CAPTCHA - reCAPTCHA

Protect your store from spam messages and spam user accounts

A product of PrestaHero

Contents

I. WELCOME

Thank you for purchasing our product. We hope to guide you through all the aspects of the module installation and the module setup within this document. If you have any questions that are beyond the scope of this documentation, please feel free to contact us.

Note:

All instruction screenshots are taken from PrestaShop 1.7, but installing and configuring this module on PrestaShop 1.6 is similar.

II. INTRODUCTION

Getting annoyed with spam messages continuously sent from your website contact form? Have a headache with spam customer accounts registered daily on your money website?

Say "Goodbye" to spam issues now! **CAPTCHA - reCAPTCHA** will solve all the spam issues that you're dealing with.

** "**CAPTCHA - reCAPTCHA**" is compatible with PrestaShop from version 1.5.x to version 8.x*

III. INSTALLATION

1. Navigate to **"Modules / Modules & Services",** click on **"Upload a module / Select file"**

2. Select the module file **"ets_advancedcaptcha.zip"** from your computer then click on **"Open"** to install

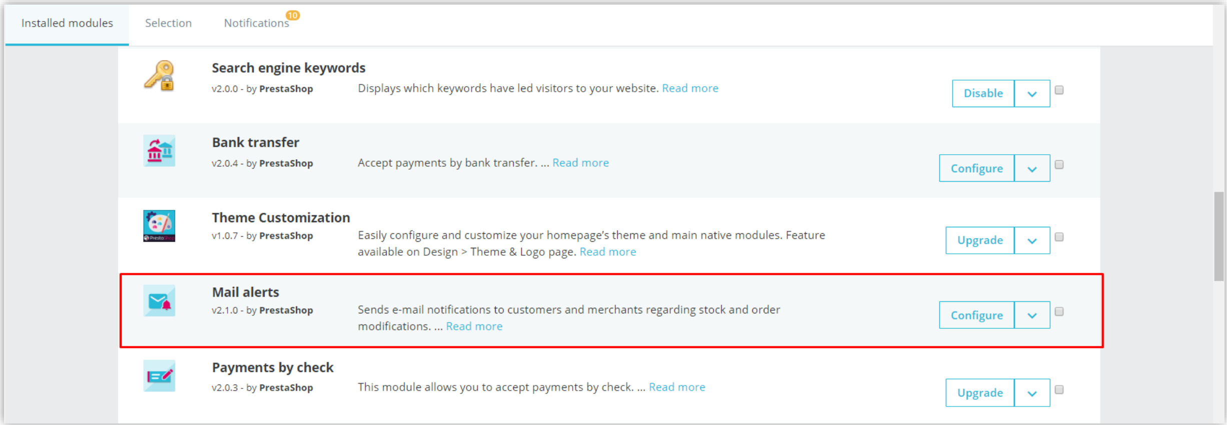
❖ Click on **"Configure"** button of the module you just installed to open the module's configuration page.

IV. CONFIGURATION

From your installed module list (Located at **"Modules/Modules & services/Installed modules"**), find "**CAPTCHA - reCAPTCHA**" then click on the **"Configure"** button to open its configuration page.

Note:

a) To enable "**Out of product alert form**", you must install **"Mail alert"** module first.



Search engine keywords
v2.0.0 - by **PrestaShop** Displays which keywords have led visitors to your website. Read more

Bank transfer
v2.0.4 - by **PrestaShop** Accept payments by bank transfer. ... Read more

Theme Customization
v1.0.7 - by **PrestaShop** Easily configure and customize your homepage's theme and main native modules. Feature available on Design > Theme & Logo page. Read more

Mail alerts
v2.1.0 - by **PrestaShop** Sends e-mail notifications to customers and merchants regarding stock and order modifications. ... Read more

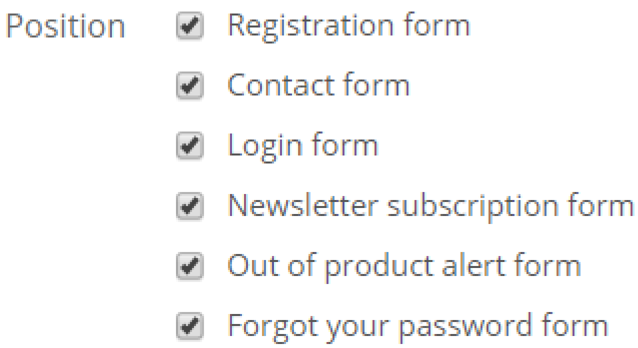
Payments by check
v2.0.3 - by **PrestaShop** This module allows you to accept payments by check. ... Read more

b) When using the *PrestaHero* **CAPTCHA - reCAPTCHA** module alongside the "**Creative Elements**" module developed by *WebshopWorks*, please be aware that the CAPTCHA - reCAPTCHA functionality will not be supported for forms created by the "**Creative Elements**" module.

If you need to display CAPTCHA/reCAPTCHA on forms generated by "**Creative Elements**," please get in touch with the developer *WebshopWorks* for further assistance.

1. Position

You can select the form where captcha box will be displayed. **CAPTCHA - reCAPTCHA** supports display captcha box on 6 different types of form:

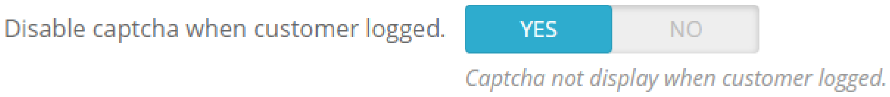


Position
☑ Registration form
☑ Contact form
☑ Login form
☑ Newsletter subscription form
☑ Out of product alert form
☑ Forgot your password form

*Note:

***CAPTCHA** does not support captcha feature for “**Newsletter subscription form**” on PrestaShop 1.5.x*

For online shop owners who are using **PrestaShop 1.7.x**, after choosing positions to show captcha box, there is an option to enable/disable captcha when customer logged in.



