User Guide v 1.1.1

2020

Table of Contents

Introduction

PC Matic Mac is for consumers that are looking to protect 10 or fewer endpoints. It is available as a 5 or 10 license per year subscription or lifetime subscription (Evergreen).

PC Matic consists of several parts:

- Real time whitelist based malware protection known as SuperShield.
  - SuperShield is active and protects the computer 24/7; the scans will be scheduled to meet your needs.
- An on demand scanner that will clean and maintain each endpoint.
  - You can schedule scans at several different intervals: one time, daily, weekly or monthly. Choose a start day and time and insert an email address to receive the clean reports after the scan completes.

Optimal System Requirements

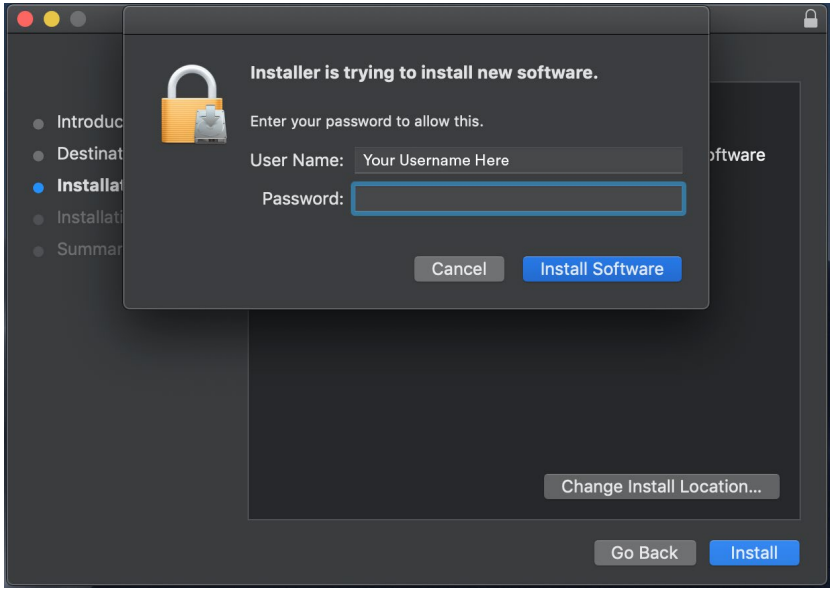
- **Computer Operating System**: macOS Sierra, macOS High Sierra, macOS Mojave
- **Processor**: 1 GHz or faster
- **Memory**: 1024 MB or more
- **Hard Disk**: Need 1 GB or more of free space
- Active Internet Connection
- **Current PC Matic Mac Version**: 0.0.39 (Build 180)

Installation

The process for installing PC Matic Mac begins with a .pkg file that is used for all Mac application installs. Our installer file is named “PC Matic.pkg”. If you don’t already have the proper installer file on your Mac, you can click here to download the .dmg file that has our installer inside it.

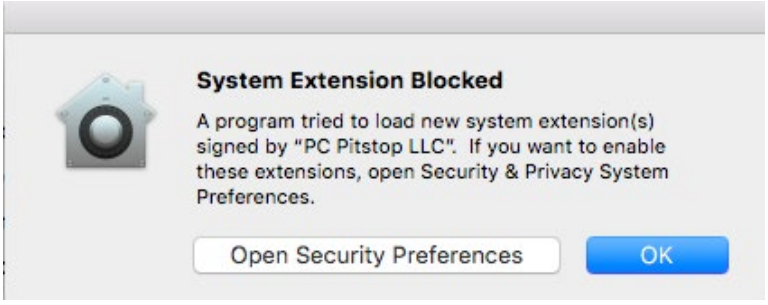
To complete the install process, you will need to know the administrator password for the computer. This is most likely the password you use to login to your Mac on a daily basis.

1. Navigate to where you downloaded and/or saved the .dmg file linked above and double click it.
2. Inside you’ll see the PC Matic.pkg file to begin the install process, right click that file and select Open.
3. Click Open again.
4. Click Continue.

