# Begrijp de Endpoint Diagnostics Tool (CEDT)

## Inhoud

# Inleiding

Dit document beschrijft de CEDT om diagnostische gegevens van uw systeem te verzamelen en deze te uploaden naar een ondersteuningsgeval voor Cisco TAC.

# Voorwaarden

De tool is beschikbaar voor MacOS en Windows. Download de tool.

Cisco raadt kennis van de volgende onderwerpen aan:

- MacOS: Dubbelklik op Cisco Endpoint Diagnostics Tool (CEDT).app om te starten.
- Windows: Dubbelklik op CEDT.exe om te starten.
- Een actieve internetverbinding.
- Een Cisco TAC Case ID en Token (alleen vereist als u de resultaten rechtstreeks wilt uploaden).

# verzamelde systeemgegevens

De tool verzamelt deze systeemgegevens, gerangschikt per categorie. Er worden geen persoonlijke gegevens van welke aard dan ook verzameld.

## Algemene systeeminformatie

| 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 |

## Netwerkconfiguratie

| 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-productinformatie

| 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 |

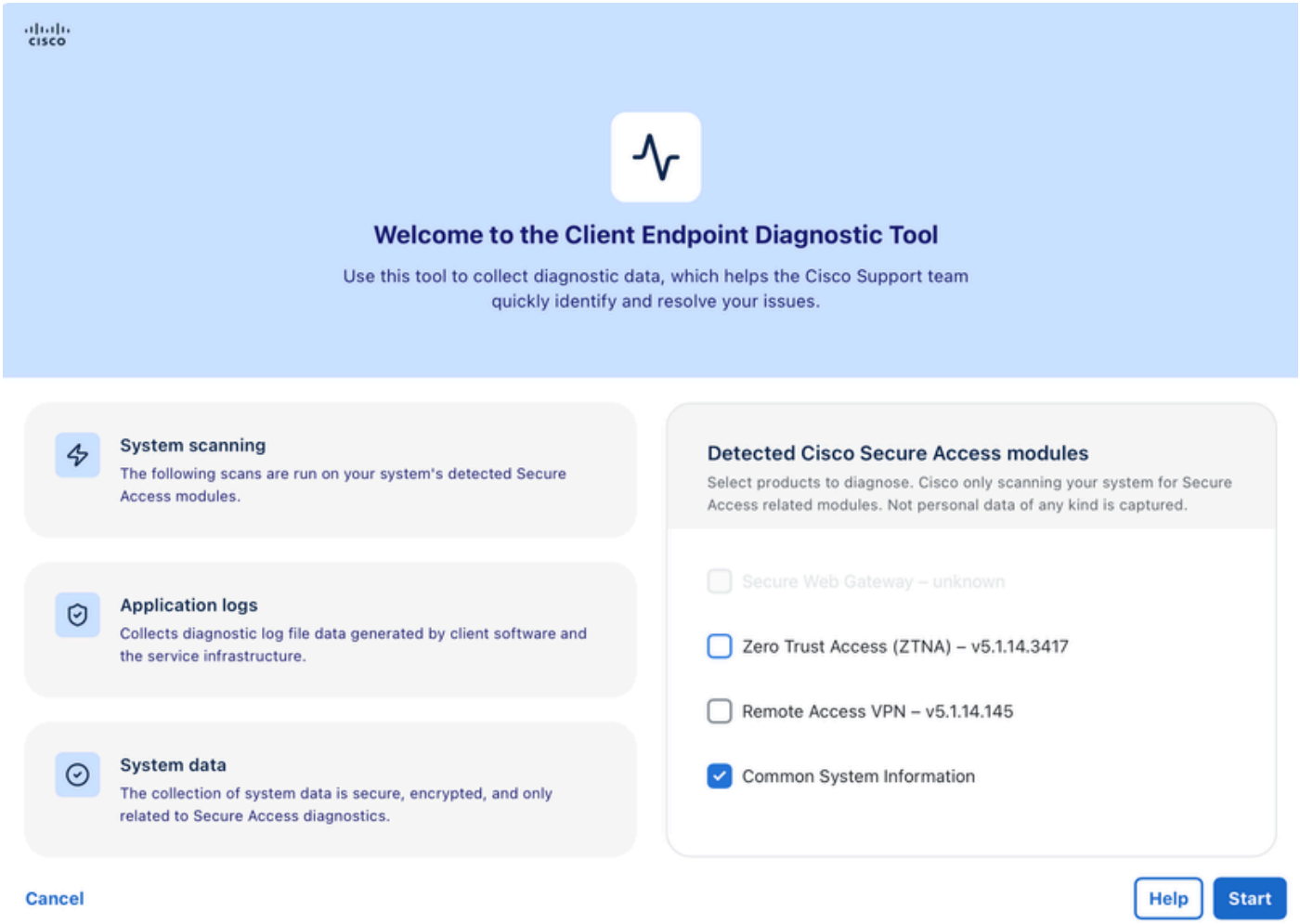
# Stap-voor-stap walkthrough

## Welkomstscherm

Wanneer u CEDT start, wordt het welkomstscherm weergegeven. Het geeft een overzicht van wat de tool doet:

- Systeemscanning — Scant uw systeem op gedetecteerde Cisco Secure Access-modules.
- Toepassingslogboeken — Verzamelt diagnostische logbestandgegevens die worden gegenereerd door clientsoftware en de service-infrastructuur.
- Systeemgegevens — De verzameling van systeemgegevens is beveiligd, gecodeerd en

heeft alleen betrekking op diagnostiek voor beveiligde toegang.




Aan de rechterkant detecteert de tool automatisch alle geïnstalleerde Cisco Secure Access-modules op uw systeem. U ziet selectievakjes voor elke gedetecteerde module, samen met het versienummer:

- Zero Trust Access (ZTNA)
- Secure Web Gateway (SWG)
- Remote Access VPN (RAVPN)
- Gemeenschappelijke systeeminformatie (altijd beschikbaar)

