Informazioni sullo strumento di diagnostica degli endpoint (CEDT)

Sommario

Introduzione

Questo documento descrive il CEDT per raccogliere i dati diagnostici dal sistema e caricarli in una richiesta di assistenza TAC Cisco.

Prerequisiti

Lo strumento è disponibile per MacOS e Windows. Scaricatelo.

Cisco raccomanda la conoscenza dei seguenti argomenti:

- MacOS Fare doppio clic su Cisco Endpoint Diagnostics Tool (CEDT).app per avviarlo.
- Windows: Fare doppio clic su CEDT.exe per avviare.
- Una connessione Internet attiva.
- Un ID richiesta TAC e un token Cisco (richiesto solo se si desidera caricare i risultati direttamente).

Dati di sistema raccolti

Lo strumento raccoglie i dati di sistema, organizzati per categoria. Non vengono acquisiti dati personali.

Informazioni generali sul sistema

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

Configurazione della rete

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`

Informazioni sul prodotto

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

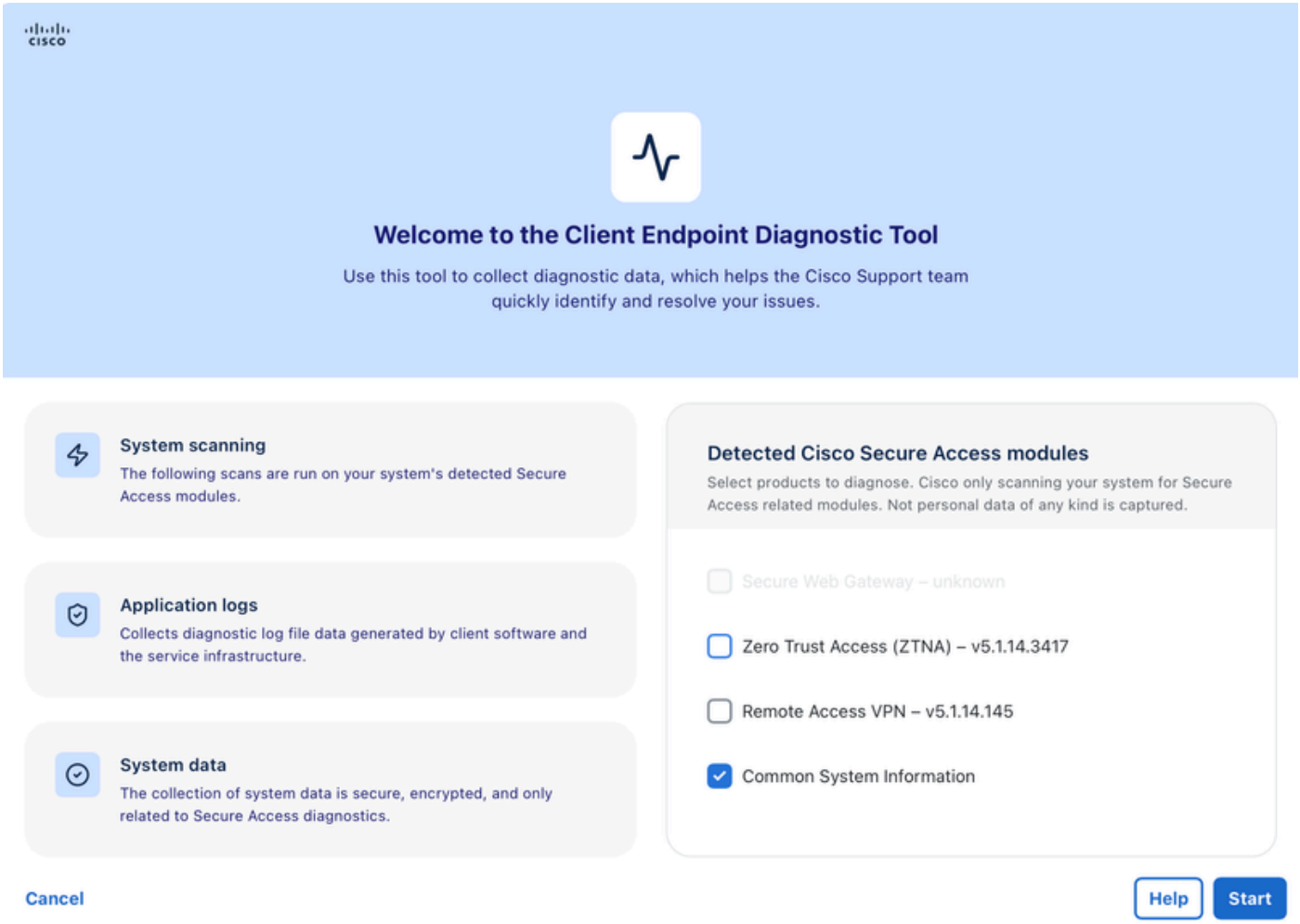
Procedura dettagliata

Schermata iniziale

Quando si avvia CEDT, viene visualizzata la schermata iniziale. Fornisce una panoramica delle operazioni eseguite dallo strumento:

- Scansione del sistema: analizza il sistema per individuare i moduli Cisco Secure Access rilevati.
- Registri applicazioni: raccoglie i dati dei file di log di diagnostica generati dal software client e dall'infrastruttura di servizio.

- Dati di sistema: la raccolta dei dati di sistema è sicura, crittografata e riguarda solo la diagnostica Secure Access.



