extensions mall

MageFence

User manual

Table of contents

1. Overview

1.1 General information

MageFence is a well-rounded security solution for Magento that keeps your website safe from the most common security threats. It acts as an additional layer of protection around your system, blocking brute force attacks and other hack attempts. It also scans your website on regular basis and notifies you about any potentially unwanted file changes. MageFence offers variety of features that help you keep your website protection up-to-date, end implement the best security practices.

1.2 Key features

- Scan your system for malware and check if your website has already been hacked
- Scan the integrity of your website system files and detect changes
- Schedule time and frequency of the scan
- Check if all Magento security patches are applied and see which patches are missing
- Protect Admin Panel by changing your Admin Panel URL to the custom one.
- Change the Magento Connect Manager URL to protect downloader directory without affecting Magento Connect functionality.
- Detect admin users created without authorization
- Detect missing .htaccess files and restore them with default ones
- Lock out IP address after too many failed login attempts
- Lock out anyone who tries to log in using wrong user name immediately.
- Send email alerts about suspicious activities
- Optionally send an email notification every time admin user logs in

1.3 About this manual

This manual is intended to give assistance to people installing and using MageFence extension for Magento.

2. Installation

2.1 Installation requirements

MageFence extension requires Cron jobs, please check if Cron is set up and working properly on your server. If you need more information about Cron jobs contact your hosting provider.

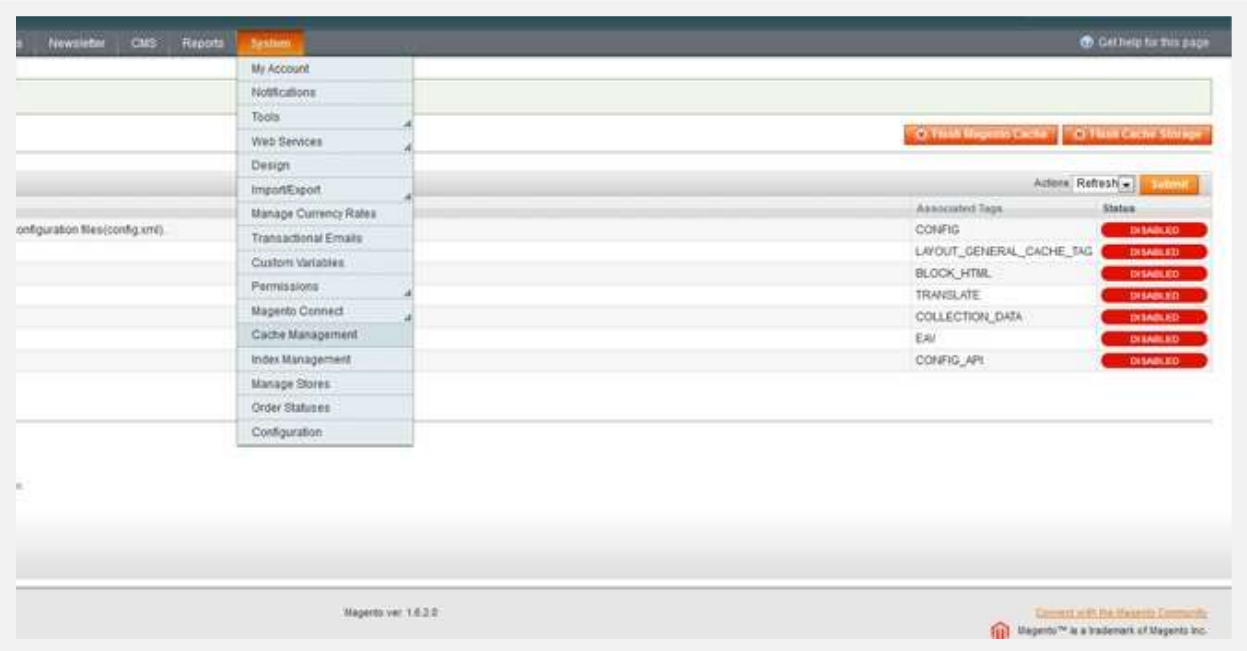
MageFence extension is encoded via ionCube. To run the extension, you must have ionCube loader (http://www.ioncube.com/loaders.php) installed on your web server. For more information about the ionCube loaders, please visit http://www.ioncube.comor contact your webmaster.

