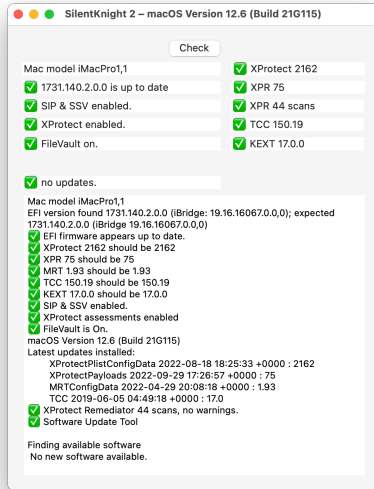# Start

SilentKnight checks your Mac's key security systems to ensure they're up to date, enabled and working. This reference explains each item shown in its window. To enlarge the contents of this window, just drag it bigger.

➜ Mac model   ➜ XProtect

➜ Firmware   ➜ XProtect Remediator

➜ SIP & Security   ➜ XPR scans   ➜ Platform security in non-English languages

➜ XProtect   ➜ TCC

➜ FileVault   ➜ KEXT

➜ Apple Studio Display   ➜ Settings

➜ Updates   ➜ Install all updates   ➜ Install Named Update…   ➜ Failed updates

➜ Report   ➜ Disable softwareupdate   ➜ Download not install   ➜ SilentKnight updates

➜ Preventing unwanted installations

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 firmware version for your Mac, 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 ✅ or 🍏 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 Those which appear to be out of date or worth attending to are prefaced by ❌.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 changed Settings to **Don't check**, the app also connects to Apple's update servers and asks 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. If you only want to install some of the updates, use the **Install Named Updates…** command in the **File** menu to open a separate **Updater** window.

SilentKnight *never* downloads or installs updates automatically: it only does so when you tell it to using a button or menu command.

➜ [Disable softwareupdate](#)   ➜ [Preventing unwanted installations](#)
➜ [Install all updates](#)   ➜ [Install Named Update…](#)   ➜ [Download not install](#)

Mac model

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

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 firmware version, so if an error occurs when obtaining the Mac model, the firmware version given is almost certainly incorrect too.

➜ [Firmware](#)

Firmware

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

SilentKnight looks up the firmware version, and compares it with that believed to be current for supported versions of macOS (Big Sur, Monterey and Ventura). If the version found is older than that expected, you will be warned. If your Mac is running beta software, its firmware is likely to have a different version.

This information is obtained using

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

➜ [SIP & Platform Security](#)

SIP & Platform Security

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

System Integrity Protection (SIP) ensures that nothing can tamper with your Mac's system files, and extends to all the bundled apps in macOS and a great deal more. 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 starting your Mac up in Recovery mode, 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`

This also checks and reports whether the Signed/Sealed System Volume (SSV) is correctly sealed.

Apple silicon Macs have several additional protections in their Platform Security as well as SIP and the SSV. To evaluate those, SilentKnight checks all that are available, and summarises results in this box. Full details of each security setting are given in the text box at the bottom of the window.

➔ XProtect   ➔ Platform security in non-English languages

XProtect

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

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 periodically updates its signature and malware definitions using pushed security updates. To determine the current version of XProtect data files installed, SilentKnight obtains the version number of /Library/Apple/System/Library/CoreServices/XProtect.bundle.

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

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

➔ [FileVault](#)

FileVault

|	
Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

FileVault protects the contents of disks by encrypting them. Data volumes on the internal storage of Macs equipped with T2 chips and Apple silicon models 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 Data volume on internal storage, although external volumes can also be encrypted using FileVault when you wish to protect them.

