SQWARQ

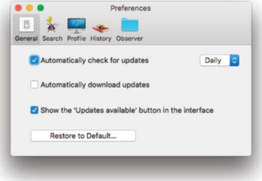
Welcome to DetectX Swift

Search and Rescue for your Mac

Quick Start

Welcome to DetectX Swift

Preferences

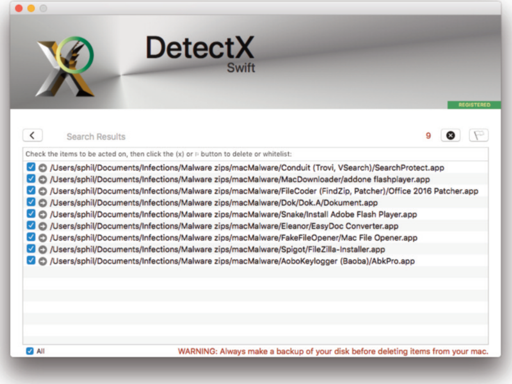


☑ Automatically check for updates — Daily

□ Automatically download updates

☑ Show the 'Updates available' button in the interface

Search

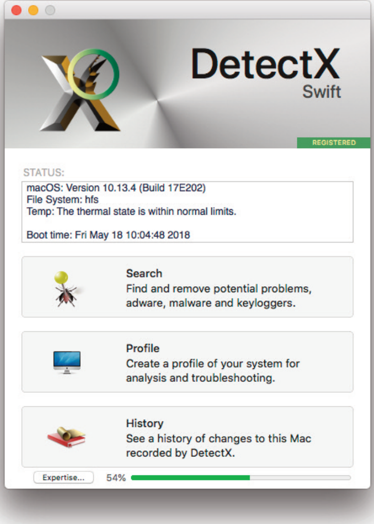


Check the items to be acted on, then click the (x) or ⚐ button to delete or whitelist:

- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/Conduit (Trovi, VSearch)/SearchProtect.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/MacDownloader/addone flashplayer.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/FileCoder (FindZip, Patcher)/Office 2016 Patcher.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/Dok/Dok.A/Dokument.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/Snake/Install Adobe Flash Player.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/Eleanor/EasyDoc Converter.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/FakeFileOpener/Mac File Opener.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/Spigot/FileZilla-Installer.app
- ☑ /Users/sphil/Documents/Infections/Malware zips/macMalware/AoboKeylogger (Baoba)/AbkPro.app

☑ All

WARNING: Always make a backup of your disk before deleting items from your mac.



STATUS:

macOS: Version 10.13.4 (Build 17E202)
File System: hfs
Temp: The thermal state is within normal limits.

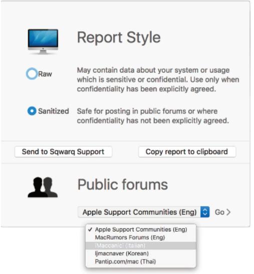
Boot time: Fri May 18 10:04:48 2018

Search
Find and remove potential problems, adware, malware and keyloggers.

Profile
Create a profile of your system for analysis and troubleshooting.

History
See a history of changes to this Mac recorded by DetectX.

Profile



Report Style

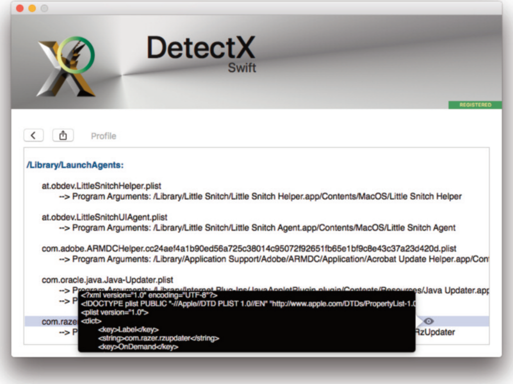
○ Raw — May contain data about your system or usage which is sensitive or confidential. Use only when confidentiality has been explicitly agreed.

● Sanitized — Safe for posting in public forums or where confidentiality has not been explicitly agreed.

Public forums

Apple Support Communities (Eng)

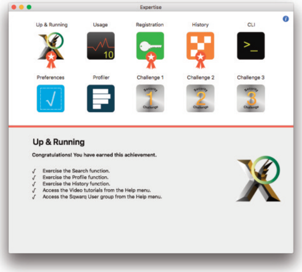
✓ Apple Support Communities (Eng)
MacRumors Forums (Eng)
iMaccanici (Italian)
Ijmacnaver (Korean)
Pantip.com/mac (Thai)



```
/Library/LaunchAgents:

    at.obdev.LittleSnitchHelper.plist
        --> Program Arguments: /Library/Little Snitch/Little Snitch Helper.app/Contents/MacOS/Little Snitch Helper

    at.obdev.LittleSnitchUIAgent.plist
        --> Program Arguments: /Library/Little Snitch/Little Snitch Agent.app/Contents/MacOS/Little Snitch Agent

    com.adobe.ARMDCHelper.cc24aef4a1b90ed56a725c38014c95072f92651fb65e1bf9c8e43c37a23d420d.plist
        --> Program Arguments: /Library/Application Support/Adobe/ARMDC/Application/Acrobat Update Helper.app/Con

    com.oracle.java.Java-Updater.plist
        --> Program Arguments: /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app
        --> P

    com.raze
        --> P                                                                                       RzUpdater
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>com.razer.rzupdater</string>
        <key>OnDemand</key>
```

Achievements

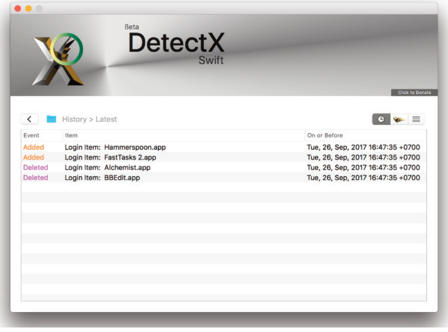


Up & Running

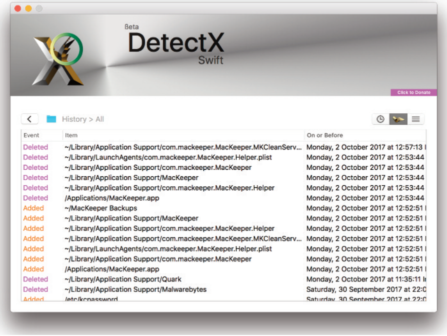
Congratulations! You have earned this achievement.

- ✓ Exercise the Search function.
- ✓ Exercise the Profile function.
- ✓ Exercise the History function.
- ✓ Access the Video tutorials from the Help menu.
- ✓ Access the Sqwarq User group from the Help menu.

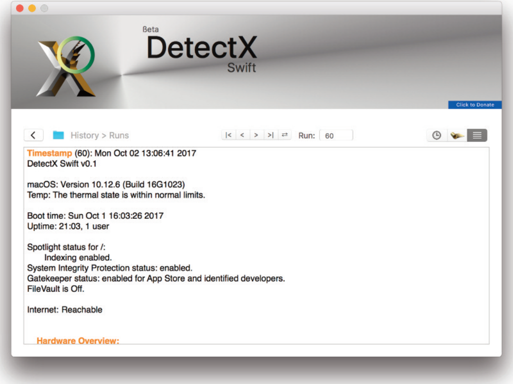
History



Event	Item	On or Before
Added	Login Item: Hammerspoon.app	Tue, 26, Sep, 2017 16:47:35 +0700
Added	Login Item: FastTasks 2.app	Tue, 26, Sep, 2017 16:47:35 +0700
Deleted	Login Item: Alchemist.app	Tue, 26, Sep, 2017 16:47:35 +0700
Deleted	Login Item: BBEdit.app	Tue, 26, Sep, 2017 16:47:35 +0700



