KDF-logboeken verzamelen voor beveiligde client op Windows en MacOS

Inhoud

Inleiding

In dit document wordt beschreven hoe u KDF-logs en andere belangrijke logboeken voor probleemoplossing kunt verzamelen op Windows en MacOS.

Windows- en MacOS-vlaggen

DNS-gerelateerd (wanneer OpenDNS is betrokken):	0x20801FF
Web flow (SWG) proxy en DNS Gerelateerd:	0x70C01FF
ZTA	0x400080152

KDF-logboeken, Wireshark- en DART-bundel verzamelen

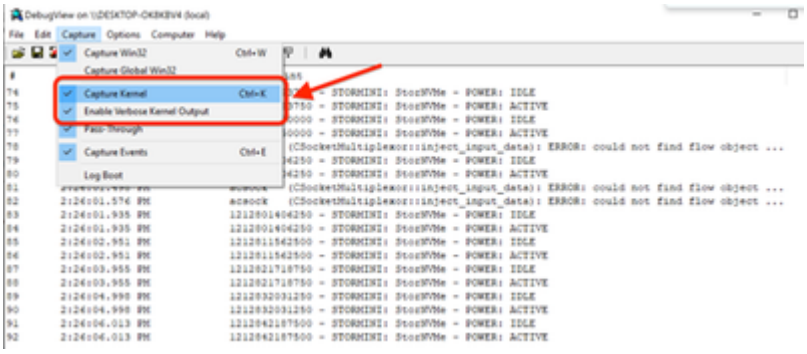
Opmerking: wanneer u de resultaten indient, laat het TAC-team altijd weten welke instellingen zijn gebruikt en sta open voor het wijzigen van TAC's.

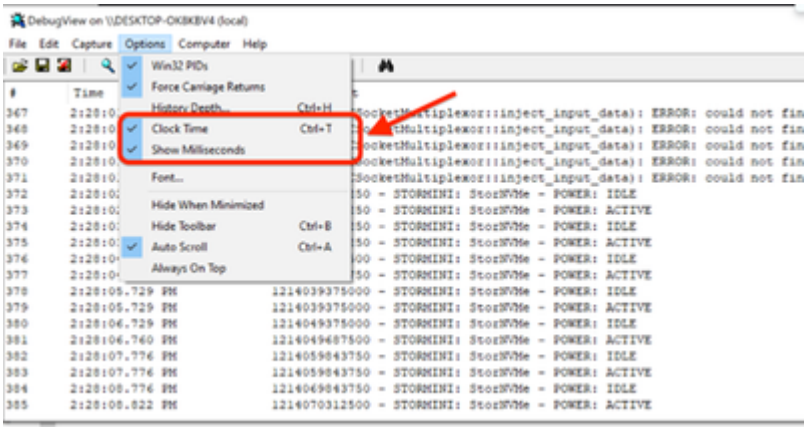
Windows

Open een CMD met beheerdersbevoegdheden en voer de volgende opdracht uit:

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

- Download DebugView van SysInternal om het KDF-log vast te leggen
- Uitvoeren DebugView als administrator en de volgende menuopties inschakelen:
- Klik op Capture
    - vinkje Capture Kernel
    - vinkje Enable Verbose Kernel Output
- Opties
    - vinkje Clock Time
    - vinkje Show Milliseconds