➔ [Updates](#)

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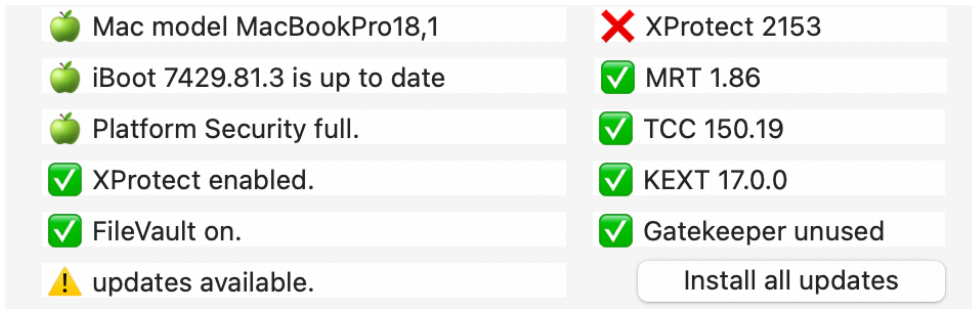
When SilentKnight starts up, and when you click the **Check** button, it connects to Apple's servers and asks them for a list of all system and security updates available for your Mac, using the following command:
`softwareupdate -l --include-config-data`

This doesn't require authentication, and still works when automatic updates are disabled. When updates are available, this in turn displays the **Install all updates** button (unless disabled in Settings), allowing you to download and install them when you wish. If you only want to install some of the updates, use the **Install Named Updates…** command in the **File** menu to open a separate **Updater** window.

You can disable this softwareupdate check if you wish, in Settings.

➜ [Failed updates](#)   ➜ [Preventing unwanted installations](#)

➜ [Install all updates](#)   ➜ [Install Named Update](#)   ➜ [Download not install](#)

➜ [Disable softwareupdate](#)   ➜ [Settings](#)

XProtect Remediator

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

This new tool to replace MRT was introduced in Monterey 12.3, and is now standard in Catalina and later,and found at /Library/Apple/System/Library/CoreServices/XProtect.app. It's routinely updated every two weeks, and consists of a number of scanning modules that are run in the background when your Mac isn't busy. Most are designed to detect and remediate specific types of malware, and one module replaces MRT in its functions.

The version number shown is that of the XProtect.app bundle.

➜ [XProtect Remediator scans](#)

XProtect Remediator Scans

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

When any of XProtect Remediator's scanning modules completes a scan, it should write a short report in the Unified log. SilentKnight checks those log reports over the last 24 hours, and here reports the total number it has found, the number of any detections/remediations as ⛔ alerts, and the number of any others meriting your attention as ⚠️ warnings. If your Mac hasn't been running long enough over that period for any scans to have been reported, that is declared with a red question mark ❓ . To save time, this check *isn't* repeated when you click the **Check** button.

To be able to inspect the log, you need to be running as an admin user. When SilentKnight opens, it checks that, and the state of your log files. If you're only running as a regular user, or it's unable to access your log for another reason, this check isn't performed.

To obtain further information about XProtect Remediator reports, use XProCheck. In Ventura and Sonoma, security apps using Apple's Endpoint Security may be able to provide more details too.

➔ **XProtect Remediator**

MRT

In Catalina and later, the task of detecting and removing known malware previously performed by MRT has been taken over by XProtect Remediator. For the sake of completeness, the current version of MRT installed is reported in the detailed report at the foot of the window.

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

Some recent macOS versions including Ventura may not install MRT at all. However, softwareupdate may still find and install the last version.

Should Apple ever update MRT, it 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.

➜ [XProtect Remediator](#)
➜ [TCC](#)

TCC

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

Protection for the privacy of data by Transparency Consent and Control (TCC) relies on private data which Apple periodically changes using its pushed update service to replace /Library/Apple/Library/Bundles/TCC_Compatibility.bundle.

SilentKnight shows the version number of that bundle.

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

➔ **KEXT**

KEXT

Mac model iMacPro1,1	✅ XProtect 2162
✅ 1731.140.2.0.0 is up to date	✅ XPR 75
✅ SIP & SSV enabled.	✅ XPR 44 scans
✅ XProtect enabled.	✅ TCC 150.19
✅ FileVault on.	✅ KEXT 17.0.0

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 /Library/Apple/System/Library/Extensions/ AppleKextExcludeList.kext.