Event	Item	On or Before
Deleted	~/Library/Application Support/com.mackeeper.MacKeeper.MKCleanServ...	Monday, 2 October 2017 at 12:57:13 I
Deleted	~/Library/LaunchAgents/com.mackeeper.MacKeeper.Helper.plist	Monday, 2 October 2017 at 12:53:44
Deleted	~/Library/Application Support/com.mackeeper.MacKeeper	Monday, 2 October 2017 at 12:53:44
Deleted	~/Library/Application Support/MacKeeper	Monday, 2 October 2017 at 12:53:44
Deleted	~/Library/Application Support/com.mackeeper.MacKeeper.Helper	Monday, 2 October 2017 at 12:53:44
Deleted	/Applications/MacKeeper.app	Monday, 2 October 2017 at 12:53:44
Added	~/MacKeeper Backups	Monday, 2 October 2017 at 12:52:51 I
Added	~/Library/Application Support/MacKeeper	Monday, 2 October 2017 at 12:52:51 I
Added	~/Library/Application Support/com.mackeeper.MacKeeper.Helper	Monday, 2 October 2017 at 12:52:51 I
Added	~/Library/Application Support/com.mackeeper.MacKeeper.MKCleanServ...	Monday, 2 October 2017 at 12:52:51 I
Added	~/Library/LaunchAgents/com.mackeeper.MacKeeper.Helper.plist	Monday, 2 October 2017 at 12:52:51 I
Added	~/Library/Application Support/com.mackeeper.MacKeeper	Monday, 2 October 2017 at 12:52:51 I
Added	/Applications/MacKeeper.app	Monday, 2 October 2017 at 12:52:51 I
Deleted	~/Library/Application Support/Quark	Monday, 2 October 2017 at 11:35:11 I
Deleted	~/Library/Application Support/Malwarebytes	Saturday, 30 September 2017 at 22:0
Added	/etc/kcpassword	Saturday, 30 September 2017 at 22:0



```
Timestamp (60): Mon Oct 02 13:06:41 2017
DetectX Swift v0.1

macOS: Version 10.12.6 (Build 16G1023)
Temp: The thermal state is within normal limits.

Boot time: Sun Oct 1 16:03:26 2017
Uptime: 21:03, 1 user

Spotlight status for /:
      Indexing enabled.
System Integrity Protection status: enabled.
Gatekeeper status: enabled for App Store and identified developers.
FileVault is Off.

Internet: Reachable


   Hardware Overview:
```

LICENSE AGREEMENT

1. Terms of Use
The user (hereafter “you”) is granted the non-exclusive right to use the software program, ‘DetectX Swift’ (herein ‘the software”) only in case you agree in full with the terms and conditions set out below in this License Agreement. If you do not so agree, you are not licensed to use the software. Beta versions of the software are indicated by the word ‘Beta’ or equivalent representation in the main user interface, above the ‘DetectX Swift’ label and/or by a version number beginning with ‘0’ (for example, v0.1 would be a Beta version, whereas v1.0 would be a Release version). Beta versions of DetectX Swift may be used without payment for both personal and institutional/commercial-like use. **Release versions may be used without payment for personal home use only**. An optional Home use registration key is available for users wishing to support development of the program. **Institutional, organisational and commercial or commercial-like use of Release versions requires the purchase of a DetectX Swift Pro or DetectX Swift Management License.** Please contact support@sqwarq.com for details.

2. Copyright
The software is owned by Philip A. Stokes and is protected by copyright laws and international treaty provisions.

3. Restrictions
You may not modify, reverse-engineer, decompile or disassemble the software.
You may not claim that the software is yours, and you may not use the names ‘DetectX Swift’ or ‘Sqwarq’ or the name Philip A. Stokes to endorse or promote services or other products related to the software or use of the software without prior written permission.

4. Disclaimer of Warranties and Limitation of Liability
THE SOFTWARE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND. PHILIP A. STOKES DISCLAIMS ANY IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU. SHOULD THE SOFTWARE PROVE DEFECTIVE, YOU (AND NOT PHILIP A. STOKES) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING OR REPAIR.

IN NO EVENT SHALL PHILIP A. STOKES OR ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, MARKETING, DISTRIBUTION, OR DELIVERY OF THE SOFTWARE, BE LIABLE FOR ANY DAMAGES WHATSOEVER; INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, FOR BUSINESS INTERRUPTION, FOR LOSS OF BUSINESS INFORMATION, OR FOR OTHER MONETARY LOSS, ARISING OUT OF THE USE OF THE SOFTWARE OR THE INABILITY TO USE THE SOFTWARE, EVEN IF YOU HAVE BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO EVENT SHALL PHILIP A. STOKES BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR FOR ANY DAMAGES WHATSOEVER, WHETHER IN A CONTRACT ACTION, NEGLIGENCE OR OTHER TORT ACTION, OR OTHER CLAIM OR ACTION, ARISING OUT OF, OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THE SOFTWARE OR DOCUMENTS AND OTHER INFORMATION PROVIDED TO YOU BY PHILIP A. STOKES, OR IN THE PROVISION OF, OR FAILURE TO PROVIDE, SERVICES OR INFORMATION.

5. Notification of Changes to this Agreement
Any or all of the above conditions may change without notice.

COPYRIGHT NOTICE. Copyright 2017 by Philip A. Stokes. All rights reserved. Any rights not expressly granted in this License Agreement are reserved.

Credits & Acknowledgements

Software Design & Engineering: Philip Stokes
Application, Search and History icons: Armin Redinger
Preferences and Advanced images in this User Guide: Armin Redinger
NSComputer icon for iMac: Copyright 2014 Apple Inc.

DetectX Swift contains code licensed from the following:
Sparkle Framework Copyright 2006 Andy Matuschak
CocoaFob Copyright 2015 PixelEspresso/Gleb Dolgich

While all bugs, errors and faults in DetectX Swift are entirely the responsibility of the programmer, DetectX Swift would not have been possible without valuable input from a number of others, all of whom have generously given their time and advice. Many thanks to you all.

Document Revision History

Published on 8th November, 2017.
Revised on 18th January 2018. -> Corrections
Revised on 25th January 2018. -> Version changes 1.02
Revised on 12th February 2018. -> Version changes 1.03
Revised on 13th February 2018. -> Version changes 1.03
Revised on 18th May 2018. -> Version changes 1.070

Overview

Why and when to use DetectX Swift, What happens when DetectX Swift launches, License Agreement, Credits & acknowledgements.

Read more

Search

Search your mac for security threats and performance issues such as adware, malware, keyloggers and potentially unsafe or unwanted software.

Read more

Profile

Examine your mac's current state, unravel the cause of new or unexpected performance problems, and share your profile with experts for further help.

Read more

History

Review the history of changes recorded by DetectX, examine and compare earlier profiles with the current state of the mac.

Read more

Preferences

Reset DetectX to default settings, reset the whitelist, delete history and runs, enable or disable the Folder Observer function.

Read more

Advanced

Achievements, AppleScript, Command Line Tool, Folder Observer Options, Network Administration.

Read more

Appendix

System requirements, Installing, Uninstalling, What does DetectX detect?

Read more

Index

Go

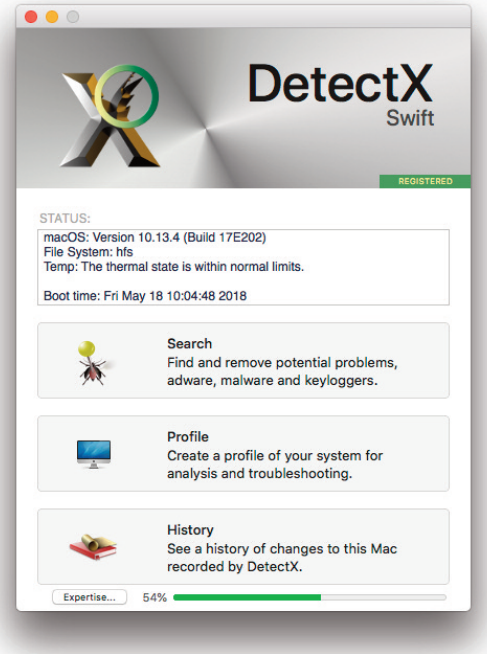
Why and when to use DetectX

Our macs are great, and out of the box they perform just as Apple designed them to.

However, as we start to use our macs to accomplish our needs, we add software to them that was not designed and tested by Apple.

Sometimes, we add software to our macs unknowingly, as a consequence of some other action we took.

And sometimes, one or more of these additions causes our macs to behave in ways that we neither want nor welcome.



STATUS:

macOS: Version 10.13.4 (Build 17E202)
File System: hfs
Temp: The thermal state is within normal limits.

Boot time: Fri May 18 10:04:48 2018

Search
Find and remove potential problems, adware, malware and keyloggers.

Profile
Create a profile of your system for analysis and troubleshooting.

History
See a history of changes to this Mac recorded by DetectX.

When this occurs, DetectX Swift's job is to help you, ourselves (if you should choose to contact us for help), or any other technical adviser you consult, to determine what happened to your mac and to fix it.

However, you should not wait for trouble to start before using DetectX Swift. DetectX Swift's troubleshooting capabilities are enhanced by the history of changes that it records over time, so running DetectX Swift on a regular basis - at least once a week - is good troubleshooting practice.

