了解终端诊断工具(CEDT)

目录

简介

本文档介绍用于从系统收集诊断数据并将其上传到Cisco TAC支持案例的CEDT。

先决条件

该工具可用于MacOS和Windows。请下载该工具。

Cisco 建议您了解以下主题：

- macOS：双击Cisco Endpoint Diagnostics Tool(CEDT)。app启动。
- Windows 窗口版本:双击CEDT.exe启动。
- 有效的 Internet 连接.
- 思科TAC案例ID和令牌（仅在您想要直接上传结果时需要）。

收集的系统数据

该工具按类别收集此系统数据。不会捕获任何类型的个人数据。

一般系统信息

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

网络配置

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`

产品信息

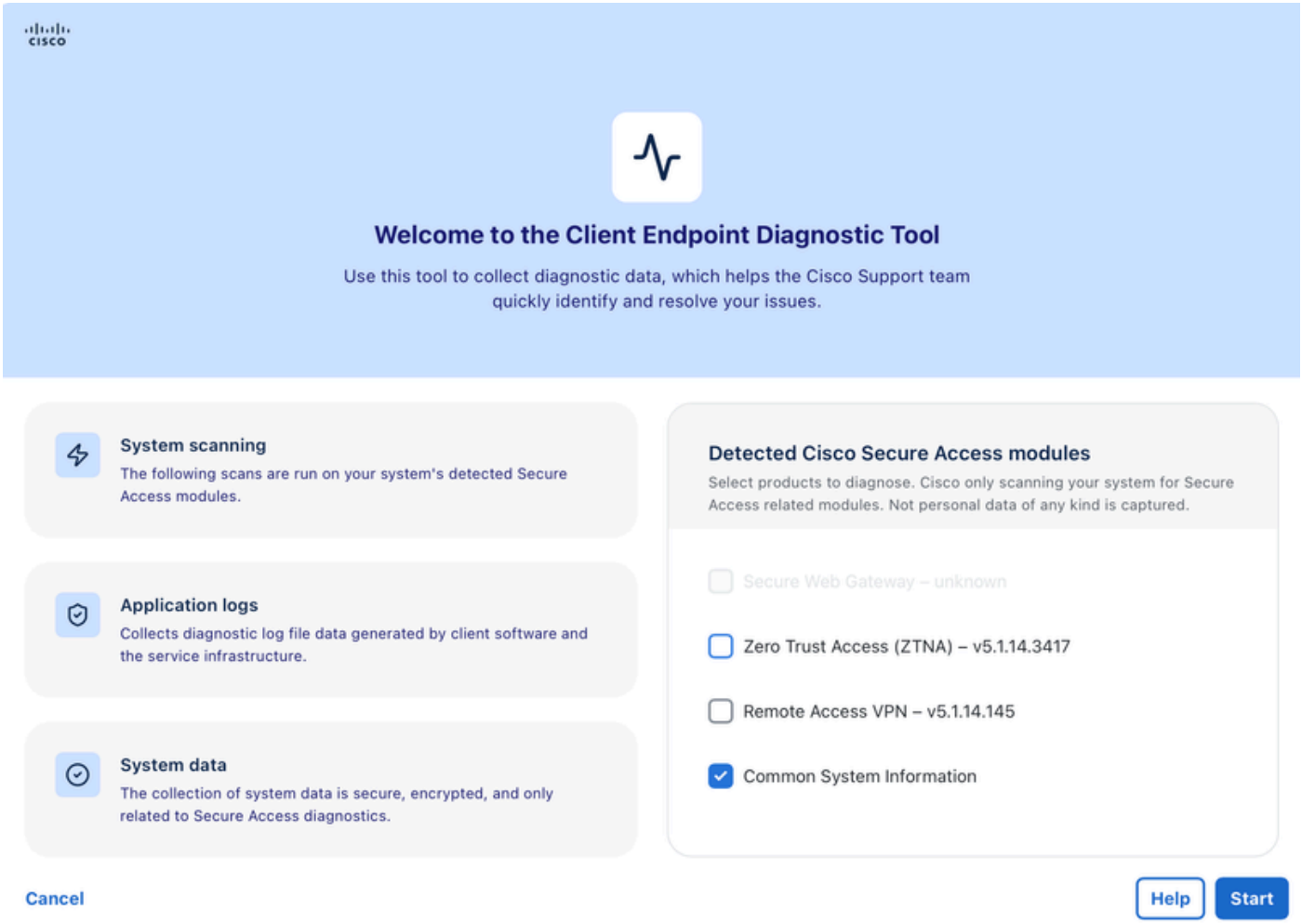
Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco.*`	Registry exports (`HKLM\SOFTWARE\Cisco`, `HKCU\SOFTWARE\Cisco`, `acsock` service)
Installation directories	`ls -laR /opt/cisco`	`%ProgramFiles%\Cisco`, `%ProgramFiles(x86)%\Cisco`, `%ProgramData%\Cisco`
Running Cisco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

逐步演练

欢迎屏幕

启动CEDT时，会显示“欢迎”屏幕。它概述了该工具的作用：

- 系统扫描 — 扫描您的系统，查找检测到的思科安全访问模块。
- 应用日志 — 收集由客户端软件和服务基础结构生成的诊断日志文件数据。
- 系统数据 — 系统数据的收集是安全的、加密的，并且仅与安全访问诊断相关。