2.2 Installation instructions

Before installing MageFence extension you need to disable compilation. Log into your Magento admin panel and go to **System>Tools>Compilation**. If the Compiler Status does not read "Disabled", click the Disable button in the upper right corner.

Extension comes in a .zip file ready for extraction. Copy the files to your Magento root directory.

Next you need to refresh Cache. Go to **Admin>System>Cache Management** and click on**Flush Magento Cache.**



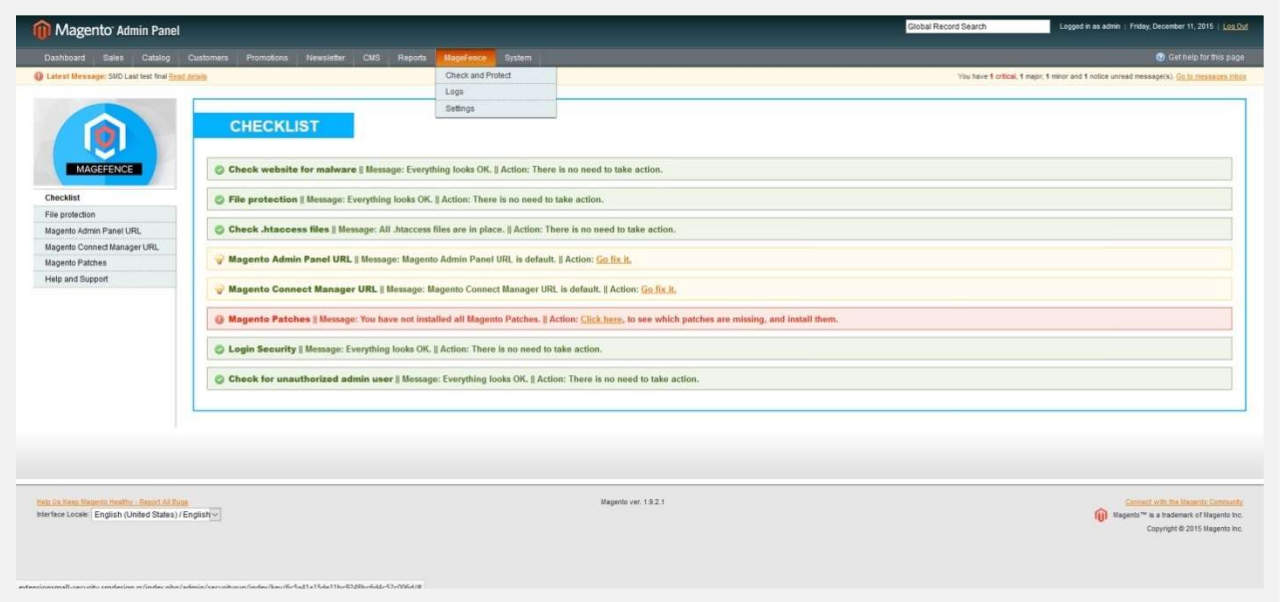
After you have successfully installed the extension, there should be a new item on your admin menu called “MageFence”.

We recommend that you log out of Magento backend and log back in when you install MageFence extension to your Magento or you could be presented with 404 page when trying to save the extension settings.

