Analyse des Endpoint Diagnostics-Tools (CEDT)

Inhalt

Einleitung

In diesem Dokument wird das CEDT beschrieben, um Diagnosedaten von Ihrem System zu sammeln und diese in einen Cisco TAC-Support-Ticket hochzuladen.

Voraussetzungen

Das Tool ist für MacOS und Windows verfügbar. Laden Sie das Tool herunter.

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- MacOS: Doppelklicken Sie auf Cisco Endpoint Diagnostics Tool (CEDT).app, um das Programm zu starten.
- Windows: Doppelklicken Sie auf CEDT.exe, um das Programm zu starten.
- Eine aktive Internetverbindung.
- Eine Cisco TAC Case-ID und ein Token (nur erforderlich, wenn Sie die Ergebnisse direkt hochladen möchten).

Erfasste Systemdaten

Das Tool sammelt diese Systemdaten, geordnet nach Kategorien. Es werden keinerlei personenbezogene Daten erfasst.

Allgemeine Systeminformationen

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

Netzwerkkonfiguration

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`

Cisco Produktinformationen

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

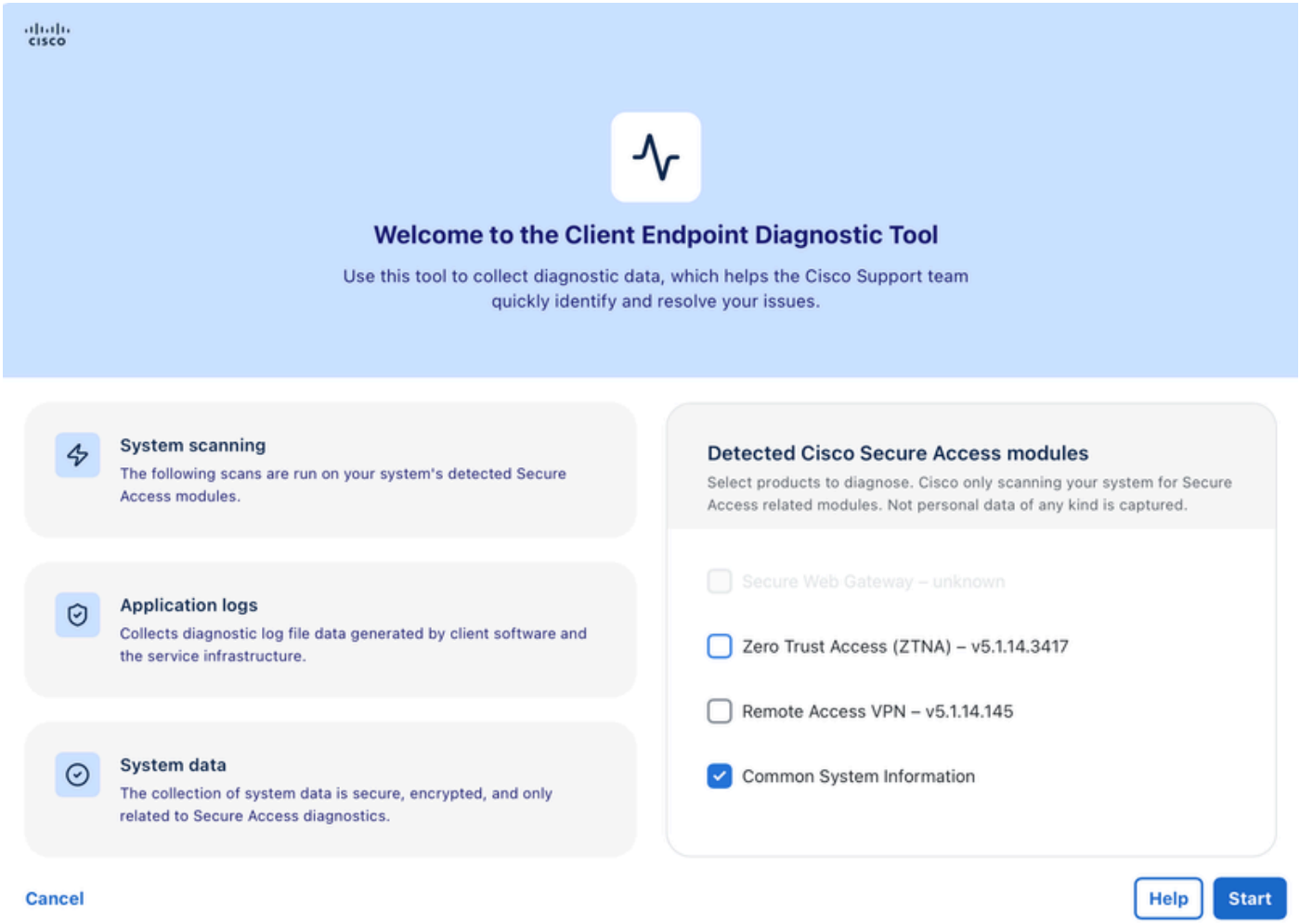
Schritt-für-Schritt-Anleitung

Willkommensseite

Wenn Sie CEDT starten, wird der Begrüßungsbildschirm angezeigt. Es bietet einen Überblick über die Funktionen des Tools:

- System-Scanning - Durchsucht Ihr System nach erkannten Cisco Secure Access-Modulen.
- Anwendungsprotokolle - Erfasst Diagnoseprotokolldateidaten, die von der Clientsoftware und der Serviceinfrastruktur generiert werden.
- Systemdaten - Die Erfassung der Systemdaten erfolgt sicher und verschlüsselt und bezieht

sich ausschließlich auf die Secure Access-Diagnose.



Auf der rechten Seite erkennt das Tool automatisch alle installierten Cisco Secure Access-Module in Ihrem System. Sie können Kontrollkästchen für jedes erkannte Modul zusammen mit seiner Versionsnummer sehen:

- ZTNA (Zero Trust Access)
- Sicheres Web-Gateway (SWG)
- Remote Access-VPN (RAVPN)
- Allgemeine Systeminformationen (immer verfügbar)