在右侧，该工具会自动检测系统中安装的任何思科安全访问模块。您可以看到每个检测到的模块的

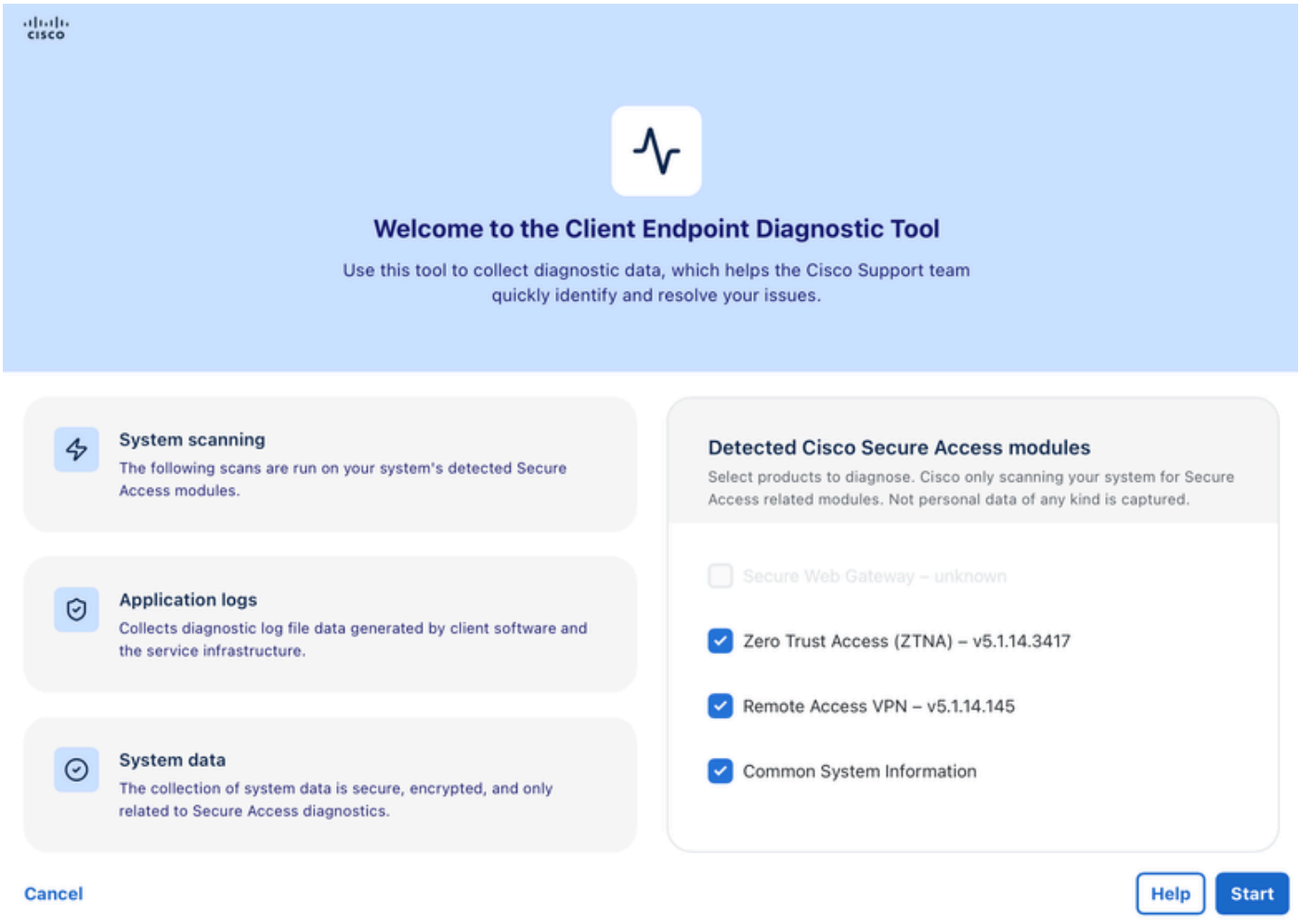
复选框及其版本号：

- 零信任访问(ZTNA)
- 安全Web网关(SWG)
- 远程访问VPN(RAVPN)
- 通用系统信息（始终可用）

操作

1. 选择或取消选择您要诊断的产品。
2. 单击让我们开始以继续，或单击帮助以获取详细信息。

注意：此工具仅收集与Secure Access相关的模块的数据。不会捕获任何类型的个人数据。



步骤 1：诊断数据收集

此屏幕允许您选择要包括的诊断测试和数据收集模块。

网络诊断

选择要运行的连接测试：

- DNS查找 — 对指定主机执行DNS解析测试。支持用于目标查找的自定义解析器IP。所有结果都合并到一个输出文件(dns/dns_lookups.txt)中，带有结构化的小节分隔符。
- 数据包捕获 — 捕获指定持续时间的网络数据包（需要管理员权限）。
- Ping主机 — 对指定主机执行ping操作以检查连通性。
- 策略测试输出 — 使用思科策略测试终端(policy.test.sse.cisco.com)针对指定URL测试策略实施。 支持多个逗号分隔的主机（最多10台）。 结果包括在策略测试导航过程中自动捕获的HAR数据。
- 网络速度测试 — 根据思科速度测试终端(speed.test.sse.cisco.com)测量上传/下载速度和延迟。 收集下载速度（6个并行流）、上传速度（3个并行流）和ping延迟/抖动（10个ICMP示例）。 结果以JSON和文本摘要格式保存。
- URL可达性 — 检查使用HTTP GET请求是否可以访问指定的URL。默认支持HTTP（端口80）和HTTPS（端口443）。可以在URL中指定非标准端口(例如 https://example.com:8443)。 每次检查最多20个URL，每个URL超时为30秒。按URL收集的数据包括：URL、可达性状态、HTTP状态代码、响应时间(ms)、内容长度、解析的IP地址、TLS版本和时间戳。结果保存到reachability/reachability_results.json和reachability/reachability_summary.txt。

数据收集

选择模块以收集性能和连接数据：

- HAR捕获 — 记录来自浏览器会话的HTTP存档(HAR)数据。目前仅支持Google Chrome（通

过无头浏览器自动化使用Chrome DevTools协议）。 该工具会自动检测系统上的Chrome安装。目前不支持Firefox和Safari。HAR输出遵循HAR 1.2规范，包括完整的网络跟踪（包括JS触发的XHR/fetch调用）。

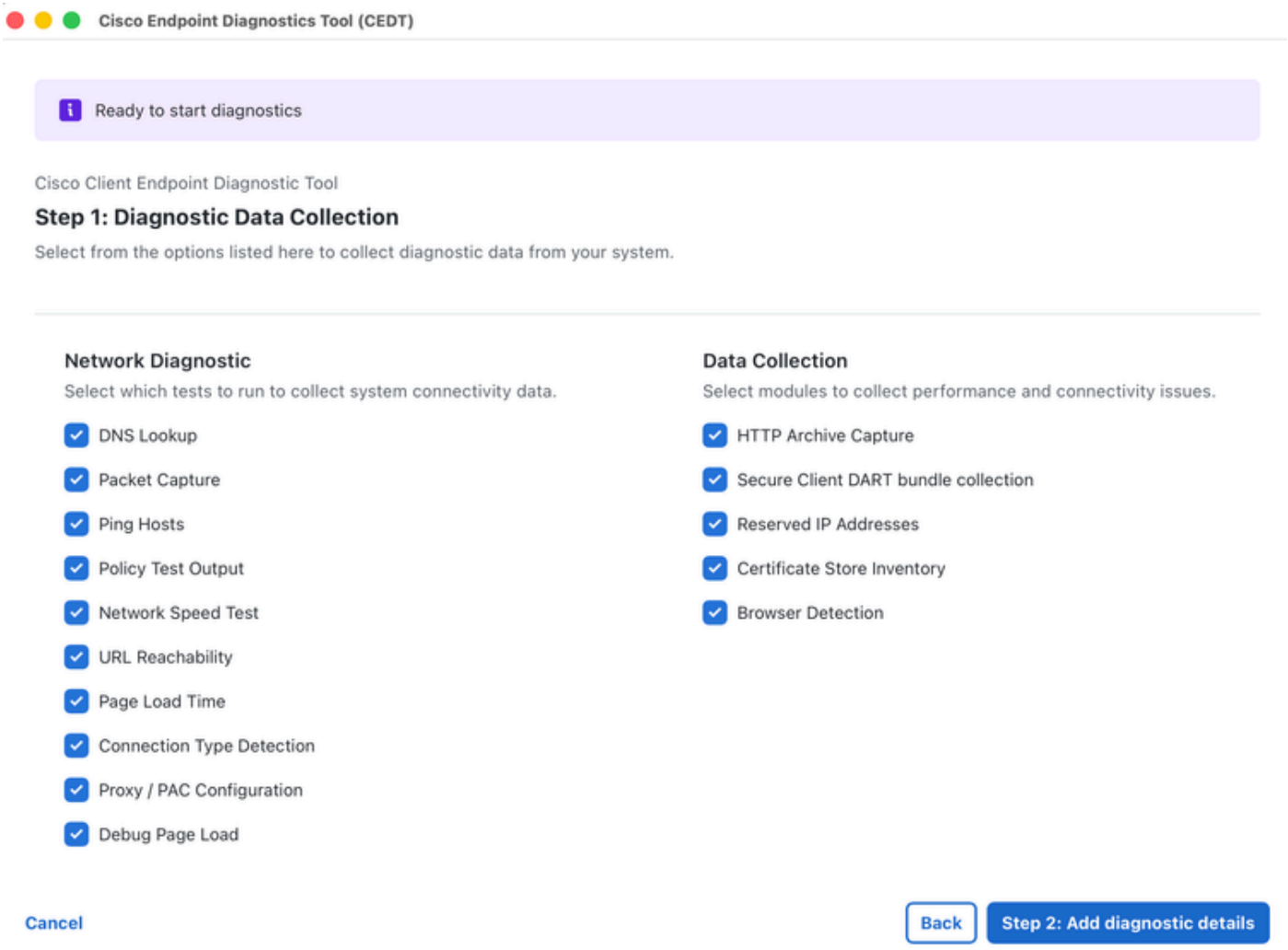
- DART捆绑包集合 — 从Cisco安全客户端收集DART诊断捆绑包。这包括所有模块日志，包括零信任访问(ZTA)日志(例如Windows上的flowlog.db，位于C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\)。
- 保留的IP — 运行保留的IP诊断检查。请参见下一部分，了解收集的诊断的完整列表。

