



VPN Client Repair User Guide

CUSTOMER GUIDE

Applies to VPN Client Repair 0.1.5 for macOS 13 or later.

VPN Client Repair identifies and safely cleans up incomplete Cisco Secure Client or Cisco AnyConnect VPN installations on a Mac. It can also inspect a Cisco installer before you use it. The app preserves Cisco Secure Endpoint and stops when it cannot verify that a repair action is safe.

Important: A repair can remove the Cisco VPN module and disconnect an active VPN or remote-support session. Read the proposed actions before approving a repair. On a work- or school-managed Mac, contact your IT administrator instead.

Quick start

You need macOS 13 or later, an Apple silicon or Intel Mac, the license key supplied with your purchase, and an administrator account for repair operations. An internet connection is not required to activate, scan, or repair.

1. Install VPN Client Repair

- 1 Download **VPN-Client-Repair-0.1.5.dmg** from the official download page supplied with your purchase.
- 2 Double-click the downloaded DMG.
- 3 Drag **VPN Client Repair** into the **Applications** folder shown in the DMG window.
- 4 Eject the **VPN Client Repair** disk image.
- 5 Open **Applications**, then double-click **VPN Client Repair**.
- 6 At the standard macOS first-launch message, confirm that the app is from **RJ Autonomous L.L.C.**, then click **Open**.

The app is signed with an Apple Developer ID and notarized by Apple. If macOS instead says the app is damaged, from an unidentified developer, or dangerous, do not bypass the warning. Delete that copy, download it again from the official source, and follow Verify the download.

2. Activate the app

- 1 Copy the license key included with your purchase.
- 2 Enter it using the format **XXX-XXXX-XXXX**.
- 3 Click **Activate**.

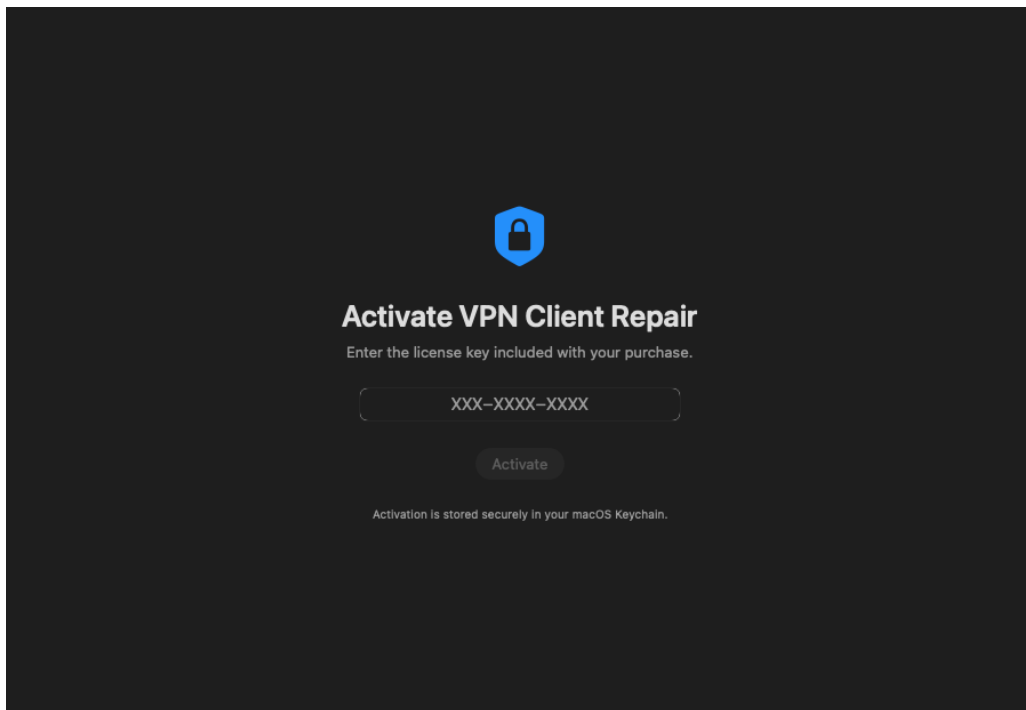


Figure 1. Enter the purchase key, including both hyphens, and click Activate.