DetectX can identify and remove malware

DetectX Swift is both a security tool and an analytical tool. It contains a rich set of features to help remedy problems including:

- browsers being redirected to sites you did not intend to visit
- loss of data due to privacy invasions by malware
- slow response times (typically indicated by the spinning color wheel)
- sudden application or system crashes

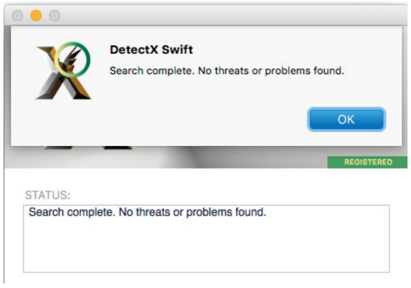
In order to help identify the cause of such problems, DetectX has three main functions, which correspond to its three main views, Search, Profile and History, accessible through the main interface or the menu bar. Subsequent sections of this guide will cover those in detail.

IMPORTANT: Please read the Licensing Agreement before using DetectX Swift.

What happens when DetectX Swift launches

On launch, DetectX Swift first runs the Search function and then the Profile function before returning control to the user.

In the event that DetectX Swift recognises an issue, the user is presented with the Search results table. Otherwise, a dialog sheet appears informing the user that no threats or issues were found (Fig.1).


DetectX Swift

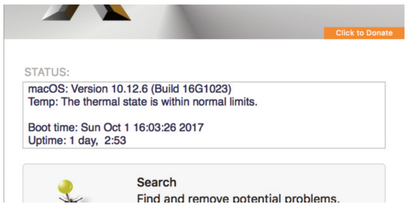
Search complete. No threats or problems found.

STATUS:

Search complete. No threats or problems found.

Fig. 1

The Status field reflects the results of the preceding action (Fig. 2). Initially, the Status information will use a dark text color. After certain events or a certain time period, the text may change to a lighter shade to indicate that the information is stale and may not represent the current status.


STATUS:

macOS: Version 10.12.6 (Build 16G1023)
Temp: The thermal state is within normal limits.

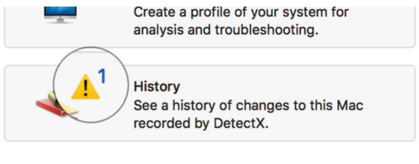
Boot time: Sun Oct 1 16:03:26 2017
Uptime: 1 day, 2:53

Search
Find and remove potential problems.

Fig. 2

The information in the Status field can be refreshed by exercising any of DetectX Swift's main functions.

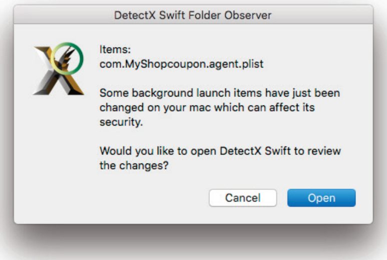
After launching DetectX Swift, you will often see a small yellow triangle with a number adjacent to it (Fig. 3). This indicates that the displayed number of changes have occurred since the last run. You can review the changes by clicking the History button. See the History section for more details.


Create a profile of your system for analysis and troubleshooting.

History
See a history of changes to this Mac recorded by DetectX.

Fig. 3

Occasionally, you may be presented with a dialog box from DetectX Swift even when it is not running (Fig. 4). This is the Folder Observer function (see the Advanced section for more details). The function can be controlled in the application's Preferences.


DetectX Swift Folder Observer

Items:
com.MyShopcoupon.agent.plist

Some background launch items have just been changed on your mac which can affect its security.

Would you like to open DetectX Swift to review the changes?

Fig. 4

SEARCH

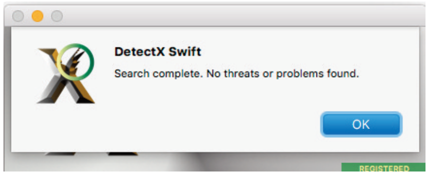
The Search function will search your mac for known threats at the following times:

i. When you launch the app
ii. After deleting any item found in a search
iii. When you manually click the ‘Search’ button in the main interface
iv. After resetting the whitelist in the Preferences panel

There are three possible results from running a search:

I. Nothing is Found

Click the ‘OK’ button to dismiss the dialog and continue using the program.



DetectX Swift

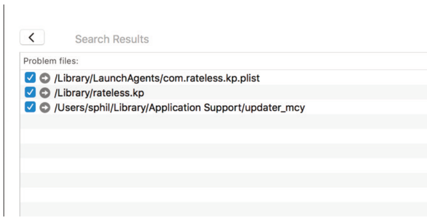
Search complete. No threats or problems found.

II. The Results Table is Populated

Use the checkboxes ☑ to select or deselect items.

Delete ⊗ or whitelist ⚐ your selected items.

Reveal an item in the Finder ➔



Search Results

Problem files:

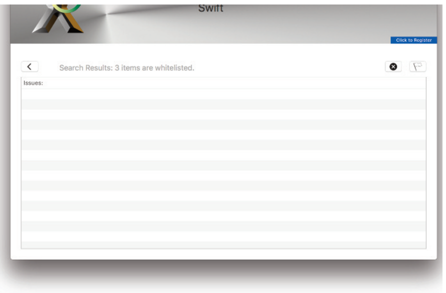
☑ ➔ /Library/LaunchAgents/com.rateless.kp.plist
☑ ➔ /Library/rateless.kp
☑ ➔ /Users/sphil/Library/Application Support/updater_mcy

III. The Results Table is Empty

You have previously whitelisted all the items found in the search.

Click the < button to return to the main interface.

Open the Preferences panel to view, reset or report the whitelisted items.



Search Results: 3 items are whitelisted.

Issues:

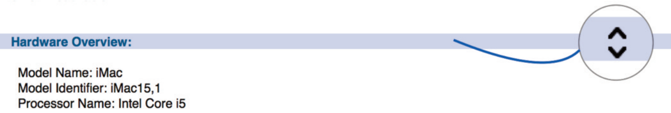
The Profile function is run at the following times:

i. When you launch the app
ii. Whenever you delete an item in the Search results
iii. When you manually click the ‘Profile’ button in the main interface
iv. When you manually click the ‘Refresh’ button in the Profile view

The Profile function creates a snapshot of your mac and saves it in DetectX Swift’s History view. However, viewing the snapshot in the Profile view allows you to investigate the snapshot dynamically in a number of ways. Watch the 1-minute video

When you move the cursor inside the view, you will notice the dynamic highlighting, which reveals different buttons depending on what line the cursor hovers over.

Navigation button

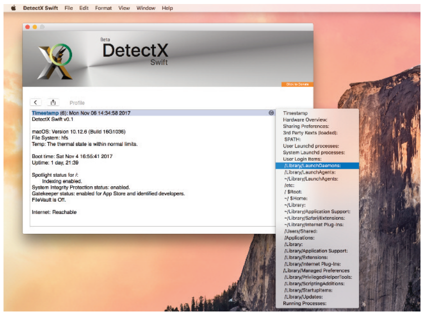


```
Hardware Overview:

Model Name: iMac
Model Identifier: iMac15,1
Processor Name: Intel Core i5
```

The Navigation button appears on any line that contains a section heading (indicated by **bolded, blue text**).

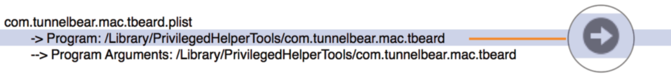
Clicking it reveals the navigation menu (shown opposite).