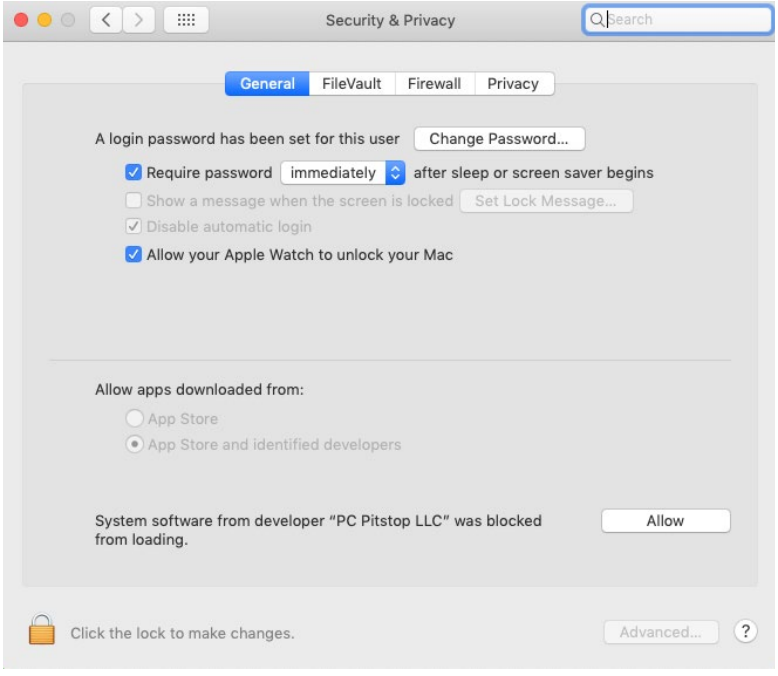


5. Click Install.
6. Type in your administrator password and click Install Software.
7. The install process may take several minutes to complete.
8. Before completion, your Mac will prompt you to allow our system extension. The system

extension is critical for antivirus products and must be allowed for PC Matic to protect your device. Click Open Security Preferences in the prompt, or click OK and then Open Settings and select Security and Privacy. (If you don't see this prompt, skip to step 12)



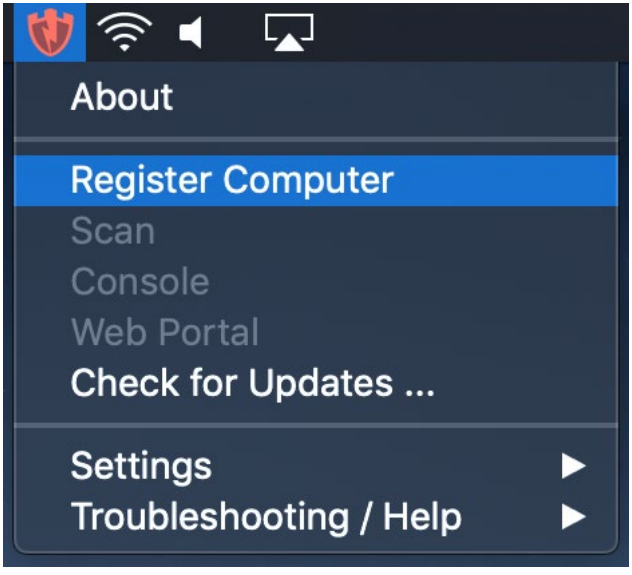
9. In the Security and Privacy window at the bottom you will see "System Software from



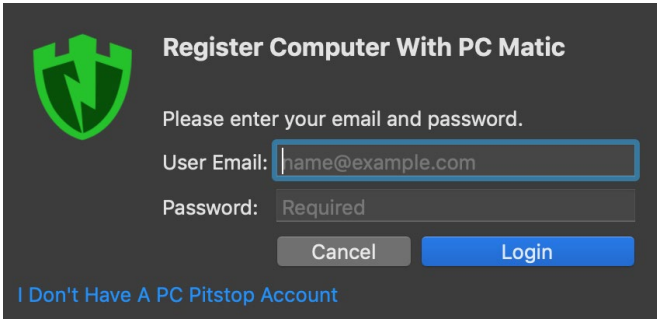
Developer "PC Pitstop LLC" was blocked from loading". Click the allow button. If you cannot click allow, select the lock in the lower left corner and enter your administrator password first.

