

Magento 2 Admin Security Checklist

Installation and User Guide for Magento 2 Security Checklist Extension

Table of Contents

1. Installation
 - *Download Extension*
 - *Installation via app/code*
 - *Installation via Composer*
2. Configuration Settings for Security Base
 - *General Settings*
3. Configuration Settings for Security Checklist
 - *General Settings*
4. Security Checklist Report
 - *Security Checklist Report*

Installation

- **Download Extension:** Once you have placed the order from our site then go to the Account section, click on My Downloadable Products, and download the extension package.

HOME

MAGENTO EXTENSIONS

MAGENTO 2 EXTENSIONS

MAGENTO SERVICES

OUR WORK

UPGRADE TO MAGENTO 2

ABOUT US

BLOG

CONTACT

ACCOUNT

ACCOUNT DASHBOARD

ACCOUNT INFORMATION

ADDRESS BOOK

MY ORDERS

MY PRODUCT REVIEWS

MY WISHLIST

NEWSLETTER SUBSCRIPTIONS

MY DOWNLOADABLE PRODUCTS

MY BASKET

You have no items in your shopping cart.

RECENTLY VIEWED



MAGENTO 2 ADMIN ACTION LOG

£74.99

ORDER #100004740 - COMPLETE

[Reorder](#) | [Print Order](#)

About This Order: [Order Information](#) [Invoices](#)

ORDER DATE: 24 FEBRUARY 2022

ITEMS ORDERED

	PRICE	QTY	SUBTOTAL
Links: Magento 2 Admin Activity Logger Version 2.0.2			
Subtotal			£89.99
VAT			£15.00
Grand Total			£89.99

- **Installation via app/code:** Upload the content of the module to your root folder. This will not overwrite the existing Magento folder or files, only the new contents will be added. After the successful upload of the package, run the below commands on the Magento 2 root directory.

```
php bin/magento setup:upgrade
php bin/magento setup:di:compile
php bin/magento setup:static-content:deploy
```

- **Installation via Composer:** Please follow the guide provided in the below link to complete the installation via composer.

<https://docs.scommerce-mage.com/magento-2-extensions/installation-via-composer/installation-via-composer>

Configuration Settings for Security Base

Go to **Admin > Stores > Configuration > Scommerce Configuration > Security Base**

General Settings

- **Enabled** - Select "Yes" or "No" to enable or disable the module.
- **License Key** - Please add the license for the extension which is provided in the order confirmation email. Please note license keys are site URL specific. If you require license keys for dev/staging sites then please email us at support@scommerce-mage.com.

General



Enabled [store view]	Yes	☐ Use system value
This setting will be used to enable or disable module		
License Key [store view]	\$2y\$10\$sNyuEo53zPwtA4G5j0l8e.8E/DaVJqc6VyLu6j	
This setting will be used to verify your license key for the give domain		
N.B. License keys are domain specific so for your testing or staging sites please email us at core@scommerce-mage.com		

Configuration Settings for Security Checklist

Go to **Admin > Stores > Configuration > Scommerce Configuration > Security Checklist**

General Settings

- **Enabled Security Checklist** - This setting will be used to enable or disable admin security checklist
- **Enable Database prefix check :-** This setting will be used to enable or disable check for DB prefix. Database prefix added in file, to make it work you also need to make changes in database.
- **Enable FE Captcha check:-** This setting will be used to enable or disable checks for Frontend Captcha. Go to **Stores > Configuration > Security > Google reCAPTCHA** Storefront in order to verify it.
- **Enable BE Captcha check:-** This setting will be used to enable or disable checks for Backend Captcha. Go to **Stores > Configuration > Security > Google reCAPTCHA** Admin Panel and **Stores > Configuration > Admin > CAPTCHA** Storefront in order to verify it.

- **Enable Magento version check-** This setting will be used to enable or disable check for Magento Version and latest security patches.

