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. Install library using console command: composer require authy/php:^3.0
2. Unpack the zip file provided into the root folder of your Magento 2 installation.
3. 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:

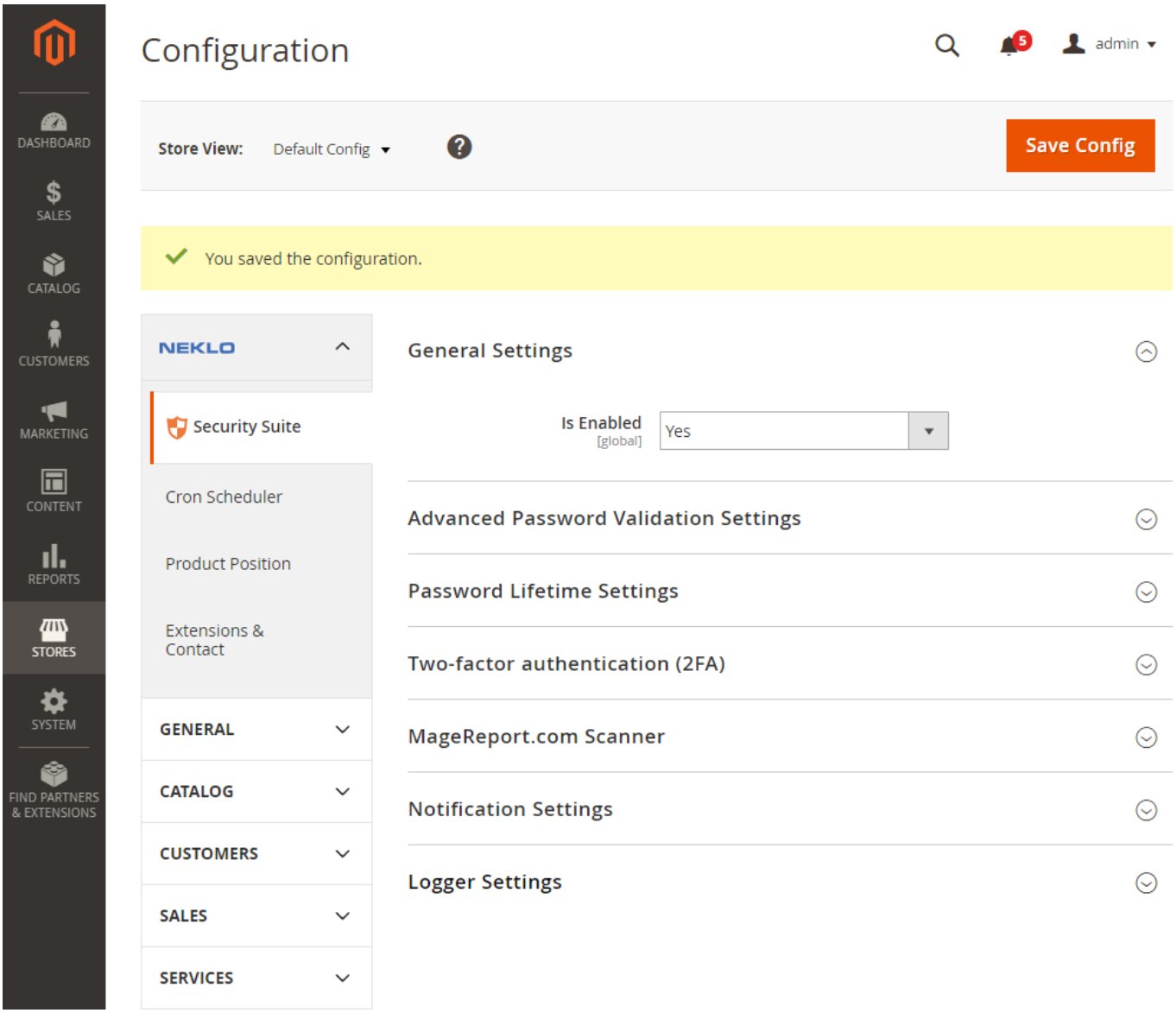
Community Edition 2.1.x - 2.2.x
Enterprise Edition 2.1.x - 2.2.x

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:

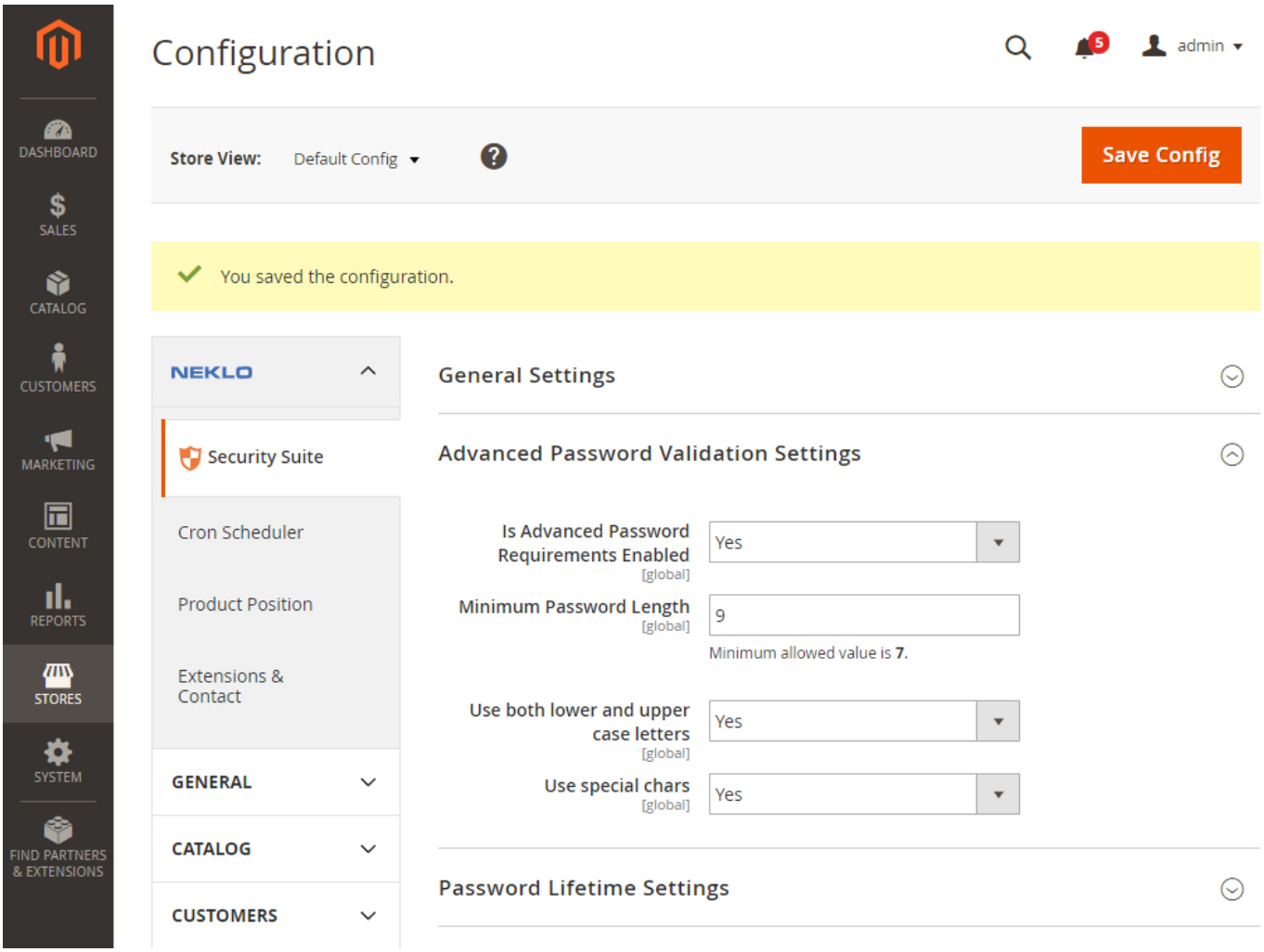
1. Log into your Magento Admin Panel.
2. Go to Stores > **Settings > Configuration > Neklo tab > Security Suite > General Settings**
3. **“In Enabled”** should be “**Yes**”.
4. Click “**Save Config**” to apply the changes.



