

Recopilación de registros KDF para Secure Client en Windows y MacOS

Contenido

[Introducción](#)

[INDICADORES de Windows y MacOS](#)

[Recopilación de registros de KDF, Wireshark y DART Bundle](#)

[Windows:](#)

[MacOS](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo recopilar registros de KDF y otros registros importantes de solución de problemas en Windows y MacOS.

INDICADORES de Windows y MacOS

| | |
|--|-------------|
| DNS relacionado (cuando OpenDNS está involucrado): | 0x20801FF |
| Proxy de flujo web (SWG) y DNS Relacionados: | 0x70C01FF |
| ZTA | 0x400080152 |

Recopilación de registros de KDF, Wireshark y DART Bundle



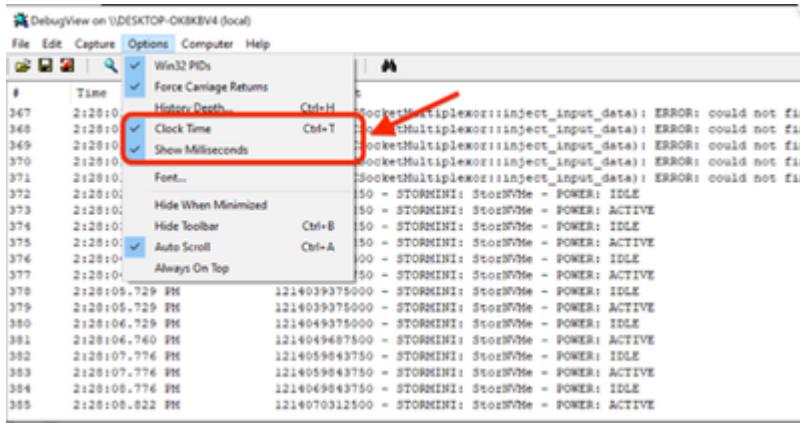
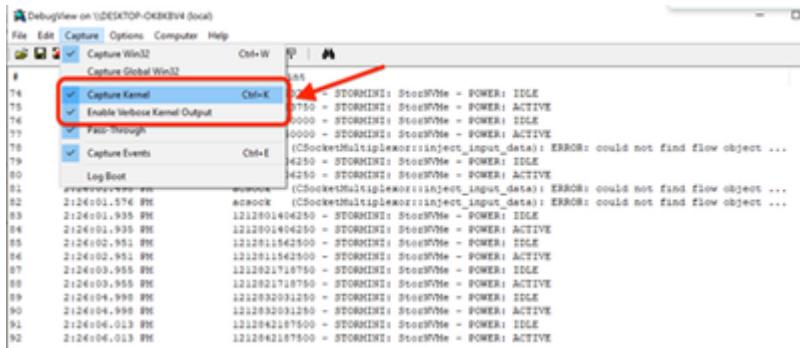
Nota: Cuando envíe los resultados, infórmeme siempre al equipo del TAC qué parámetros se han utilizado y esté abierto a cambios según lo requiera el TAC.

Windows:

Abra un CMD con privilegios de administrador y ejecute el siguiente comando:

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

- Descargue [DebugView](#) de SysInternal para capturar el registro KDF
- Ejecutar DebugView como administrador y activar las siguientes opciones de menú:
 - Haga clic en Capturar
 - Marca de verificación Capture Kernel
 - Marca de verificación Enable Verbose Kernel Output
- Opciones
 - Marca de verificación Clock Time
 - Marca de verificación Show Milliseconds



- Reinicie el servicio de cliente a través del prompt admin:

```
net stop csc_vpnaagent && net start csc_vpnaagent
```

- Si net stop csc_vpnaagent && net start csc_vpnaagent no funciona, reinicie el Cisco Secure Client servicio desde services.msc

| Services (Local) | |
|---|------------------|
| Cisco Secure Client - AnyConnect VPN Agent | |
| Stop the service | |
| Pause the service | |
| Restart the service | |
| Description: Cisco Secure Client AnyConnect VPN Agent for Windows | |
| Application Layer Gateway Service | Provides su... |
| Application Management | Processes in... |
| AppX Deployment Service (AppXSVC) | Provides inf... |
| AssignedAccessManager Service | AssignedAc... |
| Auto Time Zone Updater | Automatica... |
| AVCTP service | This is Audi... |
| Background Intelligent Transfer Service | Transfers fil... |
| Background Tasks Infrastructure Service | Windows in... |
| Base Filtering Engine | The Base Fil... |
| BitLocker Drive Encryption Service | BDESVC hos... |
| Block Level Backup Engine Service | The WBENG... |
| Bluetooth Audio Gateway Service | Service sup... |
| Bluetooth Support Service | The Bluetooth... |
| Bluetooth User Support Service_7206f | The Bluetooth... |
| BranchCache | This service ... |
| Capability Access Manager Service | Provides fac... |
| CaptureService_7206f | Enables opti... |
| Cellular Time | This service ... |
| Certificate Propagation | Copies user ... |
| Cisco Secure Client - AnyConnect VPN Agent | Cisco Secur... |
| Cisco Secure Client - ISE Posture Agent | Cisco Secur... |

