

→ [Start](#)

# Start

SilentKnight checks your Mac's key security systems to ensure they're up to date, enabled and working. It reports in five sections that can be opened and closed by clicking on the chevron v or > at the left of each section title. In Sequoia, you may then need to click on the **Refresh** tool to get that to work. When you close its main window, SilentKnight quits automatically.

→ [Release notes](#)



## Toolbar:

→ [Check All](#)

→ [List Updates](#)

→ [Save As Text](#)

→ [Install Updates](#)

→ [Export As JSON](#)

## Report:

→ [Malware protection](#)

→ [macOS & Firmware](#)

→ [Security systems](#)

→ [Reduced security](#)

→ [Updates](#)

→ [Information](#)

## Topics:

→ [FileVault](#)

→ [XProtect](#)

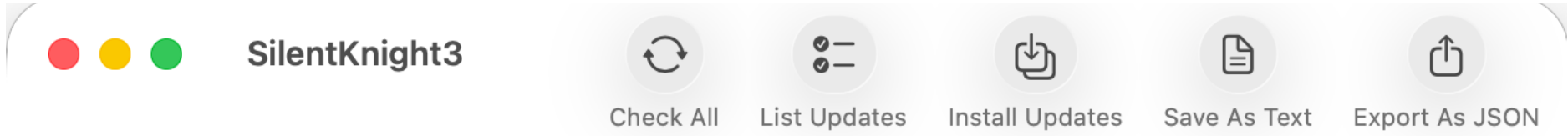
→ [XProtect Remediator](#)

→ [XProtect Remediator Scans](#)

→ [Failed updates](#)





→ [Apple silicon security on non-English systems](#)

# Check All



When you first open SilentKnight, it automatically runs the **Check All** tool in the toolbar. If that doesn't complete fully, click on the **Check All** tool to repeat those checks.

SilentKnight connects to my GitHub server and downloads details of the current versions of macOS, firmware and security data for your Mac. The app checks those 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 Those that appear to be out of date or that need attending to are prefaced by .

Once those results are shown, to check for any available updates click on the **List Updates** tool, which is now to the right of the **Check All** tool.

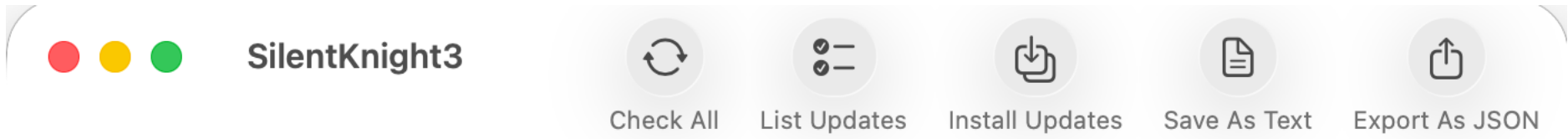
→ [List Updates](#)

→ [Install Updates](#)

→ [Save As Text](#)

→ [Export As JSON](#)

# List Updates



Click on the **List Updates** tool for SilentKnight to connect to Apple's servers and request a list of all system and security updates available for your Mac, using the following command:

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

It then analyses the list returned to see if any are macOS updates, and reports them separately. If there are updates it can install, the **Install Updates** tool is shown at the right of the toolbar, to enable you to download and install those. SilentKnight can't install macOS updates or upgrades, though: for those you'll need to use **Software Update** in System Settings. During this, a 'busy spinner' is shown at the left of the tools.

## ❗ Updates

XProtectPayloads Version: 157  
XProtectPlistConfigData Version: 5347  
❗ macOS updates found:  
macOS Tahoe 26.5.1

No updates installed yet.

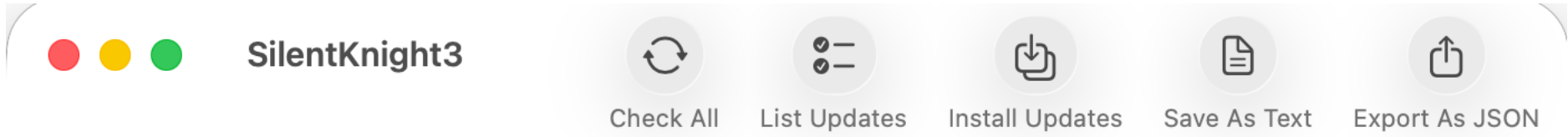
→ [Check All](#)  
→ [Updates](#)

→ [Install Updates](#)  
→ [Failed updates](#)

→ [Save As Text](#)

→ [Export As JSON](#)

# Install Updates



The **Install Updates** tool only appears when SilentKnight has found updates for your Mac that it can download and install. When you click on this button, SilentKnight runs the command:

```
softwareupdate -ia --include-config-data [list of labels]
```

with the labels for each of the updates it can install, *excluding* macOS. When those have been installed, it adds details of those installations, including any errors that may have occurred. During this, a ‘busy spinner’ is shown at the left of the tools.

