エンドポイント診断ツール(CEDT)について

内容

はじめに

このドキュメントでは、システムから診断データを収集し、Cisco TACサポートケースにアップロードするためのの CEDTについて説明します。

前提条件

このツールは、MacOSおよびWindowsで使用できます。 ツールをダウンロードします。

次の項目に関する知識があることが推奨されます。

- MacOS:Cisco Endpoint Diagnostics Tool(CEDT).appをダブルクリックして起動します。
- Windows:CEDT.exeをダブルクリックして起動します。
- アクティブなインターネット接続。
- Cisco TACケースIDとトークン（結果を直接アップロードする場合にのみ必要）

システムデータの収集

このツールは、このシステムデータをカテゴリ別に収集します。いかなる種類の個人データもキャプチャされません。

一般的なシステム情報

Data	macOS	Windows
OS, hardware, CPU, RAM, storage	`system_profiler SPSoftwareDataType SPHardwareDataType`	`systeminfo`, WMI classes (`Win32_OperatingSystem`, `Win32_ComputerSystem`, `Win32_BIOS`)
Kernel parameters	`sysctl -a`	N/A

ネットワーク設定

Data	macOS	Windows
Network interfaces & IP addresses	`ifconfig -a`	`ipconfig /all`
Routing table	`netstat -rn`	`netstat -rn`
DNS configuration	`scutil --dns`	(included in `ipconfig /all`)
Network services	`networksetup -listallnetworkservices`	`netsh interface show interface`
WiFi profiles	N/A	`netsh wlan show profiles`

製品情報

Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco.*`	Registry exports (`HKLM\SOFTWARE\Cisco`, `HKCU\SOFTWARE\Cisco`, `acsock` service)
Installation directories	`ls -laR /opt/cisco`	`%ProgramFiles%\Cisco`, `%ProgramFiles(x86)%\Cisco`, `%ProgramData%\Cisco`
Running Cisco processes	`ps aux | grep -i cisco`	`tasklist | findstr /i cisco`, WMI `Win32_Process`
Installed Cisco products	`mdfind` for Cisco apps	WMI `Win32_Product` (vendor Cisco)
Application logs	Cisco Secure Client log directories	`%ProgramData%\Cisco\Cisco Secure Client\Logs`
Event logs	N/A	Windows Event Log (`Cisco Secure Client - Zero Trust Access`, Application provider `*Cisco*`)
Crash reports	`~/Library/Logs/DiagnosticReports/cisco*` (last 7 days)	N/A

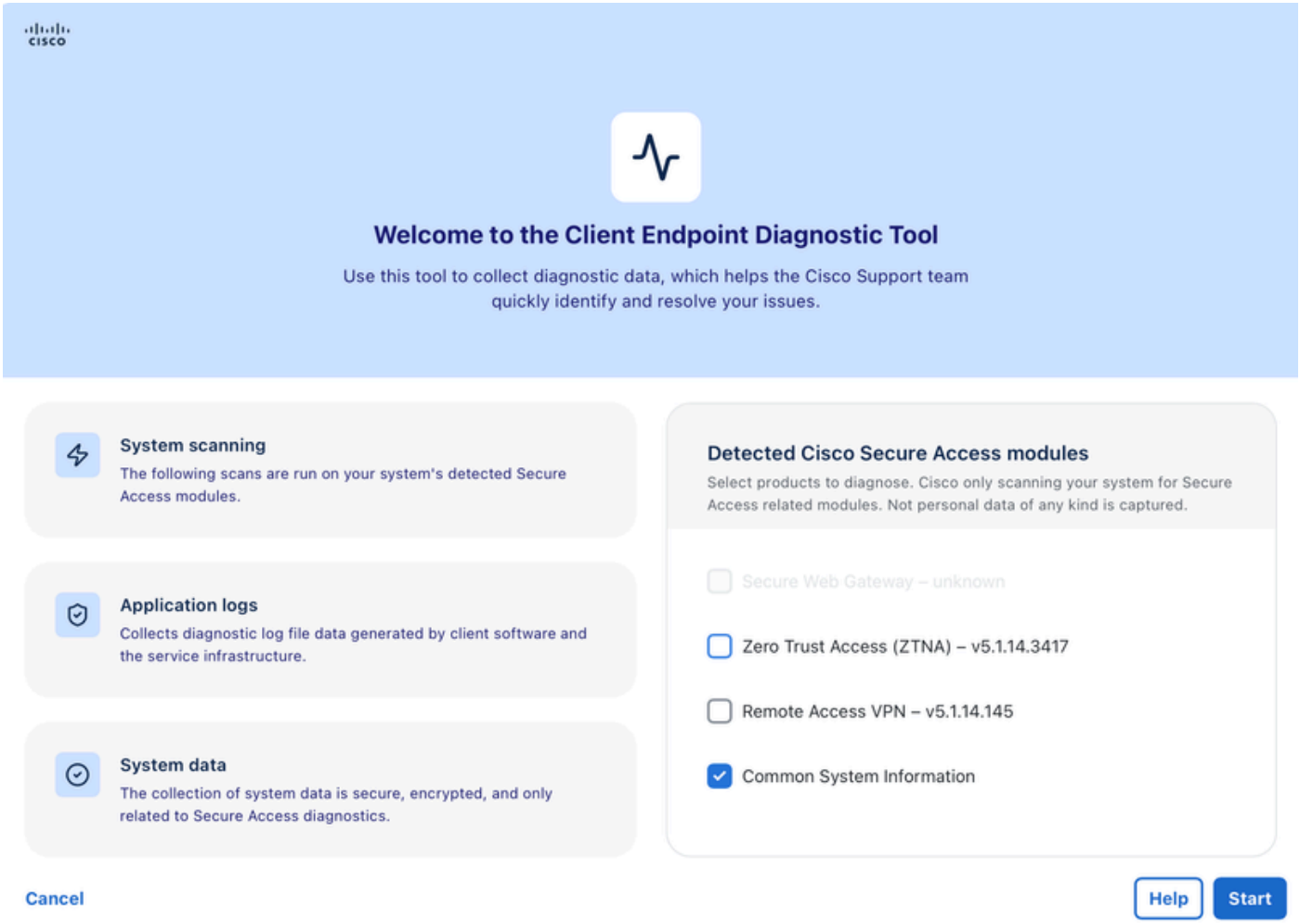
ステップバイステップウォークスルー

ウェルカム画面

CEDTを起動すると、初期画面が表示されます。このツールの機能の概要を示します。

- システムスキャン：システムをスキャンして、検出されたCisco Secure Accessモジュールを探します。
- アプリケーションログ：クライアントソフトウェアとサービスインフラストラクチャによって生成された診断ログファイルデータを収集します。
- システムデータ：システムデータの収集は、セキュアで暗号化されており、セキュアアクセ

スの診断にのみ関連します。



右側では、システムにインストールされているCisco Secure Accessモジュールが自動的に検出されます。検出された各モジュールのチェックボックスとそのバージョン番号を確認できます。