10. After you click allow the option will disappear and you can close the Security and Privacy window.

11. Once completed, click Close.
12. You should now see our PC Matic Mac icon appear in the Status Bar at the top of your desktop. It will begin as a red shield.



13. Click the red shield, and select 'Register' to connect this Mac with your PC Matic account.
14. Sign in with your PC Matic account information.



15. Once signed in, the shield will switch over to green to show that your device is protected. If you are having trouble remembering your password, you can always do a password reset here.
16. Installation is complete!

System Extensions

Beginning with the 10.13.2 update of macOS High Sierra, Apple now restricts apps that require access to the kernal of your device which is a core part of the operating system. Almost all antivirus products, like PC Matic Mac, require access to the kernal to protect the device. This requires additional steps of allowing the system extension from PC Pitstop LLC for PC Matic Mac to function properly.

The user alert and approval option for the system extension only display in Security and Privacy for 30 minutes after your installation attempt, so it is important that you allow it during the initial install.

If you did not allow the extension in time, follow the manual steps below to bring the Allow button back in Security and Privacy.

1. Navigate to your Applications Folder and find the Utilities Folder inside it.
2. Double click the program Terminal inside that folder.
3. Within Terminal, copy and paste the code below and press enter.
   - sudo kextload /Library/Extensions/PCMaticListener.kext
4. You may see an error appear on screen after this, that is normal.
5. Now return to System Preferences, and open Security and Privacy. You should see the option to 'Allow' the blocked system software from PC Pitstop LLC. Click Allow.
6. Reboot your machine.

Without allowing the System extension for PC Matic Mac either during initial install or with the manual process above, your device will not be protected.

Shield Status

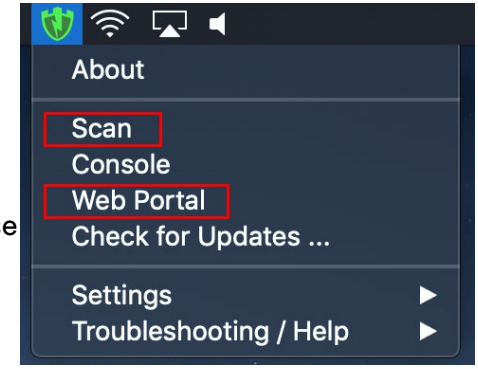
PC Matic Mac has several different shield status that are designated by the color of our shield in your Status Bar. If you hover over the shield icon, it will provide details on why it is in the current status unless it is green.

- Green Shield - Your Mac is currently protected and your account status is good.
- Yellow Shield - Your Mac is currently protected, but your account is expiring soon.
- Red Shield - Your protection is not active. Your account may be expired or not logged in correctly.

If you're unsure how to diagnose or fix a problem with a certain shield color, please check the

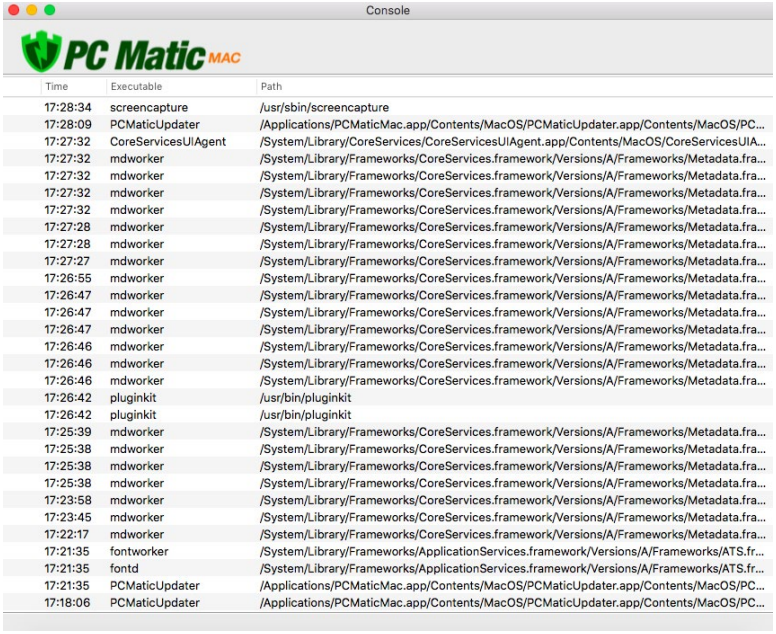
Support section of this guide and contact our customer service team for assistance.