Security Checklist

Enabled Security Checklist [global]	Yes	☐ Use system value
This setting will be used to enable or disable admin security checklist		
Enable Database prefix check [global]	Yes	☐ Use system value
This setting will be used to enable or disable check for DB prefix. Database prefix added in app/etc/env.php file, to make it work you also need to make changes in database.		
Enable FE Captcha check [global]	Yes	☐ Use system value
This setting will be used to enable or disable checks for Frontend Captcha. Go to Stores > Configuration > Security > Google reCAPTCHA Storefront in order to verify it.		
Enable BE Captcha check [global]	Yes	☐ Use system value
This setting will be used to enable or disable checks for Backend Captcha. Go to Stores > Configuration > Security > Google reCAPTCHA Admin Panel and Stores > Configuration > Admin > CAPTCHA Storefront in order to verify it.		
Enable Magento Version check [global]	Yes	☐ Use system value
This setting will be used to enable or disable check for Magento Version and latest security patches		

- **Enable Admin Users check:-** This setting will be used to enable or disable check for Admin Users Security. Especially usernames, password lifetime policy and login activity.
Go to Stores > Configuration > Advanced > Admin > Security Or Go to System > Permission > All users to manage admin users
- **Admin Usernames Stop List:-** You can add list of usernames that shouldn't be used for admin accounts. Comma separated.
- **Enabled Admin Path Check:-** This setting will be used to enable or disable check for Admin Path Security. Admin Path is configured in file or go to **Advanced > Admin > Admin Base URL > Use Custom Admin Path** to change it
- **Admin Path Stop List:-** You can add list of paths that shouldn't be used for admin. Comma separated.
- **Enable Content Script Check:-** This setting will be used to enable or disable check for scripts added in your content or configuration

Enable Admin Users check

[global]

Yes

▼

☐ Use system value

This setting will be used to enable or disable check for Admin Users Security. Especially usernames, password lifetime policy and login activity.

Go to **Stores > Configuration > Advanced > Admin > Security**

Or

Go to **System > Permission > All users** to manage admin users

Admin Usernames Stop List

[global]

admin,office,manager,support,asd,qwe

☐ Use system value

You can add list of usernames that shouldn't be used for admin accounts. Comma separated.

Enable Admin Path check

[global]

Yes

▼

☐ Use system value

This setting will be used to enable or disable check for Admin Path Security. Admin Path is configured in **app/etc/env.php** file or go to **Advanced > Admin > Admin Base URL > Use Custom Admin Path** to change it

Admin Path Stop List

[global]

admin,office,MANAGER

☐ Use system value

You can add list of paths that shouldn't be used for admin. Comma separated.

Enable Content Script Check

[global]

Yes

▼

☐ Use system value

This setting will be used to enable or disable check for scripts added in your content or configuration

- **Enabled Checklist Check Cron Job:-** If enabled the security checklist also checks whether admin 2FA is enabled or not.
- **Enabled Checklist Check Cron Job:-** This setting will be used to enable or disable checklist cron job
- **Checklist Cron Schedule:-** This will allow you to define schedule how often you want to clear Login Attempts logs cron.

Enable Admin 2FA check

[global]

Yes

▼

☐ Use system value

This setting will be used to enable or disable checks for Admin 2FA. Go to **Stores > Configuration > Security > 2FA**

Enabled Checklist Check Cron Job

[global]

Yes

▼

☐ Use system value

This setting will be used to enable or disable checklist cron job

Checklist Cron Schedule

[global]

*/2 ****

☐ Use system value

This will allow you to define schedule how often you want to clear Login Attempts logs cron

```

* * * * *
| | | | |
| | | | +---- Day of the Week (range: 1-7, 1 standing for Monday)
| | | +----- Month of the Year (range: 1-12)
| | +----- Day of the Month (range: 1-31)
| +----- Hour (range: 0-23)
+----- Minute (range: 0-59)
Example: 0 0 * Daily at midnight

```

Security Checklist Report

Go to **Admin > System > Scommerce Security> Security Checklist**

Security Checklist Report

The Security checklist grid has several distinctions for various checks: Warning, Error and Success