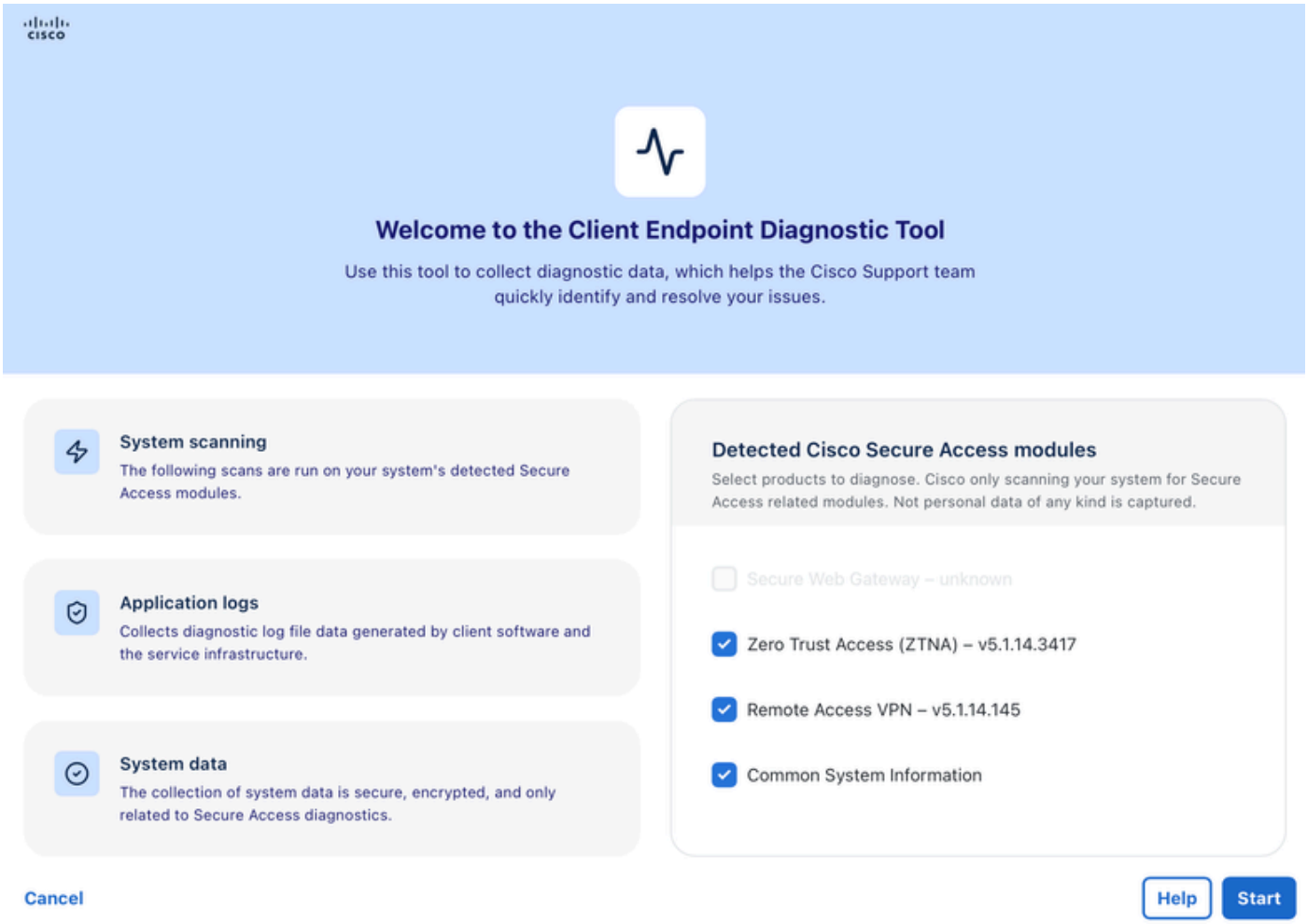
- ゼロトラストアクセス(ZTNA)
- セキュアWebゲートウェイ(SWG)
- リモートアクセスVPN(RAVPN)
- 共通システム情報（常に利用可能）

[アクション（Actions）]

1. 診断する製品を選択または選択解除します。

2. Let's Startをクリックして先に進むか、Helpをクリックして詳細を参照してください。

注：このツールは、セキュアアクセス関連モジュールのデータのみを収集します。いかなる種類の個人データもキャプチャされません。



ステップ1：診断データの収集

この画面では、含める診断テストとデータ収集モジュールを選択できます。

ネットワーク診断

実行する接続テストを選択してください：

- DNS Lookup：指定されたホストに対してDNS解決テストを実行します。ターゲットルックアップ用のカスタムリゾルバIPをサポートします。すべての結果は、構造化されたセクション区切り記号を使用して1つの出力ファイル(dns/dns_lookups.txt)に統合されます。
- パケットキャプチャ：指定した期間のネットワークパケットをキャプチャします（管理者権限が必要）。
- Ping Hosts：指定したホストにpingを実行して、接続を確認します。
- ポリシーテストの出力：シスコのポリシーテストエンドポイント(policy.test.sse.cisco.com)を使用して、指定されたURLに対するポリシーの適用をテストします。 複数のコンマ区切りホストをサポート（最大10）。 結果には、ポリシーテストナビゲーション中に自動的に取得されたHARデータが含まれます。
- ネットワーク速度テスト：シスコの速度テストエンドポイント(speed.test.sse.cisco.com)に対するアップロード/ダウンロード速度および遅延を測定します。 ダウンロード速度（6パラレルストリーム）、アップロード速度（3パラレルストリーム）、ping遅延/ジッタ（10 ICMPサンプル）を収集します。 結果は、JSON形式とテキストサマリー形式の両方で保存されます。
- URL Reachability:HTTP GET要求を使用して、指定されたURLに到達できるかどうかをチェックします。デフォルトでは、HTTP（ポート80）とHTTPS（ポート443）の両方をサポートします。非標準ポートはURLで指定できます(https://example.com:8443など)。 チェックごとに最大20のURL、URLごとに30秒のタイムアウトURLごとに収集されるデータには、URL、到達可能性ステータス、HTTPステータスコード、応答時間（ミリ秒）、コンテンツ長、解決済みIPアドレス、TLSバージョン、およびタイムスタンプが含まれます。結果はreachability/reachability_results.jsonおよびreachability/reachability_summary.txtに保存されます。

データ収集

パフォーマンスおよび接続データを収集するモジュールの選択：

- HAR Capture：ブラウザセッションからのHTTPアーカイブ(HAR)データを記録します。現在、Google Chromeのみをサポート（ヘッドレスブラウザの自動化によりChrome DevTools Protocolを使用） このツールは、システム上のChromeインストールを自動的に検出します。現時点では、FirefoxとSafariはサポートされていません。HARの出力はHAR 1.2仕様に従っており、完全なネットワークトレース（JSがトリガするXHR/fetchコールを含む）が含まれています。

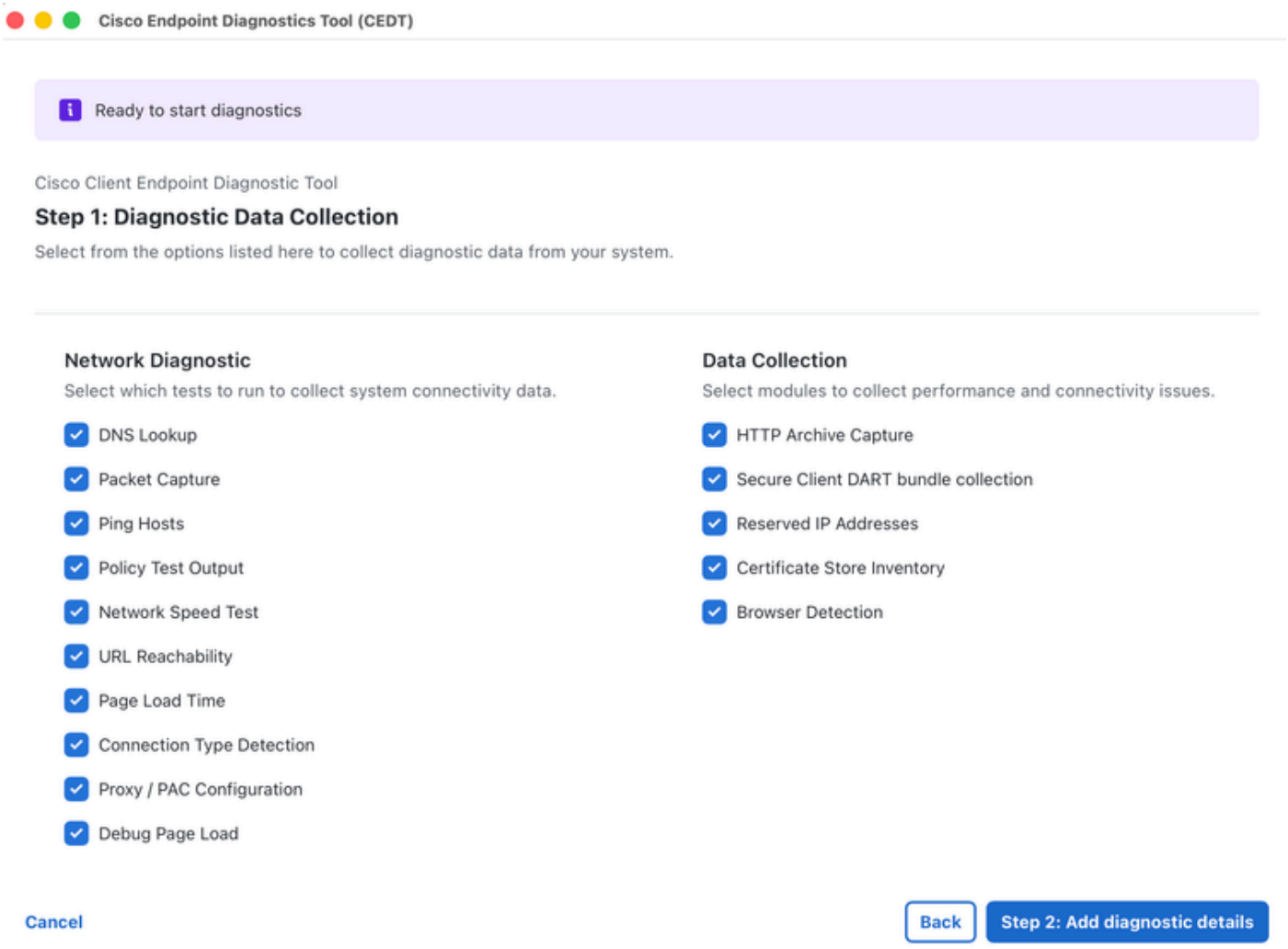
- DARTバンドル収集：Cisco Secure ClientからDART診断バンドルを収集します。これには、ゼロトラストアクセス(ZTA)ログ(WindowsのC:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\のflowlog.dbなど)を含むすべてのモジュールログが含まれます。
- Reserved IP：予約済みIP診断チェックを実行します。収集された診断の完全なリストについては、次のセクションを参照してください。

