Entender a Ferramenta de Diagnóstico de Endpoint (CEDT)

Contents

Introdução

Este documento descreve o CEDT para coletar dados de diagnóstico do seu sistema e carregá-los em um caso de suporte do Cisco TAC.

Pré-requisitos

A ferramenta está disponível para MacOS e Windows. Baixe a ferramenta.

A Cisco recomenda que você tenha conhecimento destes tópicos:

- MacOS: Clique duas vezes em Cisco Endpoint Diagnostics Tool (CEDT).app para iniciar.
- Windows: Clique duas vezes em CEDT.exe para iniciar.
- Uma conexão ativa com a Internet.
- Um ID de caso e um token do Cisco TAC (obrigatórios somente se você quiser carregar os resultados diretamente).

Dados do sistema coletados

A ferramenta coleta esses dados do sistema, organizados por categoria. Nenhum dado pessoal de qualquer tipo é capturado.

Informações gerais do 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

Configuração de rede

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`

Informações do produto

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

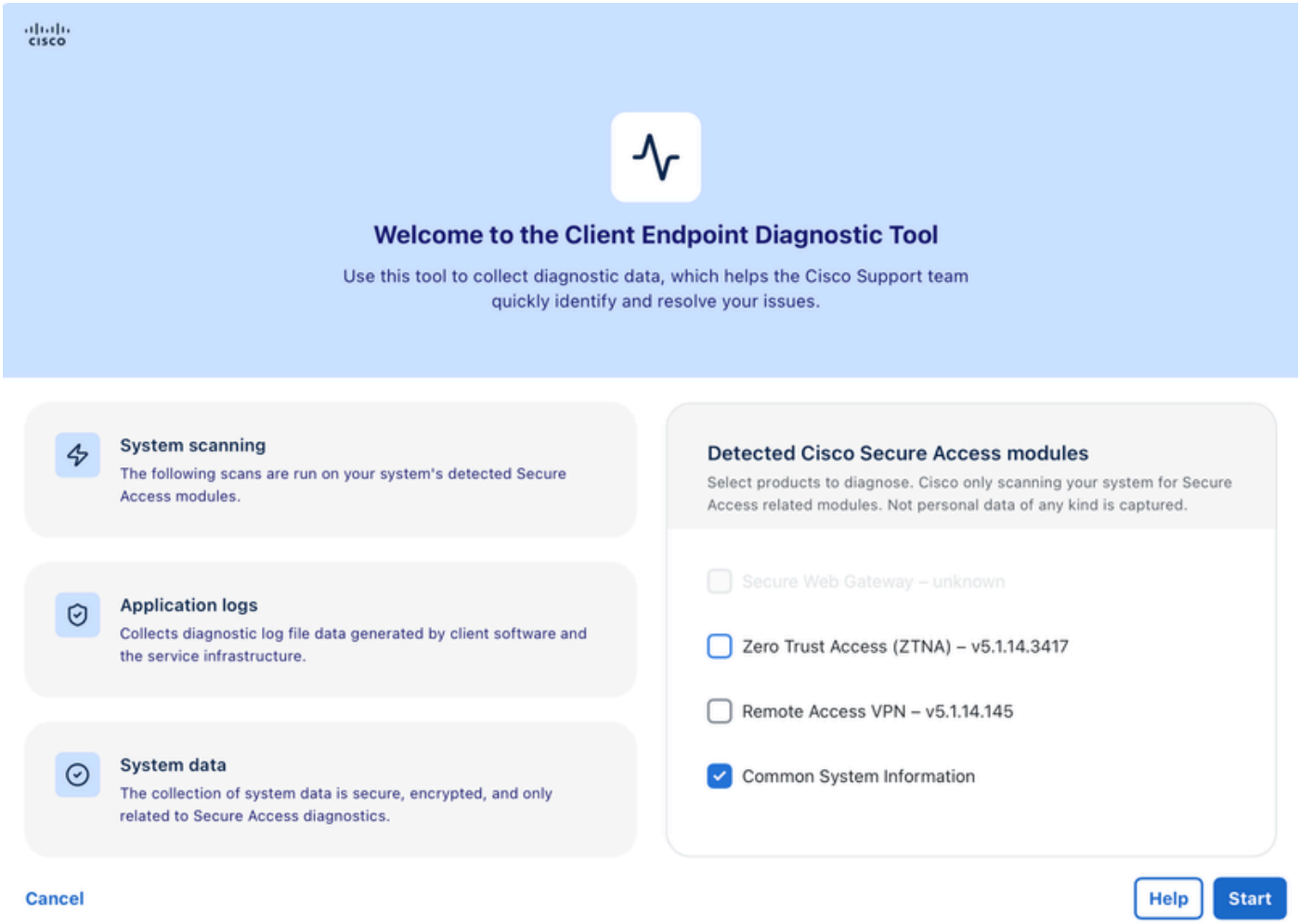
Passo a Passo

Tela de boas-vindas

Quando você inicia o CEDT, a tela Welcome (Bem-vindo) é exibida. Ele fornece uma visão geral do que a ferramenta faz:

- Varredura do sistema — Verifica o sistema em busca de módulos detectados do Cisco Secure Access.
- Logs de aplicativos — Coleta dados do arquivo de log de diagnóstico gerados pelo software cliente e pela infraestrutura do serviço.

- Dados do sistema — A coleta de dados do sistema é segura, criptografada e está relacionada apenas aos diagnósticos de acesso seguro.



No lado direito, a ferramenta detecta automaticamente qualquer módulo Cisco Secure Access instalado em seu sistema. Você pode ver caixas de seleção para cada módulo detectado juntamente com seu número de versão:

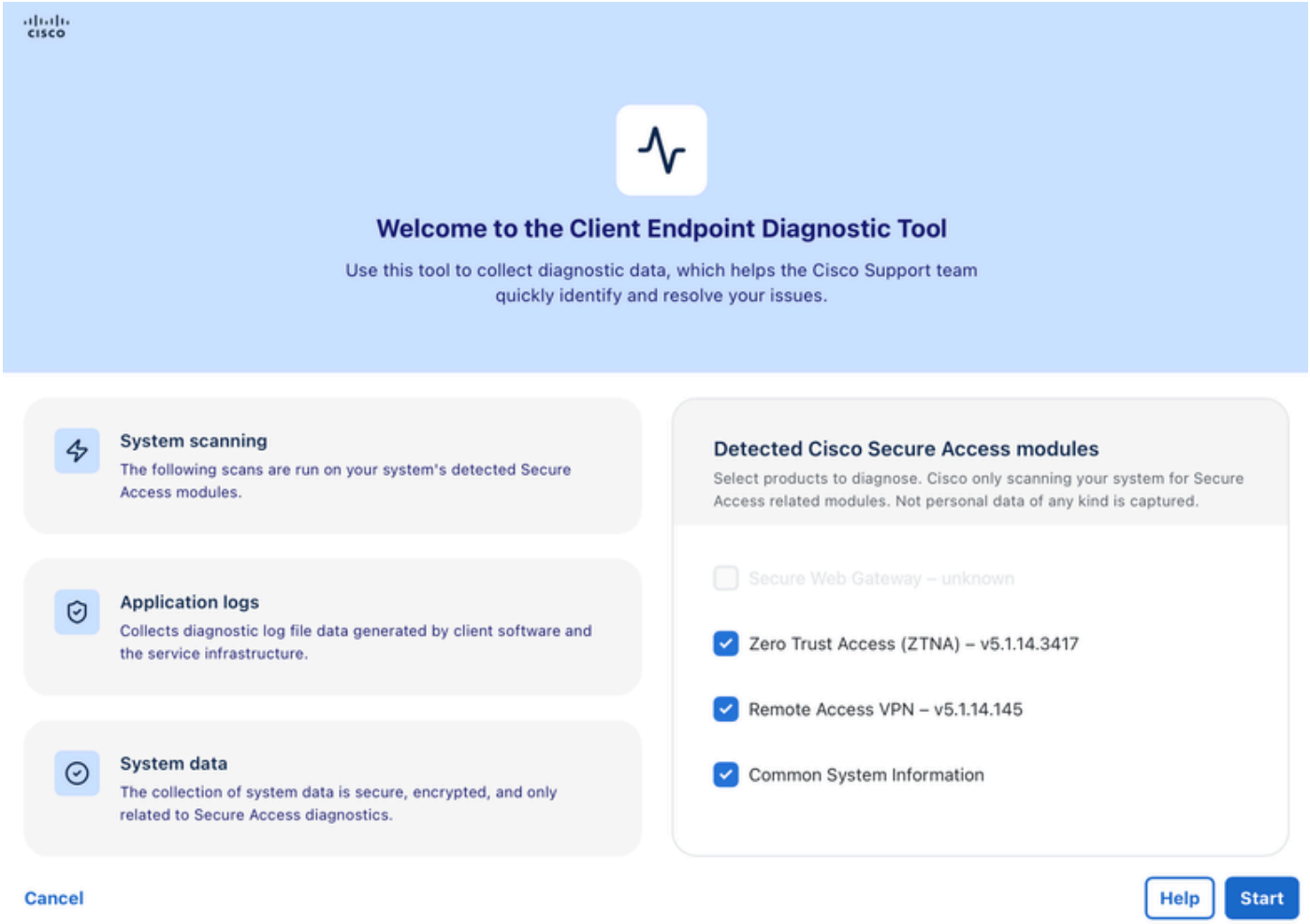
- Acesso de Confiança Zero (ZTNA)
- Gateway da Web seguro (SWG)
- VPN de acesso remoto (RAVPN)
- Informações comuns do sistema (sempre disponíveis)

Ações

1. Marque ou desmarque os produtos que deseja diagnosticar.

2. Clique em Vamos começar para continuar ou clique em Ajuda para obter mais informações.

Note: Esta ferramenta coleta apenas dados para módulos relacionados ao Acesso seguro. Nenhum dado pessoal de qualquer tipo é capturado.



Passo 1: Coleta de Dados de Diagnóstico

Esta tela permite escolher quais testes de diagnóstico e módulos de coleta de dados incluir.

Diagnóstico de rede

Selecione os testes de conectividade a serem executados:

- Pesquisa de DNS — Executa testes de resolução de DNS em hosts especificados. Suporta IPs de resolvedor personalizado para pesquisas direcionadas. Todos os resultados são consolidados em um único arquivo de saída (dns/dns_lookups.txt) com delimitadores de seção estruturada.
- Captura de Pacotes — Captura pacotes de rede por uma duração especificada (requer privilégios de administrador).
- Ping Hosts — Efetua ping nos hosts especificados para verificar a conectividade.
- Saída do teste de política — testa a aplicação da política em relação a URLs especificados usando o ponto final do teste de política da Cisco (policy.test.sse.cisco.com). Suporta vários hosts separados por vírgula (máximo de 10). Os resultados incluem dados HAR capturados automaticamente durante a navegação do teste de política.
- Network Speed Test — Mede a velocidade de upload/download e a latência em relação ao ponto de extremidade de teste de velocidade da Cisco (speed.test.sse.cisco.com). Coleta a velocidade de download (6 fluxos paralelos), a velocidade de upload (3 fluxos paralelos) e a latência/jitter do ping (10 amostras ICMP). Os resultados são salvos nos formatos JSON e resumo de texto.
- Acessibilidade de URL — Verifica se os URLs especificados podem ser acessados por meio de solicitações HTTP GET. Suporta HTTP (porta 80) e HTTPS (porta 443) por padrão. As portas fora do padrão podem ser especificadas na URL (como https://example.com:8443). Máximo de 20 URLs por verificação com um tempo limite de 30 segundos por URL. Os dados coletados por URL incluem: URL, status de acessibilidade, código de status HTTP, tempo de resposta (ms), comprimento do conteúdo, endereço IP resolvido, versão TLS e carimbo de data/hora. Os resultados são salvos em reachability/reachability_results.json e reachability/reachability_summary.txt.

Levantamento de dados

Selecione os módulos para coletar dados de desempenho e conectividade:

- Captura HAR — Registra dados HAR (HTTP Archive, arquivo HTTP) de uma sessão do navegador. Atualmente suporta apenas o Google Chrome (usa o protocolo Chrome DevTools através da automação de navegador sem cabeça). A ferramenta detecta automaticamente a instalação do Chrome no sistema. O Firefox e o Safari não são compatíveis no momento. A saída HAR segue a especificação HAR 1.2 e inclui rastreamentos de rede completos (incluindo chamadas XHR/fetch disparadas por JS).

