

# ةيليقفتل ا ZTNA تالجس عيمجت احالص او عاطخالا فاشكتسال

## تاي وتحمل

[ةمدقملا](#)

[ةيساسأتامولعم](#)

[تالجسلا عيمجت](#)

[ةينفلاتا ةدعاسمل زكرم ةلاح حتف لباق ققبس مثاققحت](#)

[اهعمج بولطملا تالجسلا](#)

[عاطخأ عبت عض و نيكمنت ZTNA](#)

[ثادحألا ضراعي ف ZTA لجس ممح ةدابن](#)

[ةمدخ لىغشت ةداعا ZTA](#)

[Windows](#)

[سواكام](#)

[رابتخالا فمزحوي ئيانثلا عاطخالا حيحةصت عضو، مزحلا طاقنلا، KDF، ليجس نيكمنت مدق](#)

[Windows](#)

[سواكام](#)

[قلص تاذ تامولعم](#)

## ةمدقملا

ةيليقفتل احالص او ZTA عاطخا فاشكتسأ تالجس عيمجت ةيفيك دنتسملا اذه حضوي. ووطخ بوطخ نيكمنتلا دنع

## ةيساسأتامولعم

نيمدختسملا نيمأتل (ZTA) "ةقثلا مادعن" ةينبل ديازتم لكشب تاسسؤملا دامتعا عم ارمأ احالص او تاسايسلا ذافن اولاصتالا تالكشم فاشكتسأ حبصأ، تاقيبطتل او ةزهجالا او ةنمآل ةقطنملا دمتعت، قاطنلا ىلع ّمئاقلا ةيديلقتللا جذامنلل افالخو. اديقعت رثكأ، ةكبشلا قايسو، زاهجلا ةيعضو، ةيوهلا رباعي ىلعنفلا تقولا يف ةددعتم تارارق ىلع (ZTA)، ةيلاع تالجسلا نوكت، لكاشم أشننت امدنعو. ةباحسلا ىلع ّمئاقلا تاسايسلا تاكرح و يرذجلا ببسلا ديدحتل ابلاغ ةيفاك ريغ يوتسمل

كولسل ةقيمع ةيور باستك ايف امساح ارود ZTA ىوتسم عبّت ليفصافت عيمجت بعل يه ذه حيتتو. ةباحسلا ةمدخ تالعافت و رورمل اك رح ضارتع او ةسمايسلا مييقتو ليمعل ىلع ّمئاقلا اهلحو تالكشملا فاشكتسأ ةيلمع زواجت ةيناكما نيسدنهملل تاراسمل او لوصولا لشف تالاح ىلا يدؤت يتلا ثادحألل قيقدل لسلستلا ليلحت و ضارعألا. عقوتملا ريغ جهنلا جئاتن او عادلأا ضافخنا

## تالجسلا عيمجت

ةينفل ا ٰدعاس ملا زكرم ٰلاح حت ف لب ق ٰقب س م تا ق ق ح ت

ـ ئىلاع ف رىڭ ألىڭىشىپ ئەلگىشىملا دىدەت ئىلۇق TAC قىرىف ئەقلىپ سىملا تامىيىقتىلا ھەذە دعا سىتىس نىكىمىي ام عرسا ئەپ كەتلىكىشىم لە ئىلۇق مەددەس يىس نىيىس دەنەمەللى تامەنەلەملا ھەذە رېفوت نىـ

- ؟اهب نيرثأتمل نيمدختسملا ددع وه امو، ةلكرشملا يه ام
  - ؟ترثأت يتل ا تارادص إل او ليغشتلا ماظن وه ام
  - عساو مأ مدختسملا ب صاخ وه له ،اعطقتم ناك اذا ؟ةعطقتم مأ ةتباث ةيضمقل له  
؟راشتنةالا
  - ؟راشتنةالا ذنم ةدوجوم اهنأ مأ ربيغتل ا دعب ةلكرشملا تأدب له
  - ؟فورعم تازفحم يأ كانه له
  - ؟رفوتم ليدب لح كانه له