デバッグ

- デバッグフラグの有効化：エンドポイントの問題を診断するために、エンドポイントアクティビティの詳細なログを収集します。このオプションは、1つ以上のCisco Secure Access製品が検出され、選択されている場合にのみ使用できます。

プラットフォーム固有

- DebugView Capture(Windows):Windows Secure Endpoint Connectorでデバッグログを有効にします。このオプションは、Windowsシステムでのみ使用できます。



[アクション（Actions）]

1. 必要な診断オプションのオン/オフを切り替えます。
2. Step 2: Add diagnostic detailsをクリックして続行します。
3. Backをクリックしてwelcome画面に戻るか、Cancelをクリックして終了します。

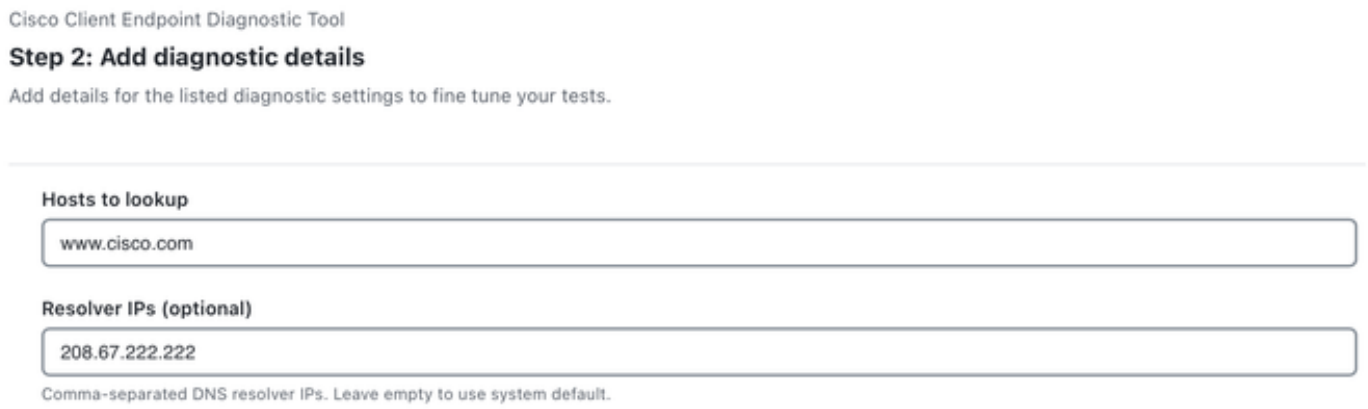
ステップ2：診断の詳細の追加

この画面では、有効な診断テストごとに特定のパラメータを設定できます。手順1で有効にしたテストの設定のみが表示されます。

DNSルックアップ設定

- 「検索するホスト」 — 1つ以上のホスト名を入力します（カンマ区切り）。 例：cisco.com
- 「リゾルバIP」(Resolver IPs)（オプション）– カスタムDNSリゾルバIPを入力します（カンマ区切り）。 例：208.67.222.222、208.67.220.220システムのデフォルトのDNSリゾルバを使用するには、空のままにします。指定すると、各ホストが各リゾルバに対して照会され、異なるDNSサーバ間での比較DNS解決結果が提供されます。

すべてのDNSルックアップ結果は、dns/dns_lookups.txtという1つの出力ファイルに統合されます。このファイルには、各ホスト/リゾルバの組み合わせごとに構造化されたTextFSMセクション区切り文字が含まれています。



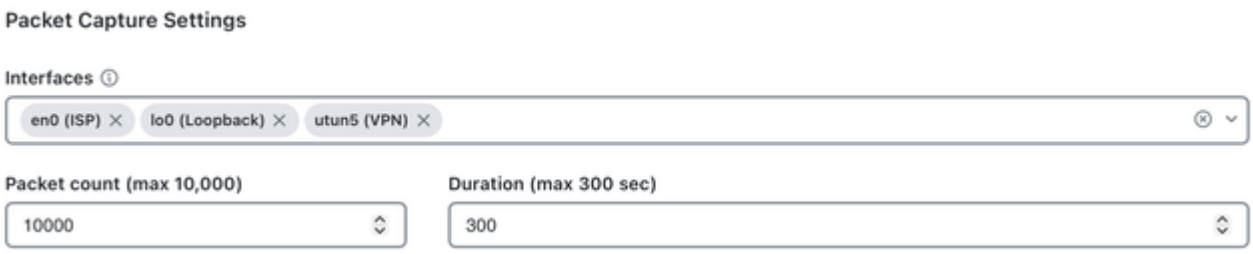
パケットキャプチャの設定

- Interfaces：キャプチャするネットワークインターフェイスを選択します（または「All」のままにしておきます）。
    - 「すべて」(All)（自動モード）に設定した場合
        - macOS/Linux：このツールはtcpdump -Dを実行して、使用可能なすべてのインターフェイスを列挙した後、動作中のインターフェイス（切断されたインターフェイスを除く）をフィルタリングします。 アクティブなインターフェイスが見つからない場合は、特別なanyインターフェイスにフォールバックします。キャプチャは、一致するすべてのインターフェイスで並行して実行されます。
        - Windows：選択したキャプチャバックエンドを使用するすべてのNICのキャプチャ（次のセクションのツールを参照）。 インターフェイスが選択されていないdumpcapを使用すると、検出された最初の3つのインターフェイスまでが同時にキャプチャされます。
- パケットカウント：インターフェイスごとにキャプチャするパケットの数。デフォルト：100。最大：10,000。
- Duration (sec) – キャプチャの最大時間（秒）。デフォルト：macOS/Linuxでは20秒、Windowsでは5秒。最大：300秒。パケットカウントまたは制限時間のうち、いずれか早い方に達すると、キャプチャは停止します。

プラットフォーム別のパケットキャプチャツール

注:(Windows)：このツールでは、使用可能な最適なキャプチャバックエンドが自動的に選択されます。pktmonが推奨され（Windows 10 v2004+に組み込み）、dumpcapにフォールバックして（Wiresharkがインストールされている場合）、最後の手段としてnetsh traceが使用されます。

