CEDT(Endpoint Diagnostics Tool) 이해

목차

소개

이 문서에서는 시스템에서 진단 데이터를 수집하고 이를 Cisco TAC 지원 사례에 업로드하는 CEDT에 대해 설명합니다.

사전 요구 사항

이 도구는 MacOS 및 Windows에서 사용할 수 있습니다. 도구를 다운로드하십시오.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- MacOS: Cisco CEDT(Endpoint Diagnostics Tool).app을 두 번 클릭하여 시작합니다.
- 창: CEDT.exe를 두 번 클릭하여 시작합니다.
- 활성 인터넷 연결.
- Cisco TAC 케이스 ID 및 토큰(결과를 직접 업로드하려는 경우에만 필요함)

시스템 데이터 수집됨

이 도구는 범주별로 구성된 이 시스템 데이터를 수집합니다. 어떤 종류의 개인 데이터도 캡처되지 않습니다.

일반 시스템 정보

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

네트워크 설정

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 제품 정보

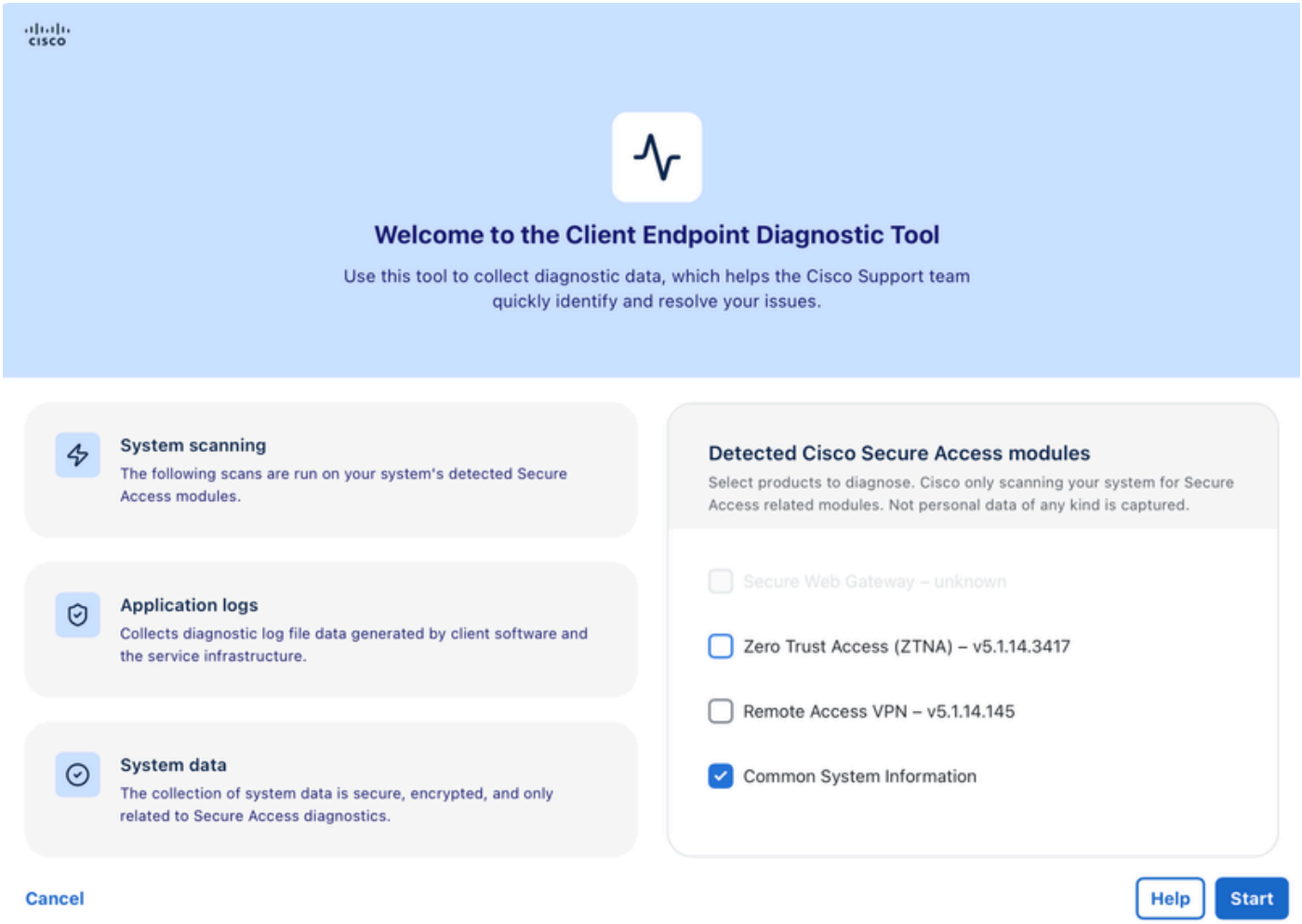
Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco.*`	Registry exports (`HKLM\SOFTWARE\Cisco`, `HKCU\SOFTWARE\Cisco`, `acsock` service)
Installation directories	`ls -laR /opt/cisco`	`%ProgramFiles%\Cisco`, `%ProgramFiles(x86)%\Cisco`, `%ProgramData%\Cisco`
Running Cisco 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

단계별 연습

시작 화면

CEDT를 실행하면 Welcome 화면이 표시됩니다. 툴의 기능에 대한 개요를 제공합니다.

- 시스템 검사 — 시스템에서 탐지된 Cisco Secure Access 모듈을 검사합니다.
- 애플리케이션 로그 — 클라이언트 소프트웨어 및 서비스 인프라에서 생성된 진단 로그 파일 데이터를 수집합니다.
- 시스템 데이터 — 시스템 데이터의 수집은 안전하고 암호화되며 Secure Access 진단에만 관련됩니다.



