Información sobre Endpoint Diagnostics Tool (CEDT)

Contenido

Introducción

Este documento describe el CEDT para recopilar datos de diagnóstico de su sistema y cargarlos en un caso de soporte del TAC de Cisco.

Prerequisites

La herramienta está disponible para MacOS y Windows. Descargue la herramienta.

Cisco recomienda que tenga conocimiento sobre estos temas:

- MacOS: Haga doble clic en Cisco Endpoint Diagnostics Tool (CEDT).app para iniciar.
- Windows: Haga doble clic en CEDT.exe para iniciar.
- Una conexión a Internet activa.
- Un ID de caso y un token del TAC de Cisco (necesario solo si desea cargar los resultados directamente).

Datos del sistema recopilados

La herramienta recopila estos datos del sistema, organizados por categoría. No se capturan datos personales de ningún tipo.

Información general del 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

Configuración de red

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`

Información del producto

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

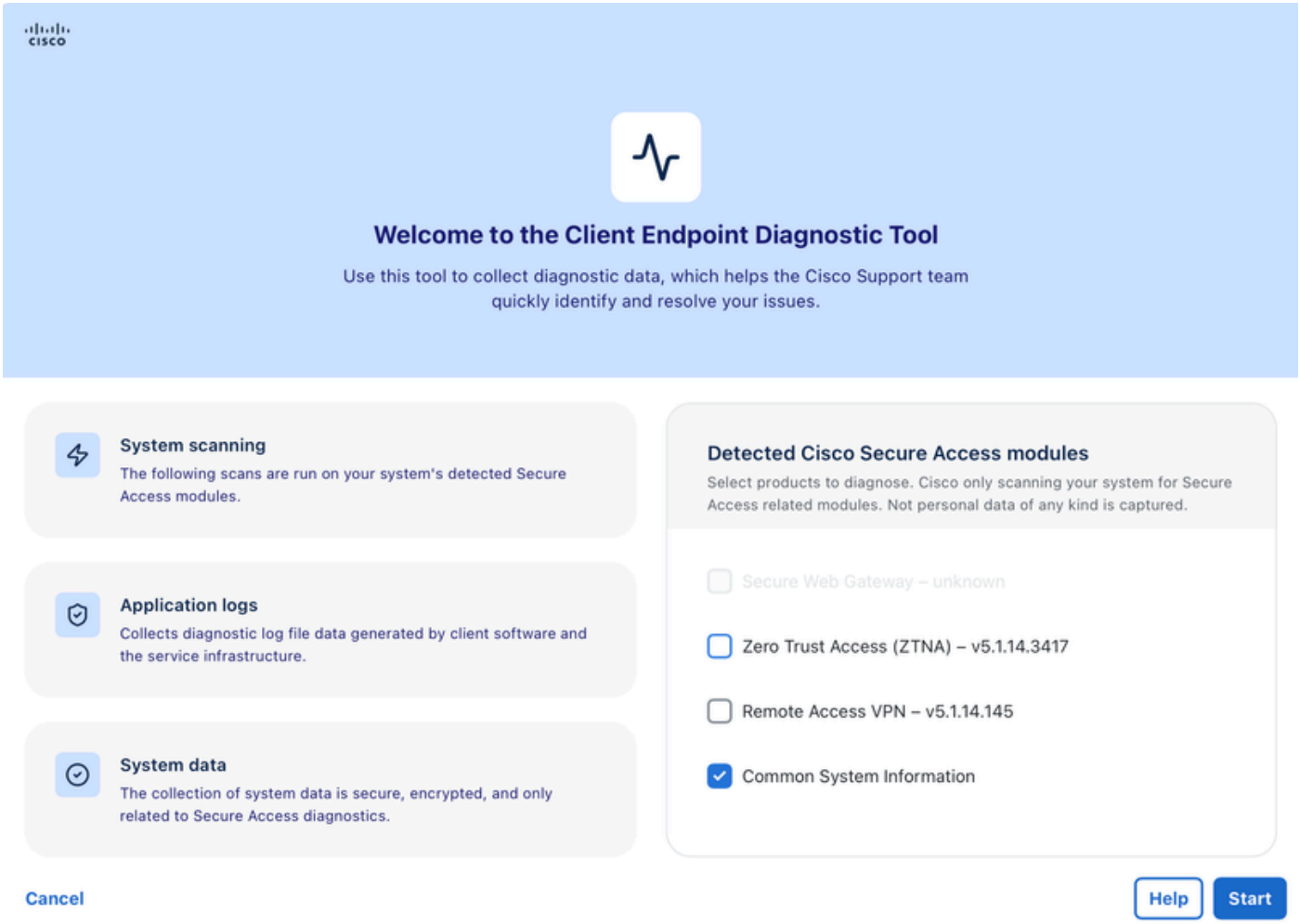
Tutorial paso a paso

Pantalla de bienvenida

Al iniciar CEDT, se muestra la pantalla Welcome (Bienvenido). Proporciona una descripción general de lo que hace la herramienta:

- Análisis del sistema: analiza el sistema en busca de módulos de Cisco Secure Access detectados.
- Registros de aplicaciones: recopila los datos del archivo de registro de diagnóstico generados por el software cliente y la infraestructura de servicio.

- Datos del sistema: la recopilación de datos del sistema es segura, está cifrada y solo está relacionada con los diagnósticos de acceso seguro.



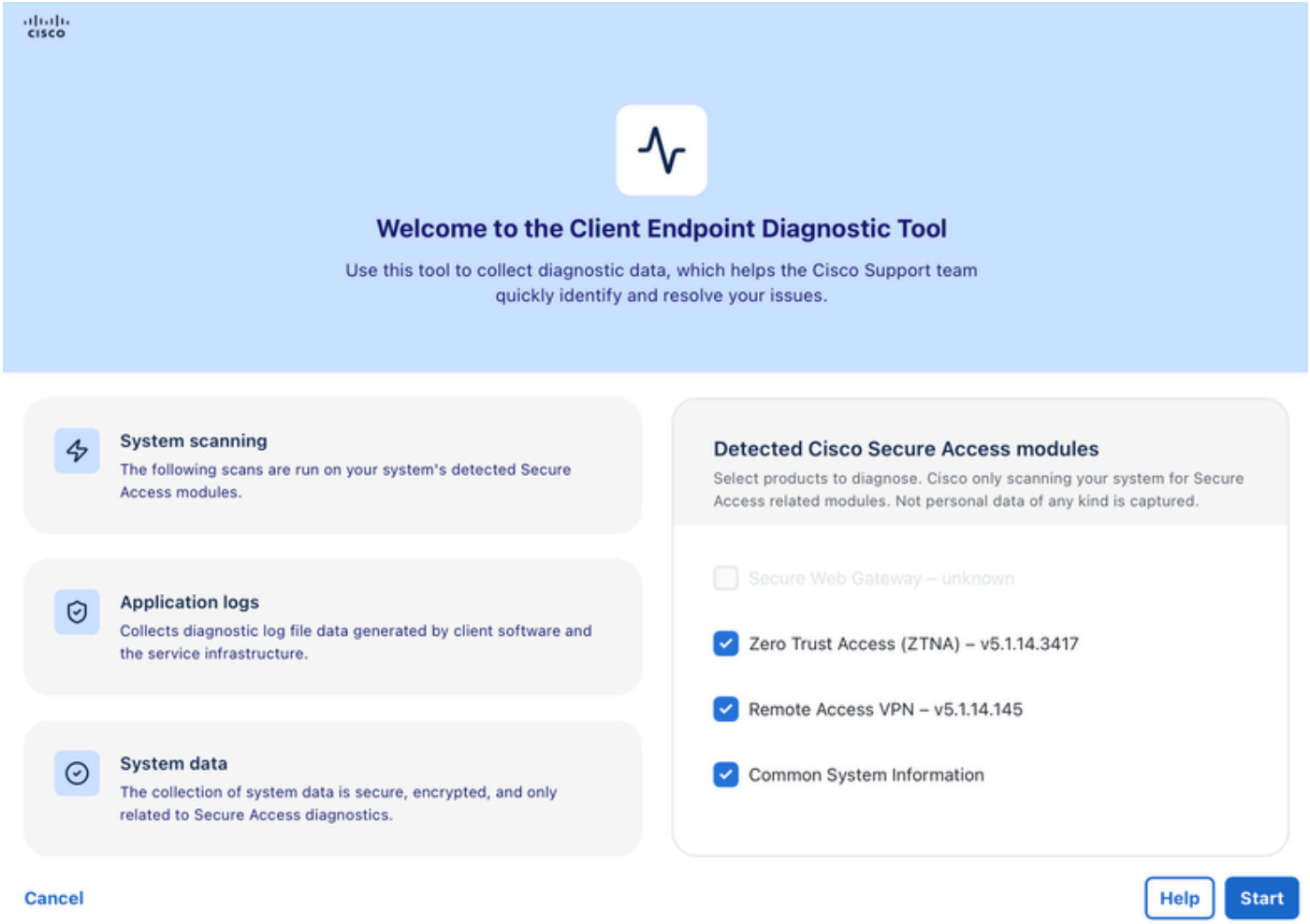
En el lado derecho, la herramienta detecta automáticamente cualquier módulo Cisco Secure Access instalado en el sistema. Puede ver casillas de verificación para cada módulo detectado junto con su número de versión:

- Acceso de confianza cero (ZTNA)
- Gateway web seguro (SWG)
- VPN de acceso remoto (RAVPN)
- Información común del sistema (siempre disponible)

Acciones

1. Seleccione o deseleccione los productos que desea diagnosticar.
2. Haga clic en Let's Start para continuar o haga clic en Help para obtener más información.

Nota: Esta herramienta solo recopila datos para los módulos relacionados con Secure Access. No se capturan datos personales de ningún tipo.



Paso 1: Recopilación de datos de diagnóstico

Esta pantalla le permite elegir qué pruebas de diagnóstico y módulos de recopilación de datos

desea incluir.

Diagnóstico de red

Seleccione las pruebas de conectividad que desea ejecutar:

- Búsqueda de DNS: realiza pruebas de resolución de DNS en hosts especificados. Admite IP de resolución personalizadas para búsquedas específicas. Todos los resultados se consolidan en un único archivo de resultados (dns/dns_lookups.txt) con delimitadores de sección estructurados.
- Captura de paquetes: captura paquetes de red durante un período de tiempo especificado (requiere privilegios de administrador).
- Hosts de ping: hace ping a los hosts especificados para comprobar la conectividad.
- Resultado de la prueba de política: prueba la aplicación de políticas frente a URL especificadas mediante el extremo de prueba de política de Cisco (policy.test.sse.cisco.com). Admite varios hosts separados por comas (máximo 10). Los resultados incluyen datos HAR capturados automáticamente durante la navegación de la prueba de políticas.
- Prueba de velocidad de la red: mide la velocidad de carga/descarga y la latencia frente al terminal de prueba de velocidad de Cisco (speed.test.sse.cisco.com). Recopila la velocidad de descarga (6 secuencias paralelas), la velocidad de carga (3 secuencias paralelas) y la latencia/fluctuación de ping (10 muestras de ICMP). Los resultados se guardan en formatos JSON y de resumen de texto.
- Disponibilidad de URL: verifica si las URL especificadas son accesibles mediante solicitudes GET HTTP. Admite HTTP (puerto 80) y HTTPS (puerto 443) de forma predeterminada. Los puertos no estándar se pueden especificar en la URL (como https://example.com:8443). Máximo de 20 URL por comprobación con un tiempo de espera de 30 segundos por URL. Los datos recopilados por URL incluyen: URL, estado de disponibilidad, código de estado HTTP, tiempo de respuesta (ms), longitud del contenido, dirección IP resuelta, versión de TLS y marca de tiempo. Los resultados se guardan en reachability/reachability_results.json y reachability/reachability_summary.txt.

Recolección de datos

Seleccionar módulos para recopilar datos de rendimiento y conectividad:

- Captura HAR: registra los datos de archivo HTTP (HAR) de una sesión del explorador. Actualmente es compatible solo con Google Chrome (utiliza el Chrome DevTools Protocol a

través de la automatización del navegador sin cabeza). La herramienta detecta automáticamente la instalación de Chrome en el sistema. Firefox y Safari no son compatibles en este momento. La salida HAR sigue la especificación HAR 1.2 e incluye seguimientos de red completos (incluidas llamadas XHR/fetch activadas por JS).