Clicking an item in the menu jumps the Profile view to that section.



```
Timestamp (6): Mon Nov 06 14:34:58 2017
DetectX Swift v0.1

macOS: Version 10.12.6 (Build 16G1036)
File System: hfs
Temp: The thermal state is within normal limits.

Boot time: Sat Nov 4 16:55:41 2017
Uptime: 1 day, 21:39

Spotlight status for /:
    Indexing enabled.
System Integrity Protection status: enabled.
Gatekeeper status: enabled for App Store and identified developers.
FileVault is Off.

Internet: Reachable
```

Open button



```
com.tunnelbear.mac.tbeard.plist
    -> Program: /Library/PrivilegedHelperTools/com.tunnelbear.mac.tbeard
    --> Program Arguments: /Library/PrivilegedHelperTools/com.tunnelbear.mac.tbeard
```

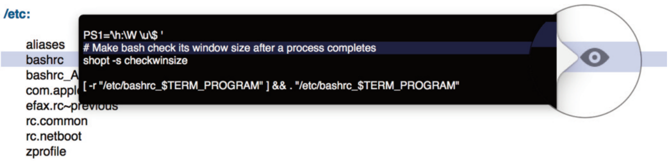
The Open button appears on any line that contains:	Clicking it:
A complete filepath that exists* A plist program argument that exists A folder that has child items	reveals the item in the Finder
The **User Login Items** section The **Sharing Preferences** section	launches System Preferences and opens the appropriate pane

**except items listed under ‘Running Processes’*

Quick Look button

The Quick Look button appears on any line that shows

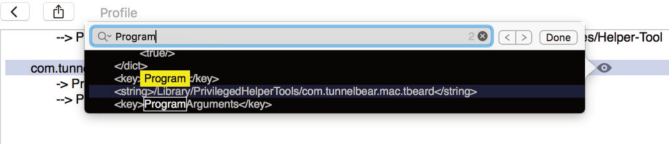
1. *.plist, .sh, .bashrc, .py, .lua extension, or is a crontab, rc.*, bash_profile, bash_history, zprofile or zshrc file.*



```
/etc:

aliases
bashrc
bashrc_A
com.appl
efax.rc~previous
rc.common
rc.netboot
zprofile
```

```
PS1='\h:\W \u\$ '
# Make bash check its window size after a process completes
shopt -s checkwinsize

[ -r "/etc/bashrc_$TERM_PROGRAM" ] && . "/etc/bashrc_$TERM_PROGRAM"
```

Clicking the button reveals the file's contents. You can search, select and copy directly from the Quick Look view.

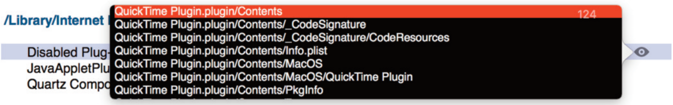


```
--> P                                                          s/Helper-Tool
com.tunn
 -> Pr
--> P
```

```
        <true/>
    </dict>
    <key>Program</key>
    <string>/Library/PrivilegedHelperTools/com.tunnelbear.mac.tbeard</string>
    <key>ProgramArguments</key>
```

2. *a folder item containing children.*

Clicking the button shows a recursive list of the folder's contents, including all subfolders, along with a file count in the top left corner.



```
/Library/Internet

Disabled Plug-
JavaAppletPlu
Quartz Compo
```

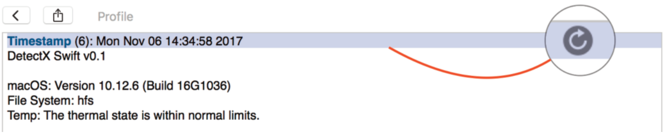
```
QuickTime Plugin.plugin/Contents                                124
QuickTime Plugin.plugin/Contents/_CodeSignature
QuickTime Plugin.plugin/Contents/_CodeSignature/CodeResources
QuickTime Plugin.plugin/Contents/Info.plist
QuickTime Plugin.plugin/Contents/MacOS
QuickTime Plugin.plugin/Contents/MacOS/QuickTime Plugin
QuickTime Plugin.plugin/Contents/PkgInfo
```

The Quick Look function is limited to displaying 10,000 items.

Refresh button

The Refresh button only appears on the top line of the Profile view.

Clicking it causes the Profile function to run.

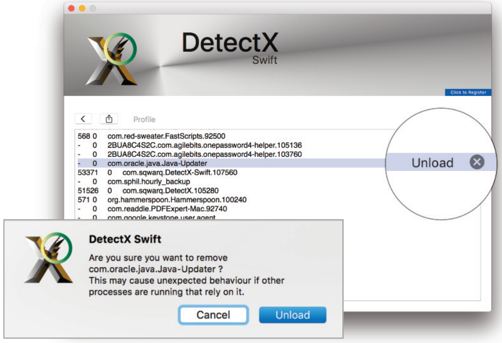


```
Timestamp (6): Mon Nov 06 14:34:58 2017
DetectX Swift v0.1

macOS: Version 10.12.6 (Build 16G1036)
File System: hfs
Temp: The thermal state is within normal limits.
```

Unload Process button

The Unload Process button appears in the **User** & **System Launchd Processes** sections for non-essential processes.

Clicking it offers the user the option to remove the process from launchctl.



```
568 0     com.red-sweater.FastScripts.92500
-     0   2BUA8C4S2C.com.agilebits.onepassword4-helper.105136
-     0   2BUA8C4S2C.com.agilebits.onepassword4-helper.103760
-     0   com.oracle.java.Java-Updater
53371     0     com.sqwarq.DetectX-Swift.107560
-     0   com.sphil.hourly_backup
51526     0     com.sqwarq.DetectX.105280
571 0     org.hammerspoon.Hammerspoon.100240
-     0   com.readdle.PDFExpert-Mac.92740
-     0   com.google.keystone.user.agent
```

DetectX Swift

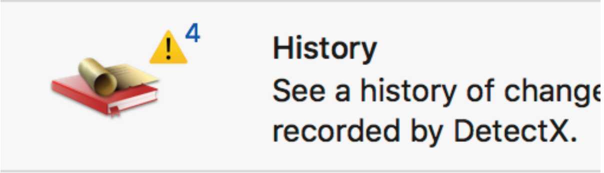
Are you sure you want to remove com.oracle.java.Java-Updater ?
This may cause unexpected behaviour if other processes are running that rely on it.

The History view appears when you click the History button in the main interface.

i. The RECENT HISTORY view show changes since DetectX Swift last ran
ii. The ALL HISTORY view shows all History ever recorded by DetectX Swift
iii. The RUNS view allows you to inspect individual runs and to run a diff on any selected run and the most recent run.

CHANGES INDICATOR

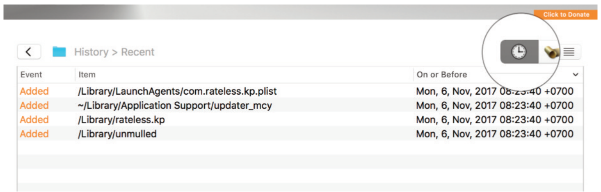
After launching DetectX Swift, running a search or profile, you will often see a small yellow triangle with a number adjacent to it.



This indicates that the displayed number of changes have occurred since DetectX's last run. You can review the changes by clicking the History button.

RECENT HISTORY

Click the first button on the tab-switcher.



Event	Item	On or Before
Added	/Library/LaunchAgents/com.rateless.kp.plist	Mon, 6, Nov, 2017 08:23:40 +0700
Added	~/Library/Application Support/updater_mcy	Mon, 6, Nov, 2017 08:23:40 +0700
Added	/Library/rateless.kp	Mon, 6, Nov, 2017 08:23:40 +0700
Added	/Library/unmulled	Mon, 6, Nov, 2017 08:23:40 +0700

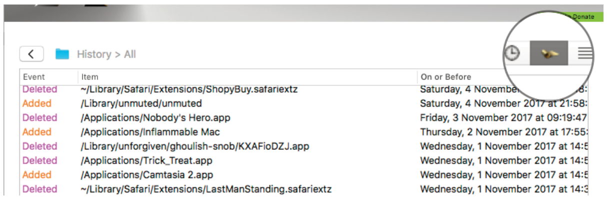
This view show changes since launch.

Double-click an item to reveal it in the Finder (if it exists).

Control-click on the table to copy the data to the clipboard.

ALL HISTORY

Click the second button on the tab-switcher.



Event	Item	On or Before
Deleted	~/Library/Safari/Extensions/ShopyBuy.safariextz	Saturday, 4 Novembe [illegible] 8:
Added	/Library/unmuted/unmuted	Saturday, 4 November 2017 at 21:58:
Deleted	/Applications/Nobody's Hero.app	Friday, 3 November 2017 at 09:19:47
Added	/Applications/Inflammable Mac	Thursday, 2 November 2017 at 17:55:
Deleted	/Library/unforgiven/ghoulish-snob/KXAFioDZJ.app	Wednesday, 1 November 2017 at 14:5
Deleted	/Applications/Trick_Treat.app	Wednesday, 1 November 2017 at 14:5
Added	/Applications/Camtasia 2.app	Wednesday, 1 November 2017 at 14:5
Deleted	~/Library/Safari/Extensions/LastManStanding.safariextz	Wednesday, 1 November 2017 at 14:3

This view shows all changes recorded by DetectX Swift.

Double-click an item to reveal it in the Finder.

Control-click on the table to copy the data to the clipboard.

RUNS

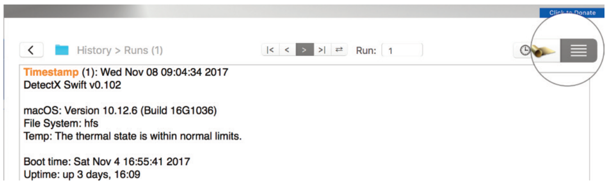
Click the third button on the tab-switcher.