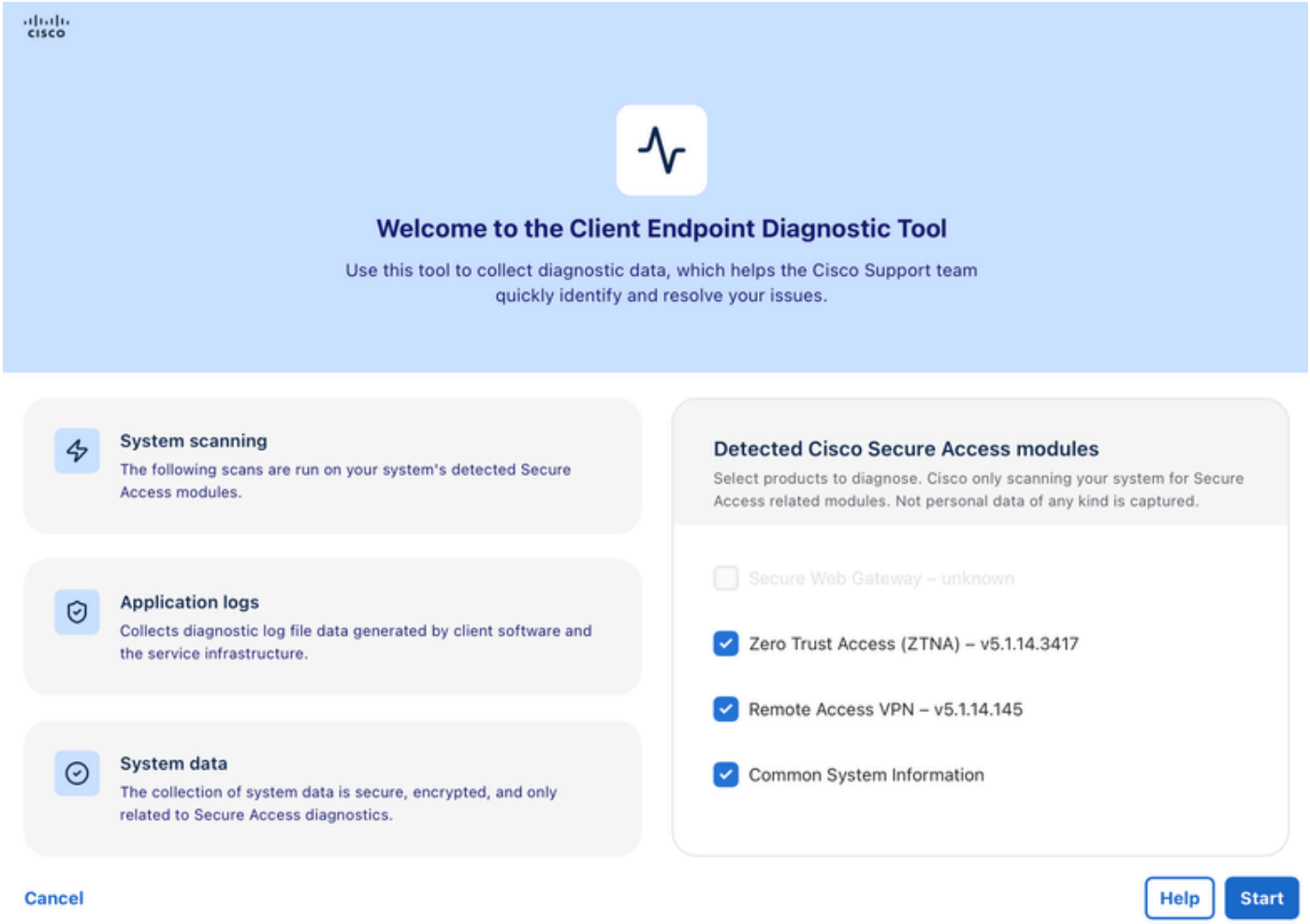
오른쪽에서 이 도구는 시스템에 설치된 모든 Cisco Secure Access 모듈을 자동으로 검색합니다. 탐지된 각 모듈에 대한 확인란과 해당 버전 번호를 확인할 수 있습니다.

- 제로 트러스트 액세스(ZTNA)
- SWG(Secure Web Gateway)
- 원격 액세스 VPN(RAVPN)
- 공통 시스템 정보(항상 사용 가능)

작업

1. 진단할 제품을 선택하거나 선택 취소합니다.
2. 계속하려면 시작을 클릭하고, 자세한 내용을 보려면 도움말을 클릭하십시오.

참고: 이 도구는 Secure Access 관련 모듈에 대한 데이터만 수집합니다. 어떤 종류의 개인 데이터도 캡처되지 않습니다.



1단계: 진단 데이터 수집

이 화면에서는 포함할 진단 테스트 및 데이터 수집 모듈을 선택할 수 있습니다.

네트워크 진단

실행할 연결 테스트 선택:

- DNS 조회 — 지정된 호스트에 대해 DNS 확인 테스트를 수행합니다. 대상 조회에 대한 사용자 지정 확인자 IP를 지원합니다. 모든 결과는 구조화된 섹션 구분 기호가 있는 단일 출력 파일(dns/dns_lookups.txt)로 통합됩니다.
- 패킷 캡처 — 지정된 기간 동안 네트워크 패킷을 캡처합니다(관리자 권한 필요). 패킷 캡처 세부 정보를 참조하십시오.
- Ping 호스트 — 연결을 확인하기 위해 지정된 호스트에 대해 ping을 수행합니다.
- 정책 테스트 출력 — Cisco 정책 테스트 엔드포인트(policy.test.sse.cisco.com)를 사용하여 지정된 URL에 대한 정책 시행을 테스트합니다. 쉼표로 구분된 여러 호스트(최대 10개)를 지원합니다. 결과에는 정책 테스트 탐색 중에 자동으로 캡처된 HAR 데이터가 포함됩니다.
- 네트워크 속도 테스트 — Cisco 속도 테스트 엔드포인트(speed.test.sse.cisco.com)에 대한 업로드/다운로드 속도 및 레이턴시를 측정합니다. 다운로드 속도(병렬 스트림 6개), 업로드 속도(병렬 스트림 3개), ping 레이턴시/지터(ICMP 샘플 10개)를 수집합니다. 결과는 JSON 및 텍스트 요약 형식으로 저장됩니다.
- URL Reachability — 지정된 URL이 HTTP GET 요청을 사용하여 연결할 수 있는지 여부를 확인합니다. 기본적으로 HTTP(포트 80) 및 HTTPS(포트 443)를 모두 지원합니다. 비표준 포트는 URL(예: https://example.com:8443)에 지정할 수 있습니다. URL당 30초 시간 초과로 검사당 최대 20개의 URL입니다. URL당 수집되는 데이터에는 다음이 포함됩니다. URL, 연결 상태, HTTP 상태 코드, 응답 시간(ms), 콘텐츠 길이, 확인된 IP 주소, TLS 버전, 타임스탬프. 결과는 reachability/reachability_results.json 및 reachability/reachability_summary.txt에 저장됩니다.

데이터 수집

성능 및 연결 데이터를 수집할 모듈 선택:

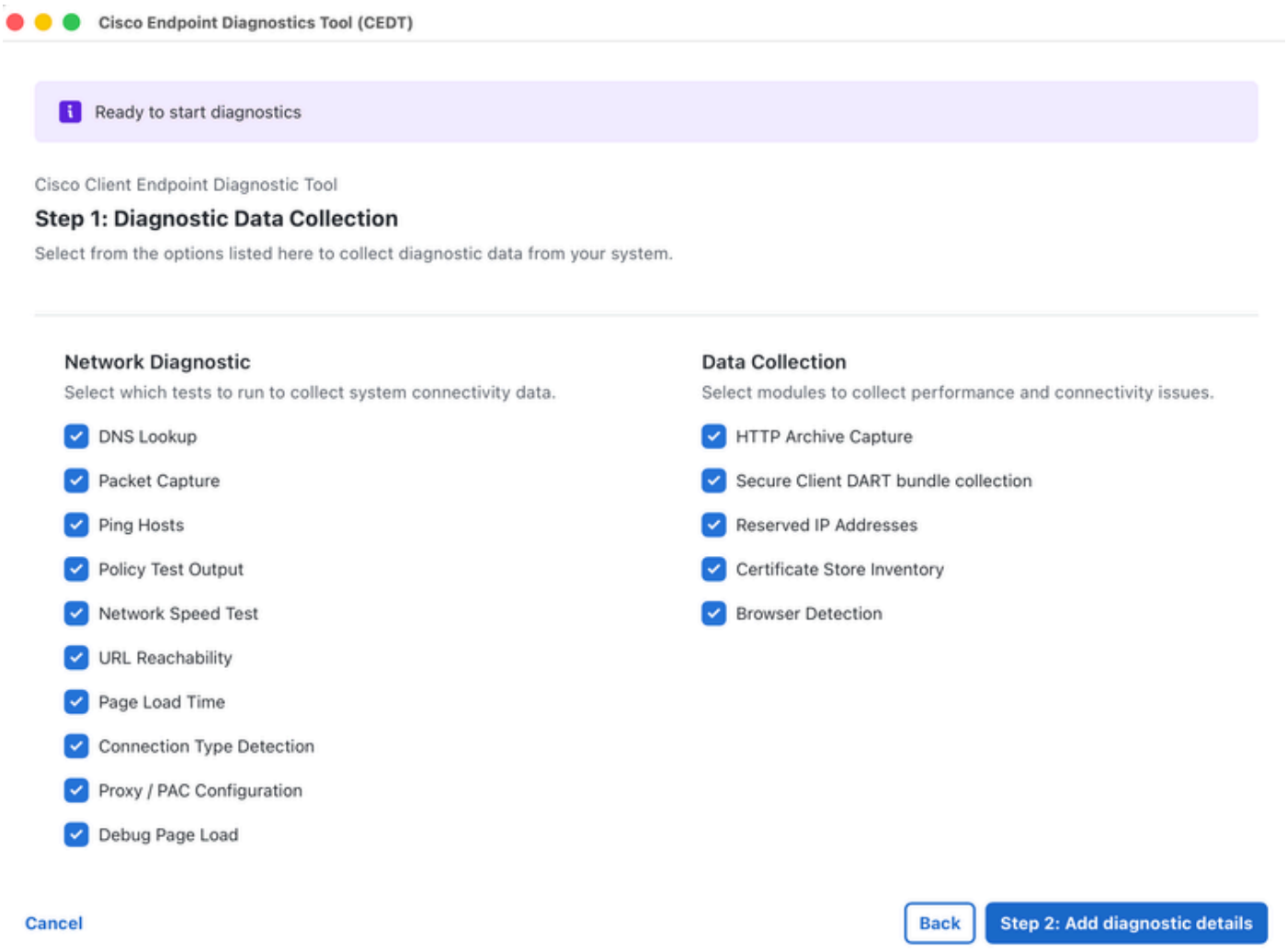
- HAR 캡처 — 브라우저 세션에서 HAR(HTTP 아카이브) 데이터를 기록합니다. 현재 Google Chrome만 지원합니다(헤드리스 브라우저 자동화를 통해 Chrome DevTools 프로토콜 사용). 이 도구는 시스템에서 Chrome 설치를 자동으로 감지합니다. Firefox 및 Safari는 현재 지원되지 않습니다. HAR 출력은 HAR 1.2 사양을 따르며 전체 네트워크 추적(JS-triggered XHR/fetch 호출 포함)을 포함합니다.
- DART Bundle Collection — Cisco Secure Client에서 DART 진단 번들을 수집합니다. 여기에는 ZTA(Zero Trust Access) 로그를 비롯한 모든 모듈 로그가 포함됩니다(예: C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\의 Windows에서 flowlog.db).
- Reserved IP — 예약된 IP 진단 검사를 실행합니다. 수집된 전체 진단 목록을 보려면 다음 섹션을 참조하십시오.

