

WindowsおよびMacOS上のセキュアクライアントのKDFログの収集

内容

[はじめに](#)

[WindowsおよびMacOSフラグ](#)

[KDFログ、Wireshark、およびDARTバンドルの収集](#)

[Windows](#)

[MacOS](#)

[関連情報](#)

はじめに

このドキュメントでは、WindowsおよびMacOSでKDFログおよびその他の重要なトラブルシューティングログを収集する方法について説明します。

WindowsおよびMacOSフラグ

DNS関連 (OpenDNSが含まれる場合) :	0x20801FF
Web flow(SWG)プロキシおよびDNS関連 :	0x70C01FF
ZTA	0x400080152

KDFログ、Wireshark、およびDARTバンドルの収集



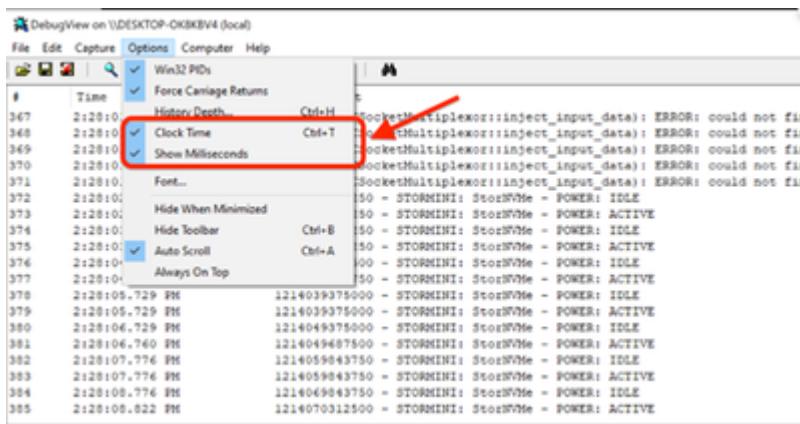
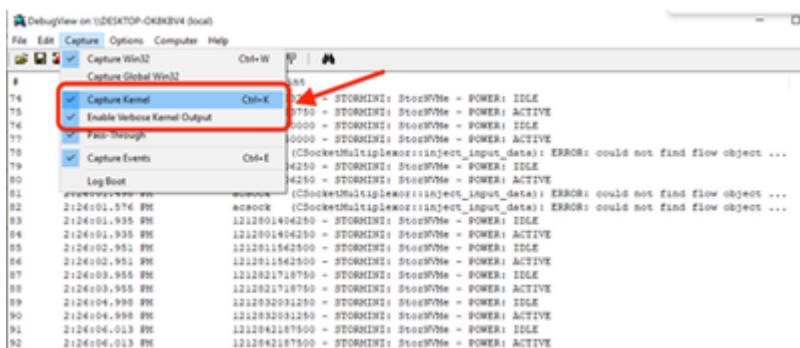
注：結果を送信する際には、使用された設定をTACチームに必ず知らせ、TACの必要に応じて変更できるようにしてください。

Windows

admin権限でCMDを開き、次のコマンドを実行します。

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

- SysInternalから[DebugView](#)をダウンロードして、KDFログをキャプチャします
 - DebugViewを管理者として実行し、次のメニューoptionを有効にします。
 - Captureをクリックします
 - キャプチャカーネルのチェックマーク
 - チェックマーク冗長カーネル出力の有効化
 - Options
 - クロック時間のチェックマーク
 - チェックマーク Show Milliseconds



- ・管理プロンプトでクライアントサービスを再起動します。

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

- net stop csc_vpnaagent && net start csc_vpnaagentが機能しない場合は、services.mscからCisco Secure Clientサービスを再起動します

Services (Local)	
Name	Description
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...