The letters are not case-sensitive, but the hyphens are required. The app saves an activation marker in the macOS Keychain on that Mac; it does not store the license key itself. On another Mac, enter the same purchase key to activate that installation.

Never send your license key or administrator password in a support request.

3. Scan and review the result

The first scan begins automatically after activation. To scan again, click **Scan** in the upper-right corner.

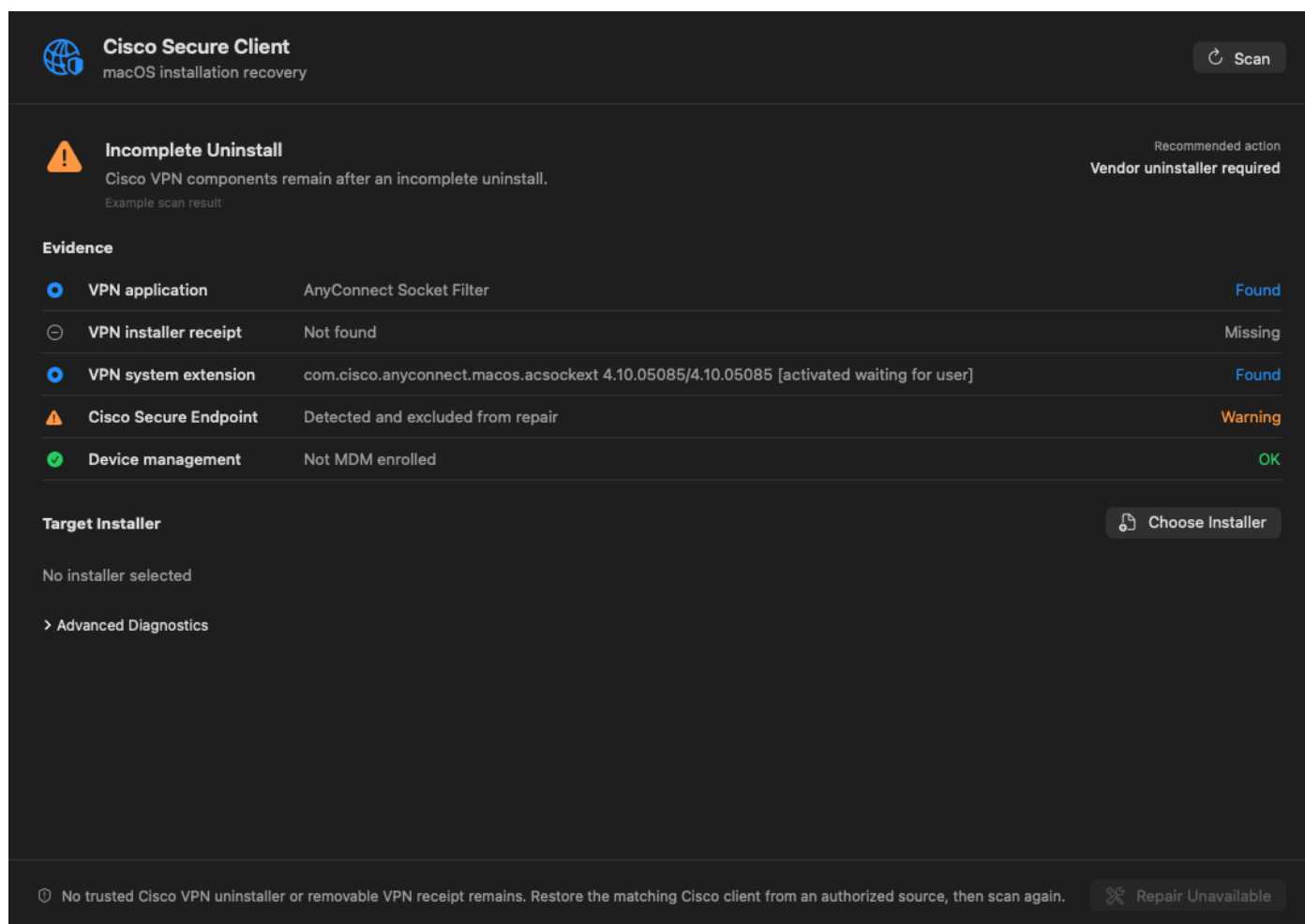


Figure 2. Review the overall status, recommended action, Evidence section, and message beside the repair button. Your results will depend on the Cisco components installed on your Mac.

Scanning is read-only and does not require administrator authorization. Before doing anything else:

- 1 Read the overall result near the top of the window.
- 2 Read the **Recommended action** on the right.
- 3 Review all five Evidence rows.