## اھم ج بول طملا تال جس ل

- DART ڦمنح
  - ZTNA عڃسو تالجس اڳٿڀا
  - (عاجرسالا کل ذي ڦف امب ، تاهج اولا عي مج) Wireshark طاقتلا
  - اه ظحالم تمت یتل اڳ خلا لئاسر
  - رادص إلل ڦينم زلا عٻاو طلا
  - CSC ZTA ڦي طمنلا ڦدھولا ڦلاح ڦشاش ڦطقنل
  - رٿأت ملاب مدخن سملاب صاخلا مدخن سملامسا

لیصف تلاب اهعی مجت و تالج سل اه نم لک نیک مت ۃی فیک ۃی لاتلا ماسق ایا حضوت

## ZTNA اطخاً عبّت عضو نیکمٽ

هاندأ لیصافتلاب logconfig.json یمسم فلم یاشن!

```
{ "global": "DBG_TRACE" }
```

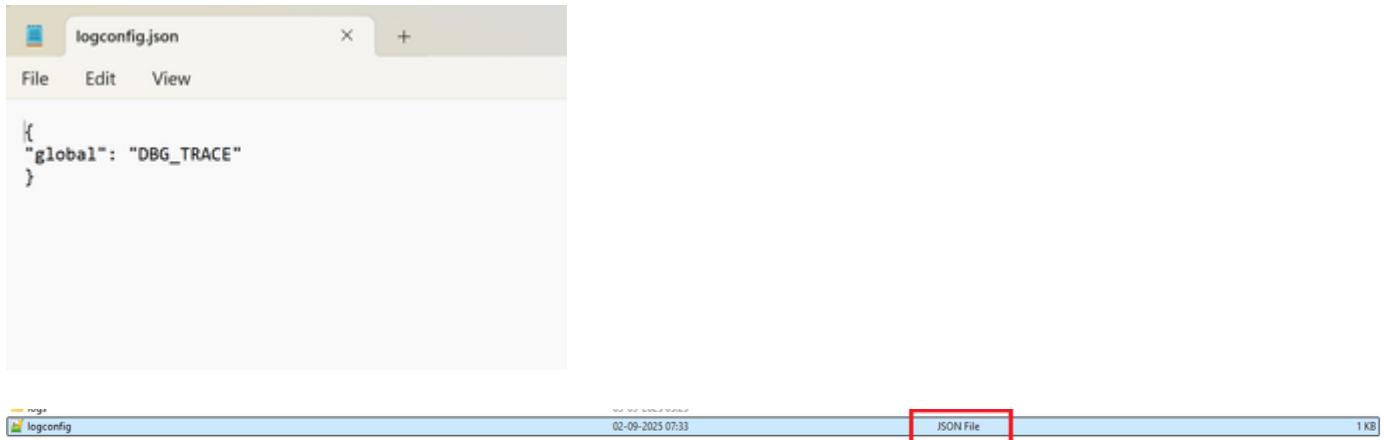


فلملا ظفح نم دکأت :ريذخت `logconfig.json`.

لیغشتلا ماظن یلع ءانب پسانملا ناكملا یف هعضا ، فلملا ءاشنادعه

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA

- ساوا:/opt/cisco/secureclient/zta



مدع ىل اوصولا لمعا" ۆمۆخ لیغشت ۆداعا بجي ، ددحمل ا فلمل ا عاشن ا درجمب : ۆظحال نکمملا نم نکي مل اذا . ۆوطخ لل [ZTA](#) ۆمۆخ لیغشت ۆداعا نم ۆقحتل ا عاچرلا )" ۆقثلا رت ویبمکلا لیغشت ۆداعا عاچرلا ، ۆمۆخ لیغشت ۆداعا .

