



# SECURITY SUITE

MAGENTO 2

## [Security Suite – Magento 2](#) [User Guide](#)

## Table Of Contents

<b>Preface.....</b>	<b>3</b>
<b>Installation Guide.....</b>	<b>4</b>
Option 1: Magento 2 install extension using COMMAND LINE .....	4
Option 2: Magento 2 install extension manually .....	5
<b>Back-end Example.....</b>	<b>6</b>

## Preface

- Security Suite Extension is the Perfect for Security Purpose. its help to protected Magento 2 store from Hackers. its easily control all back-end activities and Its effectively provide warning to you. so your store information completely protected.
  
- **Security Suite** Module Helps You to:
  - Show all Admin User Login Detail.
  - Show all Admin Actions Detail.
  - Show all File Changes Detail.
  - Show Security Checklist.
  - Take Backup as per Schedule all Admin Action Detail.
  - Send Mail After Failed Login.
  - Set Black IP Address.
  - Set Away Mode.

## Installation:

There are two ways of installing extension in magento2.

- Using COMMAND LINE.
- Manually Install extension.

### **Option 1: Magento 2 install extension using COMMAND LINE (Recommended)**

Follow below steps to install extension from the command line.

**Step 1:** Download the extension and unzip it.

**Step 2:** Upload it to code directory in your magento installation's app directory If code directory does not exists then create.

**Step 3:** Disable the cache under System -> Cache Management.

**Step 4:** Enter the following at the command line:

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

**Step 5:** Once you complete above steps log out and log in back to the admin panel and switch to **Stores -> Configuration -> Mageants** → **Security Suite**, the module will be displayed in the admin panel.

## Option 2: Magento 2 install extension manually

- Step 1:** Download the extension and unzip it.
- Step 2:** Upload it to code directory in your magento installation's app directory  
If code directory does not exists then create.
- Step3:** Disable the cache under System->Cache Management Edit  
app/etc/config.php file and add one line code:  
**'Mageants\_SecuritySuite' => 1.**
- Step 4:** Disable the cache under System -> Cache Management
- Step 5:** Once you complete above steps log out and log in back to the admin panel and switch to **Stores -> Configuration -> Mageants → Security Suite** the module will be displayed in the admin panel.

## Back-end Example

### CONFIGURATION

- ➔ After Installation of Security Suite to magento admin panel for set configuration of the extension.
- ➔ You can find configuration at **Stores -> Configuration -> Mageants -> Security Suite -> General**
- ➔ Set Module Enable “Yes” or “No”.

## Configuration

🔍 🔔 👤 admin ▾

Scope: Default Config ▾ ?

Save Config

MAGEANTS ^

Security General ⌵

Security Suite

Enable  
[store view] Yes ▾

GENERAL ▾

Security Brute Force Protection ⌵

- ➔ Stores -> Configuration -> Mageants -> Security Suite
  - > Brute Force Protection
- ➔ Set **Brute Force Protection** Enable “Yes” or “No”.
- ➔ Enter your Security Email Address(\* Require Field). Add Multiple Emails With ( , )Separate.
- ➔ Enter Maximum number of failed login attempts after mail send admin email address and mention email address.
- ➔ Set **User Alert** “Yes” or “No”.
- ➔ After Maximum number Failed Attempt User lock For Mention time(Min).

## Security Brute Force Protection



**Enable**  
[store view] Yes ▼

**Send Warning Emails**  
[store view] support@mageants.com

Mention Multiple Email Separated With (,). All Warning Letters Will Be Sent In Mention Emails.

**How Many Times Allow For Failed Login Attempts**  
[store view] 2

**Blocked Duration**  
[store view] 2

User Attempts(How Many Times Allow For Failed Login Attempts).The Period Of Time(min) The Failed User Not Able To Login.

**Locked User Alert**  
[store view] Yes ▼

**Email Template**  
[store view] Bad Login Warning Template (Default) ▼

➔ After complete Block Duration time admin can login with correct user name and password.