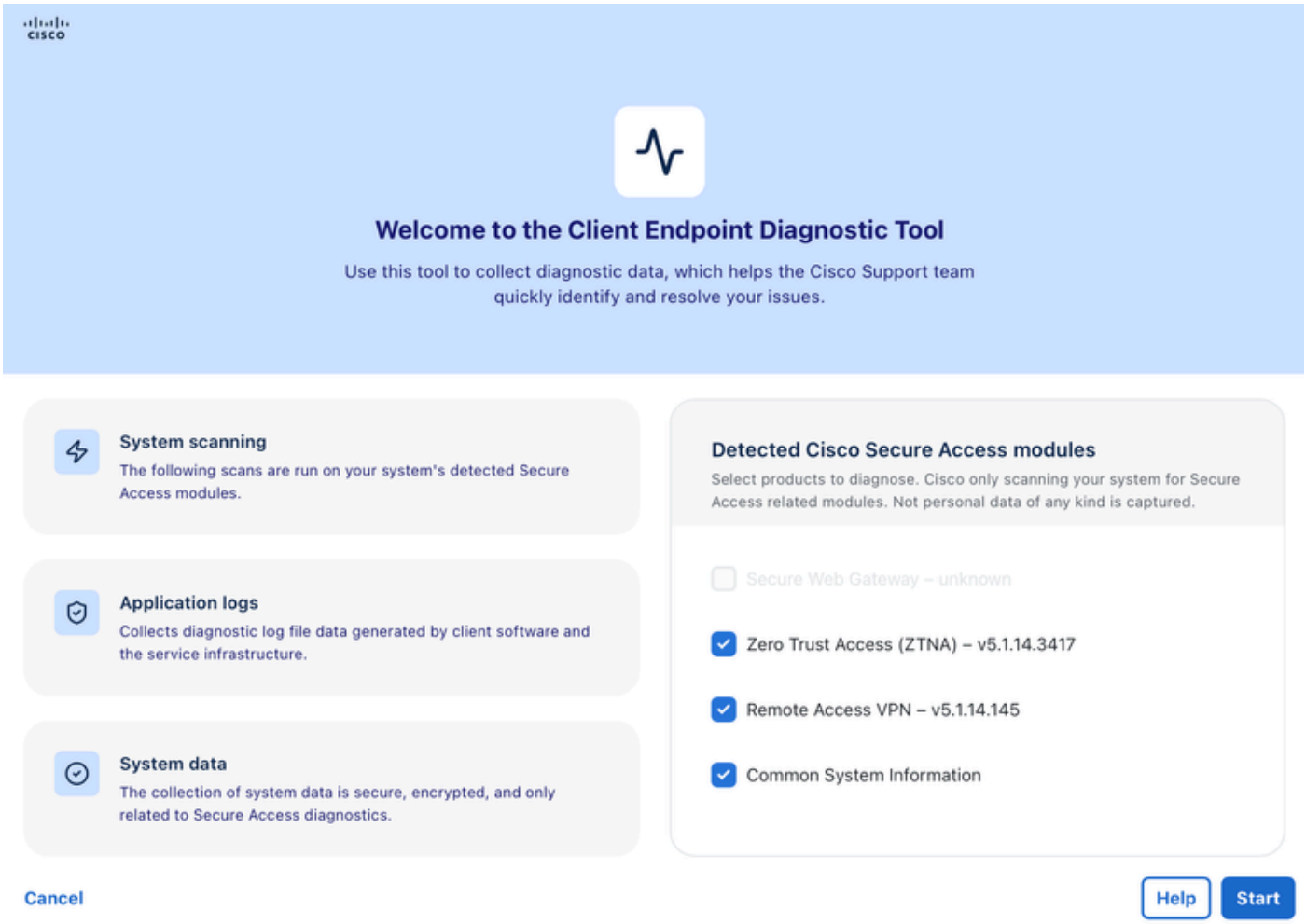
Aktionen

1. Wählen Sie die Produkte aus, die Sie diagnostizieren möchten, oder heben Sie die Auswahl

auf.

2. Klicken Sie auf Starten, um fortzufahren, oder klicken Sie auf Hilfe, um weitere Informationen zu erhalten.

Anmerkung: Dieses Tool erfasst nur Daten für Module, die im Zusammenhang mit sicherem Zugriff stehen. Es werden keinerlei personenbezogene Daten erfasst.



Schritt 1: Diagnosedatenerfassung

In diesem Bildschirm können Sie auswählen, welche Diagnosetests und Datenerfassungsmodule enthalten sein sollen.

Netzwerkdiagnose

Auswählen der auszuführenden Verbindungstests:

- DNS Lookup (DNS-Suche): Führt DNS-Auflösungstests für angegebene Hosts durch. Unterstützt benutzerdefinierte Resolver-IPs für zielgerichtete Suchvorgänge. Alle Ergebnisse werden in einer einzigen Ausgabedatei (dns/dns_lookups.txt) mit strukturierten Abschnittstrennzeichen zusammengefasst.
- Paketerfassung — Erfasst Netzwerkpakete für einen bestimmten Zeitraum (erfordert Administratorrechte). Siehe Paketerfassungsdetails.
- Ping-Hosts - Ping an angegebene Hosts, um die Verbindung zu überprüfen.
- Richtlinientestausgabe - Testet die Richtliniendurchsetzung mit angegebenen URLs unter Verwendung des Cisco Richtlinientestendpunkts (policy.test.sse.cisco.com). Unterstützt mehrere durch Kommata getrennte Hosts (maximal 10). Die Ergebnisse umfassen HAR-Daten, die während der Richtlinientestnavigation automatisch erfasst werden.
- Network Speed Test: Misst die Upload-/Download-Geschwindigkeit und die Latenz mit dem Cisco Speed Test-Endgerät (speed.test.sse.cisco.com). Erfasst Download-Geschwindigkeit (6 parallele Streams), Upload-Geschwindigkeit (3 parallele Streams) und Ping-Latenz/Jitter (10 ICMP-Samples). Die Ergebnisse werden sowohl im JSON- als auch im Textübersichtsformat gespeichert.
- URL-Erreichbarkeit - Überprüft, ob die angegebenen URLs mithilfe von HTTP GET-Anforderungen erreichbar sind. Unterstützt standardmäßig HTTP (Port 80) und HTTPS (Port 443). Nicht standardmäßige Ports können in der URL angegeben werden (z. B. https://example.com:8443). Maximal 20 URLs pro Prüfung mit einem Timeout von 30 Sekunden pro URL. Zu den pro URL erfassten Daten gehören: URL, Erreichbarkeitsstatus, HTTP-Statuscode, Antwortzeit (ms), Inhaltslänge, aufgelöste IP-Adresse, TLS-Version und Zeitstempel. Die Ergebnisse werden unter reachability/reachability_results.json und reachability/reachability_summary.txt gespeichert.

Datensammlung

Wählen Sie Module aus, um Leistungs- und Verbindungsdaten zu erfassen:

- HAR Capture: Zeichnet HAR-Daten (HTTP Archive) aus einer Browsersitzung auf. Derzeit wird nur Google Chrome unterstützt (verwendet das Chrome DevTools Protocol über

Headless Browser-Automatisierung). Das Tool erkennt automatisch die Chrome-Installation auf Ihrem System. Firefox und Safari werden derzeit nicht unterstützt. Die HAR-Ausgabe entspricht der HAR 1.2-Spezifikation und umfasst vollständige Netzwerk-Traces (einschließlich JS-ausgelöster XHR-/Fetch-Aufrufe).

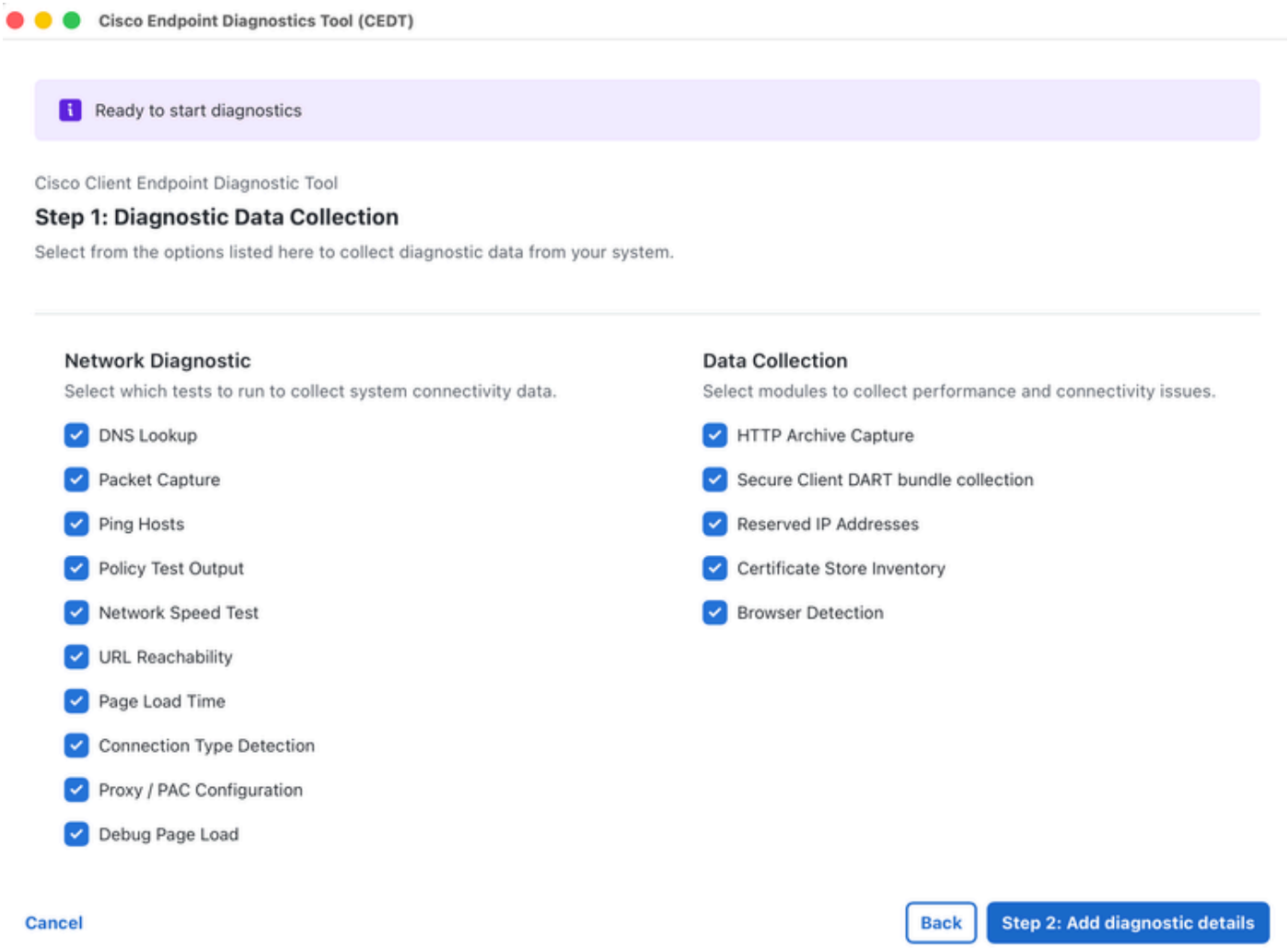
- DART Bundle Collection: Erfasst ein DART-Diagnosepaket vom Cisco Secure Client. Dies umfasst alle Modulprotokolle, einschließlich ZTA-Protokolle (Zero Trust Access) (wie z. B. flowlog.db unter C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\).
- Reserved IP (Reservierte IP): Führt Diagnoseprüfungen mit reservierten IP-Adressen durch. Eine vollständige Liste der erfassten Diagnosen finden Sie im nächsten Abschnitt.

