SiteLock

User Guide

Summary Contents

How to Access Your SiteLock® Dashboard:

1. Login to your SiteLock® dashboard. Depending on where you purchased services, you have two options:

Dashboard Features

At the top left of your dashboard, you will see:

A. Clicking the SiteLock®® logo in the top left will always bring you back to the main dashboard page.

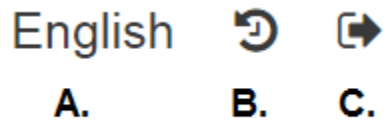
B. Clicking these three lines will collapse the menu on the left side of the screen to only show icons. Click it again to expand it.

C. The "!" icon will bring you to the compliance page.

D. The seal icon allows you to bring up the Trust Seal settings.

E. Clicking the envelope icon will show any SiteLock®® notifications you have.

At the top right of your dashboard you will see:

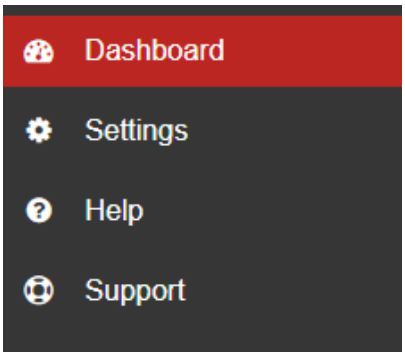


A. Clicking this will allow you to select the Dashboard language

B. Clicking this will bring you back to the old SiteLock®® dashboard.

C. Clicking this will log you out of the SiteLock® dashboard.

On the left side of your dashboard you will see:



Dashboard - This will always bring you back to the main dashboard page.

Users - This will take you to a page that lets you add users to have access to the SiteLock® dashboard.

Settings - This will take you to a page that lets you change a plethora of settings.

Help - This will take you to the SiteLock® help page which contains a lot of information about your products including setup, references, FAQs and more.

Support - This allows you to submit a Support Ticket. Please include as much detail as possible for the issue you are having. Please note that it may take between 24 - 48 hours to resolve your issue.

Understanding Your Dashboard

Under your Security Summary, you should see some circles with symbols on them. If you hover over the circles, it will tell you more detail.

Here are the basic meanings behind them:

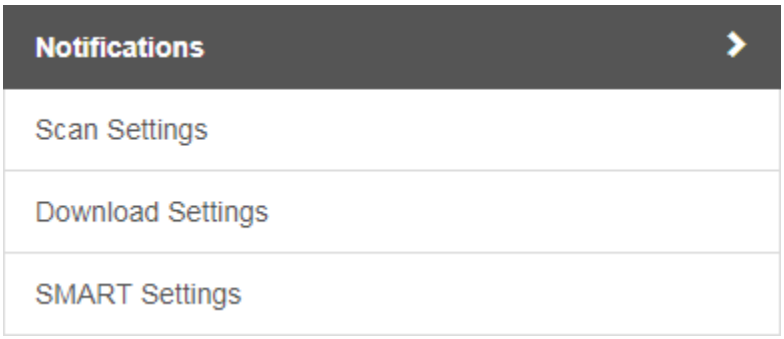
Green Check - Everything is good, and in compliance.

Yellow Exclamation Point - Something is pending (like a scan) or needs to be configured.

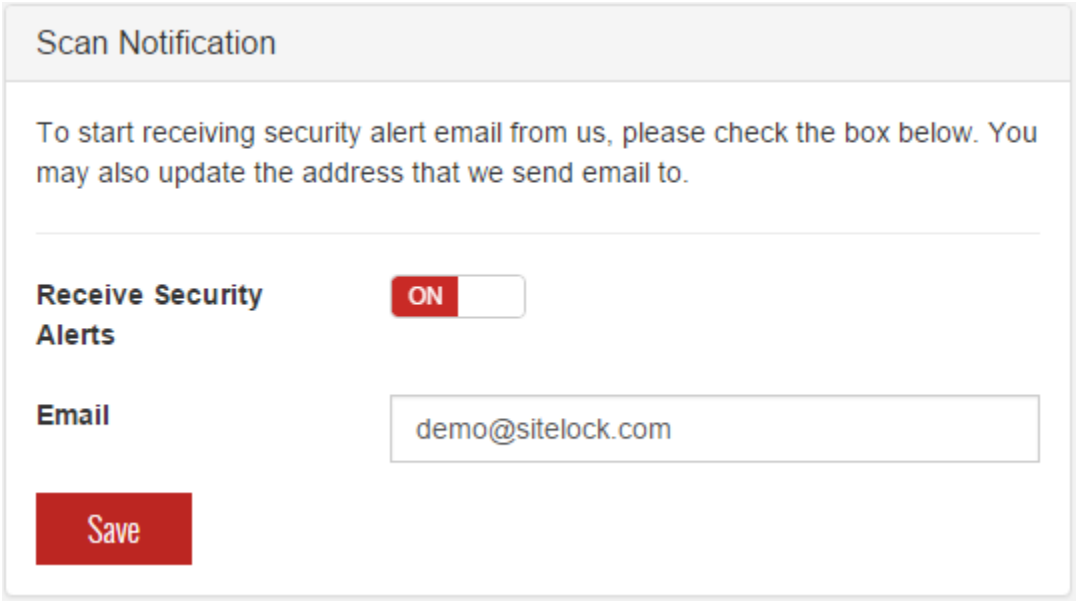
Red X - Something failed, or malware/vulnerabilities were found.

Grey Arrow - Your service needs to be upgraded in order to use this feature.

Dashboard Settings



Notifications -This will allow you to set whether or not you would like to receive security alerts about your website. We do not recommend turning this off.