- 4 If needed, expand **Advanced Diagnostics** for exact package, extension, and file details.
- 5 Only continue if a repair button is available and you understand the proposed action.

Found is evidence, not necessarily an error. The overall result and recommended action determine whether a repair is appropriate.

4. Review and run a repair

- 1 Save your work and disconnect from Cisco VPN if practical.
- 2 Run a fresh scan.
- 3 Click **Repair VPN Installation** or **Repair Receipt**.
- 4 Read every item in the **Review VPN Repair** window.
- 5 If warned about a possible disconnection, select the acknowledgement checkbox.

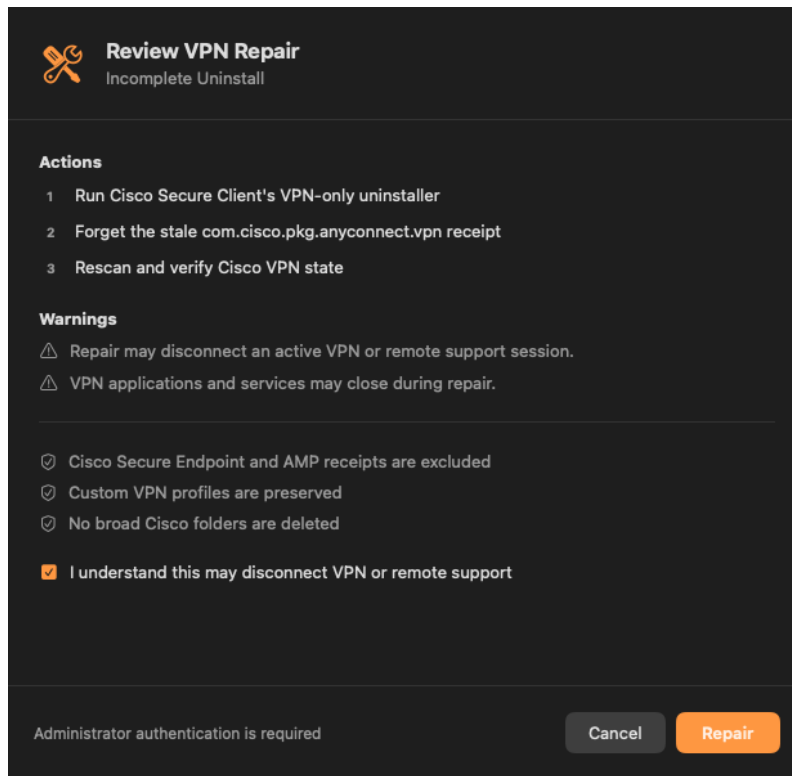


Figure 3. Confirm the exact actions, warnings, and protected Cisco components before continuing.

- 6 Click **Repair**.
- 7 macOS will display its administrator-authorization dialog. Enter an administrator account name and password there.
- 8 Wait while the app repairs and rescans the Mac.

