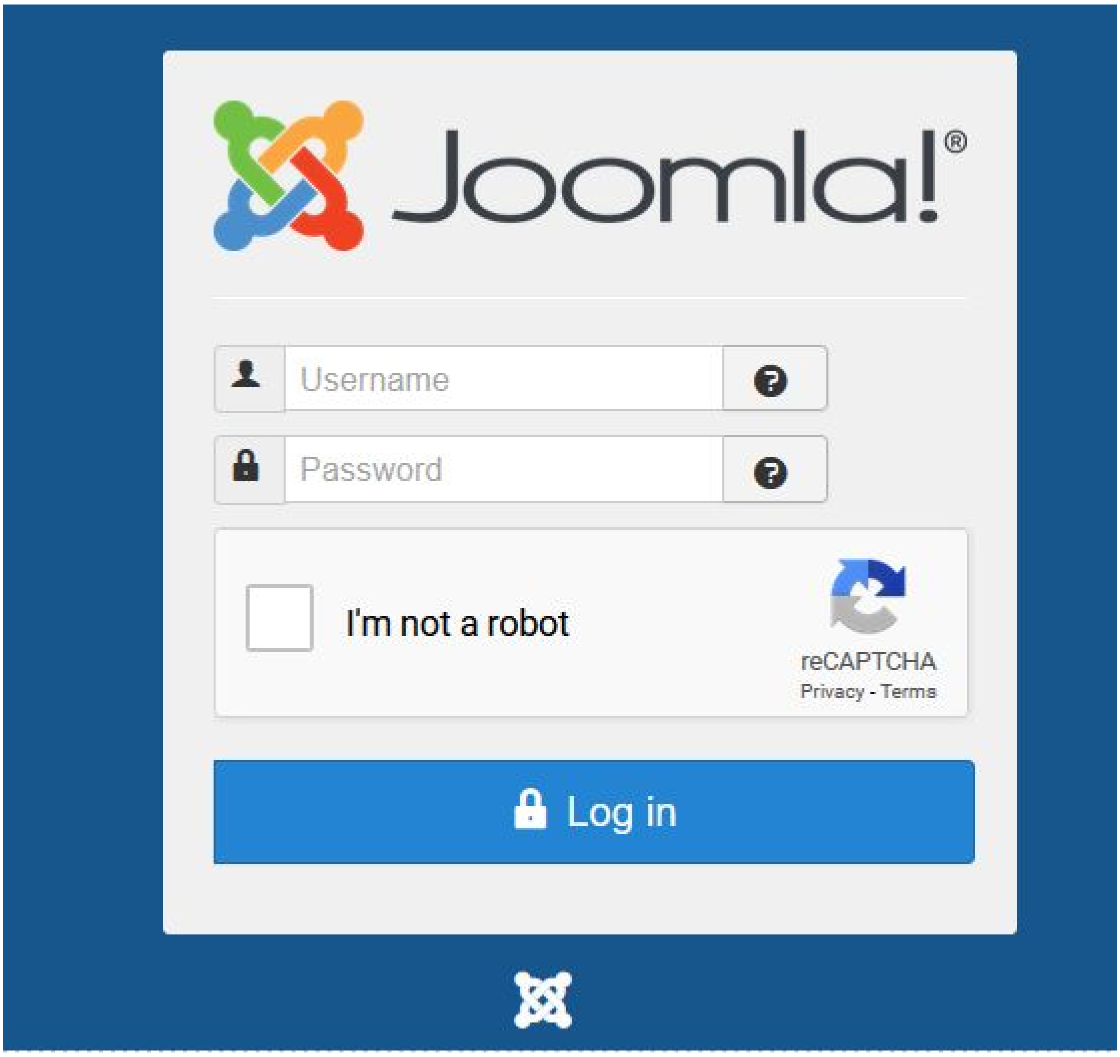
1) Enable Option - If you are facing some issue with jsecure you can quickly disable the whole extension by disabling this option.
2) Pass Key - There are two options through which you can protect the administration panel of joomla using jsecure.
    a) URL - If you select this option you will have to enter the key along with your administration url. For eg if you have set the passkey as jsp then while logging in to the administration section you have to type the following url http://example.com/administrator/?jsp.
    b) Form: If you enable this option you don't have to enter the key in the url but once you visit the administration url you will get a form to enter the key. This provides an additional layer of security to your administration panel.

JSECURE AUTHENTICATION

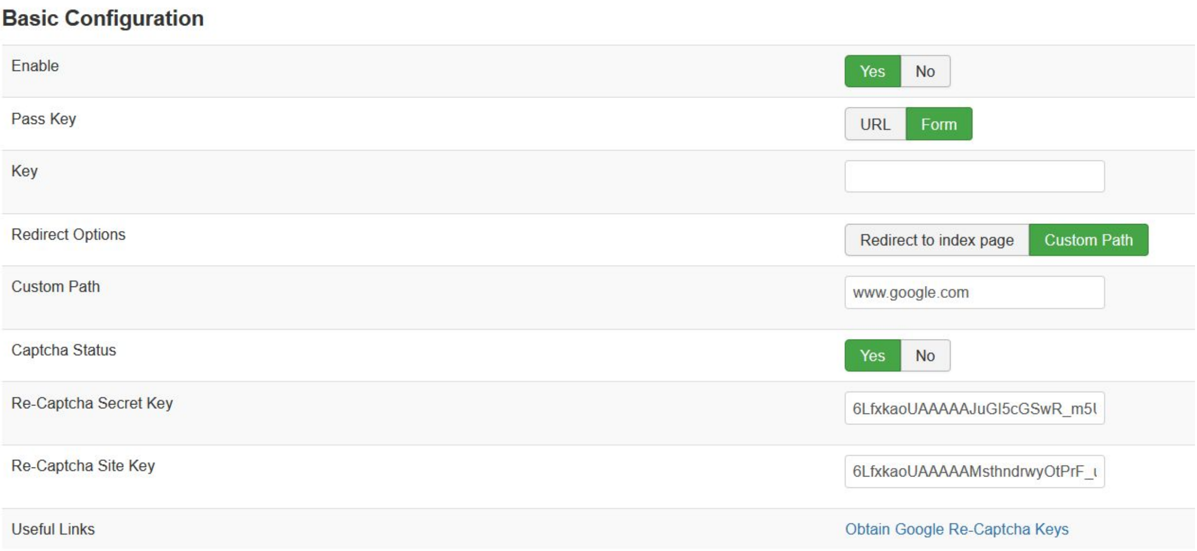


3) Key - Enter the key which you want to use for controlling the login. The key should be between 5 - 20 characters and should be hard to brute force. If you don't set a key by default it is set to jSecure.
4) Redirect Options -
    a) Redirect to index page - If the user enters a invalid key while accessing the backend the user will be redirected to the frontend of the website automatically.
    b) Custom Path: If you want to redirect the unauthenticated user to a custom path you select this option and enter the url of the page where you want to redirect the user.
5) Captcha Status: If you want to protect your backend login screen from spam bots you can enable this option to enable captcha on your website. The plugin only supports v2 of recaptcha so be sure to create recaptcha keys for v2 only. You can find more information here https://developers.google.com/recaptcha/docs/versions. Once you have created a v2 api key you have to make a note of recaptcha secret key and recaptcha site key and enter them inside of jsecure. This is the login screen after

enabling this feature.



