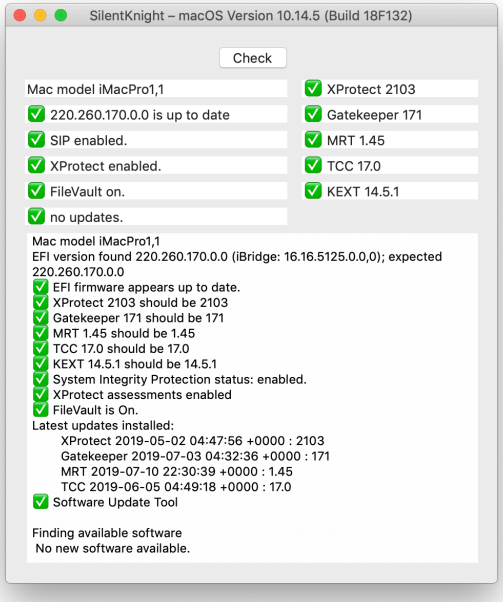
Start

SilentKnight checks your Mac's key security systems to ensure they're up to date and enabled. This reference explains each item shown in its window.



➜ Check

➜ Mac model
➜ EFI firmware
➜ SIP
➜ XProtect
➜ FileVault
➜ Updates
➜ Report

➜ XProtect
➜ Gatekeeper
➜ MRT
➜ TCC
➜ KEXT
➜ Install all updates
➜ Disable softwareupdate

➜ Start

Check

When you first open SilentKnight, it runs its standard checks and completes the result boxes. Click on the **Check** button, or use the **Check** command in the **File** menu, to repeat those checks and generate a new report.

SilentKnight connects to my GitHub server and downloads the current EFI firmware version for this model, then connects to obtain the current list of security data versions. The app checks those versions found on your Mac, compares them, and displays the results.

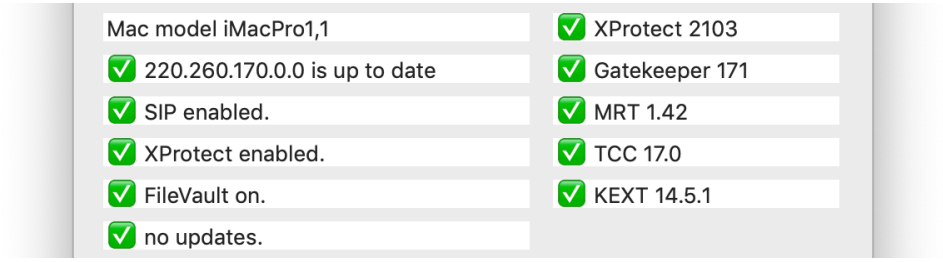
Those considered to be up to date are prefaced by the emoji ✅ to indicate a ‘pass’. Those considered to merit further checking or action on your part are prefaced by ⚠️. Those which appear to be out of date or worth attending to are prefaced by ❌. Items updated in the last 24 hours are shown with a 👈 by them.

If you haven’t disabled the softwareupdate feature, the app also connects to Apple’s update servers and asks them whether there are security or system updates available for your Mac. This takes longer to complete: while waiting for the result, a circular busy spinner is displayed next to the Updates box. If there are updates available, the **Install all updates** button next to the spinner is shown, so you can decide whether to download and install them.

➜ Disable softwareupdate
➜ Install all updates

➜ Start

Mac model



This displays the specific model of Mac using a standard code, in which *type* of Mac is given first, e.g. MacBookPro, then two digits separated by a comma to identify the *series* and specific *model,* e.g. 10,2. Use these when referring to your Mac so that others can know exactly which it is.

This information is obtained using:

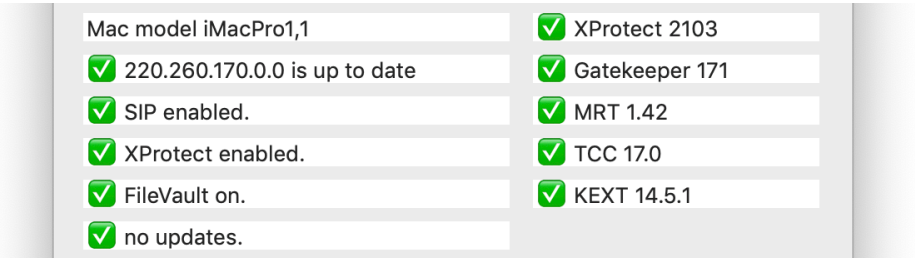
```
let platformExpert = IOServiceGetMatchingService(kIOMasterPortDefault, IOServiceMatching("IOPlatformExpertDevice"))
let modelAsCFString = IORegistryEntryCreateCFProperty(platformExpert, "model" as CFString, kCFAllocatorDefault, 0)
```

It's used to look up the expected EFI firmware version, so if an error occurs when obtaining the Mac model, the EFI firmware version given is almost certainly incorrect too.