Disable captcha when customer logged. YES NO

Captcha not display when customer logged.

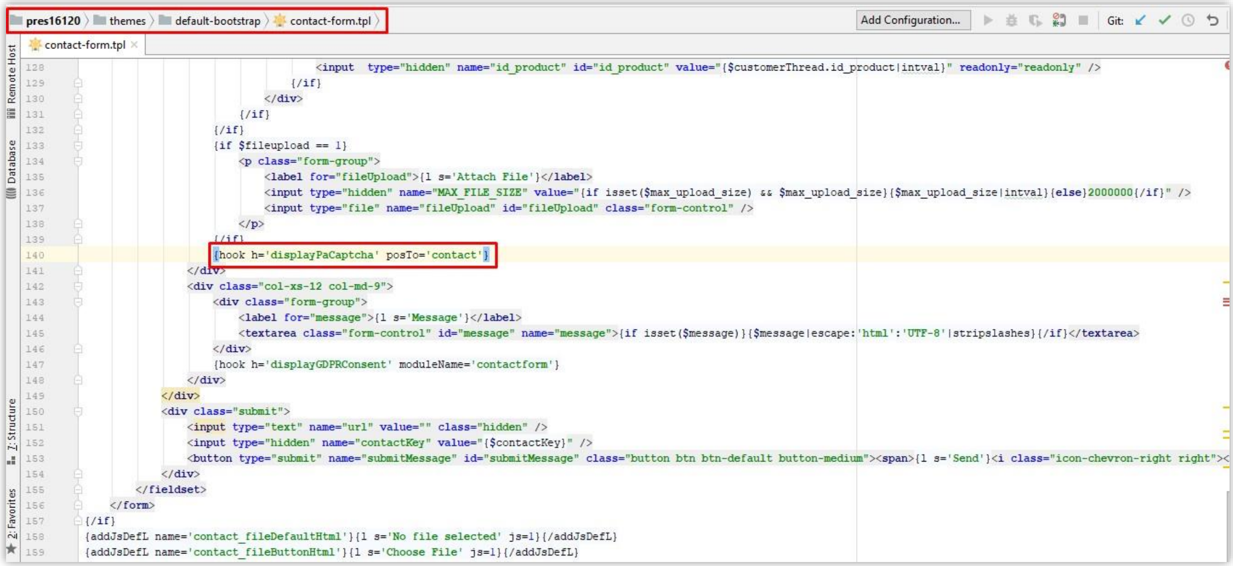
With shop owners using **PrestaShop 1.5.x and 1.6.x**, for certain locations you will see more options to set up. If you're using a custom theme or another custom module, you may get into some problems when installing **CAPTCHA - reCAPTCHA** to your website. To avoid these troubles, please follow our following guide:

❖ Contact form

Copy this code: *{hook h='displayPaCaptcha' posTo='contact'}*

Open this file: *root/YOUR-SITE/themes/YOUR-THEME/contact-form.tpl*

Paste the code you copied before into the *contact-form.tpl* just below the **file upload field** then save your changes.



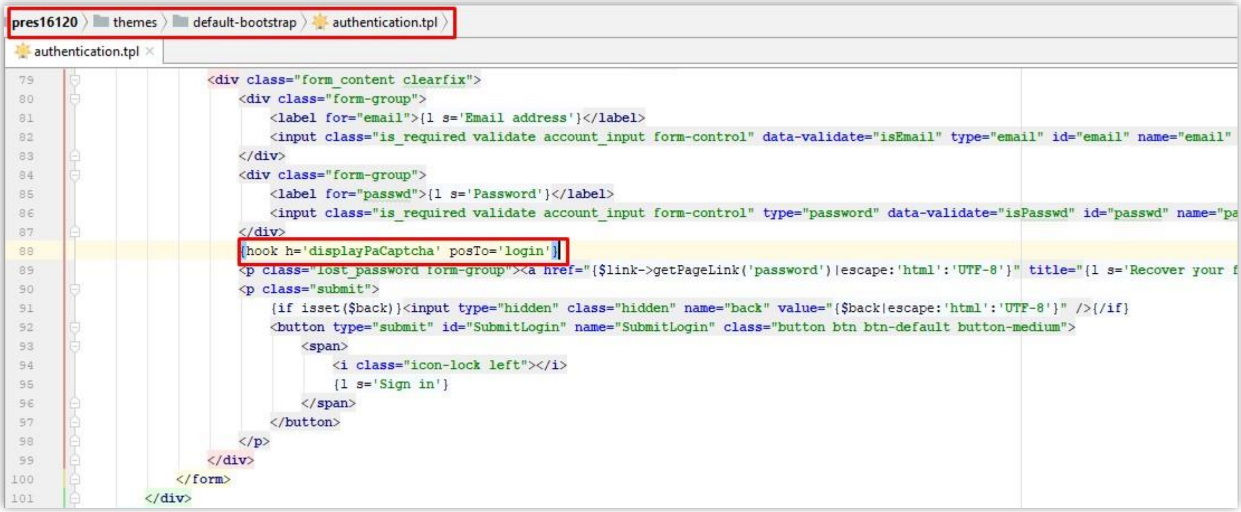
```
                                    <input  type="hidden" name="id_product" id="id_product" value="{$customerThread.id_product|intval}" readonly="readonly" />
                                {/if}
                            </div>
                        {/if}
                    {/if}
                    {if $fileupload == 1}
                        <p class="form-group">
                            <label for="fileUpload">{l s='Attach File'}</label>
                            <input type="hidden" name="MAX_FILE_SIZE" value="{if isset($max_upload_size) && $max_upload_size}{$max_upload_size|intval}{else}2000000{/if}" />
                            <input type="file" name="fileUpload" id="fileUpload" class="form-control" />
                        </p>
                    {/if}
                    {hook h='displayPaCaptcha' posTo='contact'}
                </div>
                <div class="col-xs-12 col-md-9">
                    <div class="form-group">
                        <label for="message">{l s='Message'}</label>
                        <textarea class="form-control" id="message" name="message">{if isset($message)}{$message|escape:'html':'UTF-8'|stripslashes}{/if}</textarea>
                    </div>
                    {hook h='displayGDPRConsent' moduleName='contactform'}
                </div>
            </div>
            <div class="submit">
                <input type="text" name="url" value="" class="hidden" />
                <input type="hidden" name="contactKey" value="{$contactKey}" />
                <button type="submit" name="submitMessage" id="submitMessage" class="button btn btn-default button-medium"><span>{l s='Send'}<i class="icon-chevron-right right"><
            </div>
        </fieldset>
    </form>
{/if}
{addJsDefL name='contact_fileDefaultHtml'}{l s='No file selected' js=1}{/addJsDefL}
{addJsDefL name='contact_fileButtonHtml'}{l s='Choose File' js=1}{/addJsDefL}
```