Platform	Primary Tool	Fallback 1	Fallback 2
macOS/Linux	`tcpdump`	N/A	N/A
Windows	`pktmon` (Packet Monitor) — captures to ETL, converts to PCAPNG	`dumpcap` (Wireshark) — captures to PCAP	`netsh trace` — captures to ETL



パケットキャプチャ出力ファイル

各インターフェイスのキャプチャは、命名規則tcpdump/{interface_name}_capture.pcap（en0_capture.pcap、eth0_capture.pcapなど）を使用して個別のファイルとして保存されます。 メタデータマニフェストファイル(tcpdump/packet_capture_manifest.txt)も生成され、使用されるプラットフォーム、パケット数、期間、キャプチャされたインターフェイス、およびキャプチャバックエンドが記録されます。

Ping設定

- Host/s to ping:pingするホストを入力します（カンマ区切り）。 例：www.cisco.com

URL到達可能性の設定

- 「チェックするURL」 – テストするURLを入力します（カンマ区切り）。 例：https://github.com
  - HTTP GET要求を使用して、到達可能性をテストします。
  - デフォルトポート：80(HTTP)/443(HTTPS)。 非標準ポート(ashttps://example.com:8443など)のURLにそのポートを含めます。
  - チェックごとの最大20のURL
  - タイムアウト：URLごとに30秒
  - URLごとに収集されるデータ：URL、到達可能性ステータス、HTTPステータスコード、応答時間（ミリ秒）、コンテンツ長、解決済みIPアドレス、TLSバージョン、およびタイムスタンプ。
  - 結果はreachability/reachability_results.jsonおよびreachability/reachability_summary.txtに保存されます。

ポリシーテストの設定

- 「ホストURL」 – ポリシーテスト用のホストを入力します（カンマ区切り、最大10）。 例：www.cisco.com
- ポリシーテストは、シスコのポリシーテストエンドポイント(policy.test.sse.cisco.com)で実行されます。
- 結果には、構造化ポリシーテストの出力と、テストナビゲーション中に自動的にキャプチャされたHARデータの両方が含まれます。

HARキャプチャ設定

- 「ターゲットURL」 — HARキャプチャのURLを入力します（カンマ区切り）。 例：https://www.cisco.com/

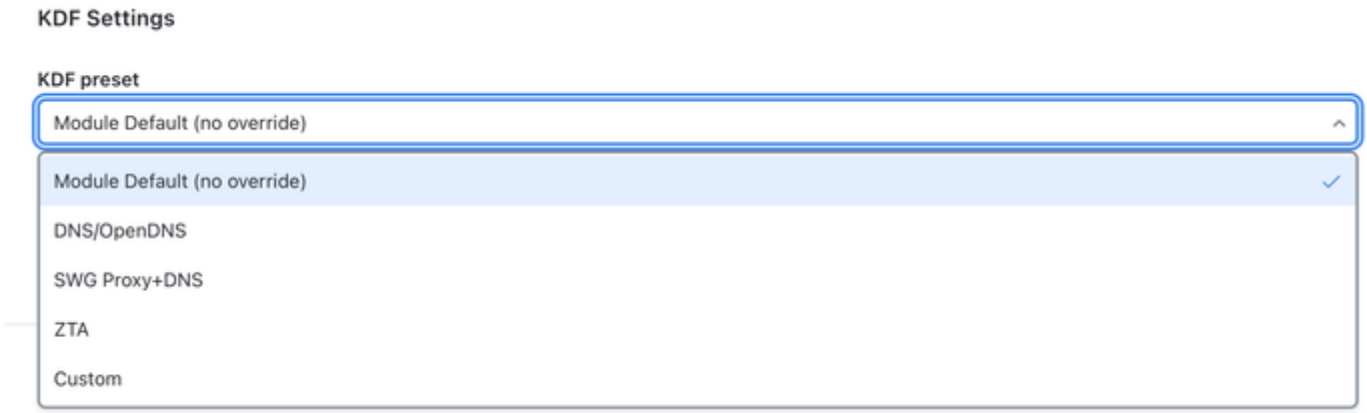
ヒント:HARキャプチャは現在Google Chromeのみをサポートしています。このツールは、Chrome DevToolsプロトコル（chromedp経由）を使用して、ヘッドレスChromeセッションを自動化し、ネットワークトラフィックをキャプチャします。Google Chromeがシステムにインストールされていることを確認します。現時点では、FirefoxとSafariはサポートされていません。

KDF設定

診断コレクション中に使用されるキー導出関数フラグを構成します。KDFフラグは、Cisco Secure Clientで有効にするデバッグカテゴリを制御します。

- 「KDFプリセット」 –「キー導出関数」プリセットを選択します。
- KDF HEX:16進数値は、選択したプリセットに基づいて自動的に入力されます。「カスタム」を選択した場合は、独自の16進数値を入力します。

Preset	Hex Value	Description
Module Default	*(none)*	No KDF override is applied. The Cisco Secure Client's built-in module defaults are used. This preserves the customer's current debug settings.
DNS/OpenDNS	`0x20801FF`	Enables DNS resolution and OpenDNS proxy debug flags via `acsocktool -sdf`.
SWG Proxy+DNS	`0x70C01FF`	Enables SWG + DNS debug flags via `acsocktool -sdf`. Also sets `SWGConfigOverride.json` with `"logLevel": "1"` for enhanced SWG logging.
ZTA (ZTNA)	`0x400080152`	Enables ZTA debug flags via `acsocktool -sdf`. Also sets `logconfig.json` with `"global": "DBG_TRACE"` for maximum verbosity logging. May trigger a VPN agent restart on Windows.
Custom	User-provided	Allows entering a custom hex value for advanced troubleshooting.



予約済みIP設定

- NSLookup URLs：オプションのカスタムnslookupホスト（カンマ区切り）。 最大10個のURL各カスタムホストは、設定されたすべてのリゾルバに対して照会されます。
- トレースURL：オプションのカスタムtraceroute/tracertホスト（カンマ区切り）。 最大10個のURLこのツールは、macOS/Linuxではtraceroute、Windowsではtracertを自動的に使用します。
- リゾルバIP:nslookupクエリ用のオプションのカスタムリゾルバIP（カンマ区切り。例：208.67.222）。
- 222、208.67.220.220)。 最大5つのIP指定した場合、3つの組み込みリゾルバ（システムデフォルトDNS、127.0.0.1、208.67.222.222）に加えてカスタムリゾルバが使用されます。

予約済みIPの詳細

予約済みIP診断は、デフォルトで次のデータを収集します。

デフォルトのtraceroute/tracertターゲット（これらすべてに対して自動的に実行）:

target	目的
208.67.222.222	OpenDNSプライマリネームサーバへのルート
208.67.220.220	OpenDNSセカンダリネームサーバへのルート
146.112.255.50	Cisco SWGインフラストラクチャIPへのルート
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	SWGプロキシホスト名へのルート

- macOS/Linux:tracerouteコマンドを使用する
- Windows:tracertコマンドを使用する

デフォルトのNSLookupクエリ（これらすべてに対して自動的に実行）:

各nslookupターゲットは、リゾルバリスト内の各リゾルバに対して照会されます。デフォルトでは、リゾルバリストには3つの組み込みリゾルバが含まれています。

Resolver	Description
System default DNS	The OS-configured DNS resolver (no explicit server argument)
`127.0.0.1`	Localhost / local DNS proxy (e.g., Cisco Secure Client's local resolver)
`208.67.222.222`	OpenDNS public resolver

カスタムリゾルバIP（208.67.222.222など）が設定されている場合、それらはリゾルバリストに追加され、すべてのnslookupターゲットもそれらに対して照会されます。

NSLookupターゲット：

Target	Query Type	Purpose
`debug.opendns.com`	TXT (`-type=txt`)	OpenDNS debug record — returns device identity, organization ID, policy flags, and server info
`swg-url-proxy-https-sse.sigproxy.qq.opendns.com`	A (default)	SWG proxy hostname resolution — verifies DNS is correctly resolving the SWG proxy endpoint