➜ EFI firmware

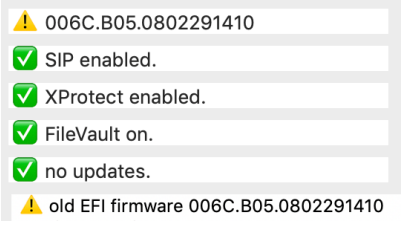
➜ Start

EFI firmware



SilentKnight looks up the EFI firmware version used by your Mac, and compares it with that believed to be current for supported versions of macOS (High Sierra, Mojave, Catalina). If the version found is older than that expected, you will be warned. If your Mac is running beta software, its firmware may have a different version.

Macs running Sierra and El Capitan haven't had firmware updates for some time, and are now left running older versions, which can't be checked against current release versions. Older systems, and some Mac Pro models, still use a different version numbering system. SilentKnight can't determine whether those older versions are the latest available, so shows the result with a ⚠️ warning triangle, so that you can check the version manually:



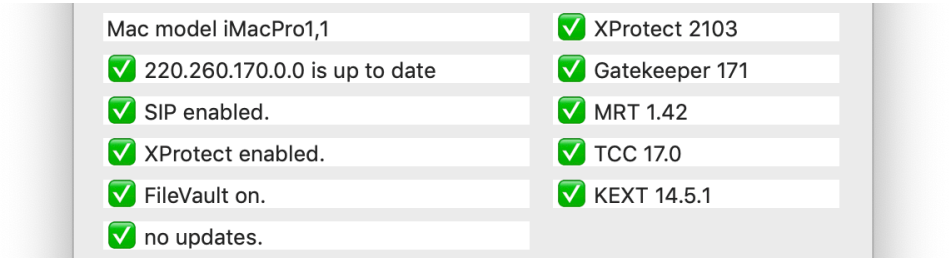
This information is obtained using

```
let theEntry = IORegistryEntryFromPath(0, "IODeviceTree:/rom")
let efiAsCFString = IORegistryEntryCreateCFProperty(theEntry, "version" as CFString, kCFAllocatorDefault, 0)
```

➜ SIP

➜ Start

SIP



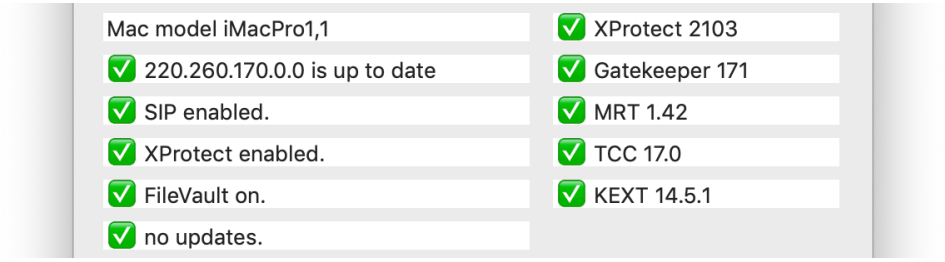
System Integrity Protection or SIP ensures that nothing can tamper with your Mac's system files, and now extends to all the bundled apps in macOS and more besides. Although sometimes it can be helpful to disable SIP, you should never run a Mac for any longer than is essential with SIP turned off.

If SIP is turned off, turn it back on by restarting your Mac in Recovery mode holding Command-R, opening Terminal there and typing in the command
`csrutil enable; reboot`
When you press Return, your Mac will then restart in regular mode again with SIP turned back on.

To check SIP, SilentKnight runs the shell command
`csrutil status`

➜ XProtect

XProtect



XProtect is responsible for checking apps and some other files for tell-tale signatures indicating that they are malicious. It should always be enabled: if it's reported in its box at the left to be disabled, contact Apple support as a matter of urgency, as your Mac may have already been attacked by malware. Apple infrequently updates its signature and malware definitions using a pushed security update.

