

# Security Suite for Magento 2 User Guide

Welcome to the User Guide for NEKLO Security Extension. Thank you for choosing our product. This User Guide describes the functionality of the Security Extension made by NEKLO and explains how to use it. Enjoy.

## Introduction

Neklo Security is an extension for Magento 2 that makes your online store secured and protected from unauthorized admin users, malware, and hack attacks. The extension grants you a range of options to take the security of your online store to the new level.

The extension is a combination of the best proven solutions, created to make your Magento 2 website a safe place for buying. Two-factor authentication, advanced password verification procedure, the Lock User function, and MageReport.com Scanner will give you a total control over your store 24/7.

Decide, who may access your store as an admin, and stay in the know. Detect login attempts, monitor actions made by admin users, and get email notifications of Magento Admin Activities. With the Security extension for Magento 2 you will get a full picture of what is happening in your store.

## Installation

1. Unpack the zip file provided into the root folder of your Magento 2 installation.

2. From a command line run

```
bin/magento module:enable Neklo_Core  
bin/magento module:enable Neklo_Security  
bin/magento setup:upgrade  
bin/magento setup:static-content:deploy
```

## Magento Compatibility:

**Community Edition** 2.1.x - 2.2.x

**Enterprise Edition** 2.1.x - 2.2.x

If you experience any issues with the installation, please contact us.

## Configuration - How to enable Security Suite

To enable Security Suite for your store, you need to complete the following steps:

1. Log into your Magento Admin Panel.
2. Go to Stores > **Settings** > **Configuration** > **Neklo tab** > **Security Suite** > **General Settings**
3. **“In Enabled”** should be **“Yes”**.
4. Click **“Save Config”** to apply the changes.

The screenshot shows the Magento Admin Panel Configuration page. On the left is a vertical sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, System, and Find Partners & Extensions. The main content area is titled 'Configuration' and includes a search icon, a notification bell with '5', and a user profile 'admin'. Below this is a 'Store View' dropdown set to 'Default Config' and a 'Save Config' button. A yellow success message states 'You saved the configuration.' The left sidebar menu is expanded to show 'NEKLO' and 'Security Suite'. Under 'Security Suite', there are sub-menus for 'Cron Scheduler', 'Product Position', 'Extensions & Contact', 'GENERAL', 'CATALOG', 'CUSTOMERS', 'SALES', and 'SERVICES'. The 'GENERAL' sub-menu is selected, showing 'General Settings' with a 'Is Enabled [global]' dropdown set to 'Yes'. Below this are expandable sections for 'Advanced Password Validation Settings', 'Password Lifetime Settings', 'Two-factor authentication (2FA)', 'MageReport.com Scanner', 'Notification Settings', and 'Logger Settings'.

## Advanced User Validation

**Advanced Password Validation Settings** allow you to set advanced password requirements for your users to reduce the possibility of password phishing.

1. To view Advanced Password Validation Settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Advanced Password Validation Settings tab**.
2. To unfold the list of password requirements, choose **“Yes”** in the **“Use advanced password requirements”** field.
3. The advanced settings include **“Minimum Password Length”**, **“Use both lower and upper-case letters”**, and **“Use special chars”** fields. It is recommended to set all these options to **“yes”** to increase the security of your password policy to maximum. Minimum password length should not be less than 7 characters.

The screenshot shows the 'Configuration' page in the Neklo admin interface. On the left is a dark sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, System, and Find Partners & Extensions. The main content area has a 'Configuration' header with a search icon, a notification bell with '5', and a user profile 'admin'. Below the header is a 'Store View: Default Config' dropdown and a 'Save Config' button. A yellow success message states 'You saved the configuration.' The left sidebar menu is expanded to 'Security Suite', which includes options for Cron Scheduler, Product Position, Extensions & Contact, GENERAL, CATALOG, and CUSTOMERS. The 'Advanced Password Validation Settings' section is active, showing three settings: 'Is Advanced Password Requirements Enabled' (Yes), 'Minimum Password Length' (9, with a note 'Minimum allowed value is 7'), and 'Use both lower and upper case letters' (Yes). Below this is the 'Password Lifetime Settings' section.

