Google Authenticator Back-Office Security Module for Prestashop
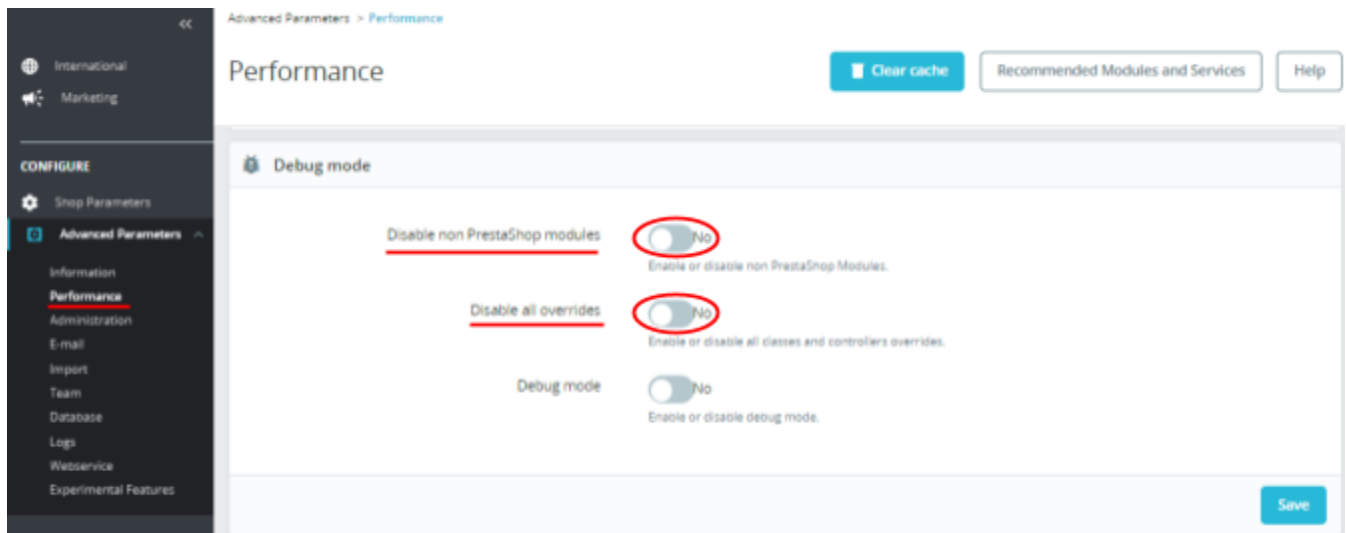
Compatible with all Prestashop versions starting with 1.6, 1.7, and 8

Version: 1.25+

Author: Rinku Kazeno

Thanks for purchasing my **Google Authenticator Security Module for Prestashop**. Here's how to install and use it.

Previous Considerations

For this module to work, the *Disable non PrestaShop* modules and *Disable all overrides* options on the **Performance** page of the **Advanced Parameters** menu must be set to **<u>No</u>**.

Prestashop version upgrades sometimes change these options to *Yes*, so if the module stops working after one of these upgrades, it's very likely you will need to adjust these options again.

Installation
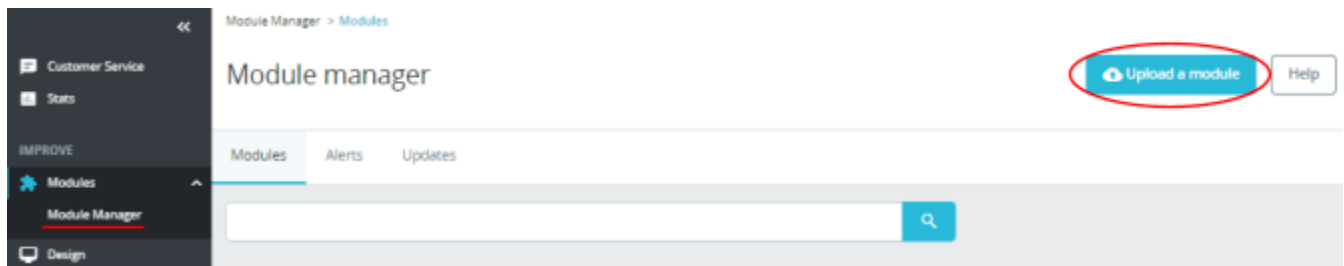
1. You can add the module automatically from your **Back Office** by going into the **Modules Manager** in the **Modules** menu, selecting **_Upload a module_**, and uploading the zip file from your web browser.

If you're using an older Prestashop version, or are having problems with the automatic installer, you need to extract and upload the **gauthenticator** folder (inside the zip file) to your **modules** folder inside your Prestashop directory by FTP.

2. Install the module from your **Back Office** if it wasn't already automatically installed during the upload. It should appear in the **Administration** section of your **Modules** tab.

That's it, your module is now installed! Your admin login area should now have an extra input field for Google Authenticator codes. Don't worry if you and your employees haven't synced your mobile devices yet; since it's an opt-in feature, **users who haven't synced their devices yet can leave the new field blank** and login just the same.

