

Sammeln von KDF-Protokollen für Secure Client unter Windows und MacOS

Inhalt

[Einleitung](#)

[Windows- und MacOS-FLAGS](#)

[KDF-Protokolle, Wireshark und DART-Paket sammeln](#)

[Windows](#)

[MacOS](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie KDF-Protokolle und andere wichtige Fehlerbehebungsprotokolle unter Windows und MacOS gesammelt werden.

Windows- und MacOS-FLAGS

DNS-bezogen (bei OpenDNS):	0 x 20801 FF
Webflow-Proxy (SWG) und DNS-bezogen:	0 x 70 C01FF
ZTA	0x400080152

KDF-Protokolle, Wireshark und DART-Paket sammeln



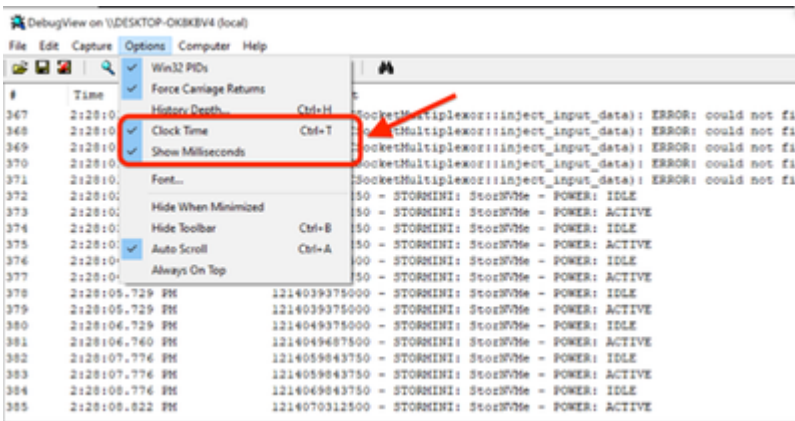
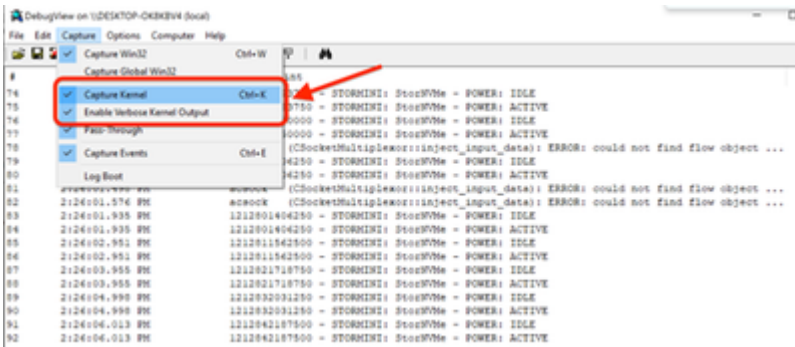
Anmerkung: Teilen Sie dem TAC-Team bei der Übermittlung der Ergebnisse stets mit, welche Einstellungen verwendet wurden, und seien Sie offen für Änderungen entsprechend den Anforderungen des TAC.

Windows

Öffnen Sie einen CMD mit Administratorberechtigungen, und führen Sie den folgenden Befehl aus:

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf [FLAG]
```

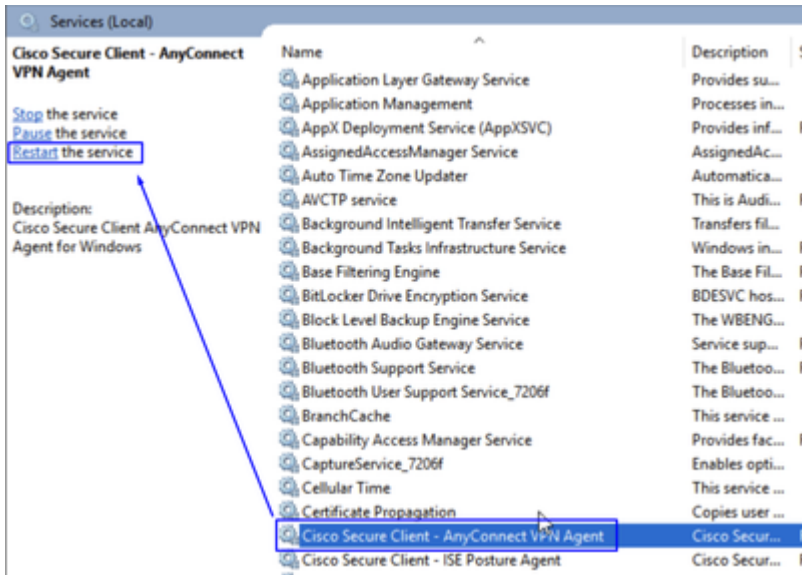
- [DebugView](#) von SysInternal herunterladen, um das KDF-Protokoll zu erfassen
- Führen Sie DebugView als aus administrator, und aktivieren Sie die nächsten Menüoptionen:
- Auf Erfassung klicken
 - Markierung Capture Kernel
 - Markierung Enable Verbose Kernel Output
- Optionen
 - Markierung Clock Time
 - Markierung Show Milliseconds



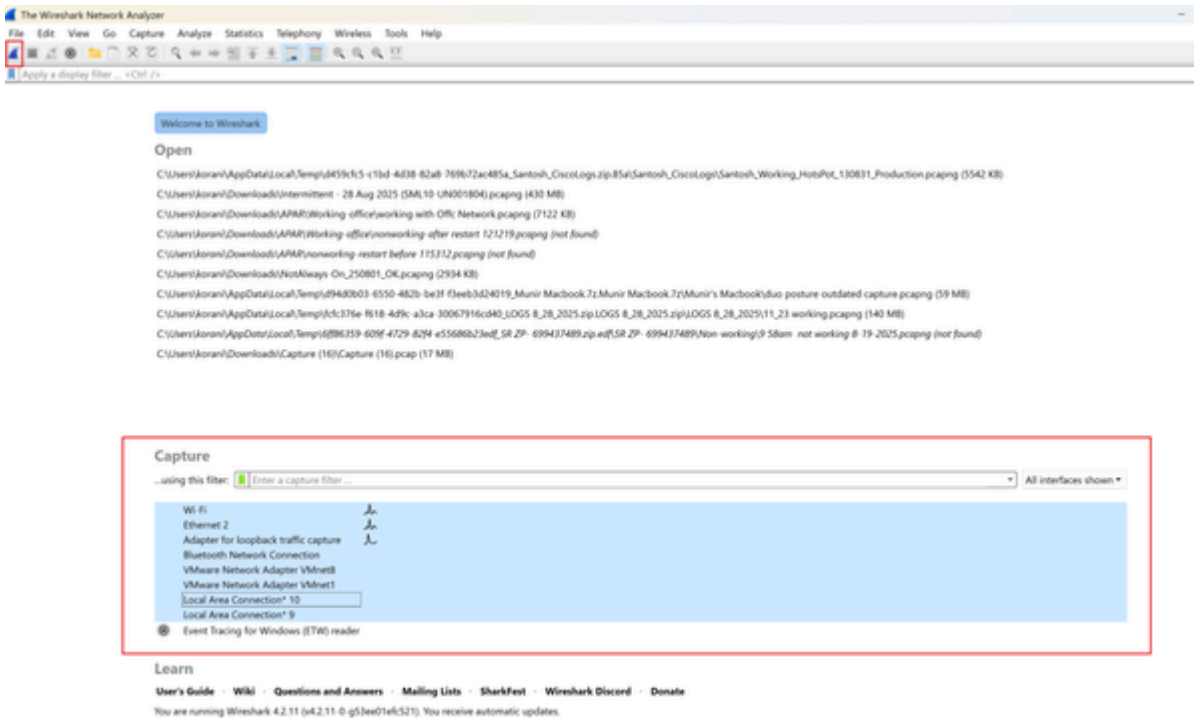
- Starten Sie den Client-Dienst über die Admin-Eingabeaufforderung neu:

```
net stop csc_vpnagent && net start csc_vpnagent
```

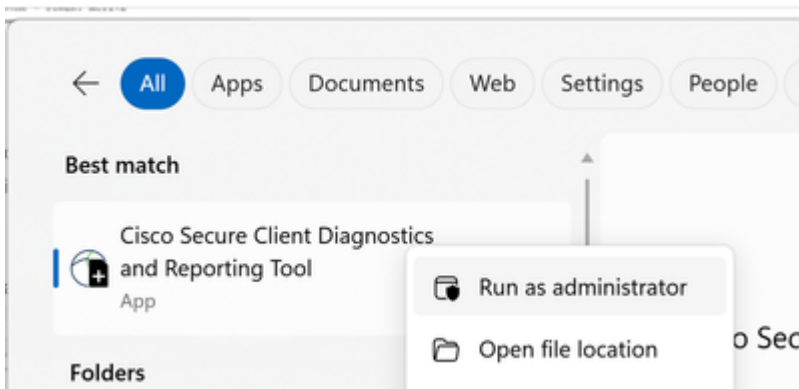
- Wenn net stop csc_vpnagent && net start csc_vpnagent nicht funktioniert, starten Sie den Dienst von services.msc neu Cisco Secure Client.



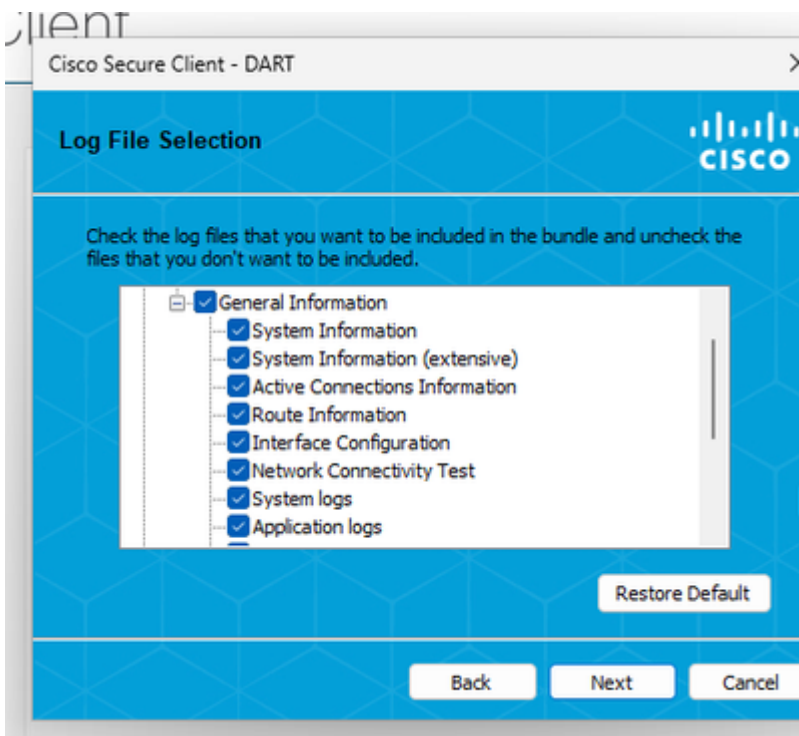
- Start Wireshark Capture
- Wählen Sie alle Schnittstellen aus, und starten Sie die Paketerfassung.



- Reproduzieren Sie das Problem, speichern KDF Logs Sie es und Wireshark Capture und befolgen Sie dann die Schritte zur Erfassung DART Bundle
- Öffnen Sie das Cisco Secure Client Diagnostics & Reporting Tool (DART) mit Administratorrechten.



- Klicken Sie Custom
 - Einschließen System Information Extensive und Network Connectivity Test



Anmerkung: Sammeln Sie alle Protokolle, KDF-Protokolle, Wireshark Capture und DART-Pakete bis zum TAC-Gehäuse.

- Um die KDF-Protokollierung unter Windows zu beenden, verwenden Sie den folgenden Befehl:

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

MacOS

Öffnen Sie Terminal und folgen Sie der nächsten Befehlskette, um KDF Logging unter MacOS zu aktivieren:

- Stop Service