たとえば、デフォルトの3つのリゾルバがある場合、6つのnslookupクエリ（2つのターゲットx 3つのリゾルバ）が生成されます。 1つのカスタムリゾルバIPを追加すると、このクエリは8つになります（2ターゲットx 4リゾルバ）。

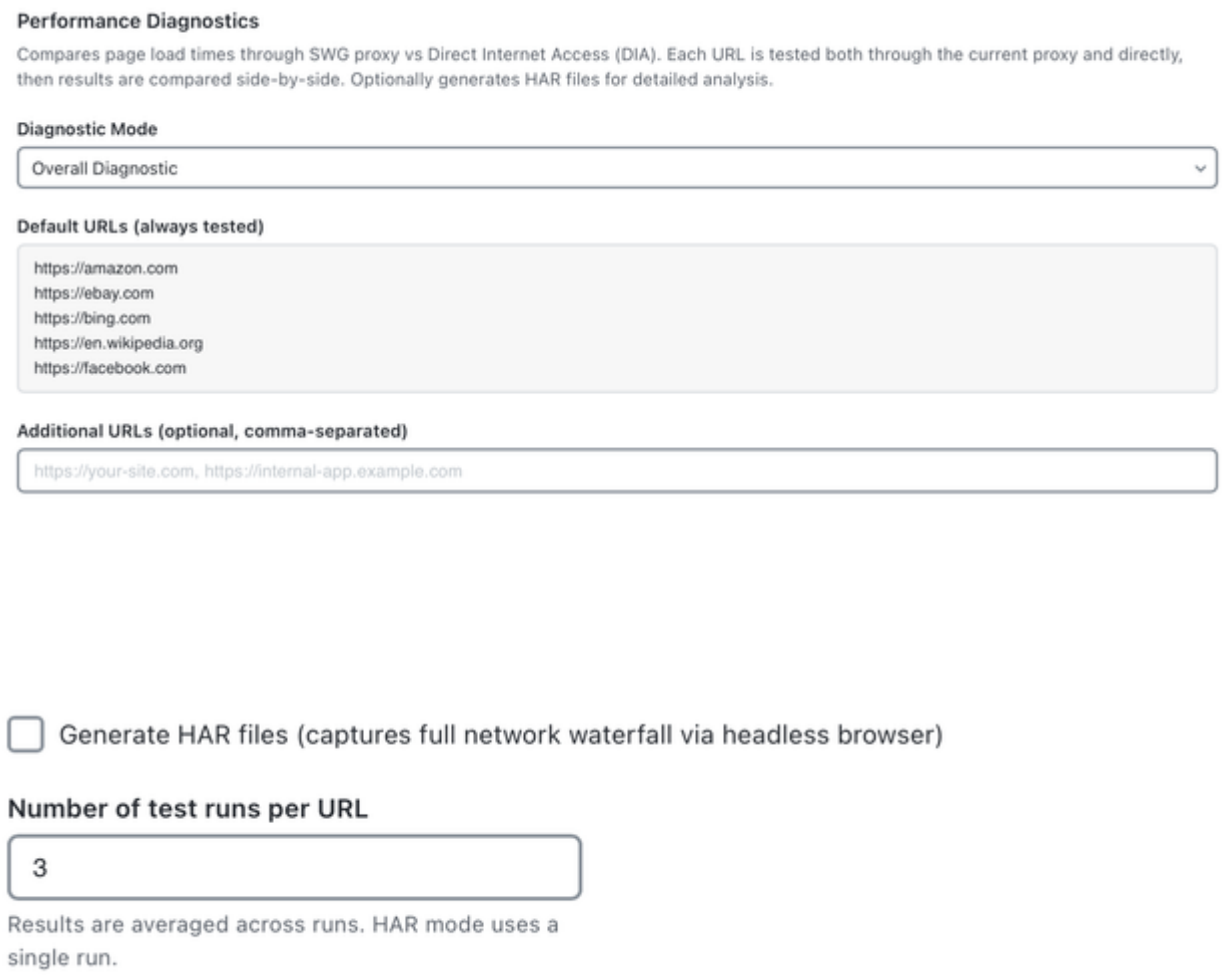
ユーザが指定したカスタムNSLookup URLは、それぞれ同じ完全なリゾルバリスト（組み込み+カスタムリゾルバ）に対して照会されます。

すべての結果は、単一のファイルreserved_ip/reserved_ip_diagnostics.txtに統合され、セクション(traceroute、nslookup)ごとにグループ化されます。このファイルには、エントリごとのターゲットとリゾルバを示す、人間が読める形式のヘッダーが含まれます。

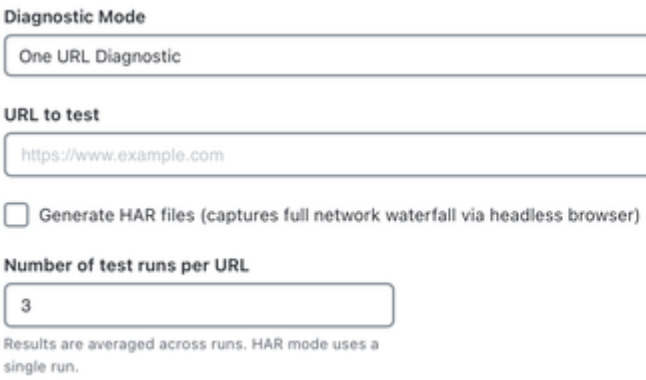
パフォーマンス診断

SWGプロキシとDirect Internet Access(DIA)を使用してページのロード時間を比較します。 次の2つのモードがあります。

1 全体診断モード：各URLは現在のプロキシと直接の両方でテストされ、結果が並べて比較されます。オプションで、詳細な分析用にHARファイルを生成します。



2 1つのURLの診断モード:現在のプロキシを介して、および直接の両方を介してテストされる特定のURLを入力できます。その結果は並べて比較されます。オプションで、詳細な分析用にHARファイルを生成します。

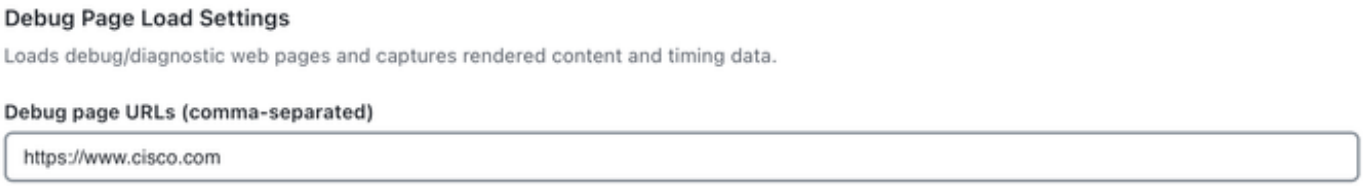


証明書ストアのインベントリ設定

- 構成された証明書ストアから証明書を列挙します：
  - システム
  - ログイン
  - Root
  - その他
- 不足している証明書、期限切れの証明書、信頼できない証明書をすばやく特定

デバッグページ読み込みの設定：

- 設定可能なデバッグURLをロードします。
- キャプチャ：
  - 応答ヘッダー
  - 応答本文
  - タイミング情報
  - SSLメタデータ



[アクション（Actions）]

1. 有効な診断ごとに設定を入力または調整します。
2. Start Diagnosticsをクリックして、診断の実行を開始します。
3. Backをクリックしてステップ1に戻るか、Cancelをクリックして終了します

注：検証エラーのあるフィールドは強調表示されます。診断を開始する前に、これらを修正する必要があります。

一時停止して続行

高度なトラブルシューティング(ZTNAまたはSWGトレースなど)を含む診断コレクションを実行すると、Cisco Endpoint Diagnostic Toolが実行の途中で一時停止し、続行する前に問題を再現するように求めるメッセージを表示することがあります。