## Password Lifetime Settings

**Password Lifetime Settings** allow to configure various time restrictions for the users' passwords.

1. To view Password Lifetime Settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Password Lifetime Settings**.
2. In order to use the Security Suite Password Lifetime Settings, you should clear a tick box on the right of the fields you want to use.

The screenshot displays the 'Configuration' page for 'NEKLO'. The left sidebar contains navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, System, and Find Partners & Extensions. The main content area is titled 'Configuration' and includes a 'Save Config' button. The 'Security Suite' section is expanded, showing 'Password Lifetime Settings' with the following configuration options:

Setting	Value	Use system value
Password Lifetime (days) [global]	90	<input type="checkbox"/>
We will disable this feature if the value is empty.		
Password Lifetime (successful logins) [global]	30	<input type="checkbox"/>
We will disable this feature if the value is empty.		
Password Change [global]	Forced	<input type="checkbox"/>
We will disable this feature if the value is empty.		
Maximum Login Failures to Lockout Account [global]	10	<input type="checkbox"/>
We will disable this feature if the value is empty.		
Lockout Mode [global]	Time	<input type="checkbox"/>
We will disable this feature if the value is empty.		
Lockout Time (minutes) [global]	30	<input type="checkbox"/>
We will disable this feature if the value is empty.		

Password lifetime restrictions include the following:

1. **"Password Lifetime (days)"** allows to choose how many days the passwords will be used. It is recommended to set the Password Lifetime to no more than 90 days. Upon expiration of this time period, the user will be notified to change their password in Admin Panel.
2. **"Password Lifetime (successful logins)"** allows to set the number of logins before the password should be changed. For example, after 30 successful logins the user will not be able to login with the old password.

3. **“Password change”** notifies the user about the Password Lifetime is running short. If **“Recommended”**, a small window will appear on the top of the page telling it is time to change the password. If **“Forced”**, then the system will force the user to change the password by constantly redirecting him to the Account Settings page.
4. **Maximum Login Failures to Lockout Account** regulates the number of maximum login attempts before blocking the user. After the successful login, the number of previous login failures is accumulated for the rest of the password lifetime.
5. **Lockout Mode** allows to set whether the user blocking will be temporary or permanent. In **Lock Time (minutes)** you can set up the period in minutes. Account will be unlocked after Lock Time (minutes) expires. Permanent mode locks user permanently until the account is manually unblocked.

Please note that you can lock any user automatically. Security Suite provides Lock User functionality similar to the default Active/Inactive functionality. Locked users will be unable to login into your Magento instance. To lock user manually, go to **System > Permissions > All Users** and choose the user you want to lock.