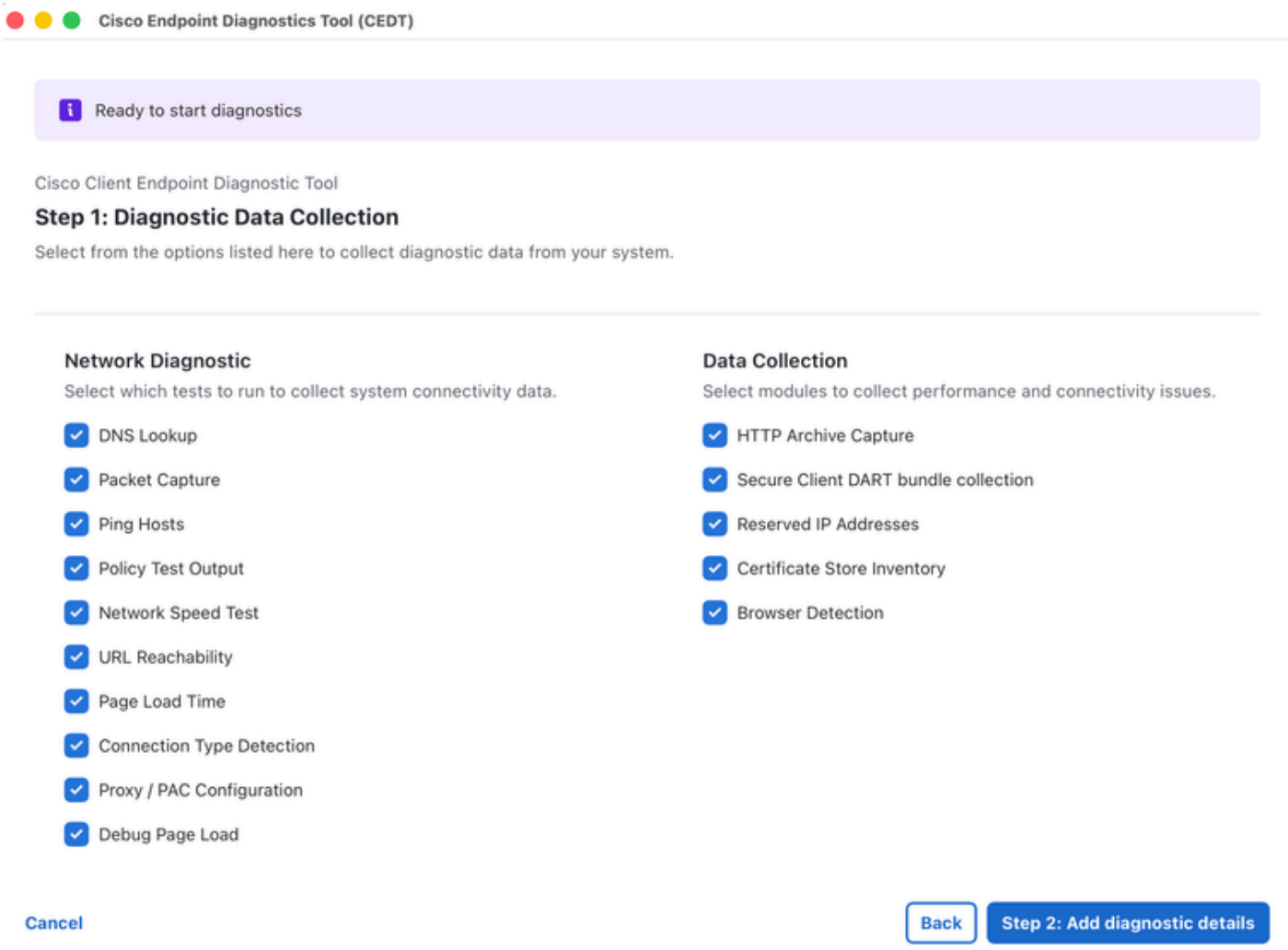
- DART Bundle Collection — Coleta um pacote de diagnóstico DART do Cisco Secure Client. Isso inclui todos os logs do módulo, inclusive os logs ZTA (Zero Trust Access) (como flowlog.db no Windows em C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\).
- IP reservado — Executa verificações de diagnóstico de IP reservado. Consulte a próxima seção para obter a lista completa de diagnósticos coletados.

Debug

- Ativar Flags de Depuração — Coletar logs detalhados de atividades de endpoint para diagnosticar problemas de endpoint. Essa opção está disponível apenas quando pelo menos um produto Cisco Secure Access é detectado e selecionado.

Específico da plataforma

- Captura DebugView (Windows) — Habilita o log de depuração no Conector de Ponto de Extremidade Seguro do Windows. Essa opção está disponível apenas em sistemas Windows.



Ações

1. Marque ou desmarque as opções de diagnóstico desejadas.
2. Clique na Etapa 2: Adicione detalhes de diagnóstico para continuar.
3. Clique em Voltar para retornar à tela de Boas-vindas ou em Cancelar para sair.

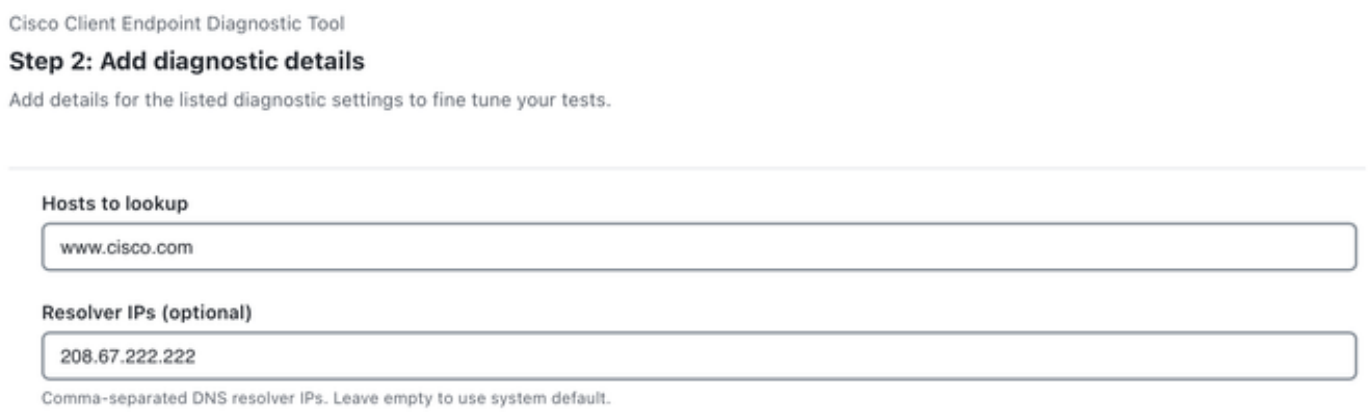
Passo 2: Adicionar Detalhes de Diagnóstico

Esta tela permite configurar os parâmetros específicos para cada teste de diagnóstico ativado. Somente as configurações para testes que você habilitou na Etapa 1 são mostradas.

Configurações de pesquisa DNS

- Hosts a pesquisar — Insira um ou mais nomes de host (separados por vírgula). Exemplo: cisco.com
- IPs do resolvedor (opcional) — Insira os IPs do resolvedor de DNS personalizado (separados por vírgula). Exemplo: 208.67.222.222, 208.67.220.220. Deixe em branco para usar o resolvedor DNS padrão do sistema. Quando especificado, cada host é consultado em relação a cada resolvedor, fornecendo resultados de resolução DNS comparativos em diferentes servidores DNS.

Todos os resultados da pesquisa de DNS são consolidados em um único arquivo de saída: dns/dns_lookups.txt, com delimitadores de seção TextFSM estruturados para cada combinação de host/resolvedor.



Configurações de captura de pacote

- Interfaces — Selecione a interface de rede na qual capturar (ou deixe como All).
    - Quando definido como Todos (modo automático):
        - MacOS/Linux: A ferramenta executa tcpdump -D para enumerar todas as interfaces disponíveis e, em seguida, filtra as interfaces que estão Ativas e em

Execução (excluindo as interfaces desconectadas). Se nenhuma interface ativa for encontrada, ela voltará para a interface any especial. As capturas são executadas em todas as interfaces correspondentes em paralelo.

- Windows: Capturas em todas as NICs usando o back-end de captura selecionado (consulte as ferramentas na próxima seção). Ao usar dumpcap sem nenhuma interface selecionada, até as 3 primeiras interfaces detectadas são capturadas simultaneamente.

- Contagem de pacotes — Número de pacotes a capturar por interface. Padrão: 100. Máximo: 10,000.
- Duração (seg) — Duração máxima da captura em segundos. Padrão: 20 segundos no MacOS/Linux, 5 segundos no Windows. Máximo: 300 segundos. A captura é interrompida quando a contagem de pacotes ou o limite de duração é atingido, o que ocorrer primeiro.

Ferramentas de captura de pacotes por plataforma

Note: (Windows): A ferramenta seleciona automaticamente a melhor infraestrutura de captura disponível. o pktmon é preferencial (incorporado no Windows 10 v2004+), voltando para o dumpcap (se o Wireshark estiver instalado) e, em seguida, o netsh trace como último recurso.

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

Arquivos de saída de captura de pacote

A captura de cada interface é salva como um arquivo separado usando a convenção de nomenclatura: tcpdump/{interface_name}_capture.pcap (como en0_capture.pcap, eth0_capture.pcap). Um arquivo de manifesto de metadados (tcpdump/packet_capture_manifest.txt) também é gerado, registrando a plataforma, a contagem de pacotes, a duração, as interfaces capturadas e o back-end de captura usado.

