

# Coletando registros KDF para cliente seguro no Windows e MacOS

## Contents

---

[Introdução](#)

[SINALIZADORES Windows e MacOS](#)

[Coletando registros KDF, Wireshark e pacote DART](#)

[Windows](#)

[MacOS](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como coletar logs KDF e outros logs de solução de problemas importantes no Windows e MacOS.

## SINALIZADORES Windows e MacOS

Relacionado ao DNS (quando o OpenDNS está envolvido):	0x20801FF
Proxy de fluxo da Web (SWG) e DNS relacionados:	0x70C01FF
ZTA	0x400080152

## Coletando registros KDF, Wireshark e pacote DART

---



Note: Ao enviar os resultados, sempre informe à Equipe do TAC quais configurações foram usadas e esteja aberto a alterações, conforme exigido pelo TAC.

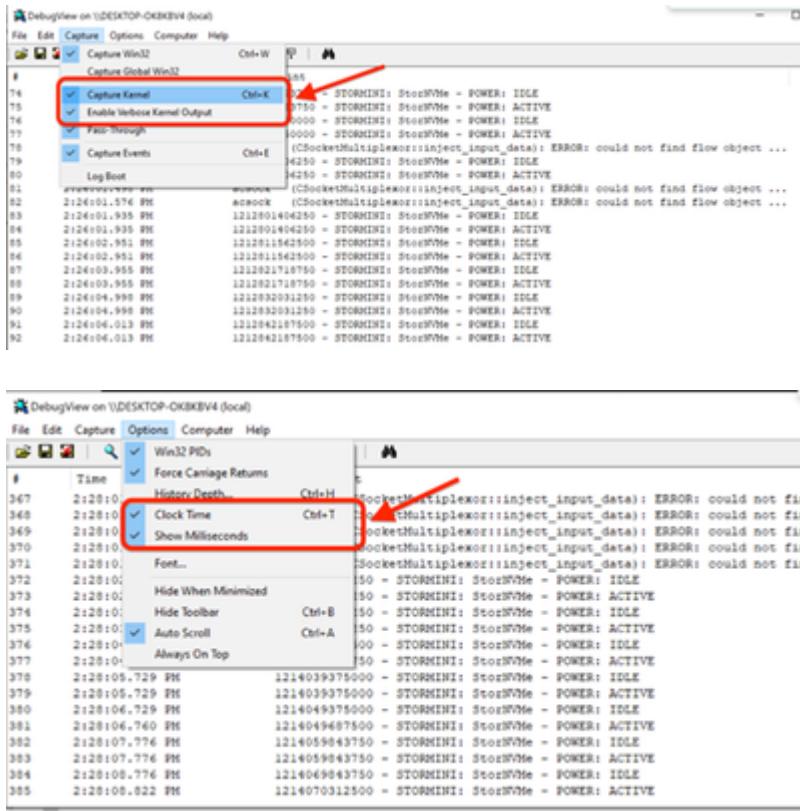
---

### Windows

Abra um CMD com privilégios de administrador e execute o próximo comando:

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

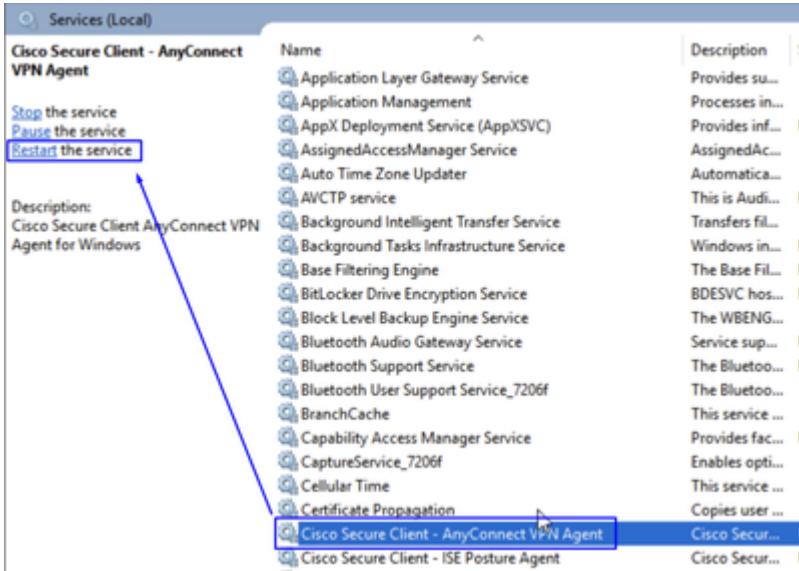
- Baixe [DebugView](#) de SysInternal para capturar o log KDF
- Execute DebugView como administrador e ative as próximas opções de menu:
- Clique em Capture
  - Marca de seleção Capture Kernel
  - Marca de seleção Enable Verbose Kernel Output
- Opções
  - Marca de seleção Clock Time
  - Marca de seleção Show Milliseconds