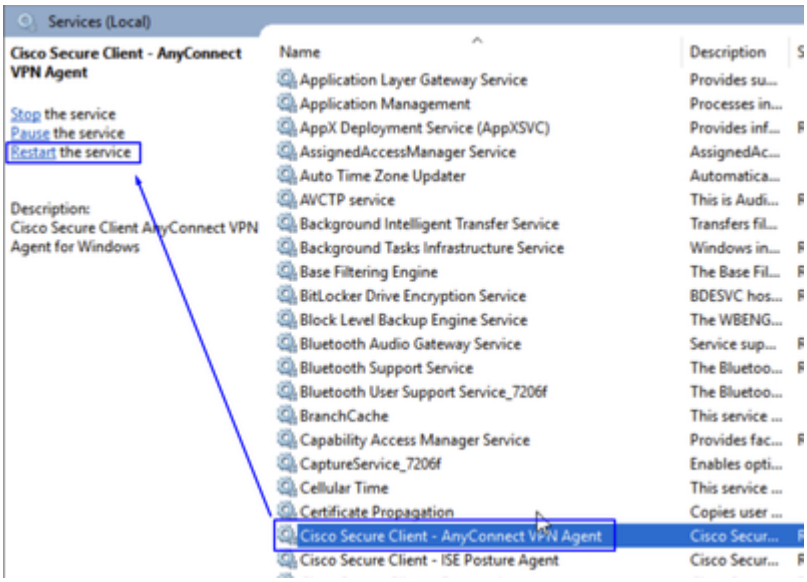




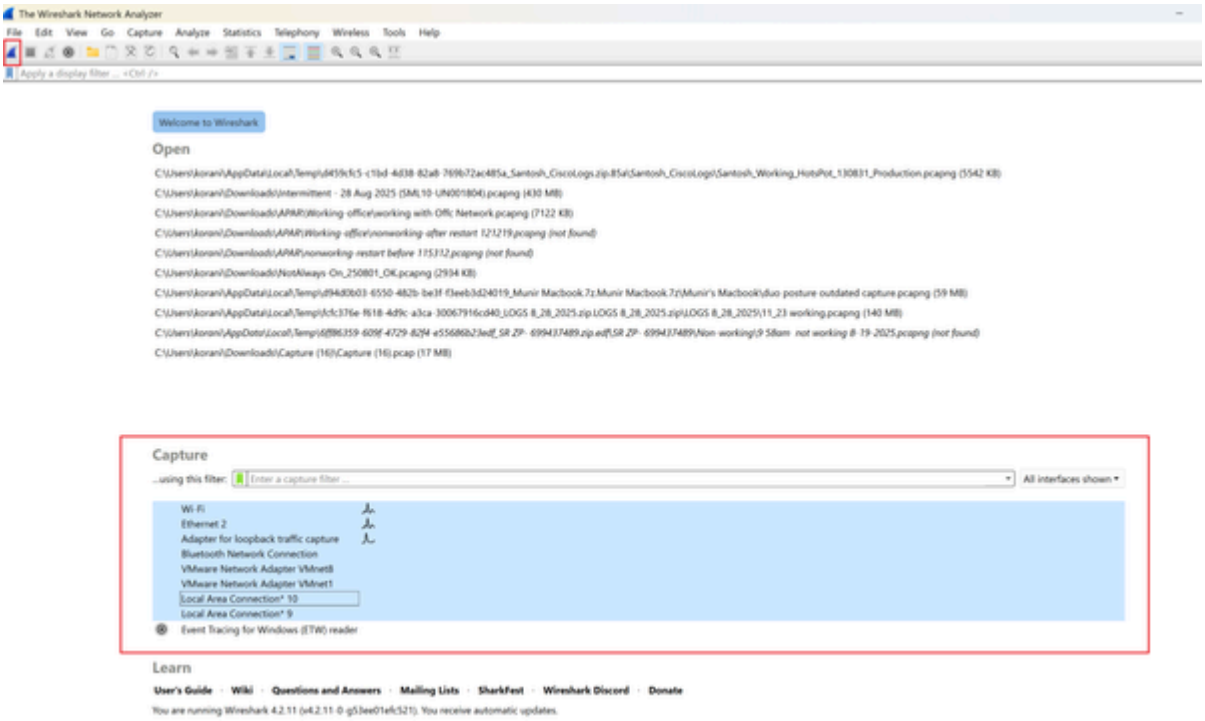
- Start de clientservice opnieuw op via de beheerdersprompt:

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

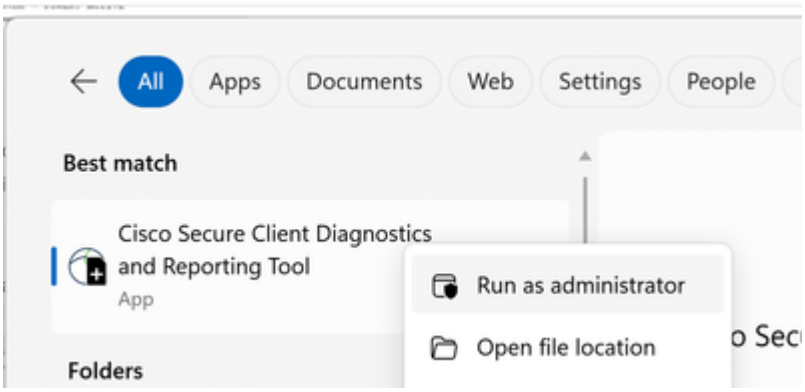
- Als dit net stop csc_vpnagent && net start csc_vpnagent niet werkt, start u de service opnieuw Cisco Secure Client op via services.msc



