Collecting KDF Logs for Secure Client on Windows and MacOS

Contents

Introduction

This document describes how to collect KDF logs and other important troubleshooting logs on Windows and MacOS.

Windows and MacOS FLAGS

DNS Related (When OpenDNS is involved):	0x20801FF
Web flow (SWG) proxy and DNS Related:	0x70C01FF
ZTA	0x400080152

Colleting KDF Logs, Wireshark and DART Bundle

Note: When you submit the results, always let the TAC Team know what settings were used and be open to changing as TAC requires.

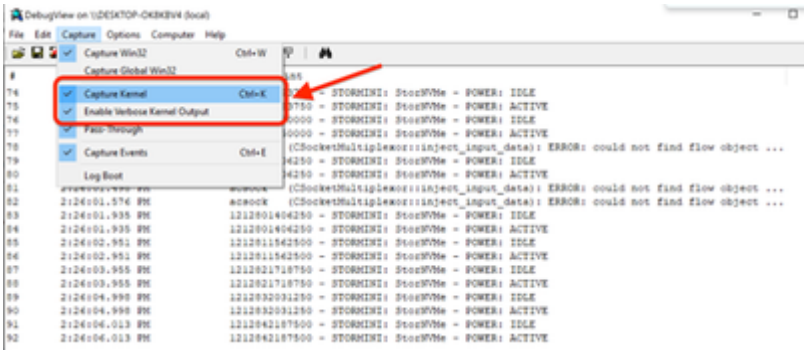
Windows

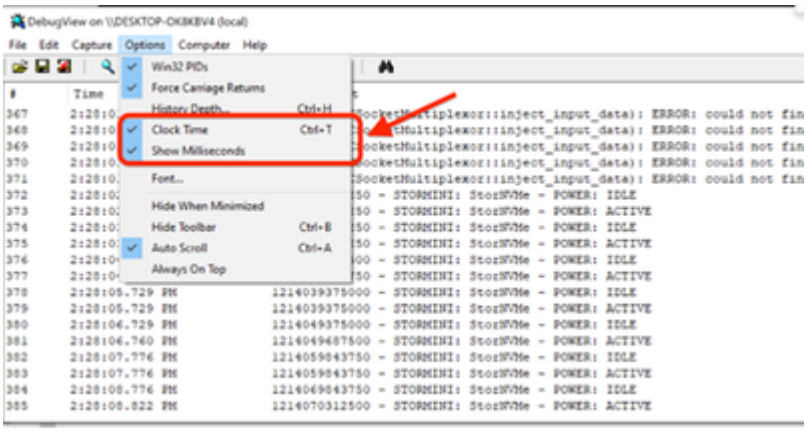
Open a CMD with admin privileges and run the next command:

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

- Download DebugView from SysInternal to capture the KDF log
- Run DebugView as administrator and enable the next menu options:
- Click on Capture

    - Checkmark Capture Kernel
    - Checkmark Enable Verbose Kernel Output
- Options
    - Checkmark Clock Time
    - Checkmark Show Milliseconds