- Wiresharkキャプチャの開始
- すべてのインターフェイスを選択し、パケットキャプチャを開始します



Welcome to Wireshark

Open

C:\Users\koran\AppData\Local\Temp\d459cf5-11bd-4d38-82ab-769872ac485a_Santosh_CiscoLogs.zip.lsf\|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 115132.pcapng (not found)
C:\Users\koran\Downloads\NotAlways On_250801_OK.pcapng (2934 KB)
C:\Users\koran\AppData\Local\Temp\d94d0603-6550-482b-be1f\3eebf3d24019_Munir Macbook.7z\|Munir's MacBook\duo posture outdated capture.pcapng (59 MB)
C:\Users\koran\AppData\Local\Temp\fc371e_8118-49fc-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\688c319_605f-4729-82f4-e55698b23ed_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)

Capture

...using this filter: Enter a capture filter ...

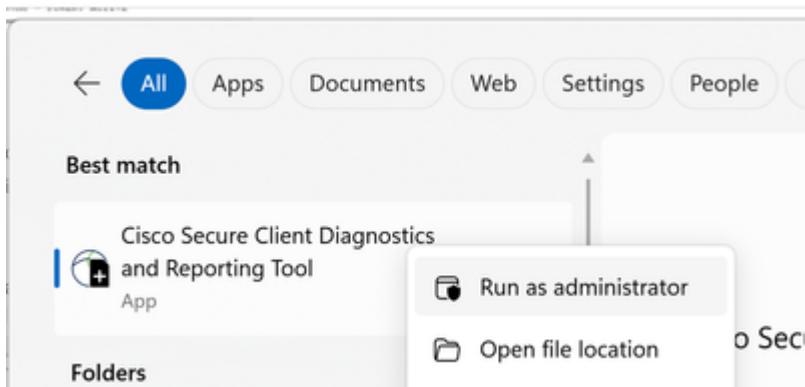
All interfaces shown *

Wi-Fi
Ethernet 2
Adapter for loopback traffic capture
Bluetooth Network Connection
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 10
Local Area Connection* 9
Event Tracing for Windows (ETW) reader

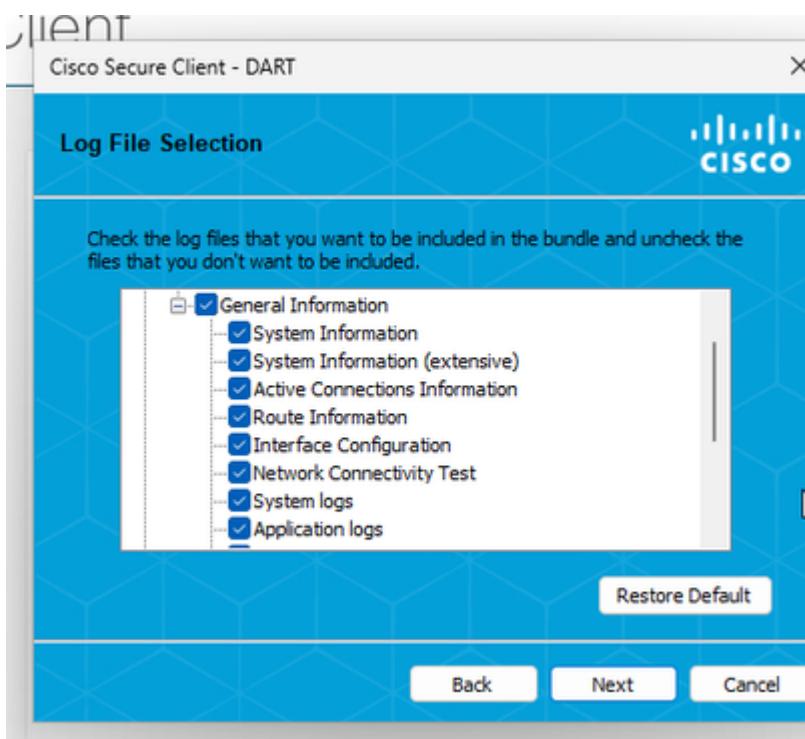
Learn

User's 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.

