

Magento 2 Security Suite

Installation and User Guide for Magento 2 Security Suite 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. Configuration Settings for Admin Activity Logger
 - *General Settings*
 - *Modules Activity Logger*
 - *Admin Activity Logger*
 - *Admin Activity Grid*
 - *Admin Logger Detailed View for Admin Activities*
 - *Admin Logger Detailed View for Item Info*
 - *Login Activity Grid*
 - *Active Sessions Grid*
5. Configuration Settings for Advanced Login Security
6. Scommerce Admin Login Security
 - *Admin Login Attempts*
 - *Blacklist*
 - *Whitelist*
7. Security Checklist Report
 - *Security Checklist Report*

Installation

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@sccommerce-mage.com.

General

Enabled
[store view] Use system value

This setting will be used to enable or disable module

License Key
[store view]

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@sccommerce-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 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

<p>Enabled Security Checklist <small>[global]</small></p>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
<p><small>This setting will be used to enable or disable admin security checklist</small></p>		
<p>Enable Database prefix check <small>[global]</small></p>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
<p><small>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.</small></p>		
<p>Enable FE Captcha check <small>[global]</small></p>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
<p><small>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.</small></p>		
<p>Enable BE Captcha check <small>[global]</small></p>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
<p><small>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.</small></p>		
<p>Enable Magento Version check <small>[global]</small></p>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
<p><small>This setting will be used to enable or disable check for Magento Version and latest security patches</small></p>		

- **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 and 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] 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] Use system value

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

Enable Admin Path check [global] 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] Use system value

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

Enable Content Script Check [global] 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:-** 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.