Local Device Options



After installing our macOS client, you'll notice a SuperShield icon in the Status bar of your Mac. Inside this SuperShield icon there are several options you can take advantage of right from the device.

- **Scan** - The scan option allows you to run an immediate manual scan on the device. This scan will automatically use the defaults for a PC Matic scan and when finished, the results will display inside your PC Matic Web Portal.
- **Console** - The console of PC Matic Mac provides insight into what is attempting to run on your device. You can open and view the Console by selecting it in the menu. You should always see activity filling up the console, which means that SuperShield is monitoring everything and keeping you secure. If nothing is populating in the console, your account may be expired or you did not allow the system extension after install.

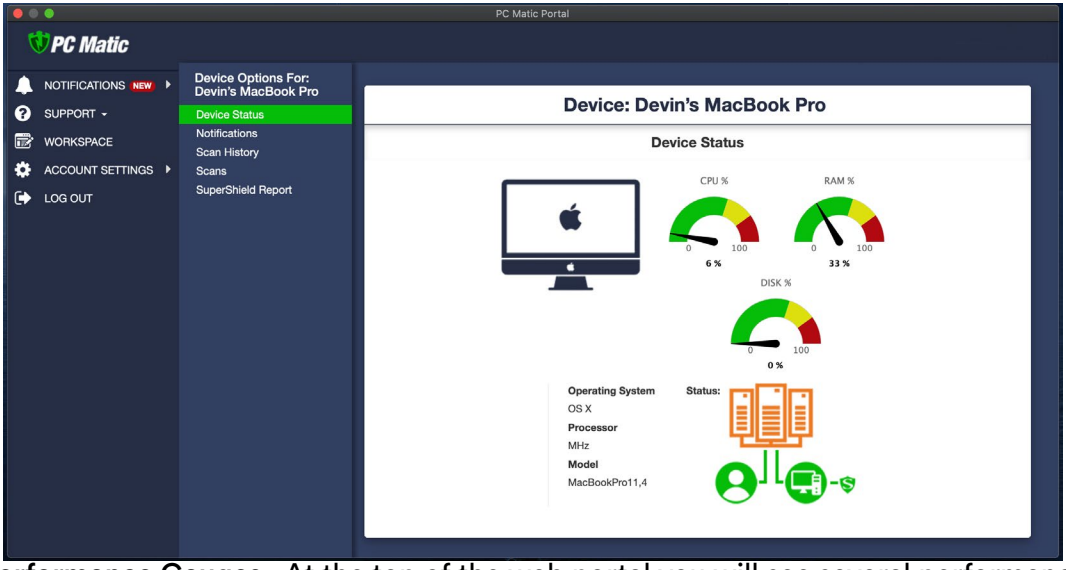


Time	Executable	Path
17:28:34	screencapture	/usr/sbin/screencapture
17:28:09	PCMaticUpdater	/Applications/PCMaticMac.app/Contents/MacOS/PCMaticUpdater.app/Contents/MacOS/PC...
17:27:32	CoreServicesUIAgent	/System/Library/CoreServices/CoreServicesUIAgent.app/Contents/MacOS/CoreServicesUIA...
17:27:32	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:32	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:32	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:32	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:28	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:28	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:27:27	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:55	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:47	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:47	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:47	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:46	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:46	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:46	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:26:42	pluginkit	/usr/bin/pluginkit
17:26:42	pluginkit	/usr/bin/pluginkit
17:25:39	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:25:38	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:25:38	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:25:38	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:23:58	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:23:45	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:22:17	mdworker	/System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.fra...
17:21:35	fontworker	/System/Library/Frameworks/ApplicationServices.framework/Versions/A/Frameworks/ATS.fr...
17:21:35	fontd	/System/Library/Frameworks/ApplicationServices.framework/Versions/A/Frameworks/ATS.fr...
17:21:35	PCMaticUpdater	/Applications/PCMaticMac.app/Contents/MacOS/PCMaticUpdater.app/Contents/MacOS/PC...
17:18:06	PCMaticUpdater	/Applications/PCMaticMac.app/Contents/MacOS/PCMaticUpdater.app/Contents/MacOS/PC...