The screenshot displays the Magento login interface. At the top left is the Magento logo, consisting of an orange hexagon with a white 'M' inside, followed by the word 'Magento' in a grey sans-serif font. Below the logo is a yellow rectangular warning box containing a small orange triangle with an exclamation mark and the text: 'Now You Not Login Store Because You Max Time Fail Logins Try. Now You Try Login After 2 Min'. Underneath the warning box are two input fields: 'Username \*' and 'Password \*', each with a red asterisk indicating a required field. Below the password field is a blue link that says 'Forgot your password?'. At the bottom of the form is an orange rectangular button with the text 'Sign in' in white.



➔ If admin user try login with incorrect credential. so mail goes to admin and your mention security email address .



## Bad Login Notification

Mageants Security detected unusual activities in your store

User Name	Ip	Time
admin		12:07:26

You received this email to let you know about important security alerts to your store.

Copyright (c) 2020 Mageants.

→ If anonymous admin user try to login with incorrect credentials then mail goes to your mention security email address .



## Anonymous Person Try to Login Notification

---

Mageants Security detected unusual activities in your store

User Name	Ip	Time
admininfo		12:21:13

---

You received this email to let you know about important security alerts to your store.

Copyright (c) 2020 Mageants.

➔ Stores -> Configuration -> Mageants -> Security Suite -> Blacklist IPs

➔ Enter Black List IP(s).

➔ Login Attempts from these Ips will be prevented store to login.

## Security Blacklist IPs



Blacklist(s)  
[store view]

Place The IPs Which You Want To Block. Separated with add (,), ex 192.127.0.1,190.127.\*.\*

➔ If login attempts from these IPs will be prevented Your Store to Login.



➔ Stores -> Configuration -> Mageants -> Security Suite

-> Action Log Backup

➔ Set **Action Log Backup** Enable “Yes” or “No”.

➔ Select Backup Frequency.

➔ As per your select backup frequency option your Csv file generated automatically and saved.

---

## Security Action Log Backup ⌵

**Enable**  
[store view] Yes ▾

**Frequency**  
[store view] Daily ▴

- Daily
- Weekly
- Monthly

---

## Security Away Mode ⌵

- ➔ Stores -> Configuration -> Mageants -> Security Suite -> Away Mode
- ➔ Set **Away Mode** Enable “Yes” or “No”.
- ➔ Select From Time(Start Time) – To Time(End Time).
- ➔ Select Days of Week.