❖ Login form

Copy this code: *{hook h='displayPaCaptcha' posTo='login'}*

Open this file: *root/YOUR-SITE/themes/YOUR-THEME/authentication.tpl*

Paste the code you copied before into the *authentication.tpl* just below the file upload field then save your changes.



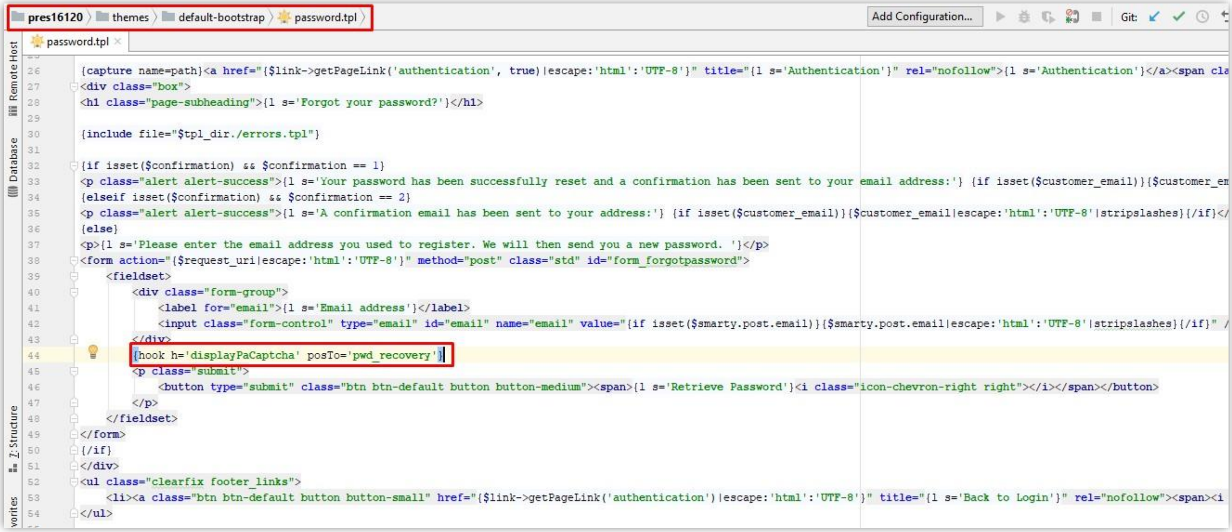
```
        <div class="form_content clearfix">
            <div class="form-group">
                <label for="email">{l s='Email address'}</label>
                <input class="is_required validate account_input form-control" data-validate="isEmail" type="email" id="email" name="email"
            </div>
            <div class="form-group">
                <label for="passwd">{l s='Password'}</label>
                <input class="is_required validate account_input form-control" type="password" data-validate="isPasswd" id="passwd" name="pa
            </div>
            {hook h='displayPaCaptcha' posTo='login'}
            <p class="lost_password form-group"><a href="{$link->getPageLink('password')|escape:'html':'UTF-8'}" title="{l s='Recover your f
            <p class="submit">
                {if isset($back)}<input type="hidden" class="hidden" name="back" value="{$back|escape:'html':'UTF-8'}" />{/if}
                <button type="submit" id="SubmitLogin" name="SubmitLogin" class="button btn btn-default button-medium">
                    <span>
                        <i class="icon-lock left"></i>
                        {l s='Sign in'}
                    </span>
                </button>
            </p>
        </div>
    </form>
</div>
```

- **Forgot your password form**

Copy this code: *{hook h='displayPaCaptcha' posTo='pwd_recovery'}*

Open this file: *root/YOUR-SITE/themes/YOUR-THEME/password.tpl*

Paste the code you copied before into the *password.tpl* just below the file upload field then save your changes.