```
sudo "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app/Contents/MacOS/Cisco
```

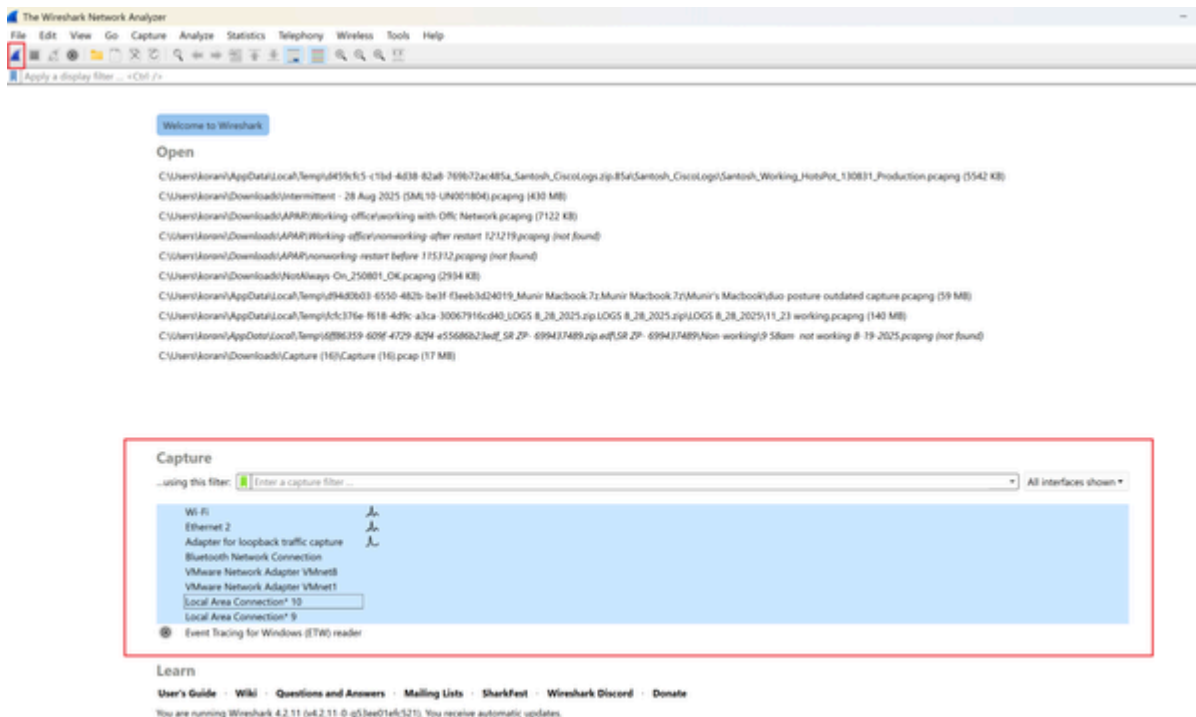
- Enable Flag

```
echo debug=[Flag Value] | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