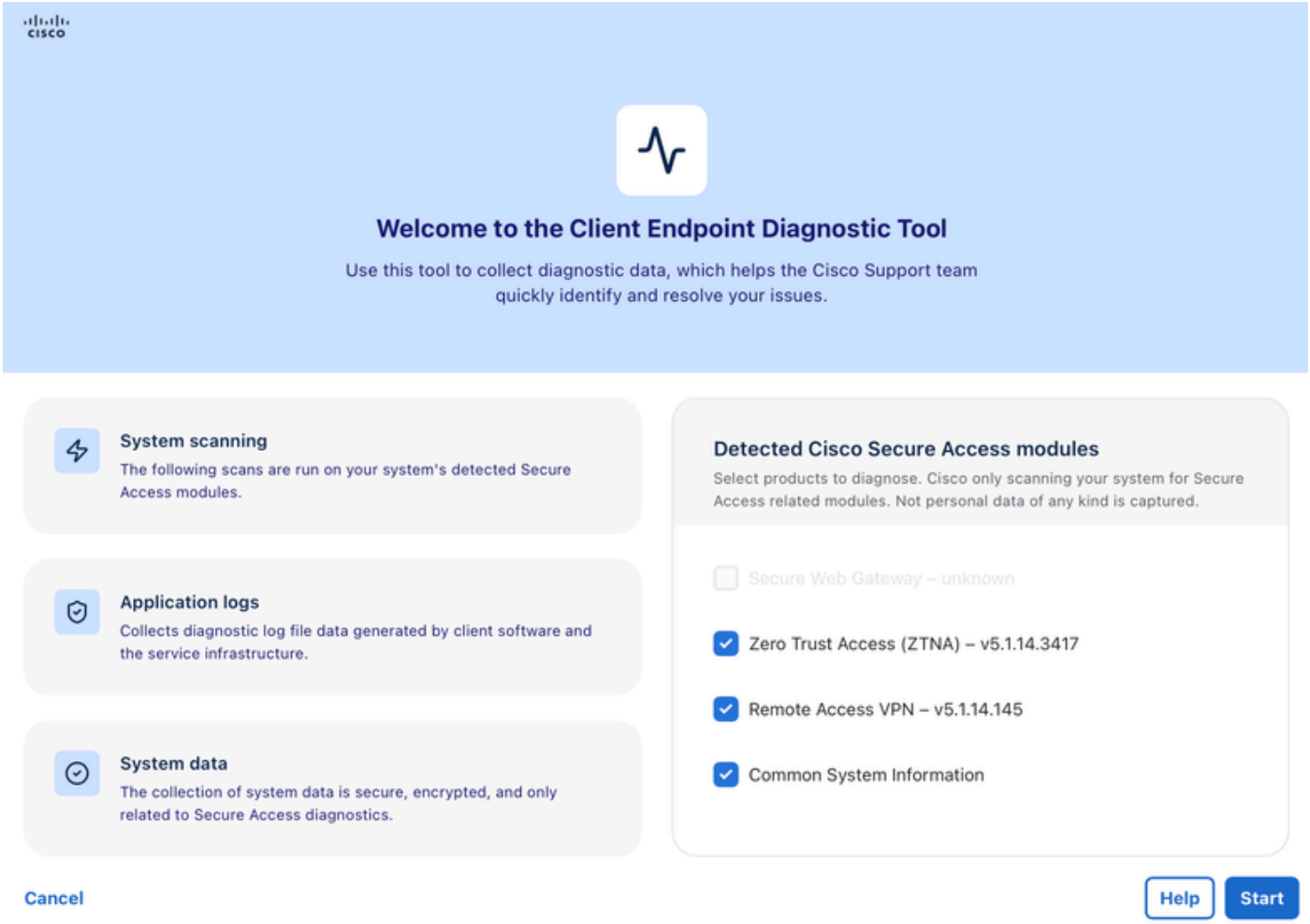
Sul lato destro, lo strumento rileva automaticamente tutti i moduli Cisco Secure Access installati sul sistema. È possibile visualizzare le caselle di controllo relative a ciascun modulo rilevato insieme al relativo numero di versione:

- ZTNA (Zero Trust Access)
- Secure Web Gateway (SWG)
- RAVPN (Remote Access VPN)
- Informazioni di sistema comuni (sempre disponibili)

Azioni

1. Selezionare o deselezionare i prodotti di cui si desidera eseguire la diagnosi.
2. Fare clic su Inizio per continuare oppure su Guida per ulteriori informazioni.

Nota: Questo strumento raccoglie solo i dati per i moduli correlati ad Accesso sicuro. Non vengono acquisiti dati personali.



Passaggio 1: Raccolta dati di diagnostica

In questa schermata è possibile scegliere i test di diagnostica e i moduli di raccolta dati da

includere.

Diagnostica di rete

Selezionare i test di connettività da eseguire:

- Ricerca DNS: esegue test di risoluzione DNS su host specificati. Supporta IP resolver personalizzati per ricerche mirate. Tutti i risultati vengono consolidati in un singolo file di output (dns/dns_lookups.txt) con delimitatori di sezione strutturati.
- Packet Capture: acquisisce i pacchetti di rete per una durata specificata (sono necessari privilegi di amministratore).
- Ping Host: esegue il ping degli host specificati per verificare la connettività.
- Output test dei criteri — testa l'applicazione dei criteri sugli URL specificati utilizzando l'endpoint dei test dei criteri Cisco (policy.test.sse.cisco.com). Supporta più host separati da virgole (massimo 10). I risultati includono i dati HAR acquisiti automaticamente durante la navigazione del test dei criteri.
- Test della velocità di rete: misura la velocità e la latenza di caricamento/download rispetto all'endpoint di test della velocità Cisco (speed.test.sse.cisco.com). Raccoglie la velocità di download (6 flussi paralleli), la velocità di caricamento (3 flussi paralleli) e la latenza/jitter ping (10 esempi ICMP). I risultati vengono salvati sia in formato JSON che in formato di riepilogo del testo.
- Raggiungibilità URL — controlla se gli URL specificati sono raggiungibili tramite richieste HTTP GET. Supporta sia HTTP (porta 80) che HTTPS (porta 443) per impostazione predefinita. È possibile specificare porte non standard nell'URL (ad esempio https://example.com:8443). Massimo 20 URL per controllo con timeout di 30 secondi per URL. I dati raccolti per URL includono: URL, stato raggiungibilità, codice di stato HTTP, tempo di risposta (ms), lunghezza del contenuto, indirizzo IP risolto, versione TLS e timestamp. I risultati vengono salvati in reachability/reachability_results.json e reachability/reachability_summary.txt.

Raccolta dati

Selezionare i moduli per raccogliere i dati sulle prestazioni e sulla connettività:

- Acquisizione HAR: registra i dati dell'archivio HTTP (HAR) da una sessione del browser. Attualmente supporta solo Google Chrome (usa il protocollo Chrome DevTools tramite l'automazione del browser headless). Lo strumento rileva automaticamente l'installazione Chrome sul sistema. Firefox e Safari non sono attualmente supportati. L'output HAR è

conforme alla specifica HAR 1.2 e include tracce di rete complete (incluse chiamate XHR/fetch attivate da JS).

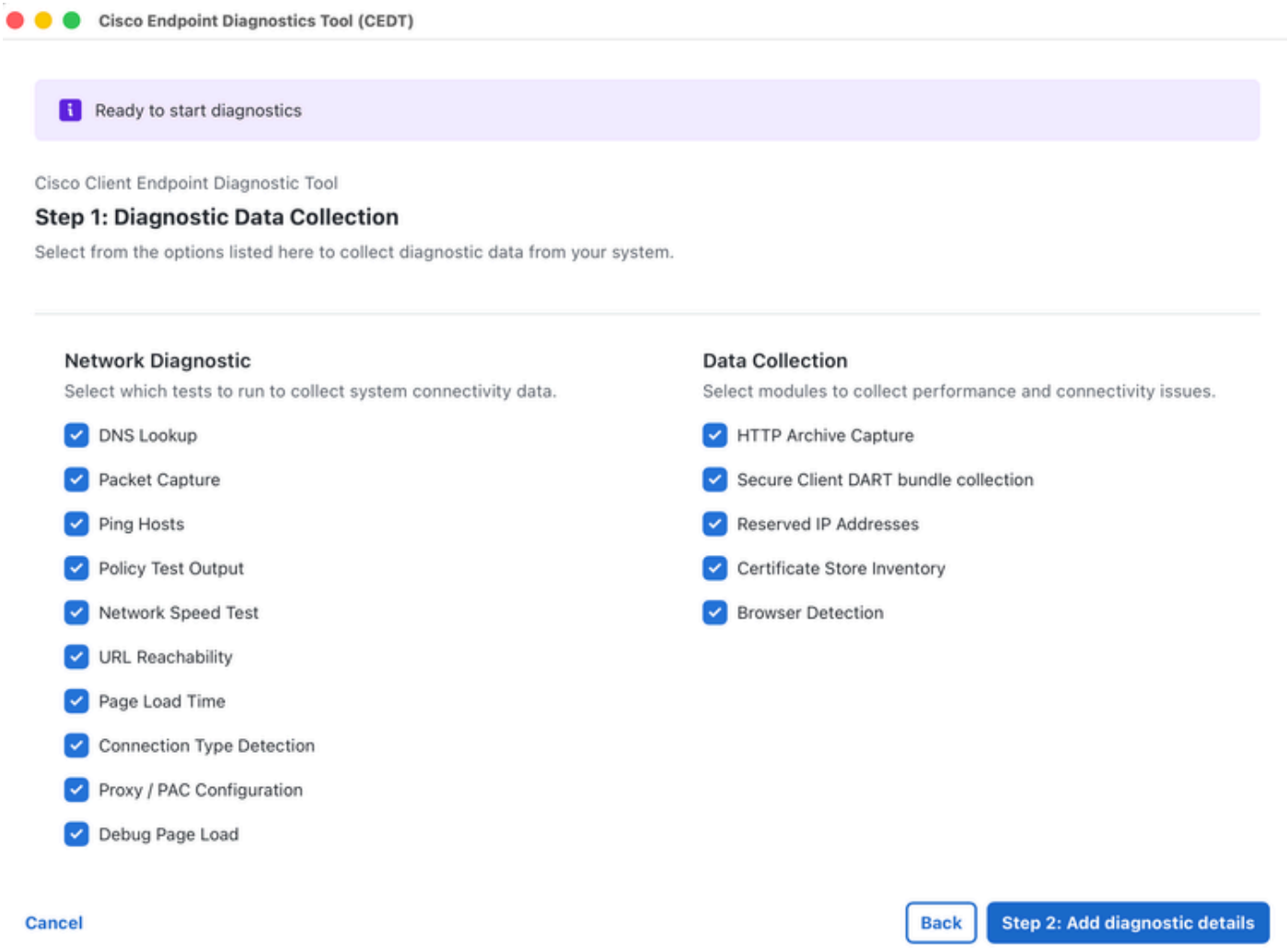
- DART Bundle Collection: raccoglie un bundle diagnostico DART da Cisco Secure Client. Sono inclusi tutti i log dei moduli, inclusi i log ZTA (Zero Trust Access), ad esempio flowlog.db in Windows all'indirizzo C:\ProgramData\Cisco\Cisco Client\ZTA\logs\.
- IP riservato - Esegue i controlli di diagnostica IP riservati. Vedere la sezione successiva per l'elenco completo di diagnostica raccolta.