Configurações de ping

- Host(s) para ping — Insira os hosts para o ping (separados por vírgula). Exemplo:www.cisco.com

Configurações de acessibilidade de URL

- URLs a serem verificados — Insira os URLs a serem testados (separados por vírgula). Exemplo: `https://github.com`
    - Usa solicitações HTTP GET para testar a acessibilidade.
    - Portas padrão: 80 (HTTP) / 443 (HTTPS). Inclua a porta no URL para portas fora do padrão (como `ashttps://example.com:8443`).
    - Máximo de 20 URLs por verificação.
    - tempo limite: 30 segundos por URL.
    - Dados coletados por URL: URL, status de acessibilidade, código de status HTTP, tempo de resposta (ms), comprimento do conteúdo, endereço IP resolvido, versão TLS e carimbo de data/hora.
    - Os resultados são salvos em reachability/reachability_results.json e

reachability/reachability_summary.txt.

Configurações do Teste de Política

- URLs do host — Insira os hosts para teste de política (separados por vírgula, máximo de 10). Exemplo: www.cisco.com
- Os testes de política são executados no endpoint de teste de política da Cisco: policy.test.sse.cisco.com
- Os resultados incluem a saída do teste de política estruturada e os dados HAR capturados automaticamente durante a navegação de teste.

Configurações de Captura HAR

- URLs de destino — Insira URLs para a captura HAR (separados por vírgula). Exemplo: https://www.cisco.com/

Tip: Atualmente, a captura HAR suporta apenas o Google Chrome. A ferramenta usa o protocolo Chrome DevTools (via chromedp) para automatizar uma sessão Chrome sem cabeça e capturar o tráfego de rede. Verifique se o Google Chrome está instalado no sistema. O Firefox e o Safari não são compatíveis no momento.

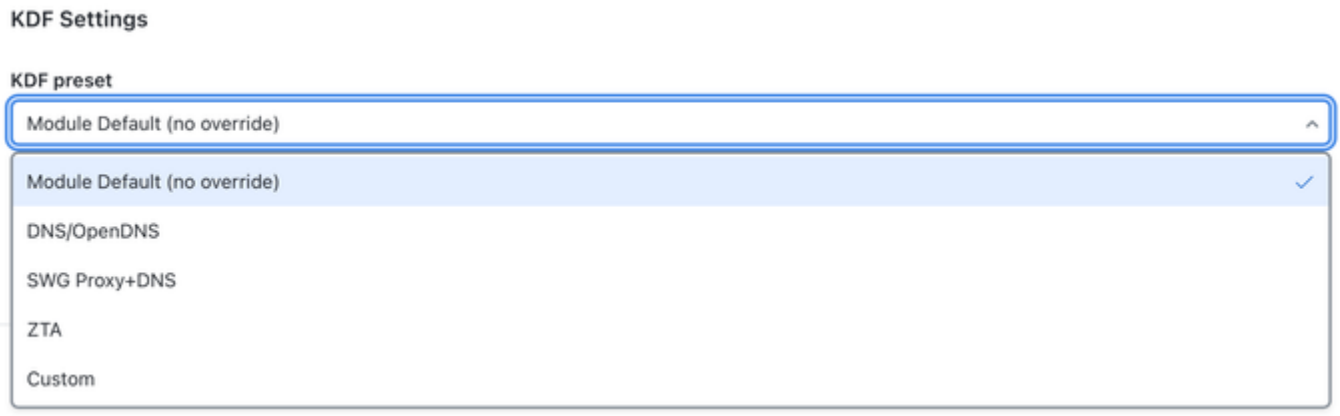
Configurações do KDF

Configure os sinalizadores de Função de Derivação de Chave usados durante a coleta de diagnóstico. Os sinalizadores KDF controlam quais categorias de depuração estão habilitadas no Cisco Secure Client:

- Predefinição de KDF — Selecione uma predefinição de Função de Derivação de Chaves.
- KDF HEX — O valor hexadecimal é preenchido automaticamente com base na predefinição selecionada. Quando "Personalizado" estiver selecionado, insira seu próprio valor hexadecimal.

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.



Configurações de IP Reservado

- URLs NSLookup — Hosts nslookup personalizados opcionais (separados por vírgula). Máximo de 10 URLs. Cada host personalizado é consultado sobre todos os resolvedores

configurados.

- URLs de rastreamento — Hosts traceroute/tracert personalizados opcionais (separados por vírgula). Máximo de 10 URLs. A ferramenta usa automaticamente traceroute no macOS/Linux e tracert no Windows.
- IPs do resolvedor — IPs do resolvedor personalizado opcionais para consultas de nslookup (separados por vírgula, como 208.67.222.
- 222, 208.67.220.220) Máximo de 5 IPs. Quando especificado, os resolvedores personalizados são usados além dos três resolvedores internos (DNS padrão do sistema, 127.0.0.1, 208.67.222.222).

Detalhes do IP Reservado

O diagnóstico de IP reservado coleta estes dados por padrão:

Destinos Traceroute/Tracert padrão (executar em todos eles automaticamente):

Destino	Propósito
208.67.222.222	Rota para o servidor de nome primário OpenDNS
208.67.220.220	Rota para o servidor de nomes secundário OpenDNS

146.112.255.50	Rota para IP de infraestrutura Cisco SWG
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	Rota para o nome de host do proxy SWG

- MacOS/Linux: Usa o comando traceroute
- Windows: Usa o comando tracert

Consultas NSLookup padrão (são executadas em todas elas automaticamente):

Cada destino de nslookup é consultado em relação a cada resolvedor na lista de resolvedores. Por padrão, a lista de resolvedores inclui três resolvedores internos:

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 IPs do resolvedor personalizados forem configurados (como 208.67.222.222), eles serão adicionados à lista de resolvedores e cada destino nslookup também será consultado em relação a eles.

Destinos de 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

Por exemplo, com os 3 resolvedores padrão, isso produz 6 consultas nslookup (2 destinos x 3 resolvedores). Adicionar um IP de resolvedor personalizado aumenta esse número para 8 consultas (2 destinos x 4 resolvedores).