Acties

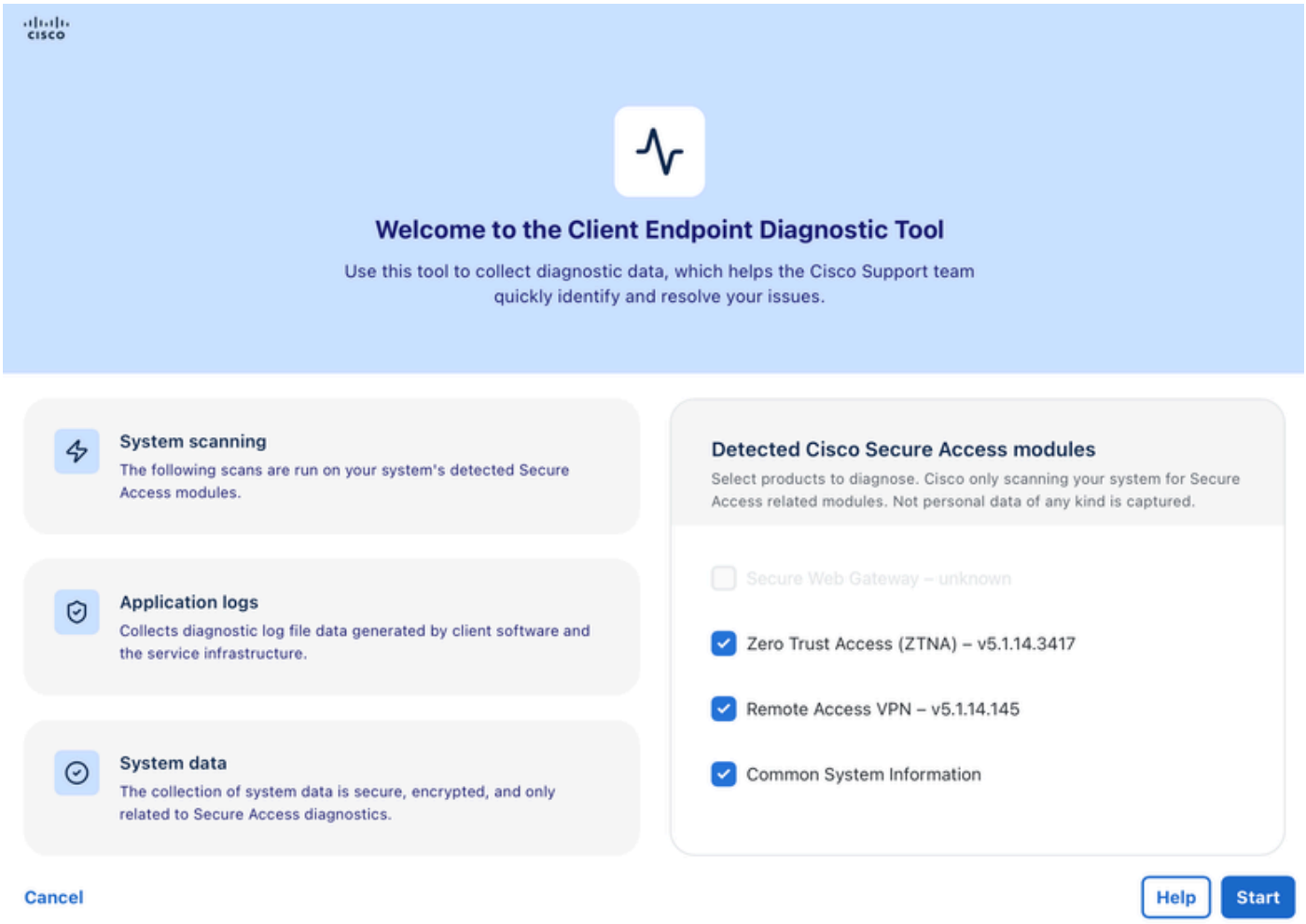
1. Selecteer of deselecteer de producten die u wilt diagnosticeren.

2. Klik op Laten we beginnen om verder te gaan of klik op Help voor meer informatie.

---

Opmerking: Deze tool verzamelt alleen gegevens voor modules met betrekking tot beveiligde toegang. Er worden geen persoonlijke gegevens van welke aard dan ook verzameld.

---




## Stap 1: Diagnostische gegevensverzameling

In dit scherm kunt u kiezen welke diagnostische tests en gegevensverzamelingsmodules u wilt opnemen.

netwerkdiagnose

Selecteer welke connectiviteitstests moeten worden uitgevoerd:

- DNS Lookup — Voert DNS-resolutietests uit tegen specifieke hosts. Ondersteunt aangepaste IP-resolvers voor gerichte opzoekingen. Alle resultaten worden geconsolideerd in één uitvoerbestand (dns/dns_lookups.txt) met gestructureerde sectiebegrenzers.
- Packet Capture — legt netwerkpakketten vast voor een bepaalde duur (vereist beheerdersbevoegdheden). Zie Details pakketopname.
- Ping-hosts — Pings-gespecificeerde hosts om de connectiviteit te controleren.
- Output van beleidstest — Test de handhaving van beleid aan de hand van opgegeven URL's met behulp van het eindpunt voor beleidstest van Cisco (policy.test.sse.cisco.com). Ondersteunt meerdere door komma gescheiden hosts (maximaal 10). De resultaten omvatten HAR-gegevens die automatisch worden vastgelegd tijdens de navigatie van de beleidstest.
- Netwerksnelheidstest — meet de upload-/downloadsnelheid en latentie ten opzichte van het Cisco-eindpunt voor de snelheidstest (speed.test.sse.cisco.com). Verzamelt downloadsnelheid (6 parallelle streams), uploadsnelheid (3 parallelle streams) en ping-latentie/jitter (10 ICMP-samples). De resultaten worden opgeslagen in zowel JSON- als tekstoverzichtsindelingen.
- URL Bereikbaarheid — Controleert of opgegeven URL's bereikbaar zijn met HTTP GET-verzoeken. Ondersteunt standaard zowel HTTP (poort 80) als HTTPS (poort 443). Niet-standaard poorten kunnen worden opgegeven in de URL (zoals https://example.com:8443). Maximaal 20 URL's per controle met een time-out van 30 seconden per URL. De verzamelde gegevens per URL omvatten: URL, bereikbaarheidsstatus, HTTP-statuscode, responstijd (ms), lengte van de inhoud, opgelost IP-adres, TLS-versie en tijdstempel. De resultaten worden opgeslagen op reachability/reachability_results.json en reachability/reachability_summary.txt.

gegevensverzameling

Selecteer modules om prestatie- en connectiviteitsgegevens te verzamelen:

- HAR Capture: registreert HTTP Archive (HAR)-gegevens van een browsersessie. Momenteel ondersteunt Google Chrome alleen (gebruikt het Chrome DevTools-protocol via browserautomatisering zonder kop). De tool detecteert automatisch de Chrome-installatie op uw systeem. Firefox en Safari worden momenteel niet ondersteund. HAR-uitvoer volgt de HAR 1.2-specificatie en bevat volledige netwerksporen (inclusief door JS getriggerde XHR / fetch-oproepen).

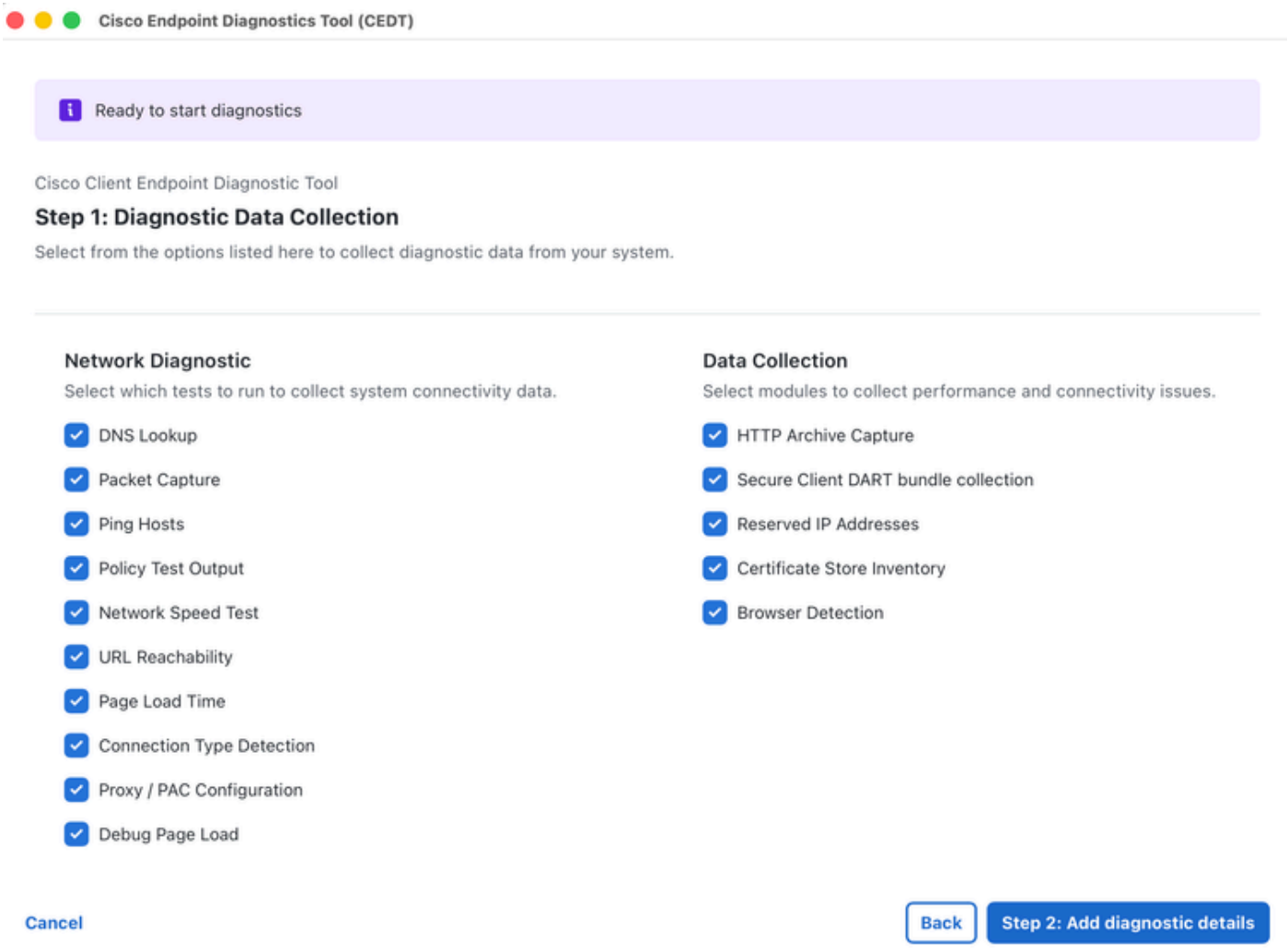
- DART Bundle Collection — Verzamelt een diagnostische DART-bundel van de Cisco Secure Client. Dit omvat alle modulelogs, inclusief Zero Trust Access (ZTA)-logs (zoals flowlog.db op Windows op C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\).
- Gereserveerd IP — voert gereserveerde IP-diagnostische controles uit. Zie de volgende sectie voor de volledige lijst met verzamelde diagnoses.