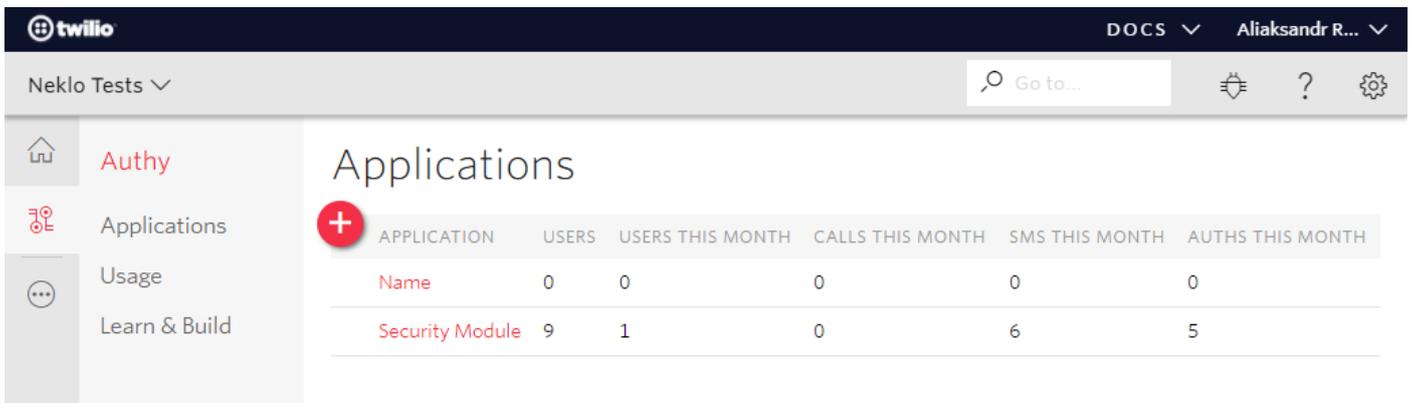
## Twilio Settings

Before enabling 2FA, you need to create and configure an account on Twilio.com.

Please note that NEKLO is not currently associated with Twilio, so this service may charge fees for its functionality. If you have any issue with your Twilio account, please contact them through their support website or at [support@twilio.com](mailto:support@twilio.com).

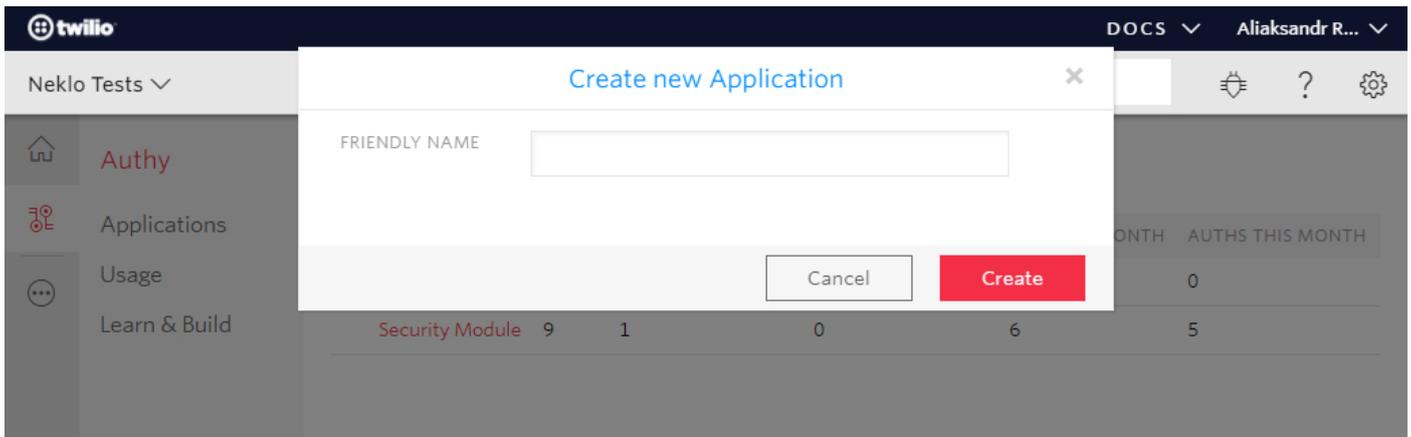
To connect your Twilio account to your Magento store, complete the following steps:

1. Log in into your Twilio account and go to **Authy section**.
2. Create new application by following the directions

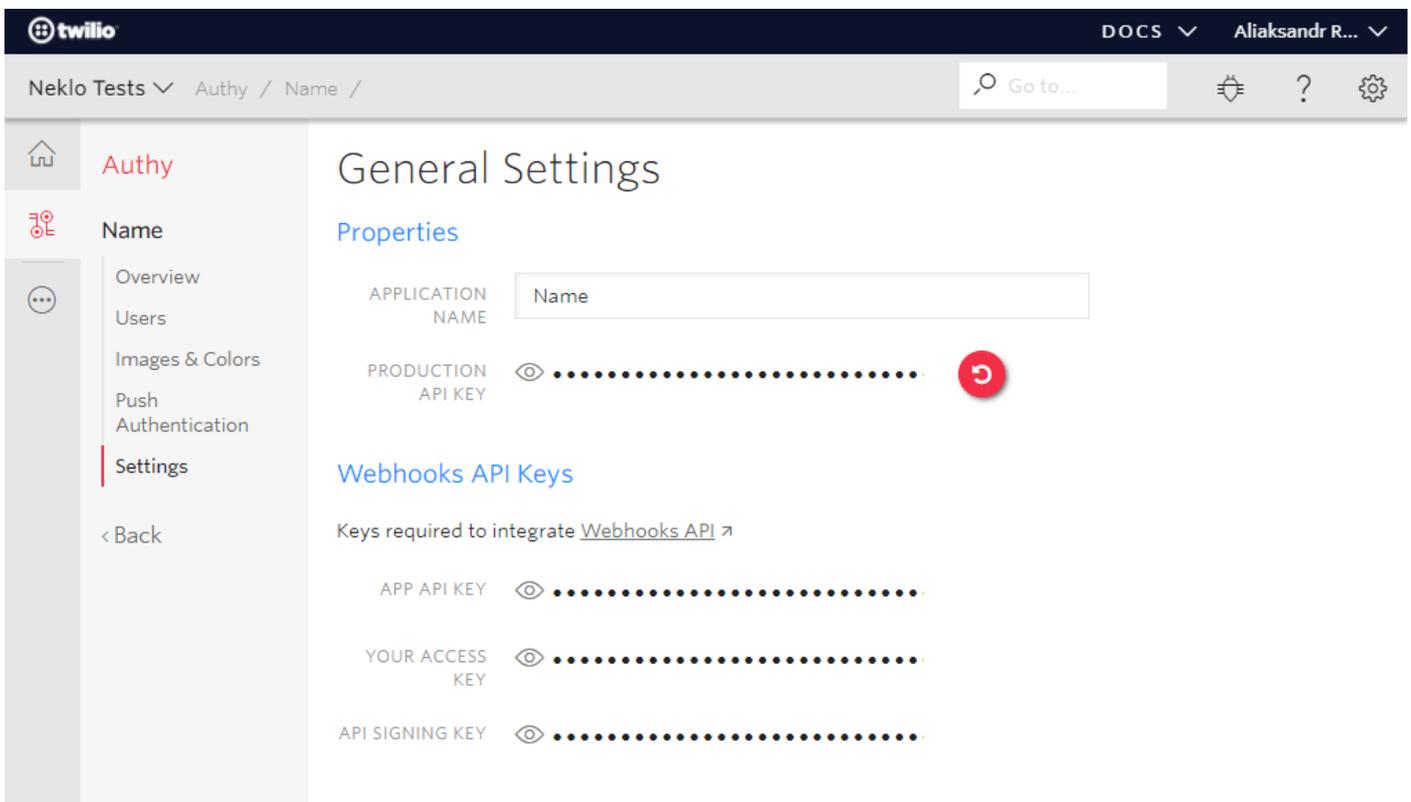


The screenshot shows the Twilio web interface. The top navigation bar includes the Twilio logo, 'DOCS', and the user name 'Aliaksandr R...'. The main content area is titled 'Applications' and features a table with the following data:

APPLICATION	USERS	USERS THIS MONTH	CALLS THIS MONTH	SMS THIS MONTH	AUTHS THIS MONTH
Name	0	0	0	0	0
Security Module	9	1	0	6	5



3. Go to **Authy > Name > Settings** and configure the settings according to your preferences. These are the recommended settings are for the smooth work of Security Suite extension: Authentication via SMS - Enabled.
  - Force SMS - DISABLED (please use this configuration only in case if «Sync tokens in Authy app» is enabled)
  - Force Phone Calls - DISABLED.
  - Sync tokens in Authy app - Enabled.
4. After the settings are configured, you can copy your production API Key at the top of the page. You will need in further Security extension configuration.



## Two-Factor authentication (2FA)

This set of settings allows you to choose how **2FA** will be performed in your Magento store.