Fehlersuche

- Debug-Flags aktivieren - Sammeln detaillierter Protokolle von Endpunktaktivitäten, um Endpunkteprobleme zu diagnostizieren. Diese Option ist nur verfügbar, wenn mindestens ein Cisco Secure Access-Produkt erkannt und ausgewählt wurde.

Plattformspezifisch

- DebugView Capture (Windows) - Aktiviert die Debug-Protokollierung auf dem Windows Secure Endpoint Connector. Diese Option ist nur auf Windows-Systemen verfügbar.



Aktionen

1. Aktivieren bzw. deaktivieren Sie die gewünschten Diagnoseoptionen.
2. Klicken Sie auf Schritt 2: Fügen Sie Diagnosedetails hinzu, um fortzufahren.
3. Klicken Sie auf Zurück, um zum Willkommensbildschirm zurückzukehren, oder auf Abbrechen, um den Vorgang zu beenden.

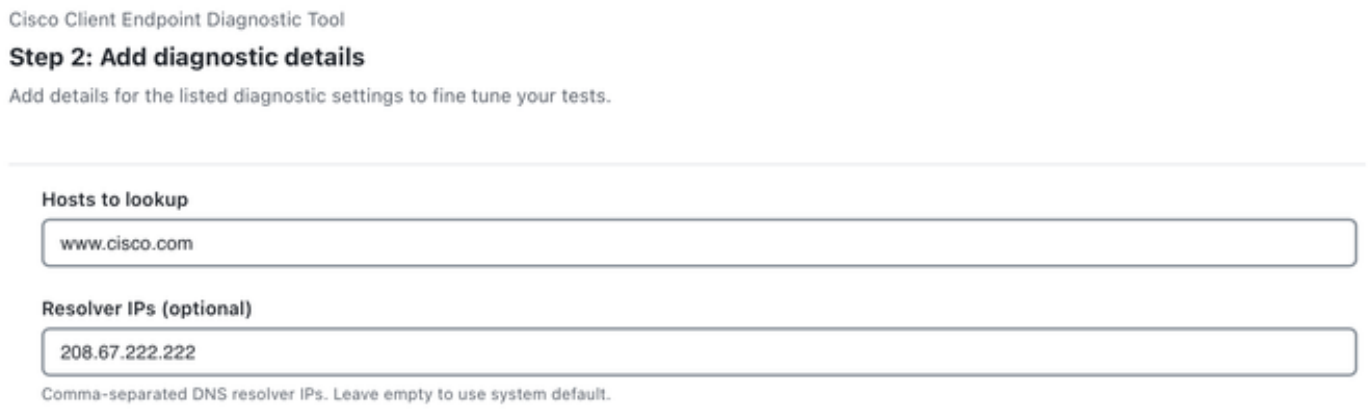
Phase 2: Diagnosedetails hinzufügen

Auf diesem Bildschirm können Sie die spezifischen Parameter für jeden aktivierten Diagnosetest konfigurieren. Es werden nur Einstellungen für Tests angezeigt, die Sie in Schritt 1 aktiviert haben.

DNS-Sucheinstellungen

- Zu suchende Hosts — Geben Sie einen oder mehrere Hostnamen ein (durch Komma getrennt). Beispiel: cisco.com
- Resolver-IPs (optional) — Geben Sie benutzerdefinierte DNS-Resolver-IPs ein (durch Komma getrennt). Beispiel: 208.67.222.222, 208.67.220.220. Leer lassen, um den DNS-Standardresolver des Systems zu verwenden. Wenn angegeben, wird jeder Host für jeden Resolver abgefragt, um Vergleichsergebnisse für die DNS-Auflösung auf verschiedenen DNS-Servern zu erhalten.

Alle DNS-Suchergebnisse werden in einer einzigen Ausgabedatei zusammengefasst: dns/dns_lookups.txt, mit strukturierten TextFSM-Abschnittstrennzeichen für jede Host-/Resolver-Kombination.



Einstellungen zur Paketerfassung

- Interfaces (Schnittstellen) - Wählen Sie die Netzwerkschnittstelle aus, die erfasst werden soll (oder belassen Sie diese als Alle).

- Bei Einstellung "Alle" (Auto-Modus):
    - macOS/Linux: Das Tool führt tcpdump -D aus, um alle verfügbaren Schnittstellen aufzulisten, und filtert dann nach aktiven und aktiven Schnittstellen (mit Ausnahme nicht verbundener Schnittstellen). Wenn keine aktiven Schnittstellen gefunden werden, geht dies auf die spezielle any-Schnittstelle zurück. Die Erfassungen werden auf allen übereinstimmenden Schnittstellen parallel ausgeführt.
    - Windows: Erfasst alle NICs mit dem ausgewählten Capture-Backend (siehe Tools im nächsten Abschnitt). Bei Verwendung von dumpcap ohne Interface werden bis zu die ersten 3 erkannten Interfaces gleichzeitig erfasst.
- Paketanzahl - Anzahl der Pakete, die pro Schnittstelle erfasst werden sollen. Standard: 100. Maximal: 10,000.
- Dauer (Sek.) - Die maximale Erfassungsdauer in Sekunden. Standard: 20 Sekunden unter MacOS/Linux, 5 Sekunden unter Windows. Maximal: 300 Sekunden. Die Erfassung wird beendet, wenn entweder die Paketanzahl oder die Zeitdauer erreicht ist, je nachdem, welcher Fall zuerst eintritt.

Tools zur Paketerfassung nach Plattform

Anmerkung: (Windows): Das Tool wählt automatisch das beste verfügbare Capture-Backend aus. pktmon wird bevorzugt (integriert in Windows 10 v2004+), zurück zu dumpcap (wenn Wireshark installiert ist), dann netsh trace als letztes Mittel.

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

Ausgabedateien der Paketerfassung

Die Erfassung jeder Schnittstelle wird unter Verwendung der Namenskonvention als separate Datei gespeichert: tcpdump/{interface_name}_capture.pcap (z. B. en0_capture.pcap, eth0_capture.pcap). Außerdem wird eine Metadaten-Manifestdatei (tcpdump/packet_capture_manifest.txt) generiert, in der die Plattform, die Paketanzahl, die Dauer, die erfassten Schnittstellen und das verwendete Datenerfassungs-Backend aufgezeichnet werden.