Enabled Checklist Check Cron Job [global] Use system value

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

Checklist Cron Schedule [global] 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
```

Configuration Settings for Admin Activity Logger

Go to **Admin > Stores > Configuration > Scommerce Configuration > Admin Activity Logger**

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 core@scommerce-mage.com
- **Admin Users Login Activity Enabled** - Enable / Disable activity. It will log login activity of the admin users.
- **Page visit History Enabled** - Enable / Disable page history visiting log.
- **Clear Admin Activity Logs After** - Enter value. Clear all admin activity logs will be cleared after X days.
- **Enabled Profiler** - Enable / Disable time profiler. Duration of the operations will be logged.

General Settings

Enable [global]	Yes	Select "Yes" to enable the module
License Key [global]	\$2y\$10\$CX9OoffrygtWDupfr19zhez0MIQntxWjQ5eGr/EoDzwf5p8iVUucq	Enter the License key for the module
Admin users Login Activity Enabled [global]	Yes Will log login activity of the admin users	Select "Yes" to enable the Admin users Login Activity
Page Visit History Enabled [global]	Yes Enable page history visiting log	Select "Yes" to enable the Page Visit History
Clear Admin Activity Logs After [global]	7 Clear all admin activity logs will be cleared after X days	Please add the Clear Admin Activity Logs After
Enable Profiler [global]	No Enable time profiler. Duration of the operations will be logged	Select "Yes" to enable the Profiler

Modules Activity Logger

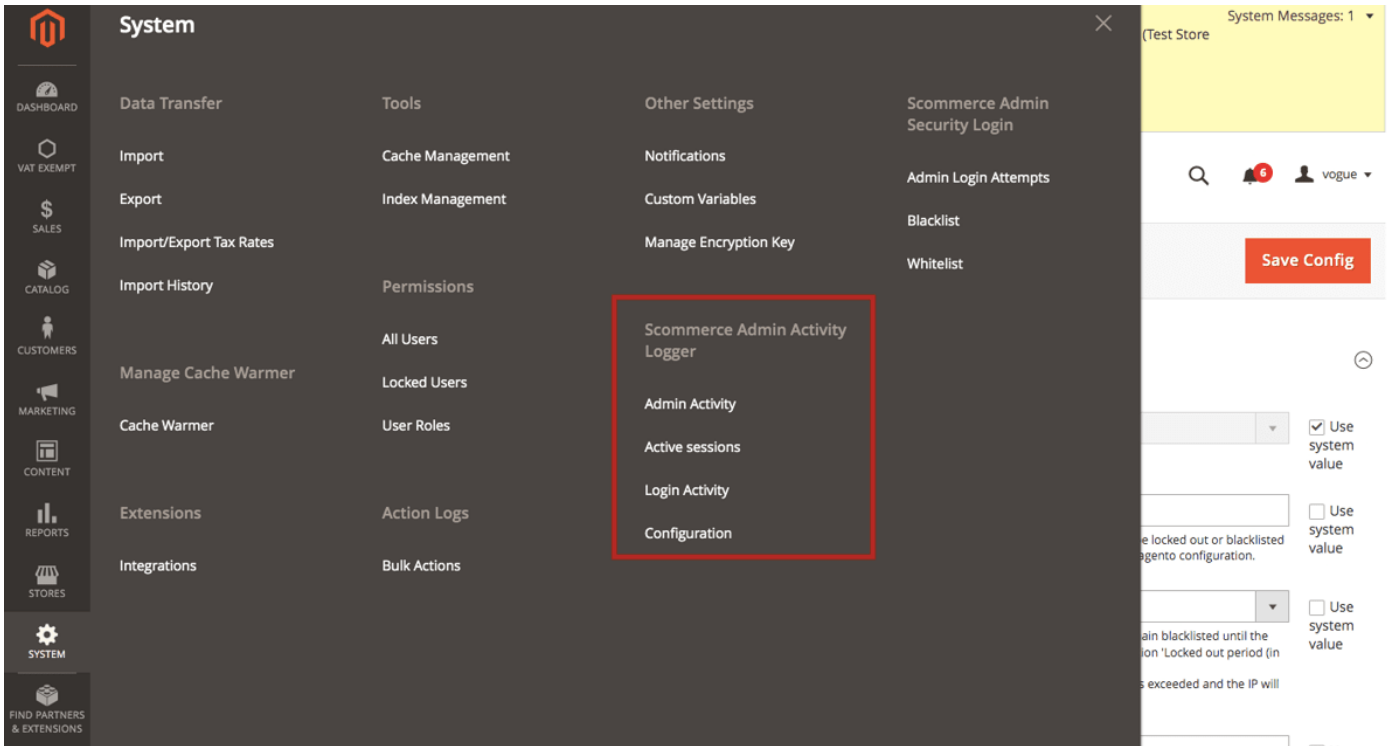
- **Order** - Select "Yes" to enable. It will log order related activities.
- **Product** - Select "Yes" to enable. It will log product related activities.
- **Category** - Select "Yes" to enable. It will log category related activities.
- **Customer** - Select "Yes" to enable. It will log customer related activities.
- **Email Template** - Select "Yes" to enable.
- **Page** - Select "Yes" or "No" to Enable / Disable.
- **Block** - Select "Yes" or "No" to Enable / Disable.
- **Widget** - Select "Yes" or "No" to Enable / Disable.
- **Theme** - Select "Yes" or "No" to Enable / Disable.
- **System Configuration** - Select "Yes" or "No" to Enable / Disable.

- **Product Attributes** - Select "Yes" or "No" to Enable / Disable.
- **Admin User** - Select "Yes" to enable. It will log all users activities.
- **SEO** - Select "Yes" or "No" to Enable / Disable.

Module Activity Logger

Order [global]	Yes	▼
Product [global]	Yes	▼
Category [global]	Yes	▼
Customer [global]	Yes	▼
Promotion [global]	Yes	▼
Email Templates [global]	Yes	▼
Page [global]	Yes	▼
Block [global]	Yes	▼
Widget [global]	Yes	▼
Theme [global]	Yes	▼
System Configuration [global]	Yes	▼
Product Attributes [global]	Yes	▼
Admin user [global]	Yes	▼
SEO [global]	Yes	▼

- **Admin Activity Logger** - You can view admin activity logger from, **Admin > System > Scommerce Admin Activity Logger > Admin Activity / Login Activity.**



- **Admin Activity Grid** - In the back-end under Admin Activity Logger grid you can view all the admin activities details from **Admin > System > Admin Activity Logger**. This grid will have, Admin Username, Name, Activity Type, Store View, Module, Full Action, IP, Item, Revert and Action columns.
 - **Date:** - The exact date and time of the activity performed.