## ثادح األا ضراع يف ZTA لجس مجح ۆدایز

مجح ۆدایز کي لع بجي ، عب ت تلا ىوت سم ليجس ت نيك م ت دع ب ، رت و يبمک ۆزه جأ يف اي و دي ZTA لجس فلم.

1. حتف Event Viewer
2. عي سوت لاب م ق ، رس يألا عز جل ا يف Applications and Services Logs.
3. نمي ألا س و امل ا رزب رق نا Cisco Secure Client – Zero Trust Access Properties.
4. (ت ياب اغ يم 200 لداعي ام) ىل ع ۆم يق ل ا ن ي يع ت ب م ق ، م ت ح ت Maximum log size (KB).

ث اه ن إل ق و ف رق ن ا Apply م ث OK.

Event Viewer

Cisco Secure Client - Zero Trust Access Number of events: 5,017

Level	Date and Time	Source	Event ID
Information	02-09-2025 15:33:31	csc_zta_agent	
Information	02-09-2025 15:28:31	csc_zta_agent	

Log Properties - Cisco Secure Client - Zero Trust Access (Type: Administrative)

General

Full Name: Cisco Secure Client - Zero Trust Access

Log path: %SystemRoot%\System32\Winevt\Logs\Cisco Secure Client - Zero Trust Access.evtx

Log size: 4.07 MB(42,63,936 bytes)

Created: 04 June 2025 12:03:07

Modified: 02 September 2025 15:34:01

Accessed: 02 September 2025 15:37:12

Enable logging

Maximum log size ( KB ): 204800

When maximum event log size is reached:

Overwrite events as needed (oldest events first)

Archive the log when full, do not overwrite events

Do not overwrite events ( Clear logs manually )

Clear Log

OK Cancel Apply

Information 02-09-2025 14:53:29 csc\_zta\_agent

## ةمداخليغشت ةداعا ZTA

### Windows

- لاخدا حاتفم طغض او باتكل جتفل Run Search services.msc + R مدخلت سأ
- اهنم عاهتنالا درجمب و قوف رقن او Cisco Secure Client - Zero trust Access Agent Restart. عقوم ددح
- ةطشن اهنأ ديكأتل CSC ZTA ئي طمنلا ئدحوللا ئدلاح نم ققحت

Services

File Action View Help

Services (Local)

Name	Description	Status	Startup Type	Log On As
Capability Access Manager Service	Provides fac...	Running	Manual	Local Syst...
CaptureService_471f42d	Enables opti...	Manual	Local Syst...	
Cellular Time	This service ...	Manual (Trig...	Local Service	
Certificate Propagation	Copies user ...	Running	Manual (Trig...	Local Syst...
Cisco Orbital	Cisco Orbit...	Running	Automatic	Local Syst...
Cisco Secure Client - AnyConnect VPN Agent	Cisco Secur...	Running	Automatic	Local Syst...
Cisco Secure Client - Cloud Management	Cisco Cloud...	Running	Automatic	Local Syst...
Cisco Secure Client - Posture Agent	Cisco Secur...	Running	Automatic	Local Syst...
Cisco Secure Client - ThousandEyes Endpoint Agent	ThousandEy...	Running	Automatic	Local Syst...
Cisco Secure Client - Umbrella Agent	Cisco Secur...	Running	Manual	Local Syst...
Cisco Secure Client - Umbrella SWG Agent	Cisco Secur...	Running	Manual	Local Syst...
<b>Cisco Secure Client - Zero Trust Access Agent</b>	Cisco Secur...	Running	Automatic	Local Syst...
Cisco Secure Endpoint 8.4.4	Cisco Secur...	Running	Automatic	Local Syst...
Cisco Security Connector Monitoring 8.4.4	Cisco Secur...	Running	Automatic	Local Syst...

ةداعا ناف، يراددا لوصوللا مدع ببساب ZTA ئمداخليغشت ةداعا رذعت اذ: ئطحالم

---

ييلاتلا رايخلالا يه لماكلا ماظنلا ليغشت.