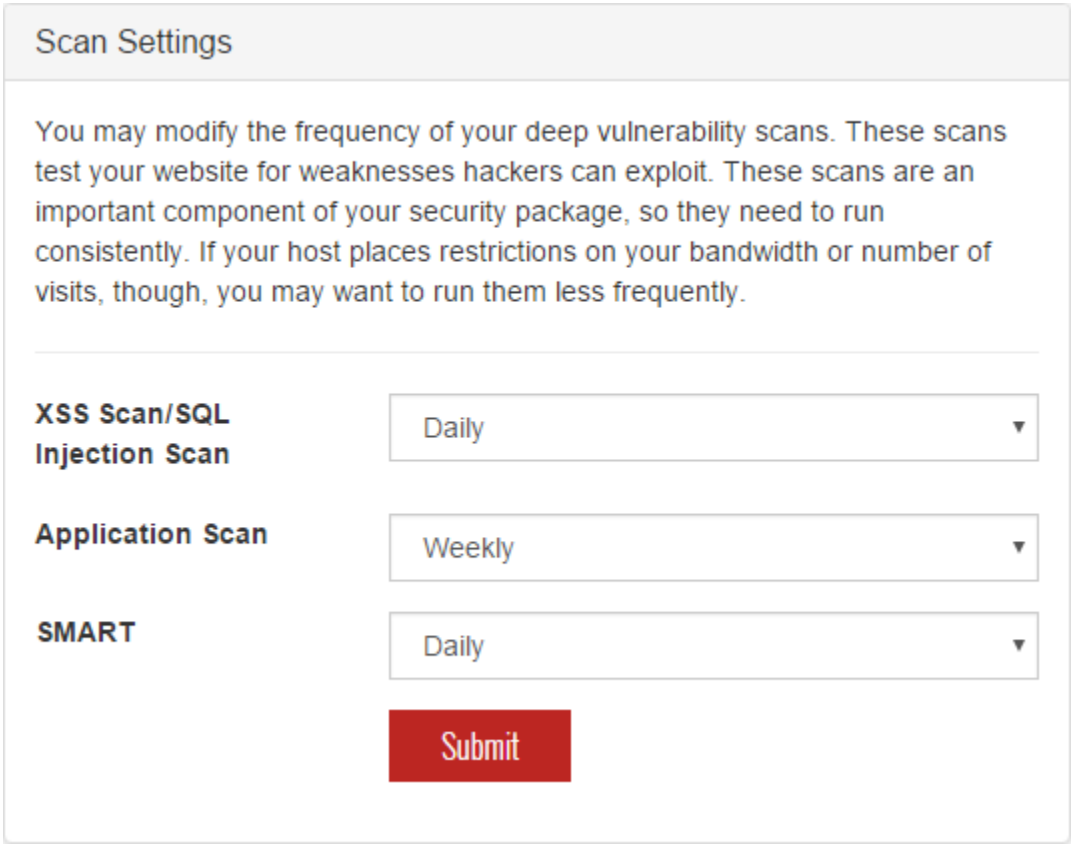


Scan Settings - Here you may change the frequency of specific scans.

You can change the XSS/SQL Injection scan to daily, weekly, monthly or quarterly.

Please note that by default, the application scan runs quarterly. You can change this to weekly, monthly or quarterly. We do not allow it to be changed to daily, as it is a very resource intensive scan on websites. Also, please note that we do not allow frequency changes to be made for certain hosting providers.

You can change the SMART scan to hourly, daily, weekly, monthly, quarterly or never. We recommend either hourly or daily.



Download/SMART/ Settings - Please refer to the SMART and Firewall section for information about these.

Dashboard FAQ

I have a dashboard question about my SMART scanner.

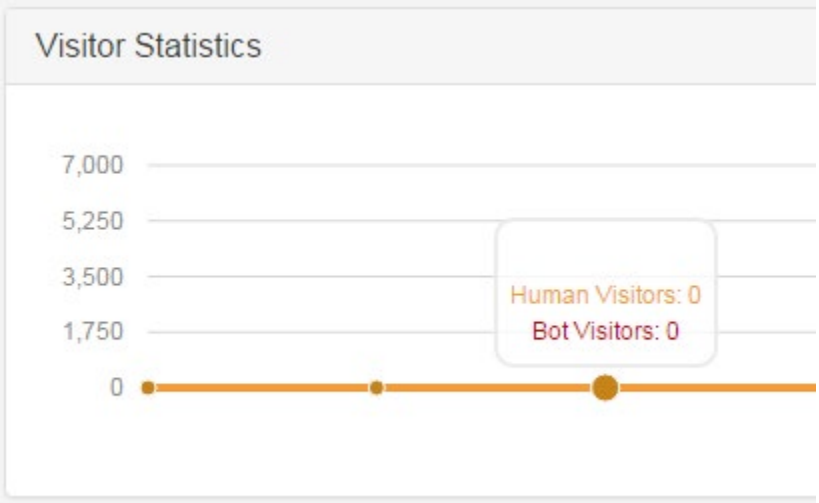
Please refer to their specific documents for specific dashboard information on those products

Why hasn't my application scan run in a long time?

By default, the application scan runs quarterly. You can change this to weekly, monthly or quarterly. We do not allow it to be changed to daily, as it is a very resource intensive scan on websites. Also, please note that we do not allow frequency changes to be made for certain hosting providers.

Main Results Page

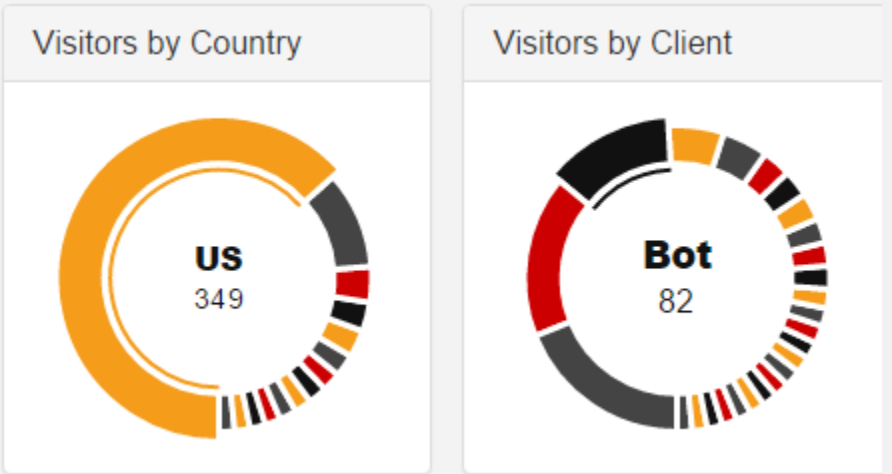
Visitor Statistics - This graph will show you visitor statistics over time with one data point per date.