## ❗ Updates

```
XProtectPayloads Version: 157
XProtectPlistConfigData Version: 5347
❗ macOS updates found:
  macOS Tahoe 26.5.1
```

```
Software Update Tool
```

```
Finding available software
```

```
Downloading XProtectPayloads
Downloading XProtectPlistConfigData
Downloaded XProtectPayloads
Downloaded XProtectPlistConfigData
Installing XProtectPayloads, XProtectPlistConfigData
Done with XProtectPayloads
Done with XProtectPlistConfigData
Done.
```

→ [Check All](#)  
→ [Updates](#)

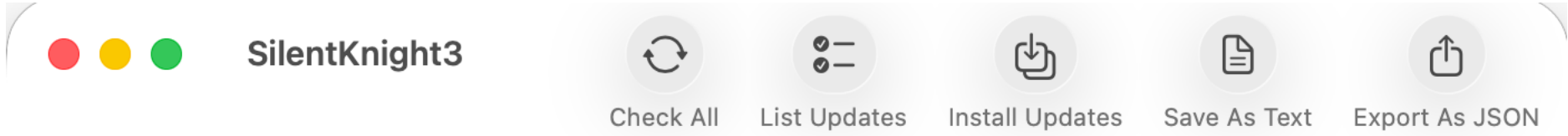
→ [List Updates](#)  
→ [Failed updates](#)

→ [Save As Text](#)

→ [Export As JSON](#)

→ [Start](#)

# Save As Text



To save the contents of SilentKnight's window, including all the results of checks as shown, click on the **Save As Text** tool. You will then be prompted to save that file using a standard Save dialog.

The text file contains the same text as displayed in the window, starting as

SilentKnight 3 Report:

🚫 Malware protection  
🚫 XProtect found 5323  
XProtect expected 5347  
XProtect last updated XProtectPlistConfigData 2025-11-11 22:09:32 +0000 : 5323  
🚫 XPR found 156  
XPR expected 157  
XPR last updated XProtectPayloads 2025-11-10 22:08:18 +0000 : 156  
👉 XPR no scans in 36 h

🚫 macOS & Firmware  
🚫 macOS found 26.1.0  
macOS expected 26.5.1  
🚫 Firmware found 13822.41.1  
Firmware expected 18000.120.36

→ [Check All](#)

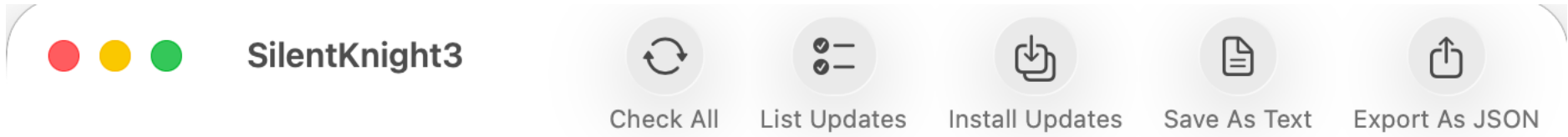
→ [List Updates](#)

→ [Install Updates](#)

→ [Export As JSON](#)

→ [Start](#)

# Export As JSON



To import the data displayed in SilentKnight's window, into a database or other app, export it by clicking on the **Export As JSON** tool. You will then be prompted to save that file using a standard Save dialog.

The JSON file contains the results used to compose the text displayed in the window, starting as

```
{
  "gateGood":true,
  "xpremFound":156,
  "xproPrefix":"🚫 ",
  "firmExpect":"18000.120.36",
  "newFound":" XProtectPayloads Version: 157\n XProtectPlistConfigData Version: 5347\n!! macOS updates found:\n\t macOS Tahoe 26.5.1\n",
  "skInfo":"SilentKnight 3.0 @ 2026-06-17T06_22_54Z",
  "malwSect":"🚫 Malware protection",
  "secSect":"✅ Security systems",
  "xpremScans":"👉 XPR no scans in 36 h",
  "remOSMaj":26,
  "firmGood":false,
  "xpremInst":"\tXProtectPayloads 2025-11-10 22:08:18 +0000 : 156",
}
```

(with newlines added for readability here). Keys are listed in a separate document supplied with the SilentKnight download.