This view allows you to search through individual runs recorded by DetectX Swift.

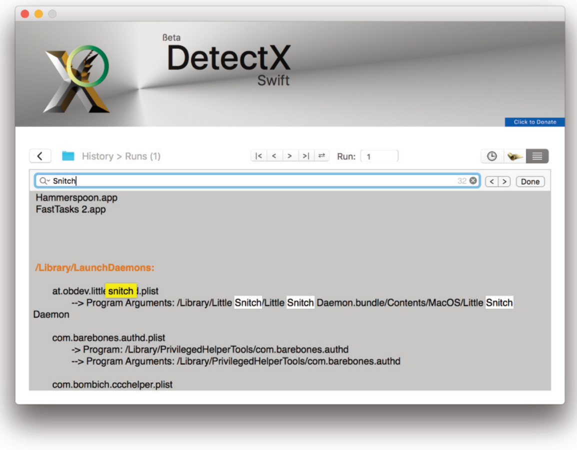
The centre console buttons allows you to move through the runs, or you can type a run number directly into the Run field.

Click inside the view and use ‘Command F’ to search the run currently in view.

Note that the Profile view’s dynamic highlighter is not available in the History Runs view.



```
Timestamp (1): Wed Nov 08 09:04:34 2017
DetectX Swift v0.102

macOS: Version 10.12.6 (Build 16G1036)
File System: hfs
Temp: The thermal state is within normal limits.

Boot time: Sat Nov 4 16:55:41 2017
Uptime: up 3 days, 16:09
```



```
Hammerspoon.app
FastTasks 2.app



/Library/LaunchDaemons:

     at.obdev.littlesnitchd.plist
          --> Program Arguments: /Library/Little Snitch/Little Snitch Daemon.bundle/Contents/MacOS/Little Snitch
Daemon

     com.barebones.authd.plist
          -> Program: /Library/PrivilegedHelperTools/com.barebones.authd
          --> Program Arguments: /Library/PrivilegedHelperTools/com.barebones.authd

     com.bombich.ccchelper.plist
```

DIFF

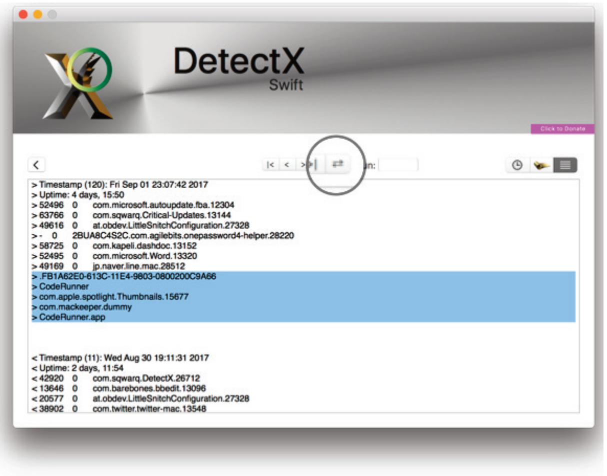
The right-most button on the centre console runs a *diff* or differences scan, comparing line by line the run currently in view with the most recent run.

The top section of the *diff* shows lines that are in the most recent run but which do not appear in the earlier run. These are marked by a **>**.

The lower section of the diff shows lines that are in the earlier run but which do not appear in the most recent run. These are marked by a **<**.

User and System Launchd processes may often appear in both, but with different PIDs.

The *diff* excludes the Running Processes section of the run, since these will likely all have different PIDs, the information would not be helpful.



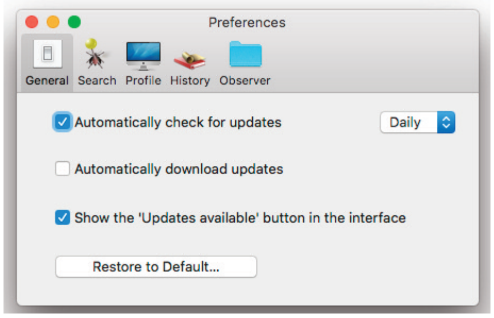
```
> Timestamp (120): Fri Sep 01 23:07:42 2017
> Uptime: 4 days, 15:50
> 52496   0     com.microsoft.autoupdate.fba.12304
> 63766   0     com.sqwarq.Critical-Updates.13144
> 49616   0     at.obdev.LittleSnitchConfiguration.27328
> -   0    2BUA8C4S2C.com.agilebits.onepassword4-helper.28220
> 58725   0     com.kapeli.dashdoc.13152
> 52495   0     com.microsoft.Word.13320
> 49169   0     jp.naver.line.mac.28512
> .FB1A62E0-613C-11E4-9803-0800200C9A66
> CodeRunner
> com.apple.spotlight.Thumbnails.15677
> com.mackeeper.dummy
> CodeRunner.app


< Timestamp (11): Wed Aug 30 19:11:31 2017
< Uptime: 2 days, 11:54
< 42920   0     com.sqwarq.DetectX.26712
< 13646   0     com.barebones.bbedit.13096
< 20577   0     at.obdev.LittleSnitchConfiguration.27328
< 38902   0     com.twitter.twitter-mac.13548
```

The **Preferences pane** opens when you choose the *Preferences* menu item from the application menu or when you use the keyboard shortcut `command ,`.

General

MANAGING UPDATES

Check `Automatically check for updates` and uncheck `Automatically download updates` if you want to be notified when updates are available and be given the option to manually download them. Set a period for the check (Hourly, Daily, Weekly, Monthly) as required. The default is `Daily`.



☑ Automatically check for updates Daily

□ Automatically download updates

☑ Show the 'Updates available' button in the interface

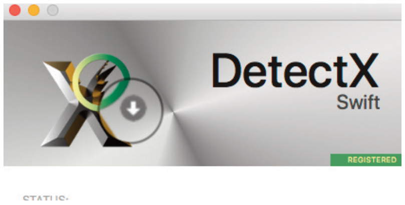
Uncheck BOTH boxes if you wish to manage updates entirely manually.

Check BOTH boxes and set a period (Hourly, Daily, Weekly, Monthly) if you wish DetectX Swift to check for and install updates silently without displaying an interface to the user.

When both options are checked, available updates are downloaded in the background and applied when the user quits the app.

Show the 'Updates Available' button in the interface

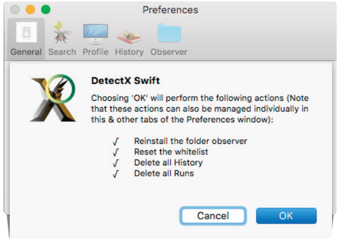
On by default, this preference alerts you when an update is available by presenting a button in the main interface. Clicking the button downloads the update.



Uncheck the preference if you do not want to see the update button in the interface.

Restore To default

Click the button to restore DetectX Swift to factory defaults. A confirmation dialog appears when you do this.



DetectX Swift

Choosing 'OK' will perform the following actions (Note that these actions can also be managed individually in this & other tabs of the Preferences window):

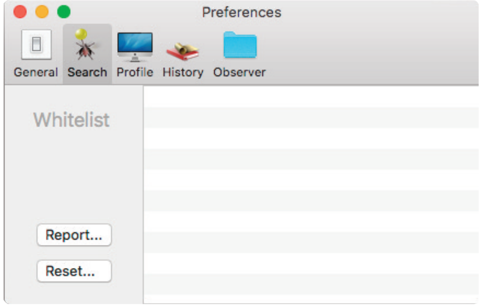
✓ Reinstall the folder observer
✓ Reset the whitelist
✓ Delete all History
✓ Delete all Runs

SEARCH

Currently, the Search preferences only control the Whitelist function.

Use the Report... button to report items to Sqwarq Support if you believe they are false positives.

Use the Reset... button to remove items previously whitelisted. This will result in a Search function starting and any of the (previously) whitelisted items found will be reported in the Search results.



PROFILE

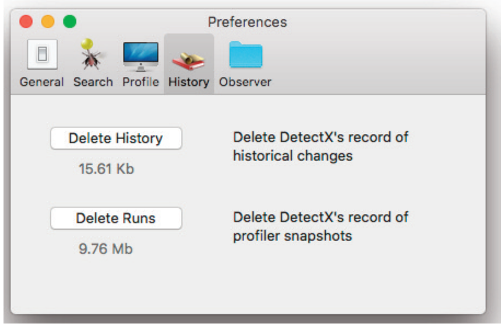
There are currently no preferences available for the Profile function. This will likely change in the future.