1. To view **Two-factor authentication (2FA)** Settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Two-factor authentication (2FA)**.
2. To unfold the list of advanced settings, choose **“Yes”** in the **“Is Enabled”** field.

The screenshot shows the Magento Configuration interface. On the left is a sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, and System. The main content area is titled 'Configuration' and has a 'Save Config' button in the top right. The 'NEKLO' brand is selected. Under the 'Security Suite' section, the 'Two-factor authentication (2FA)' settings are expanded. The 'Mode' dropdown menu is open, showing the following options: Disabled (selected), SMS Code, IP Whitelist, Both (SMS Code with IP Whitelist), and Combined (SMS Code for not whitelisted IP addresses). Other settings sections visible include General Settings, Advanced Password Validation Settings, Password Lifetime Settings, MageReport.com Scanner, Notification Settings, and Logger Settings.

There are several work modes for the 2FA to choose from in:

1. **IP Whitelist.** This setting is needed to enable admin access only for specific IP addresses. If the setting is enabled, it is necessary to add admin IP addresses in the “Allowed IP list” field. If no IP addresses will be added, no admin user will be able to login into admin panel.
  - **“Allowed IP list”** is the field where you need to add appropriate IP addresses with the “Add” button.
  - Click **“Save Config”** to apply the changes.

Configuration

Save Config

NEKLO ^

Security Suite

Cron Scheduler

Product Position

Extensions & Contact

GENERAL v

CATALOG v

CUSTOMERS v

SALES v

General Settings

v

Advanced Password Validation Settings

v

Password Lifetime Settings

v

Two-factor authentication (2FA)

v

Mode  
[global]

IP Whitelist

v

Allowed IP List <small>[global]</small>	IP Address	Note	Action
	191.192	Name	🗑
	<div style="border: 1px solid #ccc; padding: 2px 10px; display: inline-block;">Add</div>		

**IMPORTANT NOTE:** before enabling 2FA please enter your IP address in Allowed IP List. If you do not do this but enable 2FA, after a logout you will not be able to login in Magento.

2. **SMS Code.** If enabled, this mode allows sending codes for authentication to the mobile numbers stated in the User General Settings. It is necessary to complete the following steps for SMS Code to work:
  - insert Twilio API key into the “**Authy API key**” field to connect your Magento store with the specific Twilio account.
  - add phone number for at list one Magento admin user in **System > Permission > All Users > The user you want.**
  - Click “**Save Config**” to apply the changes.

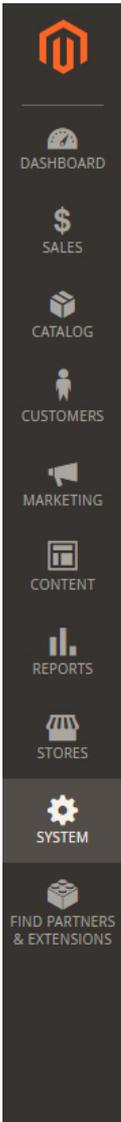
Please note that 2FA will be enabled only after at least one admin user will verify his mobile phone number with Twilio. Verification instructions are described below.

- Both** (SMS code with IP Whitelist). This mode requires the user to complete both 2FA steps. The user's IP should be listed in the IP Whitelist, and if this is so, the user should complete SMS code verification.
- Combined** (SMS code or IP Whitelist). In this mode, if you log in into Magento admin not from whitelisted IP, you will be redirected to the Confirmation page. There you need to enter the security code from the SMS. Please note that the SMS verification will work only if the user has verified his mobile phone number with Twilio.

The screenshot shows the 'Configuration' page for NEKLO. The left sidebar contains navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, and Content. The main content area is titled 'Configuration' and includes a 'Save Config' button. The 'Security Suite' section is expanded, showing 'Cron Scheduler', 'Product Position', and 'Extensions & Contact'. The 'GENERAL' section is selected. The 'Two-factor authentication (2FA)' settings are visible, including a dropdown menu for 'Mode' set to 'SMS Code' and a text input field for 'Authy API Key' with a 'Create an Authy account' link below it.