debuggen

- Foutopsporingsvlaggen inschakelen — Verzamel gedetailleerde logboeken van eindpuntactiviteiten om eindpuntproblemen te diagnosticeren. Deze optie is alleen beschikbaar als ten minste één Cisco Secure Access-product is gedetecteerd en geselecteerd.

Platformspecifiek

- DebugView Capture (Windows) — hiermee kunt u zich aanmelden voor fouten in de Windows Secure Endpoint Connector. Deze optie is alleen beschikbaar op Windows-systemen.




Acties

1. Schakel de gewenste diagnostische opties in of uit.
2. Klik op Stap 2: Voeg diagnostische gegevens toe om verder te gaan.
3. Klik op Terug om terug te keren naar het welkomstscherm of op Annuleren om af te sluiten.

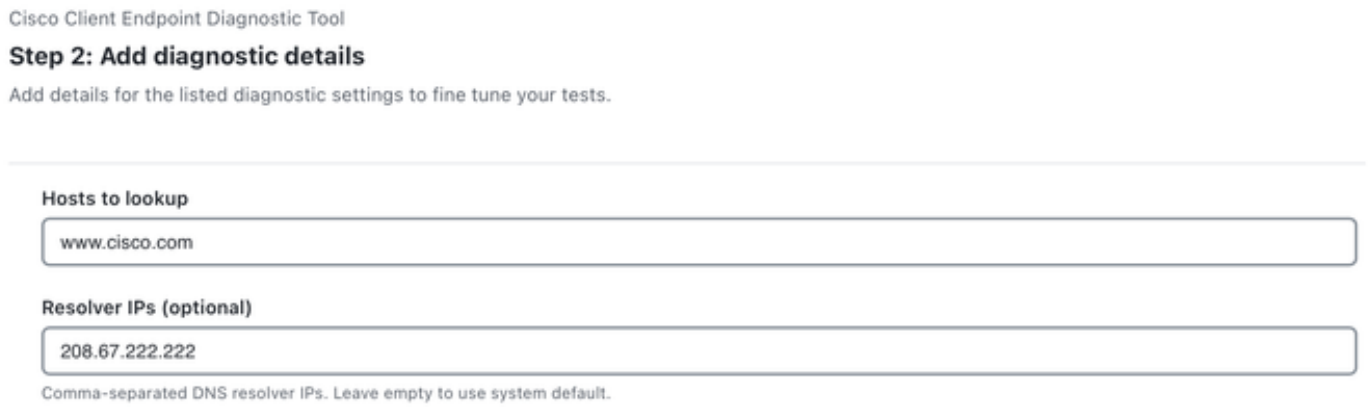
## Stap 2: diagnostische details toevoegen

In dit scherm kunt u de specifieke parameters configureren voor elke diagnostische test die is ingeschakeld. Alleen instellingen voor tests die u in stap 1 hebt ingeschakeld, worden weergegeven.

DNS-opzoekinstellingen

- Hosts om op te zoeken — Voer een of meer hostnamen in (komma-gescheiden). Voorbeeld: cisco.com
- IP's oplossen (optioneel) — Voer aangepaste IP's in voor DNS-resolver (door komma's gescheiden). Voorbeeld: 208 67 222 222, 208 67 220 220. Laat leeg om de standaard DNS-resolver van het systeem te gebruiken. Wanneer opgegeven, wordt elke host vergeleken met elke resolver, wat vergelijkbare DNS-resolutieresultaten oplevert voor verschillende DNS-servers.

Alle DNS-opzoekresultaten worden geconsolideerd in één uitvoerbestand: dns/dns_lookups.txt, met gestructureerde TextFSM-sectiebegrenzers voor elke combinatie van host en resolver.




Instellingen voor pakketopname

- Interfaces — Selecteer de netwerkinterface waarop u wilt vastleggen (of laat deze als Alle).
  - Wanneer ingesteld op All (automatische modus):
    - macOS/Linux: De tool voert tcpdump -D uit om alle beschikbare interfaces op te sommen, en vervolgens filters voor interfaces die Up and Running zijn (met

uitzondering van niet-verbonden interfaces). Als er geen actieve interfaces worden gevonden, valt deze terug naar de speciale interface. Opnamen worden parallel uitgevoerd op alle overeenkomende interfaces.

- Windows: legt op alle NIC's vast met behulp van de geselecteerde back-end voor vastleggen (zie hulpmiddelen in de volgende sectie). Bij gebruik van dumpcap zonder geselecteerde interface worden maximaal de eerste 3 gedetecteerde interfaces tegelijkertijd vastgelegd.

- Pakkettelling — aantal pakketten dat per interface moet worden vastgelegd. Standaard: 100. Maximaal: 10.000.
- Duur (sec) — Maximale opnameduur in seconden. Standaard: 20 seconden op macOS/Linux, 5 seconden op Windows. Maximaal: 300 seconden. De opname stopt wanneer het aantal pakketten of de tijdslimiet is bereikt, afhankelijk van wat het eerst komt.

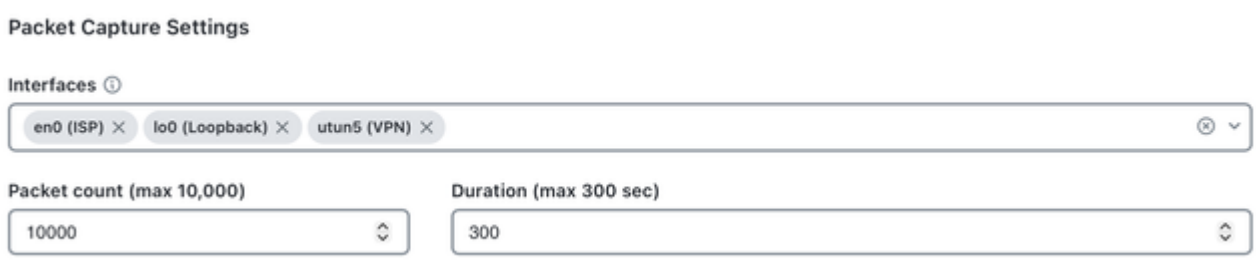
Packet Capture Tools per platform

---

Opmerking: (Windows): De tool selecteert automatisch de best beschikbare back-end voor het vastleggen. ptmon heeft de voorkeur (ingebouwd in Windows 10 v2004+), valt terug naar dumpcap (als Wireshark is geïnstalleerd), dan netsh trace als laatste redmiddel.