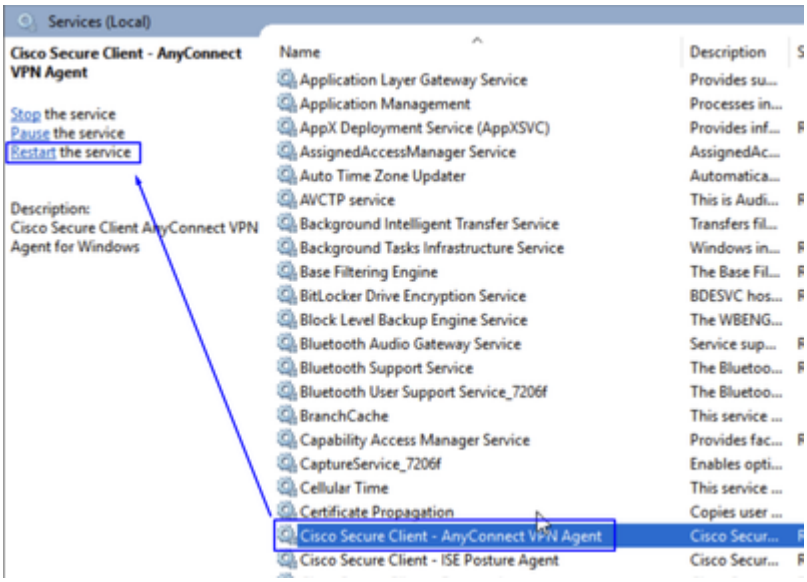




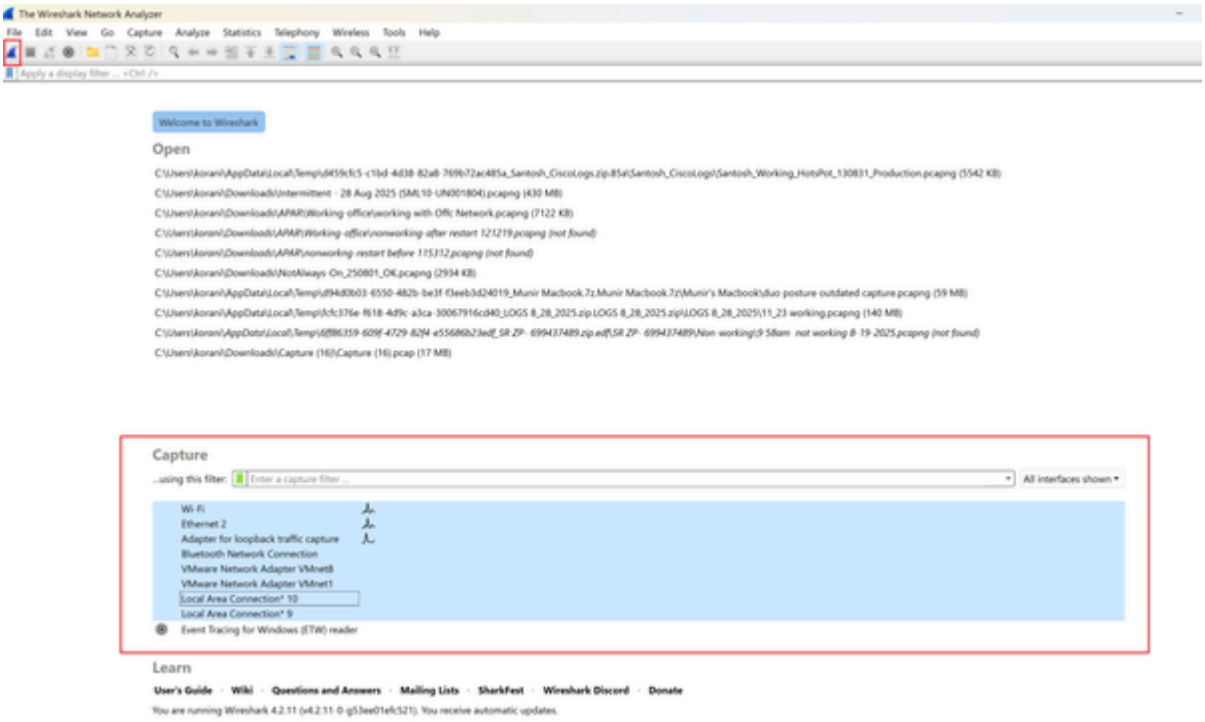
- Restart the client service via admin prompt:

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

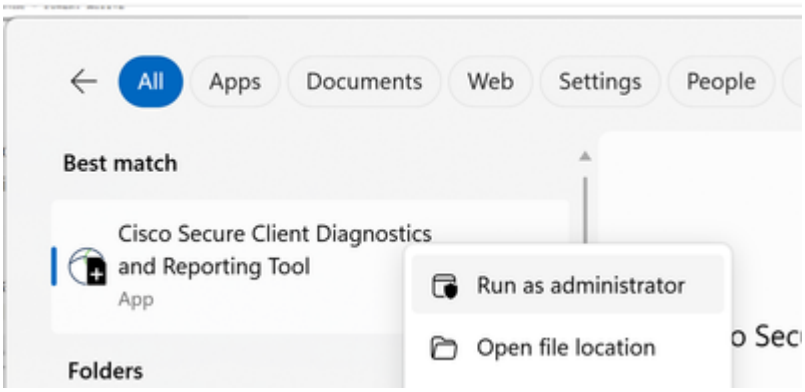
- If net stop csc_vpnagent && net start csc_vpnagent does not work, restart Cisco Secure Client service from services.msc