 - **Admin Username:** - user name of the admin.
 - **Name:** - The name of the admin.
 - **Activity Type:** - Type of activity performed
 - **Store view:** - Name of the store view
 - **Module:** - The name of the module used in the activity.
 - **Full Action:** - It contains the URL path of the activity performed.
 - **IP Address:** - The IP address of the user.
 - **Item:** - Activity related item such as a product or system configuration changes.
 - **Revert:** - If the action is not complete then the REVERT column will have the notification.
 - **Action:** - It contains view where you can see the key details of the activity such as general and item info.

Date	Admin Username	Name	Activity Type	Store View	Module	Full Action	IP	Item	Revert
2019-11-24 19:36:33	admin	System Administrator	Edit	All Store Views	System Configuration	Adminhtml/System/Config/Save	92.7.125.222	System Configuration	REVERT
2019-12-20 06:30:37	admin	System Administrator	Edit	All Store Views	System Configuration	Adminhtml/System/Config/Save	82.129.56.134	System Configuration	REVERT
2019-12-30 04:34:49	admin	System Administrator	Edit	Main Website Main Website Store Default Store View	Sales Order	Sales/Order/Create/Save	82.129.56.134		REVERT
2020-01-13 08:52:54	admin	System Administrator	Edit	All Store Views	Catalog Product	Catalog/Product/Save	59.144.175.236	Joust Duffie Bag	REVERT
2019-11-24 19:39:36	admin	System Administrator	Edit	All Store Views	System Configuration	Adminhtml/System/Config/Save	92.7.125.222	System Configuration	REVERT
2019-12-30 04:35:01	admin	System Administrator	Edit	Main Website Main Website Store Default Store View	Sales Order	Sales/Order/Create/Save	82.129.56.134	00000068	REVERT
2019-12-20 06:33:42	admin	System Administrator	Edit	All Store Views	Catalog Product	Catalog/Product/Save	82.129.56.134	Joust Duffie Bag	REVERT
2019-11-24 19:50:17	admin	System Administrator	Edit	All Store Views	Catalog Product	Catalog/Product/Save	92.7.125.222	Joust Duffie Bag	REVERT
2019-12-30 04:35:52	admin	System Administrator	Edit	Main Website Main Website Store	Sales Order	Sales/Order/Invoice/Save	82.129.56.134	00000068	REVERT

Admin Activity Logger

- **Admin Logger Detailed View for Admin Activities** - To get more details about each particular action simply click on the 'View' link from **Admin > System > Admin Activity Logger > Select Log > Click on 'View' > General, to view all the detailed data.**
 - You can view all the general details of the user's activity in the general tab.

ACTIVITY LOG DETAILS

General

General Information

Admin Username	activitylogger
Name	activitylogger activitylogger
Store View	0 Admin
Scope	default
Action Type	view

- **Admin Logger Detailed View for Item Info** - You can view the item details from **Admin > System > Admin Activity Logger > Select Log > Click on 'View' > Items info.**
 - This section contains all granular information. For instance if you place an order from the admin panel then all the details of the order such as price, store, etc. Are visible in this section.

ACTIVITY LOG DETAILS

General

Items info

Search [Reset Filter](#) 1 records found

100 per page 1 of 1

Field Name	Old Value	New Value
price	32.0000	42.0000

- **Login Activity Grid** - You can view login activities from **Admin > System > Scommerce Admin Activity Logger > Active Sessions**. It logs details of each and every single activity along with what value being changed by who and when. This section contains following information: -