---

| 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 |



Uitvoerbestanden pakketopname

De opname van elke interface wordt opgeslagen als een apart bestand met behulp van de naamgevingsconventie: tcpdump/{interface_name}_capture.pcap (zoals en0_capture.pcap, eth0_capture.pcap). Er wordt ook een manifest-bestand met metagegevens (tcpdump/packet_capture_manifest.txt) gegenereerd, waarin het platform, het aantal pakketten, de duur, de vastgelegde interfaces en de gebruikte back-end worden vastgelegd.

Ping-instellingen

- Host/s naar ping — Voer hosts naar ping in (kommagescheiden). Voorbeeld:www.cisco.com


Instellingen voor URL-bereikbaarheid

- Te controleren URL's — Voer URL's in om te testen (kommagescheiden). Voorbeeld: `https://github.com`
    - Maakt gebruik van HTTP GET-verzoeken om de bereikbaarheid te testen.
    - Standaardpoorten: 80 (HTTP) / 443 (HTTPS). Neem de poort op in de URL voor niet-standaard poorten (zoals `ashttps://example.com:8443`).
    - Maximaal 20 URL's per controle.
    - Time-out: 30 seconden per URL.
    - Gegevens verzameld per URL: URL, bereikbaarheidsstatus, HTTP-statuscode, responstijd (ms), lengte van de inhoud, opgelost IP-adres, TLS-versie en tijdstempel.
    - De resultaten worden opgeslagen op reachability/reachability_results.json en reachability/reachability_summary.txt.


Instellingen voor beleidstest

- Host-URL's — Voer hosts in voor beleidstests (door komma's gescheiden, maximaal 10). Voorbeeld: www.cisco.com
- Beleidstests worden uitgevoerd op basis van het eindpunt van de Cisco-beleidstest: policy.test.sse.cisco.com
- De resultaten omvatten zowel de output van de gestructureerde beleidstest als de HAR-gegevens die automatisch tijdens de testnavigatie worden vastgelegd.


Instellingen voor HAR-vastlegging

- Doel-URL's — Voer URL's in voor HAR-vastlegging (kommagescheiden). Voorbeeld: https://www.cisco.com/

---

Tip: HAR capture ondersteunt momenteel alleen Google Chrome. De tool maakt gebruik van het Chrome DevTools Protocol (via chromedo) om een hoofdloze Chrome-sessie te automatiseren en netwerkverkeer vast te leggen. Zorg ervoor dat Google Chrome op uw systeem is geïnstalleerd. Firefox en Safari worden momenteel niet ondersteund.

---

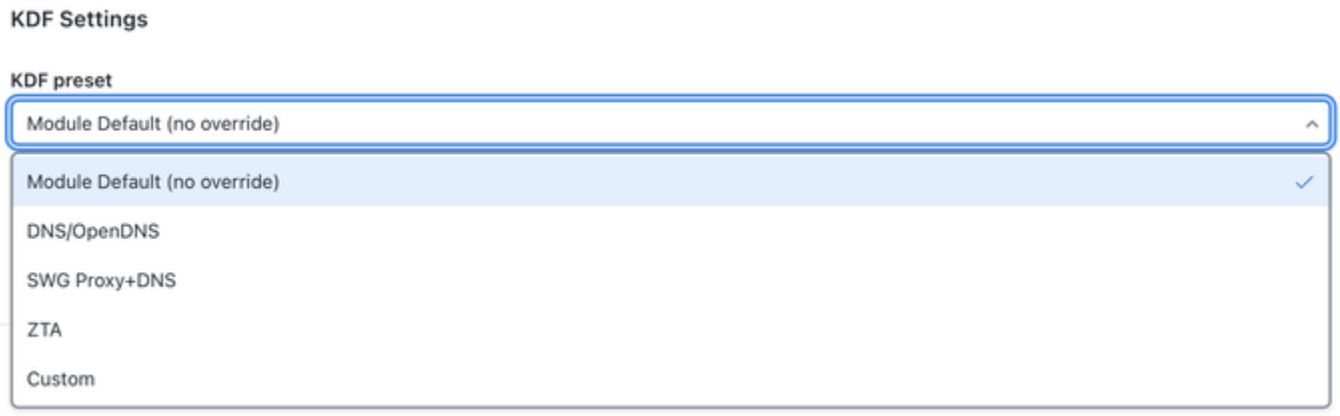

KDF-instellingen

Configureer de vlaggen voor de functie voor sleutelafleiding die worden gebruikt tijdens de diagnostische verzameling. KDF-vlaggen bepalen welke foutopsporingscategorieën zijn ingeschakeld in de Cisco Secure Client:

- KDF-preset — Selecteer een preset voor een sleutelafleidingsfunctie.
- KDF HEX — De hex-waarde wordt automatisch ingevuld op basis van de geselecteerde preset. Wanneer "Aangepast" is geselecteerd, voert u uw eigen hexadecimale waarde in.

| 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. |


Gereserveerde IP-instellingen

- NSLookup-URL's — Optionele aangepaste nslookup-hosts (kommagescheiden). Maximaal 10 URL's. Elke aangepaste host wordt gevraagd aan de hand van alle geconfigureerde

resolvers.

- Trace-URL's — Optionele aangepaste traceroute-/tracerethosts (gescheiden door komma's). Maximaal 10 URL's. De tool maakt automatisch gebruik van traceroute op macOS / Linux en tracert op Windows.
- IP's oplossen — Optionele aangepaste IP's voor nslookup-query's (kommagescheiden, zoals 208.67.222).
- 222, 208.67.220.220). Maximaal 5 IPs. Indien opgegeven, worden aangepaste resolvers gebruikt naast de drie ingebouwde resolvers (systeemstandaard DNS, 127.0.0.1, 208.67.222.222).


Gereserveerde IP-gegevens

De gereserveerde IP-diagnostiek verzamelt deze gegevens standaard:

Standaard Traceroute/Tracert-doelen (automatisch tegen al deze doelen):

| doel | Doel |
|---|---|
| 208.67.222.222 | Route naar OpenDNS primaire nameserver |
| 208.67.220.220 | Route naar OpenDNS secundaire nameserver |

| | |
|---|---|
| 146.112.255.50 | Route naar Cisco SWG Infrastructure IP |
| swg-url-proxy-https-sse.sigproxy.qq.opendns.com | Route naar SWG proxy hostnaam |

- macOS/Linux: gebruikt traceroute-opdracht
- Windows: gebruikt opdracht tracert

Standaard NSLookup-query's (worden automatisch uitgevoerd tegen al deze query's):

Elk nslookup-doel wordt getoetst aan elke resolver in de lijst met resolvers. Standaard bevat de lijst met resolvers drie ingebouwde resolvers:

| 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 |

Als aangepaste IP's zijn geconfigureerd (zoals 208.67.222.222), worden deze toegevoegd aan de lijst met resolvers en wordt elk doel voor het zoeken naar nslookup ook tegen hen opgevraagd.

NSLookup-doelen:

| 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 |

Met de standaard 3 resolvers levert dit bijvoorbeeld 6 nslookup-query's op (2 doelen x 3 resolvers). Als u één aangepaste IP-resolver toevoegt, wordt dit verhoogd tot 8 query's (2 doelen x 4 resolvers).