To determine the current version of XProtect data files installed, SilentKnight obtains the version number of /System/Library/CoreServices/XProtect.bundle (in 10.15 and later, /Library/Apple/System/Library/CoreServices/XProtect.bundle).

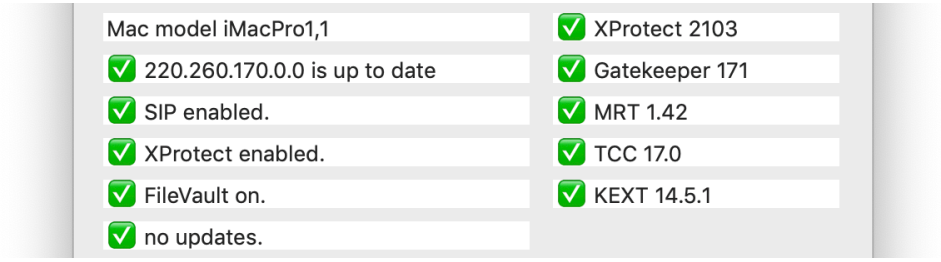
When updated, the new data takes immediate effect. You don't need to restart your Mac.

To check that XProtect blacklist protection is enabled, it runs the shell command
`spctl --status`
which should always return that assessments are enabled.

➜ FileVault

➜ Start

FileVault



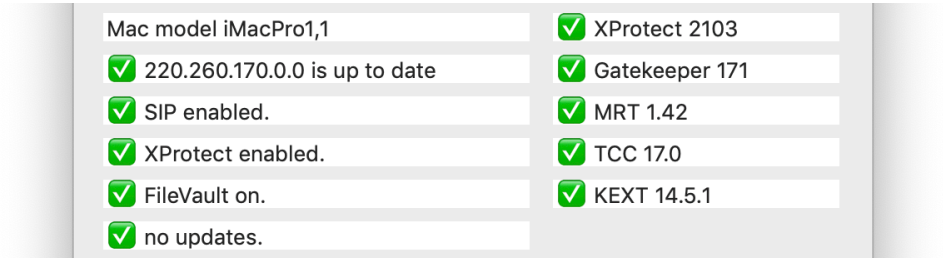
FileVault protects the contents of disks by encrypting them. Internal storage of Macs equipped with T2 chips are always encrypted, although their default encryption doesn't use your password. If there's any risk that someone else could gain access to private or sensitive data on your Mac, you should turn FileVault on. This is an option which you control in the **Security & Privacy** pane of System Preferences.

To check whether FileVault disk encryption is turned on, SilentKnight runs the shell command
`fdesetup status`
This only applies to the internal storage, although external drives can also be encrypted using FileVault when you wish to protect them.

➜ Updates

➜ Start

Updates



When SilentKnight starts up, and when you click the **Check** button, it connects to Apple's servers and asks them for a list of all system and security updates available for your Mac, using the following command:

```
softwareupdate -l --include-config-data
```

or, in El Capitan,

```
softwareupdate -l
```

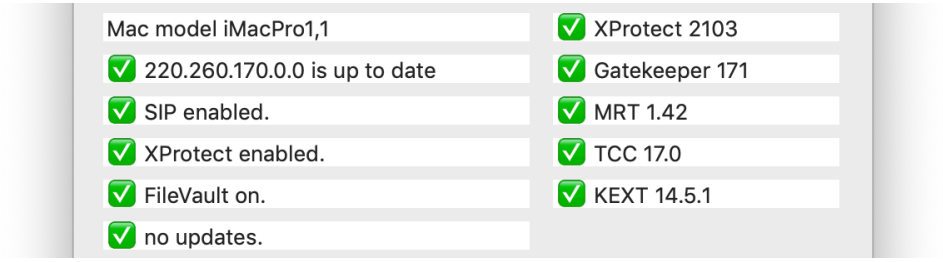
This doesn't require you to authenticate, even in El Capitan, and should still work when automatic updates are disabled. When updates are available, this in turn displays the **Install all updates** button, allowing you to download and install them when you wish.

You can disable this softwareupdate check if you wish.

➜ Gatekeeper
➜ Install all updates
➜ Disable softwareupdate

➜ Start

Gatekeeper



Gatekeeper data files include lists of revoked developer security certificates and other vital information which is used when macOS checks the authenticity of apps and some other items. This is normally performed when the app or item is being run for the first time after being downloaded from the Internet and put into quarantine, but can also be performed on other occasions.