Ping-Einstellungen

- Host/s für Ping - Geben Sie die Hosts für Ping ein (durch Komma getrennt). Beispiel:www.cisco.com

URL-Erreichbarkeitseinstellungen

- Zu prüfende URLs — Geben Sie zu testende URLs ein (durch Komma getrennt). Beispiel: `https://github.com`
    - Verwendet HTTP GET-Anforderungen, um die Erreichbarkeit zu testen.
    - Standard-Ports: 80 (HTTP)/443 (HTTPS). Schließen Sie den Port bei nicht standardmäßigen Ports (z. B. ashttps://example.com:8443) in die URL `ein`.

- Maximal 20 URLs pro Prüfung.
- Zeitüberschreitung: 30 Sekunden pro URL.
- Pro URL erfasste Daten: URL, Erreichbarkeitsstatus, HTTP-Statuscode, Antwortzeit (ms), Inhaltslänge, aufgelöste IP-Adresse, TLS-Version und Zeitstempel.
- Die Ergebnisse werden unter reachability/reachability_results.json und reachability/reachability_summary.txt gespeichert.

Richtlinien-Testeinstellungen

- Host-URLs - Geben Sie Hosts für Richtlinientests ein (durch Komma getrennt, maximal 10). Beispiel: www.cisco.com
- Richtlinientests werden mit dem Cisco-Richtlinientestendpunkt durchgeführt: policy.test.sse.cisco.com
- Die Ergebnisse umfassen sowohl strukturierte Richtlinientestausgaben als auch HAR-Daten, die während der Testnavigation automatisch erfasst werden.

HAR-Erfassungseinstellungen

- Ziel-URLs — Geben Sie URLs für die HAR-Erfassung ein (durch Komma getrennt). Beispiel: https://www.cisco.com/

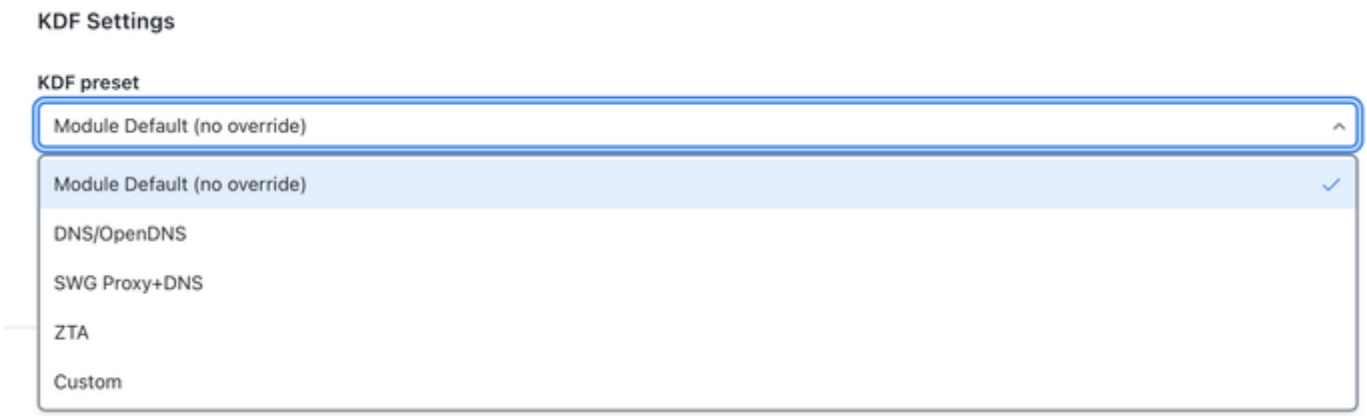
Tipp: HAR Capture unterstützt derzeit nur Google Chrome. Das Tool verwendet das Chrome DevTools Protocol (über Chromedp), um eine kopflose Chrome-Sitzung zu automatisieren und den Netzwerkverkehr zu erfassen. Stellen Sie sicher, dass Google Chrome auf Ihrem System installiert ist. Firefox und Safari werden derzeit nicht unterstützt.

KDF-Einstellungen

Konfigurieren Sie die Kennzeichen für die Schlüsselableitungsfunktion, die während der Diagnosesammlung verwendet werden. KDF-Flags steuern, welche Debug-Kategorien im Cisco Secure Client aktiviert sind:

- KDF-Vorgabe — Wählen Sie eine Vorgabe für die Tastenableitungsfunktion.
- KDF HEX - Der Hexadezimalwert wird automatisch anhand der gewählten Voreinstellung eingetragen. Wenn "Benutzerdefiniert" ausgewählt ist, geben Sie Ihren eigenen Hexadezimalwert ein.

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.



Reservierte IP-Einstellungen

- NSLookup-URLs — Optionale benutzerdefinierte nslookup-Hosts (durch Komma getrennt). Maximal 10 URLs Jeder benutzerdefinierte Host wird für alle konfigurierten Resolver abgefragt.
- Trace-URLs - Optionale benutzerdefinierte Traceroute-/Tracert-Hosts (durch Komma getrennt). Maximal 10 URLs Das Tool verwendet automatisch Traceroute unter macOS/Linux und tracert unter Windows.
- Resolver IPs - Optionale benutzerdefinierte Resolver-IPs für nslookup-Abfragen (durch Komma getrennt, z. B. 208.67.222).
- 222, 208.67.220.220). Maximal 5 IPs. Wenn angegeben, werden zusätzlich zu den drei integrierten Resolvern (System Default DNS, 127.0.0.1, 208.67.222.222) benutzerdefinierte Resolver verwendet.

Reservierte IP-Details

Die Diagnose für reservierte IP sammelt diese Daten standardmäßig:

Standardziele für Traceroute/Tracert (automatisch für alle diese Ziele ausführen):

Ziel	Zweck
208.67.222.222	Route zu OpenDNS Primärer Namenserver
208.67.220.220	Route zu sekundärem OpenDNS-Namenserver
146.112.255.50	Weiterleitung an Cisco SWG-Infrastruktur-IP
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	Route zu SWG-Proxy-Hostname

- macOS/Linux: Verwendet den Befehl traceroute
- Windows: Verwendet den Befehl tracert

Standard-NSLookup-Abfragen (automatisch für alle diese Abfragen ausführen):

Jedes nslookup-Ziel wird für jeden Resolver in der Resolverliste abgefragt. Standardmäßig enthält die Resolverliste drei integrierte Resolver:

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

Wenn benutzerdefinierte Resolver-IPs konfiguriert sind (z. B. 208.67.222.222), werden diese zur Resolverliste hinzugefügt, und jedes nslookup-Ziel wird ebenfalls für sie abgefragt.

NSLookup-Ziele:

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

Bei den drei Standardresolvern werden beispielsweise 6 nslookup-Abfragen (2 Ziele x 3 Resolver) erzeugt. Durch Hinzufügen einer benutzerdefinierten Resolver-IP-Adresse wird diese Zahl auf 8 Abfragen erhöht (2 Ziele x 4 Resolver).