Here is the basic configuration screen with all the options enabled.



Basic Configuration

Enable	[✓ Yes] No
Pass Key	URL [✓ Form]
Key	
Redirect Options	Redirect to index page [✓ Custom Path]
Custom Path	www.google.com
Captcha Status	[✓ Yes] No
Re-Captcha Secret Key	6LfxkaoUAAAAAJuGI5cGSwR_m5l
Re-Captcha Site Key	6LfxkaoUAAAAAMsthndrwyOtPrF_
Useful Links	Obtain Google Re-Captcha Keys

JSECURE AUTHENTICATION

IP Access Control

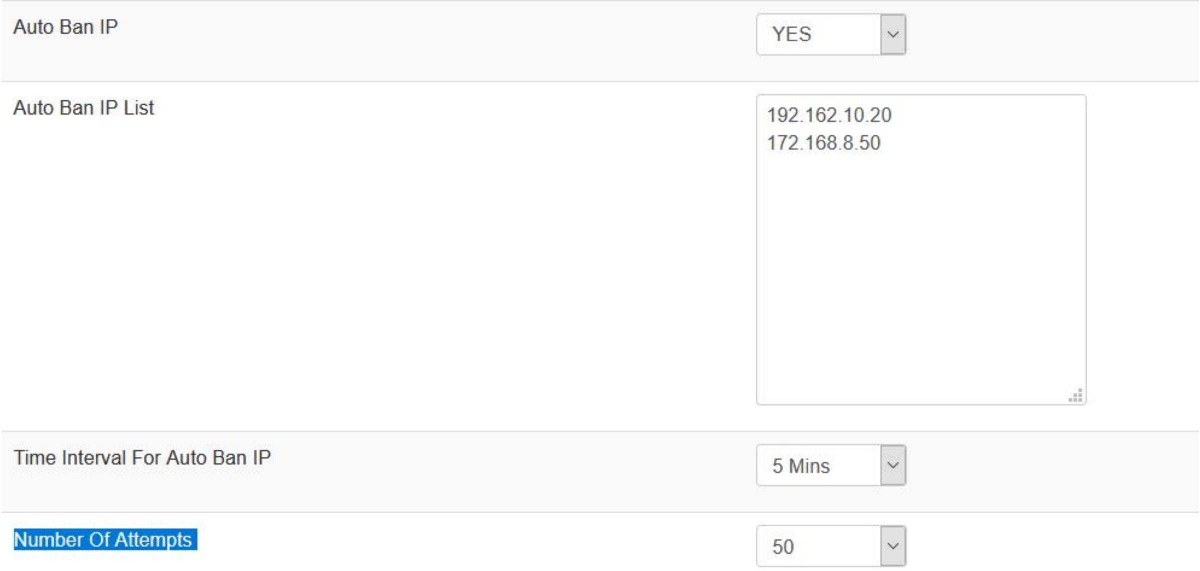
This screen provides you with two options to control access to your website.

AUTO BAN IP

This option allows you to automatically ban certain IP addresses based on the total number of login attempts. Here are the available fields.

1) Auto Ban IP List - Enter the IP address that you would like to ban . Enter each IP address on a new line without any spaces or any other special characters.
2) Time Interval For Auto Ban IP - Specify the time for which these IP addresses will be banned.
3) Number Of Attempts - Specify the number of attempts after which these IP addresses will be banned after.

Here is the complete configuration for this feature



Auto Ban IP	YES
Auto Ban IP List	192.162.10.20 172.168.8.50
Time Interval For Auto Ban IP	5 Mins
Number Of Attempts	50

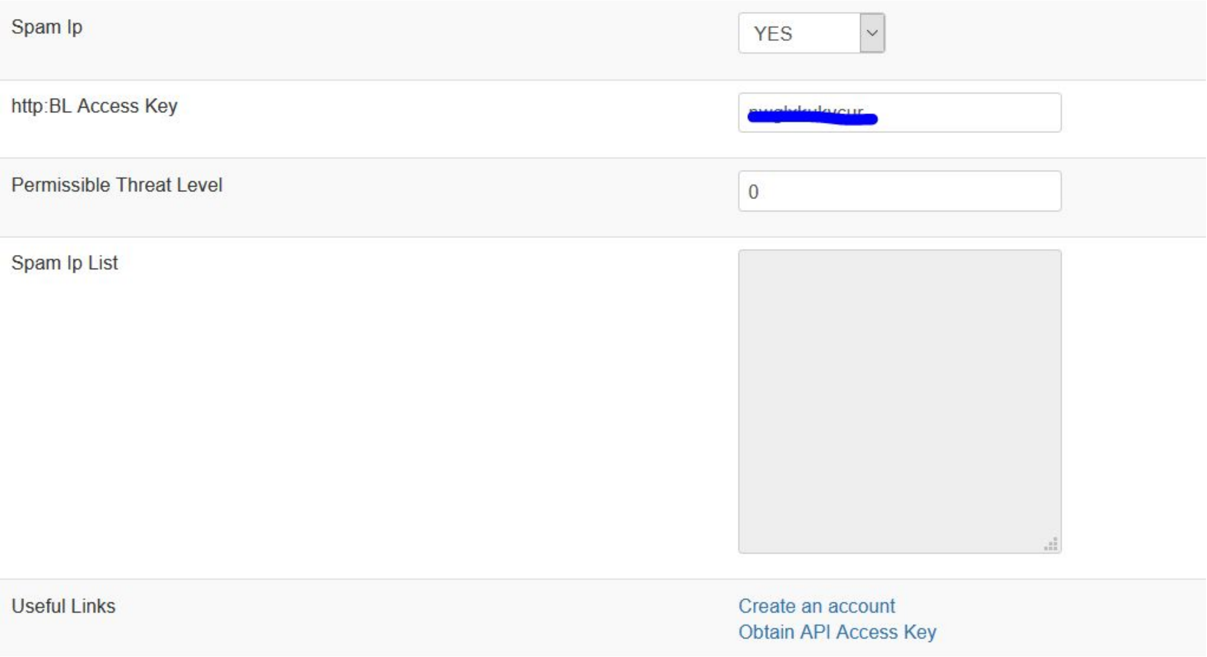
Here the IP addresses will be banned after 50 failed login attempts from the IP address for 5 minutes.

SPAM IP

This feature makes use of the Project Honey Pot which maintains a list of spam Ip addresses around the website and exposes them using an API.