- **Admin password Protection:** - For Admin password protection, if a password change is not forced, the user will see an error. If the lifetime is more than 90 days, the user will see a warning. If a password change is forced and the lifetime is less than 90 days, then the user will see success.
- **Magento version check:** - For a Magento version check, if the version is outdated, the user will see an error. Otherwise, the user will see success.
- **Database Prefix check:** - For the Database prefix check, if the table prefix is not set in the configuration file, the user will see an error. Otherwise, the user will see success.
- **Frontend ReCaptcha Protection** - For Frontend ReCaptchaProtection, if all frontend forms are protected with recaptcha, the user will see a success. When some forms are protected, the user will see a warning. If none of the forms are protected, the user will see an error.
- **Admin Captcha Protection:**- For Admin Captcha protection, if all backend forms are protected with Captcha, the user will see a success. When some forms are protected, the user will see a warning. If none of the forms are protected, the user will see an error.
- **Admin path protection:** - For Admin path protection, if the user's admin path doesn't contain words from the stop list, doesn't contain numbers or capital letters, and is at least 15 characters long, the user will see a success. If any of the criteria mentioned are not fulfilled, the user will see a warning.
- **Admin usernames check:**- For Admin usernames check, if the username contains words from the stop list or if the username contains numbers, the user will see a warning. Otherwise, success.
- **Admin users activity check:** - For Admin admin user activity check, if the account is unused, the user will see a warning. Otherwise, success.
- **Check for static scripts inserted from Config and CMS Pages:** - For Static scripts in Configuration, CMS Blocks, and CMS Pages, if a text field has a static script, the user will see a warning. Otherwise, success.
- **Check for static scripts inserted from Product Attributes:** - For Static scripts inserted by any product attributes the user will see a warning with the name of the attribute otherwise, success.
- **Check for Admin 2FA:** - It also checks whether admin 2FA is enabled or not.

Generate Report

• Your Magento version is outdated. Upgrade Magento to protect your store. Your version - 2.4.5-p2. Latest Version - 2.4.6-p4.

- Table prefix is NOT set in configuration file

- reCaptcha IS DISABLED for all frontend forms

- Admin forms are not protected with Captcha

- Following Blocks contain scripts.
 - ID - 1, Title - Footer Links Block, Identifier - footer_links_block

- Following pages contain scripts.
- ID - 5. Title - About us... Identifier - about-us

- There are several product attributes that contain static scripts
 - Attribute `meta_title` of product `Complete Track Tote` has script. SKU - 24-WB02
 - Attribute `meta_keyword` of product `Complete Track Tote` has script. SKU - 24-WB02

- Value(s) of attribute 'test_attribute' contains static scripts. Attribute Code - test_attribute

- Your admin path contain words from stop list
- Admin path should contain following characters - numbers, capital letters
- Your Admin path looks short. We recommend to set length at least 15 characters.

- This username contains words frc
- This username contains numbers
- This username contains words frc
- This username contains numbers
- This username contains numbers
- This username contains numbers
- This username contains numbers
- This username contains numbers
- This username contains words frc
- This username contains words frc
- This username contains numbers
- This username contains words frc
- This username contains numbers
- This username contains numbers
- This username contains numbers
- This username contains words frc
- This username contains words frc
- This username contains words frc
- This username contains words frc
- This username contains words frc
- This username contains words frc
- This username contains numbers
- This username contains words frc
- This username contains numbers
- We don't recommend using admin usernames that contain common words and numbers.

 Admin 2FA

- Magento Two Factor Authentication module is disabled

 Check for static scripts inserted from Config

- There are no config fields that contain scripts.

 Check for static scripts inserted from Category Attributes

- There are no product attributes that contain static scripts

 Admin password protection

- Password change is forced and its lifetime is less or equal to 3 month

Your store is **20.00%** protected

Errors - 4

Warnings - 8

Success - 3

If you have a question related to this extension please check out our **FAQ Section** first. If you can't find the answer you are looking for then please contact **support@scommerce-mage.com**.

Revision #6

Created 9 June 2025 10:35:51 by scommerce

Updated 24 October 2025 09:46:59 by scommerce