The password is handled by macOS. VPN Client Repair does not receive or store it. Cancelling the macOS authorization dialog prevents the repair from running.

Depending on the detected state, repair may run Cisco's protected VPN-only uninstaller and/or forget a stale VPN package receipt. It does not broadly delete Cisco folders. Cisco Secure Endpoint and AMP receipts are excluded, and custom VPN profiles are preserved when Cisco's uninstaller leaves them in place.

After repair:

- **Cisco VPN cleanup completed successfully:** no remaining VPN installation state was detected.
- **Repair finished, but Cisco VPN components still require review:** safe actions completed, but something remains. Read the new evidence before taking another action.
- **Administrator authorization failed:** the request was cancelled, credentials were not accepted, or a protected repair step failed. Read the complete message and scan again before retrying.

Scan-result reference

Result	Meaning	What to do
Not Installed	No Cisco VPN installation state was detected.	No repair is needed.
Installed	The Cisco VPN application and installer receipt are present.	Repair is optional. Review the actions carefully because continuing can remove the VPN module.
Stale Receipt Detected	The VPN application is gone, but its installer receipt remains.	Review and run Repair Receipt if available.
Incomplete Uninstall	One or more Cisco VPN components remain after an uninstall.	Run the offered repair, or follow the vendor-uninstaller instructions if repair is unavailable.
Administrator Managed	macOS reports that the Mac is managed by an organization.	Contact the device administrator. The app will not repair this state.
Manual Review Required	The app could not classify the state safely.	Do not force a cleanup. Review diagnostics and contact support or your IT administrator.

Evidence and diagnostics

The Evidence section reports:

- **VPN application:** Known Cisco Secure Client or AnyConnect applications found on the Mac.
- **VPN installer receipt:** The macOS installation receipt for the Cisco VPN module.
- **VPN system extension:** The registered Cisco VPN network extension and its current state.
- **Cisco Secure Endpoint:** Cisco's endpoint-security product. It is shown as a warning because VPN Client Repair deliberately excludes it from repair.
- **Device management:** Whether the Mac appears to be enrolled in mobile-device management (MDM).

Expand **Advanced Diagnostics** to view exact receipts, system-extension identifiers, versions, and known Cisco filesystem locations detected by the scan.

Optional: inspect a Cisco installer

Choose Installer is an optional safety check for a Cisco .dmg or .pkg file. It does not install Cisco software.

- 1 Click **Choose Installer**.
- 2 Select the Cisco DMG or PKG obtained from Cisco or your organization.
- 3 Confirm that **Image** says **Verified** and **Signature** says **Valid Cisco signature**.
- 4 Review the compatibility guidance for the installed macOS release.
- 5 If the signature is invalid, unavailable, or belongs to another developer, do not install the package.

The app recognizes Cisco packages by Cisco's signing Team ID, DE8Y96K9QP. Inspection does not guarantee that a package is appropriate for your organization; follow your IT administrator's deployment instructions.

When repair is unavailable

The repair button is intentionally disabled when the app cannot identify a safe automatic action.

Vendor uninstaller required

This means Cisco VPN components remain, but the matching protected Cisco uninstaller is missing or could not be verified.

- 1 Obtain the matching official Cisco Secure Client or AnyConnect installer from Cisco or your organization.
- 2 Use **Choose Installer** to inspect the file.
- 3 If the app reports a valid Cisco signature and the package is appropriate for the Mac, install it using Cisco's instructions. Selecting it inside VPN Client Repair only inspects it; it does not install it.
- 4 Open VPN Client Repair and click **Scan** again.
- 5 If repair becomes available, review and run it.

Do not download Cisco installers from unofficial websites, manually delete system-extension files, disable System Integrity Protection (SIP), or bypass Gatekeeper to complete a cleanup.

Managed Mac

If **Device management** reports MDM enrollment, VPN Client Repair will not perform a repair. Contact the organization that manages the Mac. Local changes might violate policy or be restored automatically.