3. MageFence Features

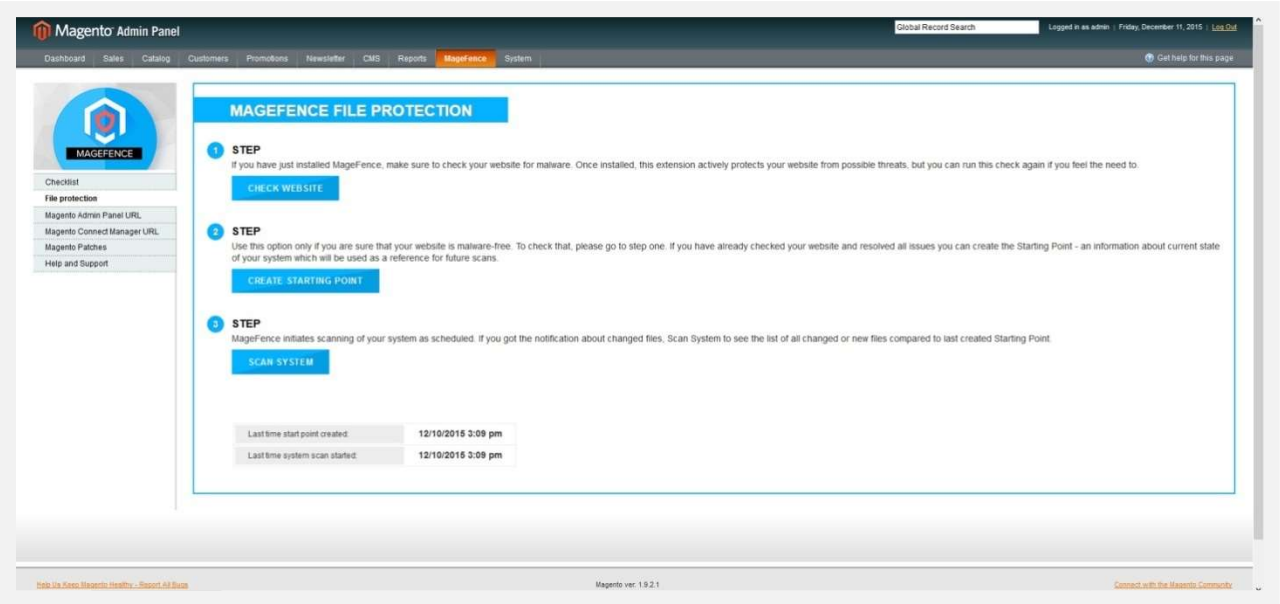
MageFence extension offers essential features for keeping your Magento website safe and secure. To access the features go to **MageFence>Check and Protect**.

3.1 Checklist



This checklist provides general guidelines to achieve optimal security of your Magento website. It contains all the information needed about security status of your Magento: current issues,scan results and actions you need to take.

3.2 File protection



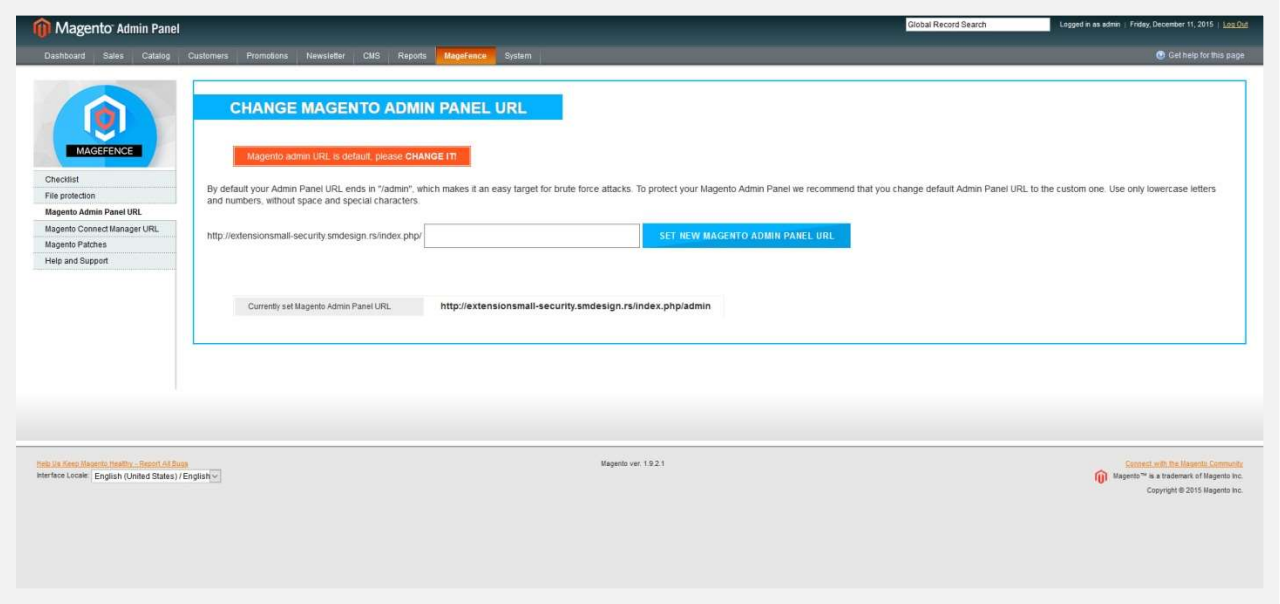
This section contains steps for scanning your website for malware and file changes.