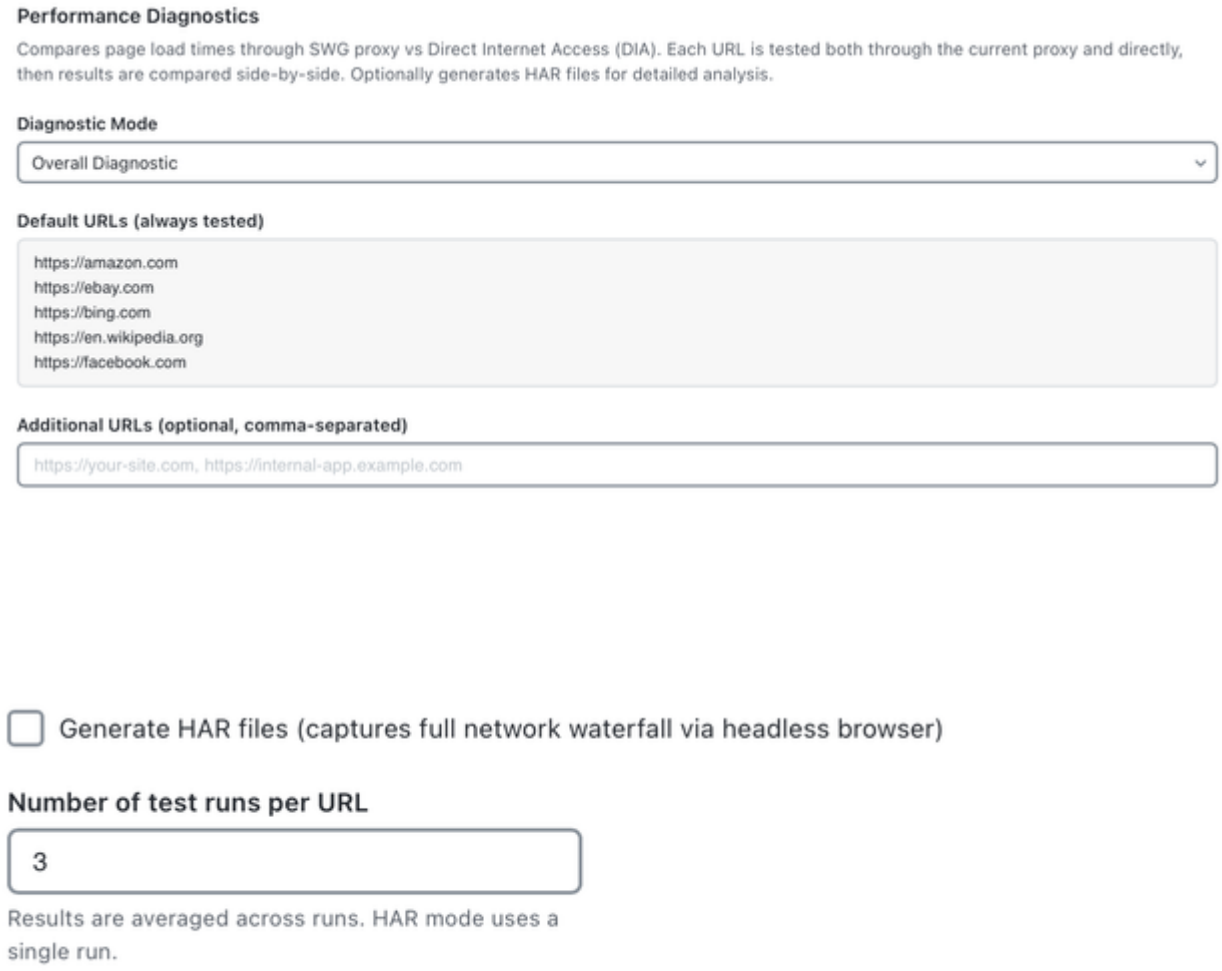
URLs NSLookup personalizadas fornecidas pelo usuário são consultadas na mesma lista de resolvedores completa (resolvedores internos + personalizados).

Todos os resultados são consolidados em um único arquivo: reserved_ip/reserved_ip_diagnostics.txt, agrupados por seção (traceroute, nslookup) com cabeçalhos legíveis, indicando o destino e o resolvedor de cada entrada.

Diagnóstico de desempenho

Compara os tempos de carregamento da página através do proxy SWG vs Direct Internet Access (DIA). Ele tem dois modos:

1 Modo de diagnóstico geral: cada URL é testado através do proxy atual e diretamente, e os resultados são comparados lado a lado. Opcionalmente, gera arquivos HAR para análise detalhada.



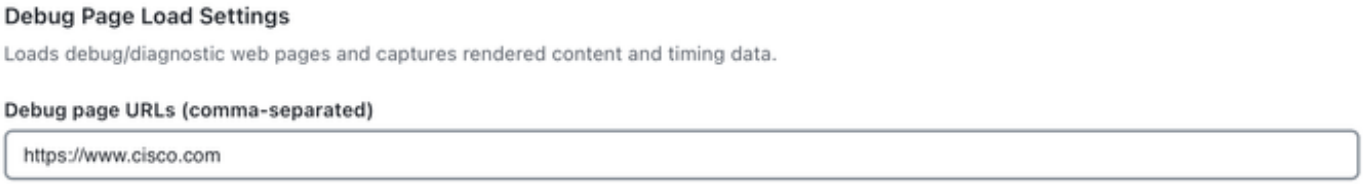
2 Um modo de diagnóstico de URL: Podemos inserir um URL específico para ser testado através do proxy atual e diretamente, e os resultados são comparados lado a lado. Opcionalmente, gera arquivos HAR para análise detalhada.

Configurações de Inventário do Repositório de Certificados

- Enumera certificados de repositórios de certificados configurados:
  - Sistema
  - Login
  - Root
  - E muito mais
- Identifica rapidamente certificados ausentes, expirados ou não confiáveis

Configurações de carregamento de página de depuração:

- Carrega URLs de depuração configuráveis.
- Capturas:
  - Cabeçalhos de resposta
  - Corpo da resposta
  - Informações de tempo
  - metadados SSL



Ações

1. Preencha ou ajuste as configurações para cada diagnóstico habilitado.
2. Clique em Start Diagnostics (Iniciar diagnósticos) para começar a execução do diagnóstico.
3. Clique em Back para voltar à Etapa 1 ou em Cancel para sair

Note: Os campos com erros de validação são realçados. Você deve corrigi-los antes de iniciar o diagnóstico.

Pausar e continuar

Quando você executa uma coleção de diagnósticos que inclui troubleshooting avançado (por exemplo, rastreamento de ZTNA ou SWG), a Ferramenta de Diagnóstico de Ponto de Extremidade Cisco pode pausar parcialmente a execução e pedir que você reproduza o problema antes de continuar.

Isso lhe dá tempo para acionar o problema enquanto o registro detalhado está ativado, para que a equipe de suporte receba mais dados de diagnóstico úteis.

- Quando a janela Diagnostics Paused for exibida, leia a mensagem: ela informa quais recursos de registro estão ativos agora.
- Reproduza o problema que você está solucionando. Por exemplo:
    - Reconectar à VPN
    - Abra o aplicativo interno que está falhando
    - Repita as etapas que causam o erro
- Quando terminar de reproduzir o problema, clique em Continuar

Deixe a corrida terminar. Em seguida, a ferramenta coleta arquivos, restaura as configurações normais e cria o arquivo de diagnóstico.

NOTA:Não feche o aplicativo enquanto estiver em pausa. O registro permanece ativo até que você clique em Continuar e a execução seja concluída.