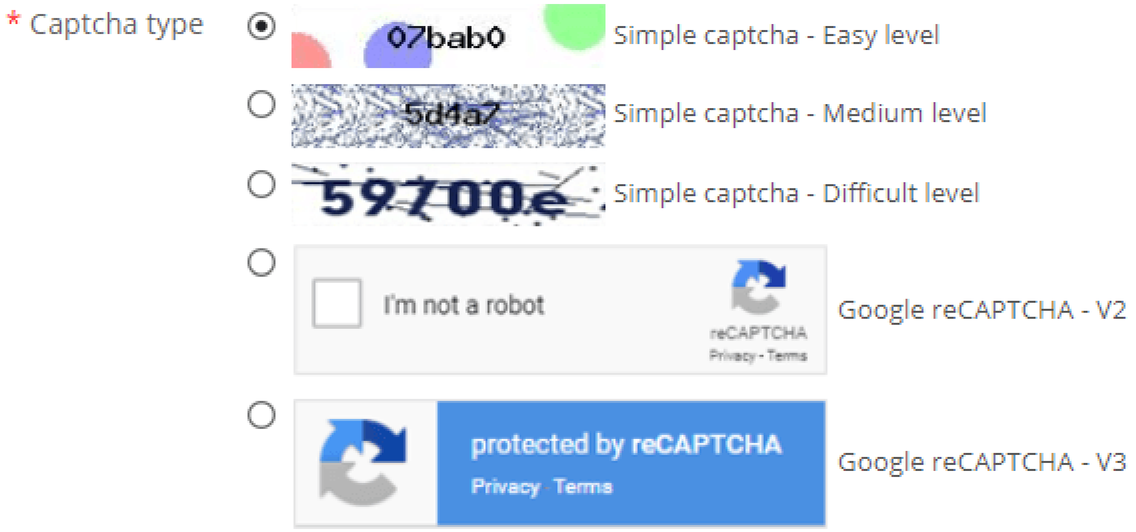
```
{capture name=path}<a href="{$link->getPageLink('authentication', true)|escape:'html':'UTF-8'}" title="{l s='Authentication'}" rel="nofollow">{l s='Authentication'}</a><span cla
<div class="box">
<h1 class="page-subheading">{l s='Forgot your password?'}</h1>

{include file="$tpl_dir./errors.tpl"}

{if isset($confirmation) && $confirmation == 1}
<p class="alert alert-success">{l s='Your password has been successfully reset and a confirmation has been sent to your email address:'} {if isset($customer_email)}{$customer_em
{elseif isset($confirmation) && $confirmation == 2}
<p class="alert alert-success">{l s='A confirmation email has been sent to your address:'} {if isset($customer_email)}{$customer_email|escape:'html':'UTF-8'|stripslashes}{/if}</
{else}
<p>{l s='Please enter the email address you used to register. We will then send you a new password. '}</p>
<form action="{$request_uri|escape:'html':'UTF-8'}" method="post" class="std" id="form_forgotpassword">
    <fieldset>
        <div class="form-group">
            <label for="email">{l s='Email address'}</label>
            <input class="form-control" type="email" id="email" name="email" value="{if isset($smarty.post.email)}{$smarty.post.email|escape:'html':'UTF-8'|stripslashes}{/if}" /
        </div>
        {hook h='displayPaCaptcha' posTo='pwd_recovery'}
        <p class="submit">
            <button type="submit" class="btn btn-default button button-medium"><span>{l s='Retrieve Password'}<i class="icon-chevron-right right"></i></span></button>
        </p>
    </fieldset>
</form>
{/if}
</div>
<ul class="clearfix footer_links">
    <li><a class="btn btn-default button button-small" href="{$link->getPageLink('authentication')|escape:'html':'UTF-8'}" title="{l s='Back to Login'}" rel="nofollow"><span><i
</ul>
```

2. Captcha types

CAPTCHA - reCAPTCHA offers 5 types of captcha for you to select the most suitable with your current theme.



* Captcha type

● Simple captcha - Easy level

○ Simple captcha - Medium level

○ Simple captcha - Difficult level

○ Google reCAPTCHA - V2

○ Google reCAPTCHA - V3

To use Google reCAPTCHA, you will need to enter **Site key and Secret key** (for the Classic reCAPTCHA key) **or reCAPTCHA ID** (for the new reCAPTCHA project created in Google Cloud Console).

Google has announced that **all reCAPTCHA Classic keys must be migrated to Google Cloud Console by the end of 2025**. Previously, reCAPTCHA keys were managed separately on **Google reCAPTCHA Admin**, where users could create keys for free without linking a credit card. However, Google is now moving all reCAPTCHA services under **Google Cloud Console** for centralized management.

❓ What Does This Mean for You?

- If you **already have reCAPTCHA Classic keys**, you can still use them **until the end of 2025**, but you need to migrate them to a **Google Cloud project**.
- If you're **setting up reCAPTCHA for the first time**, you must generate **new keys** in **Google Cloud Console** instead of the old Google reCAPTCHA Admin.