调试

- 启用调试标志(Enable Debug Flags) — 收集终端活动的详细日志以诊断终端问题。仅当检测到并选择了至少一个Cisco Secure Access产品时，此选项才可用。

平台特定

- DebugView Capture(Windows) — 在Windows安全终端连接器上启用调试日志记录。此选项仅在Windows系统上可用。



操作

1. 选中或取消选中所需的诊断选项。
2. 点击步骤2:添加诊断详细信息以继续。
3. 单击Back返回到“欢迎”屏幕，或单击Cancel退出。

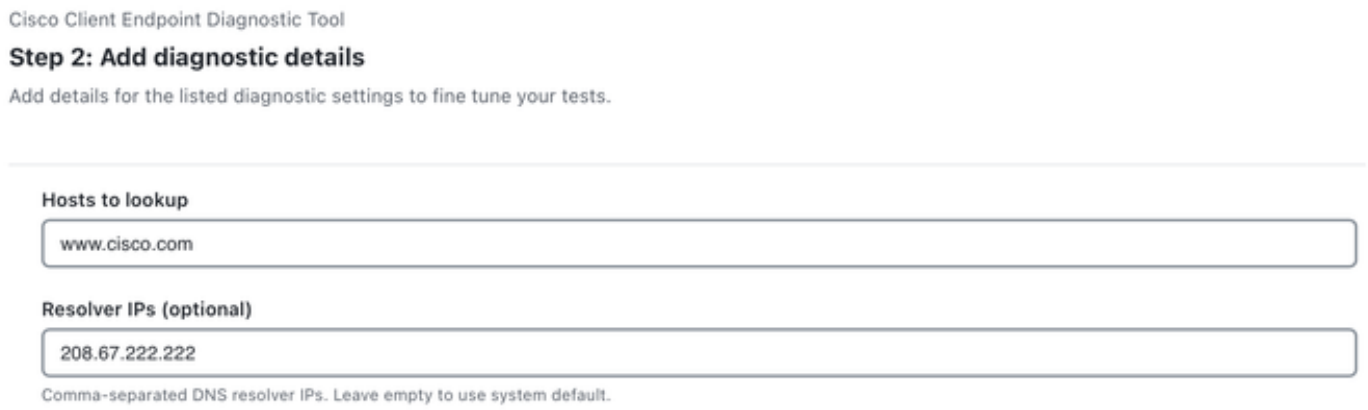
步骤 2：添加诊断详细信息

通过此屏幕，您可以为每个已启用的诊断测试配置特定参数。仅显示您在步骤1中启用的测试设置。

DNS查找设置

- 要查找的主机 — 输入一个或多个主机名（以逗号分隔）。 示例：cisco.com
- 解析器IP（可选） — 输入自定义DNS解析器IP（以逗号分隔）。 示例：208.67.222.222、208.67.220.220。保留为空以使用系统默认DNS解析器。指定后，会根据每个解析程序查询每台主机，从而提供不同DNS服务器之间的DNS解析结果比较。

所有DNS查找结果都整合到一个输出文件中：dns/dns_lookups.txt，每个主机/解析器组合使用结构化TextFSM部分分隔符。



数据包捕获设置

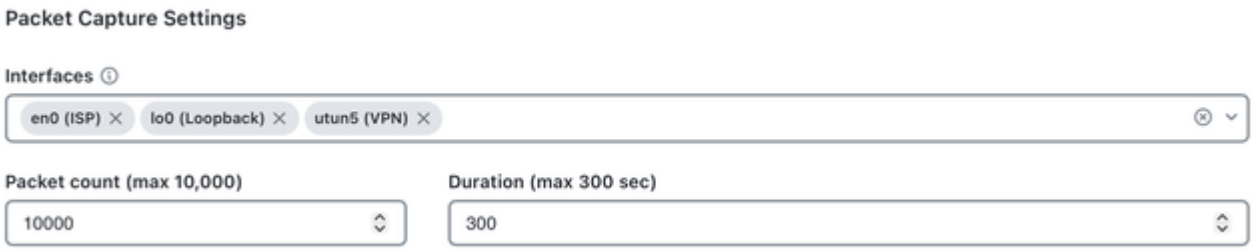
- 接口 — 选择要捕获的网络接口（或保留为所有）。
  - 当设置为All（自动模式）时：
    - macOS/Linux:该工具运行tcpdump -D以枚举所有可用接口，然后对处于Up and Running（不包括断开连接的接口）的接口进行过滤。 如果未找到活动接口，则会回退到特殊的any接口。所有匹配接口上并行运行的捕获。
    - Windows 窗口版本:使用所选捕获后端在所有NIC上进行捕获（请参阅下一节中的“工具”）。 当使用dumpcap并且未选择接口时，最多可同时捕获前3个检测到的接口。