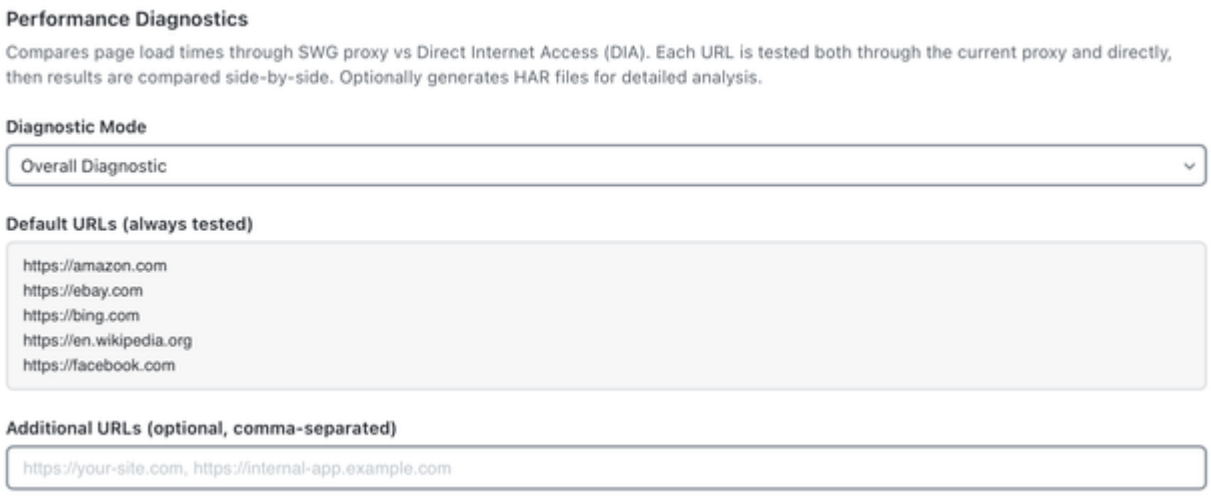
Aangepaste door de gebruiker geleverde NSLookup-URL's worden elk gevraagd aan de hand van dezelfde volledige lijst met resolvers (ingebouwd + aangepaste resolvers).

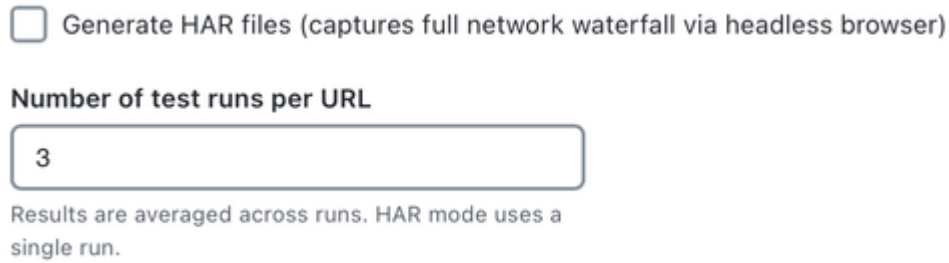
Alle resultaten worden geconsolideerd in één bestand: reserved_ip/reserved_ip_diagnostics.txt, gegroepeerd per sectie (traceroute, nslookup) met door mensen leesbare koppen die het doel en de resolver voor elk item aangeven.

prestatiediagnose

Vergelijkt laadtijden van pagina's via SWG-proxy versus Direct Internet Access (DIA). Het heeft twee modi:

1 Algemene diagnostische modus: elke URL wordt getest, zowel via de huidige proxy als rechtstreeks, waarna de resultaten naast elkaar worden vergeleken. Optioneel genereert HAR-bestanden voor gedetailleerde analyse.





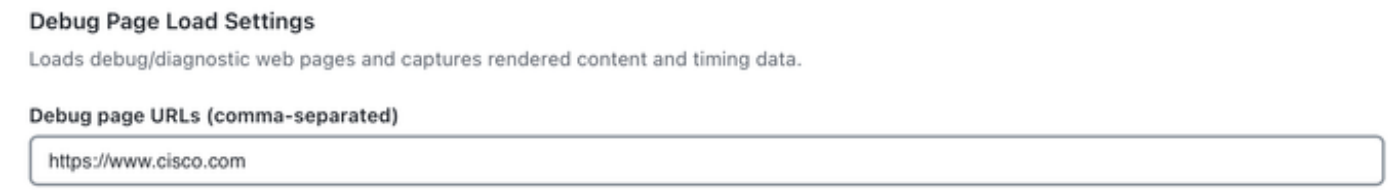

2 Diagnostische modus voor URL's: we kunnen specifieke URL invoeren die via zowel de huidige proxy als rechtstreeks moet worden getest, waarna de resultaten naast elkaar worden vergeleken. Optioneel genereert HAR-bestanden voor gedetailleerde analyse.


Instellingen voor certificaatvoorraad

- Numereert certificaten uit geconfigureerde certificaatstores:
  - systeem
  - Inloggen
  - wortel
  - En meer
- Identificeert snel ontbrekende, verlopen of niet-vertrouwde certificaten

Instellingen voor laden van foutopsporingspagina:

- Hiermee worden configureerbare debug-URL's geladen.
- Opnamen:
  - Reactiekoppen
  - Responsorgaan
  - Timing-informatie
  - SSL-metagegevens




Acties

1. Vul de instellingen in of pas deze aan voor elke diagnostische functie die is ingeschakeld.
2. Klik op Diagnostiek starten om de diagnostische procedure te starten.
3. Klik op Terug om terug te keren naar stap 1 of op Annuleren om af te sluiten

---

Opmerking: velden met validatiefouten worden gemarkeerd. Je moet ze corrigeren voordat de diagnose kan beginnen.

---

## Pauzeer en ga verder

Wanneer u een diagnostische verzameling uitvoert die geavanceerde probleemoplossing bevat (bijvoorbeeld ZTNA of SWG-tracering), kan de Cisco Endpoint Diagnostic Tool halverwege de uitvoering pauzeren en u vragen het probleem te reproduceren voordat het wordt voortgezet.

Dit geeft u de tijd om het probleem te activeren terwijl gedetailleerde logboekregistratie is ingeschakeld, zodat het ondersteuningsteam nuttigere diagnostische gegevens ontvangt.

- Wanneer het venster Diagnostics Paused (Diagnostiek onderbroken) wordt weergegeven,

leest u het bericht. Dit bericht vertelt u welke functies voor logboekregistratie nu actief zijn.

- Reproduceer het probleem dat u probeert op te lossen. Voorbeeld:
    - Opnieuw verbinding maken met VPN
    - Open de interne toepassing die faalt
    - Herhaal de stappen die de fout veroorzaken
- Wanneer u klaar bent met het reproduceren van het probleem, klikt u op Doorgaan