These data files are stored at /private/var/db/gkopaque.bundle, and it's that bundle's version number which SilentKnight checks and displays. Apple pushes quite frequent updates, every week or two, to ensure that certificate revocations are promulgated promptly.

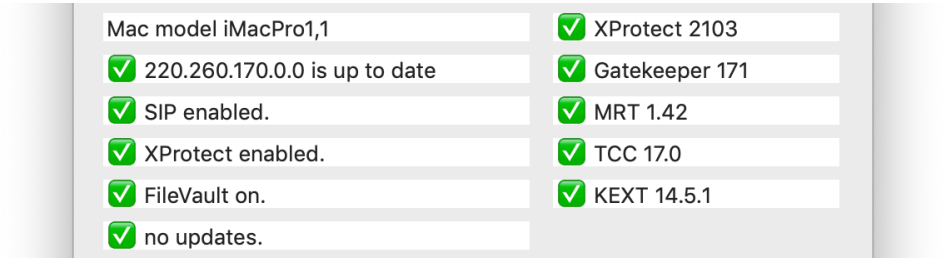
Catalina and Big Sur have additional data stored at /private/var/db/gke.bundle (which used to be tiny), so in 10.15 and later the version of that bundle is given after the number for the main gkopaque.bundle, e.g. **181, 8.0**. If either is out of date in Catalina or Big Sur, a warning results.

When updated, the new data takes immediate effect. You don't need to restart your Mac.

➜ MRT

➜ Start

MRT



If the system detects that malware is present, it calls on the Malware Removal Tool MRT to do the job. Although this hasn't been updated very often over the last year or so, it remains a central part of macOS system security, and Apple does still maintain it.

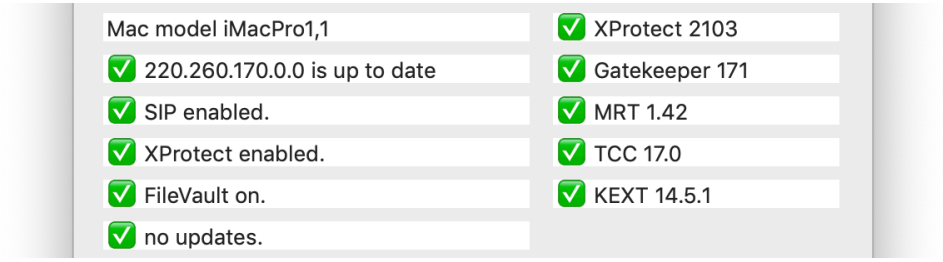
The app's data are contained within the app at /System/Library/CoreServices/MRT.app (in 10.15 and later /Library/Apple/System/Library/CoreServices/MRT.app), and the version given here is that of that app.

When updated, MRT may be run automatically to check for any malware which needs to be removed. As MRT is normally only run after starting up, you may prefer to restart after updating, to ensure that the new version scans your Mac promptly. It's also possible to run MRT manually, but that doesn't appear as reliable as restarting.

➜ TCC

➜ Start

TCC



macOS Mojave introduced new protection for private data in Transparency Consent and Control or TCC. That uses private data which Apple periodically changes using its pushed update service to replace /System/Library/Sandbox/TCC_Compatibility.bundle (in 10.15 and later /Library/Apple/Library/Bundles/TCC_Compatibility.bundle).

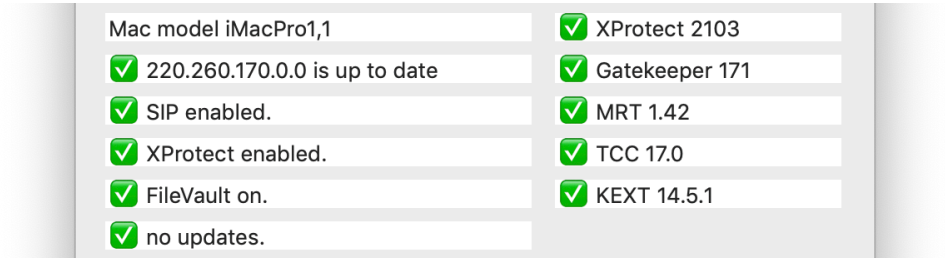
SilentKnight shows the version number of that bundle. This differs considerably between Mojave and Catalina/Big Sur.