- 数据包计数 — 每个接口要捕获的数据包数。默认:100.最大值：10,000.
- 持续时间（秒）— 捕获最长持续时间（秒）。默认:在macOS/Linux上为20秒，在Windows上为5秒。最大值：300 秒.当达到数据包计数或持续时间限制时（以先到者为准），捕获将停止。

按平台划分的数据包捕获工具

注意：(Windows):该工具会自动选择最佳可用捕获后端。首选pktmon（内置于Windows 10 v2004+），回退到dumpcap（如果安装了Wireshark），然后作为最后手段使用netsh trace。

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



数据包捕获输出文件

使用命名约定将每个接口的捕获保存为单独的文件：tcpdump/{interface_name}_capture.pcap（例如en0_capture.pcap、eth0_capture.pcap）。还会生成元数据清单文件 (tcpdump/packet_capture_manifest.txt)，记录使用的平台、数据包计数、持续时间、捕获的接口和

捕获后端。

Ping设置

- Host/s to ping — 输入要执行ping操作的主机（以逗号分隔）。 示例：www.cisco.com

URL可达性设置

- 要检查的URL — 输入要测试的URL（以逗号分隔）。 示例：https://github.com
  - 使用HTTP GET请求测试可达性。
  - 默认端口：80(HTTP)/443(HTTPS)。 将端口包含在非标准端口的URL中(例如ashttps://example.com:8443)。
  - 每次检查最多20个URL。
  - 超时：每个URL30秒。
  - 按URL收集的数据：URL、可达性状态、HTTP状态代码、响应时间(ms)、内容长度、解析的IP地址、TLS版本和时间戳。
  - 结果保存到reachability/reachability_results.json和reachability/reachability_summary.txt。

策略测试设置

- 主机URL — 输入用于策略测试的主机（逗号分隔，最多10个）。 示例：www.cisco.com

- 针对思科策略测试终端执行策略测试：policy.test.sse.cisco.com
- 结果包括结构化策略测试输出和测试导航过程中自动捕获的HAR数据。

HAR捕获设置

- 目标URL — 输入HAR捕获的URL（以逗号分隔）。 示例：https://www.cisco.com/

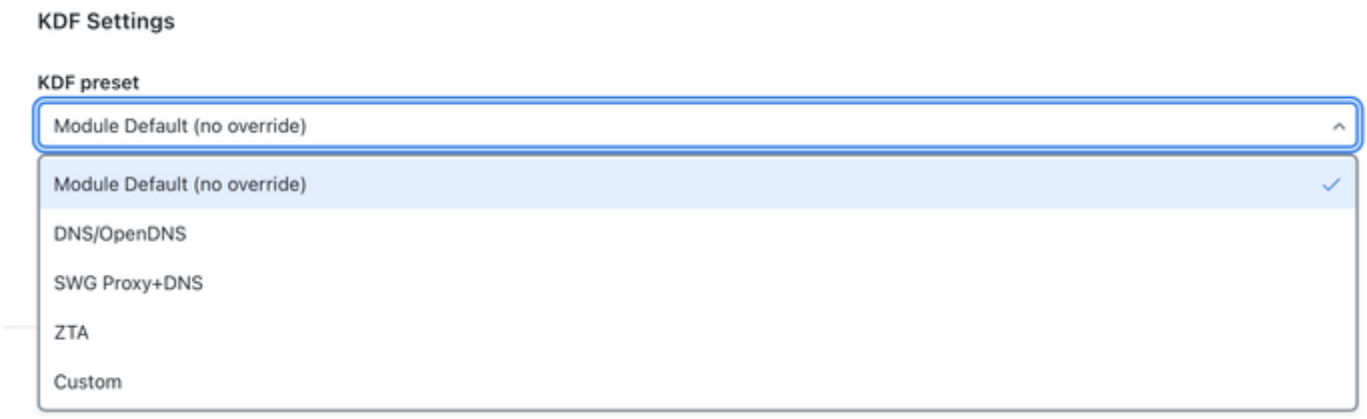
提示：HAR捕获当前仅支持Google Chrome。该工具使用Chrome DevTools协议（通过chromedp）自动执行无头Chrome会话并捕获网络流量。确保您的系统上已安装Google Chrome。目前不支持Firefox和Safari。

KDF设置

配置诊断收集过程中使用的密钥派生功能标志。KDF标记控制在Cisco安全客户端中启用了哪些调试类别：

- KDF预设 — 选择密钥派生函数预设。
- KDF HEX — 根据选定的预设自动填充十六进制值。选择“Custom”时，请输入您自己的十六进制值。

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.



保留的IP设置

- NSLookup URLs — 可选的自定义nslookup主机（以逗号分隔）。 最多10个URL。系统会根据所有已配置的解析程序查询每个自定义主机。
- 跟踪URL — 可选的自定义traceroute/tracert主机（以逗号分隔）。 最多10个URL。该工具在macOS/Linux上自动使用traceroute，在Windows上自动使用tracert。
- 解析器IP — 用于nslookup查询的可选自定义解析器IP（以逗号分隔，例如208.67.222）。
- 222、208.67.220.220)。 最多5个IP。指定后，除了使用三个内置解析器（系统默认DNS、127.0.0.1、208.67.222.222）外，还会使用自定义解析器。

保留的IP详细信息

默认情况下，保留IP诊断收集以下数据：

默认Traceroute/Tracert目标（自动针对所有这些目标运行）：

目标	目的
208.67.222.222	到OpenDNS主要名称服务器的路由
208.67.220.220	到OpenDNS辅助名称服务器的路由
146.112.255.50	路由到Cisco SWG基础设施IP
swg-url-proxy-https-sse.sigproxy.qq.op endns.com	路由到SWG代理主机名

- macOS/Linux:使用traceroute命令
- Windows 窗口版本:使用tracert命令

默认NSLookup查询（自动针对所有这些查询运行）：

根据解析程序列表中的每个解析程序查询每个nslookup目标。默认情况下，解析程序列表包括三个内置解析程序：

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

如果配置了自定义解析器IP（例如208.67.222.222），则会将这些解析器IP添加到解析器列表，并

且还会根据它们查询每个nslookup目标。

NSLookup目标：

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

例如，使用默认的3个解析器时，会产生6 nslookup查询（2个目标x 3个解析器）。 添加一个自定义解析器IP会将此问题增加为8个查询（2个目标x4个解析器）。