Step 1: check if your website has already been hacked. If you have just installed MageFence, this is the FIRST thing you should do, to insure that your website is malware-free.

Step 2:create starting point.If you have checked your website for malware and resolved possible issues, you can create starting point. This feature will collect information about current state of your Magento system, which will be used as a reference for future scans. That means that MageFence will compare scan results to the starting point and detect all changed and new files.

Step 3:scan system. MageFence scans your website as scheduled, and it is not necessary to manually scan the system. Use this step when you get notification about changed files to scan the system and see the list of changed and new files so you can confirm changes you made and spot potentially unwanted changes that can be result of hacker attack, malware infection, etc.

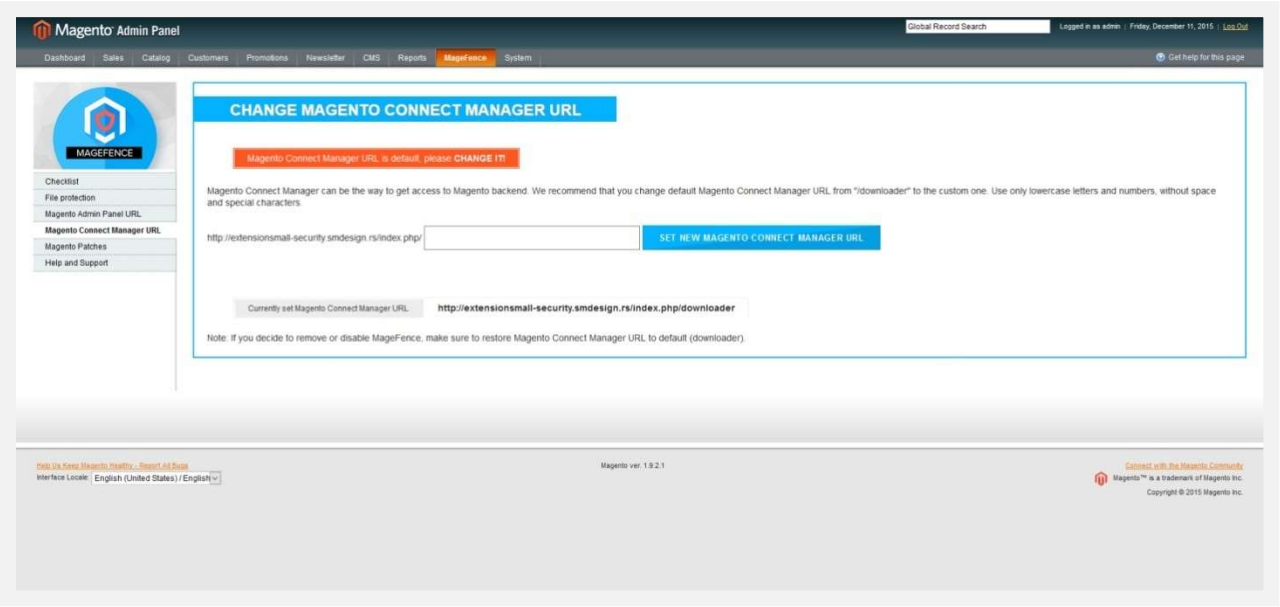
3.3 Magento Admin Panel URL



Admin Panel URL is a location for logging into your Magento backend. By default it is set to “admin” which can be exploited for brute force attacks. To protect access to your backend, we recommend that you change the default Admin Panel URL into the unique, custom one.

MageFence offers you a way to easily change your Admin Panel URL by typing in your custom Admin Panel URL using lowercase letters and numbers, without space and special characters.

