Welcome to DetectX Swift
Search and Rescue for your Mac

Quick Start
Welcome to DetectX Swift

Preferences

Search

Profile

History
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. Institutional, organisational and commercial or commercial-like use of Release versions requires the purchase of a Commercial Use 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

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

This document was published on 10 November, 2017.
Welcome to DetectX Swift

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

Schedule DetectX to run at certain times, access DetectX’s hidden preference settings, tips and tricks for expert troubleshooters.
Read more
Welcome to DetectX Swift

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.

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,
Welcome to DetectX Swift

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 first 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).

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.

The information in the Status field can be refreshed by exercising any of DetectX’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.

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.
**The Search function** will scan your mac for known threats at the following times:

i. When you launch the app  
ii. After deleting any item found in a scan  
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 scan:

**I. NOTHING IS FOUND**

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

**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 ➕

**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.
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.

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.

The Open button appears on any line that contains:

- A complete filepath that exists
- A plist program argument that exists
- A folder that has child items

Clicking it:

- reveals the item in the Finder
- 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.

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

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.

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.

**Remove Process Button**

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

1. The recent history view shows changes since DetectX Swift last ran.
2. The all history view shows all history ever recorded by DetectX Swift.
3. 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.

This view shows 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.

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.
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.

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.
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`.

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 FastTasks 2 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.

#### Folder Observer

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

Uncheck the preference if you do not want these alerts.

#### Restore To Default

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

You can access DetectX Swift’s Application Support folder easily by clicking the blue folder icon in any of the History views.
This chapter is not yet available as some of the features are not yet implemented in the beta version.

Please contact Sqwarq Support or post in the Slack group if you have any questions, enhancement requests or feedback.

Email: support@sqwarq.com

Details of how to join the Slack group can be found on the DetectX Swift Beta page.
INDEX

ADVANCED 15
APPLICATION SUPPORT FOLDER 14
CHANGES INDICATOR 11
DELETE HISTORY 14
DELETE RUNS 14
DIFF 12
FOLDER OBSERVER 13
MANAGING UPDATES 13
NAVIGATION BUTTON 9
ALL HISTORY 11
HISTORY 11
RECENT HISTORY 11
OPEN BUTTON 9
PREFERENCES 13
GENERAL 13
QUICK LOOK BUTTON 10
REFRESH BUTTON 10
REMOVE PROCESS BUTTON 10
RESET 14
RESTORE TO DEFAULT 13
RESULTS 8
RUNS 12
WHITELIST 8