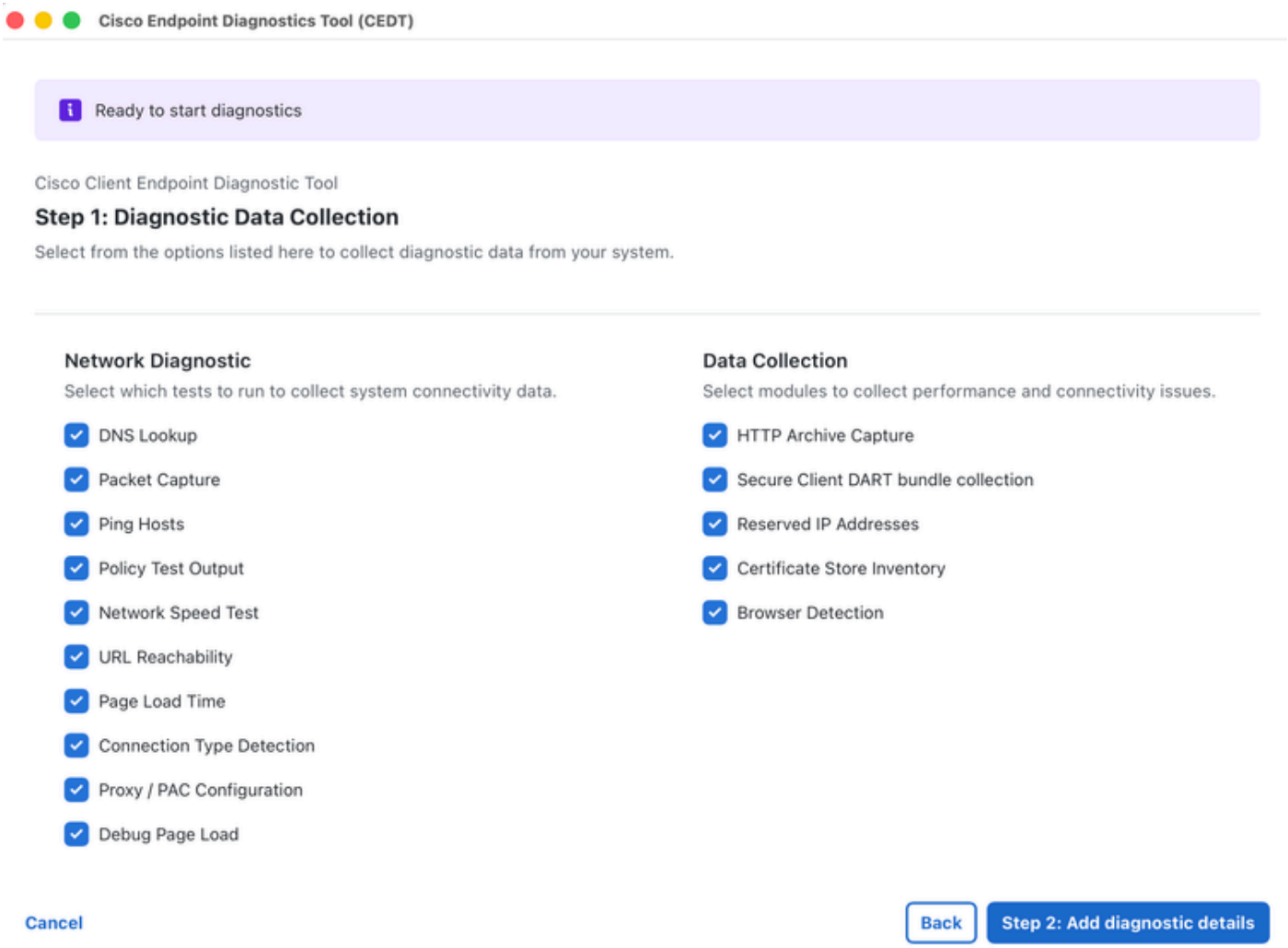
- Colección de paquetes DART: recopila un paquete de diagnóstico DART de Cisco Secure Client. Esto incluye todos los registros de módulos, incluidos los registros de acceso de confianza cero (ZTA) (como flowlog.db en Windows en C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\).
- IP reservada: ejecuta comprobaciones de diagnóstico de IP reservada. Consulte la siguiente sección para obtener la lista completa de los diagnósticos recopilados.

Depurar

- Habilitar indicadores de depuración: recopile registros detallados de actividades de terminales para diagnosticar problemas de terminales. Esta opción solo está disponible cuando se detecta y selecciona al menos un producto Cisco Secure Access.

Específicos de plataforma

- Captura de DebugView (Windows): habilita el registro de depuración en Windows Secure Endpoint Connector. Esta opción sólo está disponible en sistemas Windows.



Acciones

1. Marque o desmarque las opciones de diagnóstico que desee.
2. Haga clic en el paso 2: Agregue detalles de diagnóstico para continuar.
3. Haga clic en Back para volver a la pantalla Welcome (Bienvenido) o en Cancel para salir.