Map- This map allows you to see where traffic is coming from. The more visitors in an area, the darker that area will appear. You can also hover your cursor over a specific area to see that area's number of visitors.

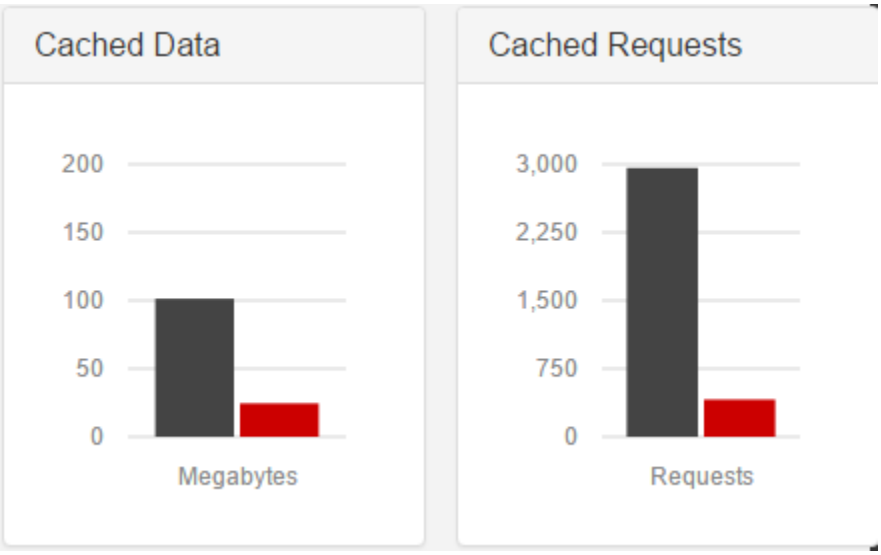
Visitors by Country - On the bottom of the Visitors by Country tab, there will be a chart representing visitors per country. The countries will be abbreviated. You can also hover your cursor over a specific section to see that countries number of visitors.

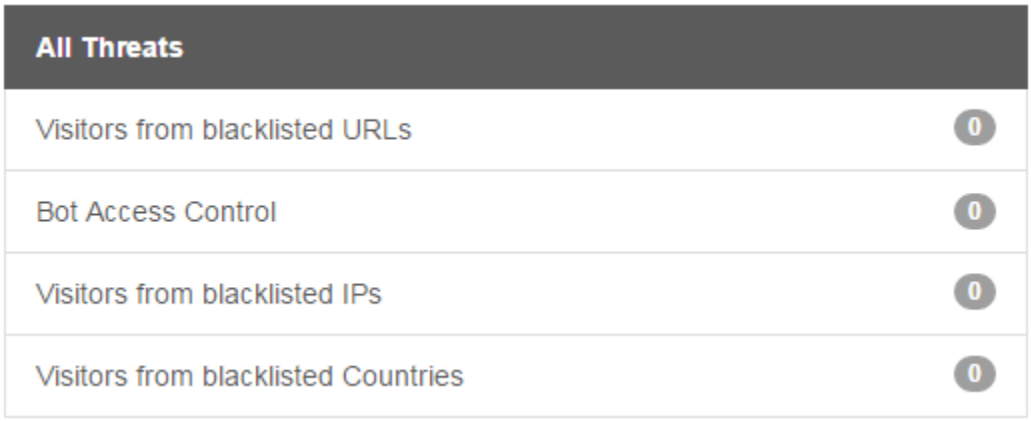
Visitors by Client - On the Visitors by Client, there will be a chart representing the usage of different clients used to access your site. These can include web browsers, bots, proxy applications and more.



Cached Data - The black bar represents the amount of data that was served without using the cache. The red bar represents the amount of data that was served using the cache.

Cached Requests - The black bar represents the number of requests that displayed the website without using a cached version. The red bar represents the number of requests that displayed a cached version of the website.





What is SiteLock SMART® scanner?

SiteLock SMART® (Secure Malware Alert and Removal Tool) is a tool that protects your website by scanning your files for malicious or suspicious content and automatically removing any detected malware.

SiteLock® FIX performs malware and vulnerability scanning on your website. SiteLock® Fix attempts malware detection with a tandem approach of scanning the website both externally and internally.

The external scan refers to crawling each page of your website, much like a search engine, and identifying vulnerabilities and malware (malicious links or scripts). No configuration is required prior to executing an external scan.

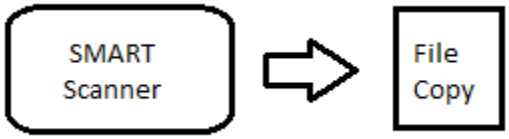
The internal scan (SMART), on the other hand, downloads your website files and analyzes them. It utilizes both signatures and machine learning techniques to identify malicious code and to remove it being proactive with malware prevention helps avoid search engine blacklisting, which means keeping your website online and your business running. SiteLock® FIX also performs additional web app scanning to identify vulnerabilities, such as cross-site scripting (XSS), SQL injection (SQLi), and other common vulnerabilities.

In order for SiteLock® to perform the internal SMART scan, you will need to provide FTP/S or SSH access to your website's files and enable the SMART scan. You will find instructions on how to setup your SMART scan later on this document.

How SMART Works

1. **SMART downloads a copy of the files from the website server to SiteLock server.**

2. **SMART scans a downloaded copy for any malicious code.**



3. **From here, there are two things that can happen to the file if SMART is set up to automatically clean your files:**

a. **If malicious code is found,** SMART removes that code from the file and queues the file to be uploaded with the rest of the clean files back to the website server and replace the original infected file.
b. **If malicious code is not found,** the file is not changed in any way and is not queued with the rest of the clean files to be uploaded to the website server. The original file is still on the website server as it was deemed clean in the first place.