Debug

- Abilita flag di debug: raccoglie i log dettagliati delle attività dell'endpoint per diagnosticare i problemi dell'endpoint. Questa opzione è disponibile solo quando viene rilevato e selezionato almeno un prodotto Cisco Secure Access.

Specifico della piattaforma

- DebugView Capture (Windows): abilita la registrazione di debug su Windows Secure Endpoint Connector. Questa opzione è disponibile solo nei sistemi Windows.



Azioni

1. Selezionare o deselezionare le opzioni di diagnostica desiderate.
2. Fare clic su Passaggio 2: Aggiungere i dettagli di diagnostica per continuare.
3. Fare clic su Indietro per tornare alla schermata iniziale o su Annulla per uscire.

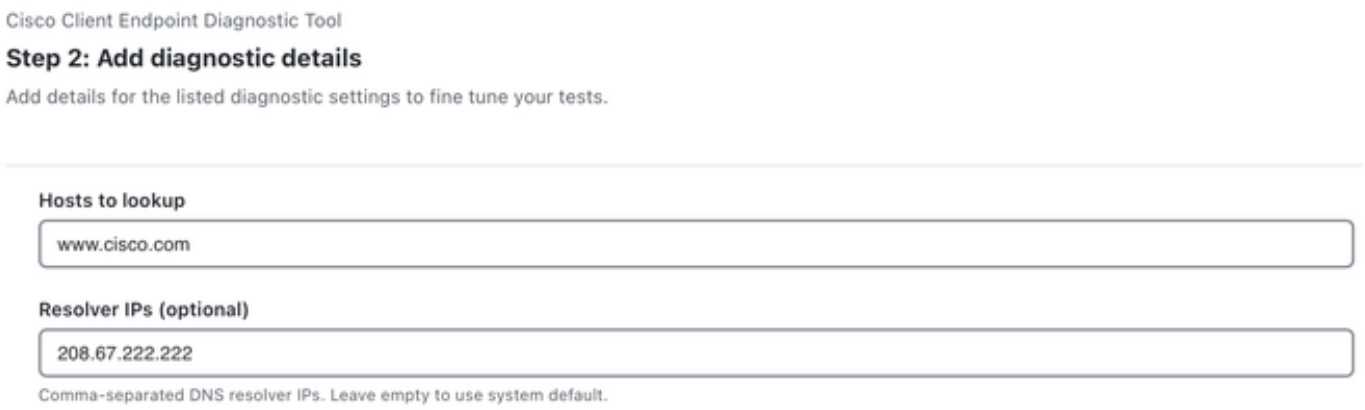
Passaggio 2: Aggiungi dettagli diagnostica

Questa schermata consente di configurare i parametri specifici per ogni test diagnostico abilitato. Vengono visualizzate solo le impostazioni per i test abilitati nel passaggio 1.

Impostazioni ricerca DNS

- Host da cercare: immettere uno o più nomi host (separati da virgole). Esempio: cisco.com
- IP resolver (facoltativo): immettere IP resolver DNS personalizzati (separati da virgole). Esempio: 208.67.222.222, 208.67.220.220. Lasciare vuoto per utilizzare il sistema di risoluzione DNS predefinito. Quando specificato, ogni host viene interrogato su ogni resolver, fornendo risultati comparativi di risoluzione DNS su server DNS diversi.

Tutti i risultati della ricerca DNS vengono consolidati in un singolo file di output: dns/dns_lookups.txt, con delimitatori di sezione TextFSM strutturati per ogni combinazione host/resolver.



Impostazioni di acquisizione pacchetti

- Interfacce - Selezionare l'interfaccia di rete su cui eseguire l'acquisizione (o lasciare il campo All).
    - Se impostato su All (modalità automatica):
        - macOS/Linux: Lo strumento esegue tcpdump -D per enumerare tutte le interfacce disponibili, quindi filtra per le interfacce attive e in esecuzione (escluse le interfacce disconnesse). Se non vengono trovate interfacce attive, viene

restituita l'interfaccia speciale any. Acquisizioni eseguite su tutte le interfacce corrispondenti in parallelo.

- Windows: Cattura su tutte le NIC utilizzando il back-end di acquisizione selezionato (vedere gli strumenti nella sezione successiva). Quando si utilizza il dump cap senza selezionare alcuna interfaccia, vengono acquisite contemporaneamente fino alle prime 3 interfacce rilevate.

- Numero di pacchetti: numero di pacchetti da acquisire per interfaccia. Predefinito: 100. Massimo: 10,000.
- Durata (sec): durata massima dell'acquisizione in secondi. Predefinito: 20 secondi su macOS/Linux, 5 secondi su Windows. Massimo: 300 secondi L'acquisizione si interrompe quando viene raggiunto il numero di pacchetto o il limite di durata, a seconda di quale condizione si verifica per prima.

Strumenti di acquisizione pacchetti per piattaforma

Nota: (Windows) Lo strumento seleziona automaticamente il miglior back-end di acquisizione disponibile. pktmon è preferito (incorporato in Windows 10 v2004+), fallback to dumpcap (se Wireshark è installato), quindi netsh trace come ultima risorsa.