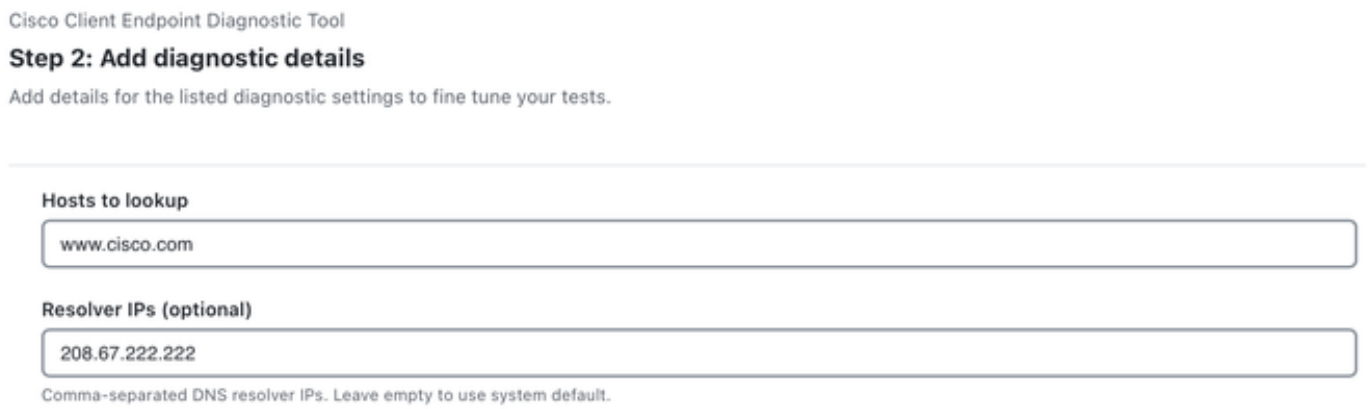
Paso 2: Agregar detalles de diagnóstico

Esta pantalla permite configurar los parámetros específicos para cada prueba de diagnóstico activada. Sólo se muestran los ajustes de las pruebas que ha activado en el paso 1.

Configuración de búsqueda de DNS

- Hosts a buscar: introduzca uno o varios nombres de host (separados por comas). Ejemplo: cisco.com
- IP de resolución (opcional): especifique IP de resolución de DNS personalizadas (separadas por comas). Ejemplo: 208.67.222.222, 208.67.220.220. Deje vacío para utilizar la resolución de DNS predeterminada del sistema. Cuando se especifica, se consulta a cada host en cada resolución, lo que proporciona resultados de resolución DNS comparativos entre los distintos servidores DNS.

Todos los resultados de la búsqueda de DNS se consolidan en un único archivo de salida: dns/dns_lookups.txt, con delimitadores de sección TextFSM estructurados para cada combinación de host y resolución.



Configuración de captura de paquetes

- Interfaces: seleccione la interfaz de red que desea capturar (o déjela como Todo).
    - Cuando se establece en All (modo automático):
        - macOS/Linux: La herramienta ejecuta tcpdump -D para enumerar todas las interfaces disponibles y, a continuación, filtra las interfaces que están en

funcionamiento (excluidas las interfaces desconectadas). Si no se encuentra ninguna interfaz activa, vuelve a la interfaz any especial. Las capturas se ejecutan en todas las interfaces coincidentes en paralelo.

  - Windows: Capturas en todas las NIC utilizando el backend de captura seleccionado (consulte las herramientas de la siguiente sección). Cuando se utiliza dumpcap sin ninguna interfaz seleccionada, se capturan simultáneamente hasta las primeras 3 interfaces detectadas.

- Número de paquetes: número de paquetes que se capturarán por interfaz. Predeterminado: 100. Máximo: 10,000.
- Duración (s): duración máxima de la captura en segundos. Predeterminado: 20 segundos en macOS/Linux, 5 segundos en Windows. Máximo: 300 segundos. La captura se detiene cuando se alcanza el conteo de paquetes o el límite de duración, lo que ocurra primero.