Configuration

0. (optional) If you want non-Admin employees to have access to their own Google Authenticator account configuration, you need to go to the **Permissions** sub-tab of the **Team** tab in the **Advanced Parameters** menu (*Prestashop 8* and *1.7*) or the **Permissions** sub-tab of the **Administration** menu (*Prestashop 1.6*), and make sure their User Group has *View* permissions for the **Employees** class and *Full* permissions for the **Google Authenticator** class.
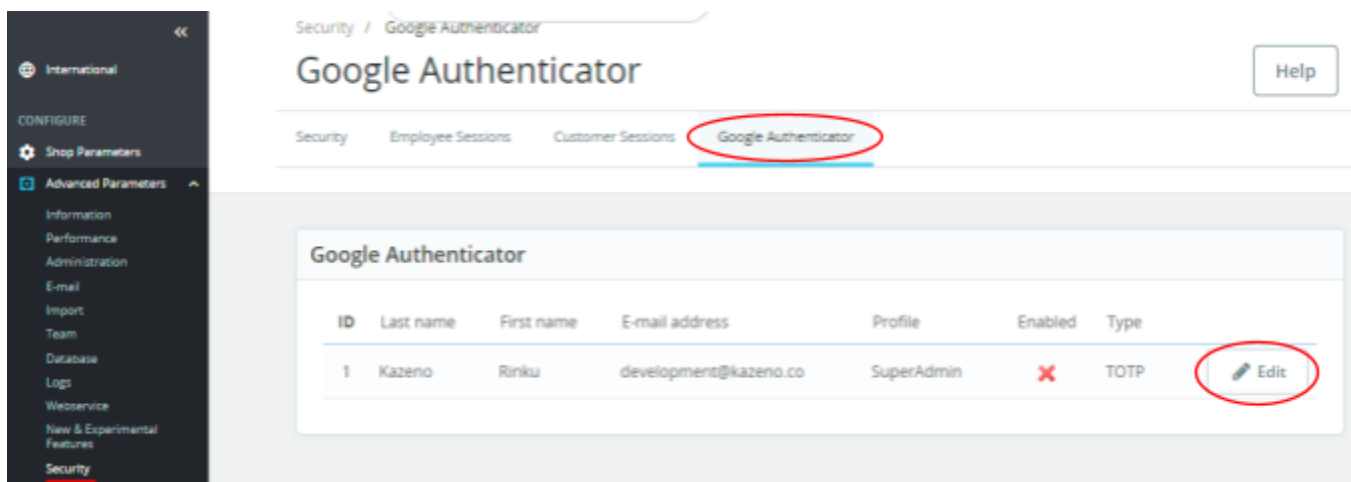
1. A new tab called **Google Authenticator** should've been created in the following place, depending on your *Prestashop* version:
- *Prestashop 8*: **Advanced Parameters** > **Security** page
- *Prestashop 1.7*: **Advanced Parameters** > **Team** page
- *Prestashop 1.6*: **Administration** menu

In it there should be a list of your employees (or just your account, if you're not an Admin). To sync a mobile device with a particular employee account, click on their respective *Edit* button.

2. Change the *Status* to *Enabled*, change the *Authentication Type* if you wish, and click **_Save_**. If you haven't downloaded the free **Google Authenticator** app for your mobile device from its official App Store, you should do that now.

The *Authentication Type* options are the following:

- *TOTP*: **You should use this option**, unless you really know what you're doing. The one-time codes are *time-based*, which means they change automatically every 30 seconds.
- *HOTP*: **Not recommended** unless you specifically need it for some advanced use scenario. The one-time codes are *counter-based*, and there's a risk of your mobile device getting desynced from the module if you use this option.

3. You should now be at the Device Sync screen. In your mobile device open the ***Google Authenticator*** app, and select <u>*Add Account*</u> from the menu. Either scan the QR Code, or add the account information manually. Once the account has been added to your device, input the 6 digit code that appears on your device (*if you're in HOTP mode you must generate it first*) into the <u>*Enter the first Verification Code*</u> input field. Now wait for the code on your device to update (*or regenerate it if you're in HOTP mode*), and add this new code to the <u>*Enter second Verification Code*</u> field input.

Copy the displayed ***Recovery Code*** and click <u>***Confirm***</u> before the code in your app changes again. Save the ***Recovery Code*** somewhere safe, as you can use it instead of the Google Authenticator One-Time Code at login to generate a single-use token sent to your email in case you lose access to your mobile device.

4. The account is now synced, which means that from now on you will need to generate a new code with your mobile device each time you login under that account. This makes it near impossible for a hacker to brute force or even intercept your account credentials!

Important Information

➢ If you ever lose your device or somehow get locked out of your account and don't have your Recovery Code at hand, you can temporarily disable the Google Authenticator login check by going into your FTP account and adding the following line at the end of your **config/defines.inc.php** file:

define('_GOOGLE_AUTHENTICATOR_DISABLE_', true);

➢ Some *Prestashop 1.7* minor versions have a bug where the Back Office login can go blank after disabling the module. If that happens, open the module's zip file, extract the file **AdminLoginController.php** that's inside the **backup** folder, and upload it by FTP into your store's **override/controllers/admin** folder.

Final Notes

I hope you found this module easy to use, and I especially hope it can help keep your online store safe. If you liked it (or if you didn't), rate it at the **Prestashop Addons Store** and let the world know, I would love to read your opinion.

As a customer, you have access to all future updates of this module at no extra charge from your Prestashop Addons account. Remember that if you have any problems, questions or suggestions, you can always contact me through the Prestashop Addons support system.

If you're reporting a problem, please include the Prestashop version of your store, as well as the version of this module you're running.

Happy selling!