 - **Date:** - The precise date and time of the log.
 - **Type:** - whether logged in or logged out.
 - **Username:** - Username of the person is stored here.
 - **Name:** - Name of the user
 - **Ip Address:** - You can see the IP address here.
 - **User Agent:** - The browser and device details of the user are shown here.
 - **Status:** - If the login fails then the status will show FAILED and if the login or logout is successful then it shows SUCCESS

Login Activity Logger

29 records found

Date	Type	Username	Name	IP Address	User Agent	Sta
2019-01-09 18:08:50	Login	activitylogger	Activitylogger Activitylogger	92.2.1.188	Browser Name: Chrome Browser Version: 71.0.3578.98 Platform: Windows Device: Desktop	S
2019-01-09 18:08:37	Logout			92.2.1.188	Browser Name: Chrome Browser Version: 71.0.3578.98 Platform: Windows	S

Filters Default View CC

20 per page 1 of 1

- **Active Sessions Grid**- You can view Active Sessions from **Admin > System > Login Activity > Login Acti**. It logs details of every active admin session on the store. The active session is listed with various useful details. Also, it gives the admin the option to terminate any active admin session through the "Terminate" button under the action column. Once terminated that admin will be logged out of the account automatically. Furthermore, the grid is completely filterable using various columns. This section contains the following information: -
 - **Id:** - A Unique ID for each active session.
 - **Admin Username:** - Username of the admin of that particular active session.
 - **IP:** - IP address of the admin of that session.
 - **Last Action:** - Last action performed by the admin of this session.

- **User Agent:** - Various platform, device, and browser information of the admin of this session.
- **Action:** - Contains the option to terminate this particular session.

Active Sessions

Search:

Filters:

Actions:

2 records found | 20 per page | 1 of 1

id	Admin Username	IP	Last Action	User Agent	Action
1315	admin.login	27.72.103.14	None	Browser Name: unknown Browser Version: unknown Platform: unknown Device: Desktop	Terminate
1316	vogue	106.51.62.187	None	Browser Name: Chrome Browser Version: 116.0.0.0 Platform: Apple Device: Desktop	Terminate

Configuration Settings for Admin Login Security

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

General Settings

- **Enabled Admin Login Security** - Select "Yes" or "No" to enable or disable the module.
- **Failed Attempts Limit** :- Set the attempt limit for admin login. Once exceeded the account will be locked out or blacklisted as per further configuration. Make sure this limit is less than default Magento configuration.
- **Apply Action On Exceed Limit**:- Choose the penalty for exceeding the failed attempt limit, between "Lockout" or "Blacklist.
 - Lockout** - When the number of failed attempts exceeds, the IP will remain blacklisted until the 'Valid till' time limit. The 'Valid till' limit can be defined by the configuration 'Locked out period (in hours)'
 - Blacklist** - This action will be applied when the 'Failed Attempts Limit' is exceeded and the IP will be blacklisted until it is manually removed.
- **Locked out period (in hours)**:- Set the "Valid Till" limit for the Lockout feature. The accounts will be locked out for period entered in this configuration.