JSECURE AUTHENTICATION

1) To start using these features you have to first register on their website http://www.projecthoneypot.org/create_account.php.
2) Then you can create a api access key using the following url http://www.projecthoneypot.org/httpbl_configure.php
3) Once you have created the api access key you can then fill in the fields as below



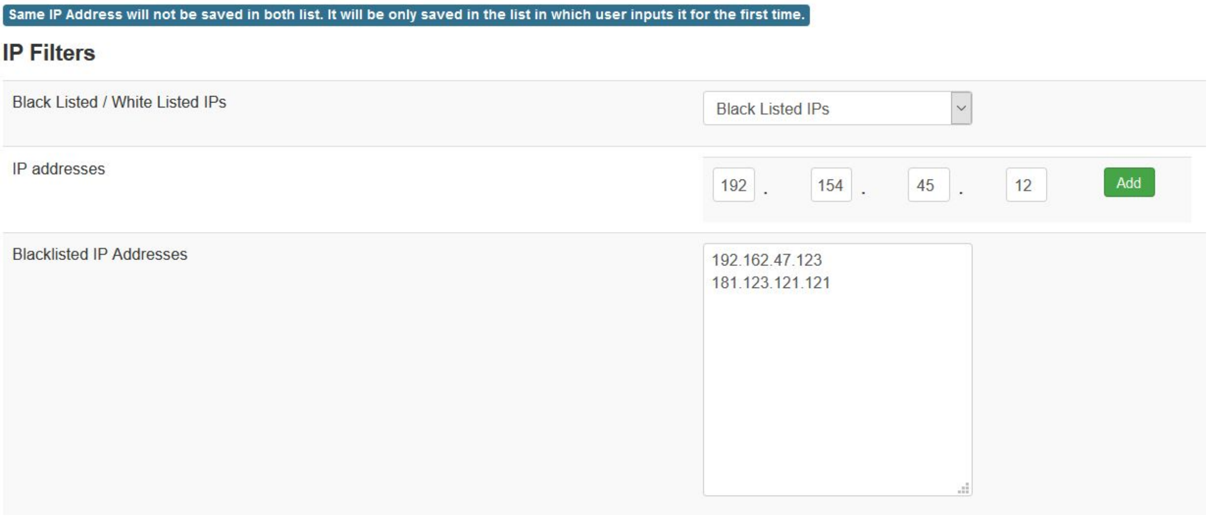
Spam Ip	YES
http:BL Access Key	[redacted]
Permissible Threat Level	0
Spam Ip List	
Useful Links	Create an account Obtain API Access Key

a) http:BL Access key - This is the access key which you have created on honey pot
b) Permissible Threat Level - Enter a value between 0 to 255. Project Honey Pot assigns a threat level for each IP which will be compared against the user-provided threat level. The threat level - '0' denotes lowest threat level & '255' denotes the highest threat level
c) Spam Ip List: This box displays a list of spam IP addresses trying to access the website and filtered out using the honey pot api.

IP FILTERS

This feature allows you to specify the list of whitelisted and blacklisted IP addresses for the website. This is a example configuration for the feature

JSECURE AUTHENTICATION



Same IP Address will not be saved in both list. It will be only saved in the list in which user inputs it for the first time.

IP Filters

Black Listed / White Listed IPs: Black Listed IPs

IP addresses: 192 . 154 . 45 . 12

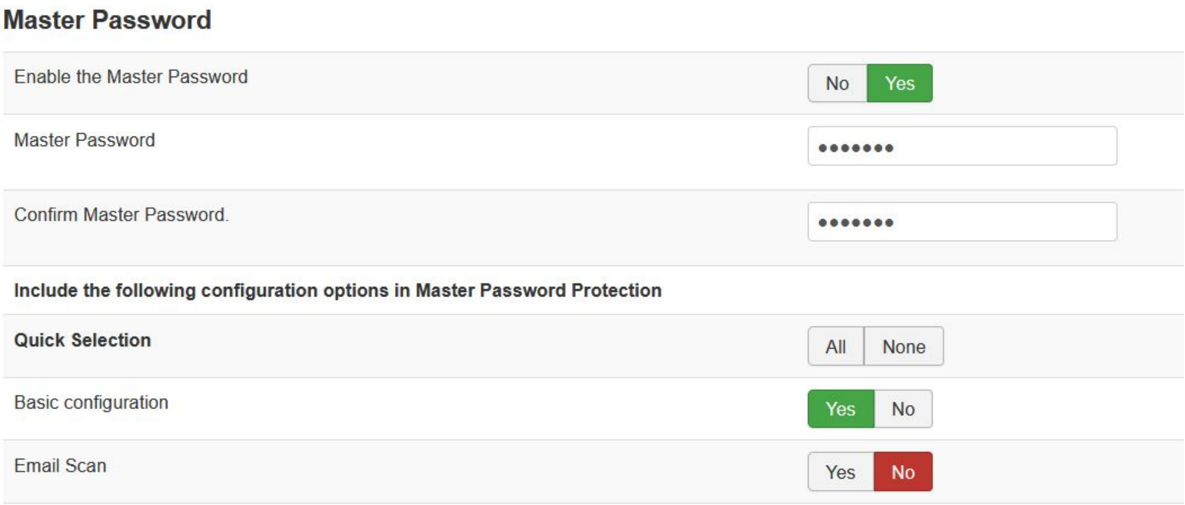
Blacklisted IP Addresses:
192.162.47.123
181.123.121.121

Here are the fields and their description

1. Black Listed / White Listed Ips - Specify if you want to blacklist or whitelist a IP Address.
2. IP addresses - Type the IP addresses and click on Add. This will add the IP addresses to the list based on the first option.
3. Blacklist IP Addresses/ White Listed IP Addresses - This will display a list of blacklisted or whitelisted IP addresses based on the first option.

MASTER PASSWORD

If you wish that certain configuration of jsecure should only be configured by certain users you can add a master password (additional password) to lock these configurations.



Master Password

Enable the Master Password: No [✓ Yes]

Master Password: •••••••

Confirm Master Password.: •••••••

Include the following configuration options in Master Password Protection

Quick Selection: All None

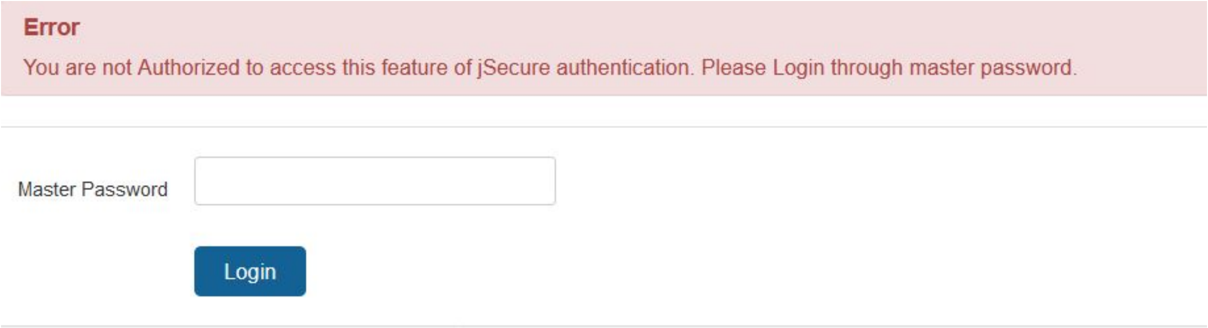
Basic configuration: [✓ Yes] No

Email Scan: Yes [✓ No]

In the above screen, we have enabled the master password protection for the basic configuration screen and not for the email scan component.