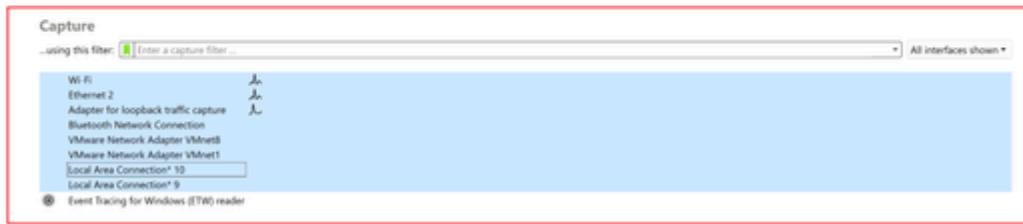
- Inicio Wireshark Capture
- Seleccione todas las interfaces e inicie la captura de paquetes



Welcome to Wireshark

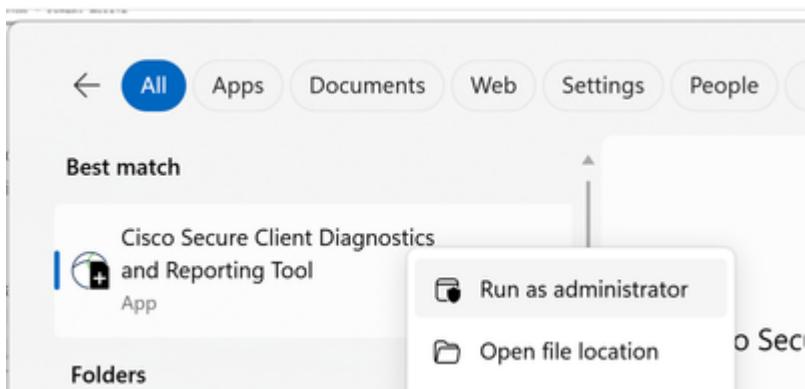
Open

C:\Users\koran\AppData\Local\Temp\d459cf5-11bd-4d38-82ab-769b72ac485a_Santosh_CiscoLogs.zip\85\{Santosh_CiscoLogs\Working_Hub\Production.pcapng (5542 KB)
C:\Users\koran\Downloads\Intermittent - 28 Aug 2025 (SMI-10-UN001804).pcapng (430 MB)
C:\Users\koran\Downloads\APAR\Working office\working with Offic Network.pcapng (7122 KB)
C:\Users\koran\Downloads\APAR\Working office\working after restart 121219.pcapng (not found)
C:\Users\koran\Downloads\APAR\monworking-restart before 115312.pcapng (not found)
C:\Users\koran\Downloads\NotAlways On_250801_OK.pcapng (2934 KB)
C:\Users\koran\AppData\Local\Temp\d94d0603-6550-482b-be1f\3eeb\3d24019_Munir Macbook.7z\{Munir's MacBook\}duo posture outdated capture.pcapng (59 MB)
C:\Users\koran\AppData\Local\Temp\fc371e_8118-4d9c-alca_30067916c40.LOGS_8_28_2025.zip\LOGS_8_28_2025.zip\LOGS_8_28_2025\11_23 working.pcapng (140 MB)
C:\Users\koran\AppData\Local\Temp\688c319_609f-4729-82f4-e55698b23ed_SR.ZP_699437489.zip\edf58_ZP_699437489\Non working\9.5dam not working 8_19_2025.pcapng (not found)
C:\Users\koran\Downloads\Capture (16)\Capture (16).pcap (17 MB)