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

File di output acquisizione pacchetti

L'acquisizione di ciascuna interfaccia viene salvata come file separato utilizzando la convenzione di denominazione: tcpdump/{interface_name}_capture.pcap (ad esempio en0_capture.pcap, eth0_capture.pcap). Viene inoltre generato un file manifesto dei metadati (tcpdump/packet_capture_manifest.txt), che registra la piattaforma, il numero di pacchetti, la durata, le interfacce acquisite e il back-end di acquisizione utilizzato.

Impostazioni ping

- Host da ping: immettere gli host su cui eseguire il ping (separati da virgole). Esempio:www.cisco.com

Impostazioni raggiungibilità URL

- URL da controllare: immettere gli URL da verificare (separati da virgole). Esempio: `https://github.com`
    - Utilizza le richieste HTTP GET per verificare la raggiungibilità.
    - Porte predefinite: 80 (HTTP) / 443 (HTTPS). Includere la porta nell'URL per le porte non standard (ad esempio `ashttps://example.com:8443`).
    - Massimo 20 URL per controllo.
    - Timeout : 30 secondi per URL.
    - Dati raccolti per URL: URL, stato raggiungibilità, codice di stato HTTP, tempo di risposta (ms), lunghezza del contenuto, indirizzo IP risolto, versione TLS e timestamp.
    - I risultati vengono salvati in reachability/reachability_results.json e reachability/reachability_summary.txt.

Impostazioni test criteri

- URL host: immettere gli host per il test dei criteri (separati da virgole, massimo 10). Esempio: www.cisco.com
- I test dei criteri vengono eseguiti sull'endpoint dei test dei criteri Cisco: policy.test.sse.cisco.com
- I risultati includono sia l'output dei test delle regole strutturate che i dati HAR acquisiti automaticamente durante la navigazione dei test.

Impostazioni di acquisizione HAR

- URL di destinazione: immettere gli URL per l'acquisizione di HAR (separati da virgole). Esempio: https://www.cisco.com/

Suggerimento: L'acquisizione HAR attualmente supporta solo Google Chrome. Lo strumento utilizza il protocollo Chrome DevTools (tramite chromedp) per automatizzare una sessione Chrome headless e acquisire il traffico di rete. Assicurarsi che Google Chrome sia installato sul sistema. Firefox e Safari non sono attualmente supportati.

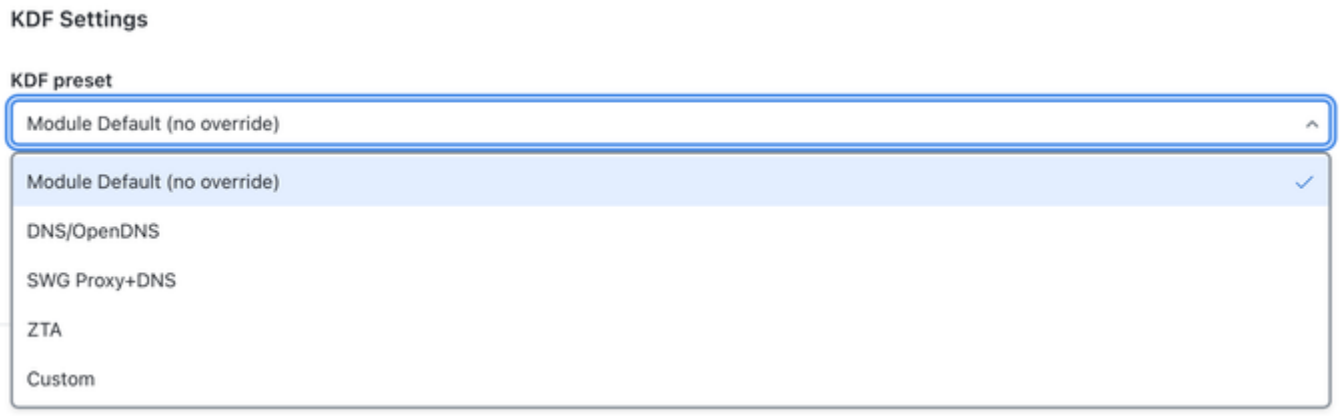
Impostazioni KDF

Configurare i flag della funzione di derivazione della chiave utilizzati durante la raccolta diagnostica. I flag KDF controllano le categorie di debug abilitate in Cisco Secure Client:

- Predefinito KDF — Selezionare un predefinito Funzione di derivazione chiave.
- KDF HEX: il valore esadecimale viene popolato automaticamente in base alla preimpostazione selezionata. Quando è selezionato "Personalizzato", immettere il proprio valore esadecimale.

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.



Impostazioni IP riservate

- URL di NSLookup: host nslookup personalizzati facoltativi (separati da virgola). Massimo 10 URL. Ogni host personalizzato viene interrogato su tutti i resolver configurati.

- Trace URL (URL di traccia) - Host traceroute/tracert personalizzati facoltativi (separati da virgola). Massimo 10 URL. Lo strumento usa automaticamente traceroute su macOS/Linux e tracert su Windows.
- IP resolver: IP resolver personalizzati opzionali per query nslookup (separate da virgole, ad esempio 208.67.222).
- 222, 208.67.220.220). Massimo 5 indirizzi IP. Se specificato, oltre ai tre resolver incorporati vengono utilizzati i resolver personalizzati (DNS predefinito del sistema, 127.0.0.1, 208.67.222.222).

Dettagli IP riservato

Per impostazione predefinita, la diagnostica degli indirizzi IP riservati raccoglie questi dati:

Destinazioni Traceroute/Tracert predefinite (eseguibili automaticamente su tutte le destinazioni seguenti):

Destinazione	Scopo
208.67.222.222	Route al server dei nomi primario OpenDNS
208.67.220.220	Route al server dei nomi secondario OpenDNS
146.112.255.50	Route to Cisco SWG infrastructure IP

swg-url-proxy-https-sse.sigproxy.qq.opendns.com	Invia a nome host proxy SWG

- macOS/Linux: Utilizza il comando traceroute
- Windows: Utilizza il comando tracert

Query NSLookup predefinite (eseguite automaticamente su tutte queste query):

Ogni destinazione nslookup viene interrogata su ogni resolver nell'elenco resolver. Per impostazione predefinita, l'elenco dei resolver include tre resolver predefiniti:

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

Se sono configurati indirizzi IP del resolver personalizzati (ad esempio 208.67.222.222), questi vengono aggiunti all'elenco del resolver e viene eseguita una query su ogni destinazione di nslookup.

Destinazioni NSLookup:

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

Ad esempio, con i 3 resolver predefiniti, vengono generate 6 query nslookup (2 destinazioni x 3 resolver). L'aggiunta di un indirizzo IP del resolver personalizzato aumenta questo numero a 8 query (2 destinazioni x 4 resolver).