디버그

- Enable Debug Flags(디버그 플래그 활성화) - 엔드포인트 문제를 진단하기 위해 엔드포인트 활동에 대한 자세한 로그를 수집합니다. 이 옵션은 하나 이상의 Cisco Secure Access 제품이 탐지되어 선택된 경우에만 사용할 수 있습니다.

플랫폼별

- DebugView 캡처(Windows) — Windows 보안 엔드포인트 커넥터에서 디버그 로깅을 활성화합니다. 이 옵션은 Windows 시스템에서만 사용할 수 있습니다.



작업

1. 원하는 진단 옵션을 선택하거나 선택 취소합니다.
2. 2단계를 클릭합니다. 계속하려면 진단 세부 정보를 추가합니다.
3. Back(뒤로)을 클릭하여 Welcome(시작) 화면으로 돌아가거나 Cancel(취소)을 클릭하여 종료합니다.

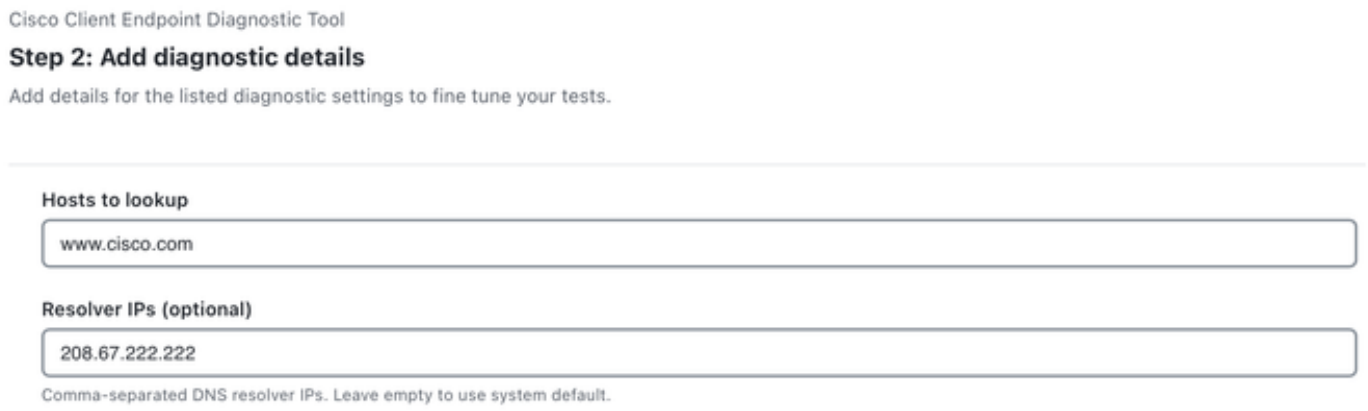
2단계: 진단 세부 정보 추가

이 화면에서는 활성화된 각 진단 테스트에 대한 특정 매개변수를 구성할 수 있습니다. 1단계에서 활성화한 테스트에 대한 설정만 표시됩니다.

DNS 조회 설정

- 조회할 호스트 — 하나 이상의 호스트 이름(쉼표로 구분)을 입력합니다. 예: cisco.com
- Resolver IPs (optional)(확인자 IP(선택 사항)) — 사용자 지정 DNS 확인자 IP(쉼표로 구분)를 입력합니다. 예: 208.67.222.222, 208.67.220.220. 시스템 기본 DNS 확인자를 사용하려면 비워 두십시오. 지정하면 각 호스트가 각 확인자에 대해 쿼리되어 서로 다른 DNS 서버 간에 비교 DNS 확인 결과를 제공합니다.

모든 DNS 조회 결과는 단일 출력 파일로 통합됩니다. 각 호스트/확인자 조합에 대해 구조화된 TextFSM 섹션 구분 기호가 있는 dns/dns_lookups.txt입니다.



패킷 캡처 설정

- Interfaces — 캡처할 네트워크 인터페이스를 선택합니다(또는 All로 유지).
    - 모두(자동 모드)로 설정된 경우:
        - macOS/Linux: 이 도구는 tcpdump -D를 실행하여 사용 가능한 모든 인터페이스를 열거한 다음 작동 및 실행 중인 인터페이스에 대해 필터링합니다(연결이 끊어진 인터페이스 제외). 활성 인터페이스를 찾을 수 없는 경우 특수 any 인터페이스로 돌아갑니다. 캡처는 모든 일치 인터페이스에서 병렬로 실행됩니다.
        - 창: 선택한 캡처 백엔드를 사용하여 모든 NIC에서 캡처합니다(다음 섹션의 툴 참조). 인터페이스를 선택하지 않은 채 dumpcap을 사용할 경우 처음 3개까지 탐지된 인터페이스가 동시에 캡처됩니다.
- Packet count — 인터페이스당 캡처할 패킷 수입니다. 기본값: 100. 최대: 10,000 .
- Duration (sec)(기간(초)) - 최대 캡처 기간(초) 기본값: macOS/Linux에서는 20초, Windows에서는 5초. 최대: 300초 패킷 수 또는 기간 제한 중 먼저 오는 것에 도달하면 캡처가 중지됩니다 .

플랫폼별 패킷 캡처 툴

참고: (Windows): 이 툴은 자동으로 사용 가능한 최상의 캡처 백엔드를 선택합니다. pktmon이 기본 설정(Windows 10 v2004+에 내장)되어 dumpcap으로 돌아간 다음 (Wireshark가 설치된 경우) netsh 추적을 마지막 수단으로 사용합니다.