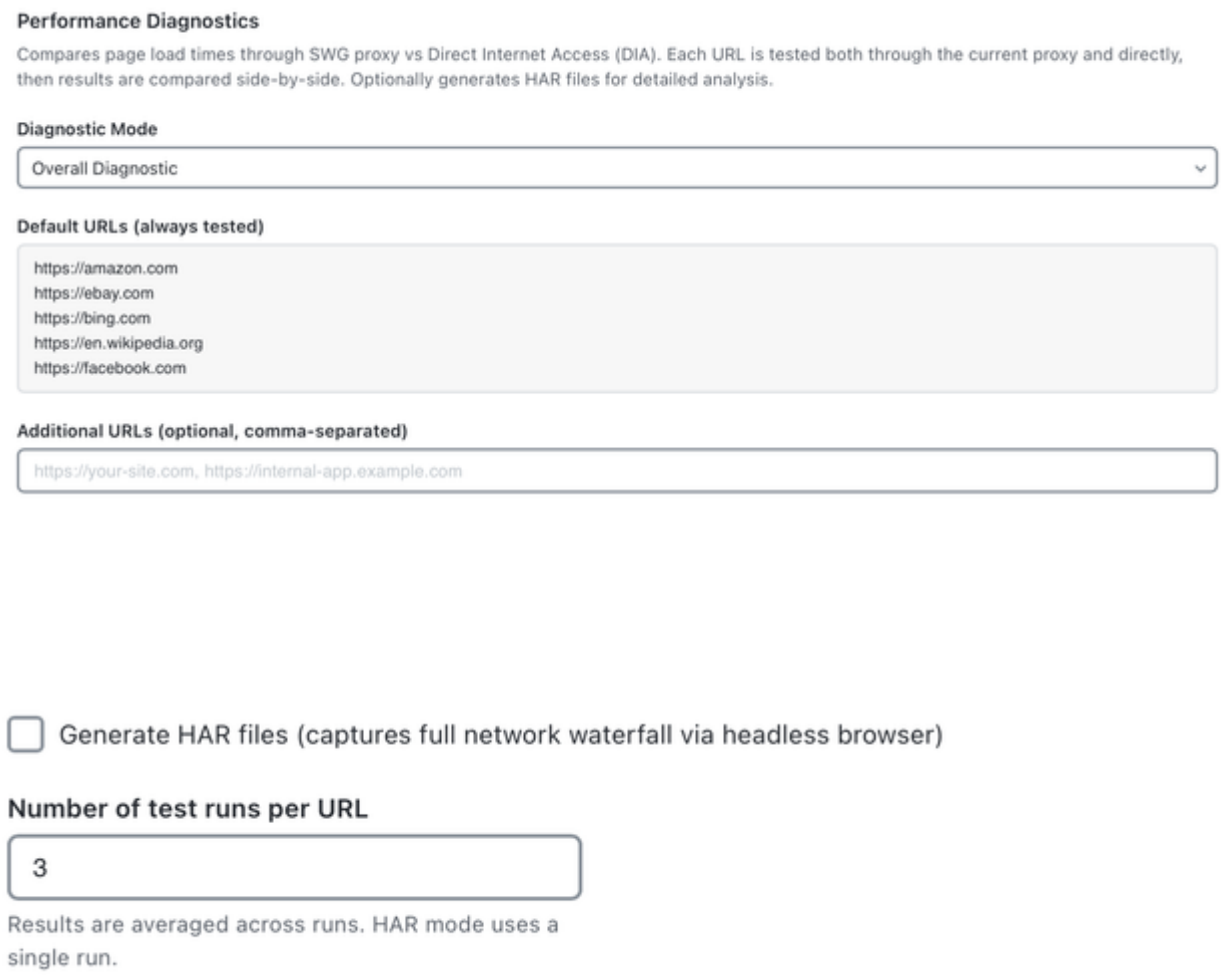
Benutzerdefinierte, vom Benutzer bereitgestellte NSLookup-URLs werden für dieselbe Liste vollständiger Resolver (integrierte + benutzerdefinierte Resolver) abgefragt.

Alle Ergebnisse werden in einer einzigen Datei zusammengefasst: reserved_ip/reserved_ip_diagnostics.txt, gruppiert nach Abschnitt (traceroute, nslookup) mit für Menschen lesbaren Headern, die das Ziel und den Resolver für jeden Eintrag angeben.

Leistungsdiagnose

Vergleicht die Ladezeiten der Seiten über den SWG-Proxy mit denen von Direct Internet Access (DIA). Es gibt zwei Modi:

1 Allgemeiner Diagnosemodus: Jede URL wird sowohl über den aktuellen Proxy als auch direkt getestet, und die Ergebnisse werden nebeneinander verglichen. Generiert optional HAR-Dateien für detaillierte Analysen.



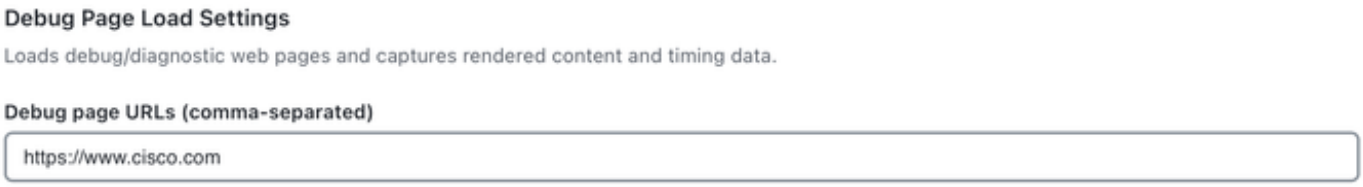
2 Ein URL-Diagnosemodus: Wir können eine bestimmte URL eingeben, die sowohl über den aktuellen Proxy als auch direkt getestet werden soll. Anschließend werden die Ergebnisse Seite an Seite verglichen. Generiert optional HAR-Dateien für detaillierte Analysen.

Bestandseinstellungen für den Zertifikatsspeicher

- Listet Zertifikate aus konfigurierten Zertifikatspeichern auf:
  - System
  - Anmelden
  - Wurzel
  - Und mehr
- Schnelle Identifizierung fehlender, abgelaufener oder nicht vertrauenswürdiger Zertifikate

Einstellungen zum Laden der Debugseite:

- Lädt konfigurierbare Debug-URLs.
- Aufnahmen:
  - Antwort-Header
  - Reaktionskörper
  - Timing-Informationen
  - SSL-Metadaten



Aktionen

1. Füllen Sie die Einstellungen für jede aktivierte Diagnose aus, oder passen Sie sie an.
2. Klicken Sie auf Diagnose starten, um den Diagnosevorgang zu starten.
3. Klicken Sie auf Zurück, um zu Schritt 1 zurückzukehren, oder auf Abbrechen, um den

Vorgang zu beenden.

Anmerkung: Felder mit Validierungsfehlern werden hervorgehoben. Sie müssen diese korrigieren, bevor die Diagnose gestartet werden kann.

Anhalten und Fortfahren

Wenn Sie eine Diagnosesammlung mit erweiterter Fehlerbehebung (z. B. ZTNA- oder SWG-Ablaufverfolgung) ausführen, hält das Cisco Endpoint Diagnostic Tool möglicherweise einen Teil der Ausführung an und fordert Sie auf, das Problem zu reproduzieren, bevor es fortgesetzt wird.

Dadurch haben Sie Zeit, das Problem auszulösen, während die detaillierte Protokollierung aktiviert ist, sodass das Support-Team weitere nützliche Diagnosedaten erhält.

- Wenn das Fenster Diagnostics Paused (Diagnose angehalten) angezeigt wird, lesen Sie die Meldung, die Ihnen mitteilt, welche Protokollfunktionen jetzt aktiv sind.
- Reproduzieren Sie das Problem, das Sie beheben. Beispiele:
    - Verbindung mit VPN wiederherstellen
    - Öffnen Sie die fehlerhafte interne Anwendung.
    - Wiederholen Sie die Schritte, die den Fehler verursachen.
- Wenn Sie das Problem nicht reproduziert haben, klicken Sie auf Weiter

Lass den Lauf zu Ende laufen. Das Tool sammelt Dateien, stellt Ihre normalen Einstellungen wieder her und erstellt das Diagnosearchiv.