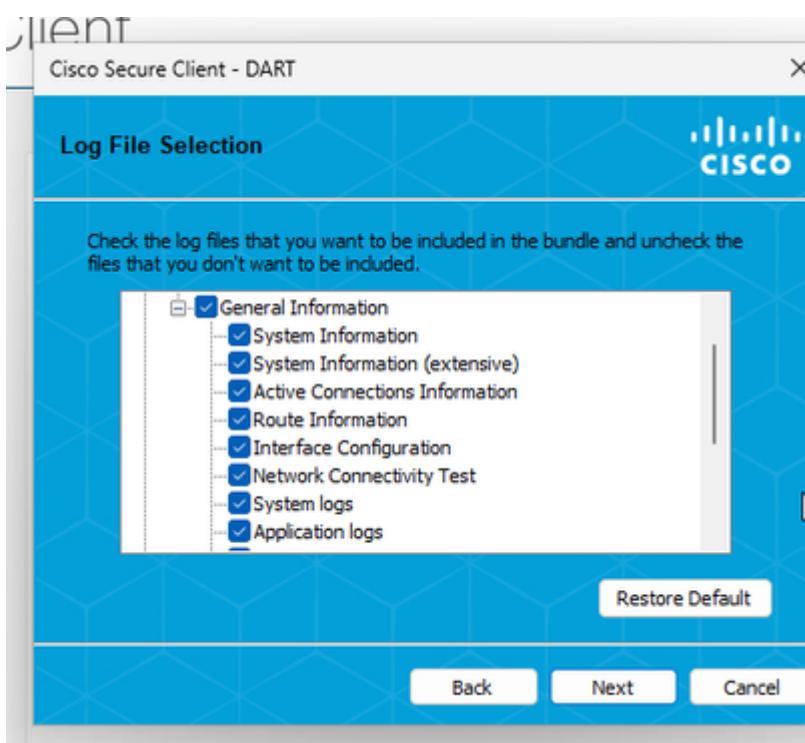


Learn
[User Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)
You are running Wireshark 4.2.11 (r42.11.0-g53ed01efc521). You receive automatic updates.

- Reproduzca el problema y guarde KDF Logs y Wireshark Capture después siga los pasos para capturar DART Bundle
- Abra el con Cisco Secure Client Diagnostics & Reporting Tool (DART) privilegios de administrador



- Haga clic en Custom
 - Incluir System Information Extensive **Y** Network Connectivity Test



Nota: Recopile todos los registros, registros KDF, captura Wireshark y paquete DART en el caso TAC.

- Para detener el registro de KDF en Windows, utilice el siguiente comando:

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

MacOS

Abra el terminal y siga la siguiente cadena de comandos para habilitar el registro de KDF en

MacOS:

- Stop Service

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

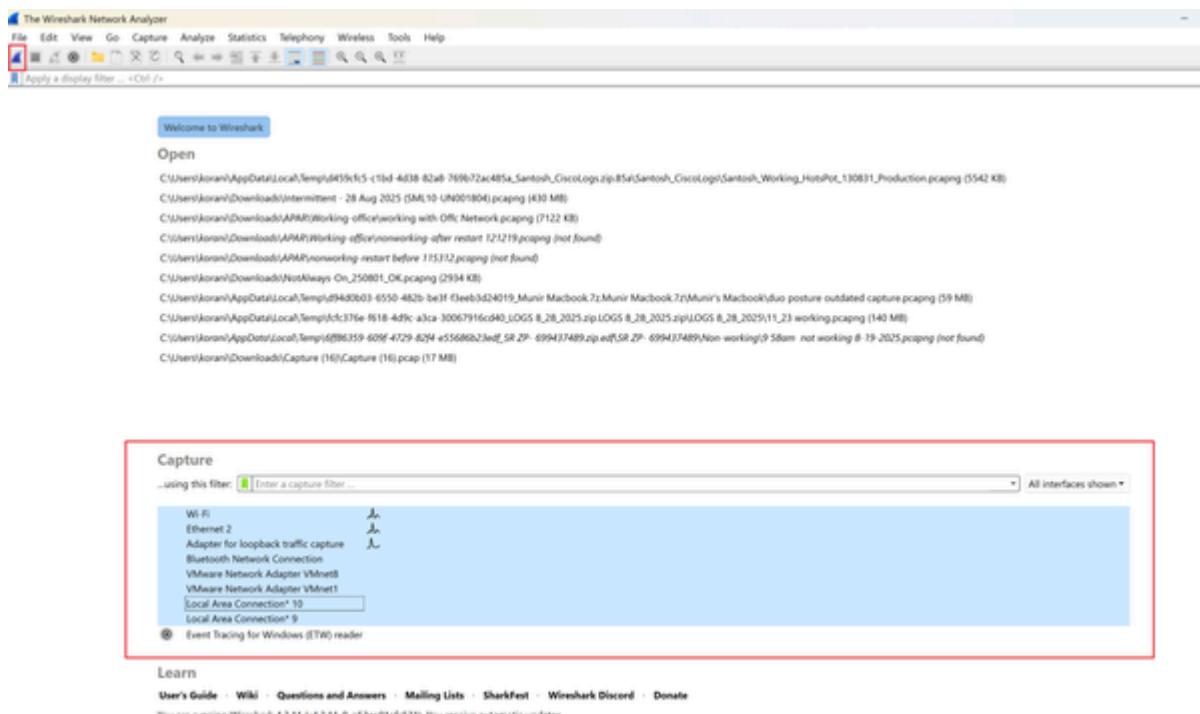
- Enable Flag

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

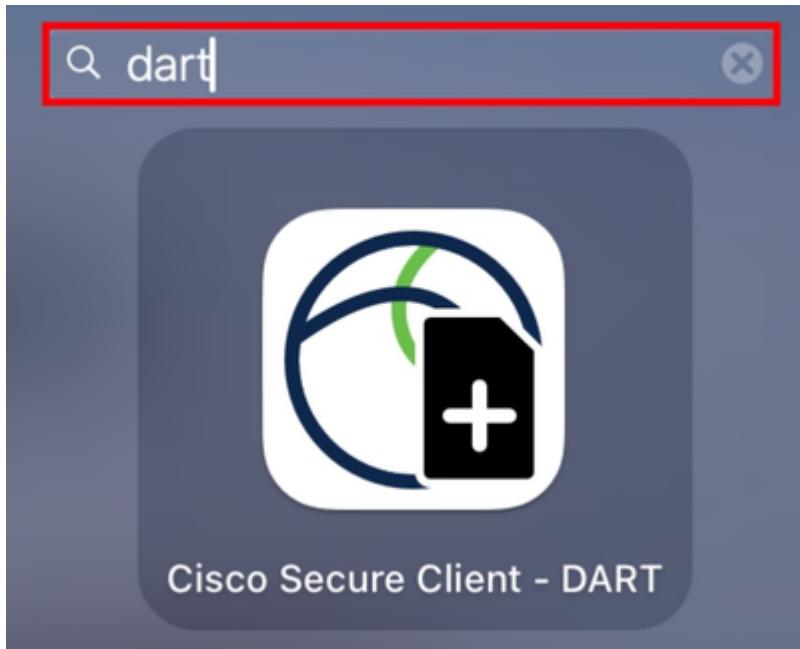
- Start Service

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

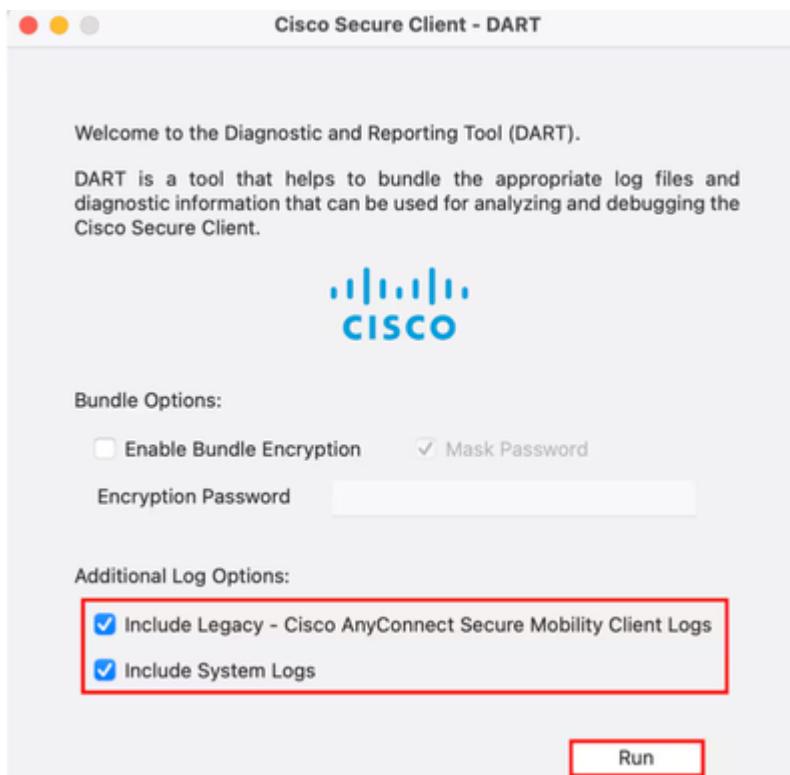
- Inicio Wireshark Capture
- Seleccione todas las interfaces e inicie la captura de paquetes



- Reproduzca el problema y guarde KDF Logs y Wireshark Capture después siga los pasos para capturar DART Bundle
- Abra el Cisco Secure Client - DART



- Marque las siguientes opciones:
 - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
 - Include System Logs
- Haga clic en Run



Nota: Recopile todos los registros, registros KDF, captura Wireshark y paquete DART en el caso TAC.

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)
- [Centro de ayuda de Cisco Secure Access](#)
- [Guía de diseño de Cisco SASE](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).