これにより、詳細なロギングがオンになっている間に問題をトリガーする時間が与えられるため、サポートチームはより有用な診断データを受信します。

- Diagnostics Pausedウィンドウが表示されたら、現在アクティブなログ機能を示すメッセージを確認します。
- トラブルシューティングを行っている問題を再現します。例：
  - VPNへの再接続
  - 失敗している内部アプリケーションを開きます
  - エラーの原因となる手順を繰り返します
- 問題の再現が完了したら、Continueをクリックします。

走りを終わらせなさい。その後、このツールはファイルを収集し、通常の設定を復元し、診断アーカイブを作成します。

注：一時停止している間はアプリケーションを閉じないでください。ロギングは、Continueをクリックして実行を完了するまでアクティブなままです。

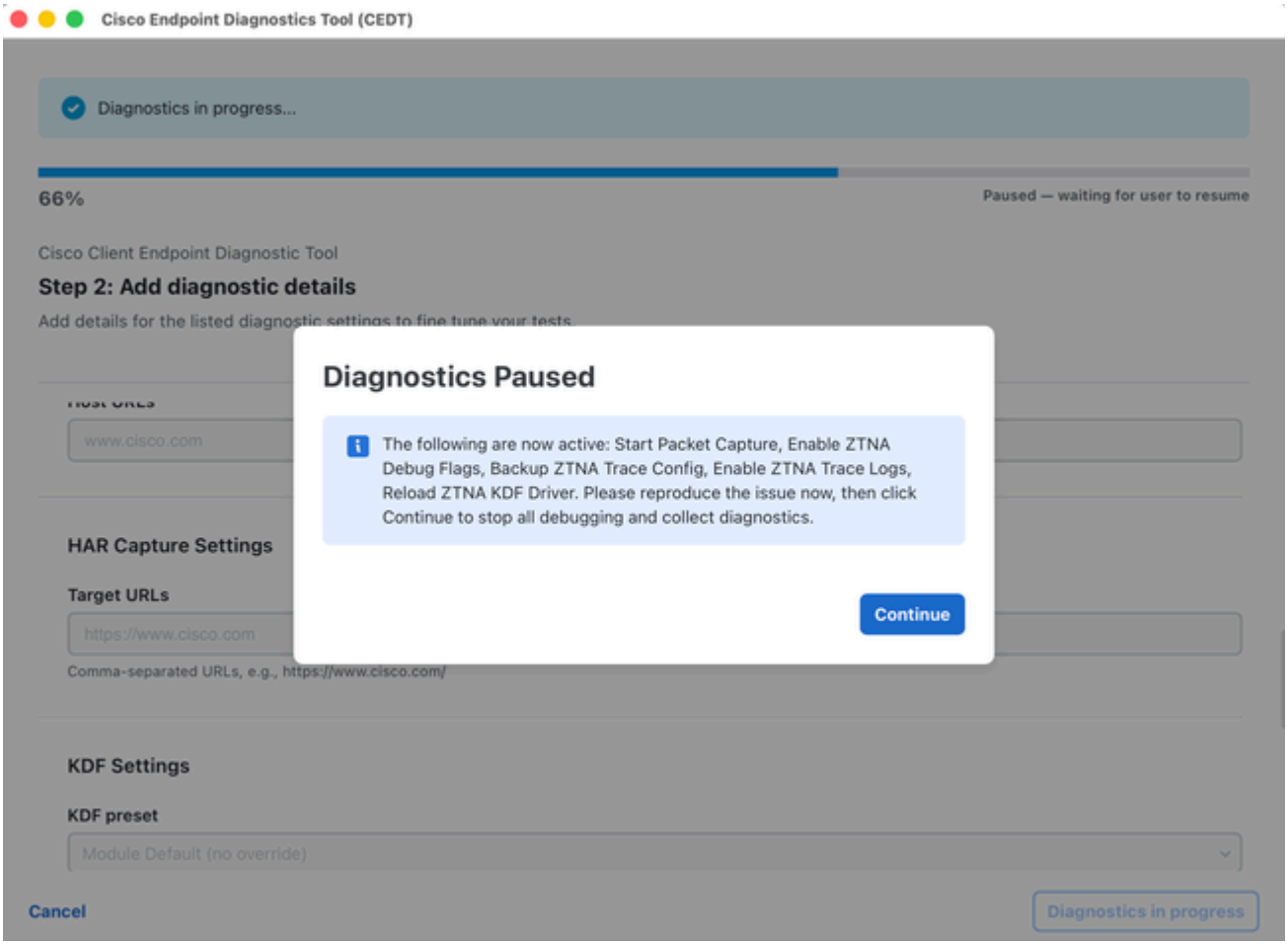
(コマンドライン)