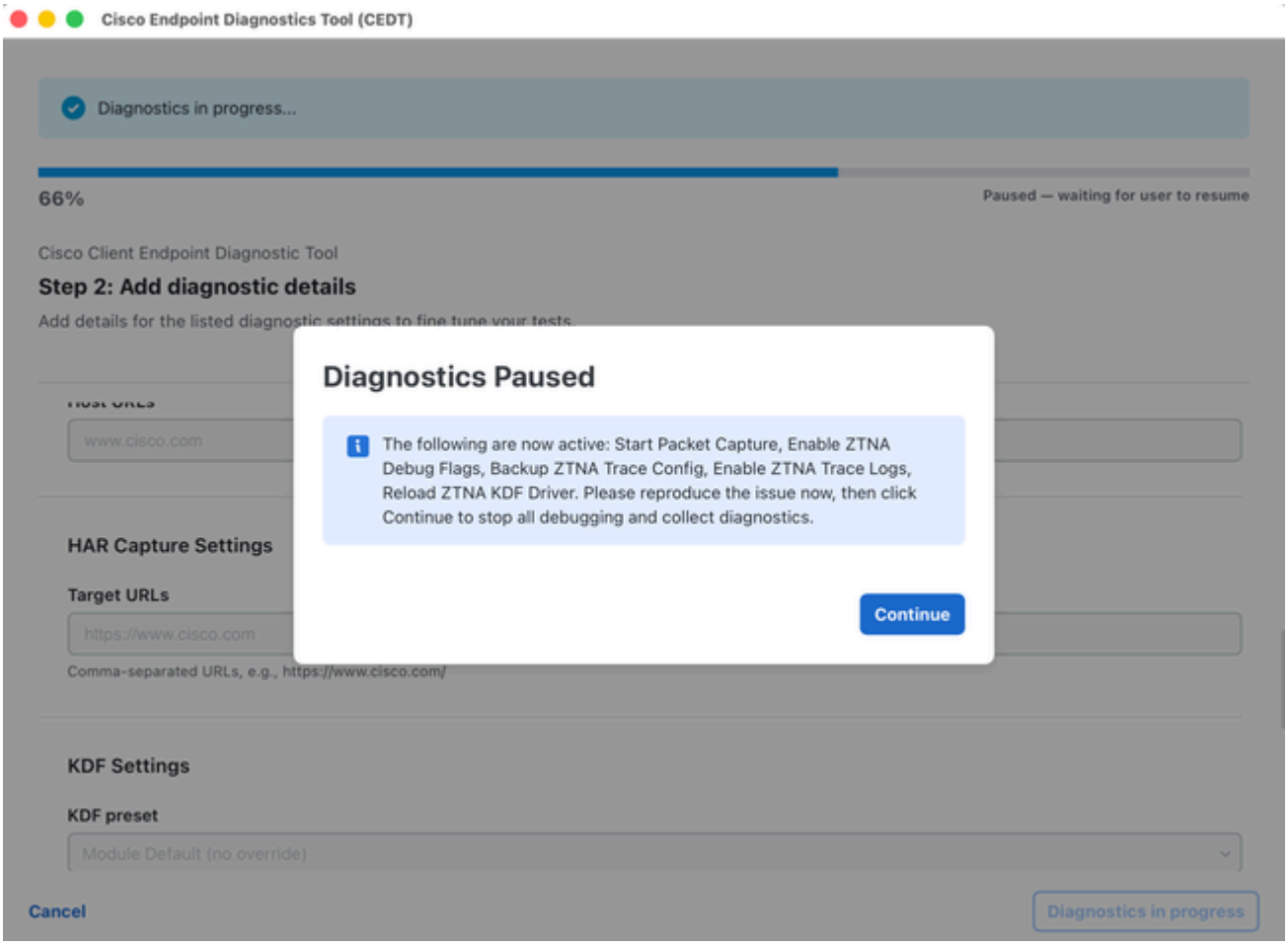
Laat de run eindigen. De tool verzamelt bestanden, herstelt uw normale instellingen en maakt het diagnostische archief.

OPMERKING: Sluit de toepassing niet tijdens het pauzeren. Logboekregistratie blijft actief totdat u op Doorgaan klikt en de uitvoering is voltooid.

(Opdrachtregel)

Als u het gereedschap vanaf een terminal uitvoert, ziet u een pauzebericht in het venster in plaats van een dialoogvenster.

1. Lees het pauzebericht in de terminal.
2. Het probleem reproduceren.
3. Ga terug naar de terminal en druk op Enter om door te gaan.
4. Wacht tot de run is afgelopen.