→ [Check All](#)


→ [List Updates](#)

→ [Install Updates](#)

→ [Save As Text](#)

# Malware protection

## ✓ Malware protection

- ✓ XProtect found 5347  
XProtect expected 5347  
XProtect last updated  
XProtectPlistConfigData 2026-06-02 17:56:02 +0000 : 5347
- ✓ XPR found 157  
XPR expected 157  
XPR last updated  
XProtectPayloads 2026-02-17 18:44:33 +0000 : 157
- ✓ XPR 83 scans  3 cancelled

This displays details of the security systems in macOS to detect and (when possible) remove malware. For XProtect and XProtect Remediator (XPR) it displays the version installed on your Mac, the version it expected to find, and details of the last update installed.

The last line reports how many scans have been performed by XPR over the last 36 hours, and includes the numbers of those that were cancelled routinely, as well as any that reported detections or remediations. These can only be performed when SilentKnight is run using an admin account, and are omitted when using a standard user account.

→ [macOS & Firmware](#)    → [Security systems](#)    → [Reduced security](#)    → [Updates](#)  
→ [Information](#)    → [XProtect](#)    → [XProtect Remediator](#)    → [XProtect Remediator Scans](#)

# macOS & Firmware



This displays details of the version of macOS running, the version expected, the mBoot firmware found, and that expected.

Firmware is only updated when macOS itself is updated, not independently. The version installed will be that included with the most recent version of macOS installed on that Mac, including any installed to an external disk. Firmware updates are normally included with security updates to older major versions of macOS, as well as those for the current version of macOS.

If you install a beta-release of macOS, that may well come with a firmware update to a higher version number than the current release of macOS. SilentKnight will report those versions, but should recognise the firmware is still up to date.

→ [Malware protection](#) → [Security systems](#) → [Reduced security](#) → [Updates](#) → [Information](#)



# Security systems

## ✓ Security systems

🍏 Platform Security full.

✓ XProtect enabled.

✓ FileVault on.

Apple Silicon Security:

🍏 Secure Boot: Full Security

🍏 System Integrity Protection: Enabled

🍏 Signed System Volume: Enabled

🍏 Kernel CTRR: Enabled

🍏 Boot Arguments Filtering: Enabled

🍏 Allow All Kernel Extensions: No

User Approved Privileged MDM Operations: No

DEP Approved Privileged MDM Operations: No

These include:

- **Secure Boot**, set in Startup Security Utility in *paired* Recovery. This should normally be **Full**, but can be **Reduced** to load third-party kernel extensions, and may even be **Permissive** when SIP is disabled.
- **SIP**, controlled by `csrutil` as usual.
- **SSV**, should always be **enabled** unless running a modified version of macOS.
- Kernel CTRR and Boot Arguments should normally be **enabled**.
- **Allow All Kernel Extensions**, set in Startup Security Utility as an additional option to Reduced Security, to allow the loading of third-party extensions when required. This should normally be set to **No**.
- Privileged MDM Operations should be set to **No**.

→ [Malware protection](#)

→ [macOS & Firmware](#)

→ [Reduced security](#)

→ [Updates](#)

→ [Information](#)

→ [FileVault](#)

→ [Apple silicon security on non-English systems](#)

# Reduced security

Macs should be run with Platform Security full whenever possible. One reason for reducing that is when it's essential to use third-party kernel extensions. Those are controlled in Startup Security Utility in Recovery. If your Mac has enabled third-party kernel extensions and doesn't need to, disable them in that utility and set Secure Boot back to Full Security.

Another reason for reduced security is when you need to disable System Integrity Protection (SIP). Although it can be necessary 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
```

Quit Terminal and open Startup Security Utility, where you should set your Mac back to Full Security.

If XProtect is shown here as being disabled, Gatekeeper checks ignore the results of its malware checks.

To enable it again, try the Terminal command

```
spctl --enable
```

although that often isn't successful, and you'll then need to use