端末からツールを実行している場合は、ダイアログボックスの代わりにウィンドウに一時停止メッセージが表示されます。

1. 端末に表示される一時停止メッセージを読みます。
2. 問題を再現します。

3. 端末に戻り、Enterキーを押して続行します。

4. 実行が完了するのを待ちます。



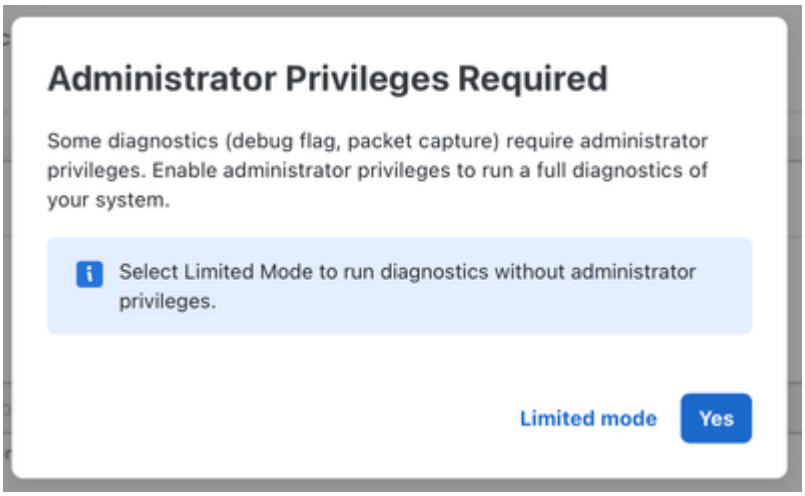
管理者権限プロンプト

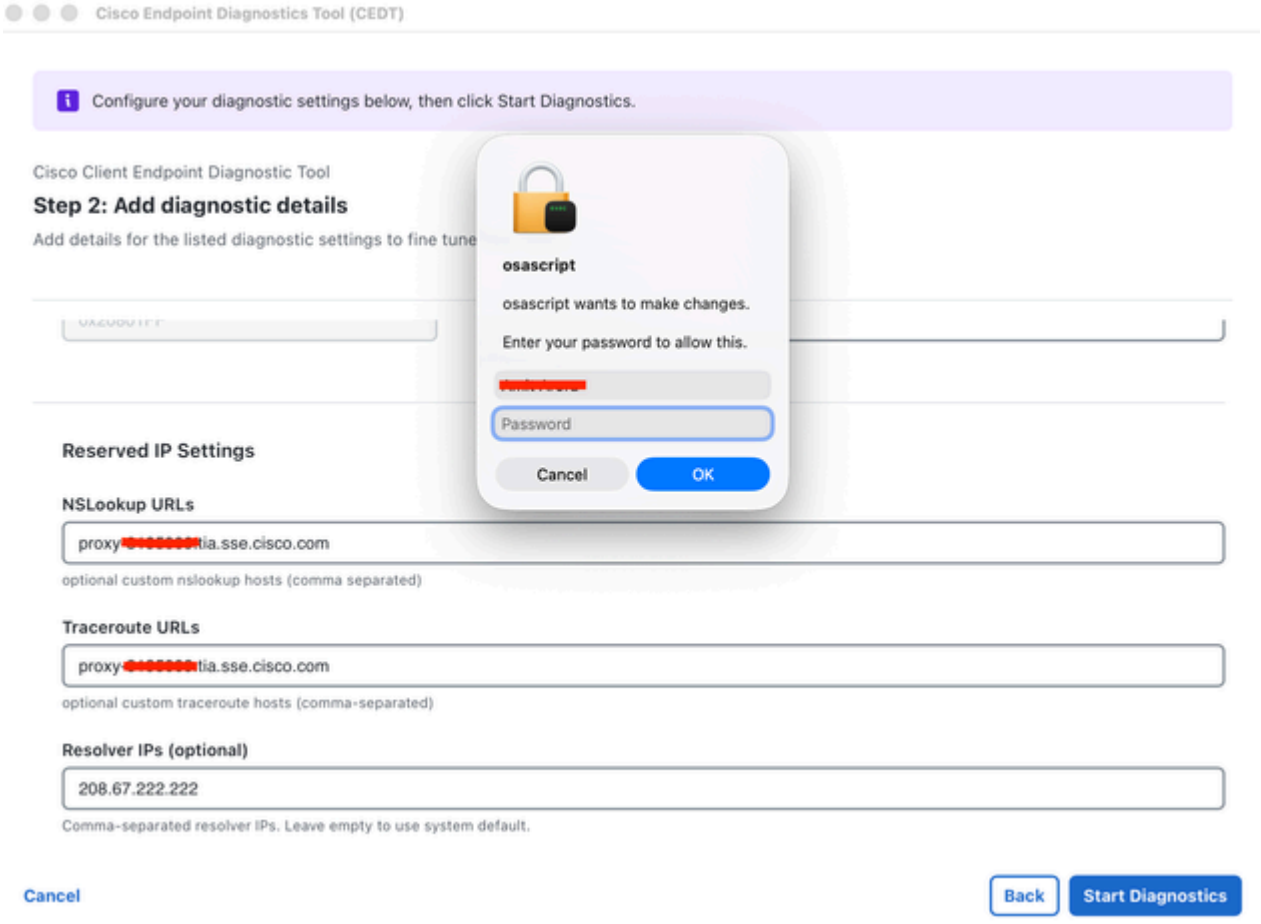
Start Diagnosticsをクリックした後、昇格されたアクセスが必要な機能（Packet CaptureやDebug Flagsなど）を有効にした場合は、管理者権限の入力を求められます。

ダイアログボックスが開き、「Administrator Privileges Required」というタイトルで表示されます。

- 管理者権限を付与するにはYesをクリックします。これにより、ネイティブmacOS/Windowsクレデンシャルプロンプトがトリガーされます。
- 制限モードをクリックして、立面図を表示せずに続行します。特権タスク（パケットキャプチャ、デバッグフラグ）はスキップされます。

- macOS: osascriptから標準のmacOSパスワードダイアログを表示できます。システムパスワードを入力し、OKをクリックします。
- Windows：標準のUAC昇格のプロンプトが表示されます。許可する場合はYesをクリックします。



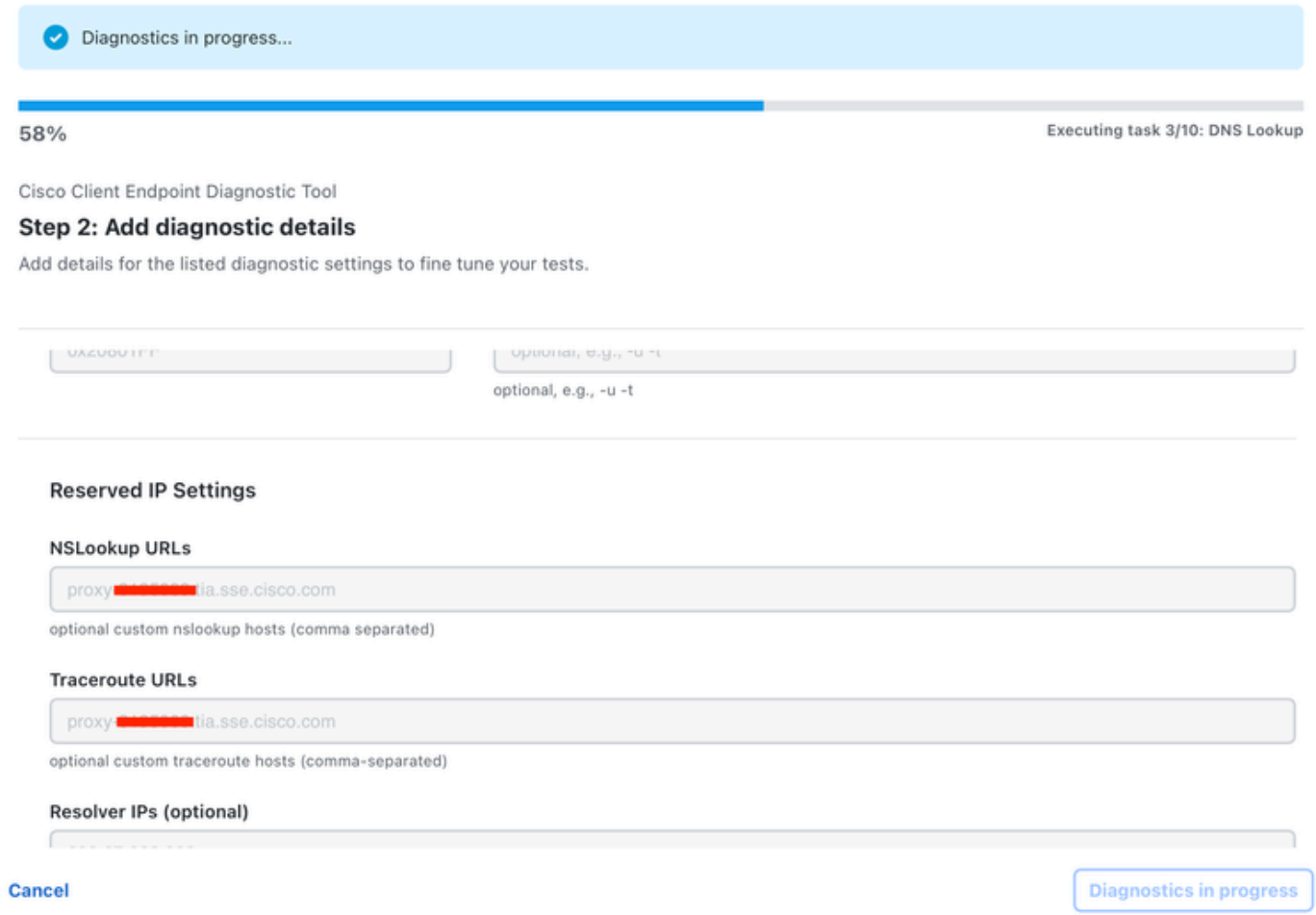


診断中

起動すると、選択したすべての診断タスクが実行されます。

- 進行状況バーに全体の完了が表示されます（59% — Executing task 3/9: DNS Lookupなど）。
- 上部に「Diagnostics in progress...」バナーが表示されます。
- 実行中は、すべての設定フィールドが無効またはグレー表示になります。
- フッターにDiagnostics in progressボタン（無効）が表示され、ツールがビジーであることが示されます。

診断が完了するまでお待ちください。アプリケーションを閉じないでください。



1.