- **Block Email Enabled**:- Enable Emails when any lockout or blacklist occurs. The email is sent to the Store Owner as well as the blacklisted/locked-out user.

Admin Login Security



Enabled Admin Login Security <small>[global]</small>	<input type="text" value="Yes"/>	<input checked="" type="checkbox"/> Use system value
	This setting will be used to enable or disable admin login security	
Failed Attempts Limit <small>[global]</small>	<input type="text" value="3"/>	<input type="checkbox"/> Use system value
	Set the attempt limit for admin login. Once exceeded the account will be locked out or blacklisted as per further configuration. Make sure this limit is less than default Magento configuration.	
Apply Action On Exceed Limit <small>[global]</small>	<input type="text" value="Lockout"/>	<input checked="" type="checkbox"/> Use system value
	Lockout - When the number of failed attempts exceeds, the IP will remain blacklisted until the 'Valid till' time limit. The 'Valid till' limit can be defined by the configuration 'Locked out period (in hours)' Blacklist - This action will be applied when the 'Failed Attempts Limit' is exceeded and the IP will be blacklisted until it is manually removed.	
Locked out period (in hours) <small>[global]</small>	<input type="text"/>	<input checked="" type="checkbox"/> Use system value
	Set the "Valid Till" limit for the Lockout feature. The accounts will be locked out for period entered in this configuration.	
Block Email Enabled <small>[global]</small>	<input type="text" value="Yes"/>	<input type="checkbox"/> Use system value
	Enable Emails when any lockout or blacklist occurs. The email is sent to the Store Owner as well as the blacklisted/locked-out user.	

- **IP Block Email Template:-** Select the email template to be used to send the email when a lockout/blacklist occurs.
- **Block And Lock Event Email Sender:-** Select the sender email from your Default Magento configuration in case of lockout or blacklist.
- **Recipient Block Email:-** Add the email (store owner) which will get emails about each and every lockout/blacklist. Whenever a lockout/blacklist happens the email will be sent to this address as well as the user.
- **Enabled Clear Login Attempts Logs Cron Job:-** Set "Yes" or "No" to enable or disable clear logs cron job.
- **Clear Login Attempts Logs Cron Schedule:-** Set the cron job to define how often you want to clear Login Attempts logs

IP Block Email Template
[global]

IP Block Email Template (Default) ▼

Select the email template to be used to send the email when a lockout/blacklist occurs.

Use system value

Block And Lock Event Email Sender
[global]

General Contact ▼

Select the sender email from your Default Magento configuration in case of lockout or blacklist.

Use system value

Recipient Block Email
[global]

Add the email (store owner) which will get emails about each and every lockout/blacklist. Whenever a lockout/blacklist happens the email will be sent to this address as well as the user.

Use system value

Enabled Clear Login Attempts Logs Cron Job
[global]

Yes ▼

This setting will be used to enable or disable clear logs cron job

Use system value

Clear Login Attempts Logs Cron Schedule
[global]

0 0 1 * *

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

Use system value