🔷 What You Need to Do

👉 **If you are using reCAPTCHA Classic keys:**

To continue using your existing keys, you must migrate them to Google Cloud Console. Follow this guide: How to Migrate reCAPTCHA Classic to Google Cloud

👉 **If you need new reCAPTCHA keys:**

You must create new keys, depending on where you want to manage them:

- **Using the old Google reCAPTCHA Admin (until it is fully deprecated):** Create reCAPTCHA Key in Google reCAPTCHA Admin
- **Using Google Cloud Console (recommended for future compatibility):** How to Create reCAPTCHA Keys in Google Cloud

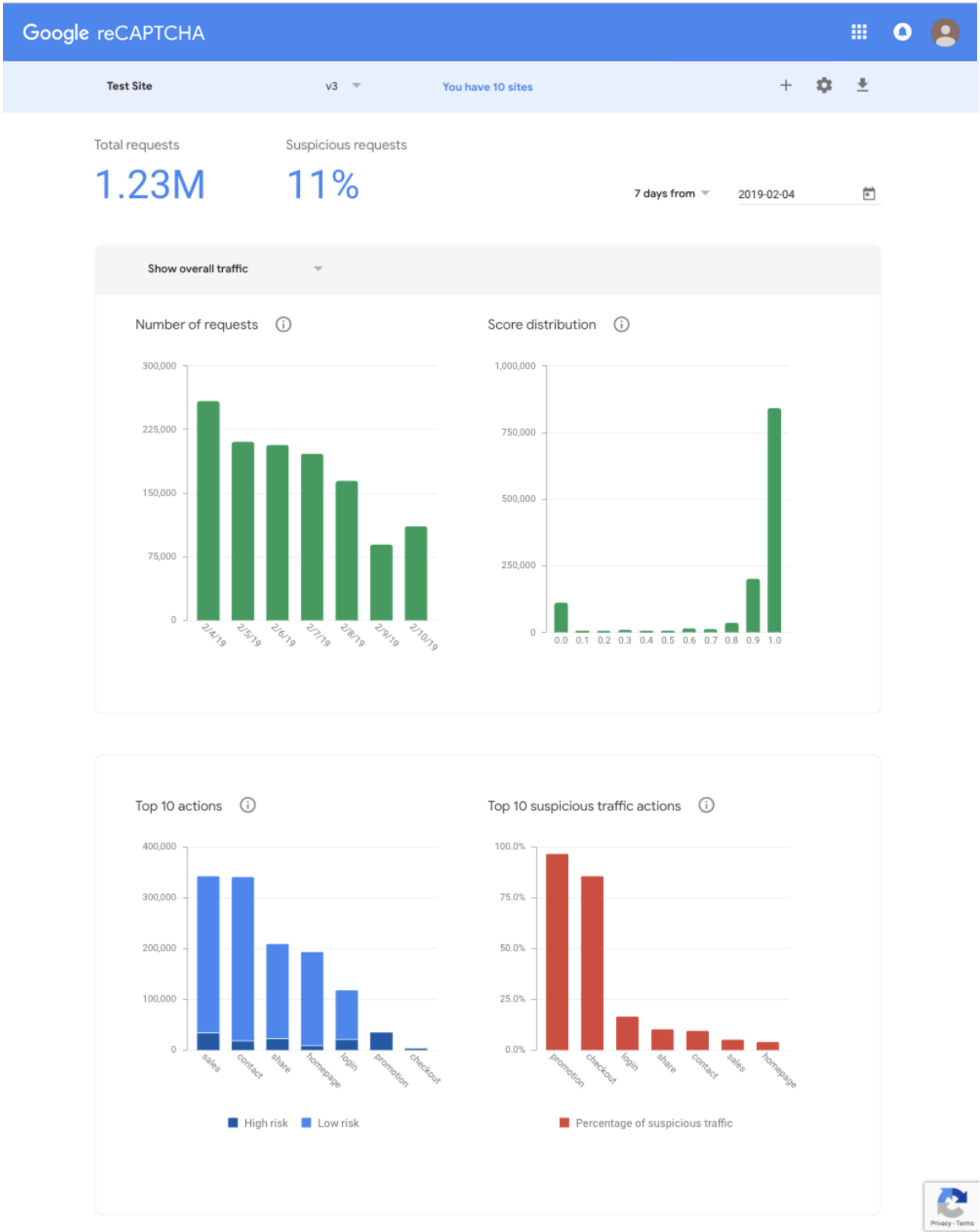
Once you have your new keys, update them in the **CAPTCHA - reCAPTCHA** module settings in your PrestaShop back office.

About Google reCAPTCHA v3

Google reCAPTCHA v3 is a powerful, non-intrusive spam prevention tool that operates in the background, analyzing user interactions with your website without requiring explicit user challenges (e.g., clicking checkboxes or solving puzzles). Instead, reCAPTCHA v3 assigns a **score** to each user interaction, ranging from **0.0** to **1.0**:

- **Score close to 1.0**: Indicates a high likelihood that the interaction is from a genuine human user.
- **Score close to 0.0**: Suggests a high probability of bot or automated activity.
- **Intermediate scores (e.g., 0.3 to 0.7)**: Indicate varying levels of confidence, requiring further evaluation or additional verification.

This score allows you to define how your PrestaShop website handles different types of traffic, such as allowing legitimate users to proceed, requiring additional verification for suspicious interactions, or blocking potential bots outright.



Google reCAPTCHA

Test Site v3

You have 10 sites

Total requests
1.23M

Suspicious requests
11%

7 days from 2019-02-04

Show overall traffic

Setting the Score Threshold:

- The **Score Threshold** determines the minimum score required to consider an interaction legitimate. Interactions with scores below this threshold may be blocked or require additional verification (depending on your module settings).
- The threshold can be set to a value between **0.0 and 1.0**.