4. **SMART then goes to the next downloaded copy and repeats the process from step 2 until all files are scanned and cleaned.**

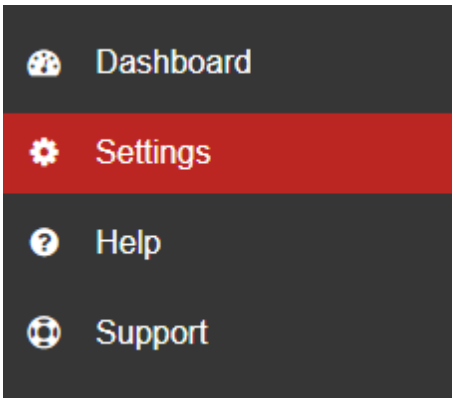
5. **Once all files downloaded have been scanned and cleaned, SMART uploads the clean files to the website server to replace the original infected files.**

6. **SMART repeats the process from step 1 on the next scheduled scan.**

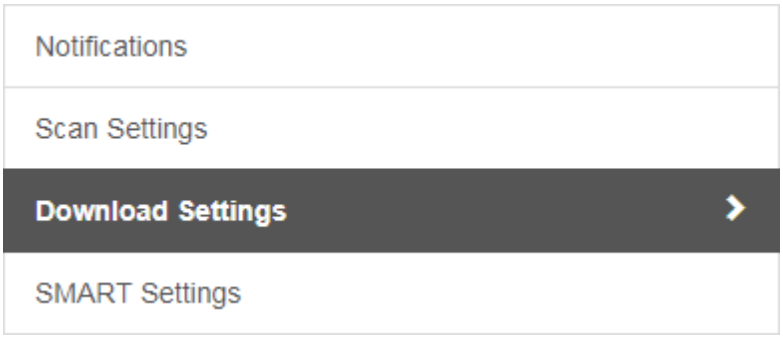
How To Set Up SMART

1. **Locate your FTP information.** If you do not have this information, or do not know where to find it, please refer to the Locating Your FTP Login Information section.

2. **On the main page of your dashboard, click the "Settings" tab.**



3. **On the Settings page, click "Download Settings".**



4. **Select if you are using FTP or SFTP in the dropdown menu next to "Method for File Transfers".** If you do not know which your website is using, you are most likely using FTP. If you are still unsure, contact your server administrator or hosting provider for assistance.

5. **Enter your FTP host address in the "FTP Host Address" field.** This is typically ftp.yourdomain.com OR your website's IP address. When in doubt, use your website's IP address.

6. **Enter the port where your FTP service is running on the server in the "FTP / SFTP Port Number" field.** Most commonly this will be port 21 for FTP, or port 22 for SFTP.

7. **Enter your website's directory in the "Root Directory" field.** If you do not know your website's directory, either contact your developer or hosting provider to find it. We will not be able to locate this information for you.

8. **Enter the FTP username in the "User ID" field.** Provide that there are no spaces before, after or in the username. SMART does not support usernames with spaces or % symbols in them.

9. **Enter the FTP password in the "Password" field.** Provide that there are no spaces before, after or in the password. SMART does not support passwords with spaces in them.

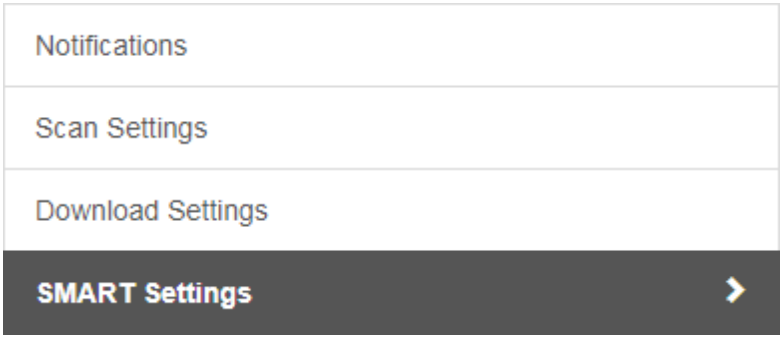
10. **Select the "File Download Speed" in the dropdown menu.** This determines how many connections SMART opens to scan files.

11. **Select the "Maximum Download Time" in the dropdown menu.** This determines how long SMART will scan files before stopping until the next cycle. SMART will continue where it left off the next day/cycle

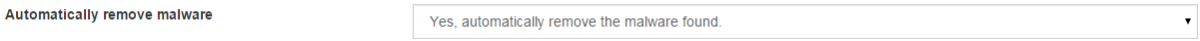
12. **Click the red "Submit" button to save the changes.** Provide that it says "Information updated successfully" after it is done saving changes. If it says "Invalid form submit", re-enter the information and try again.

If you would like SMART to remove malware automatically, continue on. If not, SMART is completely configured and you can stop here. A scan will run on the next cycle.

13. **Click the SMART Settings tab.**



14.Provide that **the dropdown box says "Yes, automatically remove the malware found."**



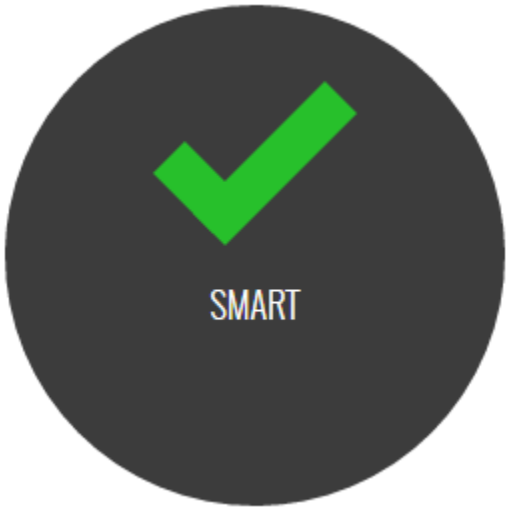
15. **Click the red "Submit" button to save the changes. SMART will now remove malware automatically and is completely configured.**

SMART Setup Tips

- If you change your FTP password, you will have to update it in the SMART download settings or else SMART will not run.
- SMART does not support usernames with spaces or % symbols in them.
- SMART does not support passwords with spaces in them.
- Provide that there are no blank spaces before or after any entries in the fields, this will cause an error if there are.
- If your dashboard is saying there was an error with SMART, please consult our "Common SMART Errors" and "SMART FAQ" section.