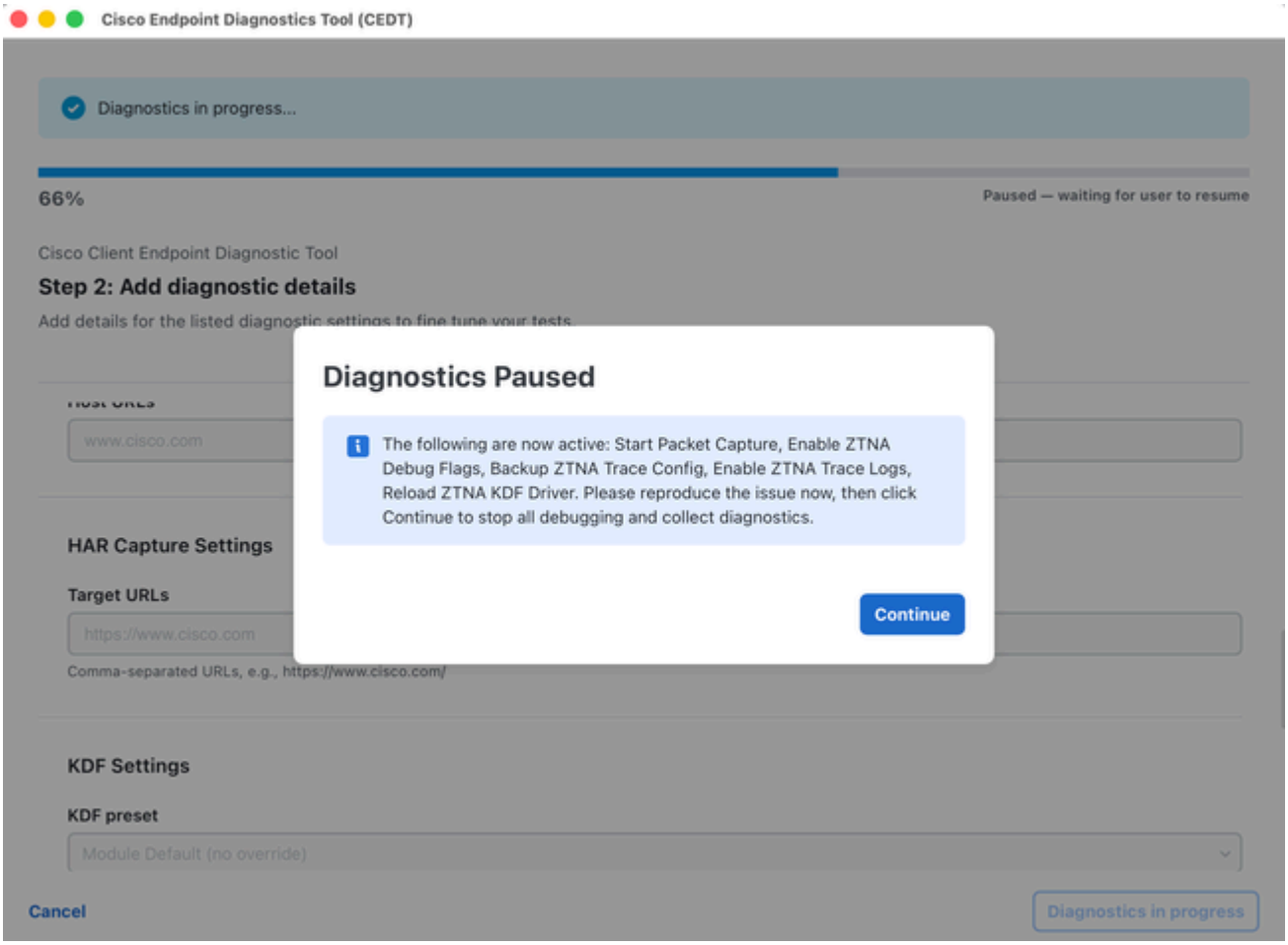
(Linha de comando)

Se você estiver executando a ferramenta a partir de um terminal, poderá ver uma mensagem de pausa na janela em vez de uma caixa de diálogo.

1. Leia a mensagem de pausa exibida no terminal.
2. Reproduza o problema.

3. Retorne ao terminal e pressione Enter para continuar.

4. Aguarde a conclusão da execução.



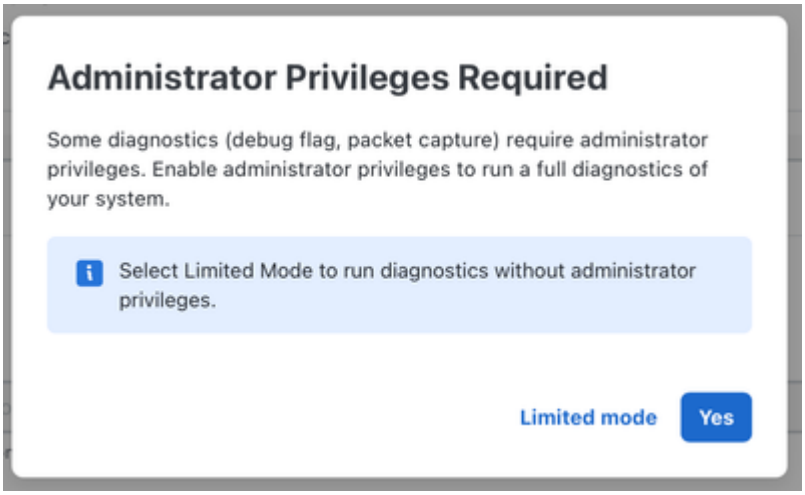
Prompt de privilégios de administrador

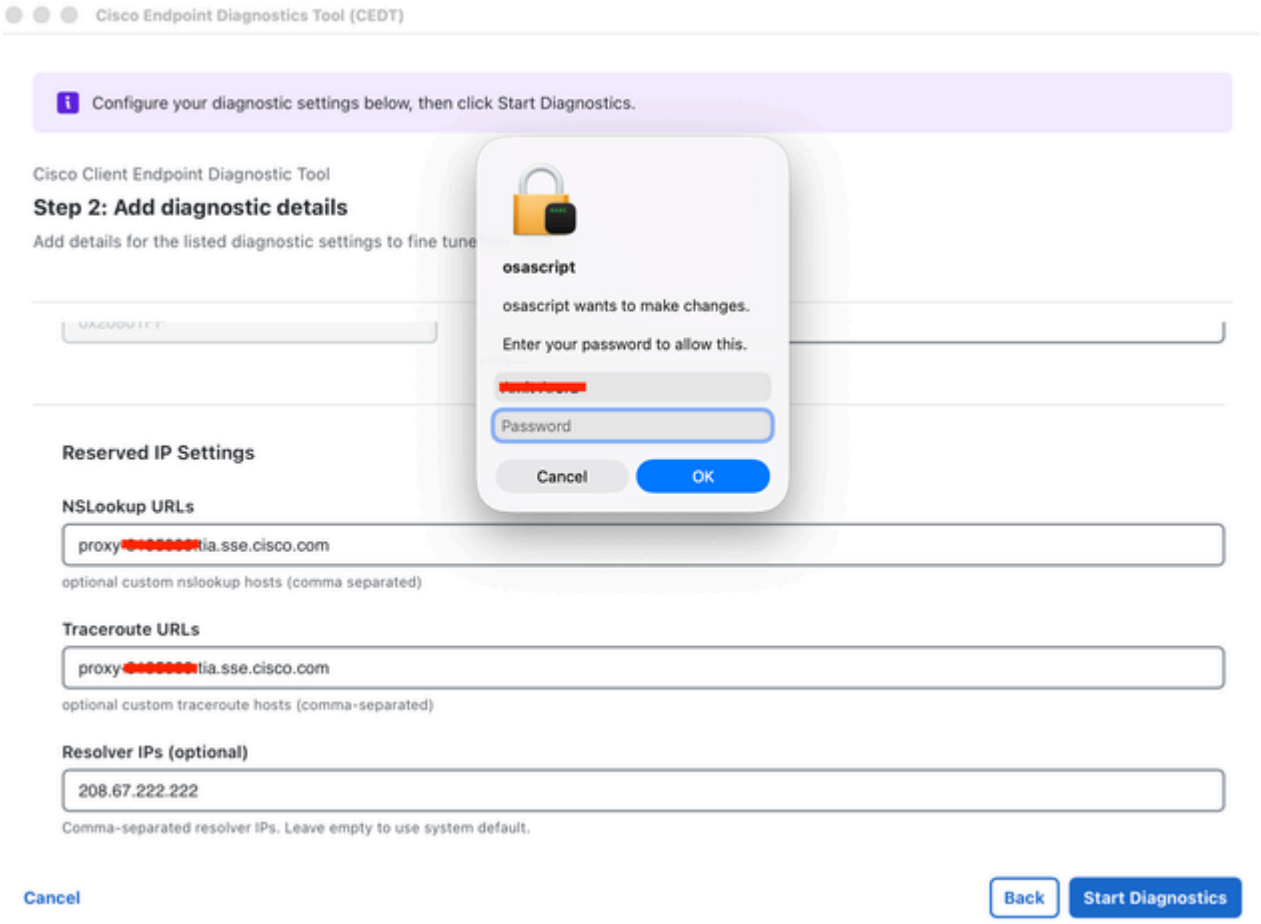
Depois de clicar em Iniciar diagnóstico, a ferramenta poderá solicitar privilégios de administrador se você tiver habilitado recursos que exigem acesso elevado (como Captura de pacotes ou Flags de depuração).