## Twilio Verification process

- Make sure you have entered a valid API Key from your Twilio account and added your IP in the allowed list.
- Proceed to System > Permission > All Users. If 2FA feature has been enabled, there will be a new required field, which is "Phone Number".
- Phone Numbers must be inputted for every user. If a user does not have a phone number assigned and this user's IP is not in the Allowed IP List, he will not be able to log in as an admin.



Admin Admin

[← Back](#)
[Delete User](#)
[Reset](#)
[Lock](#)
[Force Sign-In](#)
[Save User](#)

**USER INFORMATION**

- User Info
- User Role

Account Information

User Name \*   
 First Name \*   
 Last Name \*   
 Email \*   
 Phone Number \*    
 New Password   
 Password Confirmation   
 Interface Locale    
 This account is

- After you enter a phone number in the particular fields and saved the changes, this phone number must be confirmed.



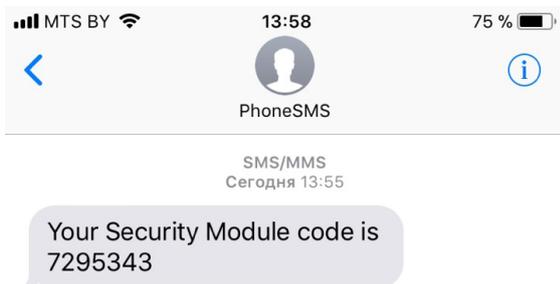
✓ You saved the user.  
✓ Verification token sent to +91 98765 43210

General

Verification Code \*



- You will get a text message with the verification code to the particular phone number.



- Once you enter a verification code and save the user, you will see a message that the phone number has been verified.

The screenshot shows a web application's user management interface. At the top, there's a navigation bar with 'user user' and buttons for 'Back', 'Delete User', 'Reset', 'Lock', 'Force Sign-In', and a prominent 'Save User' button. A yellow banner displays a green checkmark and the message: 'The phone number has been verified.' Below this, the 'USER INFORMATION' section is active, showing 'User Info' and 'User Role'. The 'Account Information' section contains several input fields: 'User Name \*' (filled with 'user'), 'First Name \*' (filled with 'user'), 'Last Name \*' (filled with 'user'), 'Email \*' (filled with 'user@demostore2.neklo.com'), and 'Phone Number \*' (with a dropdown menu set to '+375 295343' and a text field containing '7295343').

MTS BY 15:08 54%  
Requests Settings



Security Module token is:

43 288 20

Your token expires in 20



 Twilio	 Security Module	 Add Account
---	--	--

For all users that have been setup with 2FA upon the valid login with their username and password, they will receive a verification code on their mobile device in SMS or via Twilio Authy application during Magento admin login.

The system will require a second prompt for Security Code. Only upon entering the Security Code the user will be allowed to login into the Magento instance.

You should enter this security code on the login page and click on the Confirm button.



And now your account should be successfully logged in Magento Admin.

## MageReport.com Scanner

This feature will schedule an automatic scan of your Magento Instance by [www.magereport.com](http://www.magereport.com). All results of scanning will be listed in Magento Admin Panel. You may manually rescan your store any time.

To view MageReport.com Scanner settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > MageReport.com Scanner**.

To enable MageReport automatic scanning, choose **“Yes”** in the **“Is Enabled by Cron”** field. if enabled, the scan is executed once per day at midnight of the server’s local time by cron.

Rescan button allows you to run Magereport check immediately.