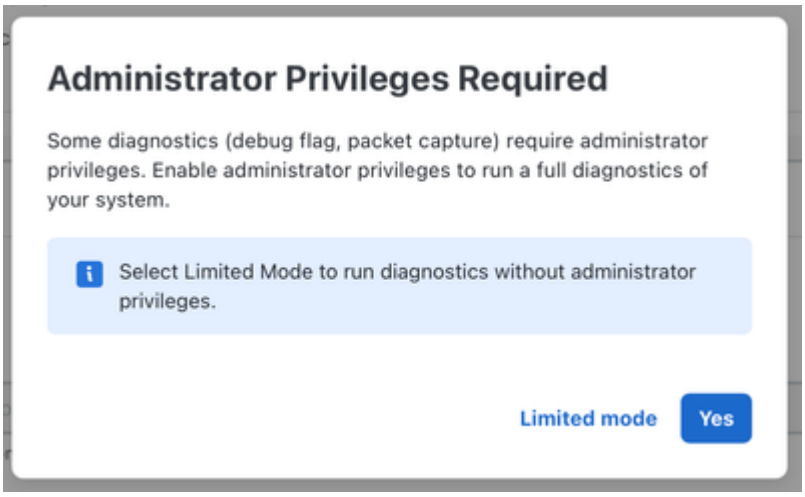


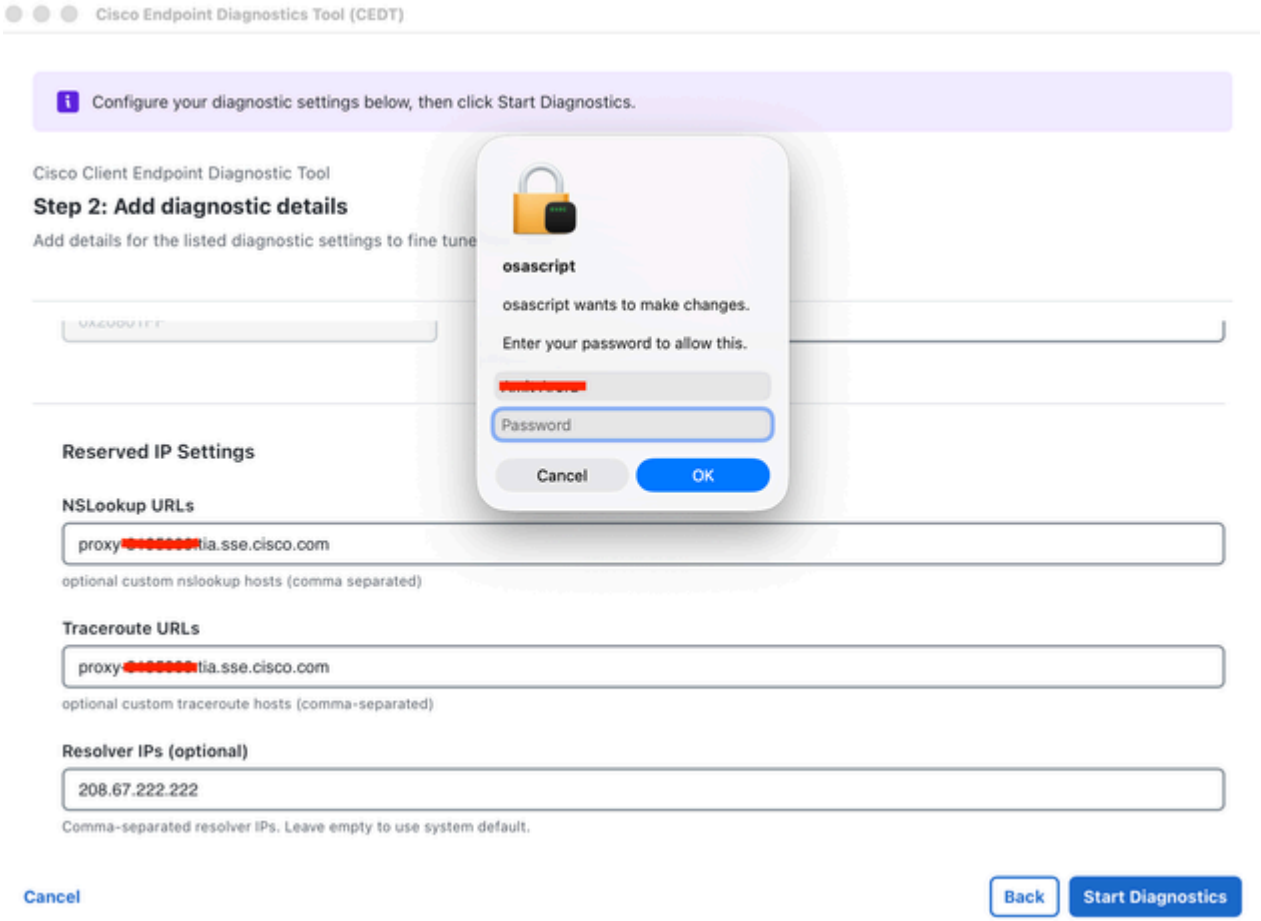

## Vragen over beheerdersrechten

Nadat u op Diagnostiek starten hebt geklikt, kunt u in het hulpprogramma vragen om beheerdersbevoegdheden als u functies hebt ingeschakeld waarvoor een hogere toegang vereist is (zoals Pakketvastlegging of foutopsporingsvlaggen).

Er wordt een dialoogvenster weergegeven met de titel Beheerdersrechten vereist:

- Klik op Ja om beheerdersrechten toe te kennen. Dit activeert de native macOS/Windows-aanmeldingsprompt.
- Klik op Beperkte modus om verder te gaan zonder verhoging. Privileged taken (pakketopname, foutopsporingsvlaggen) worden overgeslagen.
- macOS: U kunt het standaard macOS-wachtwoord dialoogvenster van osascript zien. Voer uw systeemwachtwoord in en klik op OK.
- Windows: Er verschijnt een standaard UAC-elevatieprompt. Klik op Ja om toe te staan.



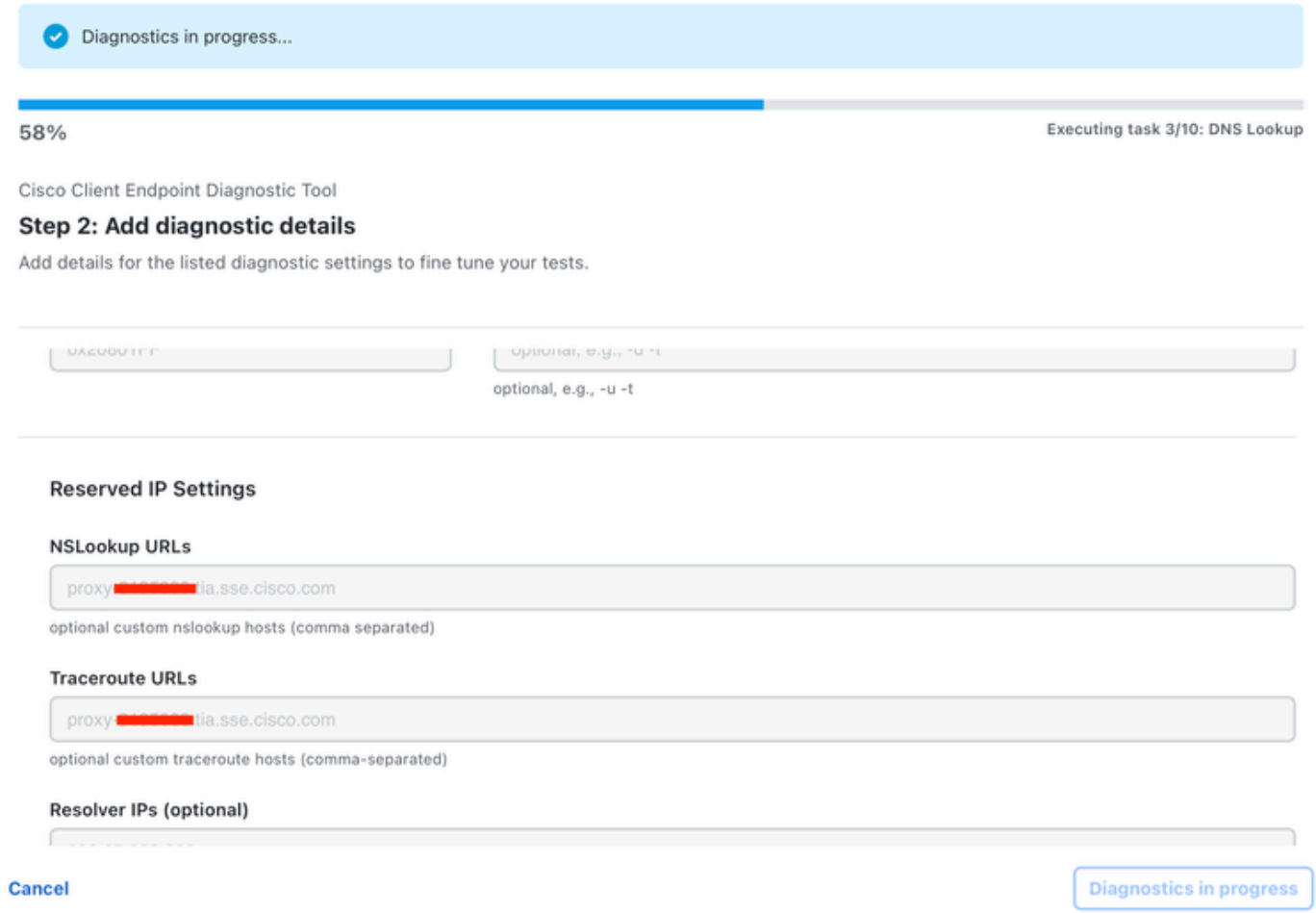

## Diagnostiek in uitvoering

Eenmaal gestart, voert het hulpprogramma alle geselecteerde diagnostische taken uit:

- Een voortgangsbalk toont de algehele voltooiing (zoals 59% — Uitvoerende taak 3/9: DNS Lookup).

- De banner Diagnostics in progress... wordt bovenaan weergegeven.
- Alle instellingenvelden zijn uitgeschakeld/grijs weergegeven tijdens het uitvoeren.
- In de voettekst ziet u een knop Diagnostics in progress (Onderzoeken aan de gang) (uitgeschakeld) om aan te geven dat het gereedschap bezig is.

Wacht terwijl de diagnostiek is voltooid. Sluit de toepassing niet.




1.

## Diagnose voltooid — Uploaden naar TAC

Wanneer alle diagnoses zijn voltooid, wordt een dialoogvenster Voltooiing weergegeven:

Diagnose voltooid. Bestand uploaden naar een TAC-zaak.

Het dialoogvenster wordt weergegeven:

- Archief — De bestandsnaam van het gegenereerde diagnostische archief (zoals cisco_diagnostics.tar.gz).
- Bestandsgrootte — De grootte van het archief (zoals 7,72 MB).
- SHA256 — De controlesom van het archiefbestand voor integriteitsverificatie.