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

패킷 캡처 출력 파일

각 인터페이스의 캡처는 명명 규칙을 사용하여 별도의 파일로 저장됩니다. tcpdump/{interface_name}_capture.pcap(예: en0_capture.pcap, eth0_capture.pcap) 또한 사용된 플랫폼, 패킷 수, 기간, 인터페이스 캡처 및 캡처 백 엔드를 기록하는 메타데이터 매니페스트 파일(tcpdump/packet_capture_manifest.txt)이 생성됩니다.

Ping 설정

- Host/s to ping — ping할 호스트(쉼표로 구분)를 입력합니다. 예:www.cisco.com

URL 연결 설정

- 확인할 URL — 테스트할 URL을 입력합니다(쉼표로 구분). 예: https://github.com
  - HTTP GET 요청을 사용하여 연결 가능성을 테스트합니다.
  - 기본 포트: 80(HTTP)/443(HTTPS) 비표준 포트의 URL에 포트를 포함합니다(예: ashttps://example.com:8443).
  - 체크당 최대 20개의 URL.

- 시간 초과: URL당 30초
- URL당 수집된 데이터: URL, 연결 상태, HTTP 상태 코드, 응답 시간(ms), 콘텐츠 길이, 확인된 IP 주소, TLS 버전, 타임스탬프.
- 결과는 reachability/reachability_results.json 및 reachability/reachability_summary.txt에 저장됩니다.

정책 테스트 설정

- Host URLs — 정책 테스트용 호스트(쉼표로 구분, 최대 10개)를 입력합니다. 예: www.cisco.com
- 정책 테스트는 Cisco 정책 테스트 엔드포인트에 대해 실행됩니다. policy.test.sse.cisco.com
- 결과에는 테스트 탐색 동안 자동으로 캡처되는 구조화된 정책 테스트 출력 및 HAR 데이터가 모두 포함됩니다.

HAR 캡처 설정

- 대상 URL — HAR 캡처(쉼표로 구분)를 위한 URL을 입력합니다. 예: https://www.cisco.com/

팁: HAR 캡처는 현재 Google Chrome만 지원합니다. 이 툴에서는 Chromedp를 통해 Chrome DevTools Protocol을 사용하여 헤드리스 Chrome 세션을 자동화하고 네트워크 트래픽을 캡처합니다. 시스템에 Google Chrome이 설치되어 있는지 확인합니다. Firefox 및 Safari는 현재 지원되지 않습니다.

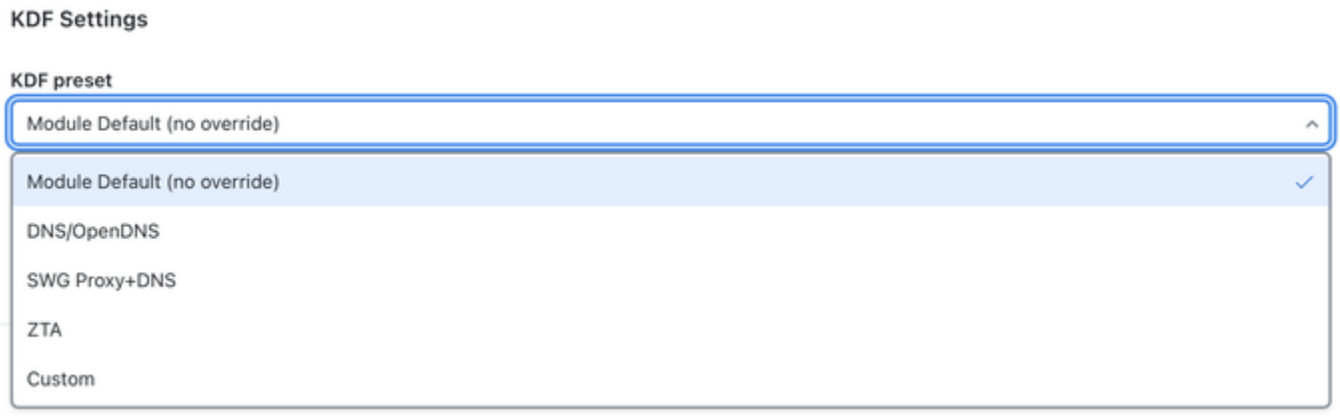
KDF 설정

진단 컬렉션 중에 사용되는 키 파생 함수 플래그를 구성합니다. KDF 플래그는 Cisco Secure Client에서 활성화되는 디버그 범주를 제어합니다.

- KDF 사전 설정 — 키 파생 함수 사전 설정을 선택합니다.
- KDF HEX — 선택한 사전 설정에 따라 16진수 값이 자동으로 채워집니다. "사용자 지정"을 선택한 경우 고유한 16진수 값을 입력합니다.

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.



예약된 IP 설정

- NSLookup URLs — 사용자 지정 nslookup 호스트(쉼표로 구분)(선택 사항) 최대 10개의 URL 구성된 모든 리졸버에 대해 각 맞춤형 호스트가 쿼리됩니다.

- Trace URLs(추적 URL) — 선택적 맞춤형 traceroute/tracert 호스트(쉼표로 구분) 최대 10개의 URL 이 툴에서는 자동으로 macOS/Linux의 traceroute와 Windows의 tracert를 사용합니다.
- Resolver IPs — nslookup 쿼리를 위한 선택적 사용자 지정 확인자 IP(쉼표로 구분, 예: 208.67.222).
- 222, 208.67.220.220). 최대 5개의 IP 지정하면 3개의 내장 리졸버(시스템 기본 DNS, 127.0.0.1, 208.67.222.222)와 함께 사용자 지정 리졸버가 사용됩니다.

예약된 IP 세부 정보

Reserved IP 진단은 기본적으로 이 데이터를 수집합니다.

기본 Traceroute/Tracert 대상(이러한 모든 대상에 대해 자동으로 실행됨):

대상	목적
208.67.222.222	OpenDNS 주 네임서버로 라우팅
208.67.220.220	OpenDNS 보조 네임서버로 라우팅
146.112.255.50	Cisco SWG 인프라 IP로 라우팅

swg-url-proxy-https-sse.sigproxy.qq.opendns.com을 참조하십시오.	SWG 프록시 호스트 이름에 라우팅

- macOS/Linux: traceroute 명령 사용
- 창: tracert 명령 사용

기본 NSLookup 쿼리(이 모든 쿼리에 대해 자동으로 실행됨):

모든 nslookup 대상이 확인자 목록의 각 확인자에 대해 쿼리됩니다. 기본적으로 확인자 목록에는 3개의 기본 제공 확인자가 포함됩니다.

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

사용자 지정 확인자 IP(예: 208.67.222.222)가 구성된 경우 확인자 목록에 추가되고 모든 nslookup 대상이 확인됩니다.

NSLookup 대상:

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

예를 들어, 기본 3개의 확인자를 사용하면 6개의 nslookup 쿼리(2개의 대상 x 3개의 확인자)가 생성됩니다. 사용자 지정 확인자 IP를 하나 추가하면 8개 쿼리(대상 2개 x 대상 4개 확인자)로 늘어납니다.