Cisco Secure Endpoint warning

This warning is informational. The app detected Cisco Secure Endpoint and will leave it untouched. Do not try to remove Secure Endpoint as part of a VPN repair.

Verify the download

The SHA-256 checksum confirms that the downloaded DMG matches the published release file.

For VPN Client Repair 0.1.5, the expected value is:

```
1cfb91235c7db18c1691b760fc8fa00a091b90eebcee75072d9f83ca7d6d9eb6
```

To check it:

- 1 Open **Terminal**.
- 2 Run:

```
shasum -a 256 ~/Downloads/VPN-Client-Repair-0.1.5.dmg
```
- 3 Compare the value printed by Terminal with the expected value above. Every character must match.

If the values do not match, do not open the DMG. Delete it and download a new copy from the official source.

Troubleshooting

The license key is rejected

- Confirm the key uses the format XXX-XXXX-XXXX.
- Include the hyphens and check for missing or extra characters.
- Copy the key directly from the purchase message when possible.
- If activation reports a Keychain error, unlock the login Keychain and try again.

The scan is unavailable or does not finish

- Quit and reopen VPN Client Repair.
- Click **Scan** again.
- Restart the Mac if macOS is still completing a Cisco installation or uninstall.
- If the problem continues, collect the information listed under Getting support.

The repair button is grey

Read the message beside the button and **Recommended action** at the top. Common reasons include a missing trusted Cisco uninstaller, MDM enrollment, unavailable device-management status, or a state that does not need repair.

A system extension says "waiting for user"

Do not force-delete it. Restore the matching signed Cisco software or uninstaller from an authorized source, then follow **Vendor uninstaller required** above. On a managed Mac, contact IT.

Administrator authorization fails

- Confirm that you are using credentials for an administrator account on the Mac.
- If you cancelled the dialog, scan again and restart repair when ready.
- If the message identifies a Cisco uninstaller or package-receipt failure, do not manually delete files. Scan again and contact support with the exact error text.

macOS blocks the app

Do not use Terminal commands or security-setting changes to bypass the warning. Confirm that the DMG came from the official source, verify its SHA-256 checksum, and check that macOS identifies **RJ Autonomous L.L.C.** as the developer.

Privacy and security

VPN Client Repair 0.1.5 performs activation, scanning, installer inspection, and repair locally on the Mac. It does not include analytics, advertising, or an online account login.

The app:

- Stores only an activation marker in the macOS Keychain, not the entered license key.
- Does not store the administrator password; macOS handles authorization.
- Mounts a selected DMG read-only for inspection and removes temporary inspection files afterward.
- Accepts only specifically approved, protected Cisco VPN uninstaller paths for privileged repair.
- Stops instead of running an untrusted or unexpectedly located uninstaller.
- Does not intentionally modify Cisco Secure Endpoint or AMP.

Remove VPN Client Repair

- 1 Quit VPN Client Repair.
- 2 Open **Applications**.
- 3 Move **VPN Client Repair** to the Trash.
- 4 Empty the Trash if desired.

Removing VPN Client Repair does not reinstall Cisco VPN software or reverse a completed repair. Its local activation marker may remain in Keychain. To remove that marker too, open **Keychain Access**, search for `com.rjautonomous.vpnclientrepair.license`, and delete the matching item.

Getting support

Provide the following through the support channel listed on the official download page:

- Mac model and whether it uses Apple silicon or Intel
- macOS version
- VPN Client Repair version
- Overall scan result and recommended action
- Exact error message, if any
- A screenshot of Evidence and Advanced Diagnostics after hiding personal or organization-sensitive information

Do not send your license key, macOS password, VPN credentials, private configuration profiles, or confidential organization information.

Trademark notice

VPN Client Repair is an independent utility and is not affiliated with, endorsed by, or sponsored by Cisco Systems, Inc. Cisco, Cisco Secure Client, AnyConnect, and Cisco Secure Endpoint are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates. Other names may be trademarks of their respective owners.