Understanding Your SMART Scan Results

You can find your SMART scan results by clicking the circle that says SMART on the main page of your SiteLock® dashboard as seen below.



Results Page

Date and Time: The date and time the scan was run. You can click a specific date and time to see more details of a scan.

Scanned: The amount of files SMART scanned.

Added: Files that were added to your server in the time from the last scan. These can also be cached or temporary files used by the web server and/or CMS.

Modified: Files that were modified on your server in the time from the last scan. These can also be cached or temporary files used by the web server and/or CMS.

Deleted: Files that were deleted from your server in the time from the last scan. Please note that our SMART scanner does not delete files on your server. This likely means you removed files from your server in between scans.

Malware Found: Files that were found to be infected with malware.

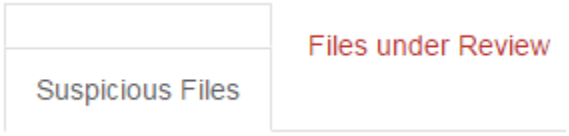
Malware Cleaned: Files that were able to be cleaned by SMART.

Review: Files that are suspicious, but are flagged to be reviewed by our research team to provide that they are malware.

Status: The status of that scan, not the status of your website. A green dot indicates the scan came back clean. A red dot indicates the scan detected malware.

Specific Scan Details

If you click on a date and time, you can see more details about the scan.



Suspicious Files - Files that SMART found to be suspicious.

Files under Review - Files that are under review by our research team.

Suspicious Files Tab

File Name - The filename of the file that SMART found to be or contain malicious code.

Malicious Code Found - If SMART found malicious code, it will say yes. Otherwise, it will say no.

Malicious Code Cleaned - If SMART was able to clean the malicious code, it will say yes. .Otherwise, it will say no.

Malicious Links Found - The number of malicious links SMART found.

Changed By You -If the code in this file was changed by you, it will say yes. Otherwise, it will say no.

Changed by Us - If the code was changed by us, it will say yes. Otherwise, it will say no.

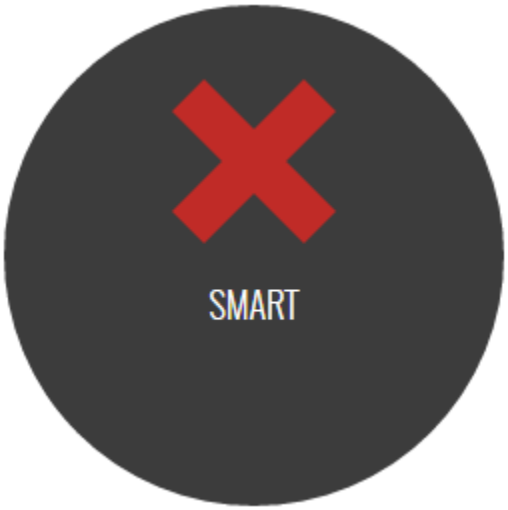
Files under Review Tab

File Name - The filename of the file that is under review by our research team.

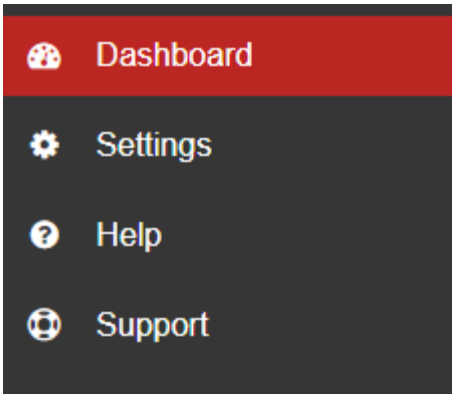
Common SMART Errors

If your dashboard is saying there is an error with SMART, you can find out the specific error by following the steps below, and then referencing the errors listed on this page.

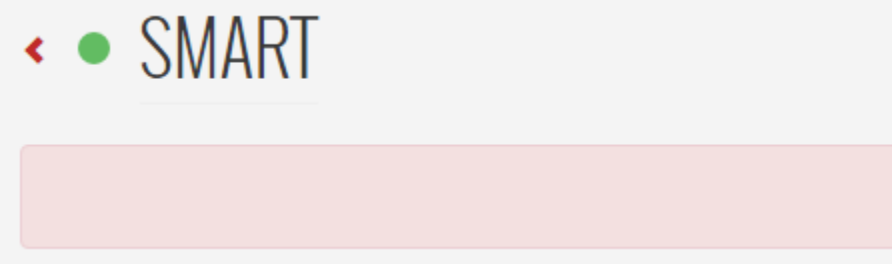
1. **On your dashboard, there should be a black circle with a red “X” that says “SMART” underneath**



2. **If you hover over this circle with your mouse, the red "X" should change to say "Error".**



3. **On this new screen, there should be an error in red or yellow text in a red or yellow rectangular box below the word "SMART". Reference that error with the ones below.**



Max retries exceeded - Any issue below that SMART has encountered multiple times in a row. Most common cause for this is a bad hostname, see below for more details on that issue.

Login authentication failed - Incorrect FTP login credentials were used in the SMART settings. Ensure you are using the correct FTP username and password, and check for spaces in the “User ID” and “Password” fields

Bad hostname - The wrong hostname was entered into your SMART settings. Check for spaces in the “FTP host address” field, use your website’s IP address, and provide that you have the correct hostname. If you have our firewall, make certain you are using your website’s IP address.

Cannot find directory - A redundant or wrong directory was entered into your SMART settings. Provide that the directory you input is not already included in the FTP user settings you created. Check the file path and resubmit the SMART settings.

Timeout Errors - Your server did not respond to our request within a certain amount of time. Either try again or contact your hosting provider for assistance

Permissions Errors - Either a file or directory has incorrect permissions. Contact your host to reset permissions on your server.

Filenames/Bad Filenames Errors - SMART cannot read certain characters in filenames. Rename the file to something generic and without spaces and run the scan again.