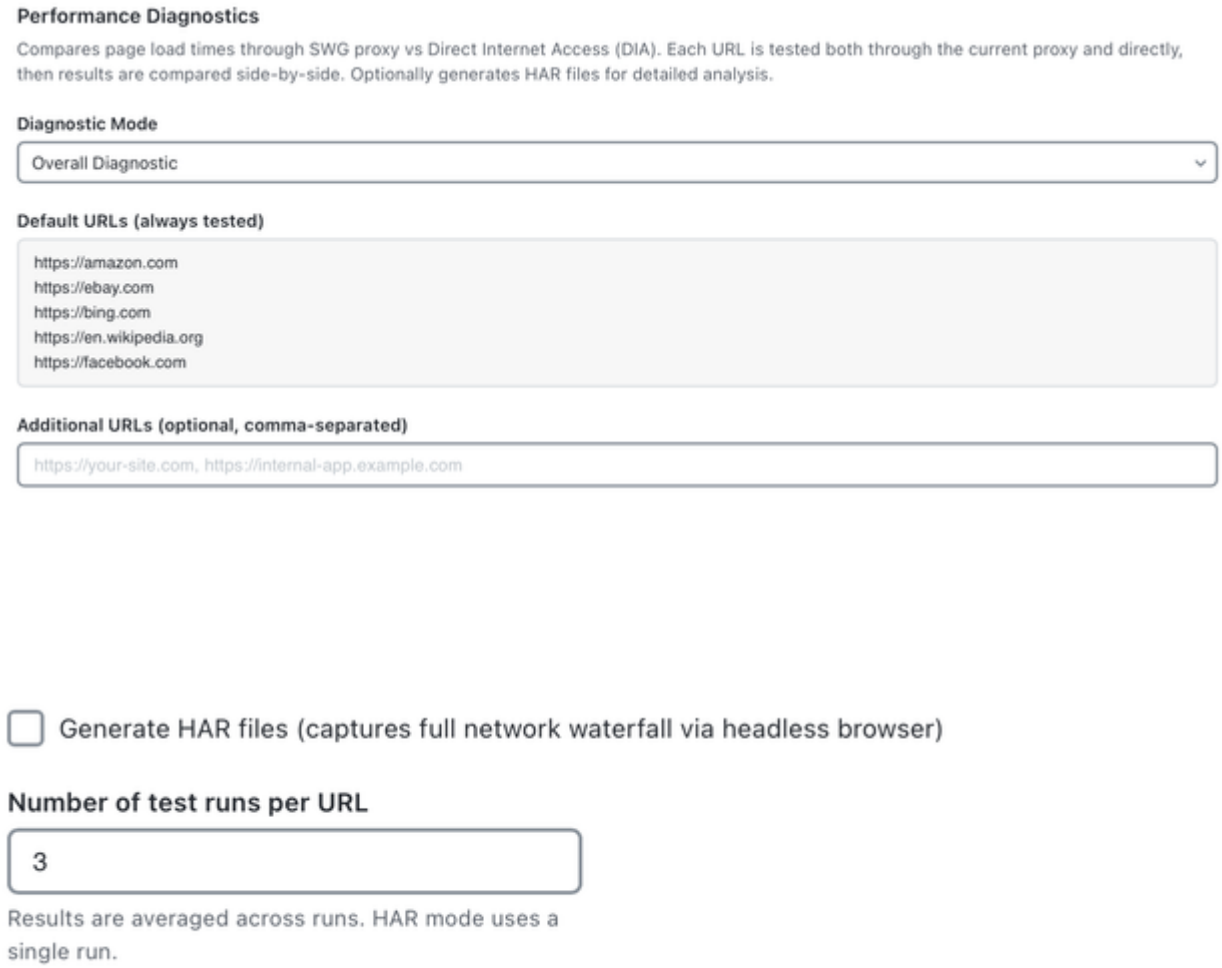
每个自定义用户提供的NSLookup URL都根据相同的完整解析程序列表（内置+自定义解析程序）进行查询。

所有结果都整合到一个文件中：reserved_ip/reserved_ip_diagnostics.txt，按节(traceroute、nslookup)分组，具有指示每个条目的目标和解析程序的可读报头。

性能诊断

比较通过SWG代理和直接互联网接入(DIA)的页面加载时间。它有两种模式：

1 总体诊断模式：通过当前代理和直接测试每个URL，然后并排比较结果。或者，生成用于详细分析的HAR文件。



2 一个URL诊断模式:我们可以通过当前代理和直接输入要测试的特定URL，然后并排比较结果。或者，生成用于详细分析的HAR文件。

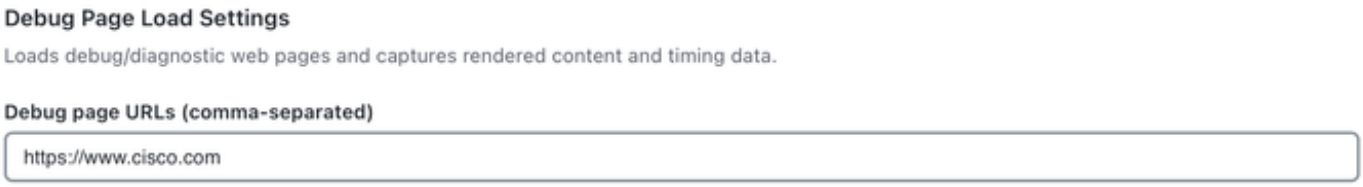
证书存储库存设置

- 枚举已配置的证书存储中的证书：

    - system
    - 登录
    - 根
    - 等等
- 快速识别缺失、过期或不受信任的证书

调试页加载设置：

- 加载可配置的调试URL。
- 捕获：
    - 响应报头
    - 响应正文
    - 计时信息
    - SSL元数据



操作

1. 填写或调整每个已启用的诊断的设置。
2. 单击Start Diagnostics开始诊断运行。
3. 单击Back返回步骤1，或单击Cancel退出

注意：带有验证错误的字段会突出显示。您必须先更正它们，然后才能开始诊断。

暂停并继续

当您运行包含高级故障排除的诊断集合(例如ZTNA或SWG跟踪)时，思科终端诊断工具可以在运行过程中暂停，并要求您在问题继续之前重现该问题。

这样，您就有时间在打开详细日志记录时触发问题，因此支持团队会收到更有用的诊断数据。

- 出现Diagnostics Paused窗口时，请阅读该消息 — 它告诉您哪些日志记录功能现在处于活动状态。
- 重现您正在解决的问题。例如：
    - 重新连接到VPN
    - 打开发生故障的内部应用程序
    - 重复导致错误的步骤
- 重现问题后，单击Continue