HISTORY

Click the Delete History button to remove DetectX Swift's record of changes to the mac.

Click the Delete Runs button to remove all the previous runs saved by DetectX Swift.

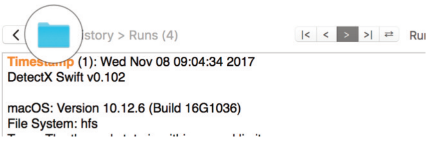
If you only wish to remove some runs to save space, you can delete individual run files manually from the Runs folder in the app's Application Support folder.



15.61 Kb — Delete DetectX's record of historical changes

9.76 Mb — Delete DetectX's record of profiler snapshots

You can access DetectX Swift's Application Support folder easily by clicking the blue folder icon in any of the History views.

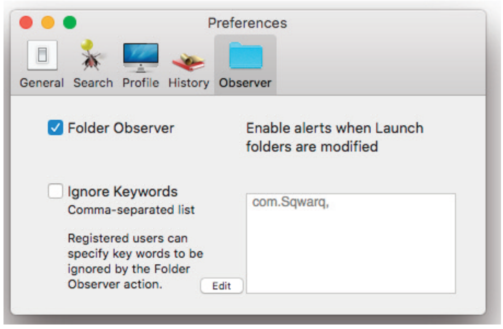


```
Timestamp (1): Wed Nov 08 09:04:34 2017
DetectX Swift v0.102

macOS: Version 10.12.6 (Build 16G1036)
File System: hfs
```

OBSERVER

Folder Observer

On by default, the Folder Observer alerts you when changes are made to any of your Launch folders even if DetectX Swift is not running.



☑ Folder Observer

Enable alerts when Launch folders are modified

□ Ignore Keywords

Comma-separated list

Registered users can specify key words to be ignored by the Folder Observer action.

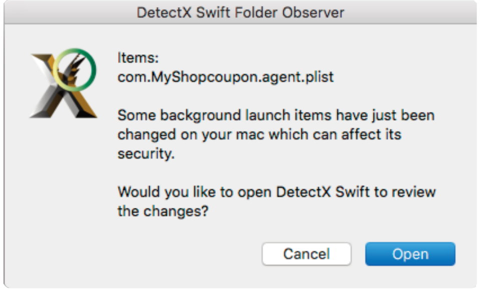
com.Sqwarq,

There are by default two launch folders in the local domain, /Library/LaunchDaemons and /Library/LaunchAgents. Property list files in these folders execute certain Apple and 3rd party programs when the Mac is powered on. Since these programs are run before the user logs in, they are a favourite place for malware, adware and other unwanted programs to place files in order to achieve persistence across reboots.

Additionally, each user on the mac may have a ~/Library/LaunchAgents folder which similarly runs programs when that user logs in but before the user takes control of the Desktop.

By enabling this preference, DetectX Swift can alert you when a program or application attempts to achieve persistence by placing an item in a Launch folder.

Uncheck the preference if you do not want these alerts.



Items:
com.MyShopcoupon.agent.plist

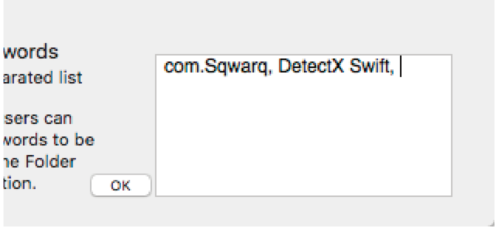
Some background launch items have just been changed on your mac which can affect its security.

Would you like to open DetectX Swift to review the changes?

Ignore Keywords

Registered users can specify key words to be ignored by the Folder observer action.

This allows you to stop the alert being thrown when items whose file name contains the key word is added or removed from one of the Launch folders.



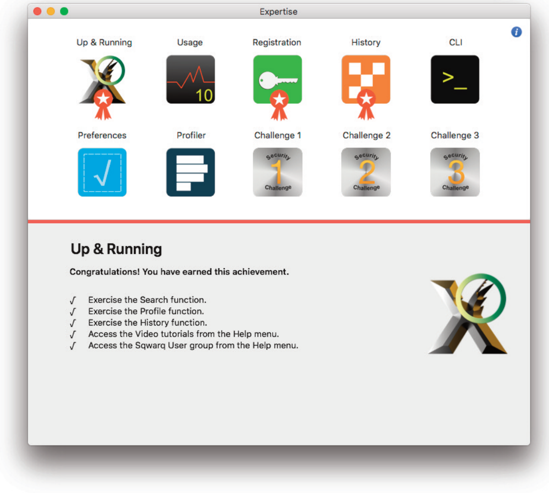
com.Sqwarq, DetectX Swift, |

Check the box, then click the 'Edit' button. Each contiguous key word or phrase should be comma-separated (*com.sqwarq, DetectX Swift,*).

Click the 'OK' button to finish editing.

Achievements

Achievements help you to learn more about macOS security and how to troubleshoot your Mac with DetectX Swift.



Up & Running

Congratulations! You have earned this achievement.

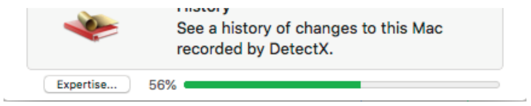
√ Exercise the Search function.
√ Exercise the Profile function.
√ Exercise the History function.
√ Access the Video tutorials from the Help menu.
√ Access the Sqwarq User group from the Help menu.

As you complete more tasks, your Expertise level increases.

You can access the Achievements pane by clicking the ‘Expertise’ button at the bottom of the main user interface.

There are at total of 10 Achievements, including three optional Security Challenges which will be made available in a forthcoming update.

Each Achievement has a number of tasks, and each Achievement contributes 10% of the Expertise score shown in the main interface.



See a history of changes to this Mac recorded by DetectX.

Completed tasks are marked with a √, and completed Achievements are marked with a rosette.

Notes

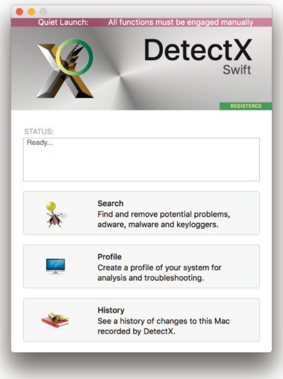
1. Some achievements and tasks are not available to unregistered users.
2. Achievements are only available if your Mac is on macOS 10.12 or higher.

APPLESCRIPT

You can control certain features of DetectX Swift via AppleScript.

As DetectX Swift by default executes a search and runs the Profile function on launch, you may wish to turn on QuietLaunch when scripting.

QuietLaunch can be turned on and off at the beginning and end of your AppleScript with a **do shell script** command:



Quiet Launch: All functions must be engaged manually

DetectX Swift

REGISTERED

STATUS:

Ready...

Search
Find and remove potential problems, adware, malware and keyloggers.

Profile
Create a profile of your system for analysis and troubleshooting.

History
See a history of changes to this Mac recorded by DetectX.

```
do shell script "defaults write com.sqwarq.DetectX-Swift QuietLaunch -boolean true"
tell application "DetectX Swift"

    -- scripting commands

end tell
do shell script "defaults write com.sqwarq.DetectX-Swift QuietLaunch -boolean false"
```

As the name suggests, when QuietLaunch is enabled, DetectX Swift will launch without running any operations.

With AppleScript, you can run a search and have the results returned to your script, run a diff on any two runs, and get information about the recorded history.

Several example scripts are provided in the ~/Library/Application Support/com.sqwarq.DetectX-Swift/Example Scripts/ support folder.

Note that you should copy these scripts and save them to another location if you intend to modify them for your own use, as DetectX Swift reserves the right to replace, update or add items to the Example Scripts folder and the scripts contained therein at a future time.

For more details about DetectX Swift's AppleScript support, consult the DetectX Swift Terminology Suite in your script editor's Dictionary viewer.

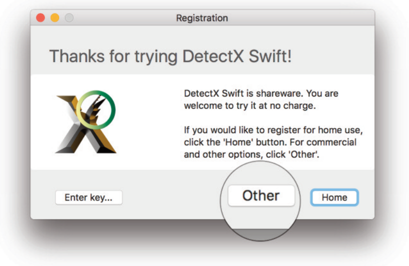
If you would like to see further elements of DetectX Swift exposed to AppleScript, please file an Enhancement Request at support@sqwarq.com.

Command Line Tool

DetectX Swift comes with the ability to run searches from the command line. This feature is enabled only for the first 20 days after install and 20 days after applying a Home use registration key.