JSECURE AUTHENTICATION

Now if anyone tries to open the basic configuration screen he cannot see the component unless he enters the master password for it.



Error

You are not Authorized to access this feature of jSecure authentication. Please Login through master password.

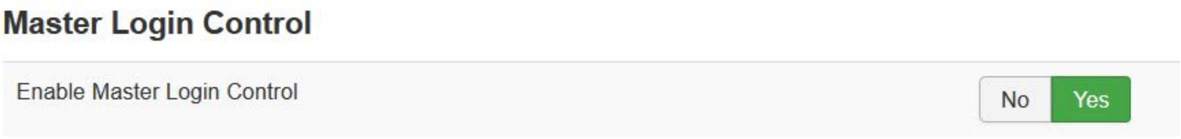
Master Password

Once, you enter the master password you will be able to access the screen. This feature would be more useful incase you have multiple administrators for the website.

MASTER LOGIN CONTROL

If you want to allow only one user to access the website at a time on a device then you can use the master login control feature for jsecure.

This feature does not have any other fields just enable the feature as shown below and you are good to go

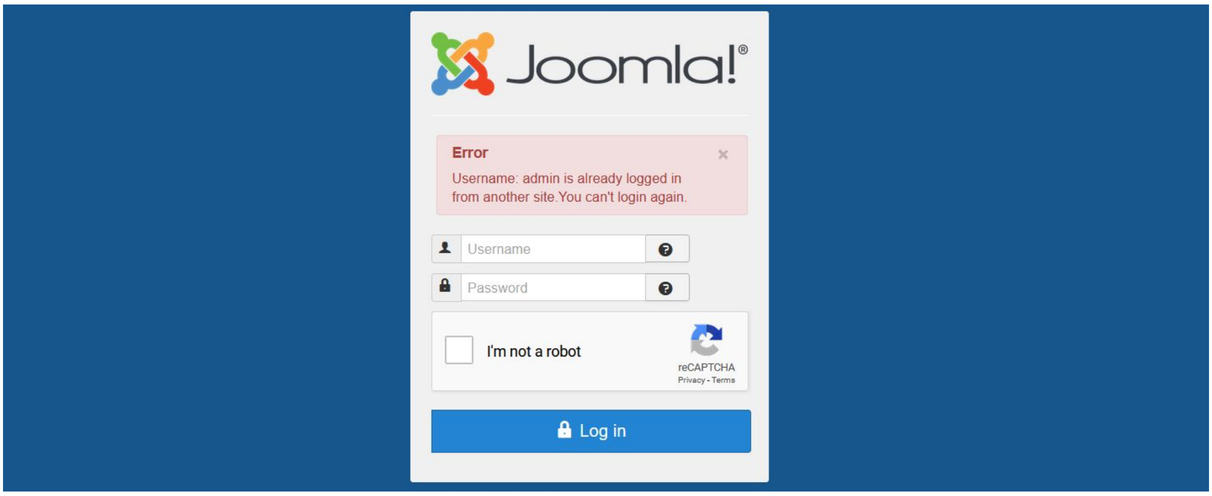


Master Login Control

Enable Master Login Control No [✓ Yes]

Now if you are logged in from a device and then if you try to login from another device you will get a message as below

JSECURE AUTHENTICATION



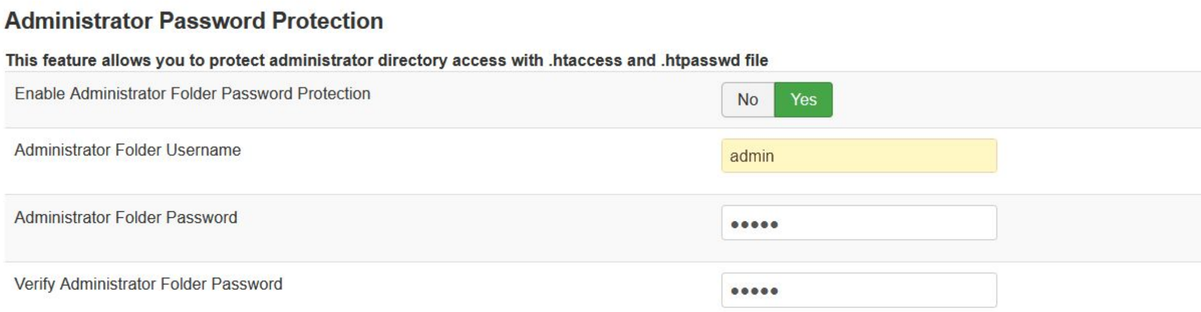
Error

Username: admin is already logged in from another site.You can't login again.

To login using the other device, you have to first logout from the first device.

ADMINISTRATOR PASSWORD PROTECTION

This feature allows you to generate a htaccess file which will protect the administrator url of your website.