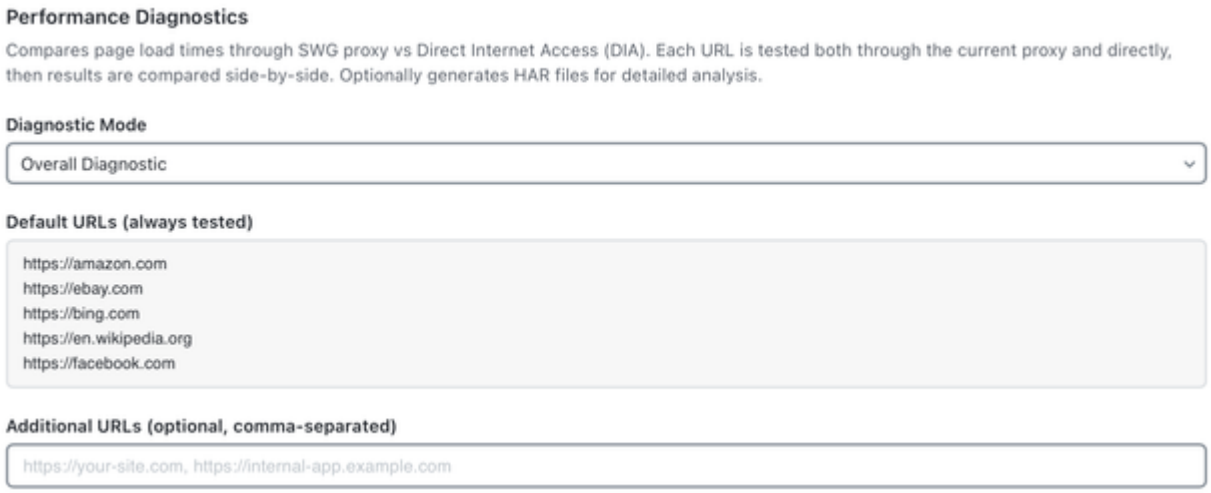
사용자 지정 사용자 제공 NSLookup URL은 동일한 전체 확인자 목록(기본 제공 + 사용자 지정 확인자)에 대해 각각 쿼리됩니다.

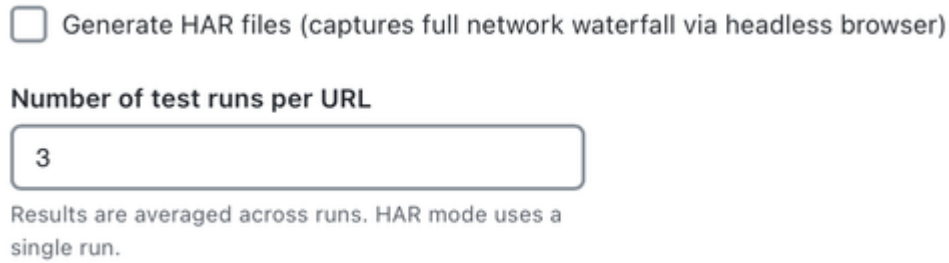
모든 결과가 단일 파일로 통합됩니다. reserved_ip/reserved_ip_diagnostics.txt, 섹션(traceroute, nslookup)별로 그룹화되고 각 항목의 대상 및 확인자를 나타내는 사람이 읽을 수 있는 헤더가 있습니다.

성능 진단

SWG 프록시와 DIA(Direct Internet Access)를 통해 페이지 로드 시간을 비교합니다. 두 가지 모드가 있습니다.

1 전체 진단 모드: 각 URL은 현재 프록시를 통해 직접 테스트한 다음 나란히 결과를 비교합니다. 자세한 분석을 위해 HAR 파일을 생성할 수도 있습니다.

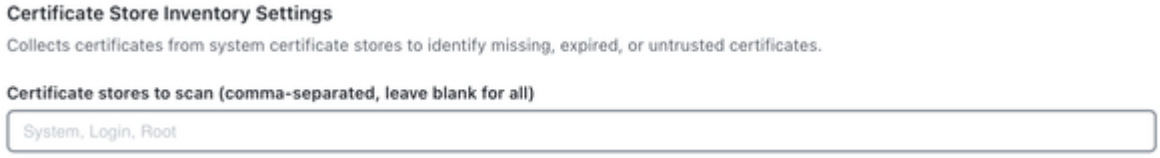




2 URL 진단 모드: 현재 프록시를 통해 그리고 직접 두 URL을 통해 테스트할 특정 URL을 입력한 다음 결과를 나란히 비교합니다. 자세한 분석을 위해 HAR 파일을 생성할 수도 있습니다.

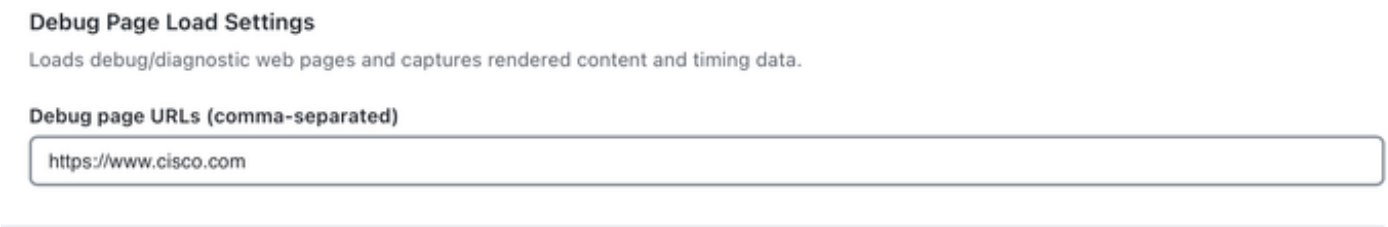
인증서 저장소 인벤토리 설정

- 구성된 인증서 저장소에서 인증서를 열거합니다.
  - 시스템
  - 로그인
  - 루트
  - 기타
- 누락, 만료 또는 신뢰할 수 없는 인증서를 신속하게 식별



디버그 페이지 로드 설정:

- 구성 가능한 디버그 URL을 로드합니다.
- 캡처:
    - 응답 헤더
    - 응답 본문
    - 타이밍 정보
    - SSL 메타데이터



작업

1. 활성화된 각 진단에 대한 설정을 채우거나 조정합니다.
2. 진단 시작을 클릭하여 진단 실행을 시작합니다.
3. Back(뒤로)을 클릭하여 1단계로 돌아가거나 Cancel(취소)을 클릭하여 종료합니다

참고: 검증 오류가 있는 필드는 강조 표시됩니다. 진단을 시작하려면 먼저 이를 수정해야 합니다.

일시 중지 후 계속

고급 문제 해결(예: ZTNA 또는 SWG 추적)이 포함된 진단 수집을 실행하면 Cisco 엔드포인트 진단 툴이 실행을 잠시 중단하고 계속하기 전에 문제를 재현하도록 요청할 수 있습니다.

그러면 자세한 로깅이 켜져 있는 동안 문제를 트리거할 수 있으므로 지원 팀에서 보다 유용한 진단 데이터를 수신합니다.

- 일시 중지된 진단 창이 나타나면 현재 어떤 로깅 기능이 활성화되어 있는지 알려주는 메시지를 읽습니다.
- 트러블슈팅 중인 문제를 재현합니다. 예를 들면 다음과 같습니다.

    - VPN에 다시 연결
    - 오류가 발생한 내부 응용 프로그램을 엽니다.
    - 오류를 발생시키는 단계를 반복합니다
- 문제 재현이 완료되면 Continue(계속)를 클릭합니다.