Unlimited access to the command line tool requires a **Pro** or **Management** license. For *Home* registration and unregistered users, this feature is enabled only for the first 20 days after install and 20 days after applying a *Home* use registration key.

Pro and **Management** licenses can be purchased via the ‘Other’ button in the Registration window, or by contacting Sqwarq support directly.



Thanks for trying DetectX Swift!

DetectX Swift is shareware. You are welcome to try it at no charge.

If you would like to register for home use, click the 'Home' button. For commercial and other options, click 'Other'.

Basic Search

To use the CLI search, specify the full path to the app executable. For example, if the app is in /Applications folder, execute this on the command line:

```
/Applications/DetectX\ Swift.app/Contents/MacOS/DetectX\ Swift search
```

Alternatively, `cd` into the MacOS folder first with

```
cd '/Applications/DetectX Swift.app/Contents/MacOS'
```

then execute

```
./DetectX\ Swift search
```

This command searches both the computer and the current user’s home directory.

Search Other Users

Probably the most important benefit of searching from the command line is the ability to search all, or selected, other users. Search all users by using sudo and the -a option:

```
sudo <path to detectx executable> search -a
```

To restrict the search to one or more users, the -u option accepts a list of shortuser names (comma-delimited):

```
sudo <path to detectx executable> search -u alice,bob
```

Verbose Output

For more verbose output, including how long the search took, try either the vsearch or vvvv commands, which give increasingly more detail:

```
sudo <path to detectx executable> vsearch -a
```

```
sudo <path to detectx executable> vvvv -a
```

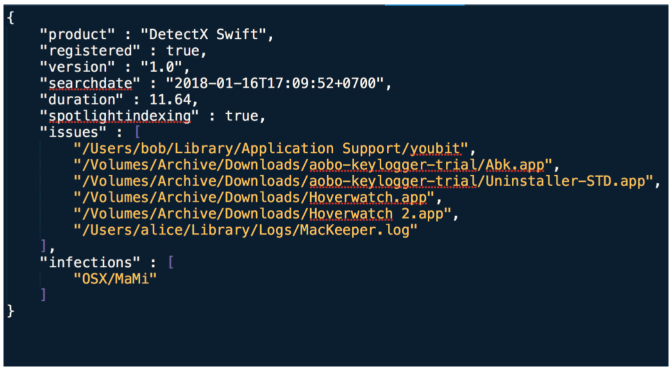
Save To File

A path can be given to write the results to file, either in regular text:

```
sudo <path to detectx executable> vvvv -a ~/Desktop/searchtest.txt
```

or, by passing the -j option for JSON format:

```
sudo <path to detectx executable>
search -aj ~/Desktop/searchtest.json
```



```
{
    "product" : "DetectX Swift",
    "registered" : true,
    "version" : "1.0",
    "searchdate" : "2018-01-16T17:09:52+0700",
    "duration" : 11.64,
    "spotlightindexing" : true,
    "issues" : [
        "/Users/bob/Library/Application Support/youbit",
        "/Volumes/Archive/Downloads/aobo-keylogger-trial/Abk.app",
        "/Volumes/Archive/Downloads/aobo-keylogger-trial/Uninstaller-STD.app",
        "/Volumes/Archive/Downloads/Hoverwatch.app",
        "/Volumes/Archive/Downloads/Hoverwatch 2.app",
        "/Users/alice/Library/Logs/MacKeeper.log"
    ],
    "infections" : [
        "OSX/MaMi"
    ]
}
```

The keys are as follows:

"*product*" - a string showing the name of the software package that produced the JSON output.

"*registered*" - a boolean value showing **true** if the command line tool is registered with a Pro or Management license and **false** otherwise.
Note that even if the product is registered in the User interface with a Home registration key, it will still show as ***false*** *in the command line tool.*

"version" - a string displaying the version number of the product when the search was run.

"searchdate" - a string in unix dateformat giving the date and time of the search, including GMT offset in hours.

"duration" - a floating point integer of how long the search took to complete, in seconds.

"spotlightindexing" - a boolean value showing whether spotlight indexing is enabled on the system startup disk. Part of DetectX Swift's search heuristics leverage Spotlight's metadata indexing. If this bool is false, it may lead to fewer results.

"issues" - an array of strings to paths that DetectX Swift has detected as requiring review. Note that the command line tool ignores any user whitelisting preferences. Paths shown under issues are always paths to 3rd party files and can be removed at the user's discretion.

“infections” - an array of strings showing the name of any found malware infections. These are not paths, as the malware may in fact not be entirely path-based, and/or may have altered otherwise benign or necessary files.

Removal of malware infections should be carried out by professionals.

REGISTER

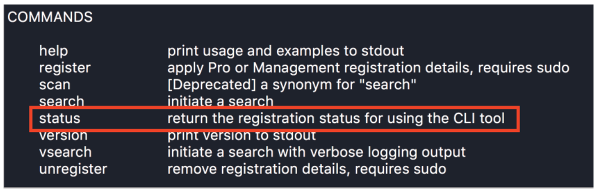
This command is required in order to register a **Pro** or **Management** license. This command must be run as root or as a sudo user. The syntax is

```
sudo <path to detectx executable> register -key GAWAE-ARQ1F-BZ...-FQQ2Z -email
bob@email.com
```

The values for -key and -email must be those shown in the order fulfilment email received after purchasing a **Pro** or **Management** license.

STATUS

This command returns the registration status for using the CLI tool. Note that for registered Home users, it will return ‘unregistered’, since the CLI tool requires a **Pro** or **Management** license



```
COMMANDS

    help            print usage and examples to stdout
    register        apply Pro or Management registration details, requires sudo
    scan            [Deprecated] a synonym for "search"
    search          initiate a search
    status          return the registration status for using the CLI tool
    version         print version to stdout
    vsearch         initiate a search with verbose logging output
    unregister      remove registration details, requires sudo
```

```
<path to detectx executable> status
```

UNREGISTER

This command can be used to remove a license key for all users on the mac. This command must be run as root or as a sudo user. The syntax is

```
sudo <path to detectx executable> unregister
```

The command will remove all classes of licenses: *Home*, **Pro** & **Management** on the mac.

HELP

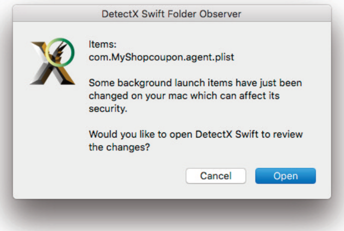
The `help` command will output the documentation to the command line.

FOLDER OBSERVER OPTIONS

There are 4 customization options available to **Pro** & **Management** license holders for the Folder Observer alert: *title*, *icon*, *body message* and the dialog *confirm* button.

```
defaults write com.sqwarq.DetectX-Swift ObserverTitle "Custom Title"
defaults write com.sqwarq.DetectX-Swift ObserverMessage "Here's a custom message from your Administrator, with our preferred icon.\n\nAnd we'd also like to point out the custom button text, too."
defaults write com.sqwarq.DetectX-Swift ObserverButton "Show Me"
defaults write com.sqwarq.DetectX-Swift ObserverIcon "/Applications/Disk Inspector.app/Contents/Resources/AppIcon.icns"
```

These preference settings are ignored for Home and Unregistered users.



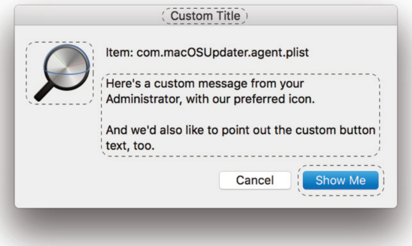
DetectX Swift Folder Observer

Items:
com.MyShopcoupon.agent.plist

Some background launch items have just been changed on your mac which can affect its security.

Would you like to open DetectX Swift to review the changes?

DEFAULT



Custom Title

Item: com.macOSUpdater.agent.plist

Here's a custom message from your Administrator, with our preferred icon.

And we'd also like to point out the custom button text, too.

CUSTOMIZABLE AREAS

To reset to default, remove the preference:

```
defaults remove com.sqwarq.DetectX-Swift ObserverIcon
defaults remove com.sqwarq.DetectX-Swift ObserverTitle
defaults remove com.sqwarq.DetectX-Swift ObserverButton
defaults remove com.sqwarq.DetectX-Swift ObserverMessage
```

NETWORK ADMINISTRATION

DetectX Swift users with **Pro** or **Management** licenses can integrate search, updates and registration functions directly with Jamf Pro and Munki as well as apply managed preferences using config Profiles. If you need help setting that up on your network, please contact Sqwarq support.

System Requirements

DetectX Swift requires macOS 10.11 or higher.