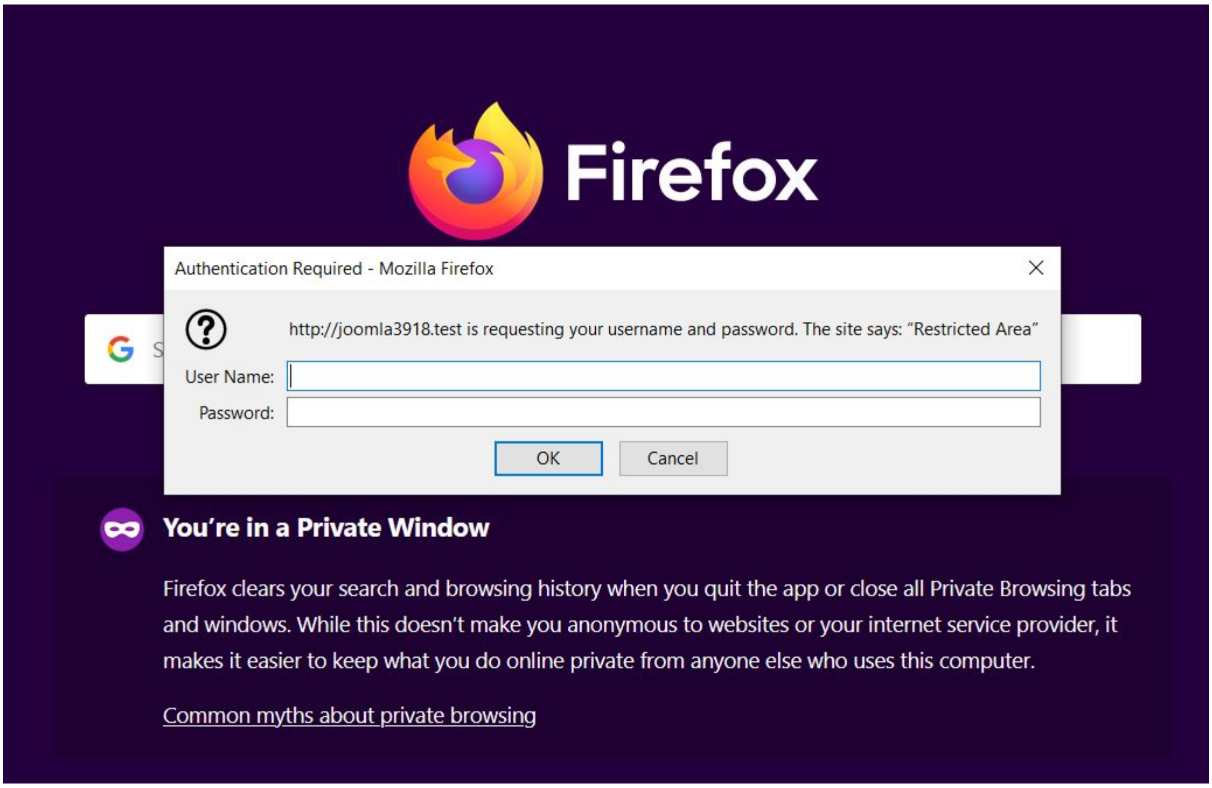
Administrator Password Protection

This feature allows you to protect administrator directory access with .htaccess and .htpasswd file

Enable Administrator Folder Password Protection	No [✓ Yes]
Administrator Folder Username	admin
Administrator Folder Password	●●●●●
Verify Administrator Folder Password	●●●●●

Once you have enabled the feature and filled in the above information, when you try to access your administrator url you will get a popup which tries to authenticate the user like this.

JSECURE AUTHENTICATION



Authentication Required - Mozilla Firefox

http://joomla3918.test is requesting your username and password. The site says: “Restricted Area”

User Name:

Password:

You’re in a Private Window

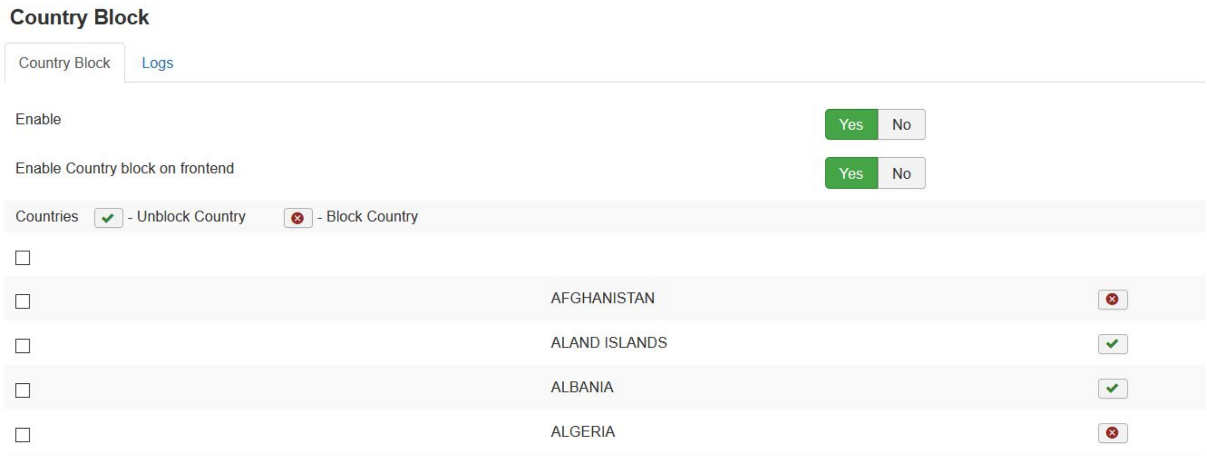
Firefox clears your search and browsing history when you quit the app or close all Private Browsing tabs and windows. While this doesn’t make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private from anyone else who uses this computer.

Common myths about private browsing

COUNTRY BLOCK

This feature of jsecure allows you to block certain countries from accessing your website. You can enable this option for the backend and optionally also for the frontend as shown below.

By default when you enable the feature all countries are unblocked you have to manually block countries.



Country Block

Enable: [✓ Yes] No

Enable Country block on frontend: [✓ Yes] No

Countries ✓ - Unblock Country ☒ - Block Country

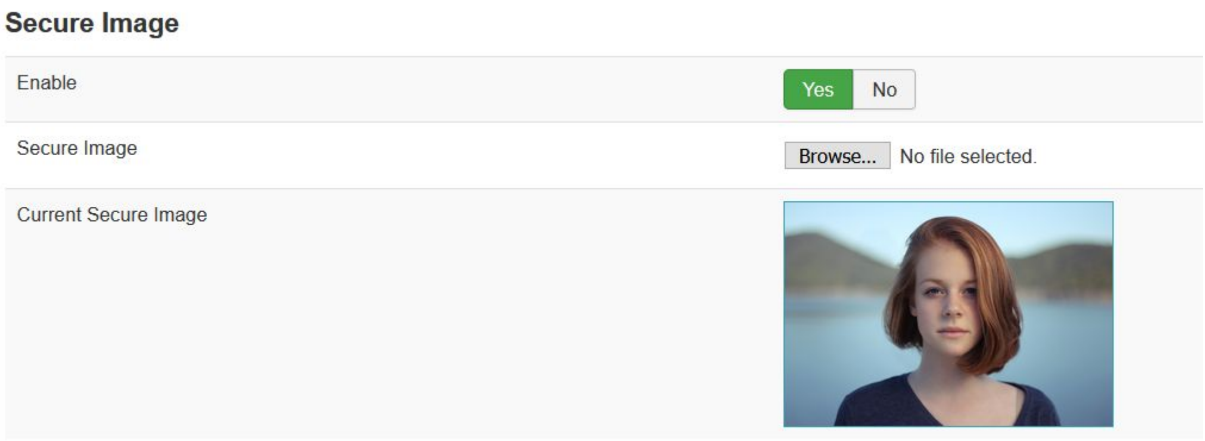
□		
□	AFGHANISTAN	☒
□	ALAND ISLANDS	✓
□	ALBANIA	✓
□	ALGERIA	☒

JSECURE AUTHENTICATION

In the above screenshot we have enable country block feature for both backend on frontend and we have blocked afghanistan and algeria from accessing the website.

SECURE IMAGE

This option allows you to specify a image which the user needs to upload in order to access the administration section of the website

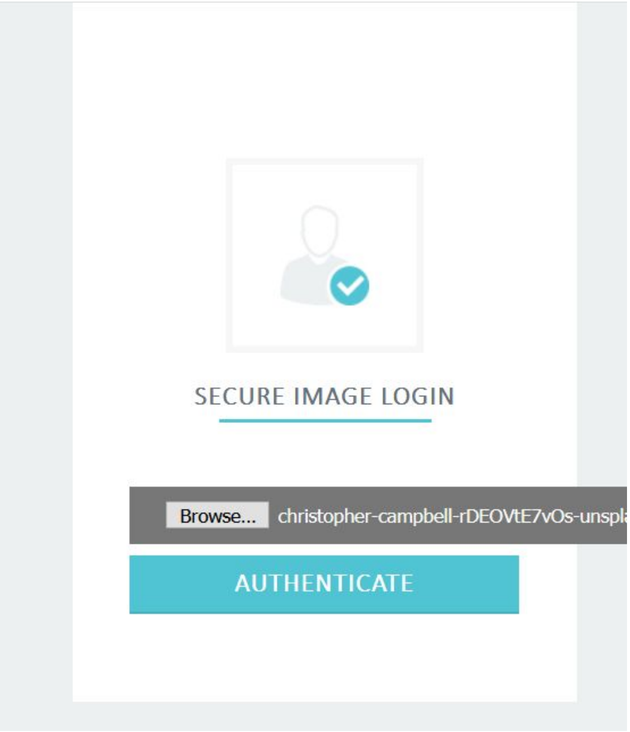


Secure Image

Enable	[✓ Yes] No
Secure Image	Browse... No file selected.
Current Secure Image	

Here is how the configured features looks like -

Now when you try to access the administration feature of the website you would be asked to upload the same image again.