Recommended Score Threshold Settings

Choosing an appropriate score threshold is crucial to balance spam prevention with a seamless user experience. The optimal threshold depends on your website's needs, the forms you're protecting, and the level of spam activity you're experiencing. Below are general recommendations:

Default recommendation: 0.5	A threshold of 0.5 is a good starting point for most PrestaShop websites. It effectively blocks interactions with a high likelihood of being bots (scores below 0.5) while allowing most legitimate users to proceed without additional verification.	Suitable for: General-purpose websites, contact forms, and login forms with moderate spam activity.
Lenient setting: 0.3	Use a lower threshold (e.g., 0.3) if you want to minimize disruptions for users, especially on forms critical to conversions (e.g., registration or checkout forms). This setting may allow some low-risk bots to pass but	Suitable for: High-traffic e-commerce stores prioritizing user experience over strict spam filtering.

	reduces the chance of blocking legitimate users.	
Strict setting: 0.7	A higher threshold (e.g., 0.7) is recommended for forms highly targeted by spam, such as newsletter subscription or forgot password forms. This setting provides stronger protection but may flag some legitimate users for additional verification, potentially impacting user experience.	Suitable for: Websites experiencing heavy spam or bot attacks.

Customizing Based on Analytics:

- After setting an initial threshold, monitor your website's analytics (e.g., spam submissions, blocked interactions, or user complaints) to fine-tune the score.
- If you notice excessive spam slipping through, increase the threshold (e.g., from 0.5 to 0.6). If legitimate users report issues (e.g., being blocked or asked for additional verification), lower the threshold slightly (e.g., from 0.5 to 0.4).
- Use the Google reCAPTCHA Admin Console to review score distributions for your site and adjust accordingly.

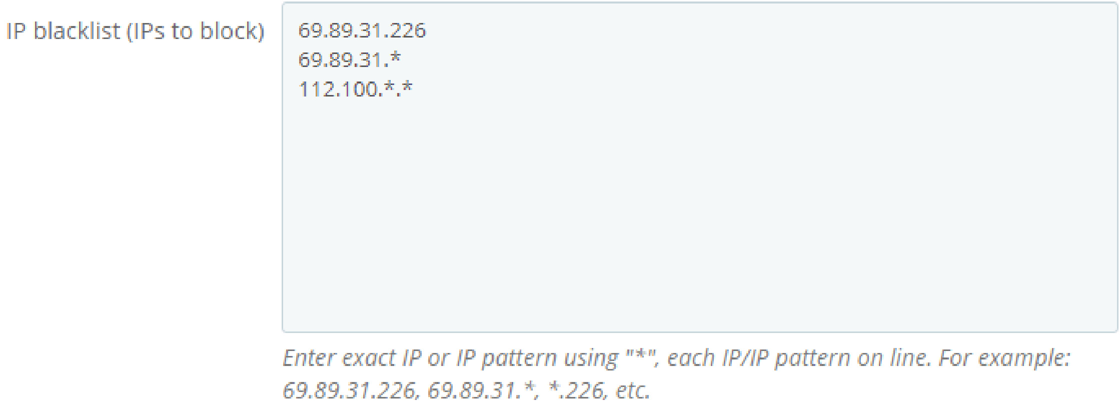
3. IP blacklist and email blacklist

❖ IP blacklist

With **CAPTCHA - reCAPTCHA**, you can enter IP addresses of spammers and ban them from submitting your forms.

Note:

IPv4 addresses are usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, each part represents a group of 8 bits (an octet) of the address.



IP blacklist (IPs to block)

```
69.89.31.226
69.89.31.*
112.100.*.*
```

Enter exact IP or IP pattern using "", each IP/IP pattern on line. For example: 69.89.31.226, 69.89.31.*, *.226, etc.*

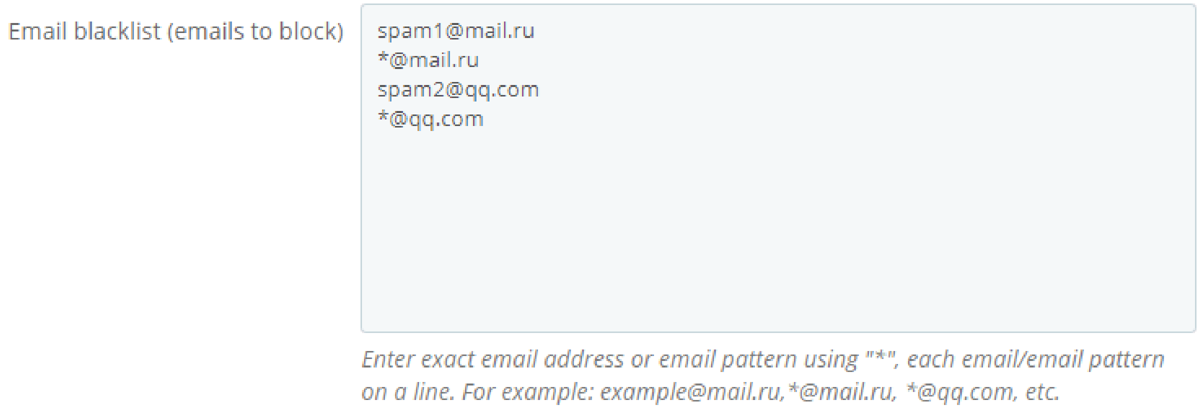
You may enter the exact IP address (for example: 69.89.31.226) or an IP pattern using "*" character, each IP/IP pattern on one line.

Note:

IP pattern is a way to represent an IP address range. You can replace one or several octets of IP address with "" character. For example, if you enter this IP pattern: 69.89.31.*, CAPTCHA will ban all IP addresses from 69.89.31.0 to 69.89.31.255*

❖ Email blacklist

Similar to banning IP addresses, you can also ban email addresses which often send spam emails to your inbox. **CAPTCHA - reCAPTCHA** also supports banning email addresses from email domain such as mail.ru, qq.com, etc.