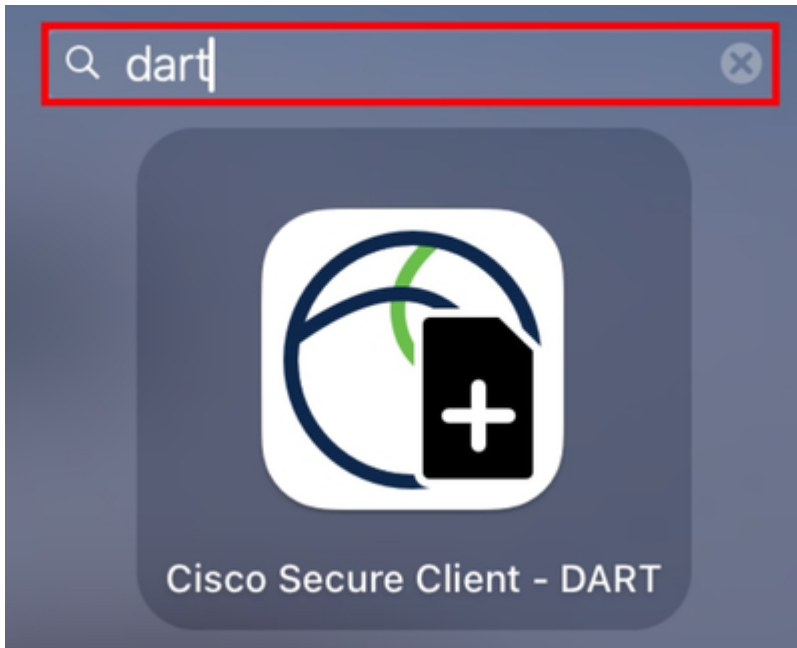
- Start Service

```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

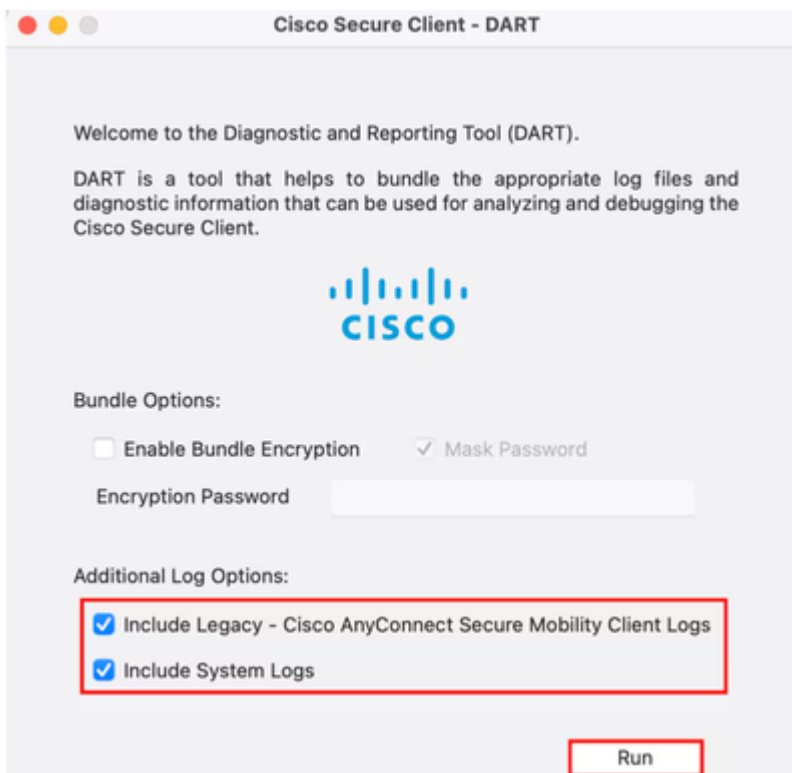
- Start Wireshark Capture
- Wählen Sie alle Schnittstellen aus, und starten Sie die Paketerfassung.



- Reproduzieren Sie das Problem, speichern KDF Logs Sie es und Wireshark Capture und befolgen Sie dann die Schritte zur Erfassung DART Bundle
- Öffnen Sie Cisco Secure Client - DART



- Markieren Sie die nächsten Optionen:
 - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
 - Include System Logs
- Klicken Sie auf Run



Anmerkung: Sammeln Sie alle Protokolle, KDF-Protokolle, Wireshark Capture und DART-Pakete bis zum TAC-Gehäuse.

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Cisco Secure Access-Hilfecenter](#)
- [Cisco SASE Designleitfaden](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.