SECURE IMAGE LOGIN

Browse... christopher-campbell-rDEOVtE7vOs-unspl

JSECURE AUTHENTICATION

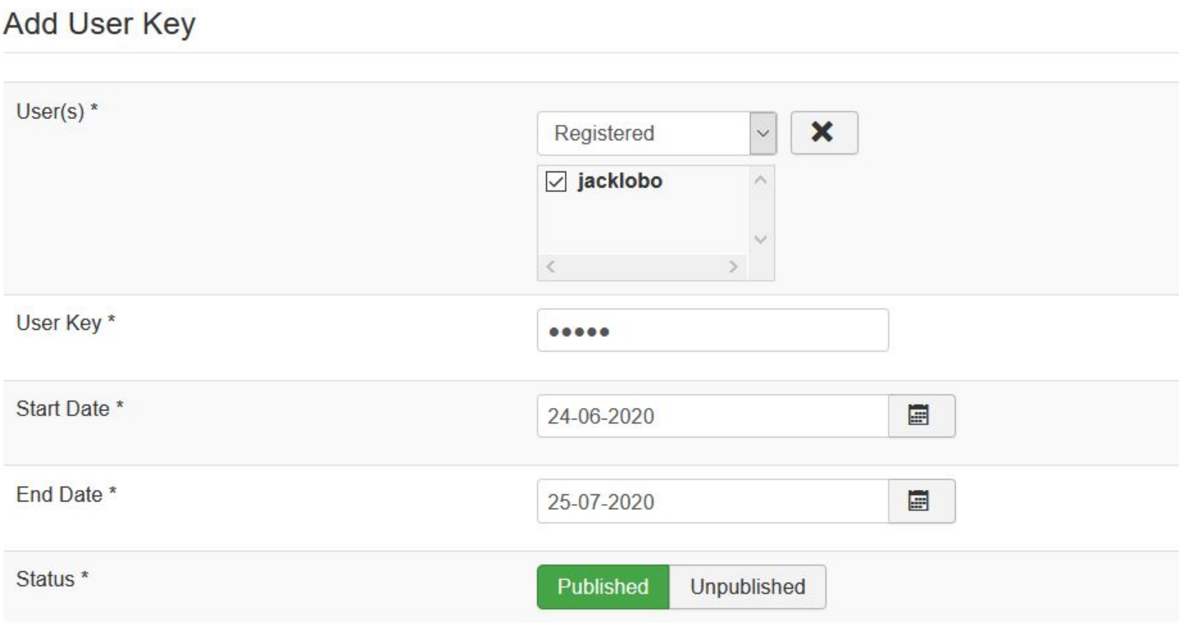
You will only be redirected to the login screen once you have uploaded the exact same image file.

USER KEYS

The key which you set in the basic configuration section of jsecure allows you to access the administration login screen of your website. You need to share this key with all the users who wish to access your website.

Instead of sharing the master key you can create a different key for different users for your website. You can also specify the duration for which the key will be active and the key automatically expires that period. Here is the sample user case -

1) John is the super admin of the website and he sets up the jsecure authentication extension on this website he has set the key as masterkey. So now if he wants to access the login screen of the website . He needs to type the following in the address bar http://example.com/administrator/?masterkey.
2) John now creates a new user for his employee Jack. Now instead of sharing the above userkey to Jack, John can also create a new user key as follows



Add User Key

User(s) *	Registered ✕ ☑ jacklobo
User Key *	•••••
Start Date *	24-06-2020
End Date *	25-07-2020
Status *	Published Unpublished

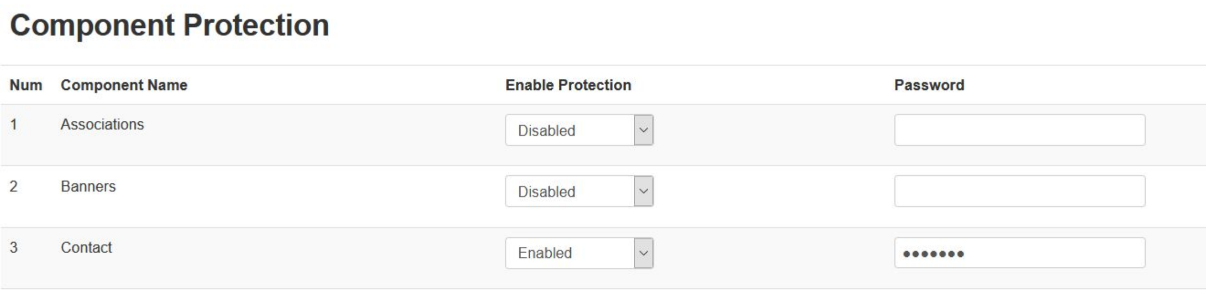
3) Now Jack would be able to see the administration login screen by visiting the following url between 24th June 2020 to 25th July 2020 http://example.com/administrator/?jack
4) You can also unpublish the userkey manually to automatically deactivate the key.

JSECURE AUTHENTICATION

COMPONENT PROTECTION

Similar to the master password feature if you want to provide a password based access to components inside of joomla you can make use of the component protection feature.

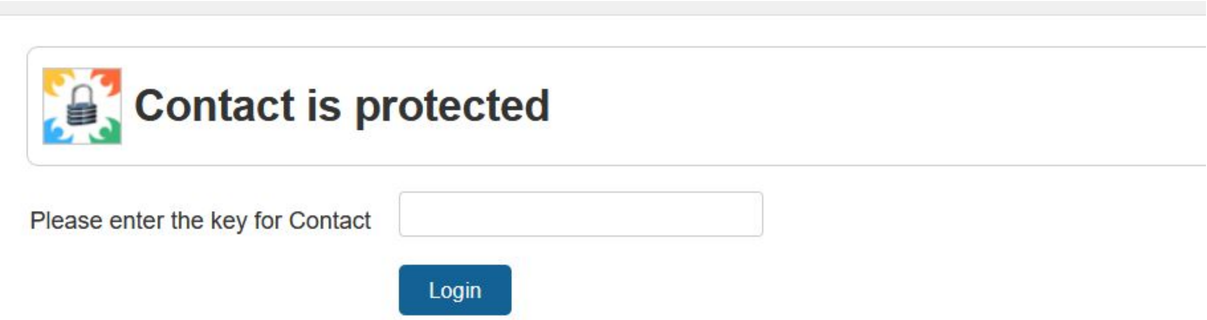
To enable component protection you have to navigate to the components > jsecure authentication > component protection.