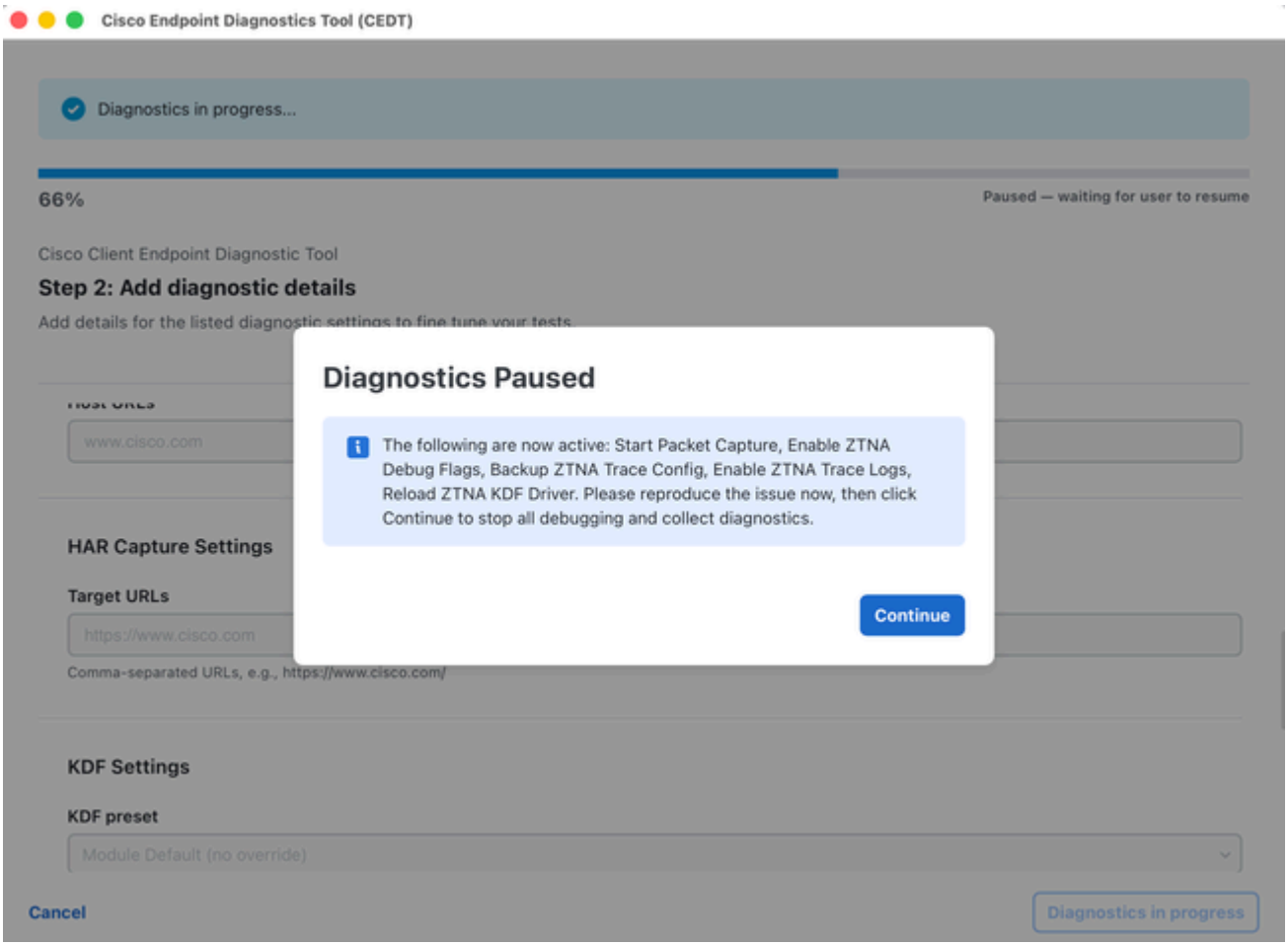
실행이 끝나도록 놔두세요. 이 도구는 파일을 수집하고, 일반 설정을 복원하고, 진단 아카이브를 만듭니다.

참고: 일시 중지된 동안에는 응용 프로그램을 닫지 마십시오. 로그는 Continue(계속)를 클릭하고 실행이 완료될 때까지 활성 상태로 유지됩니다.

(명령줄)

터미널에서 도구를 실행 중인 경우 창에 대화 상자 대신 일시 중지 메시지가 표시됩니다.

1. 터미널에 표시된 일시 중지 메시지를 읽습니다.
2. 문제를 재현합니다.
3. 터미널로 돌아가 Enter 키를 눌러 계속합니다.
4. 실행이 완료될 때까지 기다립니다.