- Reinicie o serviço do cliente através do prompt do administrador:

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

- Se net stop csc\_vpnaagent && net start csc\_vpnaagent não funcionar, reinicie Cisco Secure Client o serviço do services.msc



- Iniciar Wireshark Capture
- Selecione todas as interfaces e inicie a captura de pacotes



Welcome to Wireshark

Open

C:\Users\koran\AppData\Local\Temp\d459\fc5<11d-4d38-82ab-769b72ac485a\_Santosh\_CiscoLogs.zip.B5f\{Santosh\_CiscoLogs\{Santosh\_Working\_HubSpot\_110831\_Production.pcapng (5542 KB)

C:\Users\koran\Downloads\Intermittent - 28 Aug 2025 (SM10-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)

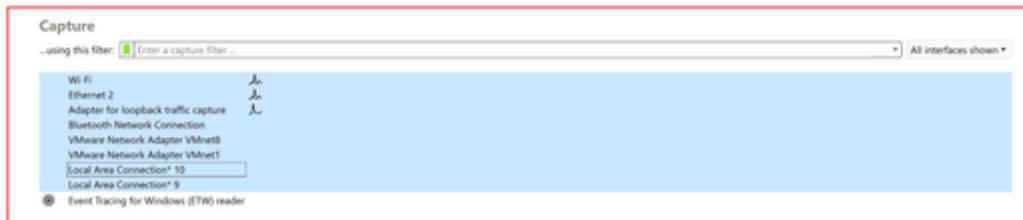
C:\Users\koran\Downloads\NotAlways On\_250801\_OK.pcapng (2934 KB)

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-30067316c40.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\d89c319\_605f-4729-82f4-e55696823ed\_SR.ZP-699437489.zip.edf\SR.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)