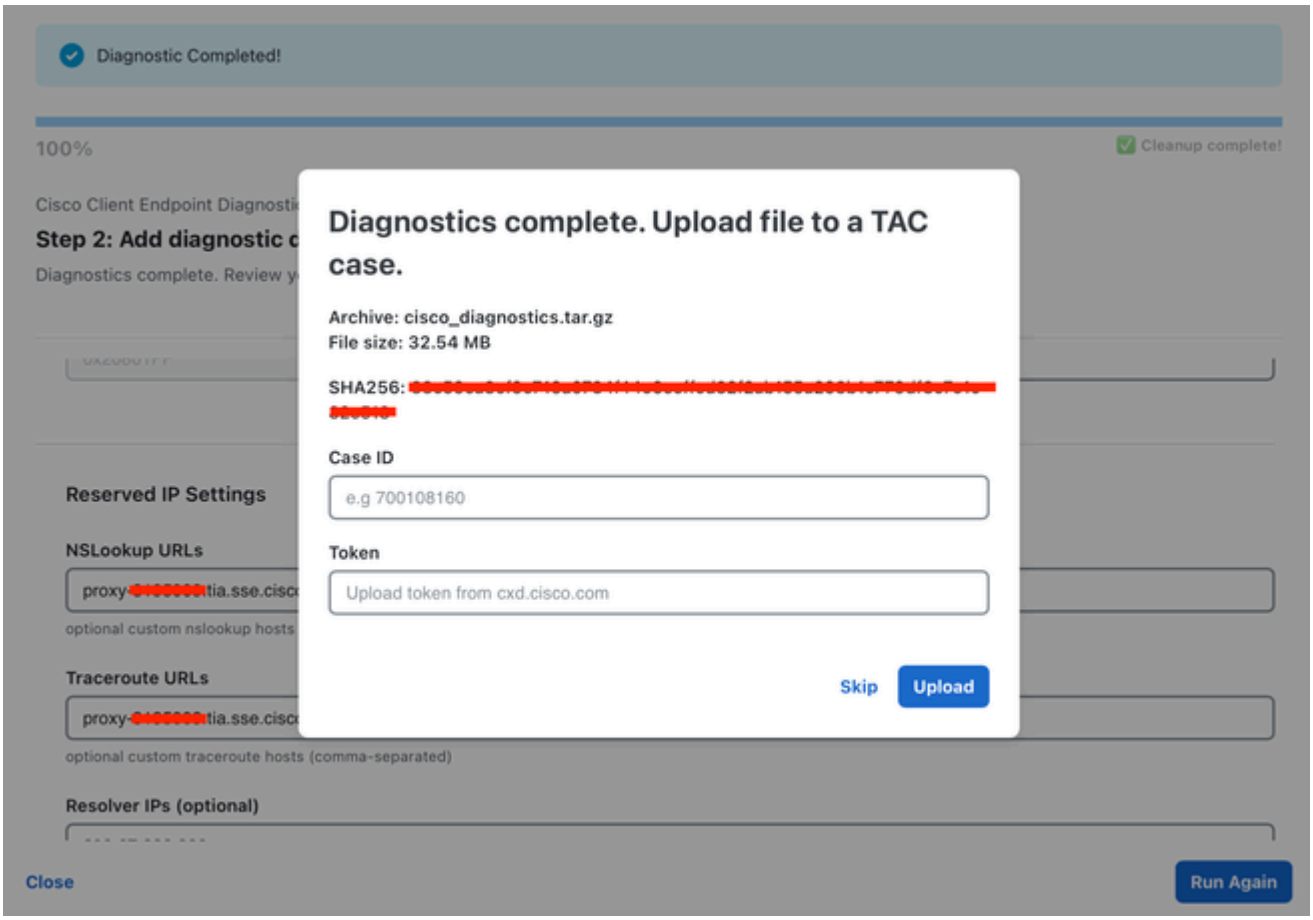
Uploaden naar een TAC-geval:

1. Voer uw case-ID in (bijvoorbeeld 698746730).
2. Voer uw token in (geleverd door Cisco-ondersteuning).
3. Klik op TAC-kwestie openen om het uploaden te starten.

Een voortgangsbalk toont de uploadstatus (zoals Uploaden... 85,0% (6,56 MB / 7,72 MB)).

De upload overslaan:

- Klik op Overslaan om het dialoogvenster te sluiten zonder te uploaden. Het archiefbestand wordt nog steeds lokaal opgeslagen.




Scherm Uploaden voltooid/definitief

Na een succesvolle upload wordt de voltooiingsbanner bijgewerkt naar:

Diagnostisch archief geüpload naar kwestie [Case ID]

De voortgangsbalk toont 100% met een volledige status voor Opruimen.

Acties

- Klik op Opnieuw uitvoeren om een nieuwe diagnostische run te starten.
- Klik op Sluiten om de toepassing af te sluiten.

## uitvoerlocatie

De diagnostische uitvoer wordt opgeslagen in:

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

Het uitvoerarchiefbestand (cisco_diagnostics.tar.gz) bevat alle verzamelde diagnostische gegevens in een gestructureerd formaat.

## Probleemoplossing

| 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

V: Welke gegevens verzamelt deze tool?
A: De tool verzamelt systeeminformatie (besturingssysteem, hardware, netwerkconfiguratie), toepassingslogboeken, Cisco-productconfiguratie en geïnstalleerde modulegegevens en diagnostische netwerkgegevens die alleen betrekking hebben op Cisco Secure Access-modules. Zie het gedeelte Welke systeemgegevens worden verzameld in het vorige gedeelte voor een

gedetailleerde uitsplitsing. Er worden geen persoonlijke gegevens verzameld.

V: Heb ik beheerderstoegang/roottoegang nodig?
A: Toegang voor beheerders is optioneel, maar wordt aanbevolen. Zonder dit worden sommige diagnostiek (pakketregistratie, foutopsporingsvlaggen) overgeslagen. De tool vraagt u en laat u kiezen.

V: Kan ik de tool meerdere keren gebruiken?
A: Ja. Nadat elke uitvoering is voltooid, kunt u op "Opnieuw uitvoeren" klikken om een nieuwe diagnosesessie te starten.

Q: Waar wordt de output opgeslagen?
A: Het diagnostische archief wordt opgeslagen op uw bureaublad in de map cisco_diagnostics.

Q: Wat als ik geen TAC Case ID heb?
A: U kunt op "Overslaan" klikken in het uploaddialoogvenster. Het archiefbestand wordt nog steeds lokaal opgeslagen. U kunt het later handmatig uploaden naar een TAC-geval of delen met uw ondersteuningsingenieur.

V: Zijn de gegevens versleuteld?
A: Het diagnostische archief wordt gecomprimeerd (tar.gz) en gevoelige gegevens worden automatisch geredigeerd voordat ze worden verpakt.

V: Welke browsers vangt HAR ondersteuning op?
A: HAR capture ondersteunt momenteel alleen Google Chrome. De tool maakt gebruik van het Chrome DevTools-protocol voor browserautomatisering zonder kop. Zorg ervoor dat Chrome is geïnstalleerd voordat u HAR capture uitvoert.

Q Het pauzescherm is nooit verschenen. Is er iets mis?

A: Niet noodzakelijk. De pauzestap wordt alleen weergegeven wanneer gedetailleerde logboekregistratie is ingeschakeld voor uw scenario. Controleer de aanmeldingsgegevens voor uitvoeren in de app — als stappen voor inschakelen zijn overgeslagen, gaat de tool door zonder te pauzeren.

Q: De run lijkt vast te zitten. Wat moet ik doen?

A: Zoek naar het venster Diagnostics Paused (Diagnostiek gepauzeerd) — dit kan zich achter andere vensters bevinden. De uitvoering gaat pas verder als u op Doorgaan klikt (of op Enter in de opdrachtregel drukt).

Q De berichtenlijst bevat functies die ik niet had verwacht. Is dat normaal?

A: Ja. Het bericht toont de logboekfuncties die zijn ingeschakeld voor uw platform en de diagnostische opties die u hebt geselecteerd.

Q Ik heb de app gesloten tijdens de pauze. Wat nu?

A: Voer de diagnostische verzameling opnieuw uit en laat deze afwerken. Als u niet zeker weet of de logboekregistratie is ingeschakeld, neemt u contact op met uw supporttechnicus voor advies.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.