```
sudo spctl --global-enable
```

→ [Malware protection](#)

→ [macOS & Firmware](#)

→ [Security systems](#)

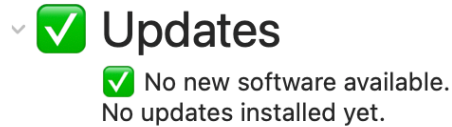
→ [Updates](#)

→ [Information](#)

→ [FileVault](#)

→ [Apple silicon security on non-English systems](#)

# Updates



This section reports the results of the **List Updates** and **Install Updates** tools.

When you click on List Updates, SilentKnight requests Apple's servers for a list of available updates for your Mac. If none are available, that's reported and no further action is needed.

When there are updates available, SilentKnight analyses the list and sorts items into two lists, those that it can download and install, and all macOS updates (apart from Safari) which it can't.

Click on Install Updates and SilentKnight then requests the list of those updates it can download and install, and reports the results in this section once that's complete. If there are also outstanding macOS updates available, you then need to use the Software Update section in System Settings to install those.

Because of the way that XProtect is now updated, its updates delivered this way don't update the primary copy of XProtect. Although you should still let SilentKnight install those updates, you may need to use the `xprotect` command in Terminal to update that primary copy of XProtect. A future version of SilentKnight should be able to do that for you.

→ [List Updates](#)      → [Install Updates](#)      → [macOS & Firmware](#)      → [Security systems](#)  
→ [Reduced security](#)      → [Failed updates](#)

# Information

## ✓ ⓘ Information

Mac mini

Model Mac16,11

Running macOS 26.5.1

Expected macOS 26.5.1

SilentKnight 3.0 @ 2026-06-14T18\_28\_13Z

This section gives useful details about your Mac:

- its regular model name
- the name used to distinguish its exact model and type
- the version of macOS it's running at the moment
- the current version of macOS it should be running
- the version of SilentKnight, and the date and time of this set of checks.

→ [Malware protection](#)

→ [macOS & Firmware](#)

→ [Security systems](#)

→ [Reduced security](#)

→ [Updates](#)

# FileVault

FileVault protects the contents of disks by encrypting them. Data volumes on the internal storage of Apple silicon Macs 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 you control in the **Privacy & Security** section of System Settings.

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.

# 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, you should enable it as soon as possible.

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 `/var/protected/xprotect/XProtect.bundle` using the command `xprotect version`. macOS Sequoia and later can only update XProtect using its command tool `xprotect`. To discover whether a newer version is available, enter into Terminal

```
sudo xprotect check
```

If that returns a version number higher than that installed and reported by SilentKnight, install that update using

```
sudo xprotect update
```

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

To check that Gatekeeper/XProtect protection is enabled, SilentKnight runs the shell command

```
spctl --status
```

which should always return that assessments are enabled.

→ [Malware protection](#)

→ [Reduced security](#)

→ [XProtect Remediator](#)

→ [XProtect Remediator Scans](#)

→ [Start](#)

# XProtect Remediator

This tool is located at `/Library/Apple/System/Library/CoreServices/XProtect.app`. It's routinely updated every month or two, 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.

→ [Malware protection](#)

→ [XProtect](#)

→ [XProtect Remediator Scans](#)

# XProtect Remediator Scans

When any of XProtect Remediator's (XPR) scanning modules completes a scan, it should write a short report in the Unified log. SilentKnight checks those log reports over the last 36 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 🔴 .

Most of those scans are run against a timer. If the scan takes longer than allowed, XPR automatically cancels further scans in that series. This is very common, and not unusual. SilentKnight now reports those cancelled scans with the 🛑 emoji symbol.

Laptop Macs can only perform scans when they're connected to mains (AC) power, and can go many days or weeks between scans if they aren't given the opportunity to do so when running awake with their power adaptor plugged in.

To obtain further information about XProtect Remediator reports, use [XProCheck](#). Security apps using Apple's Endpoint Security may be able to provide more details too.

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.

→ [Malware protection](#)

→ [XProtect](#)

→ [XProtect Remediator](#)



→ [Start](#)

# 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.

→ [List Updates](#)

→ [Install Updates](#)

→ [Updates](#)

→ [Start](#)

# 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.

→ [Security systems](#)

# Release notes

This is a bug fix to the first full release, addressing problems with disclosures in Sequoia. When running SK3 in Sequoia, you may need to click on the Refresh tool to open or close its sections correctly, after clicking on the chevron v or > at the left of each section title.

Unlike previous versions of SilentKnight, XPR scans are checked whenever the **Check All** tool is clicked. However, they can only be checked when SilentKnight is run from an admin account, as that's required to obtain the log entries required.

Because SilentKnight now excludes any macOS updates from those that it downloads and installs, there currently isn't a separate feature to download and install named updates. I don't intend adding that for the moment. If that's a problem for you, please let me know.

Currently, XProtect updates to the 'new' location still have to be run manually in Terminal. I intend adding that using a privileged helper in a future release.

## SilentKnight3 version 3.01

- addresses a bug that prevented disclosures from working reliably in Sequoia.

## SilentKnight3 version 3.0

- excluded Safari updates from those recognised as macOS updates; this should ensure that standalone Safari updates are also installed
- slower processes now moved to background threads with busy spinner
- refactored app status flags
- now automatically runs Check All when opening its window.

## Beta 2 (build 24)

- added text and JSON export
- improved compatibility with standard user mode.

## Beta 1 (build 20)

- first release.