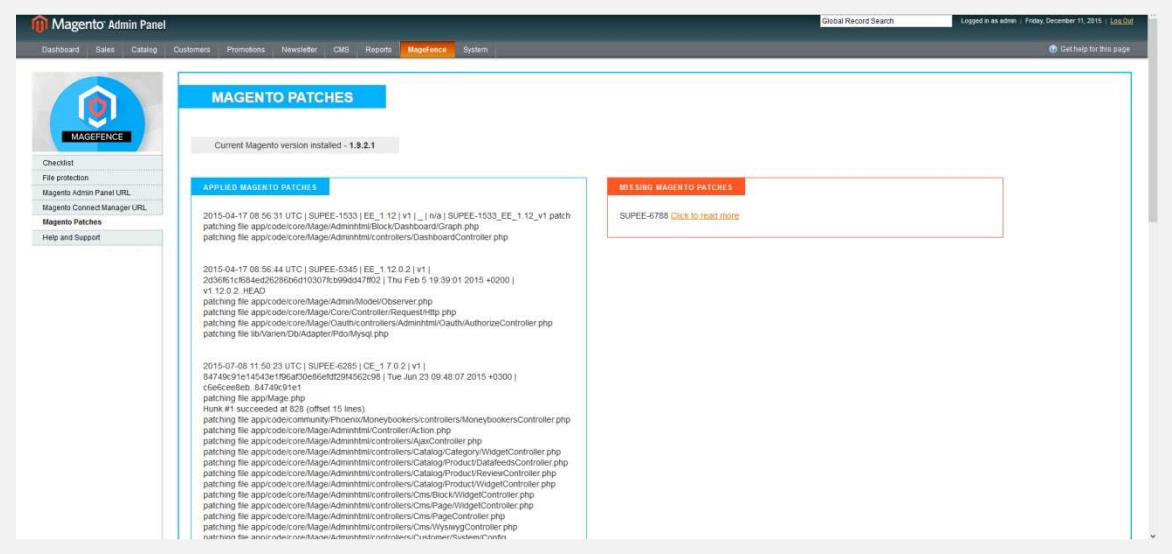
3.4 Magento Connect Manager URL



Magento uses Magento Connect Manager to conveniently install extensions to your Magento. However, thiscan also be exploited for getting access to your Magento backend. MageFence enables you to safely change Magento Connect Manager URL without affecting its functionality, since it doesn't just rename the downloader directory.

Enter custom Magento Connect Manager URL into field, using lowercase letters and numbers, without space and special characters.