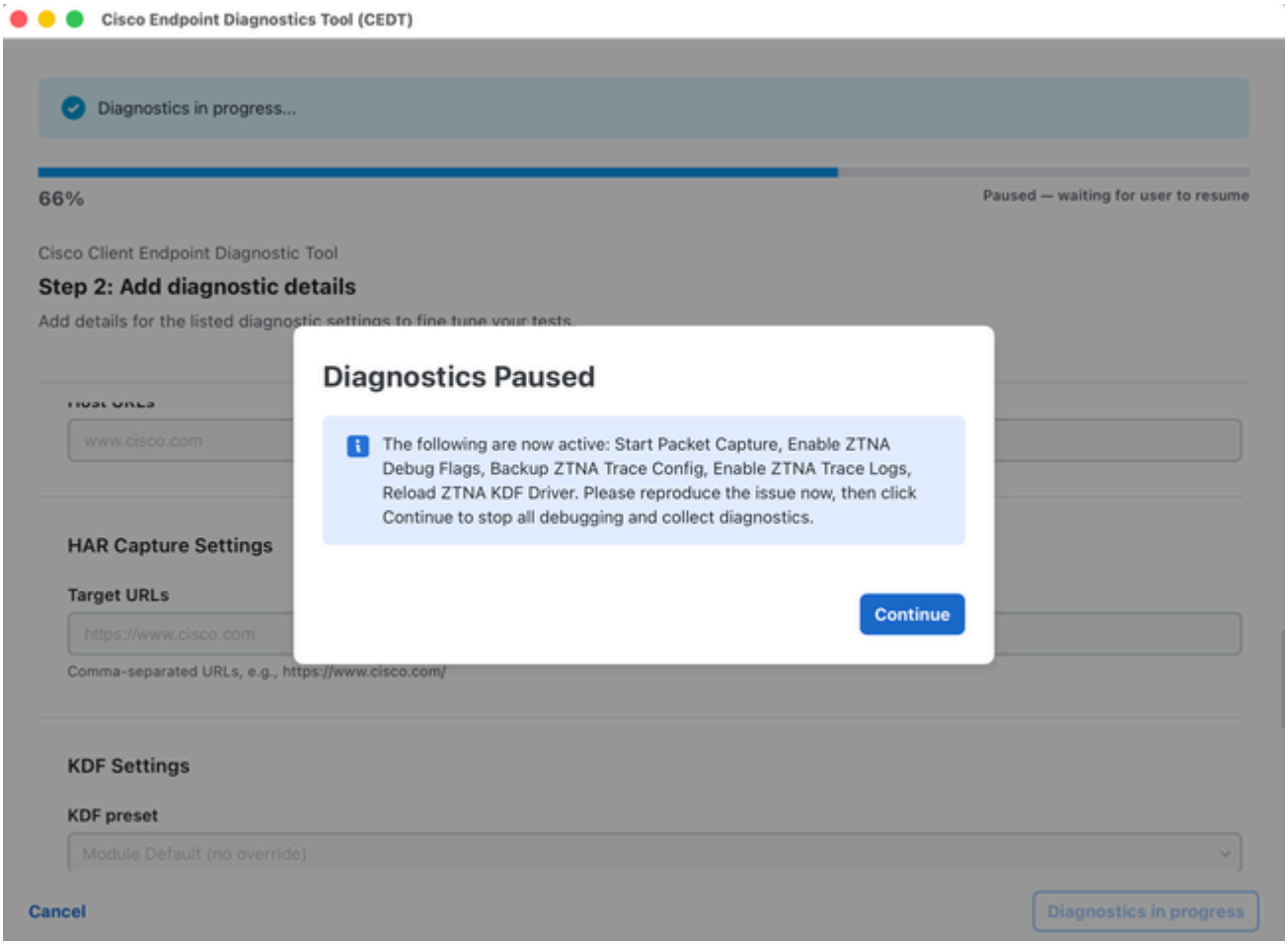
HINWEIS:Schließen Sie die Anwendung nicht, während sie angehalten wird. Die Protokollierung bleibt aktiv, bis Sie auf Weiter klicken und der Vorgang abgeschlossen ist.

(Befehlszeile)

Wenn Sie das Tool von einem Terminal aus ausführen, wird im Fenster anstelle eines Dialogfelds eine Pausenmeldung angezeigt.

1. Lesen Sie die im Terminal angezeigte Pausenmeldung.

2. Reproduzieren des Problems
3. Kehren Sie zum Terminal zurück, und drücken Sie die Eingabetaste, um fortzufahren.
4. Warten Sie, bis der Lauf beendet ist.



Aufforderung für Administratorberechtigungen

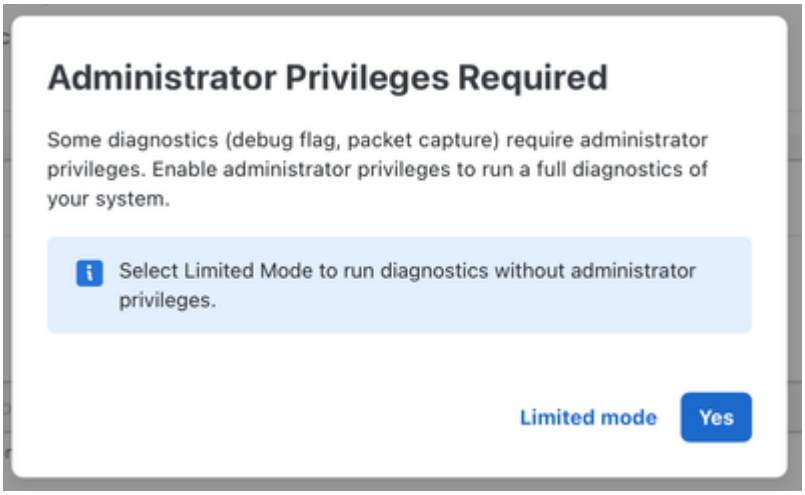
Nachdem Sie auf Diagnose starten geklickt haben, kann das Tool Sie zur Eingabe von Administratorberechtigungen auffordern, wenn Sie Funktionen aktiviert haben, für die erhöhter Zugriff erforderlich ist (z. B. Paketerfassung oder Debug-Flags).

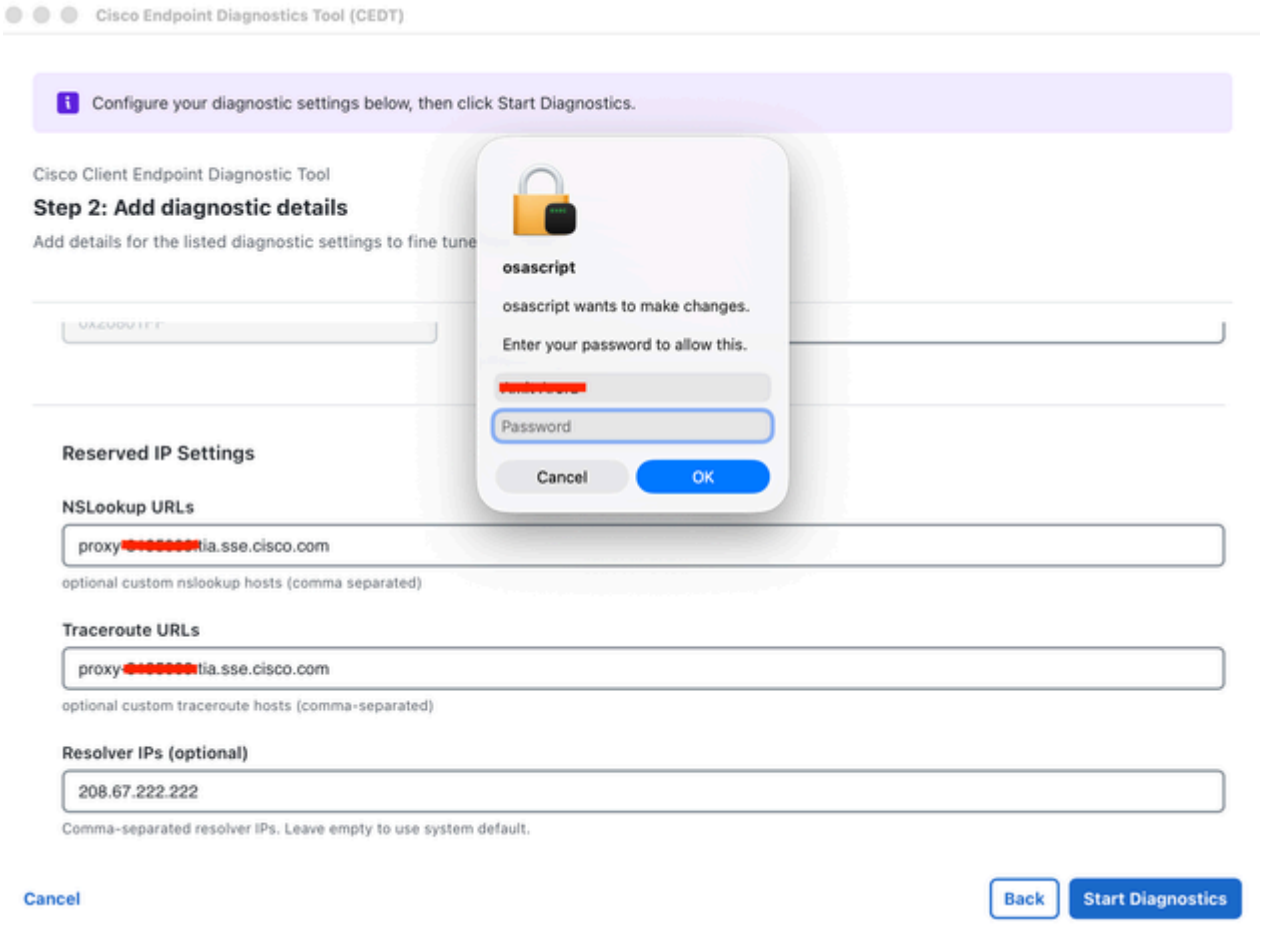
Es erscheint ein Dialogfeld mit dem Titel Administrator Privileges Required:

- Klicken Sie auf Ja, um Administratorberechtigungen zu erteilen. Dadurch wird die systemeigene macOS/Windows-Eingabeaufforderung für Anmeldeinformationen ausgelöst.
- Klicken Sie auf Eingeschränkter Modus, um ohne Erhöhung fortzufahren. Privilegierte Tasks

(Paketerfassung, Debugflags) werden übersprungen.

- MacOS: Das Standardpasswortdialogfeld von macOS ist in osascript zu sehen. Geben Sie Ihr Systemkennwort ein, und klicken Sie auf OK.
- Windows: Eine Standard-Eingabeaufforderung zur Erhöhung der Benutzerkontensteuerung wird angezeigt. Klicken Sie zum Zulassen auf Ja.



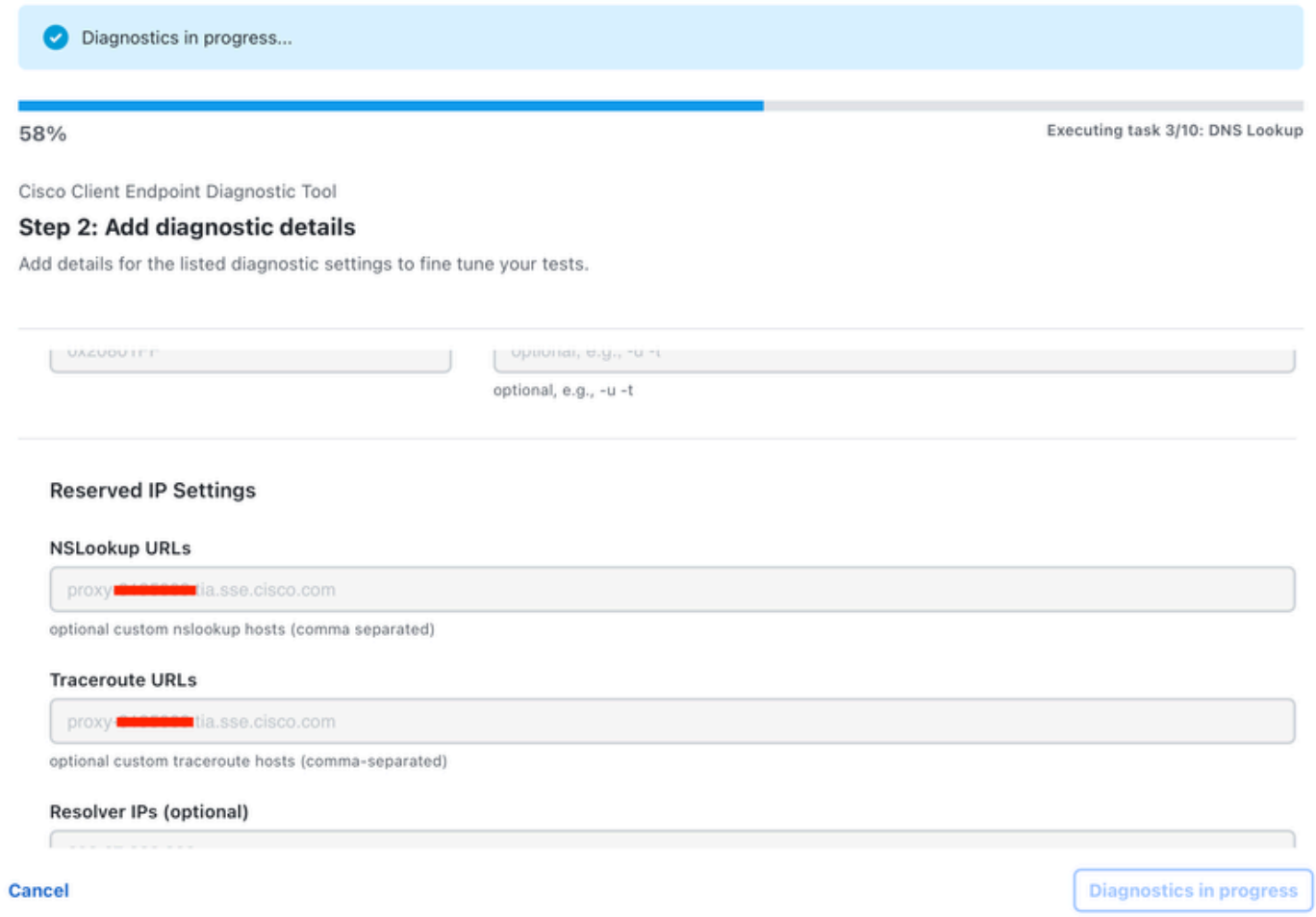


Diagnose wird durchgeführt

Nach dem Start durchläuft das Tool alle ausgewählten Diagnosetasks:

- Ein Fortschrittsbalken zeigt den Abschluss insgesamt an (z. B. 59 % - Aufgabe 3/9 wird ausgeführt: DNS Lookup).
- Eine Diagnose wird durchgeführt... Das Banner wird oben angezeigt.
- Alle Einstellungsfelder sind während des Ablaufs deaktiviert/ausgegraut.
- In der Fußzeile wird eine Schaltfläche "Diagnostics in progress" (Diagnose wird durchgeführt) angezeigt (deaktiviert), die anzeigt, dass das Tool beschäftigt ist.

Warten Sie, während die Diagnose abgeschlossen ist. Schließen Sie die Anwendung nicht.



1.

Diagnose abgeschlossen - Upload in TAC

Nach Abschluss der Diagnose wird ein Abschlussdialog angezeigt:

Die Diagnose ist abgeschlossen. Datei in ein TAC-Ticket hochladen

Das Dialogfeld wird angezeigt:

- Archiv - Der Dateiname des erzeugten Diagnosearchivs (z. B. cisco_diagnostics.tar.gz).
- Dateigröße - Die Größe des Archivs (z. B. 7,72 MB).
- SHA256 - Die Prüfsumme der Archivdatei für die Integritätsüberprüfung.