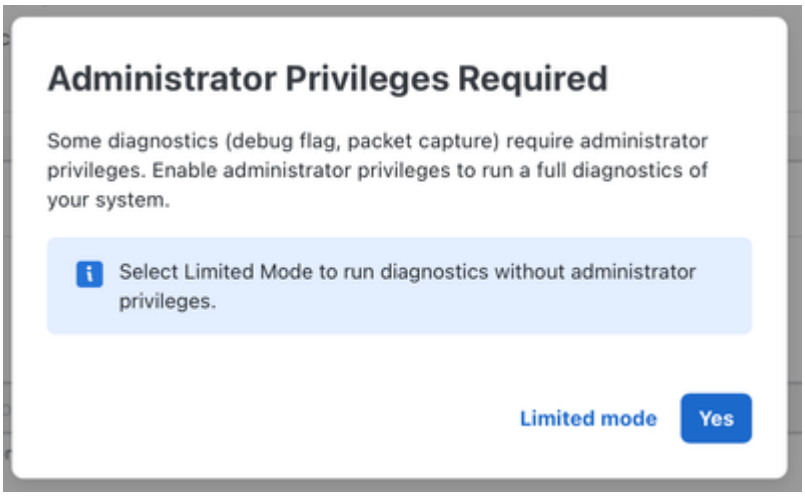


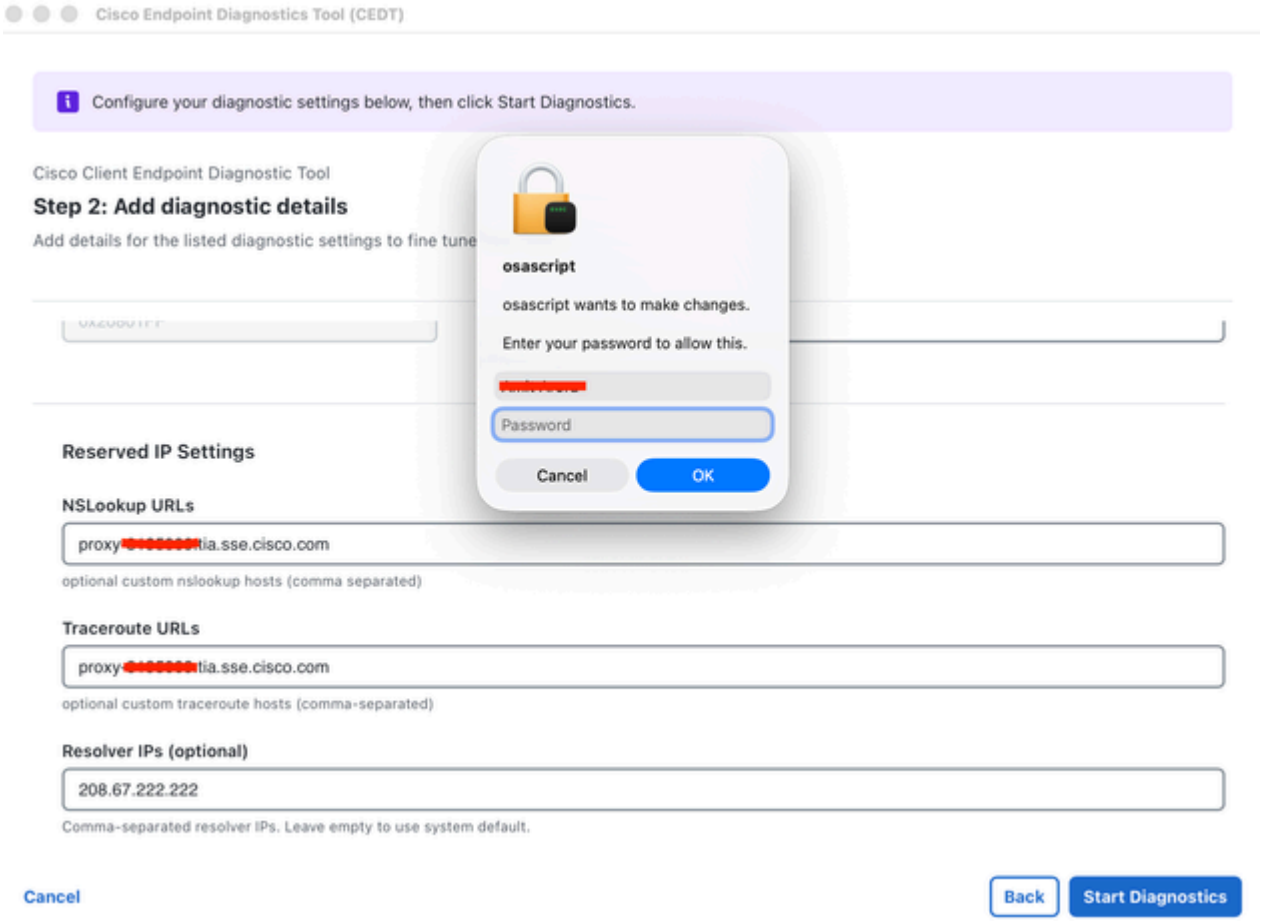
관리자 권한 프롬프트

Start Diagnostics(진단 시작)를 클릭한 후, 고급 액세스 권한이 필요한 기능(예: Packet Capture(패킷 캡처) 또는 Debug Flags(디버그 플래그))을 활성화한 경우, 툴에서 관리자 권한을 묻는 메시지를 표시할 수 있습니다.

필요한 관리자 권한이라는 제목의 대화상자가 나타납니다.

- 관리자 권한을 부여하려면 예를 누릅니다. 이렇게 하면 기본 macOS/Windows 자격 증명 프롬프트가 트리거됩니다.
- 상승 없이 진행하려면 제한 모드를 클릭합니다. 권한이 부여된 작업(패킷 캡처, 디버그 플래그)을 건너뜁니다.
- macOS: osascript에서 표준 macOS 비밀번호 대화 상자를 볼 수 있습니다. 시스템 비밀번호를 입력하고 OK(확인)를 클릭합니다.
- 창: 표준 UAC 상승 프롬프트가 나타납니다. 허용하려면 Yes(예)를 클릭합니다.





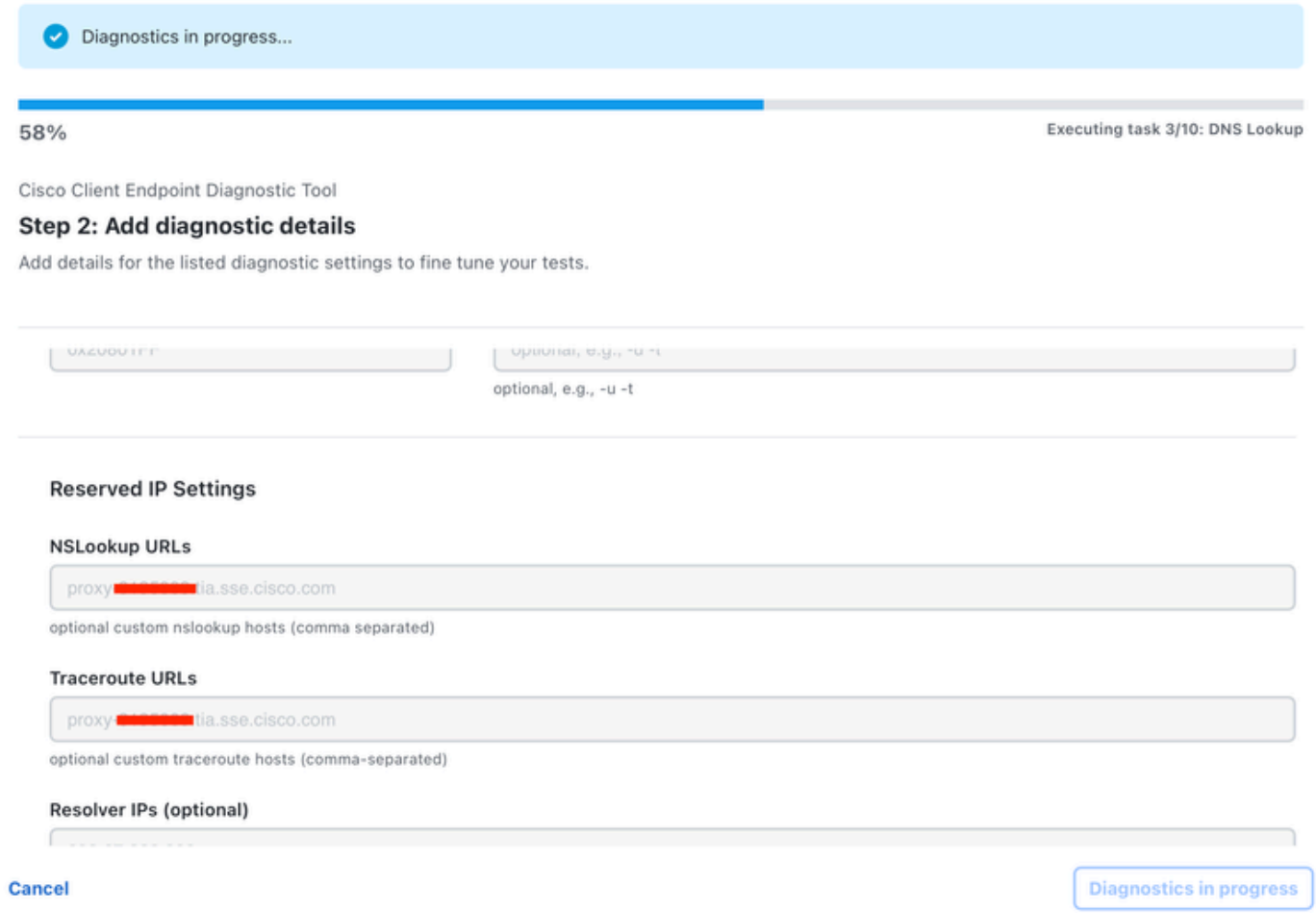
진단 진행 중

일단 시작되면 툴이 선택한 모든 진단 작업을 실행합니다.

- 진행률 표시줄에는 전체 완료(예: 59% - 작업 실행 3/9)가 표시됩니다. DNS 조회).

- 진단 진행 중... 배너는 상단에 표시됩니다.
- 실행 중에 모든 설정 필드가 비활성화되거나 회색으로 비활성화됩니다.
- 바닥글에는 툴이 사용 중임을 나타내는 Diagnostics in progress(진단 진행 중) 버튼(비활성화됨)이 표시됩니다.

진단이 완료되는 동안 잠시 기다려 주십시오. 애플리케이션을 닫지 마십시오.



1.

진단 완료 — TAC에 업로드

모든 진단이 완료되면 완료 대화 상자가 나타납니다.

진단을 완료했습니다. 파일을 TAC 케이스에 업로드합니다.

다음과 같은 대화 상자가 표시됩니다.

- 아카이브 — 생성된 진단 아카이브의 파일 이름(예: cisco_diagnostics.tar.gz).
- 파일 크기 — 아카이브의 크기(예: 7.72MB).
- SHA256 — 무결성 확인을 위한 아카이브 파일의 체크섬입니다.