Advanced User Validation

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

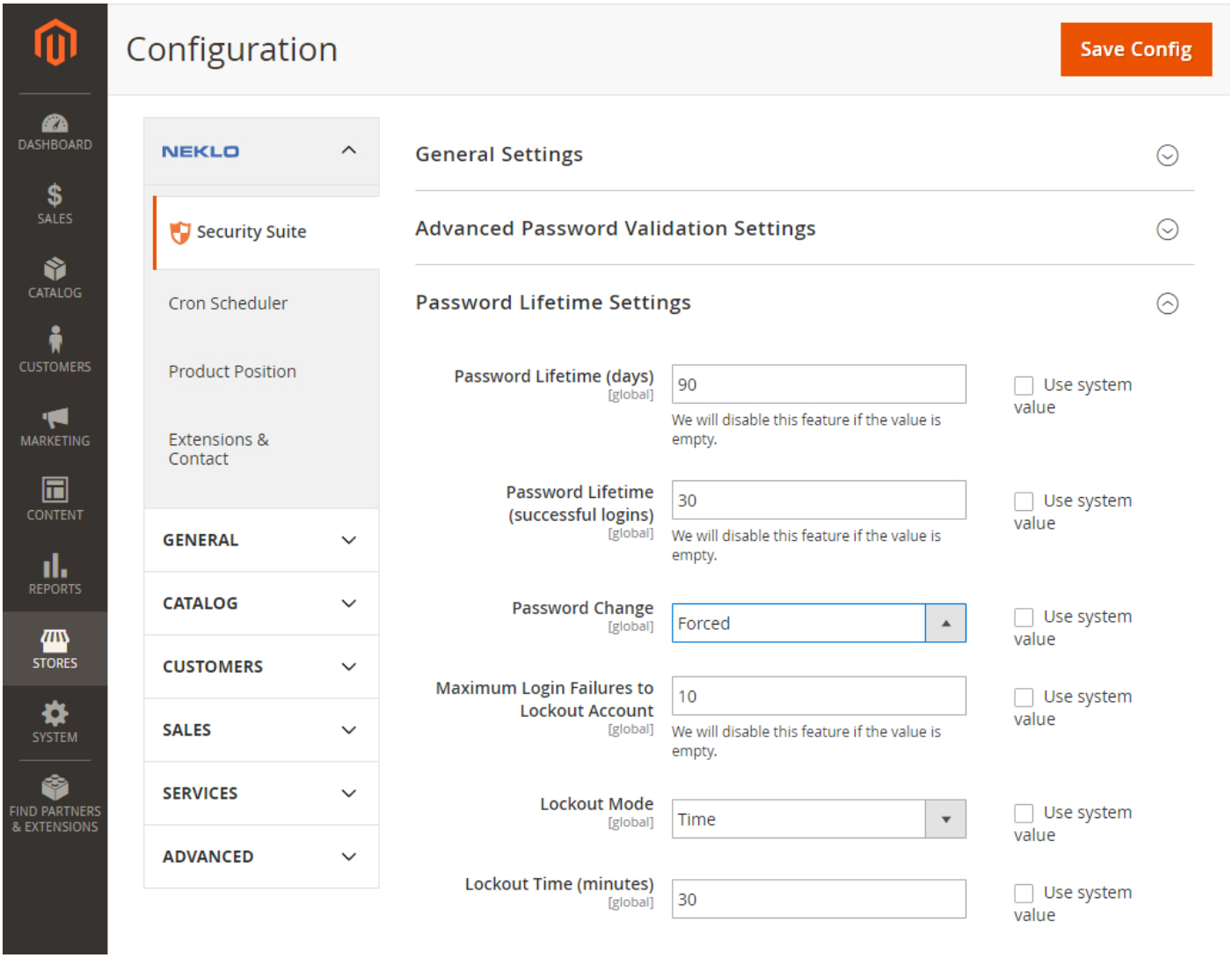
1. To view Advanced Password Validation Settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Advanced Password Validation Settings tab**.
2. To unfold the list of password requirements, choose “**Yes**” in the “**Use advanced password requirements**” field.
3. The advanced 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.



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.



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.

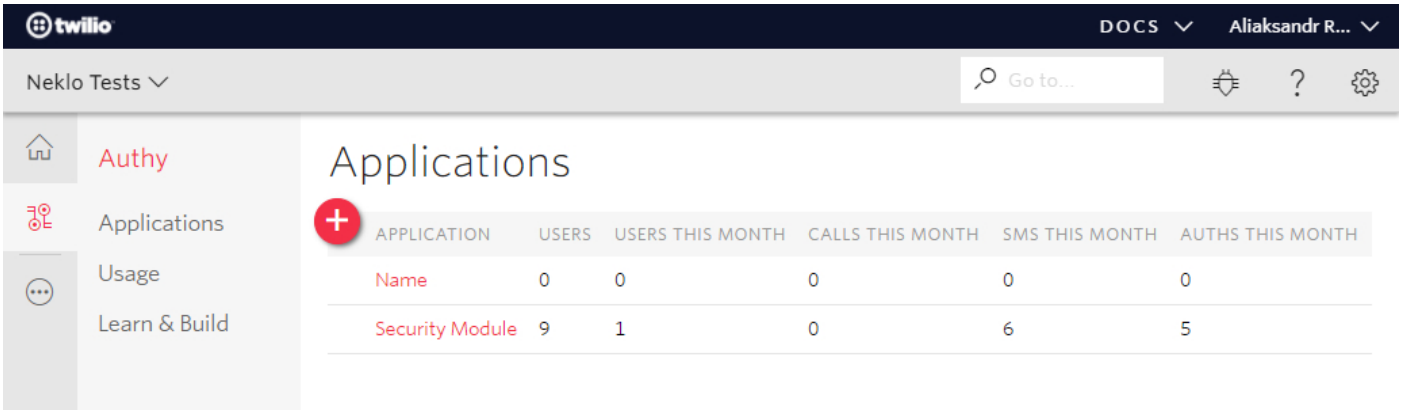
Twillio Settings

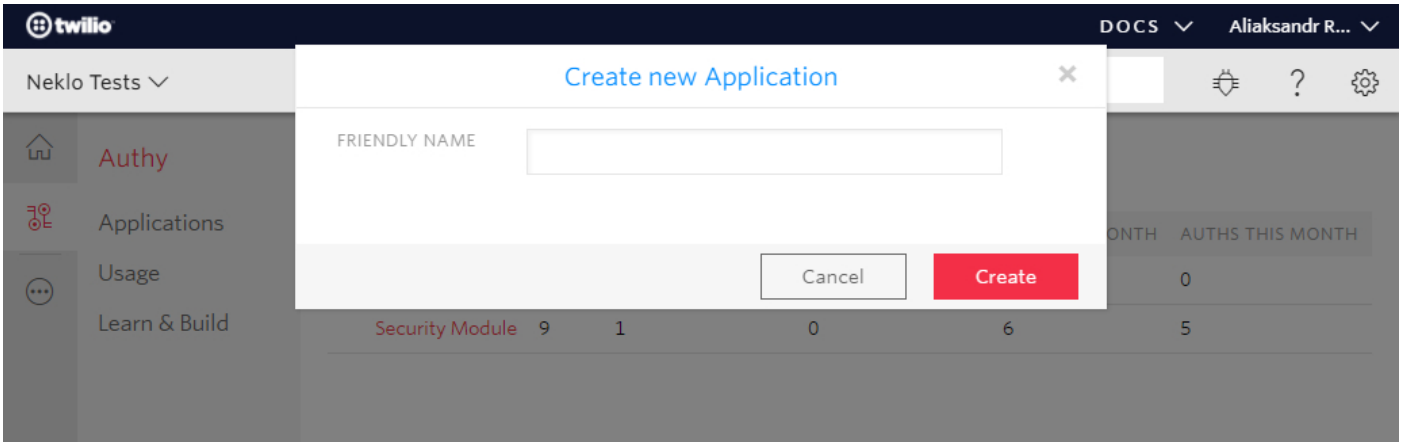
Before enabling 2FA, you need to create and configure an account on Twilio.com.

Please note that NEKLO is not currently associated with Twillio, so this service may charge fees for its functionality. If you have any issue with your Twillio account, please contact them through their support website or at support@twillio.com.

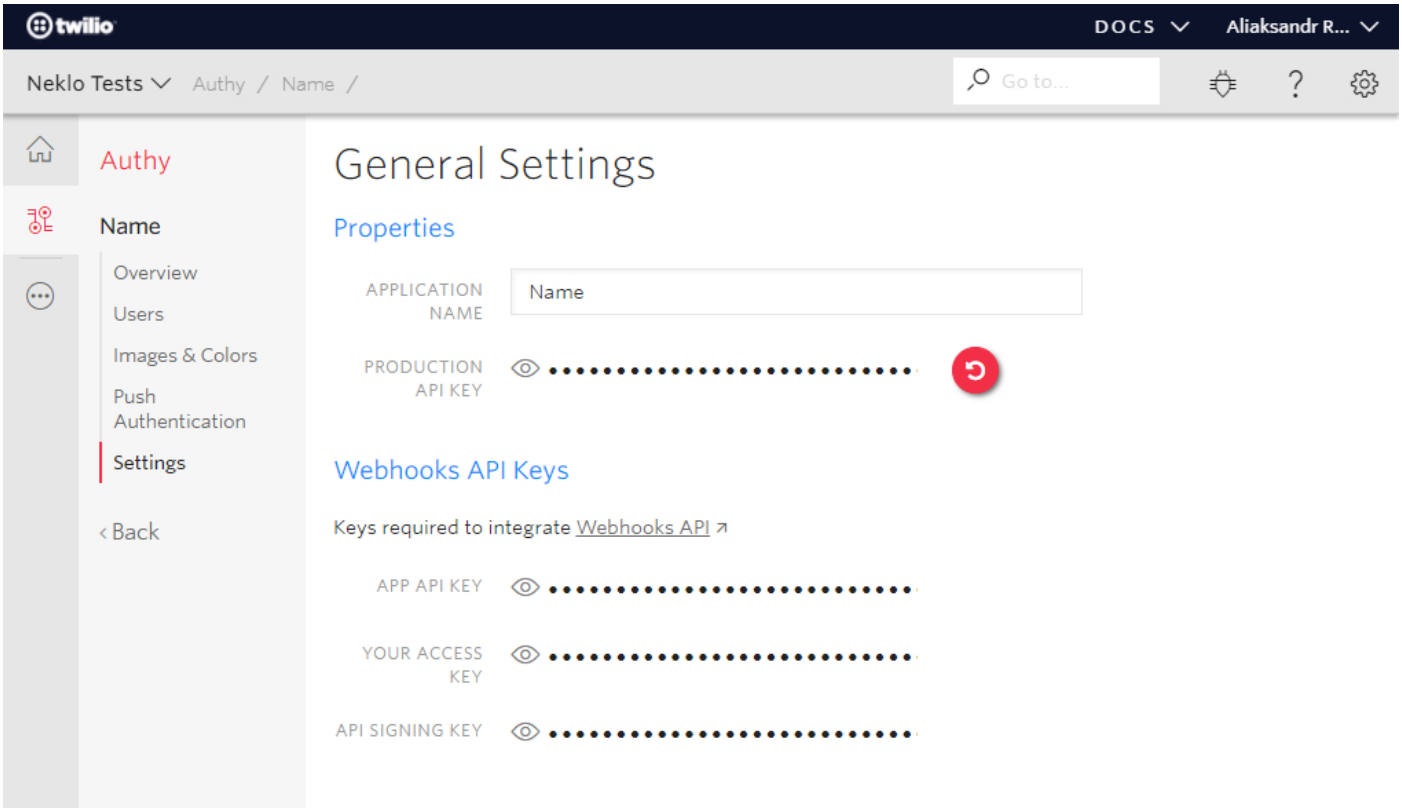
To connect your Twillio account to your Magento store, complete the following steps:

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





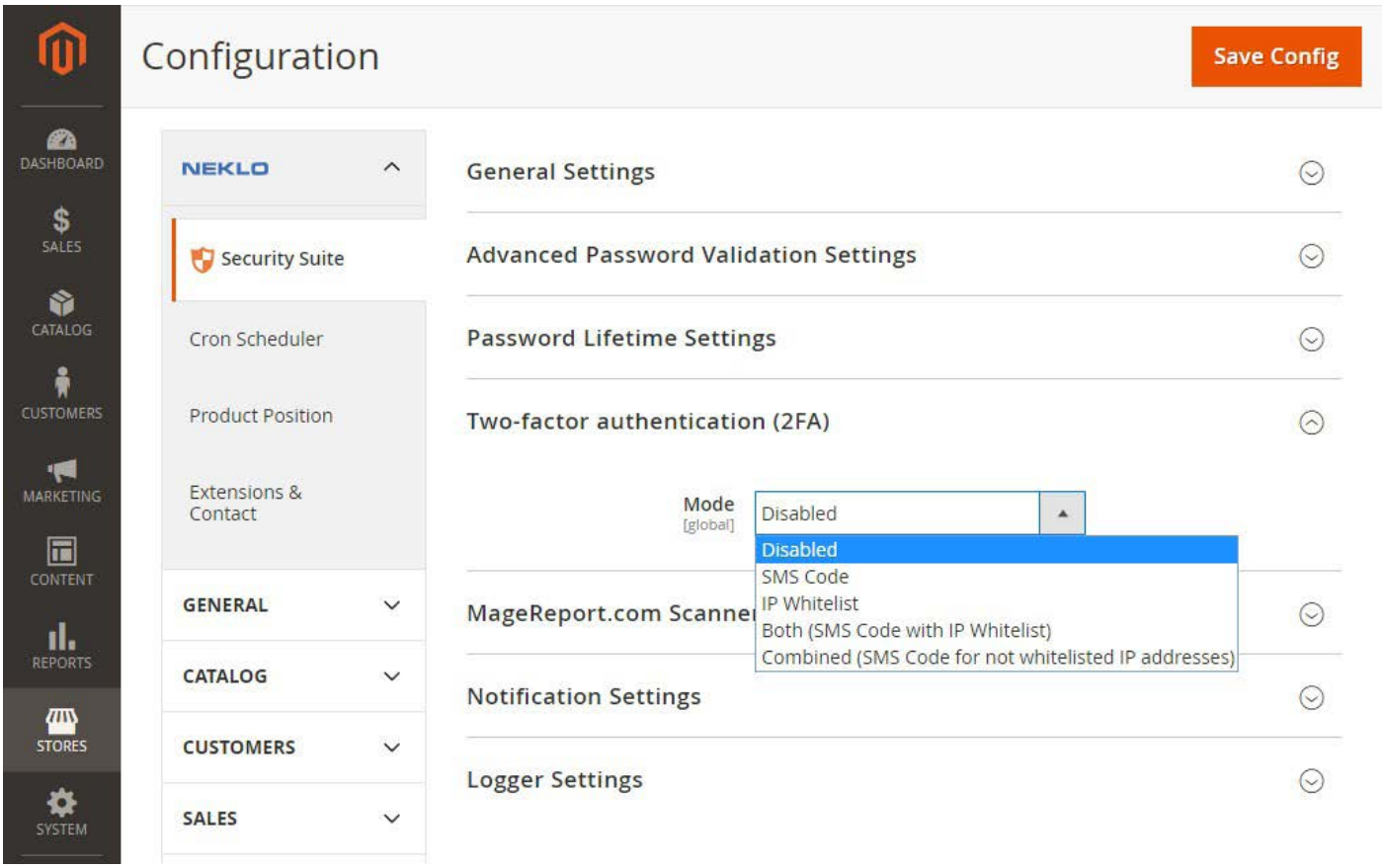
3. Go to **Authy > Name > Settings** and configure the settings according to your preferences. These are the recommended settings are for the smooth work of Security Suite extension: Authentication via SMS - Enabled.
   - Force SMS - DISABLED (please use this configuration only in case if «Sync tokens 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.

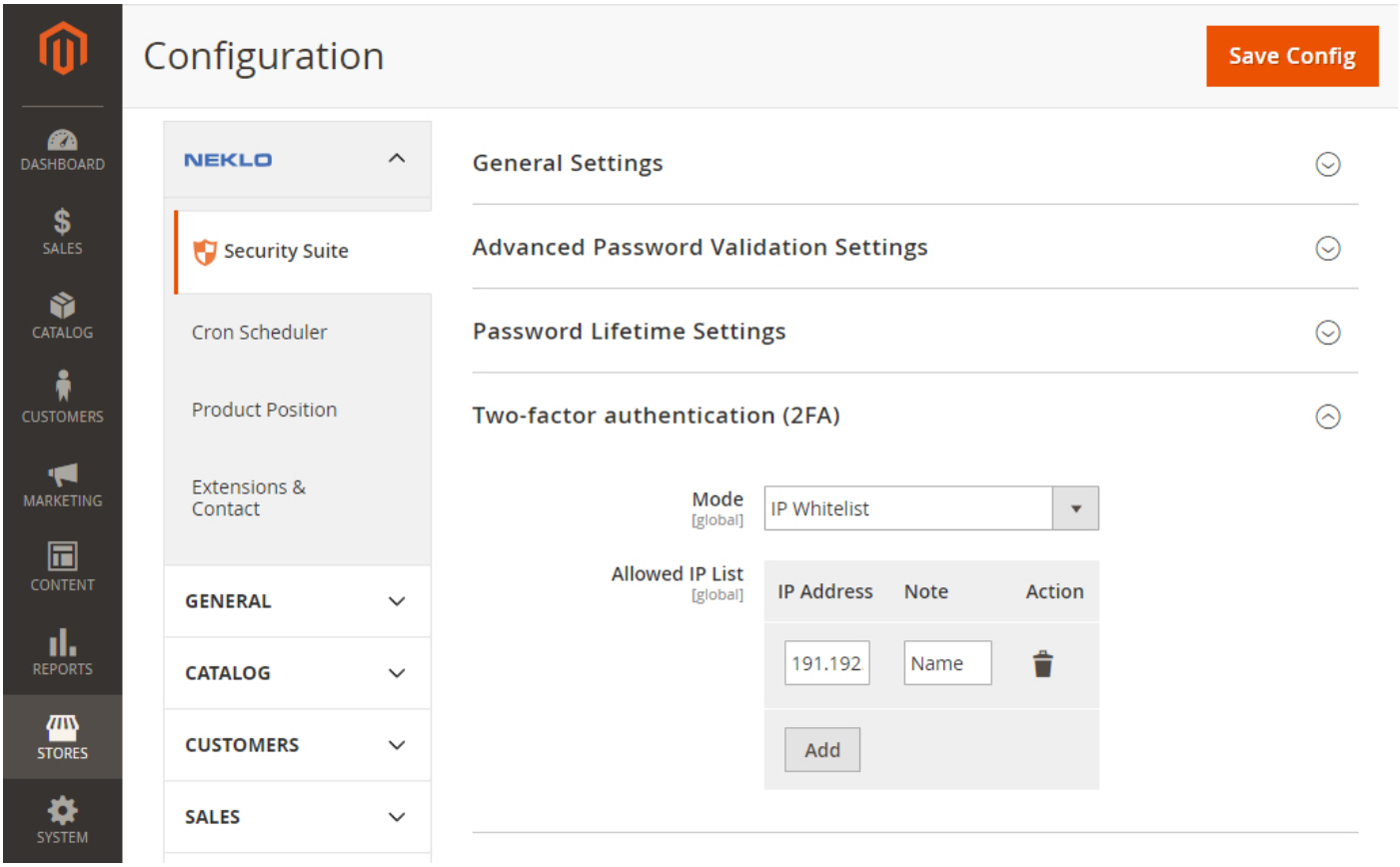
1. To view **Two-factor authentication (2FA)** Settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Two-factor authentication (2FA)**.
2. To unfold the list of advanced settings, choose "**Yes**" in the "**Is Enabled**" field.



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.