- **Web Portal** - The web portal option will open up a browser session to the PC Matic management console. The first time you open the Web Portal you will need to login with your PC Matic account information.
- **Check for Updates** - PC Matic for Mac automatically looks for updates for our software and applies them. However you can manually check for updates to ensure you are on the latest version.
- **Settings** - Inside settings you will have your main SuperShield Options. Here you can change the protection mode for SuperShield between whitelist mode (default) and blacklist mode. You can also adjust the notification setting for PC Matic to show display messages about blocked applications or allow for Prompt for Override and locally allow or block an unknown application. Prompt for Override should only be used by expert users.
  - **Display** - The default notification setting is to have Display turned on. Display will simply show a standard Mac notification when SuperShield blocks and application on your device. No action can be taken from this notification.
  - **Prompt** - With prompt turned on, a large window will pop up on your device when SuperShield is going to block an application. Inside this window, you can select to block or allow the application once or always. This will locally whitelist or blacklist the application on your device.
  - **Blacklist** - The current default for SuperShield while our whitelist mode is beta testing. Blacklist mode protects your Mac using a blacklist of known bad applications.
  - **Whitelist** - The whitelist mode protects your Mac using a global whitelist of known good software and blocks all bad and unknown applications by default.
- Troubleshooting/Help - Quick links to our customer support team and product resources will reside here. This is also where the product can be uninstalled, however, you must login with your PC Matic account credentials to confirm the uninstall.

Web Portal

All Mac devices will be located in the same management portal user interface you're familiar with for Windows devices and servers. You will see Mac device information integrated into several reports, alerts, alert notifications, device lists, scheduled scans, blocked status, local whitelisting, and more. When drilled down to and individual Mac device, there are several actions you can take and realtime information you will receive.



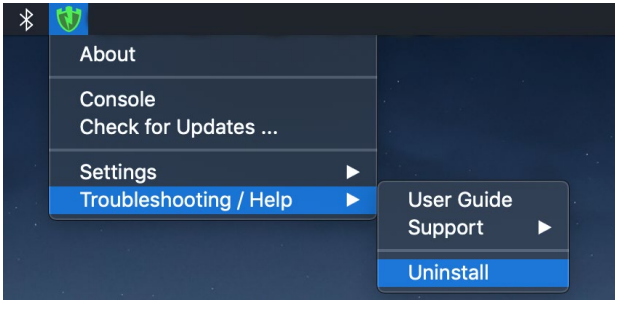
- **Performance Gauges** - At the top of the web portal you will see several performance gauges, these give you a real time idea of the current performance on your Mac. In all cases, the higher the percentage, the harder your Mac is currently working and thus may be running slower.
- **Connection Icons -** On the upper right hand side of the portal, you will find several connection icons. The person icon signfies if you are currently connected to the internet. The computer icon signifies if the device you are currently viewing is connected to the internet. The last icon, for SuperShield, will show if your device is currently secured
- **Scans -** From the Actions list you can adjust Scan settings or review the most recent test. Scan Now allows you to set up and run an immediate manual scan on a device that's online. Next Test will allow you to schedule a scan for your Mac on a daily, weekly or monthly basis. Last Test will open the report for the most recent scan that ran on your Mac to review any findings.
- **Quarantine Files** - The Quarantine Files section will contain any KNOWN BAD files that PC Matic has removed from your Mac. These files are known to be malware and have been cleaned from your machine. If you suspect any file has been mistakenly removed, please contact our support team for assistance.
- **SuperShield Report** - The SuperShield report will mirror the Console that you can review on your device from the Status Bar icon. This report shows every application that SuperShield is monitoring on your device and will also show any that have been blocked. Here you can locally whitelist an application for your mac devices by clicking the green button on the right side.