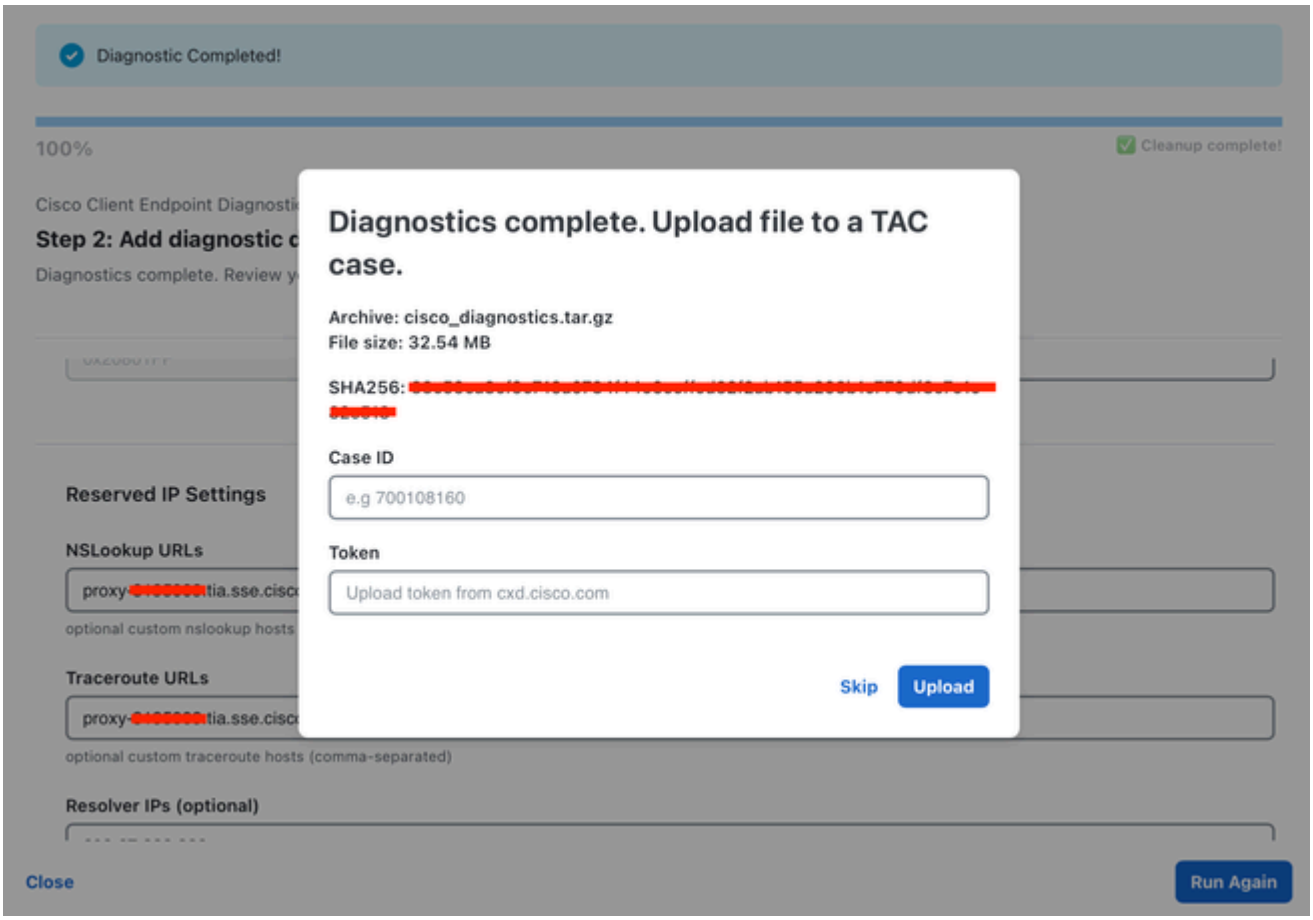
So laden Sie Daten in ein TAC-Ticket hoch:

1. Geben Sie Ihre Ticket-ID ein (z. B. 698746730).
2. Geben Sie Ihr Token ein (wird vom Cisco Support bereitgestellt).
3. Klicken Sie auf TAC-Ticket öffnen, um den Upload zu starten.

Ein Fortschrittsbalken zeigt den Uploadstatus an (z.B. Uploading... 85,0 % (6,56 MB/7,72 MB).

So überspringen Sie den Upload:

- Klicken Sie auf Überspringen, um den Dialog ohne Hochladen zu schließen. Die Archivdatei wird weiterhin lokal gespeichert.



Upload abgeschlossen/Abschlussbildschirm

Nach dem erfolgreichen Upload wird das Abschlussbanner wie folgt aktualisiert:

Diagnosearchiv erfolgreich in Ticket hochgeladen [Case ID]

Der Fortschrittsbalken zeigt 100 % mit dem Status Cleanup complete (Bereinigung abgeschlossen) an.

Aktionen

- Klicken Sie auf Erneut ausführen, um einen neuen Diagnosevorgang zu starten.
- Klicken Sie auf Schließen, um die Anwendung zu beenden.

Ausgabespeicherort

Diagnoseausgabe wird gespeichert in:

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

Die Ausgabearchivdatei (cisco_diagnostics.tar.gz) enthält alle gesammelten Diagnosedaten in einem strukturierten Format.

Fehlerbehebung

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.

Häufig gestellte Fragen

F: Welche Daten erfasst dieses Tool?
A : Das Tool erfasst nur Systeminformationen (Betriebssystem, Hardware, Netzwerkkonfiguration), Anwendungsprotokolle, Cisco Produktkonfigurationen und installierte Module sowie Netzwerkdiagnosedaten für Cisco Secure Access-Module. Eine detaillierte Aufschlüsselung finden Sie im Abschnitt Welche Systemdaten gesammelt werden im vorherigen Abschnitt. Es werden

keine persönlichen Daten erfasst.

F: Benötige ich Administrator-/Root-Zugriff?
A : Der Administratorzugriff ist optional, aber empfehlenswert. Andernfalls werden einige Diagnosen (Paketerfassung, Debugging-Flags) übersprungen. Das Tool fordert Sie auf, eine Auswahl zu treffen.

F: Kann ich das Tool mehrmals ausführen?
A : Ja. Nach Abschluss jedes Tests können Sie auf "Erneut ausführen" klicken, um eine neue Diagnosesitzung zu starten.

F: Wo wird die Ausgabe gespeichert?
A : Das Diagnosearchiv wird auf Ihrem Desktop im Ordner cisco_diagnostics gespeichert.

F: Was passiert, wenn ich keine TAC-Ticket-ID habe?
A : Sie können im Upload-Dialog auf "Überspringen" klicken. Die Archivdatei wird weiterhin lokal gespeichert. Sie können die Informationen zu einem späteren Zeitpunkt manuell in ein TAC-Ticket hochladen oder sie an Ihren Support-Techniker weitergeben.

F: Werden die Daten verschlüsselt?
A : Das Diagnosearchiv wird komprimiert (tar.gz) und sensible Daten werden vor dem Verpacken automatisch komprimiert.

F: Welche Browser werden von HAR unterstützt?
A : HAR capture unterstützt derzeit nur Google Chrome. Das Tool verwendet das Chrome DevTools Protocol für die kopflose Browser-Automatisierung. Stellen Sie sicher, dass Chrome installiert ist, bevor Sie HAR capture ausführen.

Q Der Pausenbildschirm wurde nie angezeigt. Stimmt etwas nicht?

A : Nicht unbedingt. Der Schritt zum Anhalten wird nur angezeigt, wenn die detaillierte Protokollierung für Ihr Szenario erfolgreich aktiviert wurde. Überprüfen Sie das Ausführungsprotokoll in der App. Wenn die Aktivierungsschritte übersprungen wurden, wird das Tool ohne Unterbrechung fortgesetzt.

Q Der Lauf scheint festzustecken. Was soll ich tun?

A : Suchen Sie nach dem Fenster Diagnostics Paused (Diagnose angehalten), das sich möglicherweise hinter anderen Fenstern befindet. Der Lauf wird erst fortgesetzt, wenn Sie auf Weiter klicken (oder in der Befehlszeile die Eingabetaste drücken).

F In der Nachricht sind die Funktionen aufgeführt, die ich nicht erwartet habe. Ist das normal?

A : Ja. Die Meldung zeigt an, welche Protokollierungsfunktionen das für Ihre Plattform aktivierte Tool und die von Ihnen ausgewählten Diagnoseoptionen verwenden.

F Ich habe die App während der Pause geschlossen. Was nun?

A : Führen Sie die Diagnosesammlung erneut aus, und lassen Sie sie abschließen. Wenn Sie sich nicht sicher sind, ob die Protokollierung aktiviert wurde, wenden Sie sich an Ihren Supporttechniker.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.