## Security Away Mode



**Enable**  
[store view] Yes

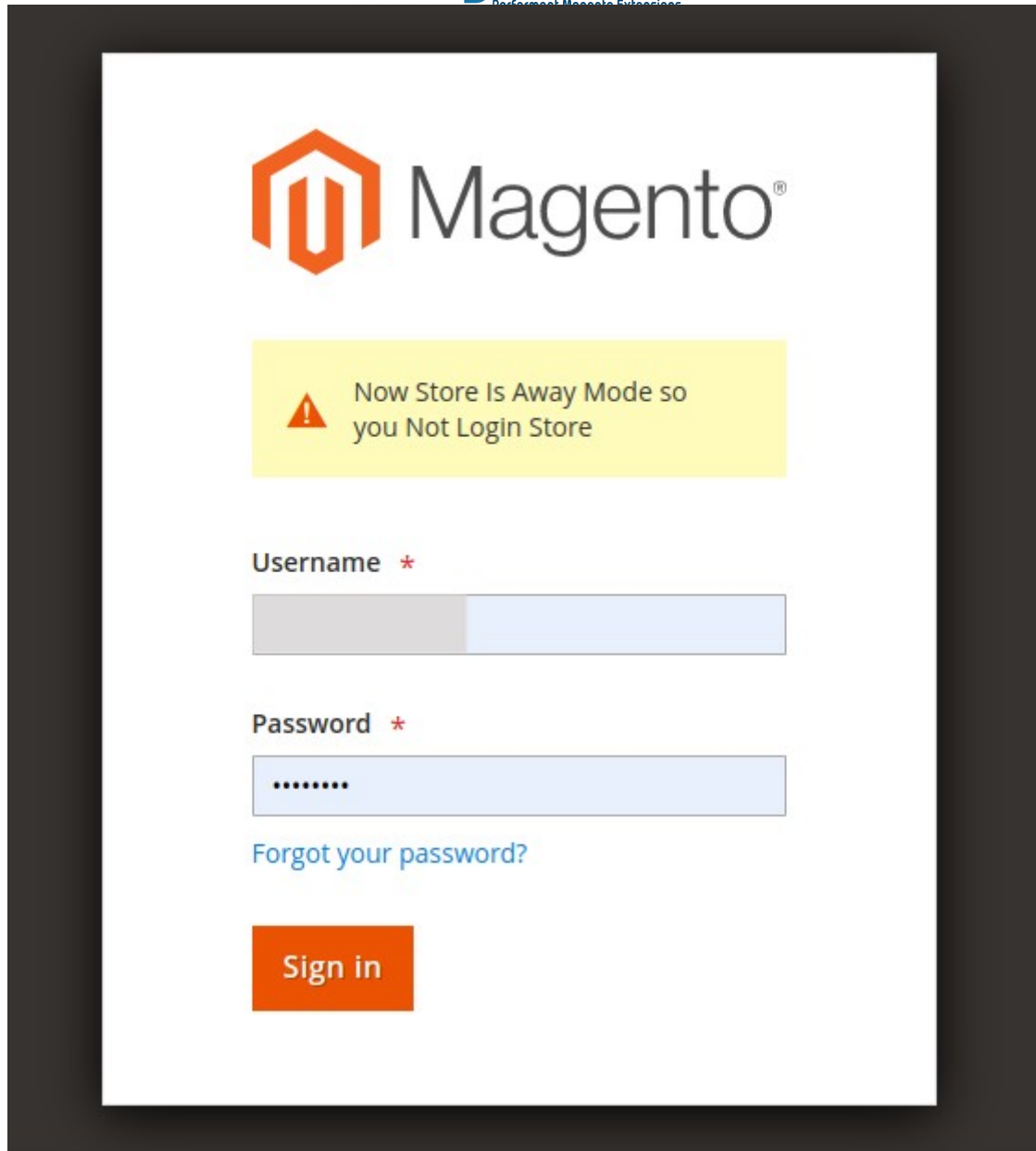
**From Time**  
[store view] 15 : 00 : 00

**To Time**  
[store view] 15 : 11 : 05

**Days Of Week**  
[store view]

- Sunday
- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday

- ➔ If away mode is enable selected days admin can't login in store.
- ➔ If away mode is enable selected start time to end time admin can't login in store.



- In an emergency case if away mode is enable and admin want to do login into store. so use **php bin/magento Awaymode:disable** and **php bin/magento cache:flush** this command for disable away mode so admin can login into store. This Command Not Available In Magento 2.1 Versions you need to Change Value In Database.

➔ Stores -> Configuration -> Mageants -> Security Suite

-> [File Change Log](#)

➔ Set [File Change Log](#) Enable “Yes” or “No”.

### Security File Change Log Enable



Enable  
[store view]

➔ **Security Suite -> File Change Log**

➔ If file Change Log is Enable Yes so Cron Runs Daily and Detect All Change File and Save Change File Details.

➔ File Change Log provide Changes files details like File Change Time, File Name, File Path, File Type.

➔ Also you can Create Csv and Excel XML File For Backup or Reference.

## File Change Log

🔍 🔔 3 👤 admin ▾

Clear Log

Filters

👁 Default View ▾

⚙ Columns ▾

📄 Export ▾

7 records found

3 per page

< 2 of 3 >

Id ↑	File Name	File Path	File Type	Time	Action
75	MailInfoData.php	/var/www/html/m2371/app/code/Mageants/Security/Block/MailInfoData.php	php	Jun 13, 2022 11:01:02 AM	<a href="#">Preview</a>
74	Checkversion.php	/var/www/html/m2371/app/code/Mageants/Security/Block/Adminhtml/Checkversion.php	php	Jun 13, 2022 11:00:49 AM	<a href="#">Preview</a>
73	Status.php	/var/www/html/m2371/app/code/Mageants/Security/Ui/Component/Listing/Column/Status.php	php	Jun 13, 2022 11:00:00 AM	<a href="#">Preview</a>

### ➔ Security Suite -> Security Checklist

➔ Check List Shows your current admin user name and it shows

It is secure or not secure.