3.5 Magento Patches

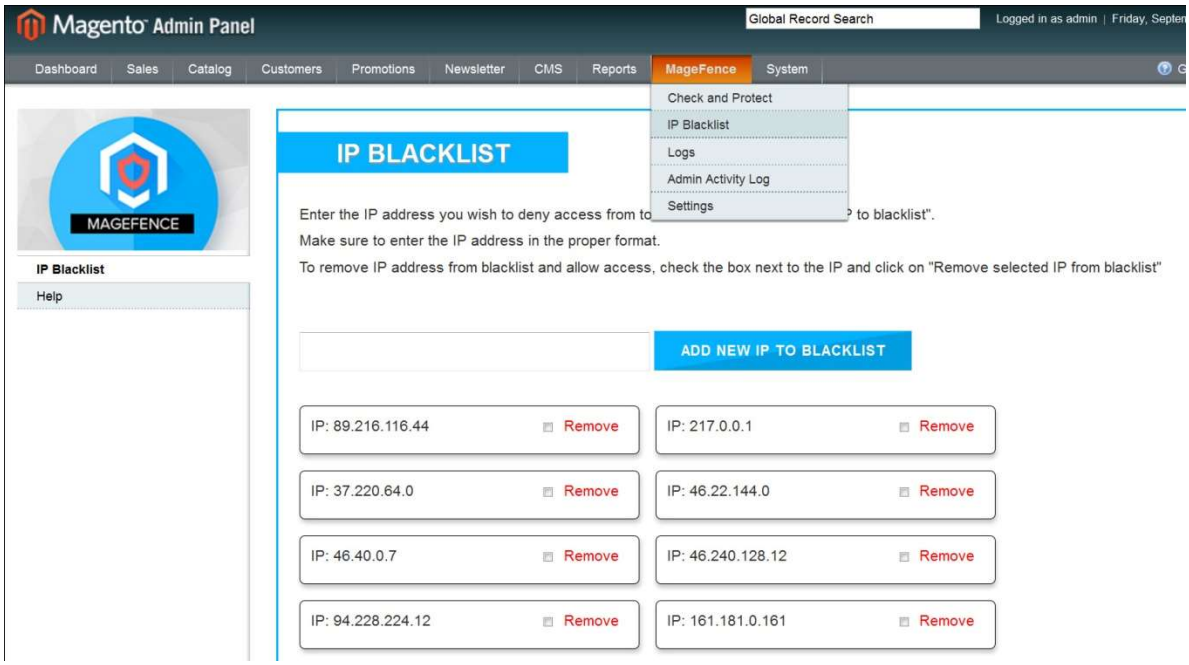


To keep your Magento security up-to-date, you should always make sure to install all the security patches that solve Magento's critical vulnerabilities.

In this section you can see the list of all Magento patches applied, as well as the missing ones that need to be installed.

3.6 IP Blacklist Feature

IP Blacklist feature allows you to block certain IP addresses from accessing your website by adding them to the Blacklist. The extension blocks blacklisted IP addresses through the .htaccess file. This doesn't allow anyone coming from these IP addresses to access your site.

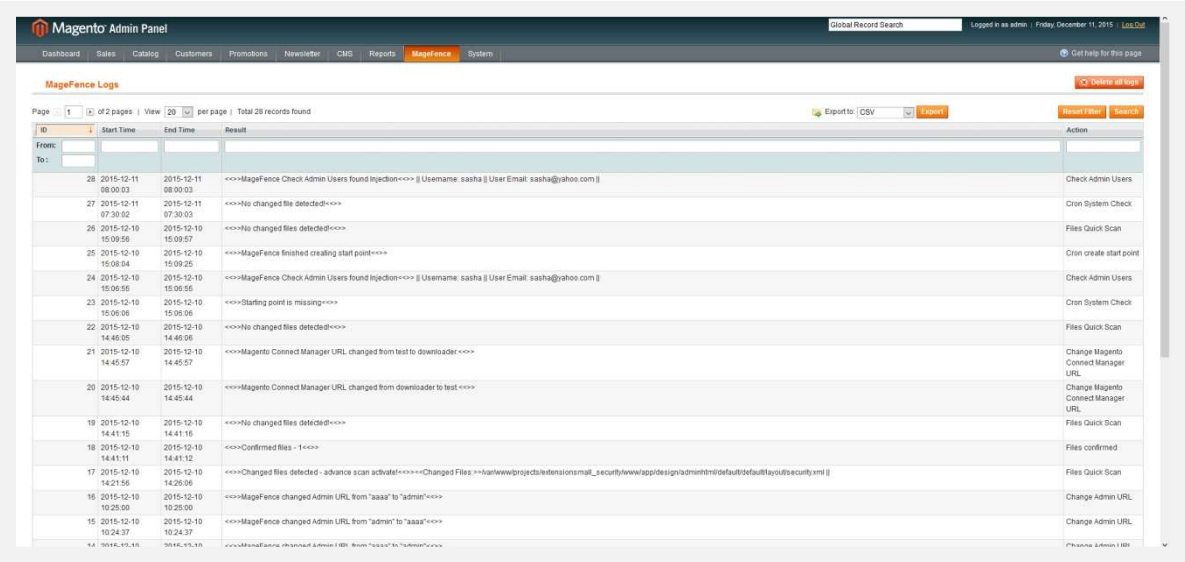


To ban unwanted visitors go to **MageFence>IP Blacklist**

Enter the IP address you wish to deny access from to the field and click "Add new IP to blacklist".