FTP user blocked/Suspicious Activity - This means your hosting provider has blocked the FTP user or IP address SMART is using. Contact your hosting provider to have them remove the block on both the FTP user and the listed IP address if there is one listed

FTP Quota Errors - The FTP quota for the FTP user has been exceeded. Either increase the quota, or contact your hosting provider for assistance

Disk Quota/Disk Space errors - The disk space on your server has been used up and SMART cannot upload files it has cleaned to your server. Remove unneeded files from your server to fix this issue as we cannot delete them for you.

SMART is scanning only one file - When you created an FTP user, it may have asked for a directory to assign to it. On some hosting dashboards, it will automatically input the username as a directory and create that directory with one file in it named ftpquota. The way to fix this is to delete that ftp user in your hosting settings, re-add it and provide that the field only says public_html. If you are still unsure of this, ask your hosting provider for assistance.

SMART FAQ

Does SMART delete any files from my server? The SMART scan result says some files were deleted. What does this mean?

No, SMART never deletes any files from your server. As our SMART scanner is programmed not to delete files, this means it saw that files were removed from your server from the last time the scan ran

If I move hosting providers, will I need to change the settings?

Yes, if you change where your website files are hosted you will need to create a new FTP user on your new server and update the settings in SMART

Does SMART scan databases?

No, SMART does not scan any databases.

SMART found malware but didn't clean it. What happened?

This could be due to one of three reasons:

1. SMART was not configured to remove malware automatically during setup. Check the SMART Settings tab in the settings portion of your dashboard and provide that it is set to automatically remove malware.

2. SMART found malware it could not clean for a number of reasons. If this is the case, your site will need to be cleaned manually.

3. Your server is blocking our attempts to upload the cleaned files back to your server.

Why can't SMART always clean the malware on my site?

There are new malicious codes and threats coming out all the time. As a result, SMART may sometimes find code it deems suspicious, but not know how to rectify the problem. This is why any suspicious code we find is reviewed by our research team to add to our database of threats.

The SMART scan results are saying it scanned only one file. Why is this?

When you created an FTP user, it may have asked for a directory to assign to it. On some hosting dashboards, it will automatically input the username as a directory and create that directory with one file in it named ftpquota. The way to fix this is to delete that ftp user in your hosting settings, re-add it and provide that the field only says public_html. If you are still unsure of this, ask your hosting provider for assistance.

How The Trust Seal Works

For example purposes, we will be using SiteLock®.com in these pictures.

After you have installed the Trust Seal on your website, it works by pulling data from our scanners running on your website, and not through the Firewall.

If our scanners determine your website is clean, it will display "Passed" in green along with the date it determined it was clean. Please note that the date displayed will be the last scan that

was run and came back clean. Check your scan frequency settings if it is displaying an older date.

If our scanners determine your site got infected with malware or a vulnerability and was not resolved after 72 hours, the Trust Seal will automatically be removed. After you have resolved these issues, the Trust Seal will automatically be displayed again on your website.

If you click on the Trust Seal, it will bring up a new window as shown below.

Company Name - This will display your business's name.

Domain -This will display your domain name.

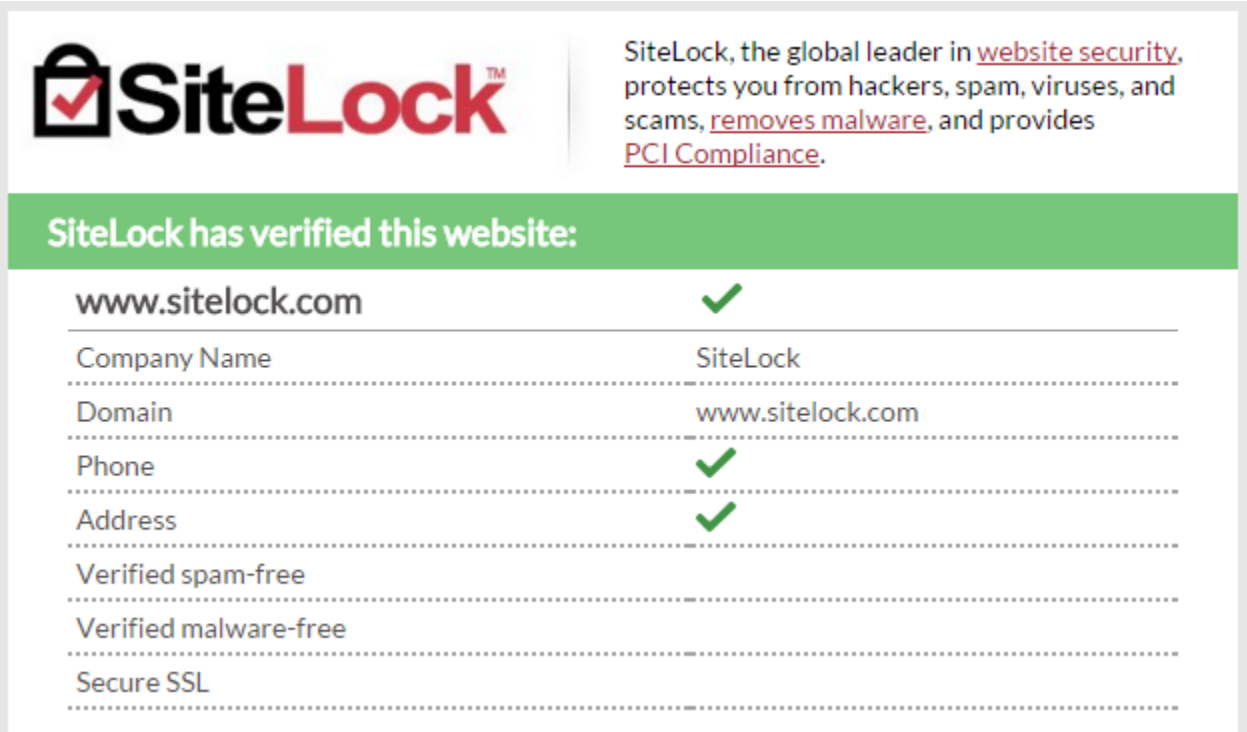
Phone -This will display whether or not we have verified your phone number. If it says otherwise, please contact us so we may verify it.

Address -This will display whether or not we have verified your address. If it says otherwise, please contact us so we may verify it.