Email blacklist (emails to block)

```
spam1@mail.ru
*@mail.ru
spam2@qq.com
*@qq.com
```

Enter exact email address or email pattern using "", each email/email pattern on a line. For example: example@mail.ru,*@mail.ru, *@qq.com, etc.*

You can enter the exact email address or email pattern using “*” character, each email or email pattern on a line.

For example, if you enter *@mail.ru email pattern, **CAPTCHA - reCAPTCHA** will ban all emails which are sent from users having “@mail.ru” on their email addresses.

4. Tips

This module should work perfectly on most Prestashop websites without any code modification, however if you website is installed with a custom theme or custom modules you may (rarely) get into some problems when installing the module to your website.

The following tips will guide you on how to quickly fix the problems by modifying some code so you can fix the problems yourself but we recommend you contact us. We're happy to support you and we'll help you solve the issues for free!

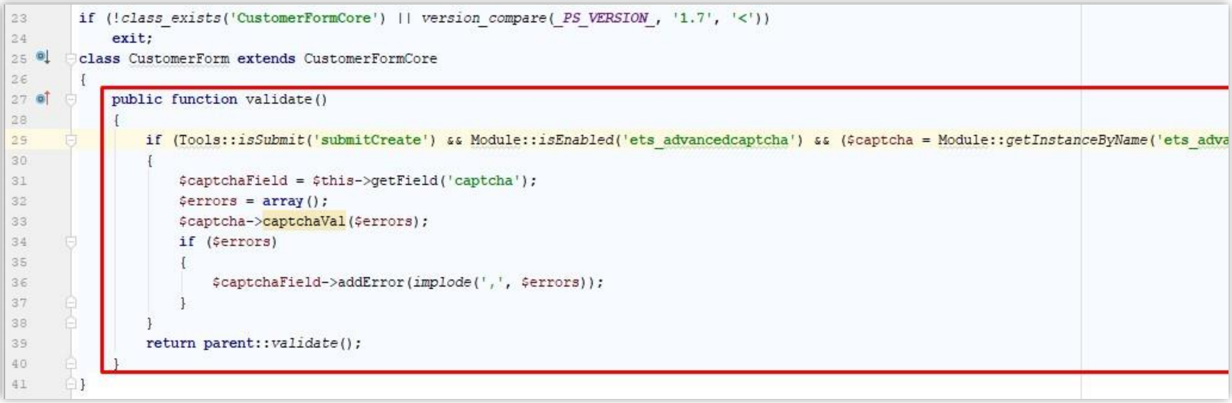
❖ **For PrestaShop 1.7.x**

If you see an error that says methods **validate** and **getFormat** are overridden already by another module, it means some other modules have overridden the method that causes blocking the **CAPTCHA - reCAPTCHA** module to implement its overriding code. To solve the problem, you need to manually edit the methods (in overriding files) with the overriding code of the **CAPTCHA - reCAPTCHA** module.

ERROR: "METHOD VALIDATE() IS OVERRIDEN ALREADY"

<u>Step 1:</u> Open this file: *root/YOUR-SITE/modules/ets_advancedcaptcha/override/classes/form/CustomerForm.php*

<u>Step 2:</u> Copy the code highlighted on the photo below



```
if (!class_exists('CustomerFormCore') || version_compare(_PS_VERSION_, '1.7', '<'))
    exit;
class CustomerForm extends CustomerFormCore
{
    public function validate()
    {
        if (Tools::isSubmit('submitCreate') && Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getInstanceByName('ets_adva
        {
            $captchaField = $this->getField('captcha');
            $errors = array();
            $captcha->captchaVal($errors);
            if ($errors)
            {
                $captchaField->addError(implode(',', $errors));
            }
        }
        return parent::validate();
    }
}
```

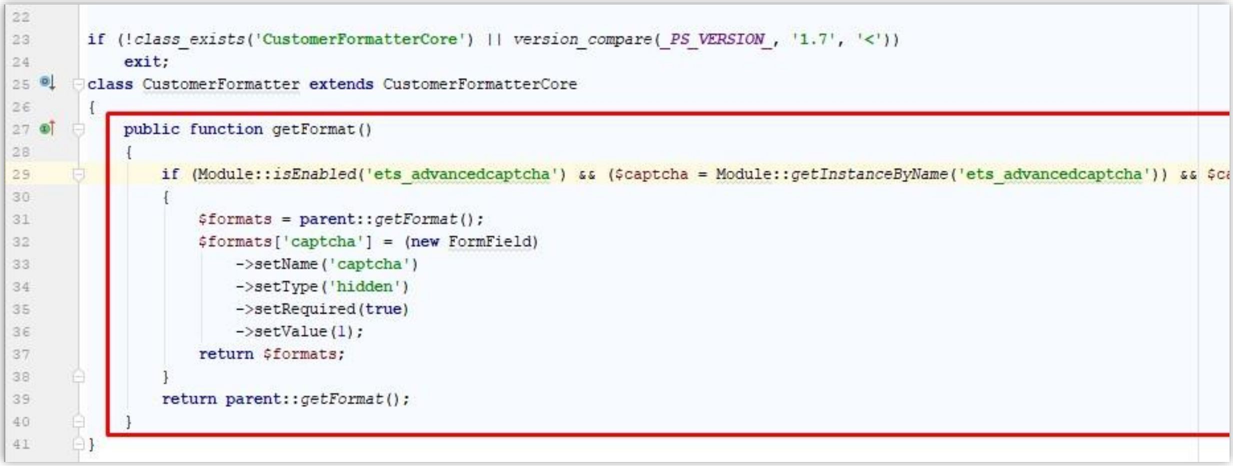
<u>Step 3:</u> Open this file: *root/YOUR-SITE/override/classes/form/CustomerForm.php*