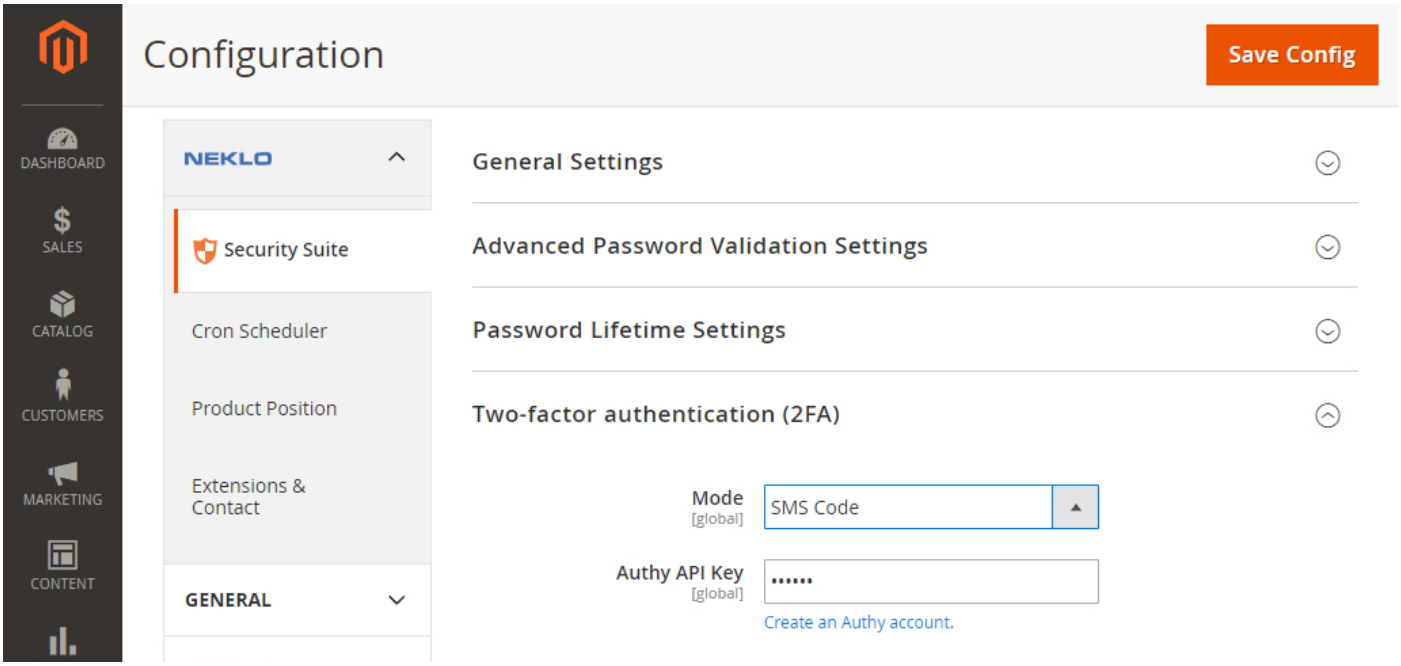
IMPORTANT NOTE: before enabling 2FA please enter your IP address in Allowed IP List. If you do not do this but enable 2FA, after a logout you will not be able to login in Magento.

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.

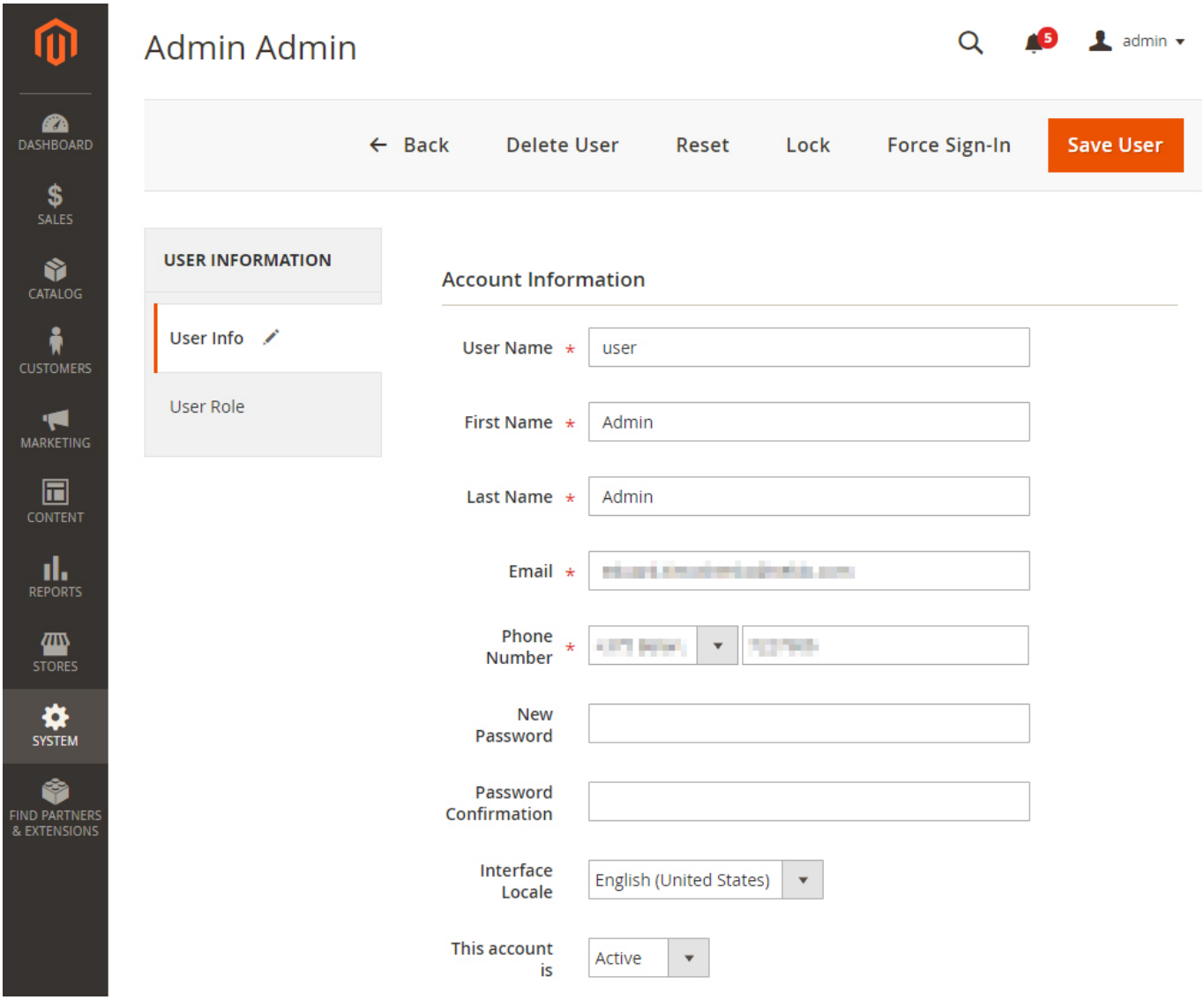
   Please note that 2FA will be enabled only after at least one admin user will verify his mobile phone number with Twilio. Verification instructions are described below.

3. **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.
4. **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.

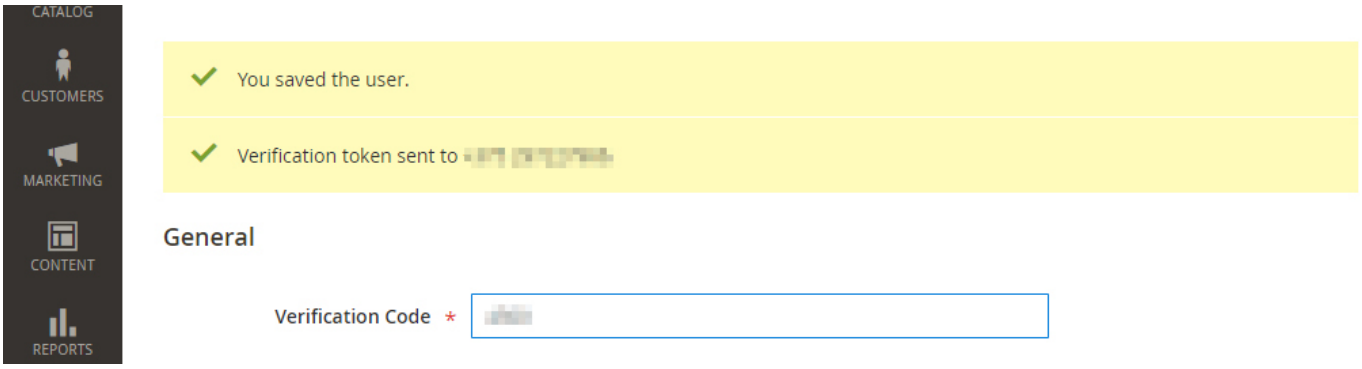


Twilio Verification process

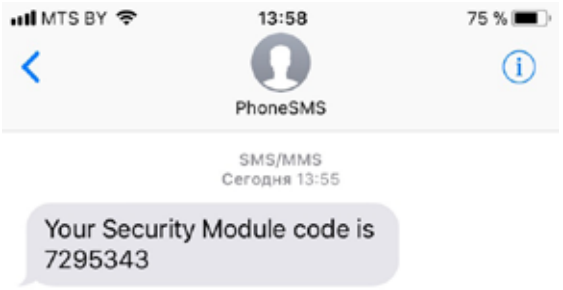
1. Make sure you have entered a valid API Key from your Twillio account and added your IP in the allowed list.
2. Proceed to System > Permission > All Users. If 2FA feature has been enabled, there will be a new required field, which is "Phone Number".
3. Phone Numbers must be inputted for every user. 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.