Component Protection

Num	Component Name	Enable Protection	Password
1	Associations	Disabled	
2	Banners	Disabled	
3	Contact	Enabled	•••••••

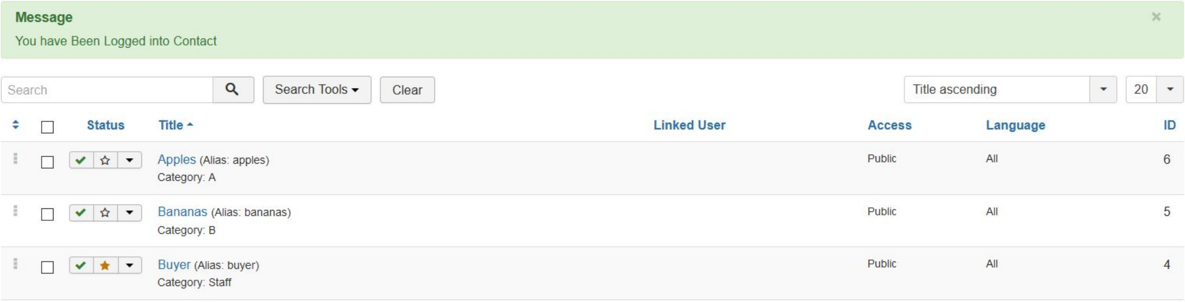
This page displays a list of components installed in your joomla website and also their status of protection. In the above screen we have enabled protection for the contact component. If we visit the contact component now. You will be displayed a screen asking for a password for that component.



Contact is protected

Please enter the key for Contact

Once you have entered the correct password you will be provided access to the component.



Message

You have Been Logged into Contact

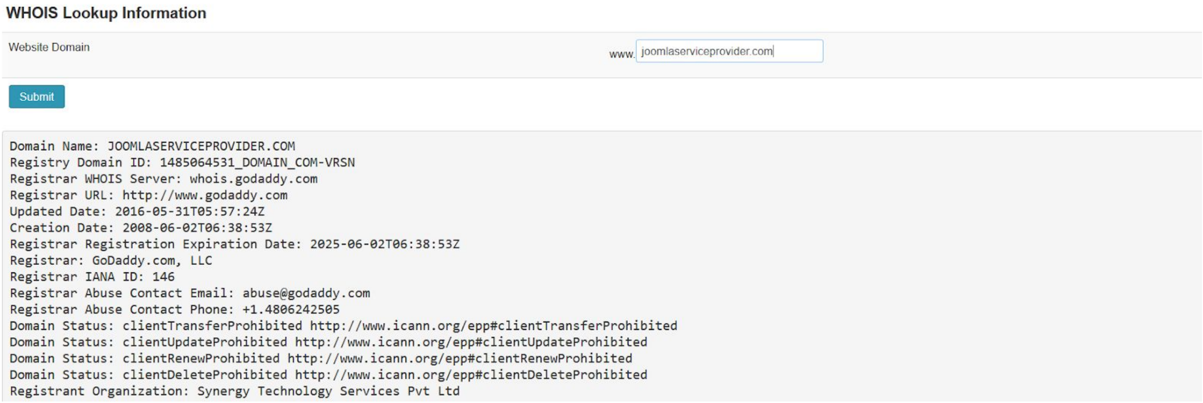
⇕	□	Status	Title ▴	Linked User	Access	Language	ID
	□	✓ ☆ ▾	Apples (Alias: apples) Category: A		Public	All	6
	□	✓ ☆ ▾	Bananas (Alias: bananas) Category: B		Public	All	5
	□	✓ ★ ▾	Buyer (Alias: buyer) Category: Staff		Public	All	4

JSECURE AUTHENTICATION

WHOIS LOOKUP

If you quickly want to check information about a host, we have integrated the whois lookup inside of the extension itself. To use this feature, navigate to components > jsecure authentication > whois lookup information.

The rest is easy, just enter the domain name you want to check the information for and you will get it.



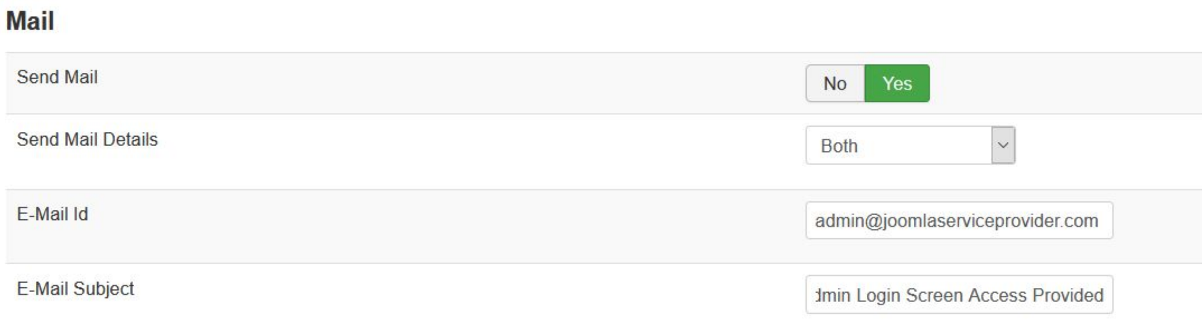
WHOIS Lookup Information

Website Domain www. joomlaserviceprovider.com

```
Domain Name: JOOMLASERVICEPROVIDER.COM
Registry Domain ID: 1485064531_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2016-05-31T05:57:24Z
Creation Date: 2008-06-02T06:38:53Z
Registrar Registration Expiration Date: 2025-06-02T06:38:53Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registrant Organization: Synergy Technology Services Pvt Ltd
```

MAIL

This feature of jsecure allows you to get notified via when a user tries to access your website using incorrect or correct keys. To use this feature navigate to components > jsecure authentication > mail. Here is the sample configuration of the feature.



Mail

Send Mail	No [✓ Yes]
Send Mail Details	Both
E-Mail Id	admin@joomlaserviceprovider.com
E-Mail Subject	dmin Login Screen Access Provided

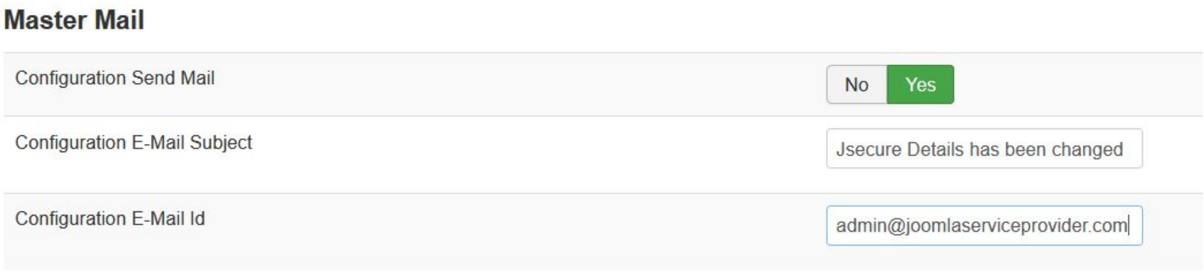
Here we have enabled the mail notification feature for both correct and incorrect keys. We have also specified the email address to which these notifications would be sent along with the subject of these mails for clarity.