```

* * * * *
| | | | |
| | | | +---- 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

```

- **Clear Login Attempts Logs Older Than X Days:-** Set the number of days based on which the Login attempts Logs will be cleared based which are older than the set days. For eg:- if set 2, any login attempts logs older than 2 days will be cleared.
- **Enabled Clear Lockouts Cron Job:-** Set "Yes" or "No" to enable or disable clear of not active lockouts by cron job
- **Clear Lockouts Cron Schedule:-** Set the cron job to define schedule how often you want to clear logs
- **Allowed Countries:-** Block users from one or multiple countries. If no country is selected, all countries are allowed.

Clear Login Attempts Logs Older Than X Days [global] Use system value
 Set the number of days based on which the Login attempts Logs will be cleared based which are older than the set days. For eg:- if set 2, any login attempts logs older than 2 days will be cleared.

Enabled Clear Lockouts Cron Job [global] Use system value
 This setting will be used to enable or disable clear of not active lockouts by cron job

Clear Lockouts Cron Schedule [global] Use system value
 This will allow you to define schedule how often you want to clear 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

Allowed Countries [website] Use system value

Congo - Brazzaville
 Congo - Kinshasa
 Cook Islands
 Costa Rica
 Côte d'Ivoire
 Croatia
 Cuba
 Curaçao
 Cyprus
 Czechia

Block users from one or multiple countries. If no country is selected, all countries are allowed.

- **Enabled Whitelist:-** Set "Yes" or "No" to enable or disable whitelisting for an IP. If enabled, the user won't be allowed to log in until the IP is whitelisted.
- **Whitelist Email Enabled:-** Set "Yes" or "No" to enable or disable whitelist Email. If this is enabled, the user will be sent an email with a link that allows them to either approve or deny the login.
 - Approve** - By approving, the IP will be added to the whitelist.
 - Deny** - The IP will be added to the blacklist if denied.
- **Whitelist request lifetime:-** Set the request lifetime to define how long whitelist request will be valid in hours By default 1 hour.
- **IP Whitelist Email Template:-** Select the email template for the login approval email that is sent to the user, based on the approval the user is whitelisted or blacklisted.
- **Whitelist Event Email Sender:-** Select the sender email to be used to send out the User approval/whitelist email to the user.
- **Recipient Email:-** Add the email (store owner) which will get emails about User approval/Whitelist emails. Whenever a user-approval/whitelist happens the email will be sent to this address as well as the user so store owner can also approve or deny the user from the email.

Enabled Whitelist <small>[global]</small>	Yes	<input type="checkbox"/> Use system value
	<small>This setting is intended to enable or disable whitelisting for an IP. If enabled, the user won't be allowed to log in until the IP is whitelisted.</small>	
Whitelist Email Enabled <small>[global]</small>	Yes	<input type="checkbox"/> Use system value
	<small>If this is enabled, the user will be sent an email with a link that allows them to either approve or deny the login. Approve - By approving, the IP will be added to the whitelist. Deny - The IP will be added to the blacklist if denied.</small>	
Whitelist request lifetime <small>[global]</small>	1	<input checked="" type="checkbox"/> Use system value
	<small>This setting will be used to define how long whitelist request will be valid in hours By default 1 hour</small>	
IP Whitelist Email Template <small>[global]</small>	Whitelist Login Attempt Email Template (Default)	<input checked="" type="checkbox"/> Use system value
	<small>Select the email template for the login approval email that is sent to the user, based on the approval the user is whitelisted or blacklisted.</small>	
Whitelist Event Email Sender <small>[global]</small>	General Contact	<input checked="" type="checkbox"/> Use system value
	<small>Select the sender email to be used to send out the User approval/whitelist email to the user.</small>	
Recipient Email <small>[global]</small>		<input checked="" type="checkbox"/> Use system value
	<small>Add the email (store owner) which will get emails about User approval/Whitelist emails. Whenever a user-approval/whitelist happens the email will be sent to this address as well as the user so store owner can also approve or deny the user from the email.</small>	

Scocommerce Admin Login Security

Go to **Admin > System > Scocommerce Admin Login Security>**

Admin Login Attempts

The Admin Login Attempts grid keeps a record of every login attempt made to the admin panel with various key details such as:-

- ID
- IP Address
- Success
- Admin Username
- Created At

The grid is completely filterable with various columns such as ID, IP Address, Admin Username, Created At, etc.

Admin Login Attempts

Filters | Default View | Columns

ID from: to: Admin Username from: to: Created At from: to: IP Address:

Cancel Apply Filters

92 records found

20 per page | 1 of 5

ID	IP Address	Success	Admin Username	Created At
112	5.64.221.36	SUCCESS	koshlesh	2023-12-27 10:08:45
113	178.205.102.186	SUCCESS	alexdemo4	2023-12-27 11:44:55
114	178.205.102.186	SUCCESS	alexdemo4	2023-12-27 11:47:26
115	178.205.102.186	SUCCESS	alexdemo4	2023-12-27 11:49:01
116	5.64.221.36	SUCCESS	login.activity	2023-12-27 12:01:37
117	178.205.102.186	SUCCESS	alexdemo4	2023-12-27 12:04:53

Blacklist

The blacklist records grid contains information about all the blacklist users with several details such as ID, IP Address, Admin Username, Valid till, Created At, and Action. This grid is completely filterable. Each of the record can be deleted or edited from the Action column.

Blacklist

Add Entry

Filters | Default View | Columns

ID from: to: Valid till from: to: Created At from: to: IP Address: Admin Username:

Cancel Apply Filters

2 records found

20 per page | 1 of 1

ID	IP Address	Admin Username	Valid till	Created At	Action
28	23.106.56.43	alexdemo4	2023-12-29 13:48:06	2023-12-29 11:48:06	Select
32	82.132.230.161			2023-12-29 12:14:05	Edit Delete

Go to **Action>Edit** and you can change various details for each of the records such as IP Address, Username, and Valid till date.

IP Address * 23.106.56.43

Admin User alexdemo4

Valid Till 12/29/2023

Created At 12/29/2023

Whitelist

The Whitelist records grid contains information about all the blacklist users with several details such as ID, IP Address, Admin Username, Created At, and Action. This grid is completely filterable. Each of the records can be deleted or edited from the Action column.

Whitelist

Add Entry

2 records found

Filters Default View Columns

20 per page 1 of 1

ID	IP Address	Admin Username	Created At	Action
3	106.51.62.187		2023-12-28 09:23:45	Select
12	178.205.102.186	alexdemo4	2023-12-29 11:26:23	Select

Go to **Action>Edit** and you can change various details for each of the records such as IP Address, and Username.

IP Address * 178.205.102.186

Admin User alexdemo4

Created At 12/29/2023

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 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.

Here is your security report from 2024-01-30 13:08:10

[Generate Report](#)

 Database prefix check
- Table prefix is NOT set in configuration file
 Magento version check
- Your Magento version is outdated. Upgrade Magento to protect your store. Your version - 2.4.5-p2. Latest Version - 2.4.6-p3.
 Frontend ReCaptchaProtection
- reCaptcha IS DISABLED for all frontend forms
 Admin Captcha protection
- Admin forms are not protected with Captcha
 Check for static scripts in CMS Blocks
- Following Blocks contain scripts. - ID - 2, Title - Contact us info, Identifier - contact-us-info
 Admin path protection
- 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.
 Admin usernames check
- This username contains words from stop list - admin

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 #9

Created 9 June 2025 12:14:12 by sccommerce

Updated 24 October 2025 09:47:18 by sccommerce