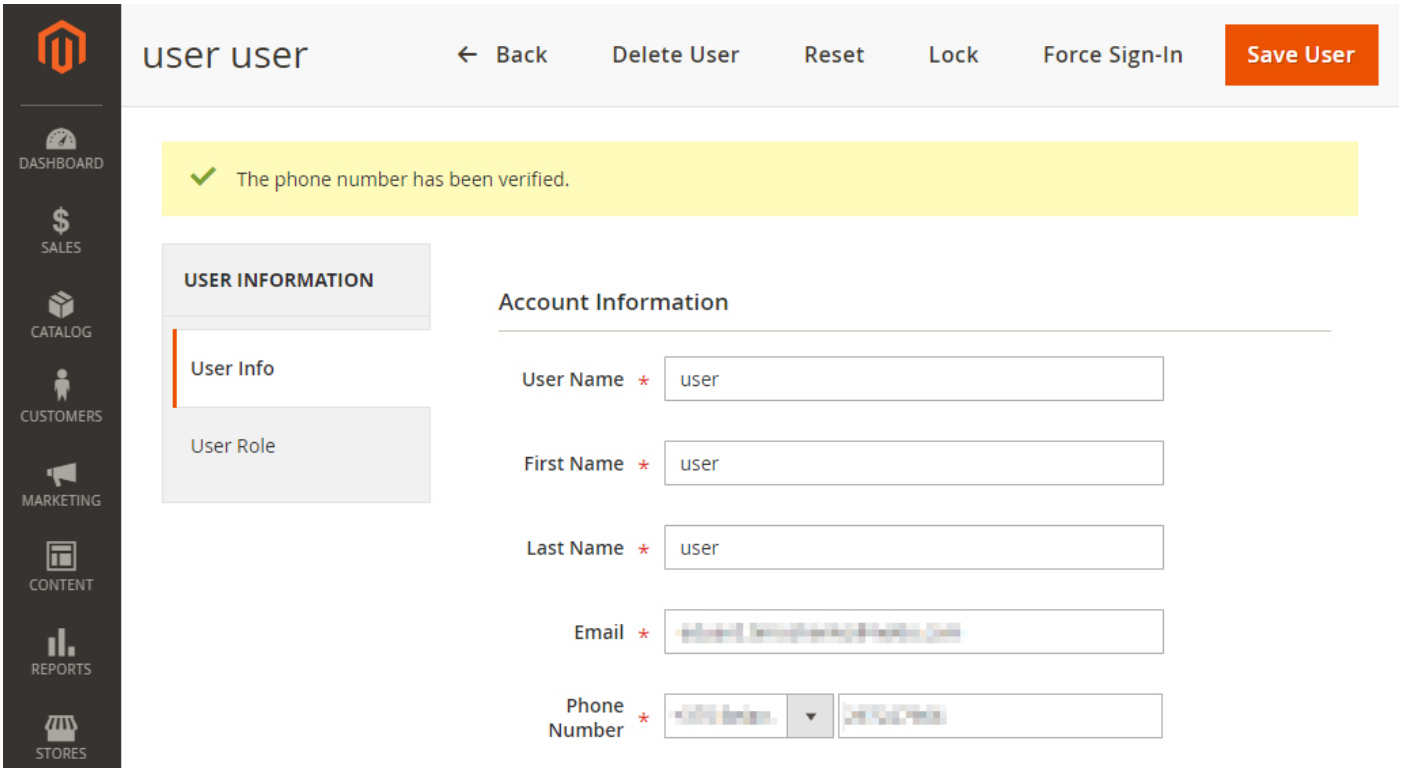
4. After you enter a phone number in the particular fields and saved the changes, this phone number must be confirmed.

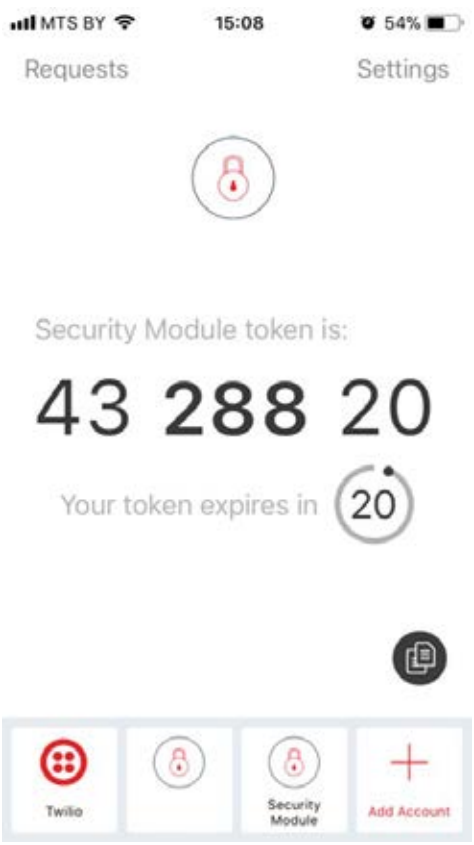


5. You will get a text message with the verification code to the particular phone number.



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

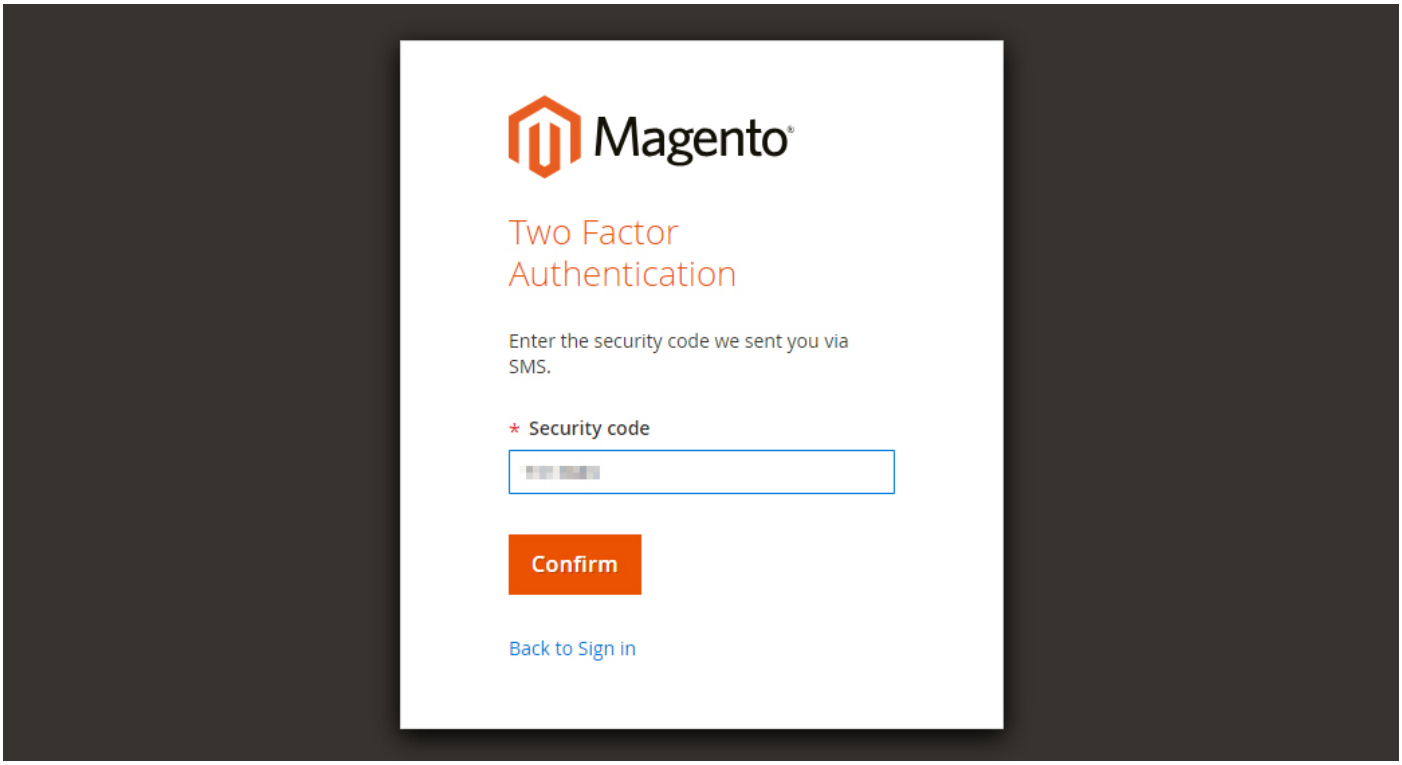




For all users that have been setup with 2FA upon the valid login with their username and password, they will receive a verification code on their mobile device in SMS or via Twilio Authy application during Magento admin login.

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.