When updated, the new data takes immediate effect. You don't need to restart your Mac.

➜ KEXT

➜ Start

KEXT



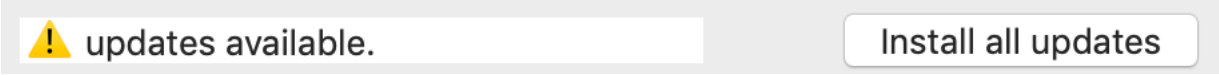
macOS uses a kernel extension exclude list to prevent some old and conflicting kernel extensions from being loaded. This is obtained from that extension, at /System/Library/Extensions/AppleKextExcludeList.kext, or in Catalina/Big Sur at /Library/Apple/System/Library/Extensions/AppleKextExcludeList.kext.

When updated, the new data is used when you next start your Mac up.

➜ Install all updates
➜ Disable softwareupdate

➜ Start

Install all updates



The **Install all updates** button only appears when SilentKnight has discovered that there are updates available for your Mac, although you can always force them to be downloaded and installed using the menu command. When you click on this button, the app runs the command:

```
softwareupdate -ia --include-config-data
```

or, in El Capitan,

```
sudo softwareupdate -ia
```

If you are running El Capitan, you need to authenticate before this command can be run, but that is not required in Sierra or later. This tries to connect to Apple's servers, and downloads and installs all pending updates for you.

⚠️ This automatically installs *all* pending system and security updates, whether you want them or not. When large updates are available, it may take several hours to complete, during which SilentKnight will display a 'busy spinner' to indicate that it is still busy. My free app LockRattler allows you to download and install individual updates instead.

➜ Disable softwareupdate
➜ Report

Disable softwareupdate

macOS High Sierra and Mojave Security Update 2020-003, and Catalina 10.15.5, change the way that Software Update works. This prevents you from turning off the red badge which indicates that an unwanted update is waiting to be downloaded and installed. It's possible to alter this, but when you next access Software Update, the red badge will reappear. To ensure that this doesn't happen when using SilentKnight, there is an option which stops SilentKnight from checking Apple's update servers for available updates.

To disable checking for available updates, select the **Check Updates** item in the **SilentKnight** menu (where you'd expect **Preferences** to be). That menu command will then change to read **Don't Check Updates**. When you next open SilentKnight, the softwareupdate check won't be run. You can also set that in SilentKnight's preferences file by entering the following command:

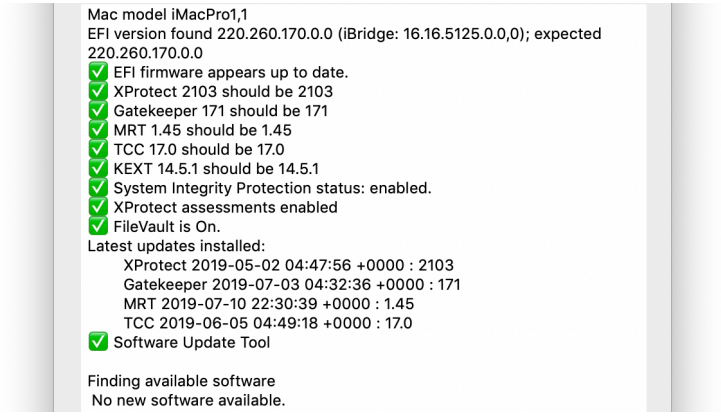
```
defaults write co.eclecticlight.SilentKnight noCheckSWU true
```

To enable softwareupdate checks again, simple select the **Don't Check Updates** command. It will change back to **Check Updates**, and when you next click on the **Check** button or open SilentKnight, the normal softwareupdate check will be run. You can also use the command

```
defaults write co.eclecticlight.SilentKnight noCheckSWU false
```

➜ Report

Report



In addition to displaying brief information in the boxes above, SilentKnight also provides more in the scrolling text area in the lower part of its window. This may include errors encountered when trying to obtain some of those values.

It also lists the latest dates of installation of security data files, which are derived from that Mac's install history at /Library/Receipts/InstallHistory.plist. Those are checked again after the installation of any updates, and should confirm that the update has been correctly received and installed. The emoji 👈 is shown by new versions for 24 hours.

Select all and copy the contents of the report to paste in as plain or rich text, or use the **Export…** command to save this to a file in plain text. Use ⌘+ and ⌘– to enlarge or shrink the text size as you wish.