Verified spam-free -This will display the last date our scanners determined your site to be spam-free.

Verified malware-free -This will display the last date our scanners determined your site to be malware-free.

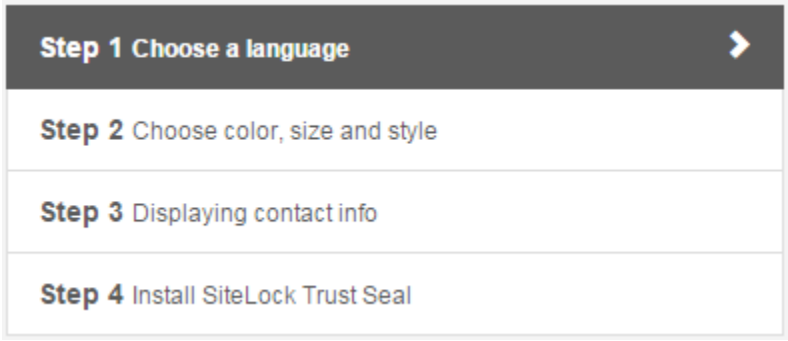
Secure SSL -This will display the last date our scanners detected your SSL.



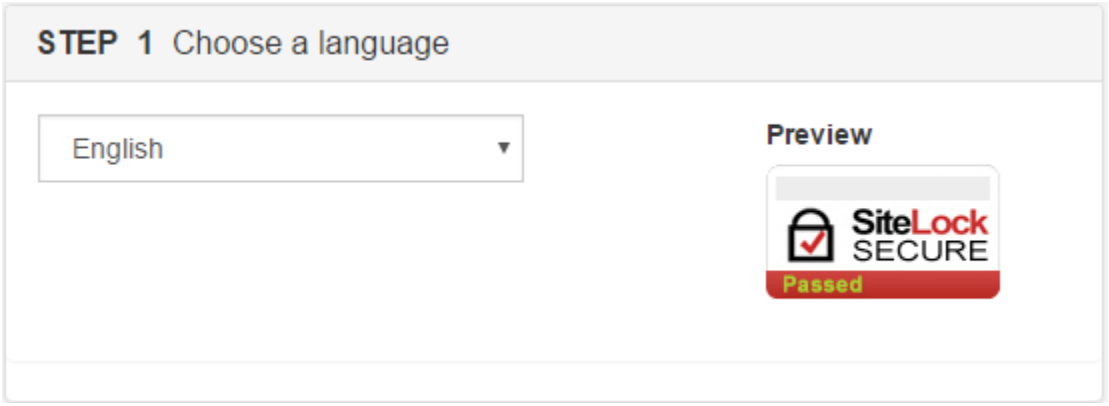
How to Install The Trust Seal

1.**Near the top of the main page of your dashboard, click the button with the shield shown below.**

2. **On the next page, you should see 4 steps. You can click each step to change their settings.** When you are finished making changes on each step, click the next button to continue to the next one.



3. **Choose a language.** Select which language you want the Trust Seal to display by using the dropdown box. When you are finished making these changes, click the next button to continue.



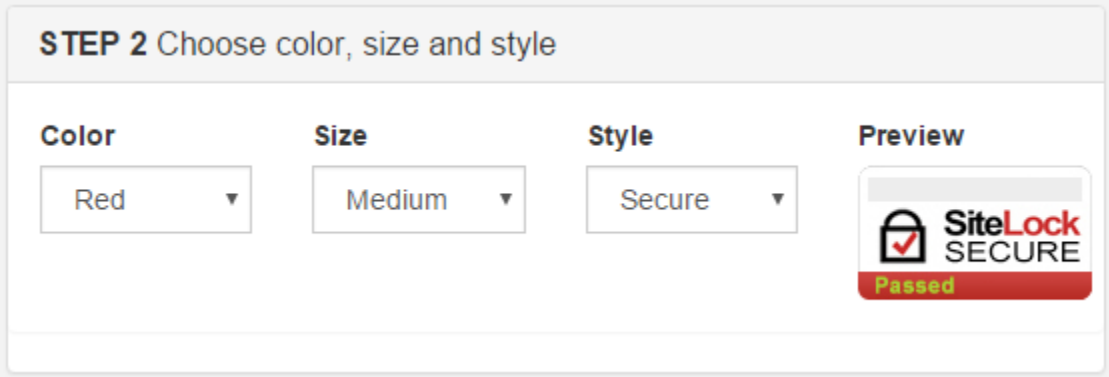
4. **Choose color, size and style.** Here you can change the size, color and style of the Trust Seal. All options you select will update the example Trust Seal on the right. When you are finished making these changes, click the next button to continue.

Please note that the Trust Seal cannot be customized further than the options listed below. We will not accommodate any customization requests.

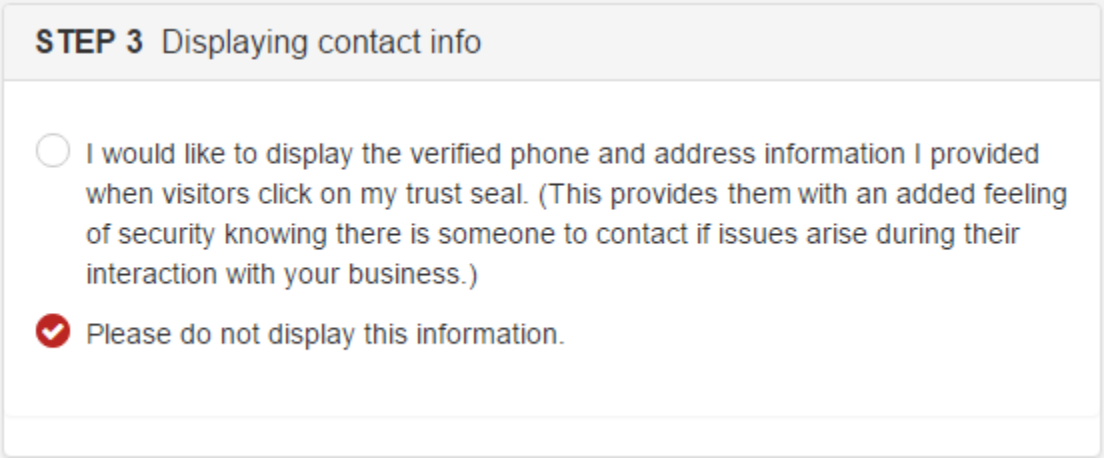
☐ **Color** - You can select from red or white. This will change the color of the small bottom portion of the Trust Seal that says “Passed”.