---

سإ وأ كام

Stop Service

```
sudo "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app/Contents/MacOS/Cisco
```

Start Service

```
open -a "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app"
```



لوصول اصقون ببسوب ZTA ۆمدىخ ليغشت ۆداعا رذعت وأ رمأوألا ذيفنت رذعت اذا: ۆظحالم  
ييلاتلا رايخلالا يه لماكلا ماظنلا ليغشت ۆداعا ناف ،يرادالا

---

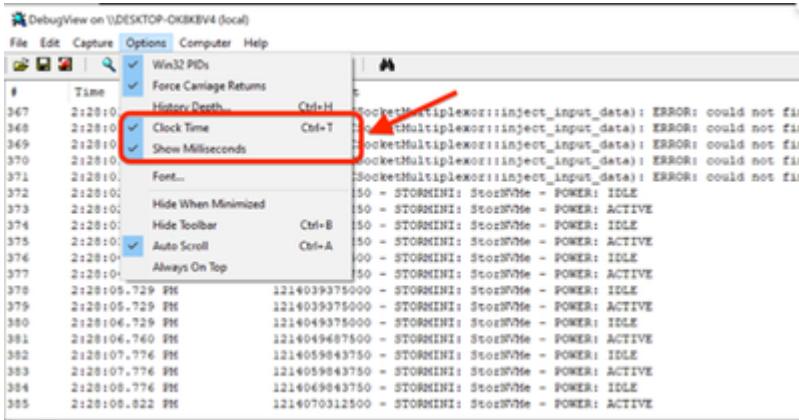
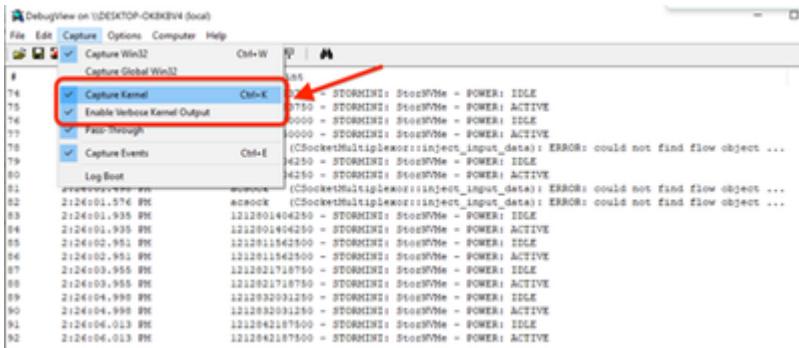
ۆمزح و يئانثلا ئاطخالا حييحت عضو، مزحلا طاقتلا، KDF، ليجست نيكمنتب مق رابتخالا

Windows

ييلاتلا رمألا ليغشتب مق و لوسملات ازايتماب CMD حتفا:

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x400080152
```

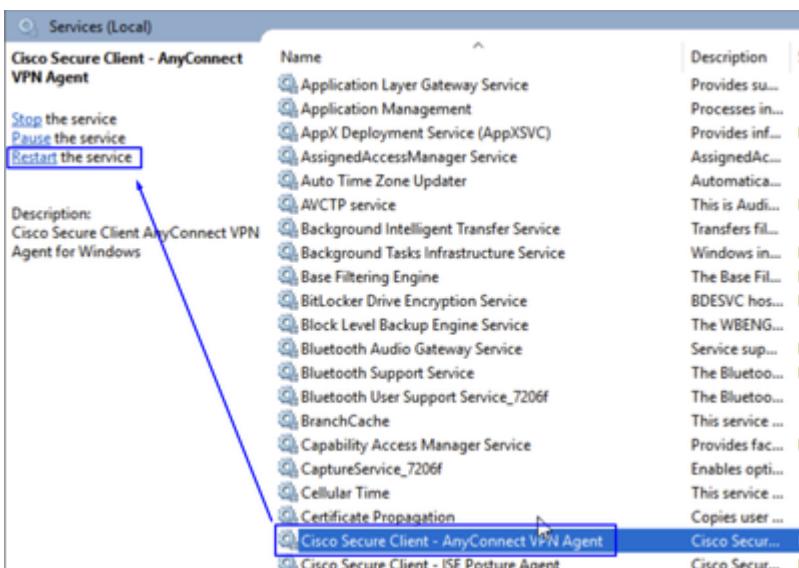
- لجس طاقتلا لـ [DebugView](#) SysInternal نم KDF
- ۆيلاتلا ۆمئاقلاتاري خ نيكمنت و DebugView Administrator لـ ليغشت
- طاقتلا ىلع رقنا
  - رايتحا ۆمالع Capture Kernel
  - رايتحا ۆمالع Enable Verbose Kernel Output
- تاري خ
  - رايتحا ۆمالع Clock Time
  - رايتحا ۆمالع Show Milliseconds



- لِوْفْسِمْلَا ءَبْلَاطْمَ رَبْعَ لِيْمَعْلَا ءَمْدَخَ لِيْغَشْتَ ءَدَاعَابَ مَقْ.

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

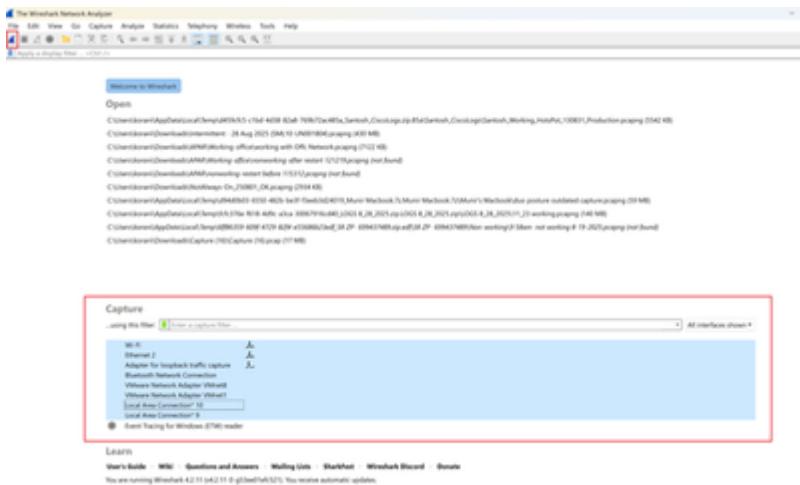
- **نم ۆم دخل Cisco Secure Client services.msc** لىغشت ۆداعاب مق، لمعى مل `net stop csc_vpnaagent && net start csc_vpnaagent` [ا]



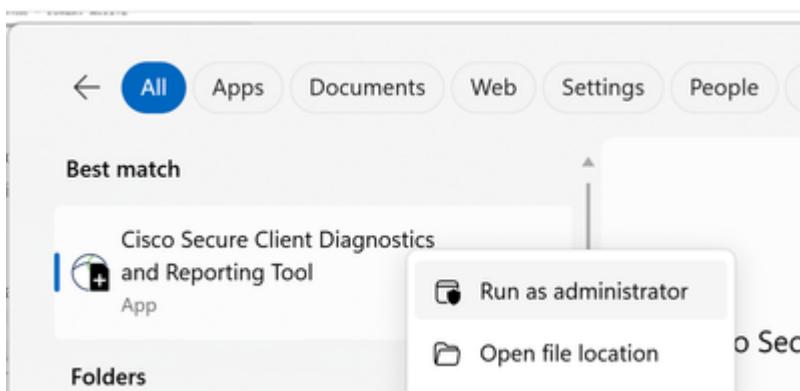
- ## • حیحصتلاءضویفیئانثلا نیکمٹ

- ## • عدّب Wireshark Capture

• مزحلا طاقتلا أدب او، تاهجاولا لك ددج



- ديرت يتلا تاو طخل ا عبتا مث، ظفح و KDF Logs Wireshark Capture، ۆلکشملا جاتن! ۆداعاب مق اه طاقتلا DART Bundle
  - لۆس مللا تازایت مادختسا ب (Cisco Secure Client Diagnostics & Reporting Tool (DART)) حتف



- **قوف رقنا** Custom Network Connectivity Test  
◦ System Information Extensive



- يلاتلا رمألا مدخل KDF ىلع Windows ليجست فاقياً:

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



ىلإ عي مجت و Wireshark طاقتلا ، KDF تالجس ، تالجسلا لك عي مجتب مق : ة طحالم ۋ ئەلەح TAC.

## سإ وڭام

ىلع KDF ليجست نيكمل ئيلاتلا رمألا ئىلسلس عبتو ئيفرطلار ئەطھملا حتفا:

- Stop Service

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

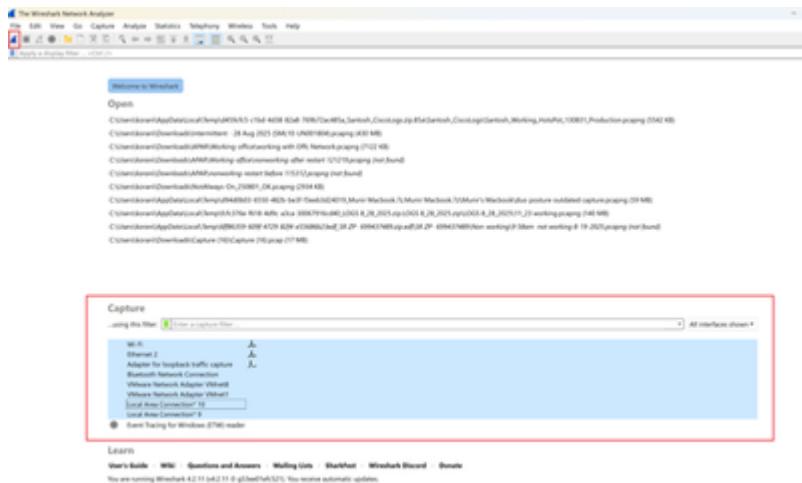
- Enable Flag