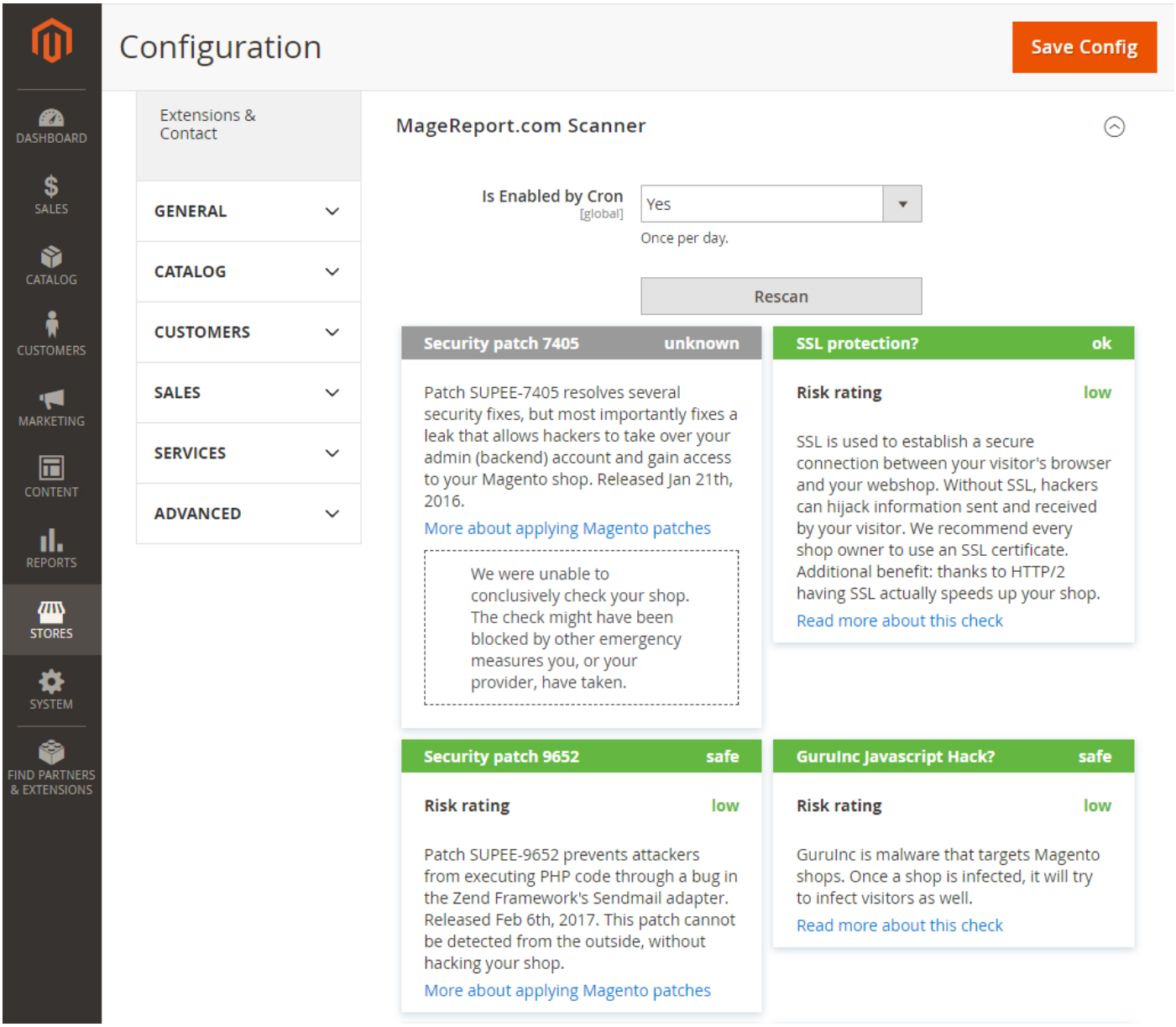
MageReport.com Scanner

This feature will schedule an automatic scan of your Magento Instance by www.magereport.com. 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.

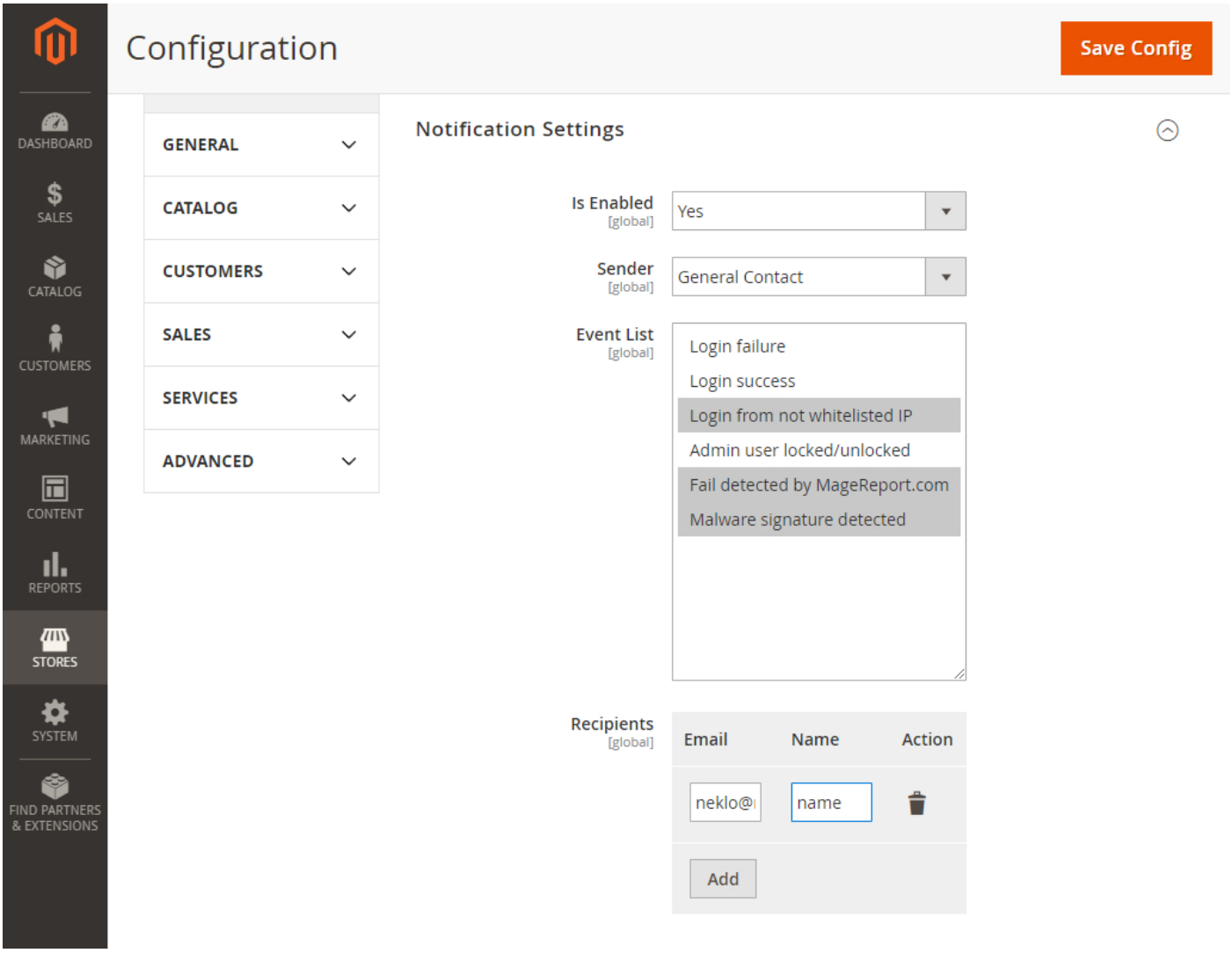
Rescan button allows you to run Magereport check immediately.