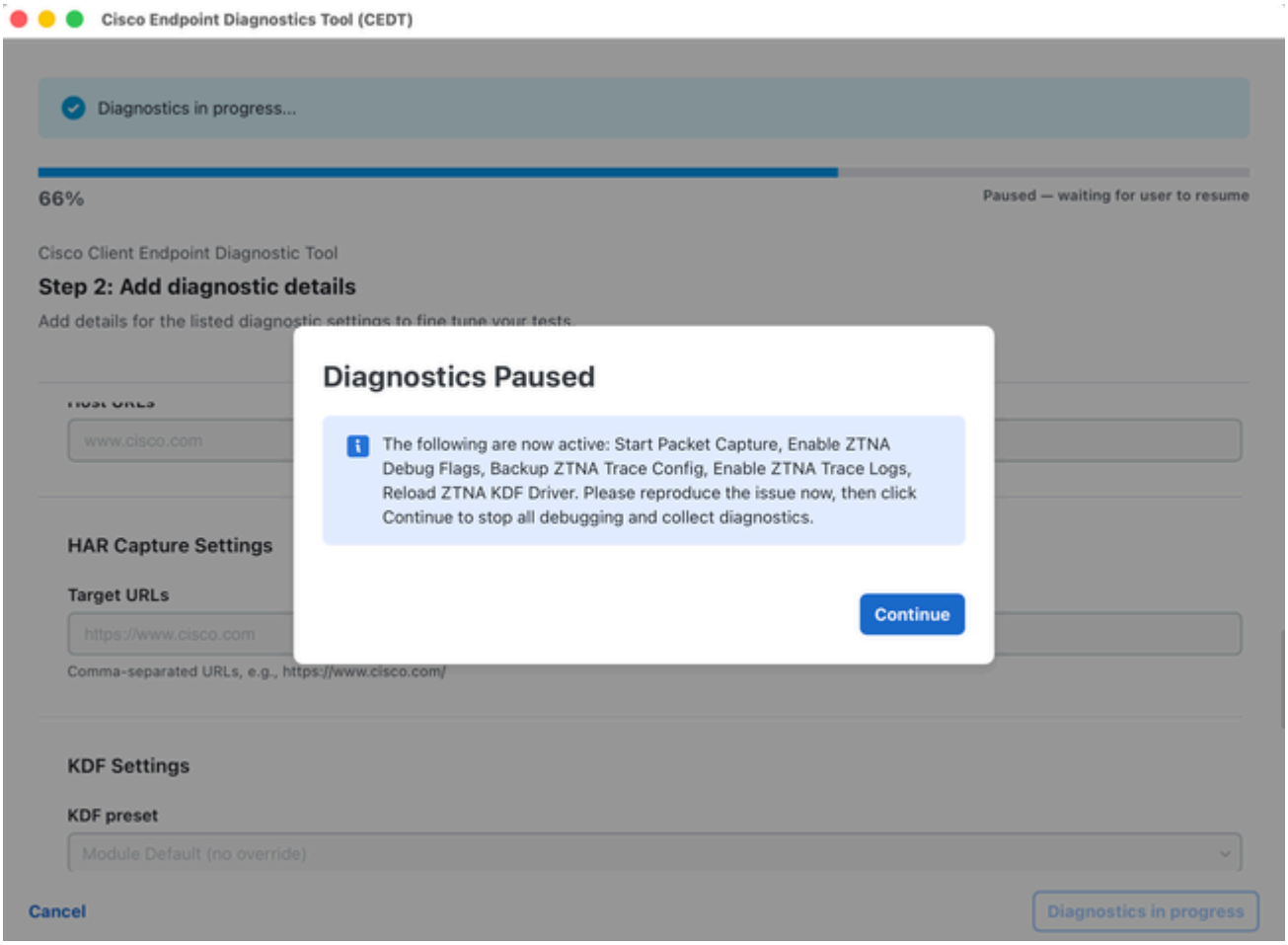
让跑完吧。然后，该工具会收集文件、恢复正常设置并创建诊断存档。

注意：暂停时不要关闭应用程序。日志记录将保持活动状态，直到您单击Continue并运行完成。

(命令行)