```
echo debug=0x400080152 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

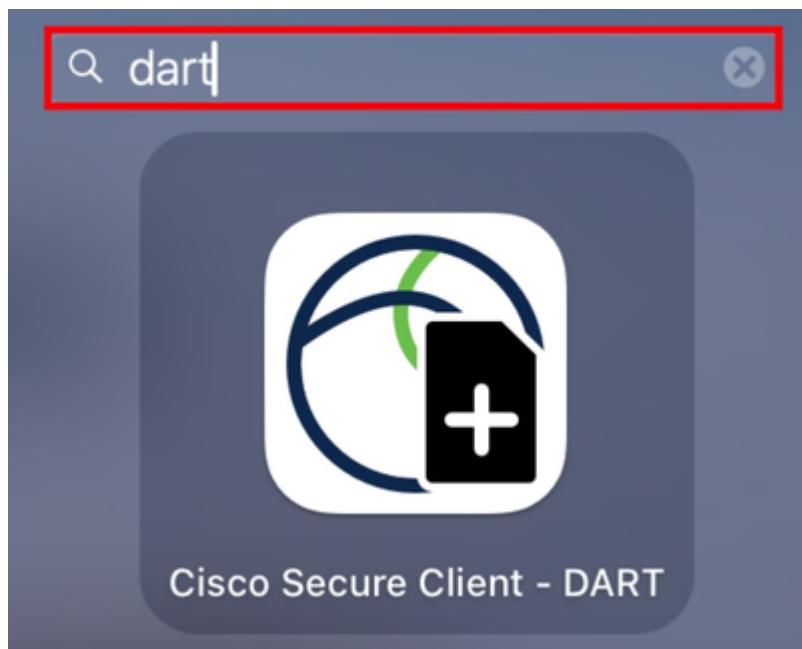
- Start Service

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

- حیحص تلا عضویف یئانثلا نیکمٽ
  - عدب Wireshark Capture
  - ۃمزح لا طاقتل ا أدباو، تاهج اولالک ددح