<u>Step 4:</u> Find a method (function) named "validate", paste the code you copied at step 2 into the method just at the START of the method then save your changes

ERROR: "METHOD GETFORMAT() IS OVERRIDEN ALREADY"

<u>Step 1:</u> Open this file: *root/YOUR-SITE/modules/ets_advancedcaptcha/override/classes/form/CustomerFormatter.php*

Step 2: Copy the code highlighted in the photo below



```php

if (!class_exists('CustomerFormatterCore') || version_compare(_PS_VERSION_, '1.7', '<'))
    exit;
class CustomerFormatter extends CustomerFormatterCore
{
    public function getFormat()
    {
        if (Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getInstanceByName('ets_advancedcaptcha')) && $ca
        {
            $formats = parent::getFormat();
            $formats['captcha'] = (new FormField)
                ->setName('captcha')
                ->setType('hidden')
                ->setRequired(true)
                ->setValue(1);
            return $formats;
        }
        return parent::getFormat();
    }
}
```

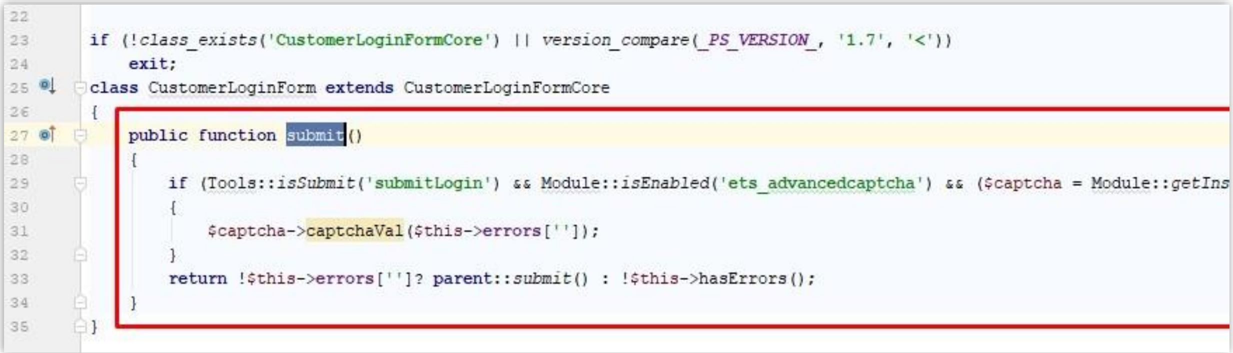
Step 3: Open this file: *root/YOUR-SITE/override/classes/form/CustomerFormatter.php*

Step 4: Find a method (function) named "getFormat", paste the code you copied at step 2 into the method just at the START of the method then save your changes.

ERROR: "METHOD SUBMIT() IS OVERRIDEN ALREADY"

Step 1: Open this file: *root/YOUR-SITE/modules/ets_advancedcaptcha/override/classes/form/CustomerLoginForm.php*

Step 2: Copy the code highlighted on the photo below



```php

if (!class_exists('CustomerLoginFormCore') || version_compare(_PS_VERSION_, '1.7', '<'))
    exit;
class CustomerLoginForm extends CustomerLoginFormCore
{
    public function submit()
    {
        if (Tools::isSubmit('submitLogin') && Module::isEnabled('ets_advancedcaptcha') && ($captcha = Module::getIns
        {
            $captcha->captchaVal($this->errors['']);
        }
        return !$this->errors['']? parent::submit() : !$this->hasErrors();
    }
}
```

Step 3: Open this file: *root/YOUR-SITE/override/classes/form/CustomerLoginForm.php*

<u>Step 4:</u> Find a method (function) named "submit", paste the code you copied at step 2 into the method just at the START of the method then save your changes.

- **For PrestaShop 1.5.x and 1.6.x**

ERROR: "OVERRIDE CONTROLLER"

If methods: *processSubmitAccount, processSubmitLogin, sendRenewPasswordLink, postProcess, initContent* are overridden already, follow these steps to fix the problem.

<u>Step 1:</u> Open 3 files: *AuthController.php, ContactController.php, PasswordController.php* that are located in "root/YOUR-SITE/modules/ets_advancedcaptcha/override/controllers/front/" folder

<u>Step 2:</u> Copy methods (functions) that are defined on the files.

<u>Step 3:</u> Open these respective overriding files (*AuthController.php, ContactController.php, PasswordController.php*) in overriding folder of your website at "root/YOUR-SITE/override/controllers/front/"

<u>Step 4:</u> Find and replace the methods defined in those files with the methods you copied in step 2 then save your changes

****Note:** if you replace the whole methods that are overridden by other modules, the other modules may not work properly anymore (but the **CAPTCHA - reCAPTCHA** module will surely work).*

So, if you have programming knowledge, you should check the existing overridden methods and only insert necessary codes that are defined on overriding files of the **CAPTCHA - reCAPTCHA** module.

We recommend you contact us for a quick and free fix of the problem (as it requires coding work), we're happy to support you.

V. THANK YOU

Thank you again for purchasing our product and going through this documentation. We hope this document is helpful and efficient in the complete setup of this module.

If you do have any questions for which the answer is not available in this document, please feel free to contact us.