如果从终端运行该工具，则可以在窗口中看到暂停消息，而不是对话框。

1. 阅读终端中显示的暂停消息。
2. 重现问题.
3. 返回终端并按Enter键继续。
4. 等待运行完成。

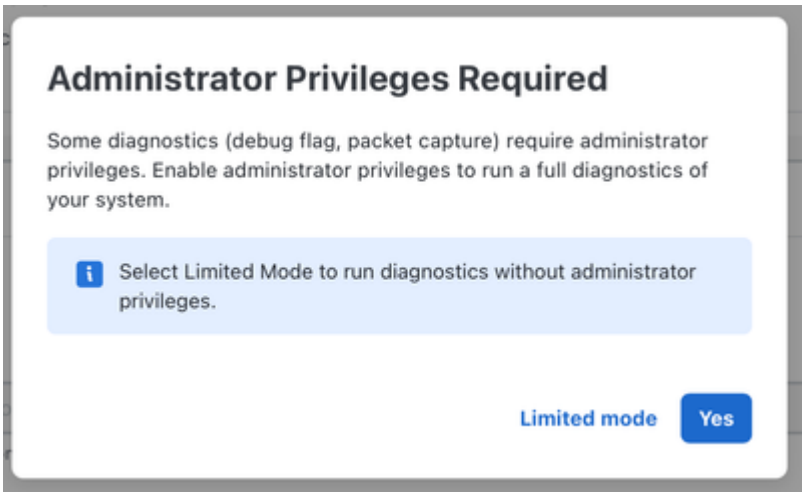


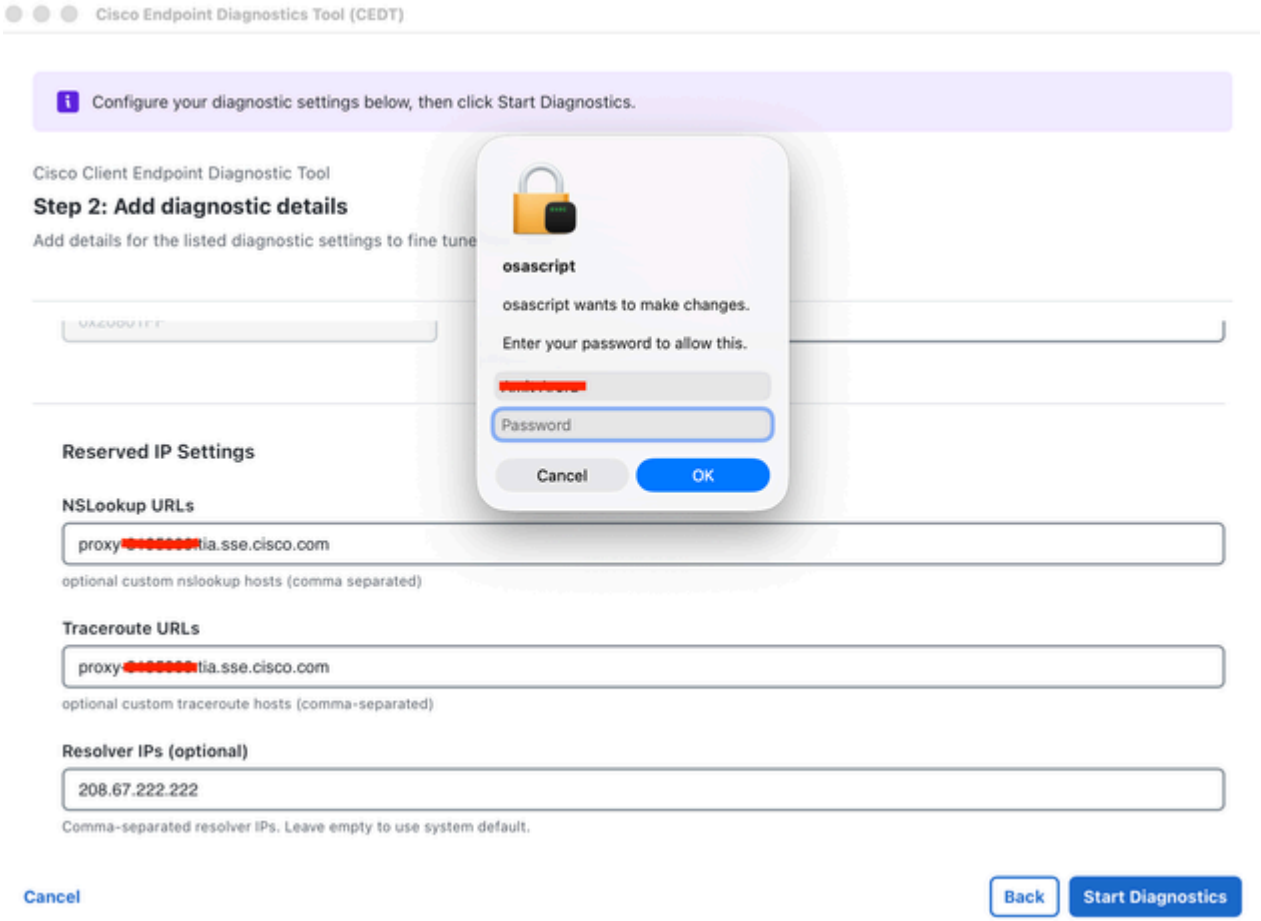
管理员权限提示

单击Start Diagnostics后，如果您启用了需要提升访问权限的功能（如数据包捕获或调试标志），则该工具可以提示您提供管理员权限。

系统将显示一个标题为Administrator Privileges Required的对话框：

- 单击Yes授予管理员权限。这将触发本地macOS/Windows凭证提示。
- 单击Limited mode以继续操作，不进行高程。已跳过特权任务（数据包捕获、调试标志）。
- macOS：您可以从osascript查看标准macOS密码对话框。输入系统密码，然后单击OK。
- Windows 窗口版本:出现标准UAC标高提示。单击Yes以允许。





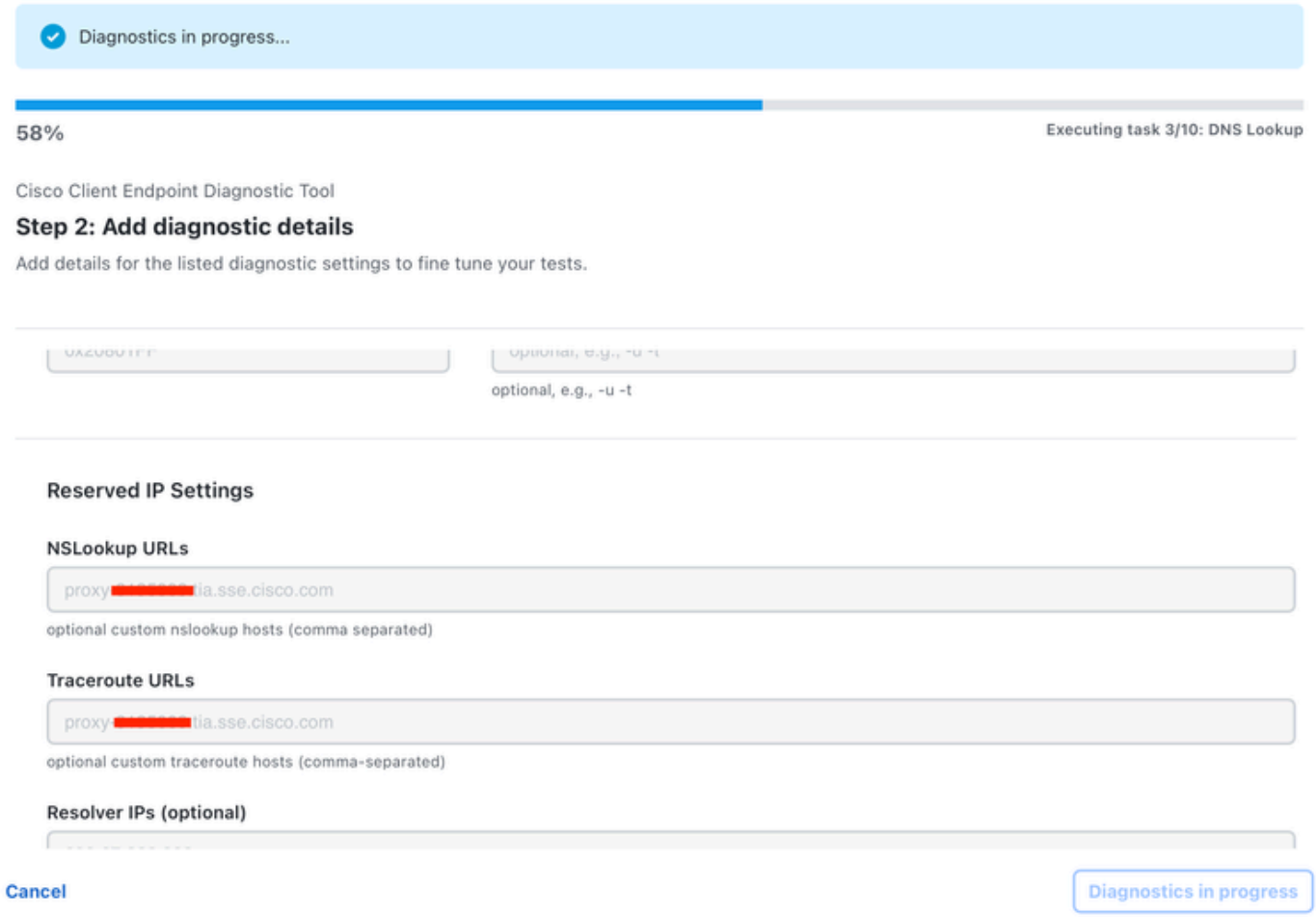
正在进行诊断

启动后，该工具将运行所有选定的诊断任务：

- 进度条显示整体完成情况(例如59% — 正在执行任务3/9:DNS查找)。

- 正在进行诊断..... 横幅显示在顶部。
- 在运行期间，所有设置字段均被禁用/灰显。
- 页脚显示Diagnostics in progress按钮（禁用），表示工具正忙。

诊断正在完成，请稍候。请勿关闭应用程序。



1.