The screenshot shows the 'Configuration' page for 'MageReport.com Scanner'. On the left is a sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, System, and Find Partners & Extensions. The main content area has a 'Save Config' button in the top right. Below the title 'MageReport.com Scanner', there is a dropdown menu for 'Is Enabled by Cron [global]' set to 'Yes', with a note 'Once per day.' and a 'Rescan' button. Below this are three security scan results:

Security patch 7405	unknown	SSL protection?	ok
<p>Patch SUPEE-7405 resolves several security fixes, but most importantly fixes a leak that allows hackers to take over your admin (backend) account and gain access to your Magento shop. Released Jan 21th, 2016.</p> <p><a href="#">More about applying Magento patches</a></p> <p>We were unable to conclusively check your shop. The check might have been blocked by other emergency measures you, or your provider, have taken.</p>		<p><b>Risk rating</b> <span style="color: green;">low</span></p> <p>SSL is used to establish a secure connection between your visitor's browser and your webshop. Without SSL, hackers can hijack information sent and received by your visitor. We recommend every shop owner to use an SSL certificate. Additional benefit: thanks to HTTP/2 having SSL actually speeds up your shop.</p> <p><a href="#">Read more about this check</a></p>	
Security patch 9652	safe	Gurulnc Javascript Hack?	safe
<p><b>Risk rating</b> <span style="color: green;">low</span></p> <p>Patch SUPEE-9652 prevents attackers from executing PHP code through a bug in the Zend Framework's Sendmail adapter. Released Feb 6th, 2017. This patch cannot be detected from the outside, without hacking your shop.</p> <p><a href="#">More about applying Magento patches</a></p>		<p><b>Risk rating</b> <span style="color: green;">low</span></p> <p>Gurulnc is malware that targets Magento shops. Once a shop is infected, it will try to infect visitors as well.</p> <p><a href="#">Read more about this check</a></p>	

## Notification Settings

Notification settings allow you to select specific Magento activities that will be notified to you via email.

1. To view MageReport.com Scanner settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Notification Settings**.
2. To enable email notifications, choose “Yes” in the “Is Enabled” field.

Configuration

Save Config



-  DASHBOARD
-  SALES
-  CATALOG
-  CUSTOMERS
-  MARKETING
-  CONTENT
-  REPORTS
-  STORES
-  SYSTEM
-  FIND PARTNERS & EXTENSIONS

- GENERAL ▼
- CATALOG ▼
- CUSTOMERS ▼
- SALES ▼
- SERVICES ▼
- ADVANCED ▼

### Notification Settings ⌵

**Is Enabled** [global]

**Sender** [global]

**Event List** [global]

Login failure

Login success

Login from not whitelisted IP

Admin user locked/unlocked

Fail detected by MageReport.com

Malware signature detected

**Recipients** [global]

Email	Name	Action
<input type="text" value="neklo@i"/>	<input type="text" value="name"/>	
<input type="button" value="Add"/>		

3. In Sender field, you can specify the email sender. Sender emails are taken from **Stores > Settings > Configuration > General > Store Email Addresses**.
4. In the **“Event List”** field, you can select what admin user activities you want to be notified about.
5. In the **“Recipients”** field, you can add and delete the users who will get email notifications.
6. Click **“Save Config”** to apply the changes.

Here is an example of how the email notification from Security Suite looks like.

## Logger Settings

Neklo Security Suite extension starts the logging process immediately after it was installed. So after all the installation instructions are done, the extension starts collecting admin activity logs. This info is stored in separate database tables and can be viewed and managed in Login Attempts and Action Logger grids.

To view Logger Settings, go to **Stores > Settings > Configuration > General > Logger Settings**. These settings include the following:

1. Action logger lifetime (Days). You can manage for how long the logs will be stored on your server and in Login Attempts grid in days. The data will be removed from the database once the specified number of days has passed.
2. Login Attempts Lifetime (Days). Here you can choose for how long the Login info will be stored on your server and in Account Logger grid. The data will be removed from the database once the specified number of days has passed.
3. Is Export Enabled. This setting allows to export file automatically before the data will be removed from server. Files are stored under var/export folder.
4. Click "Save Config" to apply the changes.