É exibida uma caixa de diálogo com o título Privilégios de administrador necessários:

- Clique em Sim para conceder privilégios de administrador. Isso aciona o prompt de credencial nativo do macOS/Windows.
- Clique em Modo limitado para continuar sem elevação. Tarefas privilegiadas (captura de pacotes, sinalizadores de depuração) são ignoradas.

- MacOS: Você pode ver o diálogo de senha padrão do macOS no osascript. Insira a senha do sistema e clique em OK.
- Windows: Um prompt de elevação UAC padrão é exibido. Clique em Yes para permitir.



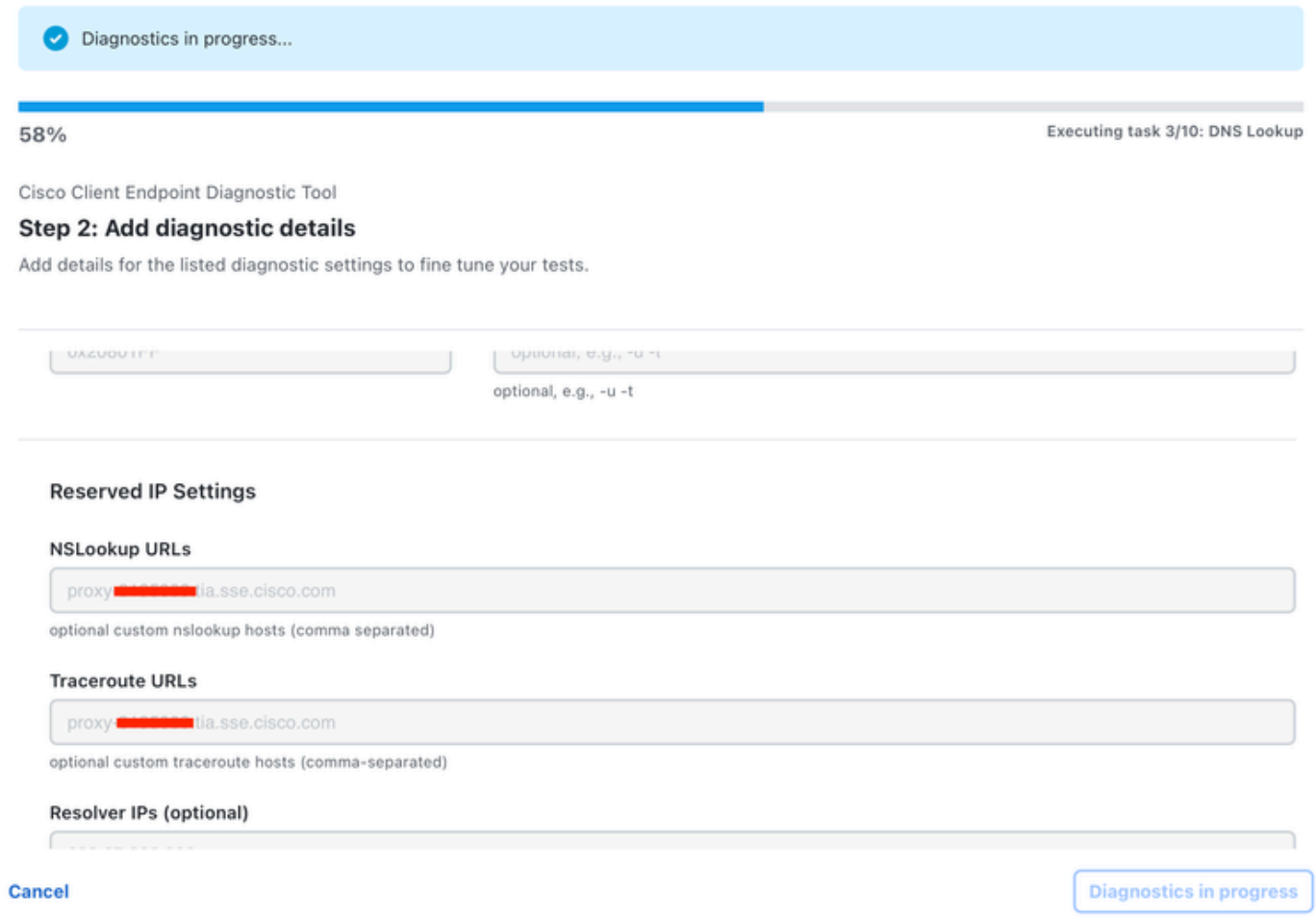


Diagnóstico em andamento

Uma vez iniciada, a ferramenta executa todas as tarefas de diagnóstico selecionadas:

- Uma barra de andamento mostra a conclusão geral (como 59% — Execução da tarefa 3/9: Pesquisa DNS).
- Um diagnóstico em andamento... banner é exibido na parte superior.
- Todos os campos de configuração ficam desativados/acinzentados durante a execução.
- O rodapé mostra um botão Diagnóstico em andamento (desativado) para indicar que a ferramenta está ocupada.

Aguarde a conclusão do diagnóstico. Não feche o aplicativo.



1.

Diagnóstico concluído — Carregar no TAC

Quando todos os diagnósticos terminarem, uma caixa de diálogo de conclusão será exibida:

Diagnóstico concluído. Faça upload do arquivo para um caso TAC.

A caixa de diálogo exibe:

- Arquivo — O nome do arquivo de diagnóstico gerado (como cisco_diagnostics.tar.gz).
- Tamanho do arquivo — O tamanho do arquivo (por exemplo, 7,72 MB).
- SHA256 — A soma de verificação do arquivo para verificação de integridade.