診断の完了 – TACへのアップロード

すべての診断が終了すると、完了ダイアログが表示されます。

Diagnosticsが完了。TACケースにファイルをアップロードします。

ダイアログに次の情報が表示されます。

- Archive：生成された診断アーカイブのファイル名（cisco_diagnostics.tar.gzなど）。
- ファイルサイズ：アーカイブのサイズ（7.72 MBなど）。
- SHA256：整合性を検証するためのアーカイブファイルのチェックサム。

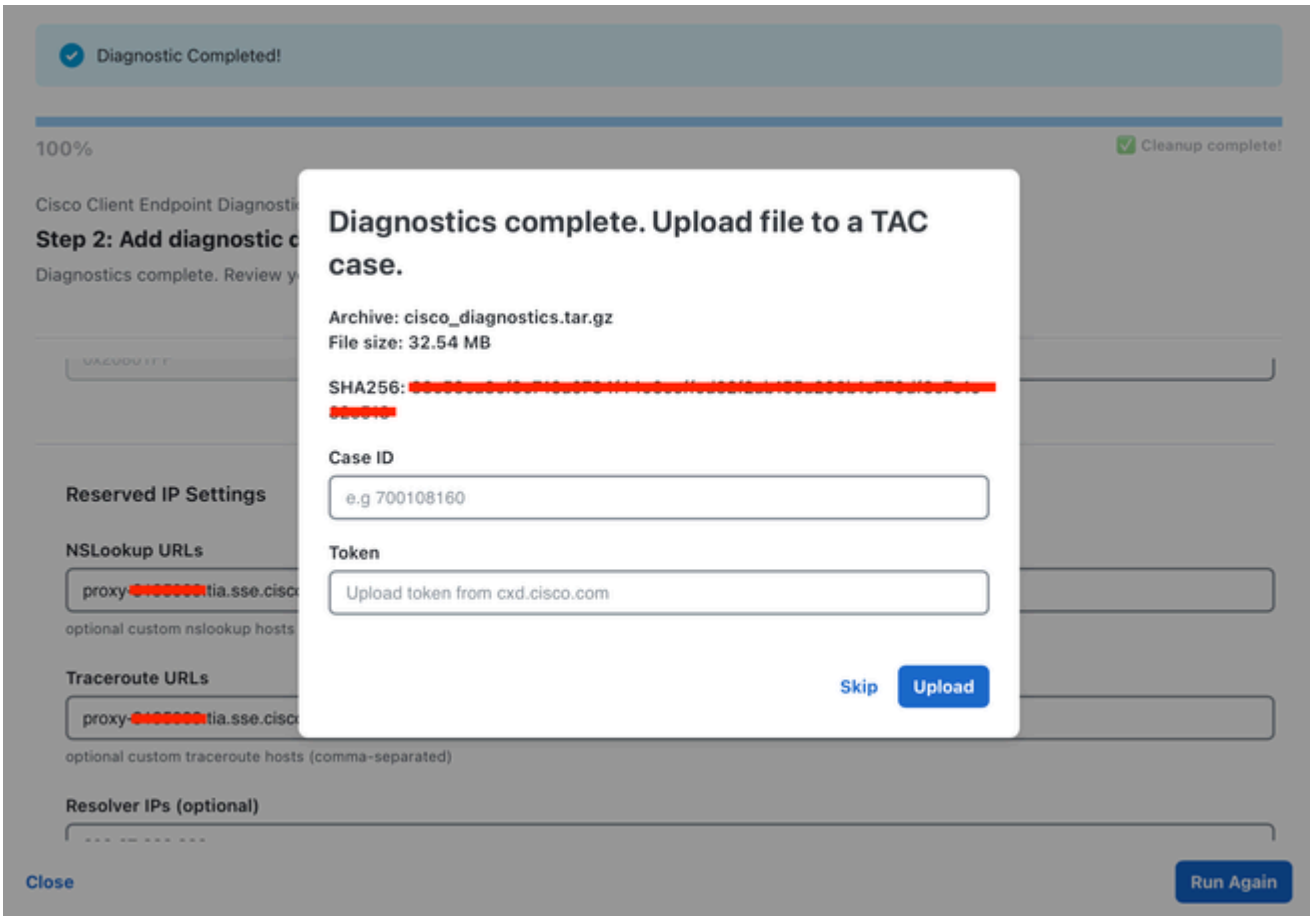
TACケースにアップロードするには、次の手順を実行します。

1. ケースID(698746730など)を入力します。
2. トークンを入力します（シスコサポートから提供）。
3. Open TAC Caseをクリックして、アップロードを開始します。

経過表示バーにアップロードステータスが表示されます(Uploading... 85.0 %(6.56 MB / 7.72 MB)など)。

アップロードをスキップするには、次の手順を実行します。

- Skipをクリックして、アップロードせずにダイアログを閉じます。アーカイブファイルはローカルに保存されたままです。



アップロード完了 – 最終画面

アップロードが成功すると、完了バナーが次のように更新されます。

診断アーカイブがケース[ケースID]に正常にアップロードされました

経過表示バーに100%とクリーンアップ完了ステータスが表示されます。

[アクション（Actions）]

- Run Againをクリックして、新しい診断実行を開始します。
- Closeをクリックして、アプリケーションを終了します。

出力場所

診断出力の保存先：

- macOS: ~ /Desktop/cisco_diagnostics/
- Windows: %USERPROFILE%\Desktop\cisco_diagnostics\

出力アーカイブファイル(cisco_diagnostics.tar.gz)には、収集されたすべての診断データが構造化された形式で含まれています。

トラブルシューティング

Issue	Resolution
No products detected	Ensure Cisco Secure Client is installed and running on your system.
Packet Capture greyed out	Enable it in Step 1, and grant administrator privileges when prompted.
Debug Flags greyed out	At least one Cisco Secure Access product must be detected and selected.
DebugView greyed out	This option is only available on Windows.
Upload fails	Verify your Case ID and Token are correct. Check your internet connection.
"Administrator credentials could not be obtained"	You cancelled the password prompt or entered an incorrect password. Click Start Diagnostics again to retry.
Limited mode warning	Some privileged tasks were skipped. Re-run with administrator privileges for a full diagnostic.

FAQ

Q：このツールでは、どのようなデータが収集されますか。
A：このツールは、Cisco Secure Accessモジュールのみに関連するシステム情報（OS、ハードウェア、ネットワーク構成）、アプリケーションログ、シスコ製品の構成とインストール済みモジュールデータ、およびネットワーク診断データを収集します。詳細な内訳については、前のセクションの「収集されるシステムデータ」を参照してください。個人データは取得されません。

Q：管理者またはrootのアクセス権は必要ですか。
A：管理者アクセスはオプションですが、推奨されます。このコマンドを使用しないと、一部の診断（パケットキャプチャ、デバッグフラグ）がスキップされます。このツールでは、プロンプトが表示され、選択できます。

Q：ツールを複数回実行できますか。
A：はい。実行が完了するたびに、[再実行]をクリックして新しい診断セッションを開始できます。

Q：出力はどこに保存されますか。
A：診断アーカイブは、デスクトップのcisco_diagnosticsフォルダに保存されます。

Q:TACケースIDがない場合はどうすればよいですか。
A：アップロードダイアログで「スキップ」をクリックできます。アーカイブファイルはローカルに保存されたままです。後でTACケースに手動でアップロードしたり、サポートエンジニアと共有したりできます。

Q：データは暗号化されていますか。
A：診断アーカイブは圧縮(tar.gz)され、機密データはパッケージ化の前に自動的に修正されます。

Q: HARキャプチャはどのブラウザをサポートしていますか。
A:HARキャプチャは、現在Google Chromeのみをサポートしています。このツールは、ヘッドレスブラウザの自動化にChrome DevTools Protocolを使用します。HARキャプチャを実行する前に、Chromeがインストールされていることを確認します。

Qポーズ画面が表示されません。何か問題でも？

A：必ずしもそうとは限りません。一時停止ステップは、シナリオに対して詳細ロギングが正常に有効化された場合にのみ表示されます。アプリの実行ログを確認します。有効化の手順をスキップした場合、ツールは一時停止せずに続行されます。

Q Runがスタックしているようです。どうすればよいでしょうか。

A: Diagnostics Pausedウィンドウを探します。このウィンドウは他のウィンドウの背後に表示されている可能性があります。Continueをクリックするか、コマンドラインでEnterキーを押すまで、配管は前方に移動しません。

Q期待していなかった機能がメッセージに記載されています。それは正常な状態ですか？

A：はい。このメッセージには、ツールでプラットフォームに対して有効になっているロギング

機能と、選択した診断オプションが表示されます。

Qポーズ中にアプリを閉じました。今度は？

A：診断コレクションを再実行し、完了させてください。ログがオンのままになっているかどうかわからない場合は、サポートエンジニアに連絡して指示を受けてください。

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。