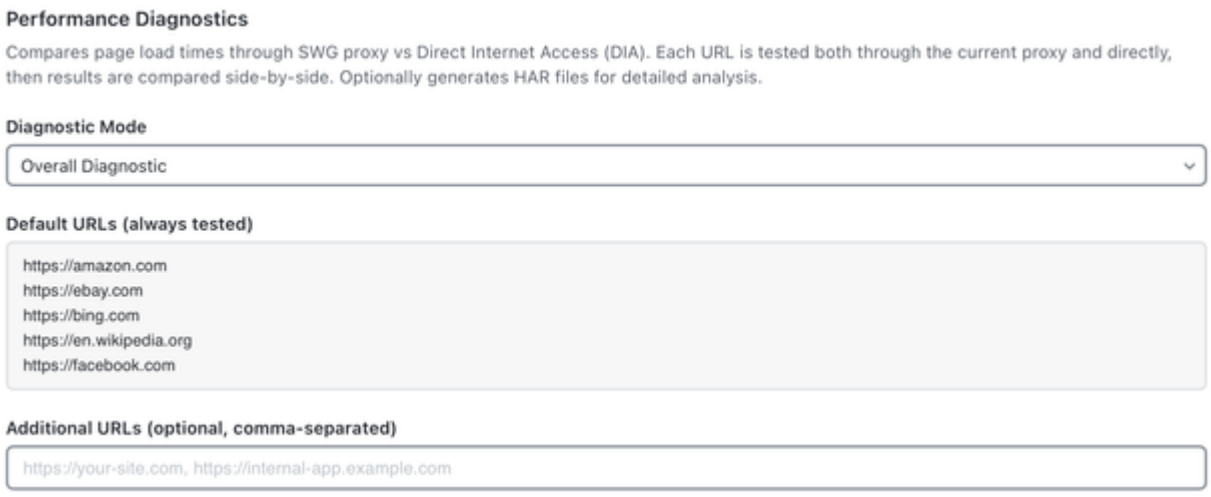
Gli URL NSLookup personalizzati forniti dall'utente vengono sottoposti a query sullo stesso elenco di resolver completo (resolver predefiniti + personalizzati).

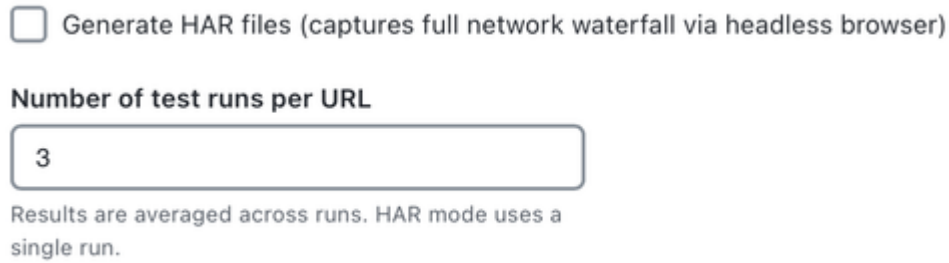
Tutti i risultati vengono consolidati in un unico file: reserved_ip/reserved_ip_diagnostics.txt, raggruppati per sezione (traceroute, nslookup) con intestazioni leggibili dall'uomo che indicano la destinazione e il resolver per ciascuna voce.

Diagnostica delle prestazioni

Confronta i tempi di caricamento delle pagine tramite proxy SWG e Direct Internet Access (DIA). È disponibile in due modalità:

1 Modalità diagnostica generale: ciascun URL viene verificato sia tramite il proxy corrente sia direttamente, quindi i risultati vengono confrontati uno accanto all'altro. Facoltativamente, genera file HAR per l'analisi dettagliata.





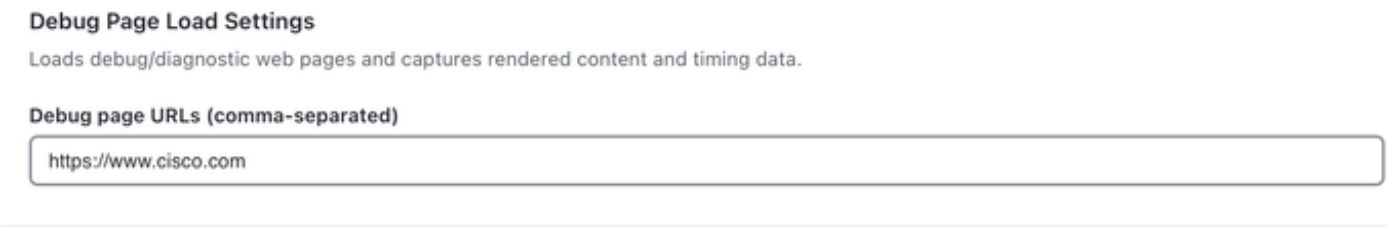
2 Modalità diagnostica URL singolo: È possibile immettere un URL specifico da verificare tramite il proxy corrente e direttamente, quindi i risultati vengono confrontati l'uno accanto all'altro. Facoltativamente, genera file HAR per l'analisi dettagliata.

Impostazioni Oggetto Archivio Certificati

- Enumera i certificati dagli archivi certificati configurati:
  - Sistema
  - Accesso
  - Radice
  - E altro ancora
- Identifica rapidamente i certificati mancanti, scaduti o non attendibili

Impostazioni caricamento pagina di debug:

- Carica gli URL di debug configurabili.
- Clip:
  - Intestazioni risposte
  - Corpo risposta
  - Informazioni sugli intervalli
  - metadati SSL



Azioni

1. Specificare o regolare le impostazioni per ogni diagnostica abilitata.
2. Fare clic su Avvia diagnostica per avviare l'esecuzione della diagnostica.
3. Fare clic su Indietro per tornare al passaggio 1 oppure su Annulla per uscire

---

Nota: I campi con errori di convalida sono evidenziati. È necessario correggerli prima di avviare la diagnostica.

Sospendi e continua

Quando si esegue una raccolta diagnostica che include funzionalità avanzate di risoluzione dei problemi (ad esempio, ZTNA o traccia SWG), lo strumento di diagnostica degli endpoint Cisco può sospendere in parte l'esecuzione e chiedere di riprodurre il problema prima che continui.

In questo modo si ha il tempo di attivare il problema mentre è attiva la registrazione dettagliata, in modo che il team di supporto riceva dati diagnostici più utili.

- Quando viene visualizzata la finestra Diagnostica sospesa, leggere il messaggio che indica

le funzionalità di registrazione attive.

- Riprodurre il problema che si sta risolvendo. Ad esempio:
    - Riconnetti a VPN
    - Aprire l'applicazione interna non riuscita
    - Ripetere i passaggi che causano l'errore
- Al termine della riproduzione del problema, fare clic su Continua