The screenshot shows the 'Configuration' page in the Neklo Security Suite. On the left is a vertical sidebar with navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, and Stores. The main content area is titled 'Configuration' and has a 'Save Config' button in the top right. A left-hand menu lists categories: Product Position, Extensions & Contact, GENERAL, CATALOG, CUSTOMERS, SALES, SERVICES, and ADVANCED. The 'Logger Settings' section is expanded, showing three settings:

- Two-factor authentication (2FA)**: A dropdown menu with a downward arrow.
- MageReport.com Scanner**: A dropdown menu with a downward arrow.
- Notification Settings**: A dropdown menu with a downward arrow.
- Logger Settings**: A dropdown menu with an upward arrow, which is currently expanded to show:
  - Action Logger Lifetime (Days)**: A text input field containing '30'. Below it, the text '[global]' and 'Leave empty to disable.' are visible.
  - Login Attempts Lifetime (Days)**: A text input field containing '30'. Below it, the text '[global]' and 'Leave empty to disable.' are visible.
  - Is Export Enabled**: A dropdown menu with 'Yes' selected and a downward arrow.

Since potentially there could be a larger amount of data recorded, Security Suite extension provides log truncation rules which will give you an ability to delete data older than Lifetime fields specify. Logs are stored on the server under var/export folder.

## Login Attempts Grid

Login Attempts grid reflects all login attempts and extensive information about them. Login Attempts grid is located under **System > Security Suite > Login Attempts**.

Created At	Admin User ID	Admin Username	Remote Address	User Agent	Message	Status
May 28, 2018 2:29:23 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36		SUCCESS
May 28, 2018 2:25:57 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36		SUCCESS
May 28, 2018 2:25:45 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36	Token is invalid	FAILURE
May 28, 2018 2:24:58 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36	Logged out.	LOGOUT
May 28, 2018 2:24:52 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36		SUCCESS
May 28, 2018 2:24:32 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36	Logged out.	LOGOUT
May 28, 2018 2:24:14 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36		SUCCESS
May 28, 2018 2:23:22 AM	3	TEST	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36	You did not sign in correctly or your account is temporarily disabled.	FAILURE

## Login Attempts Grid

Action Logger shows all the actions made by admin users. Action Logger grid is located under **System > Security Suite > Action Logger**.

Created At	Admin User ID	Admin Username	Remote Address	Full Action Name	Method	Is Ajax	URL	Query	Actions
May 22, 2018 11:14:40 AM	2	USER	46.53.188.190	nekllo_security_login_attempt_index	GET	No	http://ce223.neklodev.com/admin/nekllo_security/login_attempt/index/		<a href="#">View</a>
May 22, 2018 11:12:29 AM	2	USER	46.53.188.190	adminhtml_system_config_state	GET	Yes	http://ce223.neklodev.com/admin/admin/system_config/state/	{ "isAjax": "true", "container": "nekllo_security_logger", "value": "1" }	<a href="#">View</a>
May 22, 2018 11:12:28 AM	2	USER	46.53.188.190	adminhtml_system_config_state	GET	Yes	http://ce223.neklodev.com/admin/admin/system_config/state/	{ "isAjax": "true", "container": "nekllo_security_notification", "value": "0" }	<a href="#">View</a>
May 22, 2018 11:12:19 AM	2	USER	46.53.188.190	adminhtml_system_config_edit	GET	No	http://ce223.neklodev.com/admin/admin/system_config/edit/	{ "section": "nekllo_security" }	<a href="#">View</a>
May 22, 2018 11:12:19 AM	2	USER	46.53.188.190	adminhtml_system_config_index	GET	No	http://ce223.neklodev.com/admin/admin/system_config/index/		<a href="#">View</a>

### Request #378 ← Back

**Admin User ID** 2

**Full Action Name** catalog\_product\_massDelete

**Method** POST

**Is Ajax** No

**URL** http://ce223.neklodev.com/admin/catalog/product/massDelete/

**Remote Address** 46.53.188.190

**Requested At** May 22, 2018, 11:20:30 AM

**Request Params**

**Query**

```
{
  "selected": [
    "1"
  ],
  "filters": {
    "placeholder": "true"
  }
}
```