To remove IP address from blacklist and allow access, check the box next to the IP and click on "Remove selected IP from blacklist"

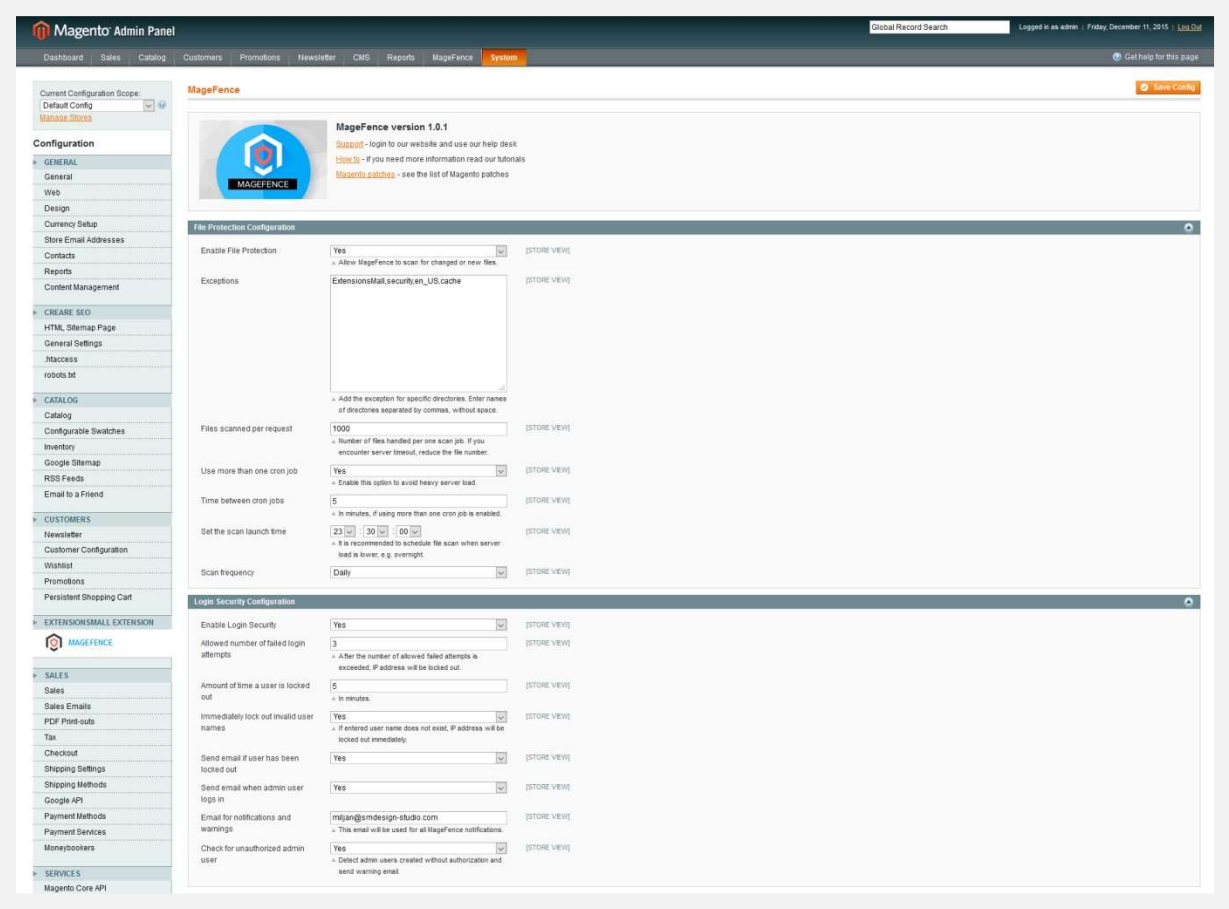
4. MageFence Logs



Mage Fence comes with the built-in logging feature that allows you to get insight into system events and MageFence actions. To see logs go to **MageFence>Logs**.

5. MageFence Settings

MageFence extension default settings are optimal for most Magento websites, butif you require any additional configuration go to **MageFence>Settings**for more options.



5.1 File Protection Configuration

This section offers different options for configuring MageFence scanning feature. Here you can schedule the file scan, set the scan frequency and add exceptions for certain directories (names of directories should be comma-separated, without space).

5.2 Login Security Configuration

Here you can find options forblocking brute force attacks: locking out user's IP address after too many login attempts, locking out user that tries to log in using the wrong user name, checking for unauthorized admin users.

You can also set the email that MageFence will send notifications and alerts to.

6. More information

For more information about MageFence, or any other Magento extension by ExtensionsMall, please visit our website:www.extensionsmall.com .