- 問題を再現し、KDFログとWiresharkキャプチャを保存して、次にDART/バンドルをキャプチャする手順に従います
- 管理者権限でCisco Secure Client Diagnostics & Reporting Tool(DART)を開きます



- Customをクリックします。
 - システム情報の広範囲にわたるテストとネットワーク接続テストを含めます。



注：すべてのログ、KDFログ、Wiresharkキャプチャ、およびDARTバンドルをTACケースに収集してください。

- WindowsでKDFロギングを停止するには、次のコマンドを使用します。

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

MacOS

ターミナルを開き、次のコマンドチェーンに従ってMacOSでKDFロギングを有効にします。

- サービスの停止

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

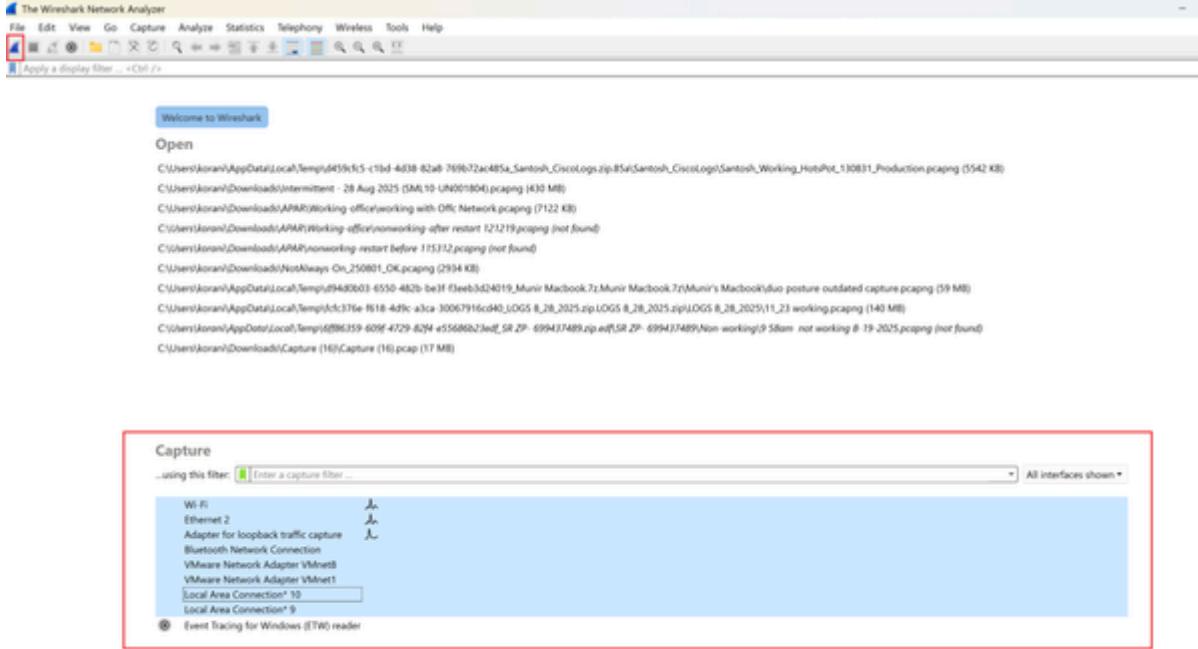
- フラグの有効化

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