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

➜ [Install all updates](#)
➜ [Download not install](#)
➜ [Install Named Update…](#)
➜ [Disable softwareupdate](#)

Apple Studio Display

When you have one or more Apple Studio Displays connected, a new row appears at the foot of the information before those about updates. This states the display recognised, and on the right the current firmware versions are given for each connected Studio Display. If SilentKnight isn't able to find an Apple Studio Display, this row remains blank. Currently, this may not recognise Studio Displays connected to external hubs or docks, due to a bug in System Information.

Firmware updates for Studio Displays are pushed in the normal way through Software Update. When one is available, don't try to download or install it using SilentKnight, but use Software Update instead.

Display firmware versions are checked against the current version stored in the GitHub database, and any discrepancy is marked with a ❌ and reported in full in the scrolling text below.

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, SilentKnight runs the command:

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

This tries to connect to Apple's servers, and downloads and installs *all* pending updates for your Mac.

⚠️ This automatically installs *all* pending system and security updates, whether you want them or not. When large updates such as macOS updates are available, install those first using Software Update, or use the **Install Named Update…** command in the **File** menu to download and install individual updates instead.

When updates have been installed, SilentKnight runs through its checks again and refreshes version numbers shown, so you can check that they have been installed correctly.

You can disable the Install All Updates button, which hides it. If you do that, you can still use the menu command to install all updates if you wish.

➜ [Failed updates](#)   ➜ [Preventing unwanted installations](#)
➜ [Install Named Update…](#)   ➜ [Download not install](#)
➜ [Disable softwareupdate](#)   ➜ [Settings](#)
➜ [Report](#)

Install named update
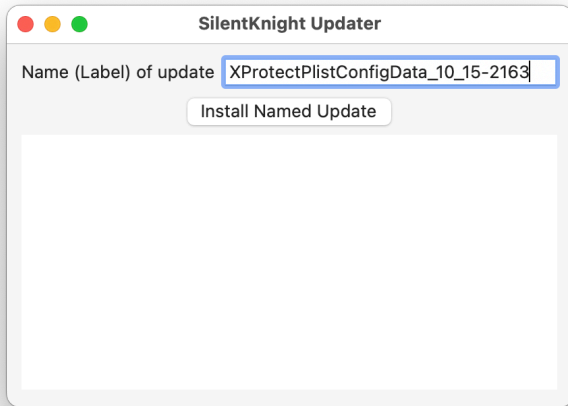
The **Install Named Update…** command in the **File** menu opens SilentKnight's Updater window, in which you can install as many individual updates as you wish.

When SilentKnight checks for updates, it shows the list of available updates in the main scrolling text view of the main window. For each update available, this normally lists the name of that update in the first of a pair of lines, starting with `* Label:`. Select that name and copy it from that window. Then paste it into the text box at the top of the SilentKnight **Updater** window. Click on the **Install Named Update** button to download and install it. Repeat this procedure for each update you wish to install.

If the command returns an error, it's most probable that you gave the wrong name. Try copying and pasting a different part of the listing from the main window until it works. Closing the Updater window doesn't quit the app.

When you click on this button, the app runs the command:
```
softwareupdate -i --include-config-data updatename
```

Failed updates

Sometimes updates aren't found, even though others can download and install them, or they fail to install correctly. The latter are clearly show in the lower text box, which records the update being downloaded, but then failing to install, leaving the version number unchanged.

If you're obtaining your Mac's updates through a local Content Caching server, the next step is to temporarily disable that in Sharing. Quit SilentKnight, open it again, and try installing the update(s) again. Once installed successfully, you can enable the Content Caching service again.

If you're not running a Content Caching server, or have other problems, try restarting your Mac and running SilentKnight again. If that still doesn't work, start your Mac up in Safe mode and repeat the process there.

Any persistent failure to obtain and install security data updates should be reported to Apple Support or, if you have access as a developer, through Feedback. Apple does take security update problems seriously, as they could compromise your Mac.