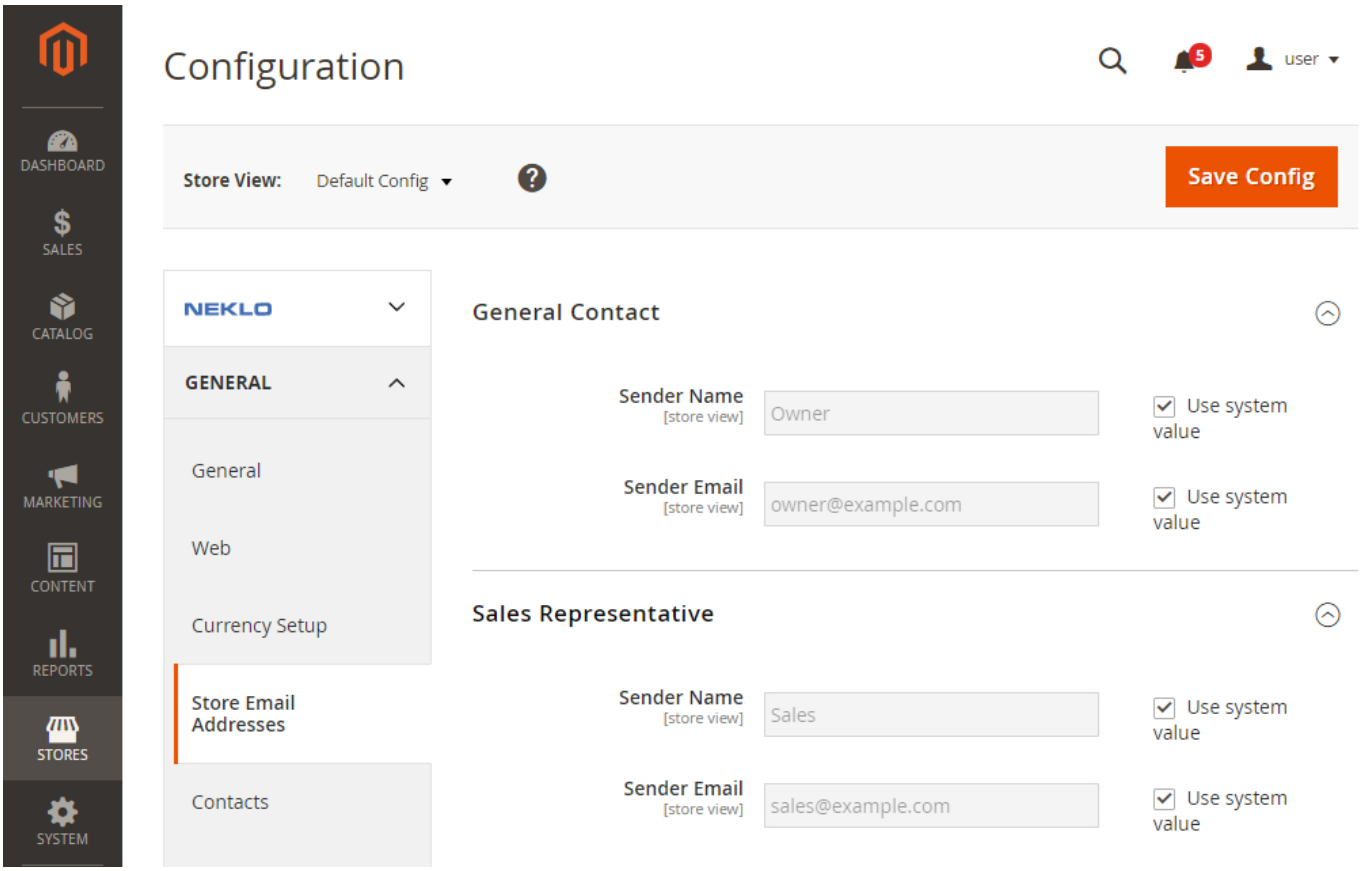
Notification Settings

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

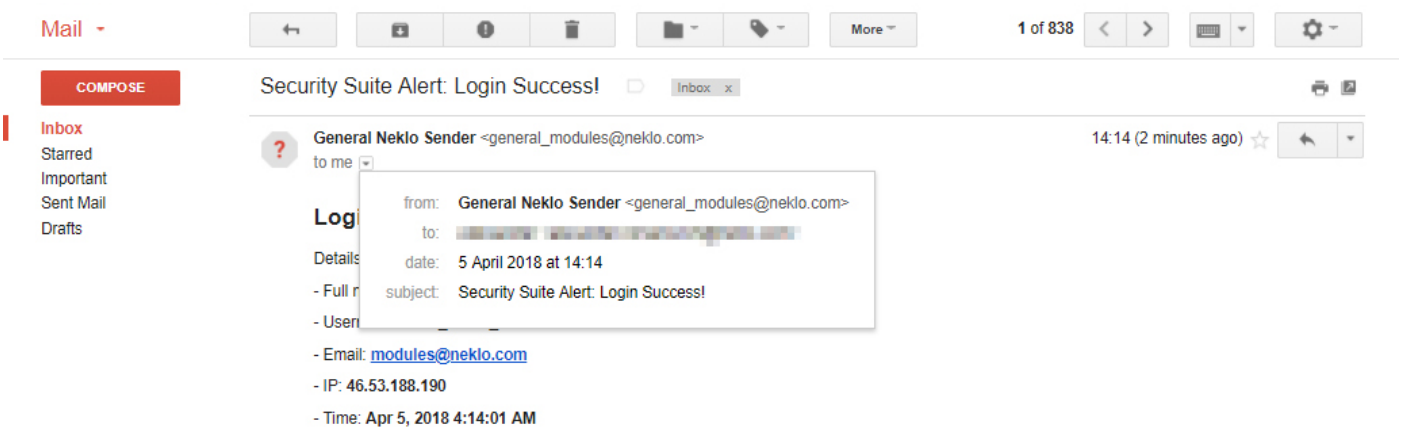
1. To view MageReport.com Scanner settings, go to **Stores > Settings > Configuration > Neklo tab > Security Suite > Notification Settings**.
2. To enable email notifications, choose “**Yes**” in the “**Is Enabled**” field.



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 examply of how the email notification from Security Suite looks like.

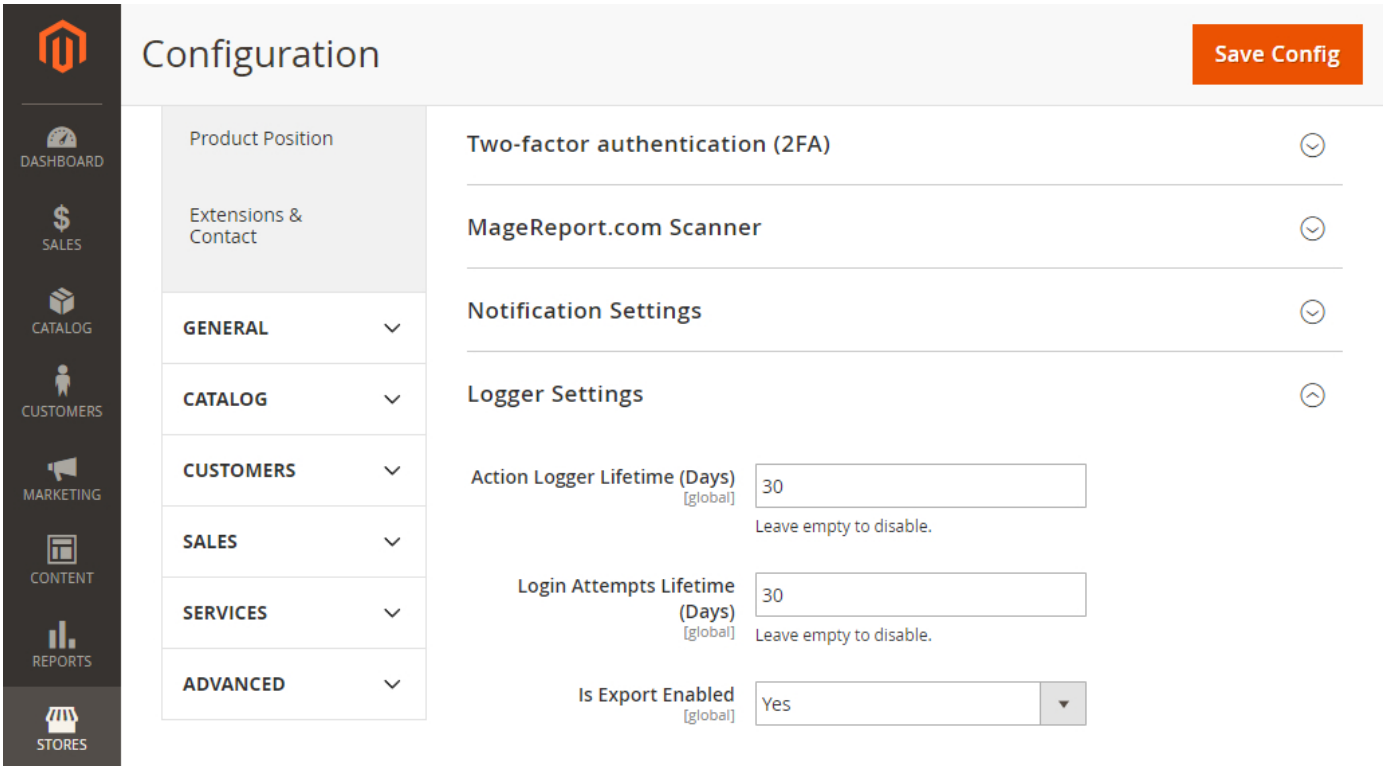


Logger Settings

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:

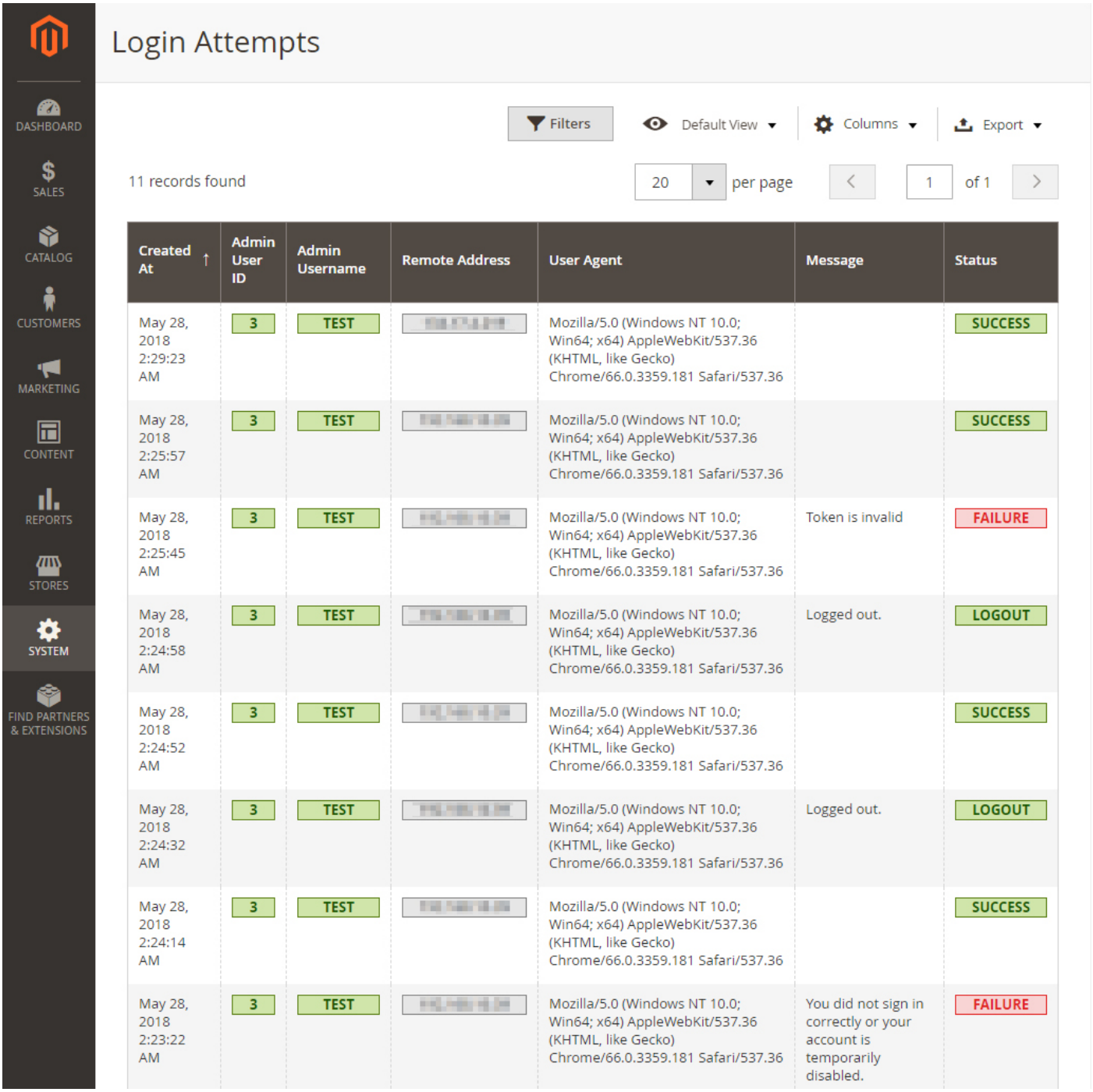
1. Action logger lifetime (Days). You can manage for how long the logs will be stored on your server and in Login Attempts grid in days. The data will be removed from the database once the specified number of days has passed.
2. Login Attempts Lifetime (Days). Here you can choose for how long the Login 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.



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

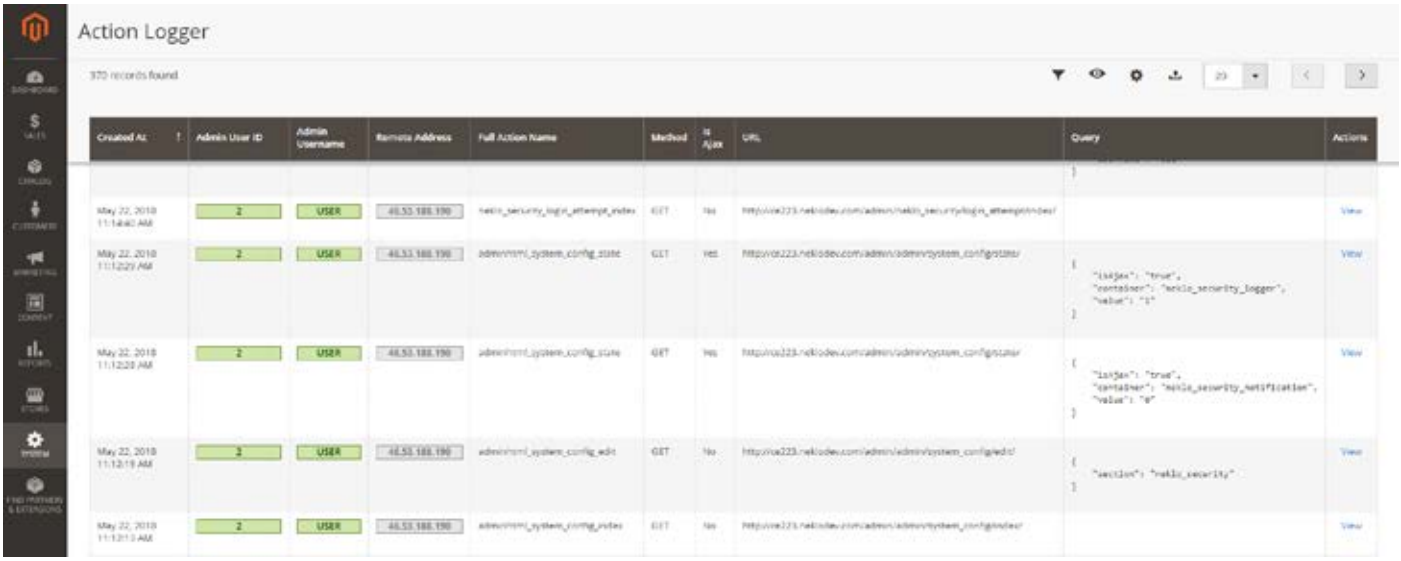
Login Attempts grid reflects all login attempts and extensive information about them. Login Attempts grid is located under **System > Security Suite > Login Attempts**.

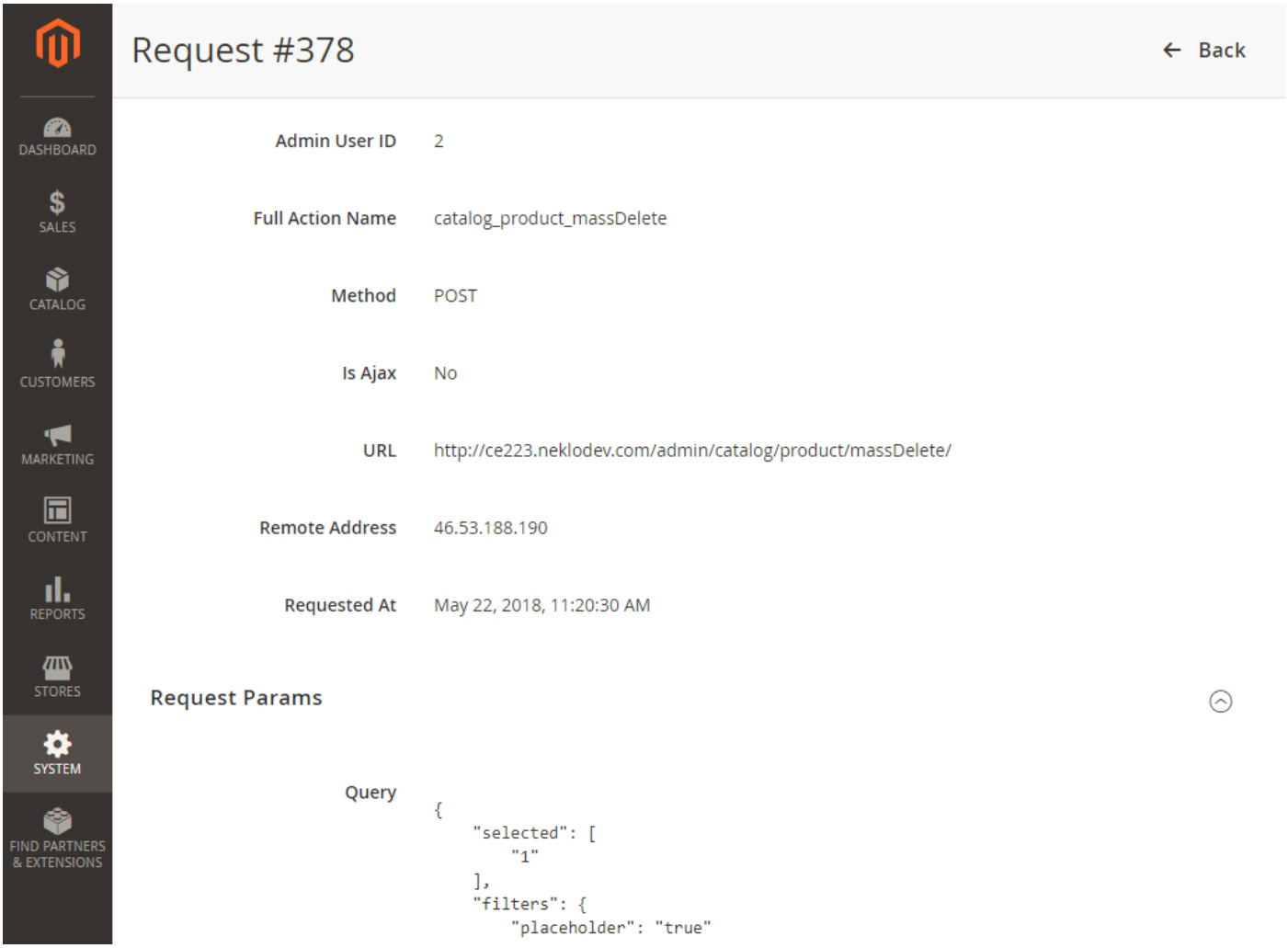


Created At	Admin User ID	Admin Username	Remote Address	User Agent	Message	Status
May 28, 2018 2:29:23 AM	3	TEST	[redacted]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36		SUCCESS
May 28, 2018 2:25:57 AM	3	TEST	[redacted]	Mozilla/5.0 (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

Action Logger Grid

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





Admin Sessions Grid

Sessions grid displays all the admin sessions both active and ended. Here you can terminate any active session you find suspicious.

You can find the grid following **My Account > Account Settings** and then scroll down. There you will see a table with all the admin sessions.

Support

Thank you for using this extension. You will find more our great solutions for Magento here: store.neklo.com