☐ **Size** - You can select from small, medium and big. This will change the size of the whole Trust Seal.

☐ **Style** - You can select from “Secure” or “Malware Free”. This will make the Trust Seal say either “Secure” or “Malware Free”. You must have a premium or higher scanner to be able to display “Secure”. Otherwise, it will always say Malware Free.



5. **Displaying contact info.** Select if you wish to display your contact information to visitors when they click on the Trust Seal. It is not required to display contact information. When you are finished making these changes, click the next button to continue.



6. **Install SiteLock® Trust Seal.**

Step 4 will display the code you need to put into your website's code.

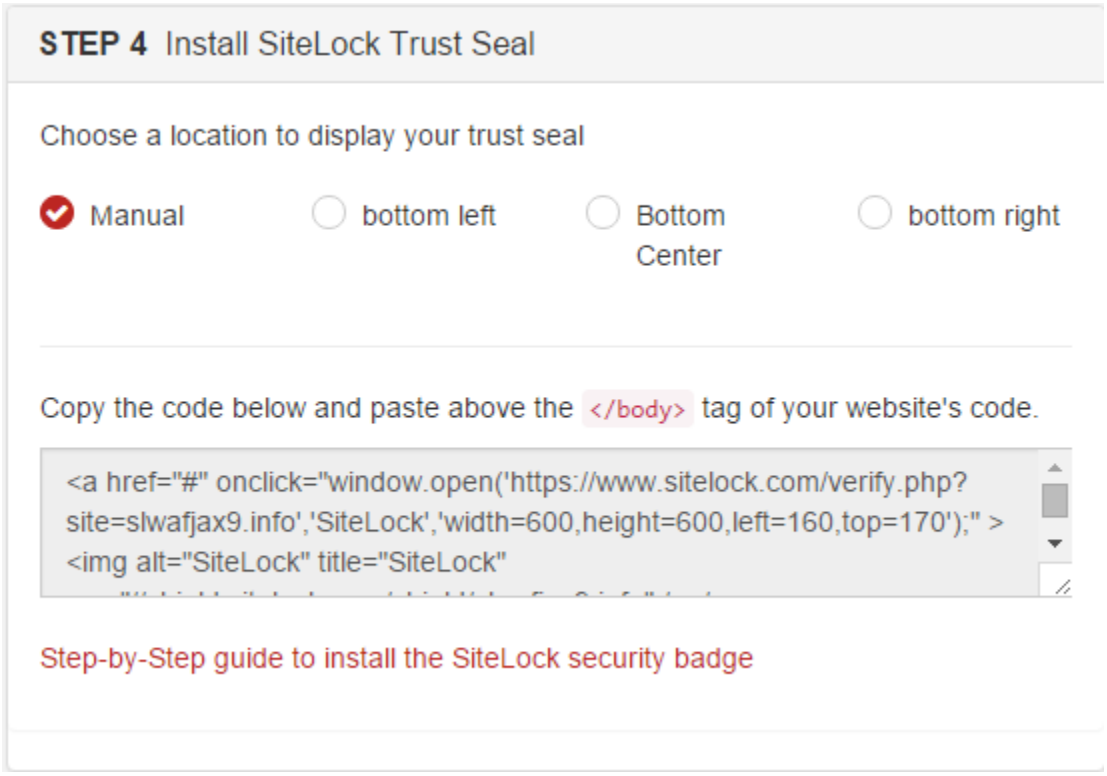
☐ **Manual** - Copy the code and put it into your website's code wherever you would want it displayed.

☐ **Bottom Left** - Copy the code and paste above the tag of your website's code. It will then display the Trust Seal on the bottom left part of your website.

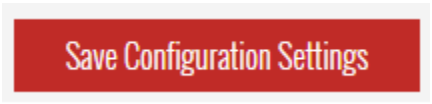
☐ **Bottom Center** - Copy the code and paste above the tag of your website's code. It will then display the Trust Seal on the bottom center part of your website.

☐ **Bottom Right** - Copy the code and paste above the </body> tag of your website's code. It will then display the Trust Seal on the bottom right part of your website.

If you need assistance with this, please contact your web developer or systems administrator as they should easily be able to do it for you. If you do not have one, please contact us for assistance.



7. **After the code is in your website, click the "Save Configuration Settings" button.** Please allow up to 24 hours for your Trust Seal to come online and appear on your website. If it does not appear, there could be a few reasons why. Refer to the Trust Seal FAQ article for more details.



If after following these instructions you still need assistance, please contact us.

Trust Seal FAQ

My Trust Seal suddenly disappeared off of my site. What happened?

This can be due to a number of reasons:

- Your site got infected with malware or a vulnerability and was not resolved after 72 hours. **You do not need to make any changes to your Trust Seal code if this is the case.** After you have resolved these issues, the Trust Seal will automatically be displayed again on your website.
- You may have made a change to your site that replaced the code.

Why isn't my website's name or URL showing up in the Trust Seal?

This happens when the domain name is too long to fit into the space. Try using a larger Trust Seal in the settings.

I updated the size/color/style of the Trust Seal after installing it, but it hasn't updated. What happened?

Clear your cache and cookies in all of your browsers.

Can SiteLock® customize my Trust Seal further than the preset options?

No, the Trust Seal cannot be customized further than the preset options.. We do not accommodate any customization requests.

I chose "Secure" as my style but it still only says "Malware Free" on my site. Why is that?

You must have a premium or higher scanner to be able to display "Secure".

Do I have to have the firewall to use the Trust Seal?

No, the TrustSeal doesn't require firewall. It pulls data from scanners.

My Trust Seal is displaying an older date. Why is that?

The date displayed will be the last scan that was run and came back clean. Please check your scan frequency settings if it is displaying an older date.