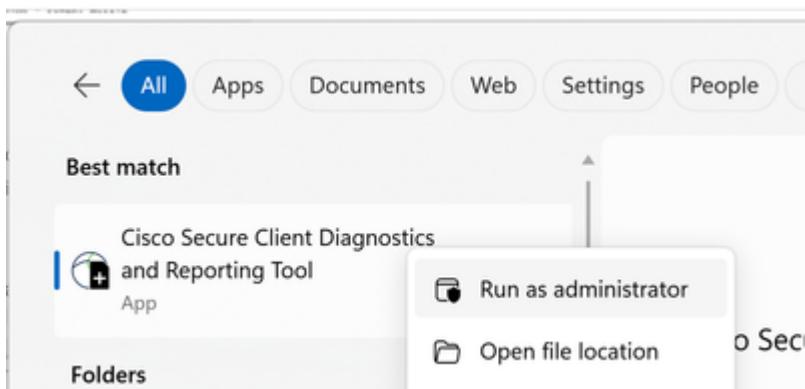


Learn

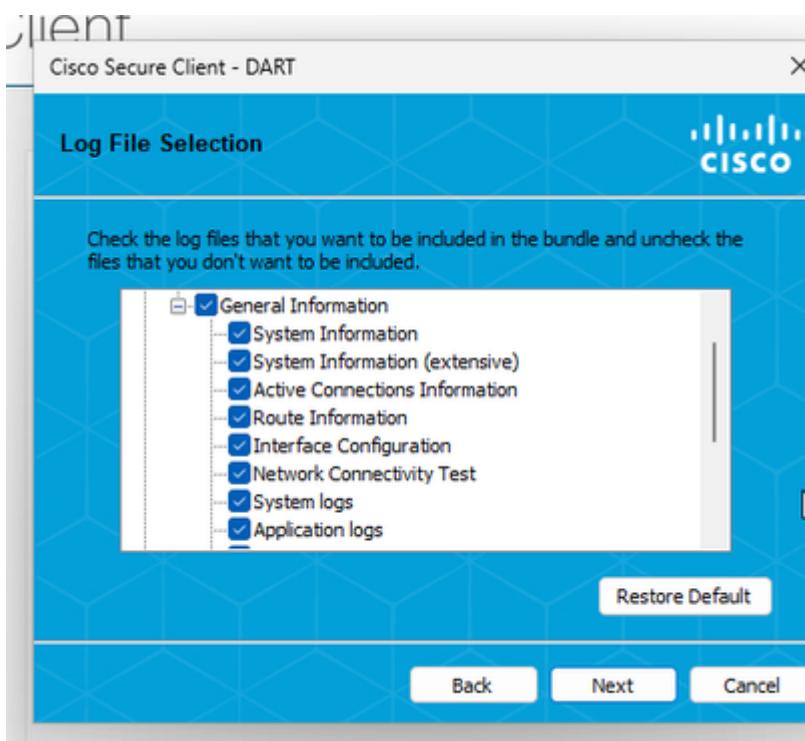
User Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.11 (r42.11.0-g53bed0efc521). You receive automatic updates.

- Reproduza o problema e salve KDF Logs e Wireshark Capture e siga as etapas para capturar DART Bundle
- Abrir o Cisco Secure Client Diagnostics & Reporting Tool (DART) com privilégios de administrador



- Clique em Custom
  - Incluir System Information Extensive e Network Connectivity Test



Note: Colete todos os registros, registros KDF, captura do Wireshark e pacote DART no caso TAC.

- Para parar o registro KDF no Windows, use o próximo comando:

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

## MacOS

Abra o terminal e siga a próxima cadeia de comandos para ativar o registro KDF no 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"
```

- Iniciar Wireshark Capture
- Selecione todas as interfaces e inicie a captura de pacotes



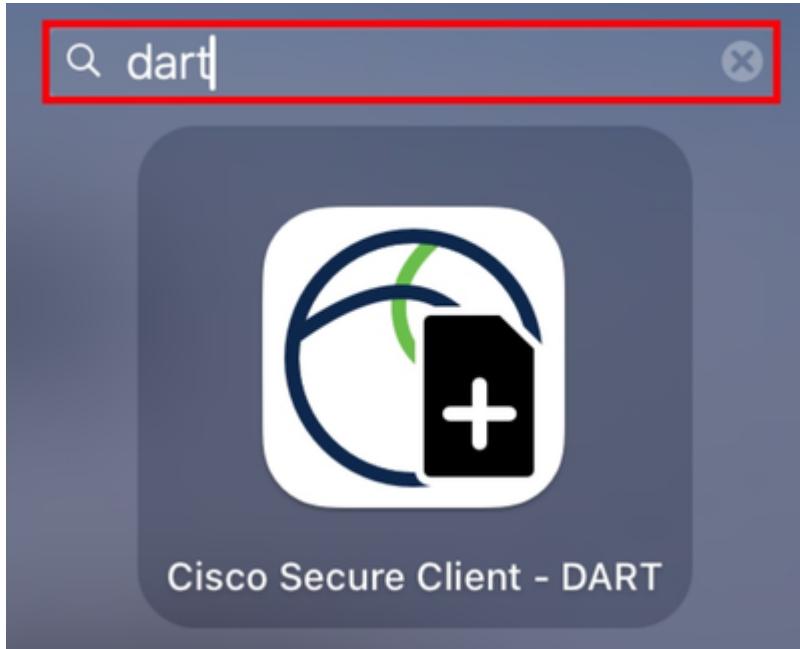
Welcome to Wireshark

Open

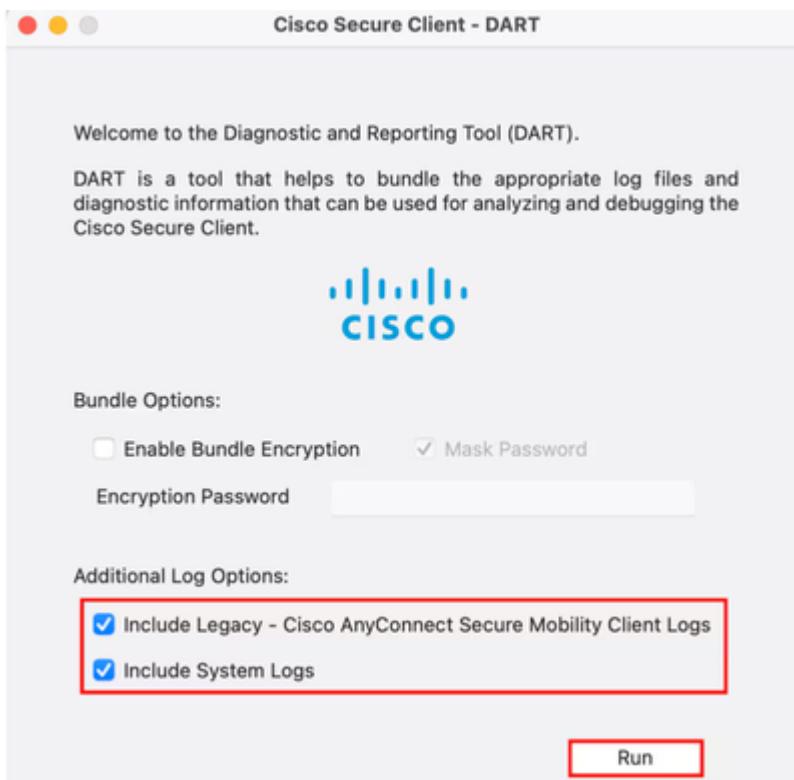
- C:\Users\koran\AppData\Local\Temp\pid459\h5<11d-4f82-a8-769b-72ac485a\_Santosh\_CiscoLogs.zip-85a\{Santosh\_CiscoLogs\}Santosh\_Working\_HubPvt\_130831\_Production.pcapng (5542 KB)
- C:\Users\koran\Downloads\Intermittent - 28 Aug 2025 (SM)10-UN001804.pcapng (410 MB)
- C:\Users\koran\Downloads\APAR\Working\_office\working with Off; Network.pcapng (7122 KB)
- C:\Users\koran\Downloads\APAR\Working\_office\unworking\_after\_restart 12.12.19.pcapng (not found)
- C:\Users\koran\Downloads\APAR\monworking\_restart before 115312.pcapng (not found)
- C:\Users\koran\Downloads\NotAlways\_Or\_250901\_OK.pcapng (294 KB)
- C:\Users\koran\AppData\Local\Temp\94d003-6550-482b-be1f\feeb3d2d4019\_Munir Macbook.7z.Munir Macbook.7z(Munir's Macbook)duo posture outdated capture.pcapng (59 MB)
- C:\Users\koran\AppData\Local\Temp\fc376e\_f618-4d9c-a1ca-30067916cd40\_1LOGS\_8\_28\_2025.zip.LOGS\_8\_28\_2025.zip.LOGS\_8\_28\_2025.LOGS\_8\_28\_2025.working.pcapng (140 MB)
- C:\Users\koran\AppData\Local\Temp\6989359-6059-4729-8294-e5568627edf\_58\_ZP-699437489.zip.edf58\_ZP-699437489\Non working\9.58am\_not working 8\_19\_2025.pcapng (not found)
- C:\Users\koran\Downloads\Capture (16).Capture (16).pcap (17 MB)



- Reproduza o problema e salve KDF Logs e Wireshark Capture e siga as etapas para capturar DART Bundle
- Abra o Cisco Secure Client - DART



- Marque as próximas opções:
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- Clique em Run



Note: Colete todos os registros, registros KDF, captura do Wireshark e pacote DART no caso TAC.

## Informações Relacionadas

- [Supporte técnico e downloads da Cisco](#)
- [Central de ajuda do Cisco Secure Access](#)
- [Guia de design do Cisco SASE](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.