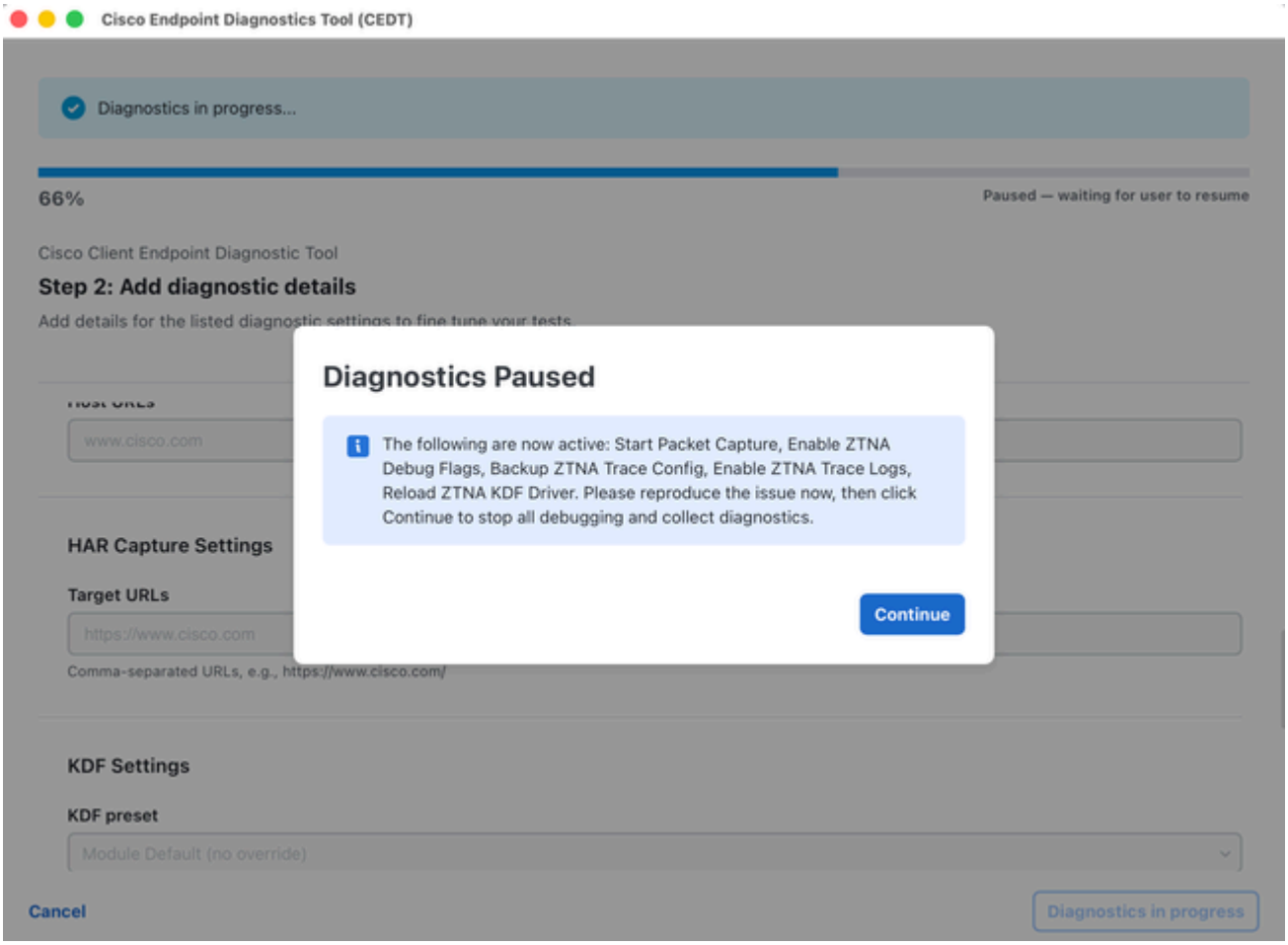
Fate finire la corsa. Lo strumento raccoglie quindi i file, ripristina le impostazioni normali e crea l'archivio di diagnostica.

NOTA: non chiudere l'applicazione durante la pausa. La registrazione rimane attiva fino a quando non si fa clic su Continua per completare l'esecuzione.

(riga di comando)

Se lo strumento viene eseguito da un terminale, nella finestra viene visualizzato un messaggio di pausa anziché una finestra di dialogo.

1. Leggere il messaggio di pausa visualizzato nel terminale.
2. Riprodurre il problema.
3. Tornare al terminale e premere Invio per continuare.
4. Aspettate che finisca la corsa.



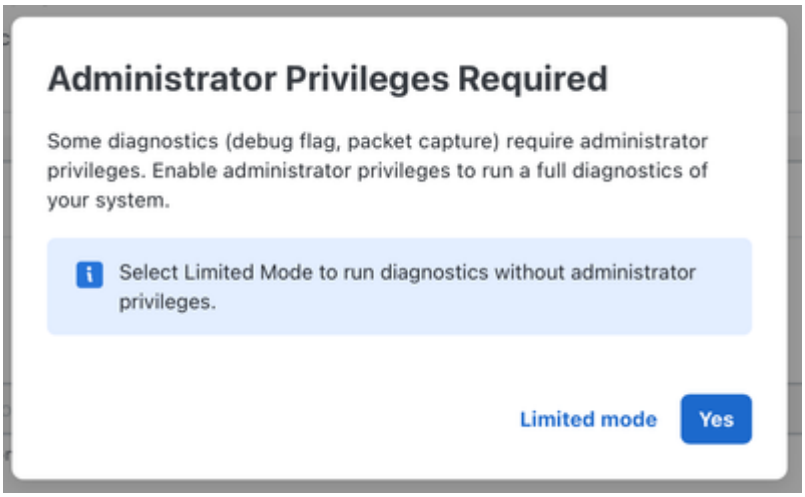
Prompt dei privilegi di amministratore

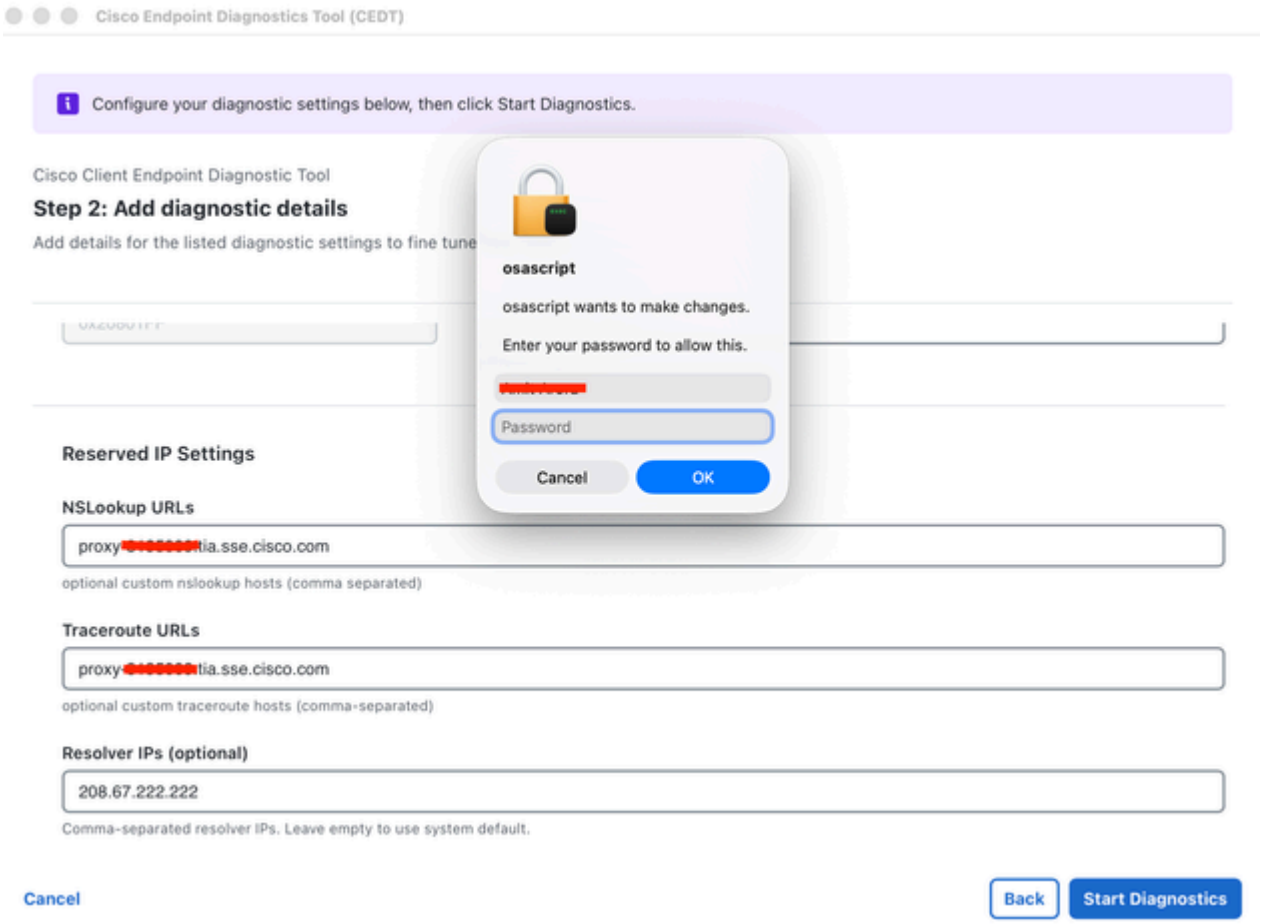
Dopo aver fatto clic su Avvia diagnostica, lo strumento può richiedere i privilegi di amministratore se sono state abilitate funzionalità che richiedono un accesso elevato (ad esempio Acquisizione pacchetto o Flag di debug).