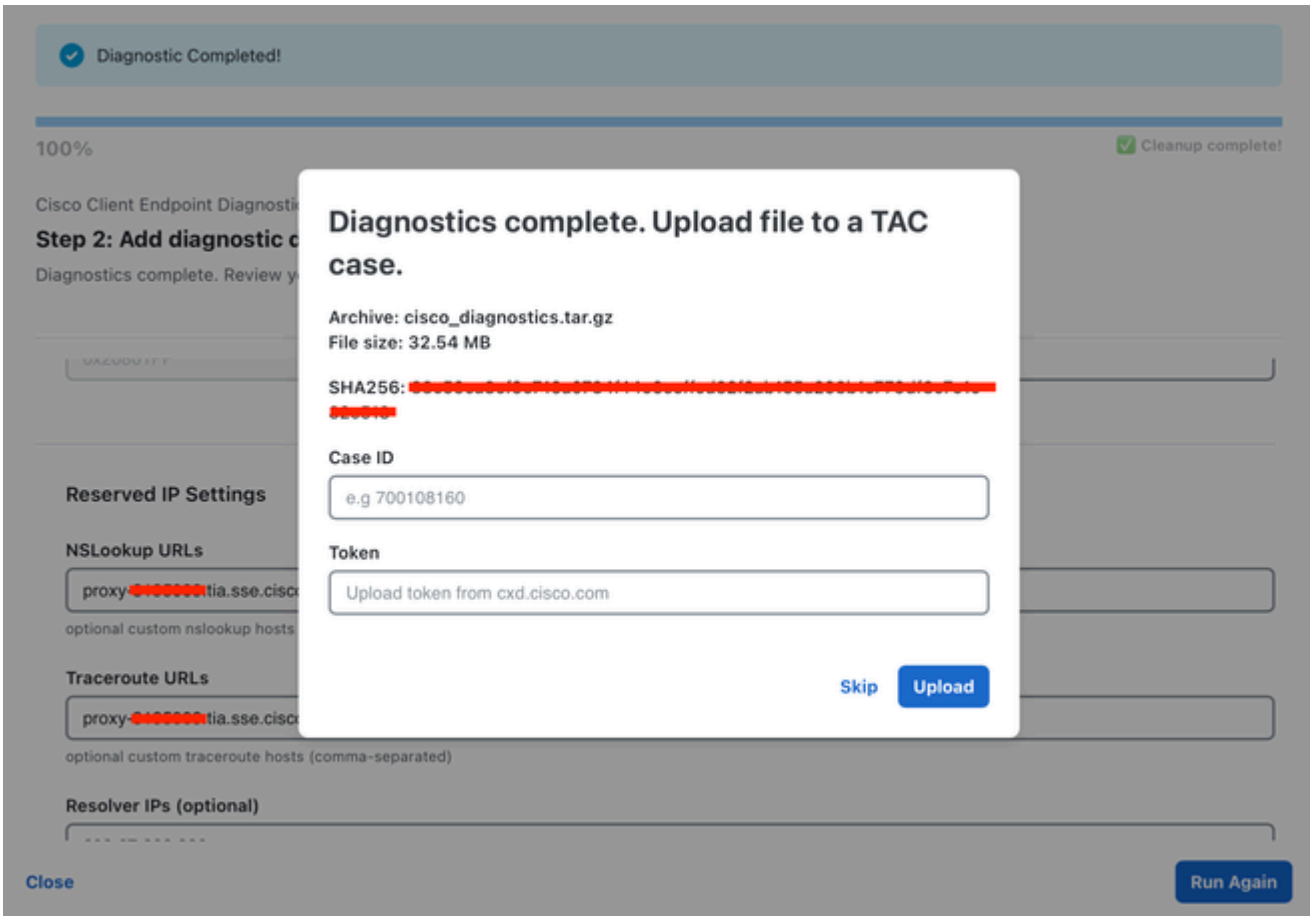
Para fazer upload em um caso de TAC:

1. Insira sua ID de caso (como698746730).
2. Insira seu token (fornecido pelo suporte da Cisco).
3. Clique em Open TAC Case para iniciar o upload.

Uma barra de progresso mostra o status do carregamento (como Carregando... 85,0% (6,56 MB / 7,72 MB).

Para ignorar o upload:

- Clique em Ignorar para fechar a caixa de diálogo sem carregar. O arquivo compactado ainda é salvo localmente.



Upload concluído — Tela final

Após um upload bem-sucedido, o banner de conclusão é atualizado para:

Arquivo de diagnóstico carregado com êxito no caso [Case ID]

A barra de progresso mostra 100% com o status Limpeza concluída.

Ações

- Clique em Run Again (Executar novamente) para iniciar uma nova execução de diagnóstico.
- Clique em Fechar para sair do aplicativo.

Local de saída

A saída do diagnóstico é salva em:

- MacOS: ~/Desktop/cisco_diagnostics/
- Windows: %PERFIL DE USUÁRIO%\Desktop\cisco_diagnostics\

O arquivo de saída (cisco_diagnostics.tar.gz) contém todos os dados de diagnóstico coletados em um formato estruturado.

Troubleshooting

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

P: Que dados essa ferramenta coleta?
R: A ferramenta coleta informações do sistema (SO, hardware, configuração de rede), registros de aplicativos, configuração de produtos da Cisco e dados de módulos instalados e dados de diagnóstico de rede relacionados apenas aos módulos do Cisco Secure Access. Consulte a seção What System Data is Collected (Quais dados do sistema são coletados) para obter detalhes.

Nenhum dado pessoal é capturado.

P: Preciso de acesso de administrador/raiz?
R: O acesso de administrador é opcional, mas recomendado. Sem isso, alguns diagnósticos (captura de pacotes, sinalizadores de depuração) são ignorados. A ferramenta solicita e permite que você escolha.

P: Posso executar a ferramenta várias vezes?
R: Yes. Após a conclusão de cada execução, você pode clicar em "Executar novamente" para iniciar uma nova sessão de diagnóstico.

P: Onde a saída é salva?
R: O arquivo de diagnóstico é salvo em seu Desktop na pasta cisco_diagnostics.

P: E se eu não tiver uma ID de caso do TAC?
R: Você pode clicar em "Ignorar" na caixa de diálogo de upload. O arquivo compactado ainda é salvo localmente. Você pode carregá-lo manualmente em um caso TAC posteriormente ou compartilhá-lo com seu engenheiro de suporte.

P: Os dados estão criptografados?
R: O arquivo de diagnóstico é compactado (tar.gz) e os dados confidenciais são automaticamente editados antes do empacotamento.

P: Quais navegadores são compatíveis com a captura HAR?
R: A captura HAR atualmente suporta apenas o Google Chrome. A ferramenta usa o protocolo Chrome DevTools para a automação do navegador sem cabeça. Certifique-se de que o Chrome esteja instalado antes de executar a captura HAR.

P A tela de pausa nunca foi exibida. Há algo errado?

R: Não necessariamente. A etapa de pausa aparece somente quando o log detalhado foi habilitado com êxito para seu cenário. Verifique o log de execução no aplicativo — se as etapas de habilitação tiverem sido ignoradas, a ferramenta continuará sem pausar.

Q A corrida parece travada. O que devo fazer?

R: Procure a janela Diagnostics Paused — ela pode estar atrás de outras janelas. A execução não avança até que você clique em Continuar (ou pressione Enter na linha de comando).

P A mensagem lista recursos que eu não esperava. Isso é normal?

R: Yes. A mensagem mostra os recursos de registro ativados pela ferramenta para sua plataforma e as opções de diagnóstico selecionadas.

P Fechei o aplicativo durante a pausa. E agora?

R: Execute a coleta de diagnóstico novamente e deixe-a terminar. Se você não tiver certeza se o registro foi mantido ativado, entre em contato com o engenheiro de suporte para obter orientação.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.