Preventing unwanted installations
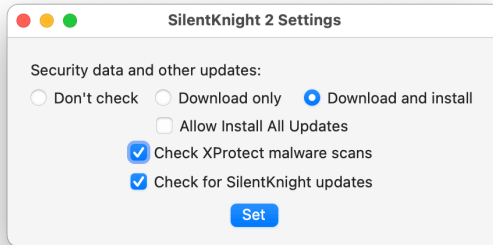
When SilentKnight gets the list of available updates, it includes some items, such as macOS updates, that you probably won't want to install using SilentKnight, or you may want to postpone. To cater for that, SilentKnight offers the option of downloading individual named updates. However, it may be too easy to miss those, and inadvertently click on the **Install All Updates** button and get what you didn't intend.

To help you avoid making mistakes like that, you can prevent the **Install All Updates** button from appearing when there are updates available. Simply open SilentKnight's Settings, and uncheck the **Allow Install All Updates** box there. When you've done that, click on the **Set** button to save that in SilentKnight's preferences, quit the app, and open it again.

When that box is unchecked (no √ tick in it), you can still install all updates using that command in the File menu, or you can open the **Install Named Update** window using that command instead.

Once you've installed the update you've been avoiding, you can tick that box in Settings again to return SilentKnight's behaviour to normal.

➔

Settings
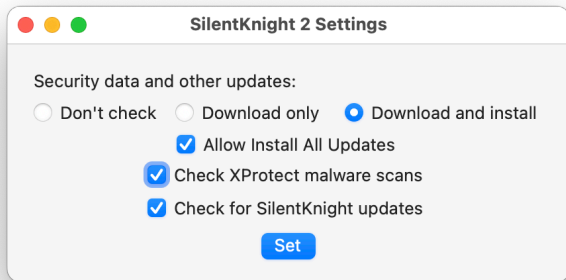
This lets you choose four different options:
- How SilentKnight checks for updates and installs them. Select **Don't check** and it won't check for updates at all. Select **Download only** and updates will be downloaded but not installed. Recommended is **Download and install**, which does the whole job for you.
- Whether SilentKinght offers its button to **Install All Updates**, or makes you install them individually.
- Whether SilentKnight checks XProtect Remediator scans in the log.
- Whether SilentKnight checks for its own app updates.

When you change settings, click on the **Set** button for them to take effect, then quit the app. When you open it, your new settings will be in effect. If you close the Settings window *without* clicking the **Set** button, those changed settings won't be applied.

➔ [Preventing unwanted installations](#)
➔ [Disable softwareupdate](#)
➔ [Download not install](#)
➔ [XProtect Remediator scans](#)
➔ [SilentKnight updates](#)

Disable softwareupdate

macOS Catalina 10.15.5 changed 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 to stop SilentKnight from checking Apple's update servers for available updates.

To disable checking for available updates, open Settings from the SilentKnight menu and click on the **Don't check** radio button, then click on the **Set** button. 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, open Settings from the SilentKnight menu and click on either the **Download only** or **Download and install** button, then click on the **Set** button. 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
```

➜ [Settings](#)
➜ [Report](#)

Download not install

By default, SilentKnight both *downloads* and *installs* updates when you tell it to. There are occasions when you may prefer only to download the update for the time being, and decide whether to install it later. For example, a bug in MRT version 1.68 caused problems on many Macs. If you wish to be cautious, you could just download future updates to MRT then, after a couple of days, if the latest update appears to be problem-free, you could install it.

To disable automatic installation, open **Settings** from the SilentKnight menu, and select the **Download only** radio button. Then click on the **Set** button, quit SilentKnight, and the next time you open the app, it should only download and not install updates.

To remind you that updates are only being downloaded, when installation is disabled a ⚠️ warning triangle is displayed in SilentKnight's windows, and all menu commands and buttons which normally read **Install** are changed to read **Download** instead.

Downloaded updates are saved in the /Library/Updates folder, which is automatically opened for you after downloading is complete. Apple's documentation (from 2012) warns that those Installer packages "are not designed to be installed by double-clicking the packages in that directory: always use [softwareupdate] --install or the App Store to actually perform the install." However, that doesn't appear necessary. Downloading can also result in spurious errors being reported when the update is in fact perfectly good.

➜ [Settings](#)
➜ [Install named update](#)

Report