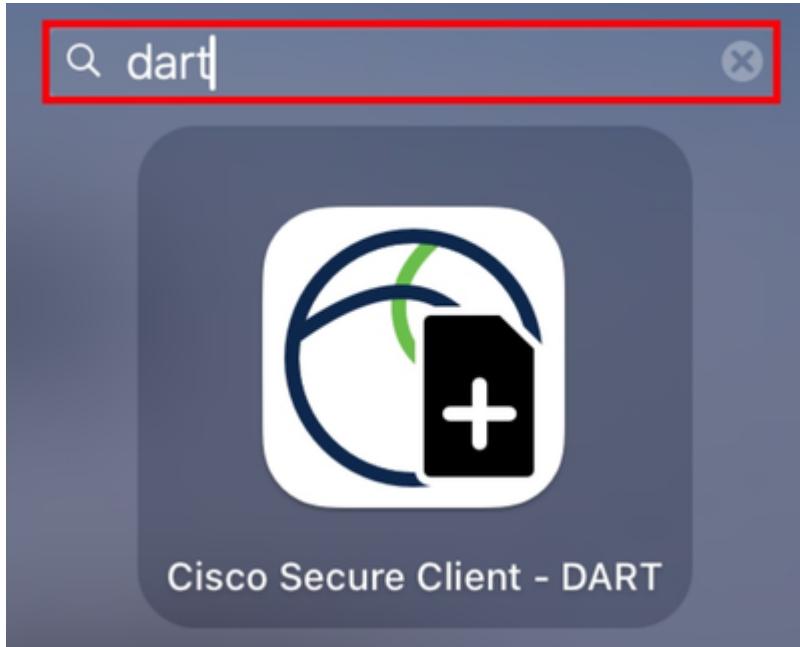
- サービスの開始

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

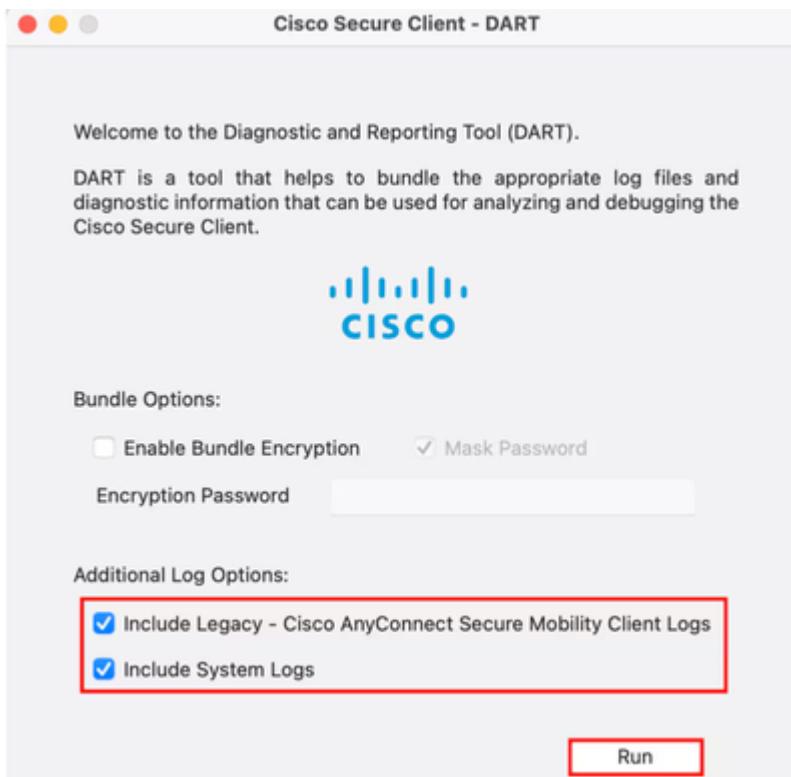
- Wiresharkキャプチャの開始
- すべてのインターフェイスを選択し、パケットキャプチャを開始します



- 問題を再現し、KDFログとWiresharkキャプチャを保存して、次にDART/バンドルをキャプチャする手順に従います
- Cisco Secure Client - DARTを開きます。



- 次のオプションにチェックマークを付けます。
 - レガシーを含める : Cisco AnyConnectセキュアモビリティクライアントログ
 - システムログを含める
- Runをクリックします。



注：すべてのログ、KDFログ、Wiresharkキャプチャ、およびDARTバンドルをTACケースに収集してください。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Accessヘルプセンター](#)
- [Cisco SASE設計ガイド](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。