诊断完成 — 上传到TAC

完成所有诊断后，将出现一个完成对话框：

诊断完成。将文件上传到TAC案例。

对话框显示：

- 存档 — 生成的诊断存档的文件名（例如cisco_diagnostics.tar.gz）。
- 文件大小 — 存档大小（例如7.72 MB）。
- SHA256 — 用于完整性验证的归档文件的校验和。

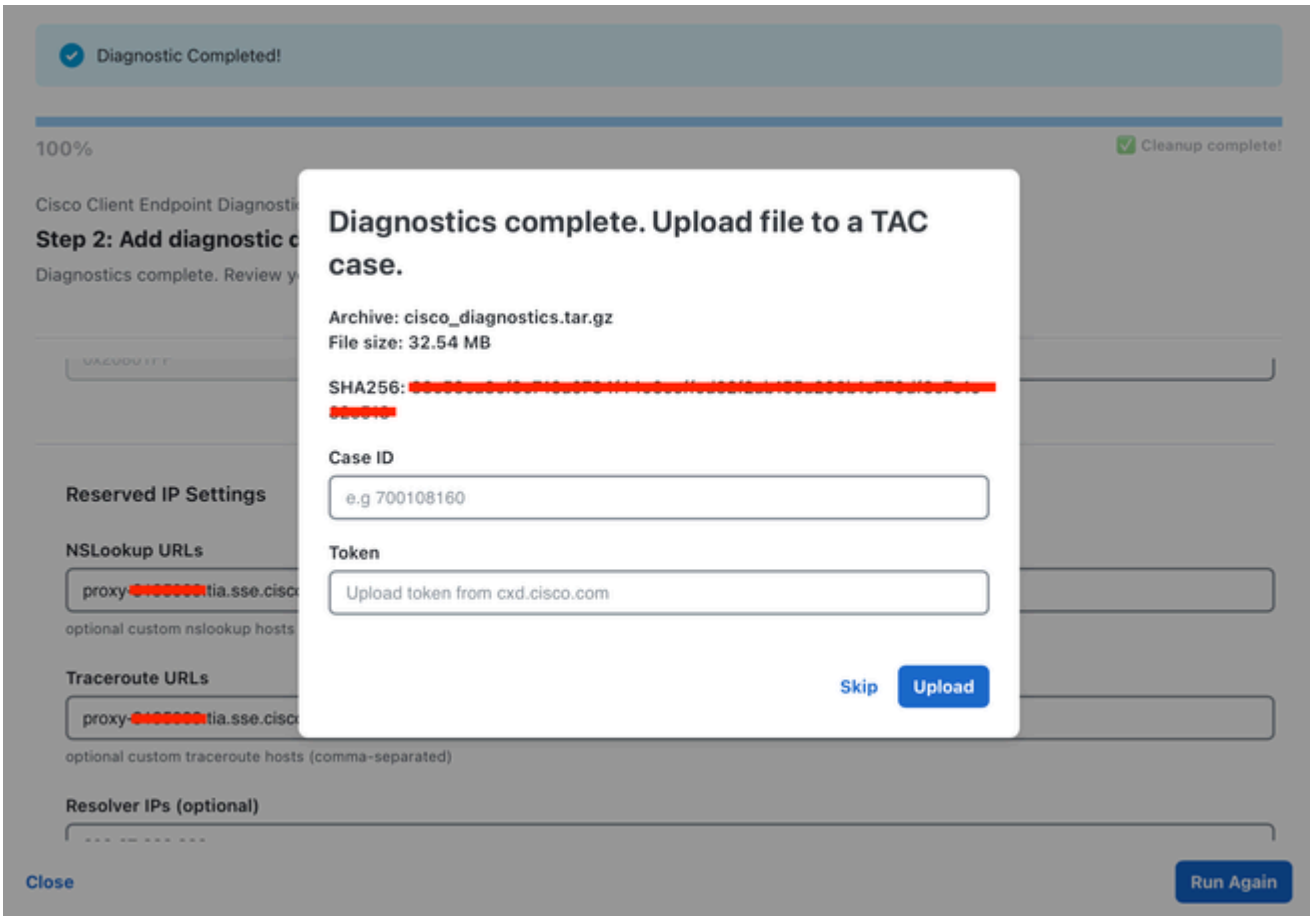
要上传到TAC案例，请执行以下操作：

1. 输入Case ID(例如698746730)。
2. 输入您的令牌（由思科支持提供）。
3. 单击Open TAC Case开始上传。

进度条显示上传状态(例如上传……85.0%(6.56 MB / 7.72 MB)。

要跳过上传，请执行以下操作：

- 单击Skip关闭对话框而不上传。存档文件仍保存在本地。



上传完成 — 最终屏幕

成功上传后，完成横幅将更新为：

诊断存档已成功上载到案例[案例ID]

进度条显示100%且状态为清除完成。

操作

- 单击Run Again开始新的诊断运行。
- 单击Close退出应用程序。

输出位置

诊断输出保存到：

- macOS：~/Desktop/cisco_diagnostics/
- Windows 窗口版本:%USERPROFILE%\Desktop\cisco_diagnostics\

输出存档文件(cisco_diagnostics.tar.gz)以结构化格式包含所有收集的诊断数据。

故障排除

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.

常见问题

问:此工具收集哪些数据？
A：此工具仅收集系统信息（操作系统、硬件、网络配置）、应用日志、思科产品配置和安装的模块数据，以及与思科安全访问模块相关的网络诊断数据。有关详细的细分，请参阅上一节中的收集了哪些系统数据。不会捕获任何个人数据。

问:是否需要管理员/根访问权限？

A：管理员访问权限是可选的，但建议使用。如果没有它，将跳过某些诊断（数据包捕获、调试标志）。该工具会提示您并允许您选择。

问:我可以多次运行该工具吗？
A：Yes.每次运行完成后，您可以点击“再次运行”以启动新的诊断会话。

问:输出保存在哪里？
A：诊断存档保存到cisco_diagnostics文件夹下的Desktop（桌面）。

问:如果没有TAC案例ID怎么办？
A：您可以在上传对话框中点击“跳过”。存档文件仍保存在本地。您可以稍后手动将其上传到TAC案例或与支持工程师共享。

问:数据是否加密？
A：诊断存档文件被压缩(tar.gz)，并且敏感数据在打包前自动被编辑。

问:HAR捕获支持哪些浏览器？
A：HAR捕获目前仅支持Google Chrome。该工具使用Chrome DevTools协议实现无头浏览器自动化。在运行HAR捕获之前，确保已安装Chrome。

Q暂停屏幕从未出现。出什么事了吗？

A：不必要。仅当为方案成功启用详细日志记录时，才会显示暂停步骤。检查应用中的运行日志 — 如果跳过启用步骤，工具将继续运行，而不会暂停。

问：这似乎是个难题。我该怎么办？

A：查找Diagnostics Paused窗口 — 该窗口可以位于其他窗口之后。只有单击Continue(或按命令行中的Enter)后，运行才会继续。

问：此消息列出了我不期望的功能。这是正常的吗？

A：Yes.该消息将显示该工具为您的平台启用的任何日志记录功能以及您选择的诊断选项。

问：我在暂停期间关闭了应用。现在怎么办？

A：再次运行诊断集合，然后让它完成。如果您不确定日志记录是否处于打开状态，请联系您的支持工程师以获取指导。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。