JSECURE AUTHENTICATION

MASTER MAIL

Similar to Mail, If you want to get notified if someone makes changes to any of the feature of jsecure authentication plugin you need to enable this feature.

Here is the sample configuration screen for the feature.



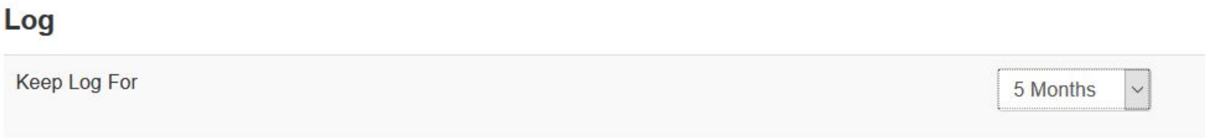
Master Mail

Configuration Send Mail	No [✓ Yes]
Configuration E-Mail Subject	Jsecure Details has been changed
Configuration E-Mail Id	admin@joomlaserviceprovider.com

Here we can specify the subject and the email address to which the notification will be send when there are changes to jsecure features.

LOG

JSecure Authentication Logs all critical security information so that you can have a look at it later when needed. But overtime these logs may get piled up. This feature works out of the box and is enabled by default and the logs are cleared after 5 months but you can select several other options using the dropdown below.



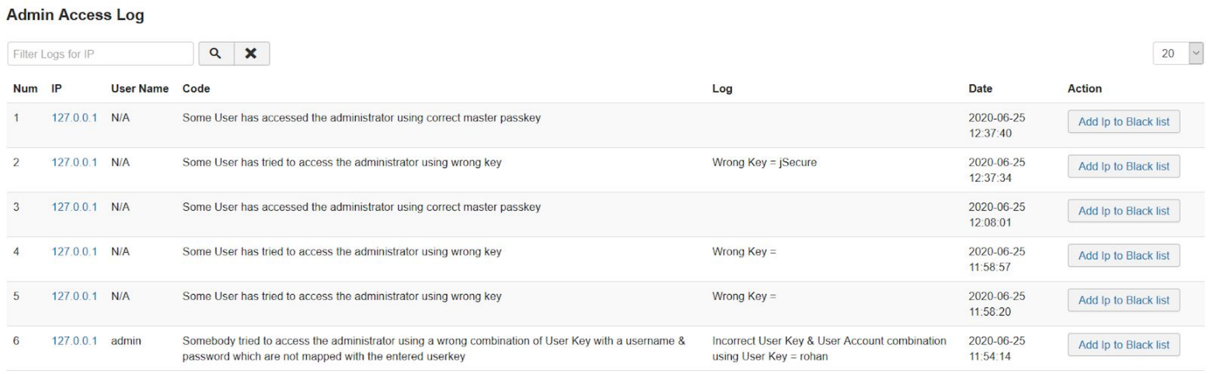
Log

Keep Log For	5 Months

VIEW LOG

This screen allows you to view the logs created by the jsecure authentication plugin and also provides certain actions on them as below.

JSECURE AUTHENTICATION



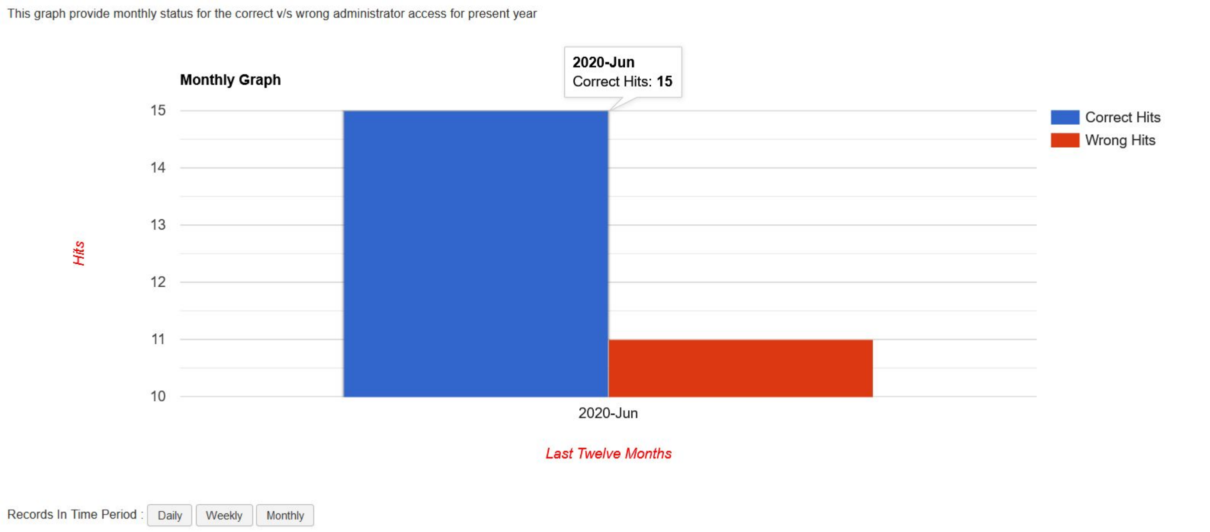
Admin Access Log

Num	IP	User Name	Code	Log	Date	Action
1	127.0.0.1	N/A	Some User has accessed the administrator using correct master passkey		2020-06-25 12:37:40	Add Ip to Black list
2	127.0.0.1	N/A	Some User has tried to access the administrator using wrong key	Wrong Key = jSecure	2020-06-25 12:37:34	Add Ip to Black list
3	127.0.0.1	N/A	Some User has accessed the administrator using correct master passkey		2020-06-25 12:08:01	Add Ip to Black list
4	127.0.0.1	N/A	Some User has tried to access the administrator using wrong key	Wrong Key =	2020-06-25 11:58:57	Add Ip to Black list
5	127.0.0.1	N/A	Some User has tried to access the administrator using wrong key	Wrong Key =	2020-06-25 11:58:20	Add Ip to Black list
6	127.0.0.1	admin	Somebody tried to access the administrator using a wrong combination of User Key with a username & password which are not mapped with the entered userkey	Incorrect User Key & User Account combination using User Key = rohan	2020-06-25 11:54:14	Add Ip to Black list

You have the option to black list ip from this screen itself if you find it suspicious.

HITS GRAPH

This page displays graphs for correct and incorrect website access tried by users in daily, weekly and month format. Be sure to check this regularly to see where you stand in terms of security.



This graph provide monthly status for the correct v/s wrong administrator access for present year

HELP SCREEN

This screen displays quick information on using the jsecure authentication and might save you some of your precious time.