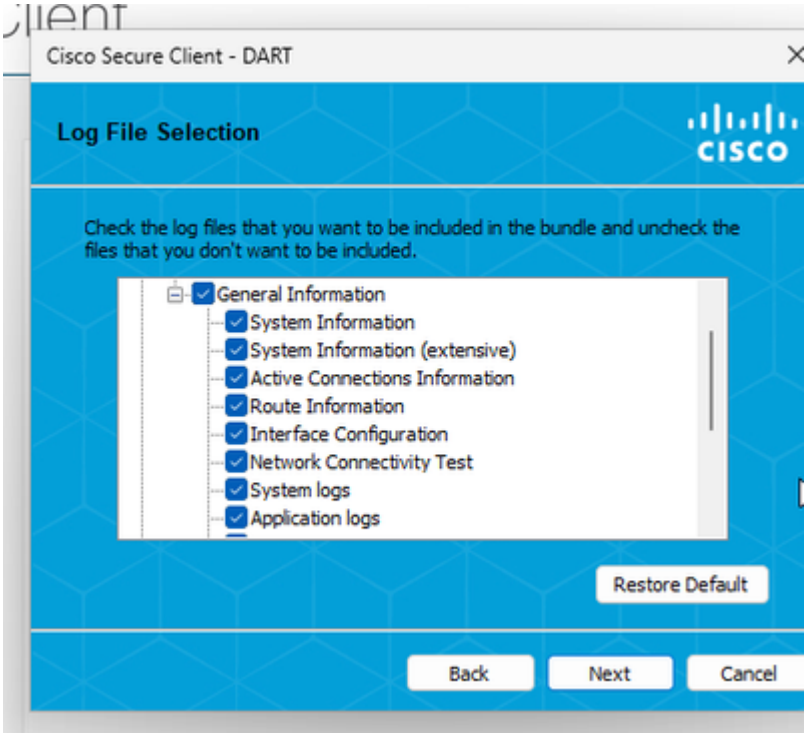
- Start Wireshark Capture
- Select all the interfaces, and start the packet capture



- Reproduce the issue, and save KDF Logs and Wireshark Capture, then follow the steps to capture DART Bundle
- Open the Cisco Secure Client Diagnostics & Reporting Tool (DART) with administrator privileges



- Click on Custom
  - Include System Information Extensive and Network Connectivity Test



Note: Collect all the logs, KDF Logs, Wireshark Capture and DART Bundle to the TAC Case.

- To stop the KDF logging on Windows use the next command:

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

MacOS

Open terminal and follow the next command chain to enable KDF Logging on MacOS:

- Stop Service

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

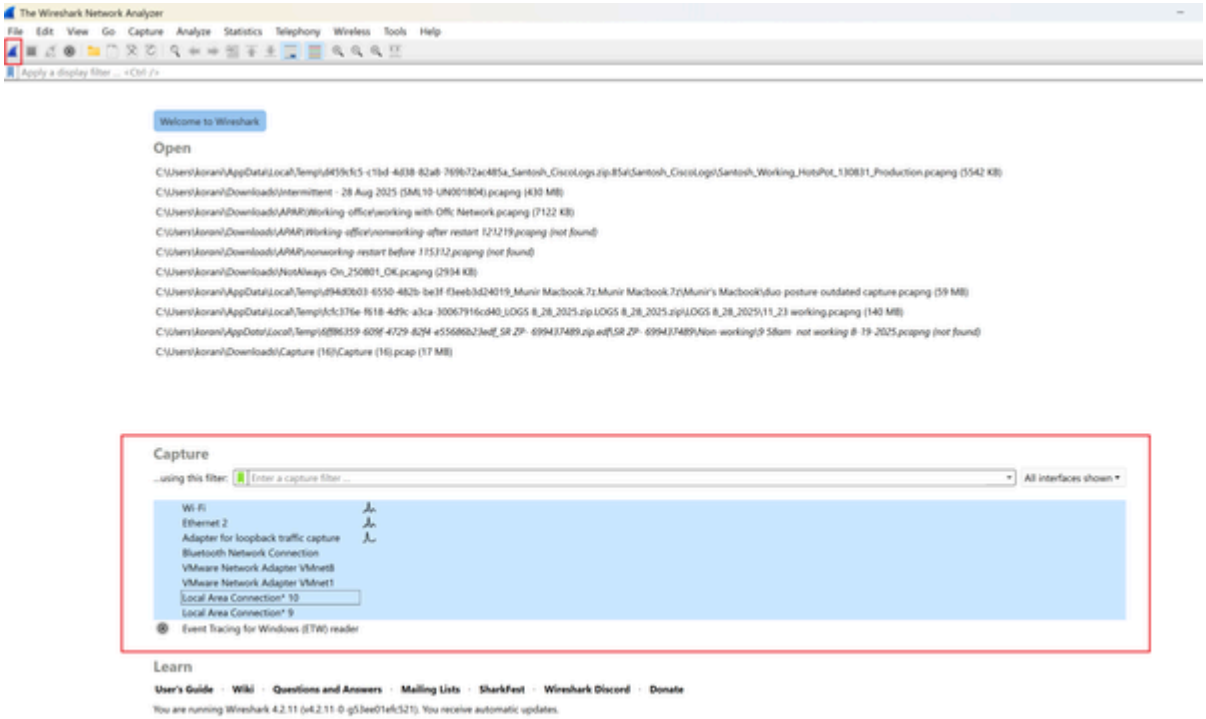
- Enable Flag

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

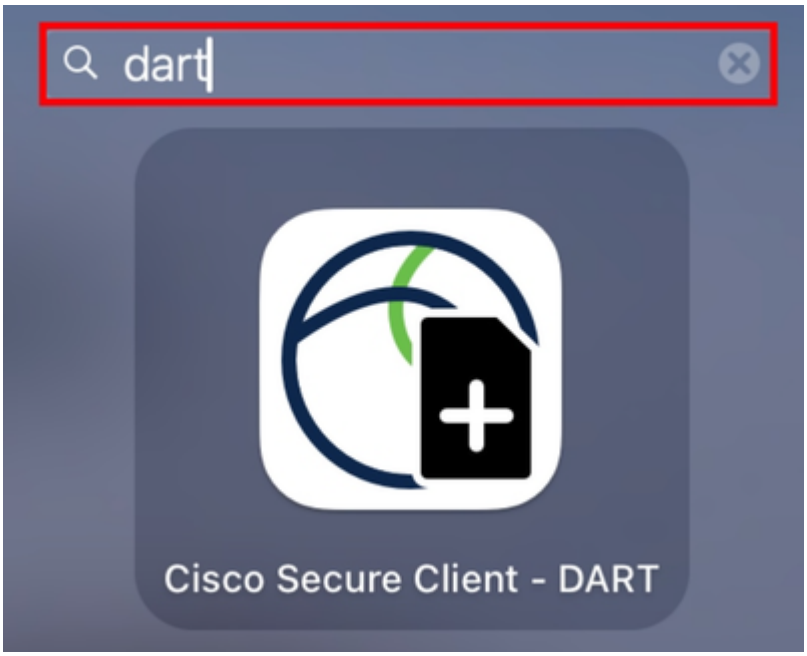
- Start Service

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

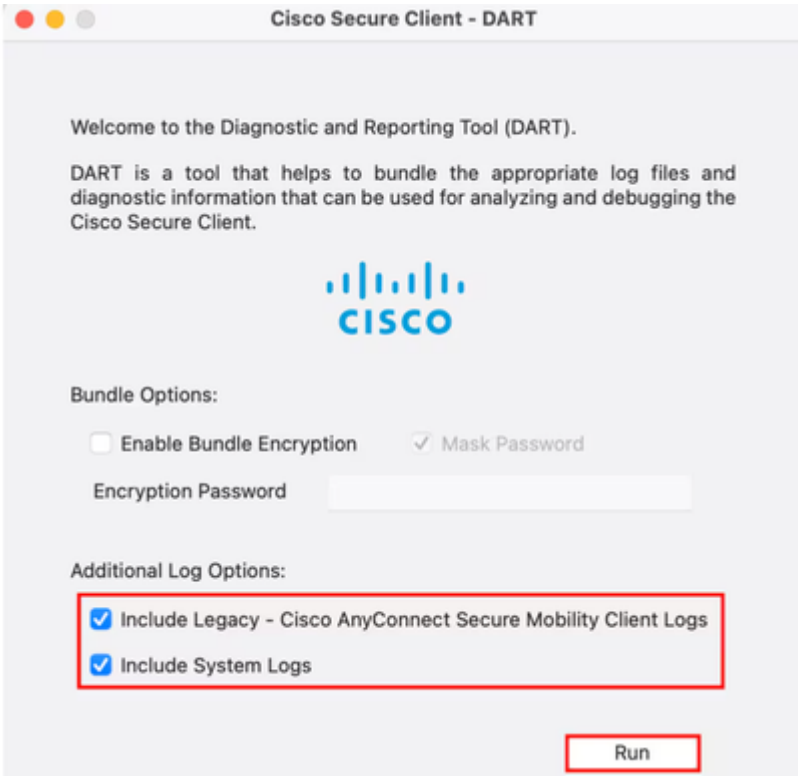
- Start Wireshark Capture
- Select all the interfaces, and start the packet capture



- Reproduce the issue, and save KDF Logs and Wireshark Capture, then follow the steps to capture DART Bundle
- Open the Cisco Secure Client - DART



- Checkmark the next options:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- Click Run



Note: Collect all the logs, KDF Logs, Wireshark Capture and DART Bundle to the TAC Case.

Related Information

- Cisco Technical Support & Downloads
- Cisco Secure Access Help Center
- Cisco SASE Design Guide