- **Scan History** - All scans and cleans that have been run on your Mac will display here to review the results and see any changes that were made.
- Live Scan Status - While a scan is running you will see a small 'eye' appear above the computer's connection icon in the web portal. When a scan finishes this eye will dissapear and you can then review the result inside the Test History tab.

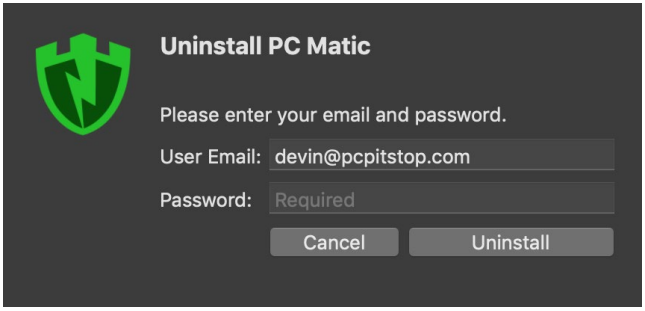
Uninstalling PC Matic Mac

You can uninstall PC Matic either through the Status Bar icon, or using the Uninstall tool that comes inside the InstallPCMatic.dmg. In order to complete the uninstall process, you will need your Administrator password. This is the same password we used to install PC Matic and most likely the password you use to login to your Mac every day. We'll begin with the easiest path using the SuperShield icon in your Status Bar following the steps below.

1. Navigate to the SuperShield icon in your Mac's Status Bar.
2. Select the icon and hover over Troubleshooting/Help at the bottom.
3. Select Uninstall from the list.



4. In order to uninstall you must confirm your PC Matic account details.
5. Once you enter your PC Matic account information and click Uninstall, the process will begin in the background.



6. You may be prompted for your Mac Administrator password, once you're done typing the password press enter.
7. The uninstall process will complete in the background and once done you will no longer see the SuperShield icon in the Status Bar.
8. Reboot your Mac to finish the full uninstall.

Settings

By clicking the SuperShield icon in your Status Bar, a menu will appear with several different options and resources. Settings allows you to change options for SuperShield on your device.

Notifications

- Display - The default notification setting is to have Display turned on. Display will simply show a standard Mac notification when SuperShield blocks and application on your device. No action can be taken from this notification.
- Prompt - With prompt turned on, a large window will pop up on your device when SuperShield is going to block an application. Inside this window, you can select to block or allow the application once or always. This will locally whitelist or blacklist the application on your device.

Protection Mode

- Blacklist - The current default for SuperShield while our whitelist mode is beta testing. Blacklist mode protects your Mac using a blacklist of known bad applications.
- Whitelist - Currently in testing, the whitelist mode protects your Mac using a global whitelist of known good software and blocks all bad and unknown applications by default.

Support

In the future, our normal customer support process can be used.

To get support from our team, you can click the Support button, which will always be in the upper right hand corner of your dashboard. From here you can visit the forums, view the user guide, and choose get support now to contact our team. You can also go directly to pcmatic.com/help and fill out a ticket to contact our team.

Our support team will always reply within 24 hours but typically during business hours will reply very quickly. Immediately after your ticket has been submitted you should see a confirmation from csticket@pcmatic.com. If this message does not appear in your inbox, check your junk or spam folders and be sure to whitelist the email csticket@pcmatic.com with your email client so you receive future communication.

Troubleshooting

No Activity Shown In Console

If there is no activity when you're looking at the console for PC Matic Mac, it's possible the protection is not running. This can be fixed by making sure you're logged in correctly, but if you are already logged in, try following the steps below to enable the System Extension again.

1. Open Application > Utilities > Terminal and run the following command:
   - sudo kextload /Library/Extensions/PCMaticListener.kext
2. After you run the command you'll see an error appear in terminal. That is normal.
3. Now open System Preferences > Security & Privacy and you should see the "Allow" prompt for the PC Matic System Extension again. Click the Allow button to allow loading the PC Matic Mac extension.
4. You MUST then re-boot system.
5. After rebooting you should see activity in the Console again.