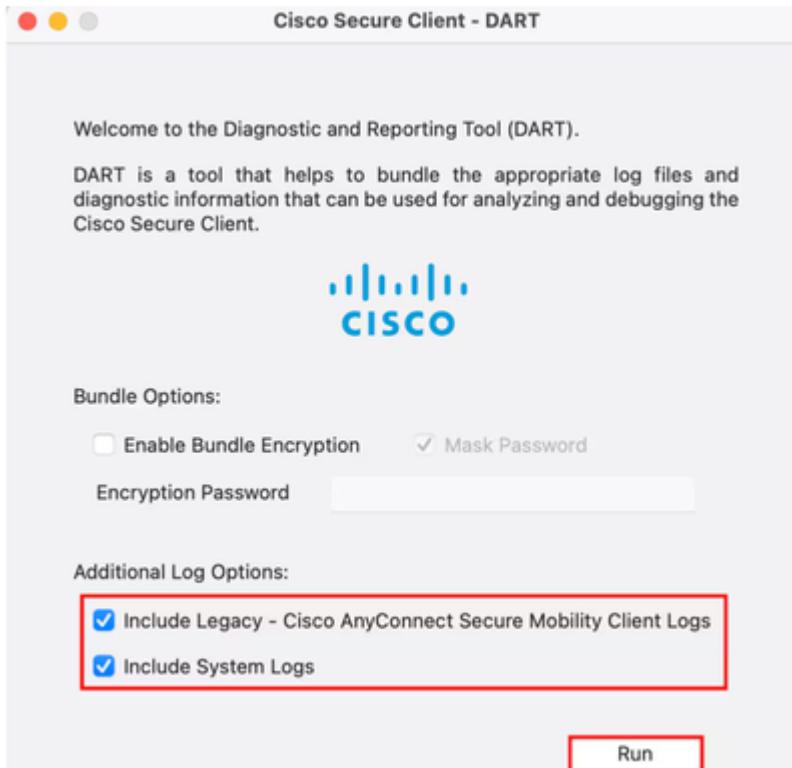
- ديرت يتلا تاوطلخا عبتا مث KDF Logs و Wireshark Capture، ۋە لکشملا جاتنإ ۋە داعاب مق اھطاقتلا DART Bundle
  - حتف Cisco Secure Client - DART





- Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs

- رقنا Run



ىلإ DART عي مجت و Wireshark طاقتلا ، تالجس ، تالجسلا لك عي مجتب مق : ة طحالم ة لاح TAC.

## ةلص تاذ تامولعم

- نم تاليزنتل اوينفلامع دلا Cisco
- نم نمآل لوصول ا تاميلع ت زكرم Cisco
- ميمصت ليلد Cisco SASE
- كم عي مجت KDF تالجس معنما لي Windows و MacOS

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
ـ لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ـ يـ رـ شـ بـ لـ اـ وـ  
ـ اـ مـ كـ ـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ـ يـ لـ آـ ـ مـ جـ رـ تـ لـ ـ ضـ فـ اـ نـ اـ ـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
ـ اـ مـ كـ ـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ـ يـ لـ آـ ـ مـ جـ رـ تـ لـ ـ فـ اـ رـ تـ حـ اـ لـ اـ ـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ـ يـ لـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ اـ مـ دـ قـ يـ يـ تـ لـ اـ ـ يـ لـ اـ مـ جـ رـ تـ لـ اـ ـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ ـ لـ إـ اـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ (ـ رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ )ـ يـ لـ صـ اـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