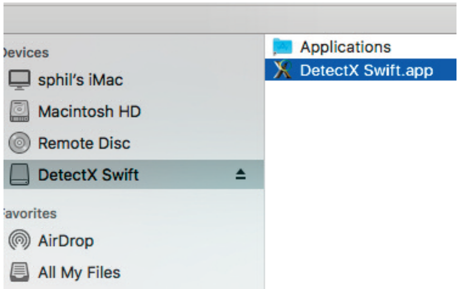
Installation

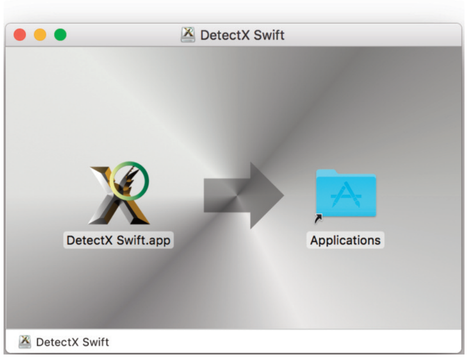
First download DetectX Swift from the Sqwarq.com website.

If the app is packaged as a .zip file, drag the unzipped application from the Downloads folder to the Applications folder.

If the app is packaged as a .dmg file, double-click the **DetectX Swift** disk image and choose whether to accept the license conditions. If you agree, the disk image will appear in the Finder sidebar.

From within the disk image, drag the DetectX Swift.app icon directly to another location within the Finder, preferably the Applications folder.





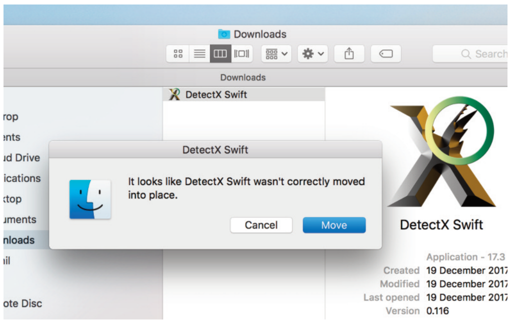
Troubleshooting Installation Issues

Watch the 1-minute video on how to successfully install DetectX Swift...

Due to security changes made by Apple in macOS 10.12 and later, it can sometimes occur that an app is not running from the location that you have saved it in.

Even correctly signed and legitimate applications are initially quarantined by Gatekeeper, and the quarantine flag is only removed when the app is dragged to a different location within the Finder from its original download location (refer to Apple documentation on *Gatekeeper Path Randomization* and *AppTranslocation* for further details).

As a result, if during installation or updating you are presented with a dialog insisting that DetectX Swift needs to move, click the 'Move' button and select the source and destination. 'Move' will allow you to select anywhere writable, including the current location (i.e, the source and destination can be the same) and DetectX will clear the quarantine flag.



DetectX Swift

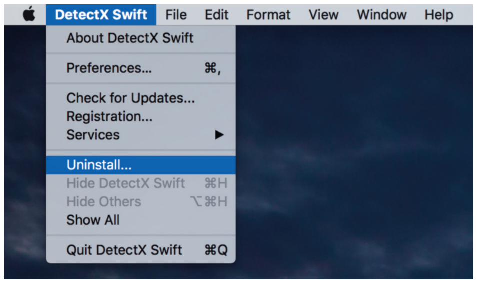
It looks like DetectX Swift wasn't correctly moved into place.

Application - 17.3
Created 19 December 2017
Modified 19 December 2017
Last opened 19 December 2017
Version 0.116

Uninstalling

Uninstalling DetectX Swift is a simple, two-step process.

Watch the uninstall video...



1. Launch the app, and from the DetectX Swift menu choose 'Uninstall...'. Press return to confirm.

2. Quit the app and drag it to the Trash.

This will uninstall all supporting components including the Folder Observer launch agent, if enabled.

Note that uninstalling the app and its components does not remove a purchased license key. Use the unregister command on the command line to do that (see the 'Command Line Tool' entry in the Advanced section in this guide).

What does DetectX detect?

The latest version of this document can be found online.

It is important to remember that DetectX Swift is a troubleshooting tool for your Mac, and not just a malware or adware scanner. DetectX Swift uses a four-fold classification system. Where an issue falls under more than one category, the search labels it according to the highest category it belongs to (where 1 is the least worrisome and 4 is the most):

1. Potentially destabilising software (**PDS**)
2. Potentially unwanted software (**PUS**)
3. Adware (**ADW**)
4. Malware (**MAL**)

1. Potentially Destabilising Software (PDS)

Items found by DetectX Swift labelled as Potentially Destabilising Software (**PDS**) include perfectly legitimate commercial applications, which may nevertheless cause the Mac or other software on the Mac to perform unexpectedly, poorly or even render the Mac unbootable under certain conditions.

These programs typically offer to remove or delete system files and caches, or to alter or remove application binaries under the claim that they will improve performance or 'clean' junk files.

While such operations can sometimes be performed without detriment, that is not always the case. Other applications may behave unexpectedly or not launch at all after being 'cleaned' by a **PDS.** For example, 'cutting' localisation (i.e., 'foreign language') binaries, deleting invisible licensing files or other required resources can all destabilise an otherwise functioning program or system service.

PDS vendors often claim their products can "speed up" or "clean" a Mac by removing caches, whereas the reality is that regularly purging caches does exactly the opposite (the whole purpose of a cache is to make loading frequently needed data faster).

Of course, sometimes caches do become corrupt or bloated, and users can sometimes be impressed with what appears to be a performance improvement after using a **PDS**. However, this is rather like improving an underperforming football team by selling the entire squad of players rather than trying to identify the specific outfielders (or is it the coach?) that are responsible for the problem.

Rather than taking a blanket 'shotgun' approach to troubleshooting, users are far better served by taking an analytical approach to discover the true cause of any poor performance problems. DetectX Swift's Search, Profiler, and History functions are designed to do exactly this. If you need expert help analysing the data provided by DetectX Swift, registered users may contact Sqwarq support for a free consultation.

The **PDS** category also includes applications found by DetectX Swift that are inherently inefficient, such as using excessive system resources to perform what should otherwise be light resource task.

Issue flag:
When DetectX Swift identifies apps that fall solely within this category it will flag them as **PDS** ***(note: issue flagging is not available in v1.0x of DetectX Swift, but will be arriving in a future update***).

2. Potentially Unwanted Software (PUS)

Whereas **PUS** items may only be destabilising in certain circumstances or when used in a certain way, items found by DetectX Swift within the **PUS** category are more consistently detrimental or a nuisance to the user.

Applications that use excessive and/or unethical marketing practices to encourage users to install either the application itself or auxiliary applications that the user may not explicitly desire are consider **PUS** by DetectX Swift. Such applications may also use excessive popups and nags to encourage users to pay premium rates for actions that can often be performed natively on the Mac or which are widely available for free or as open source software by other more reputable vendors.

PUS applications may, in some cases, expose user information to unknown or unauthorised parties, and/or perform unexpected actions.

Issue flag:
When DetectX Swift identifies apps that fall into this category it will flag them as **PUS** unless they also fall into a higher category ***(note: issue flagging is not available in v1.0 of DetectX Swift, but will be arriving in a future update***).

3. Adware (ADW)

This category includes applications, processes and files found by DetectX Swift which attempt to inject advertising into web pages, and/or redirect browser searches to sites the user had no intention of visiting in order to generate advertising revenue. **ADW** also includes software that uses excessively intrusive advertising techniques and fear-based marketing strategies.

Issue flag:
When DetectX Swift identifies items that fall into this category it will flag them as **ADW** unless they also fall into a higher category ***(note: issue flagging is not available in v1.0x of DetectX Swift, but will be arriving in a future update***).

4. Malware (MAL)

This category includes anything found by DetectX Swift that compromises the user's security or acts to harm the interests of the user. Typically this includes RATS, DNS changers, Ransomware, Trojans and Viruses among others.

The **MAL** category also includes keyloggers. Although some keylogger developers may argue that their software has genuine uses similar to parental controls or user account management software, we find the surreptitious and deceptive nature of keyloggers to fall well within our definition of malware as stated in the previous paragraph.

Parental control and user account management tools work best when the user is aware of the restrictions or limitations imposed on their use of resources managed or owned by others. Moreover, in our view, ethical software does not attempt to capture or exfiltrate a user's personal data covertly.

Issue flag:
When DetectX Swift identifies items that fall into this category it will flag them as **MAL** ***(note: issue flagging is not available in v1.0x of DetectX Swift, but will be arriving in a future update***).

INDEX