➔ Check List Shows your Frontend and Backend Captcha enable or disable.

➔ Check List Shows your current Magento 2 version.



# Security Checklist

## Check admin's username:



The following usernames are not secured: **admin,root,test,magento**,  
Hackers can guess username easily.

✘ **UserName: admin** is not secure.

## Check Captcha:

- ✔ Backend captcha is enabled.
- ✔ Frontend captcha is enabled.

## Check Magento Version:

- ✔ Your Magento Version is: **2.4.5**

## → Security Suite-> Login Log

- Login Log provide all admin login activity details like Admin Login Time, User Name, IP Address, Browser Details, Login Status, URL and Referrer URL.
- Also you can Create Csv and Excel XML File For Backup or Reference.

## Login Log

🔍 3 👤 admin ▾

Clear Log

Filters

Default View ▾

Columns ▾

Export ▾

Actions ▾

53 records found

2 ▾

per page

<

1

of 27

>

ID	Time	Name	IP	Browser Agent	Status	URL	Referer URL	Action
295	Jun 6, 2022 4:35:03 PM	admin		Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36	SUCCESS	http://localhost/m2371/pub/admin_ez14nj/admin/index/index/key/d082869915212c0e932274b84da57ecaa31f6cd5b7128dee8e8810b8b6e62e1d/	http://localhost/m2371/pub/admin_ez14nj/admin/index/index/key/d082869915212c0e932274b84da57ecaa31f6cd5b7128dee8e8810b8b6e62e1d/	Preview
296	Jun 6, 2022 4:35:20 PM	admininfo		Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.0.0 Safari/537.36	FAIL	http://localhost/m2371/pub/admin_ez14nj/admin/index/index/key/2c125d54875b443861ee60f1bd0900834904db7a179293437032065685b9a0c2/	http://localhost/m2371/pub/admin_ez14nj/admin/index/index/key/2c125d54875b443861ee60f1bd0900834904db7a179293437032065685b9a0c2/	Preview

➔ Security Suite -> Action Log



➔ Action Log provide admin Store activity details like Admin Activity

Time, User Name, IP Address, Activity Action, Status, Module and Activity Full Action Name.

➔ Also you can Create Csv and Excel XML File For Backup or Reference.

### Action Log

3894 records found

20 per page 1 of 195

ID	Time	Name	IP	Action	Module	Status	Full Action Name	Action
1	May 18, 2022 2:01:02 PM	admin		index	Magento_User	SUCCESS	adminhtml_user_index	<a href="#">Preview</a>
2	May 18, 2022 2:01:02 PM	admin		render	Magento_UI	SUCCESS	mui_index_render	<a href="#">Preview</a>
3	May 18, 2022 2:01:02 PM	admin		edit	Magento_Config	SUCCESS	adminhtml_system_config_edit	<a href="#">Preview</a>
4	May 18, 2022 2:01:02 PM	admin		edit	Magento_Config	SUCCESS	adminhtml_system_config_edit	<a href="#">Preview</a>

→ Security Suite -> Action Log Backup



→ As per Your Action Log Backup Configuration Frequency Your Action Log backup File Created automatically and You Can Download it easily.

→ Also you can Create Csv and Excel XML File For Backup or Reference.

## Action Log Backup

🔍 3 👤 admin ▾

🔼 Filters | 👁 Default View ▾ | ⚙ Columns ▾ | 📄 Export ▾

1 records found

20 ▾ per page < 1 of 1 >

Action	File Path	File Name	Time
<a href="#">Download</a>	/var/www/html/m2371/var/export/ActionLog_Backup2022-06-13 12:14:32.csv	ActionLog_Backup2022-06-13 12:14:32.csv	Jun 13, 2022 12:14:32 PM

## **Thank you!**

Should you have any questions or feature suggestions, please contact us at:  
<https://www.mageants.com/contact-us.html>

Your feedback is absolutely welcome!