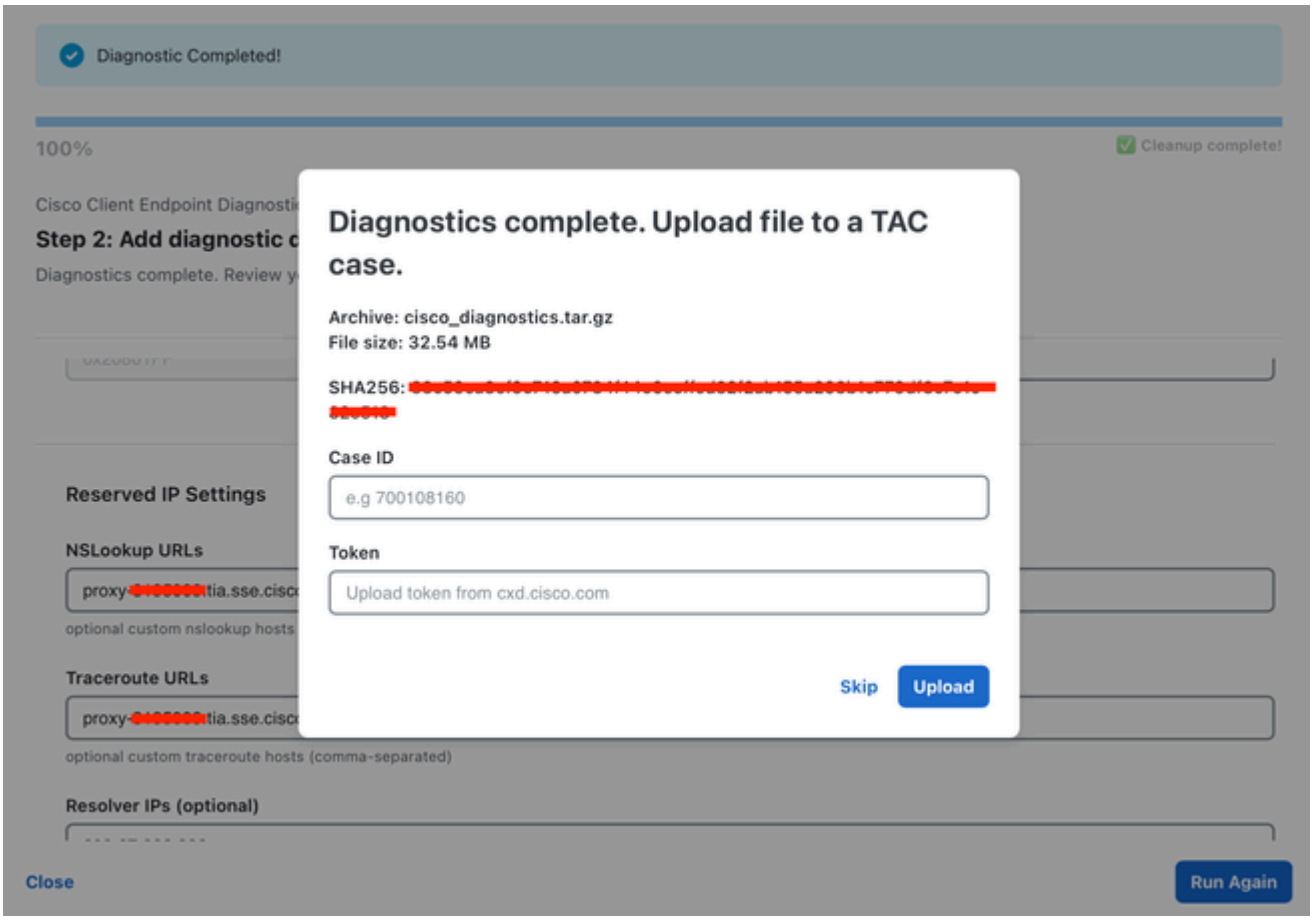
TAC 케이스에 업로드하려면

1. 케이스 ID(예698746730을 입력합니다.
2. Cisco 지원에서 제공하는 토큰을 입력합니다.
3. Open TAC Case(TAC 케이스 열기)를 클릭하여 업로드를 시작합니다.

진행률 표시줄에 업로드 상태(예: Uploading...)가 표시됩니다. 85.0%(6.56MB / 7.72MB).

업로드를 건너뛰려면

- Skip(건너뛰기)을 클릭하여 업로드하지 않고 대화 상자를 닫습니다. 아카이브 파일은 여전히 로컬에 저장됩니다.



업로드 완료/최종 화면

업로드에 성공하면 완료 배너가 다음으로 업데이트됩니다.

진단 아카이브를 케이스 [Case ID]에 업로드했습니다.

진행률 표시줄에 정리 완료 상태가 100%로 표시됩니다.

작업

- 새 진단 실행을 시작하려면 Run Again을 클릭합니다.
- 애플리케이션을 종료하려면 Close(닫기)를 클릭합니다.

출력 위치

진단 출력이 다음에 저장됩니다.

- macOS: ~/데스크톱/cisco_diagnostics/
- 창: %사용자 프로필%\Desktop\cisco_diagnostics\

출력 아카이브 파일(cisco_diagnostics.tar.gz)에는 수집된 모든 진단 데이터가 구조화된 형식으로 포함됩니다.

문제 해결

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: 이 툴은 어떤 데이터를 수집합니까?
A : 이 도구는 시스템 정보(OS, 하드웨어, 네트워크 구성), 애플리케이션 로그, Cisco 제품 구성 및 설치된 모듈 데이터, Cisco Secure Access Module과 관련된 네트워크 진단 데이터만 수집합니다. 자세한 분석은 앞의 섹션에서 수집한 시스템 데이터를 참조하십시오. 개인 데이터는 캡처되지 않습니다.

Q: 관리자/루트 액세스가 필요합니까?
A : 관리자 액세스는 선택 사항이지만 권장됩니다. 이 명령이 없으면 일부 진단(패킷 캡처, 디버그 플래그)을 건너뜁니다. 툴에서 메시지를 표시하고 선택할 수 있습니다.

Q: 도구를 여러 번 실행할 수 있습니까?
A : 예. 각 실행이 완료되면 "Run Again(다시 실행)"을 클릭하여 새 진단 세션을 시작할 수 있습니다.

Q: 출력은 어디에 저장됩니까?
A : 진단 아카이브는 cisco_diagnostics 폴더 아래에 바탕 화면에 저장됩니다.

Q: TAC 케이스 ID가 없는 경우 어떻게 합니까?
A : 업로드 대화 상자에서 "건너뛰기"를 클릭할 수 있습니다. 아카이브 파일은 여전히 로컬에 저장됩니다. 나중에 TAC 케이스에 수동으로 업로드하거나 지원 엔지니어에게 공유할 수 있습니다.

Q: 데이터가 암호화되었습니까?
A : 진단 아카이브는 압축(tar.gz)되고 중요한 데이터는 패키징 전에 자동으로 수정됩니다.

Q: HAR 캡처는 어떤 브라우저를 지원합니까?
A : HAR capture는 현재 Google Chrome만 지원합니다. 이 도구는 헤드리스 브라우저 자동화를 위해 Chrome DevTools Protocol을 사용합니다. HAR 캡처를 실행하기 전에 Chrome이 설치되어 있는지 확인합니다.

Q 일시 중지 화면이 표시되지 않습니다. 뭐가 잘못됐나요?

A : 꼭 그렇지는 않습니다. 일시 중지 단계는 시나리오에 대한 자세한 로깅이 성공적으로 활성화된 경우에만 나타납니다. 앱에서 실행 로그 확인 — 활성화 단계를 건너뛰면 툴이 일시 중지하지 않고 계속됩니다.

Q 도주량이 초과된 것 같습니다. 어떻게 해야 합니까?

A : 일시 중지된 진단 창을 찾습니다. 다른 창 뒤에 있을 수 있습니다. 계속(Continue)을 클릭하거나 명령줄에서 Enter 키를 누를 때까지 실행이 진행되지 않습니다.

Q 메시지에는 내가 예상하지 못한 기능이 나열되어 있습니다. 그게 정상인가요?

A : 예. 이 메시지는 플랫폼과 선택한 진단 옵션에 대해 툴이 활성화된 로깅 기능을 보여줍니다.

Q 일시 중지 중에 앱을 닫았습니다. 이제 어쩌지?

A : 진단 수집을 다시 실행하여 완료하십시오. 로깅이 켜져 있는지 확실하지 않은 경우 지원 엔지니

어에게 지침을 문의하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.