Viene visualizzata una finestra di dialogo con il titolo Privilegi di amministratore richiesti:

- Fare clic su Sì per concedere i privilegi di amministratore. In questo modo viene attivato il prompt nativo delle credenziali macOS/Windows.
- Fare clic su Modalità limitata per procedere senza elevazione. Le attività privilegiate (acquisizione pacchetti, flag di debug) vengono ignorate.
- macOS: È possibile visualizzare la finestra di dialogo standard della password macOS da osascript. Immettere la password di sistema e fare clic su OK.
- Windows: Viene visualizzato un prompt di elevazione UAC standard. Fare clic su Sì per

consentire l'operazione.



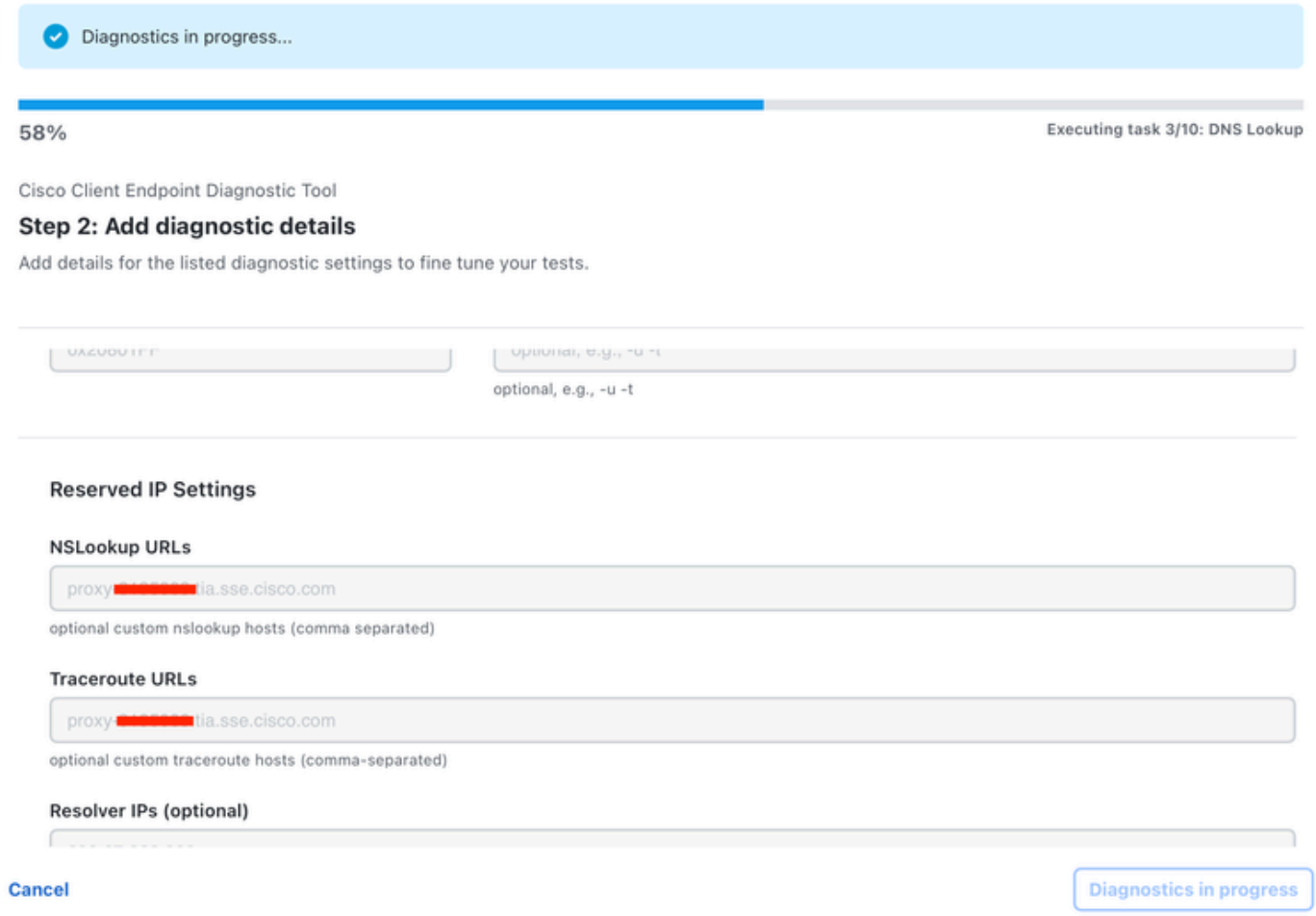


Diagnostica in corso

Una volta avviato, lo strumento esegue tutte le attività di diagnostica selezionate:

- Una barra di avanzamento indica il completamento complessivo (ad esempio, 59% — Esecuzione task 3/9 in corso: ricerca DNS).
- Diagnostica in corso... Il banner viene visualizzato nella parte superiore.
- Tutti i campi delle impostazioni sono disattivati/disattivati durante l'esecuzione.
- Nel piè di pagina viene visualizzato un pulsante Diagnostica in corso (disattivato) per indicare che lo strumento è occupato.

Attendere il completamento della diagnostica. Non chiudere l'applicazione.



1.

Diagnostica completata — Caricamento in TAC

Al termine di tutte le operazioni di diagnostica, viene visualizzata una finestra di dialogo di completamento:

Diagnostica completata. Caricare il file in una richiesta TAC.

Viene visualizzata la finestra di dialogo:

- Archivio: il nome file dell'archivio di diagnostica generato (ad esempio cisco_diagnostics.tar.gz).
- Dimensioni file — le dimensioni dell'archivio (ad esempio 7,72 MB).
- SHA256: checksum del file di archivio per la verifica dell'integrità.