```
Mac model iMacPro1,1
EFI version found 1731.140.2.0.0 (iBridge: 19.16.16067.0.0,0); expected
1731.140.2.0.0 (iBridge 19.16.16067.0.0,0)
✅ EFI firmware appears up to date.
✅ XProtect 2162 should be 2162
✅ XPR 75 should be 75
✅ MRT 1.93 should be 1.93
✅ TCC 150.19 should be 150.19
✅ KEXT 17.0.0 should be 17.0.0
✅ SIP & SSV enabled.
✅ XProtect assessments enabled
✅ FileVault is On.
macOS Version 12.6 (Build 21G115)
Latest updates installed:
     XProtectPlistConfigData 2022-08-18 18:25:33 +0000 : 2162
     XProtectPayloads 2022-09-29 17:26:57 +0000 : 75
     MRTConfigData 2022-04-29 20:08:18 +0000 : 1.93
     TCC 2019-06-05 04:49:18 +0000 : 17.0
✅ XProtect Remediator 44 scans, no warnings.
✅ Software Update Tool

Finding available software
 No new software available.
```

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.

Apple silicon security on non-English systems

Most information about macOS is available in English, regardless of the primary language in use at the time, which allows SilentKnight to analyse results. One exception to this is the information about Apple silicon Platform Security, which is only available in the current primary language.

Because of that, SilentKnight is unable to parse Platform Security information when your Mac is running with a non-English primary language. The only solution at present results in the SIP & Platform Security reporting limited or partial Platform Security. The full report is then given in the lower text box, so you can check in your primary language whether the full details of Platform Security settings.

I apologise for this inconvenience, but I have been unable to find a language-independent substitute, and can't parse dozens of different languages to work out whether the results are normal.

➔ [SIP & Platform security](#)
➔ [Report](#)

SilentKnight updates

Whenever you open SilentKnight, it may check to see if an update is available. This *doesn't* use the popular Sparkle mechanism for updating in place, but works as detailed here.

Once SilentKnight has successfully completed an integrity check, it checks whether update checking has been turned off in its preferences file. If that has, it abandons any attempt to check for updates. If checking is allowed, it then checks when it last checked for updates. If that was more than 12 hours ago, it continues to perform the check. It then connects to my GitHub server, from where it downloads a list of current versions of my apps. It doesn't upload any data to the GitHub server at all, and no statistics beyond GitHub normal connection figures are collected either: no personal identifiers are recorded.

If there is an update available, SilentKnight then checks that its location is on this WordPress blog, and posts a dialog which invites you to download the update.

If you click on the **Download** button, it then points your default browser at that update, which should trigger the update to be downloaded to your normal downloads folder. The update is received as a regular Zip archive, and is exactly the same as you would download from the Downloads page here. It also carries a quarantine flag, so that when you unZip it and install the app inside, it undergoes normal first run 'Gatekeeper' security checks. If you click on the **Ignore** button, SilentKnight won't remind you about it again for another 12 hours.

An additional item at the end of the **Help** menu explains the update status. If no update check is performed, or the check fails, the last item reads **Update not checked**. If the check is performed and update information is obtained, even when no update is available or you decline to download it, that menu item reads **Checked for update** and is ticked (but still disabled).

You can disable checking for updates in SilentKnight's Settings.

You can also customise this behaviour by changing SilentKnight's preferences. The keys to use are:
- `noUpdateCheck`, a Boolean. When set to `true`, this disables all update checking. Default is `false`.
- `updateCheckInt`, a real number (Double). When set to a value greater than 1.0, the minimum time interval between checks, in seconds. Default is 43200, which is 12 hours. If you set it to any value less than 1, Ulbow will reset it automatically to that default.

To change either of these, use a Terminal command of the form

```
defaults write co.eclecticlight.SilentKnight updateCheckInt '10'
```

which works properly through the preferences server `cfprefsd`.

The Eclectic Light Company blog – https://eclecticlight.co