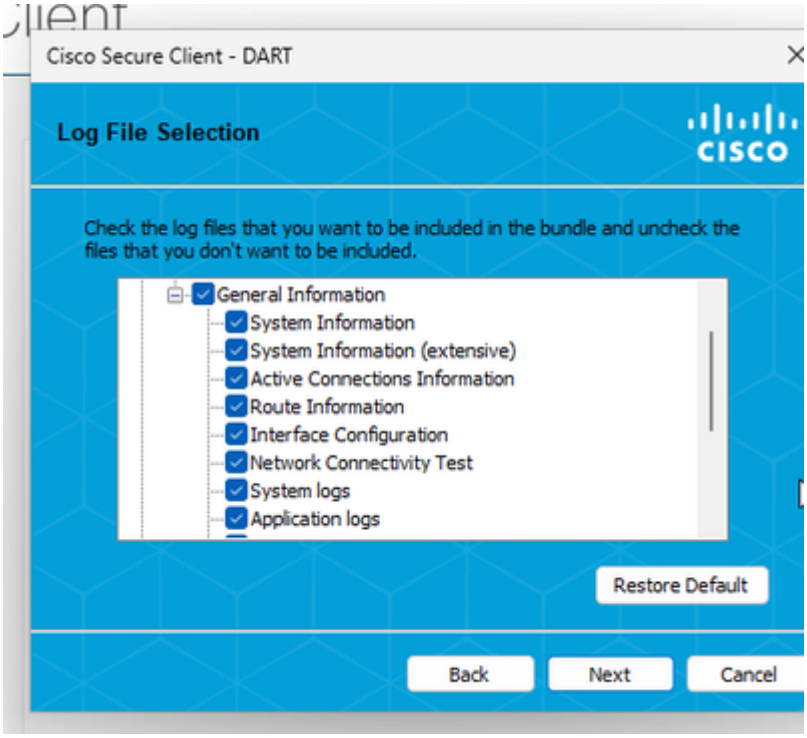
- starten Wireshark Capture
- Selecteer alle interfaces en start de pakketopname



- Reproduceer het probleem en sla op KDF Logs en Wireshark Capturevolg de stappen om vast te leggen DART Bundle
- Open de Cisco Secure Client Diagnostics & Reporting Tool (DART) met beheerdersbevoegdheden



- Klik op Custom
  - Inclusief System Information Extensive en Network Connectivity Test



Opmerking: Verzamel alle logs, KDF-logs, Wireshark Capture en DART-bundel voor de TAC-case.

- Als u de KDF-aanmelding in Windows wilt stoppen, gebruikt u de volgende opdracht:

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

MacOS

Open terminal en volg de volgende opdrachtketen om KDF Logging op MacOS in te schakelen:

- Stop Service

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

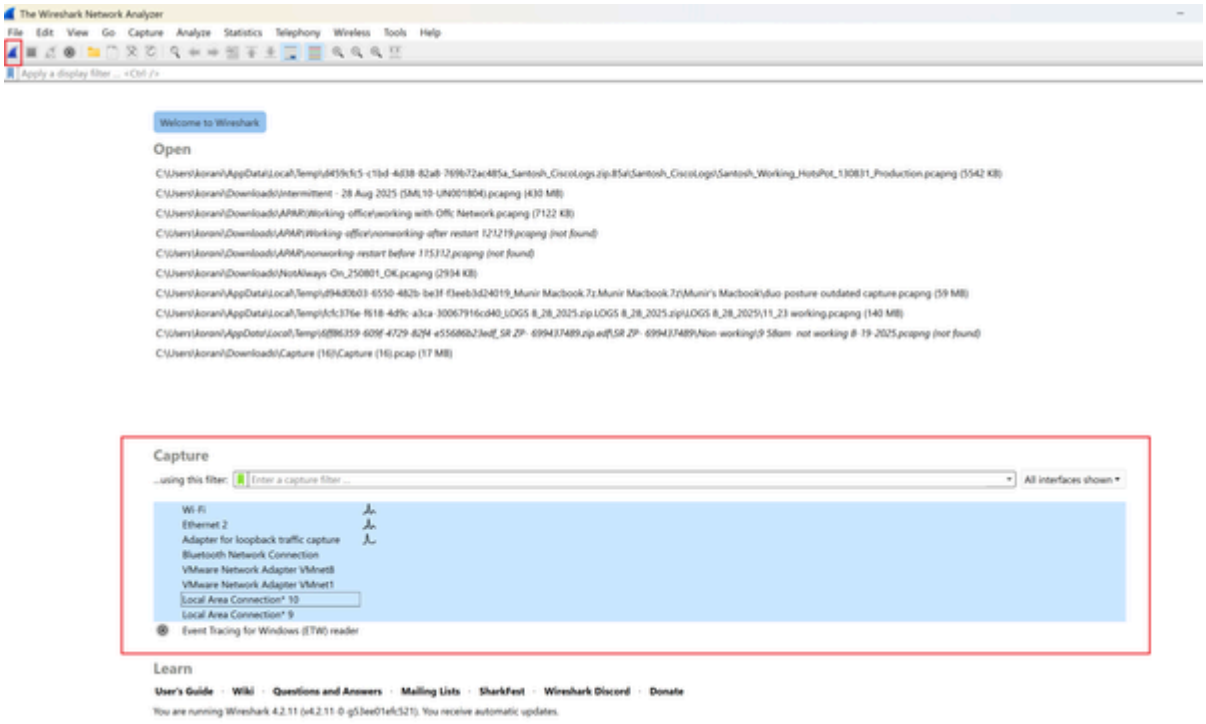
- Enable Flag

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

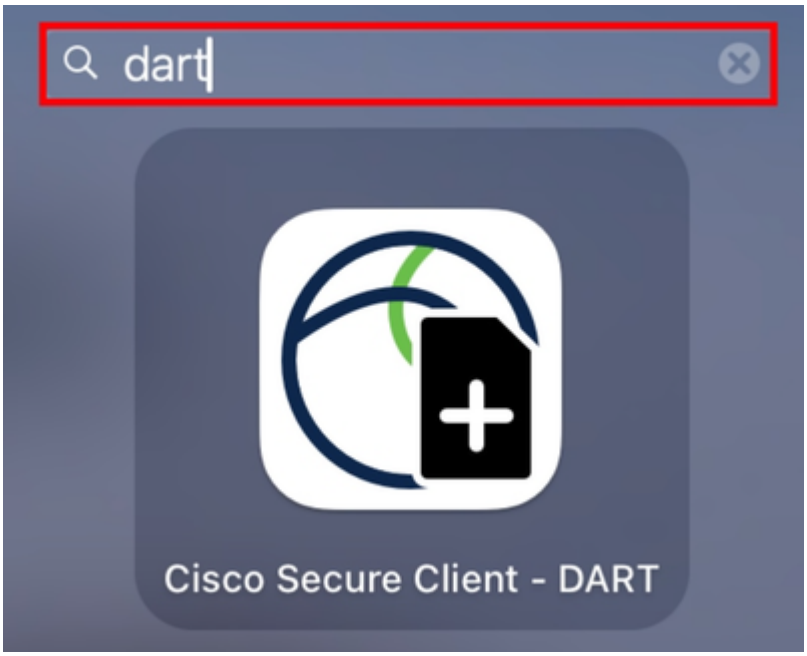
- Start Service

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

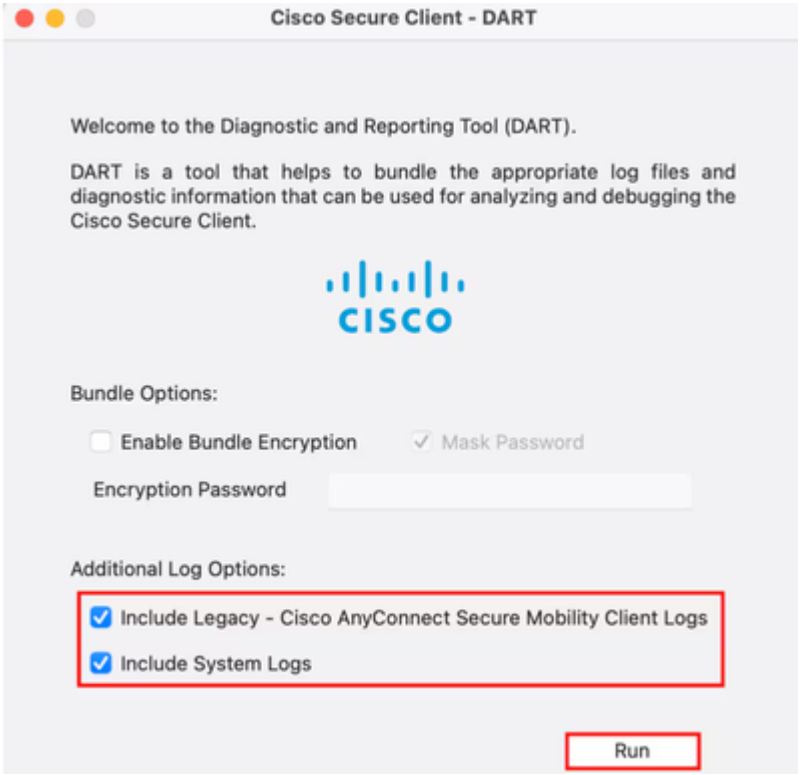
- starten Wireshark Capture
- Selecteer alle interfaces en start de pakketopname



- Reproduceer het probleem en sla op KDF Logs en Wireshark Capturevolg de stappen om vast te leggen DART Bundle
- Open de Cisco Secure Client - DART



- Selecteer de volgende opties:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- Klik op de knop Run



Opmerking: Verzamel alle logs, KDF-logs, Wireshark Capture en DART-bundel voor de TAC-case.

Gerelateerde informatie

- Cisco Technical Support en downloads
- Cisco Secure Access Help Center
- Cisco SASE-ontwerphandleiding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.