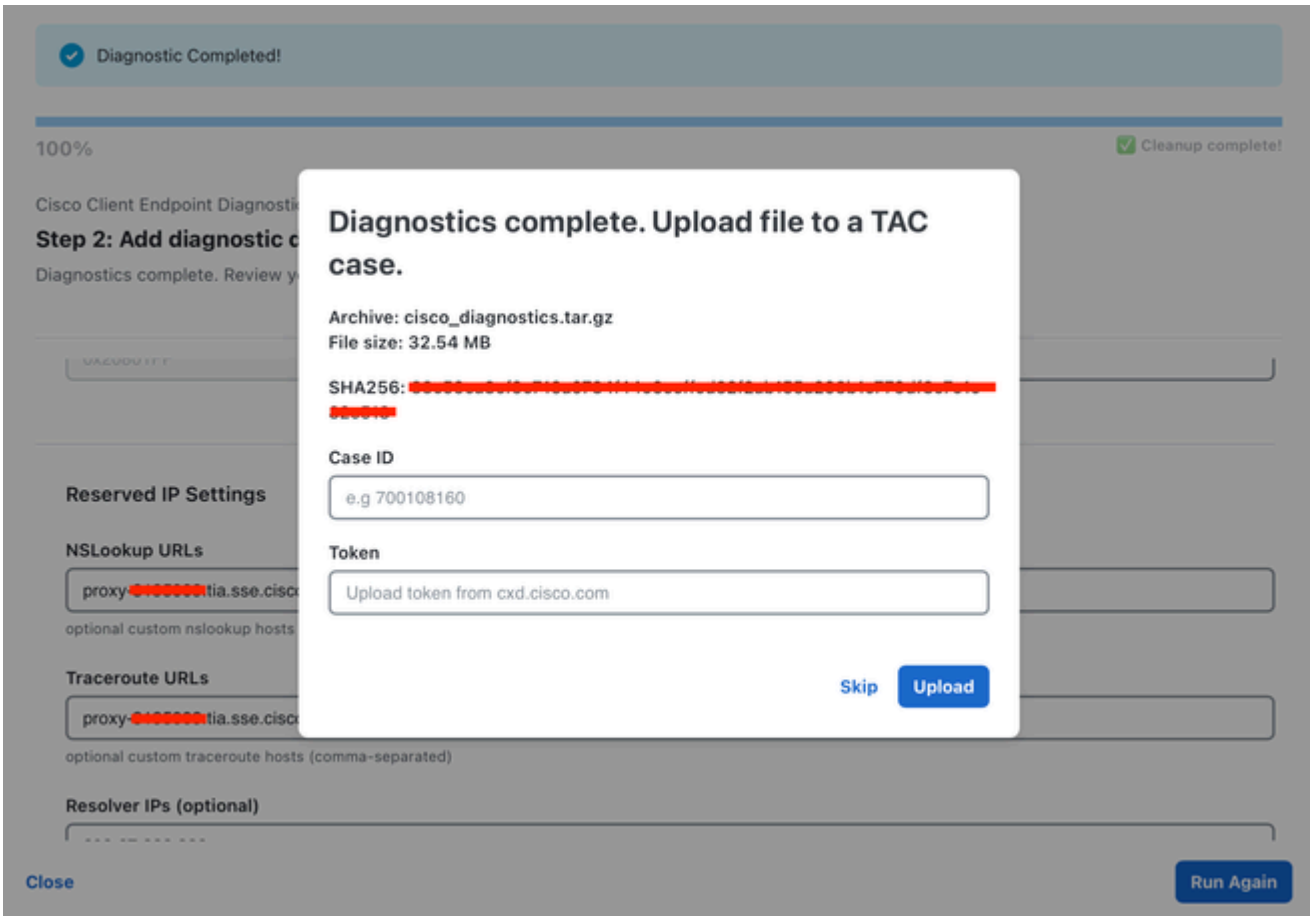
Per caricare una richiesta TAC:

1. Inserire l'ID della richiesta (ad esempio 698746730).
2. Immettere il token (fornito dal supporto Cisco).
3. Fare clic su Open TAC Case per avviare il caricamento.

Una barra di avanzamento mostra lo stato del caricamento (ad esempio Caricamento in corso... 85,0% (6,56 MB / 7,72 MB).

Per ignorare il caricamento:

- Fare clic su Ignora per chiudere la finestra di dialogo senza caricare. Il file di archivio viene comunque salvato localmente.



Caricamento completato - Schermata finale

Al termine del caricamento, il banner di completamento viene aggiornato a:

Archivio di diagnostica caricato nella richiesta [ID richiesta]

Sulla barra di avanzamento viene visualizzato 100% con lo stato Pulizia completata.

Azioni

- Fare clic su Esegui di nuovo per avviare una nuova esecuzione della diagnostica.
- Fare clic su Chiudi per uscire dall'applicazione.

Percorso di output

L'output di diagnostica viene salvato in:

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

Il file dell'archivio di output (cisco_diagnostics.tar.gz) contiene tutti i dati diagnostici raccolti in un formato strutturato.

Risoluzione dei problemi

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.

Domande frequenti

Q: Quali dati vengono raccolti dallo strumento?
A: Lo strumento raccoglie informazioni sul sistema (sistema operativo, hardware, configurazione di rete), log delle applicazioni, dati sulla configurazione dei prodotti Cisco e dei moduli installati e dati di diagnostica di rete relativi solo ai moduli Cisco Secure Access. Per una descrizione dettagliata, vedere la sezione Cosa sono i dati di sistema raccolti nella precedente sezione. Non vengono

acquisiti dati personali.

Q: È necessario l'accesso come amministratore/utente root?
A: L'accesso come amministratore è facoltativo, ma consigliato. Senza di esso, alcune operazioni diagnostiche (acquisizione pacchetti, flag di debug) vengono ignorate. Lo strumento vi chiede di scegliere.

Q: È possibile eseguire lo strumento più volte?
A: Sì. Al termine di ogni esecuzione, è possibile fare clic su "Esegui di nuovo" per avviare una nuova sessione di diagnostica.

Q: Dove viene salvato l'output?
A: L'archivio di diagnostica viene salvato sul desktop nella cartella cisco_diagnostics.

Q: Cosa succede se non ho l'ID della richiesta TAC?
A: È possibile fare clic su "Skip" nella finestra di dialogo di caricamento. Il file di archivio viene comunque salvato localmente. È possibile caricarlo manualmente in una richiesta TAC in un secondo momento o condividerlo con il tecnico di assistenza.

Q: I dati sono crittografati?
A: L'archivio diagnostico viene compresso (tar.gz) e i dati sensibili vengono automaticamente rigenerati prima del packaging.

Q: Quali browser sono supportati dall'acquisizione HAR?
A: HAR acquisizione attualmente supporta solo Google Chrome. Lo strumento utilizza il protocollo Chrome DevTools per l'automazione del browser headless. Assicurarsi che Chrome sia installato prima di eseguire l'acquisizione HAR.

Q La schermata di pausa non è mai apparsa. C'è qualcosa che non va?

A: Non necessariamente. Il passaggio di pausa viene visualizzato solo quando la registrazione dettagliata è stata abilitata per lo scenario. Controlla il log di esecuzione nell'app — se i passaggi di abilitazione sono stati ignorati, lo strumento continua senza pausa.

Q La corsa sembra bloccata. Cosa devo fare?

A: Cercare la finestra Diagnostica sospesa, che può trovarsi dietro ad altre finestre. L'esecuzione non si sposta in avanti fino a quando non si fa clic su Continua (o si preme Invio nella riga di comando).

Q Il messaggio elenca le funzioni che non mi aspettavo. È normale?

A: Sì. Il messaggio mostra le funzionalità di registrazione attivate dallo strumento per la piattaforma e le opzioni di diagnostica selezionate.

Q L'app è stata chiusa durante la pausa. E adesso?

A: Eseguire di nuovo la raccolta diagnostica e attendere il completamento. Se non si è certi che la registrazione sia stata effettuata, contattare il tecnico di assistenza.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).