Herramientas de captura de paquetes por plataforma

Nota: (Windows): La herramienta selecciona automáticamente el mejor motor de captura disponible. se prefiere pktmon (integrado en Windows 10 v2004+), volver a dumpcap (si Wireshark está instalado) y, a continuación, 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

Archivos de salida de captura de paquetes

La captura de cada interfaz se guarda como un archivo independiente utilizando la convención de nomenclatura: tcpdump/{interface_name}_capture.pcap (como en0_capture.pcap, eth0_capture.pcap). También se genera un archivo de manifiesto de metadatos (tcpdump/packet_capture_manifest.txt), que registra la plataforma, el recuento de paquetes, la duración, las interfaces capturadas y el back-end de captura utilizado.

Configuración de ping

- Host/s a ping: introduzca los hosts a ping (separados por comas). Ejemplo:www.cisco.com

Configuración de alcance URL

- URL que comprobar: introduzca las URL que desee probar (separadas por comas). Ejemplo: `https://github.com`
    - Utiliza las solicitudes HTTP GET para probar la disponibilidad.
    - Puertos predeterminados: 80 (HTTP) / 443 (HTTPS). Incluya el puerto en la URL para los puertos no estándar (como `ashttps://example.com:8443`).
    - Máximo 20 URL por verificación.
    - timeout (tiempo de espera): 30 segundos por URL.
    - Datos recopilados por URL: URL, estado de disponibilidad, código de estado HTTP, tiempo de respuesta (ms), longitud del contenido, dirección IP resuelta, versión de TLS y marca de tiempo.
    - Los resultados se guardan en reachability/reachability_results.json y reachability/reachability_summary.txt.

Configuración de prueba de política

- URL de host: introduzca hosts para la prueba de políticas (separados por comas, máximo 10). Ejemplo: www.cisco.com
- Las pruebas de políticas se ejecutan en el punto final de la prueba de políticas de Cisco: policy.test.sse.cisco.com
- Los resultados incluyen resultados de pruebas de políticas estructuradas y datos HAR capturados automáticamente durante la navegación de la prueba.

Configuración de captura HAR

- URL de destino: introduzca las URL para la captura HAR (separadas por comas). Ejemplo: https://www.cisco.com/

Consejo: Captura HAR actualmente es compatible solo con Google Chrome. La herramienta utiliza el Chrome DevTools Protocol (a través de chromedp) para automatizar una sesión de Chrome sin cabeza y capturar el tráfico de la red. Asegúrese de que Google Chrome está instalado en su sistema. Firefox y Safari no son compatibles en este momento.

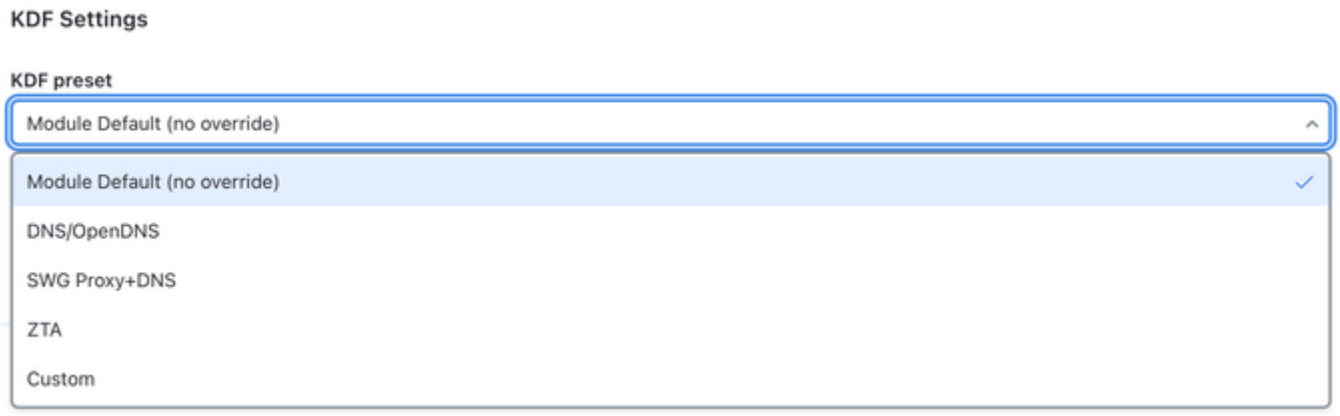
Configuración KDF

Configure los indicadores de la función de derivación de claves utilizados durante la recopilación de diagnósticos. Los indicadores KDF controlan qué categorías de depuración están habilitadas en Cisco Secure Client:

- Preajuste de KDF: seleccione un preajuste de función de derivación de teclas.
- KDF HEX: El valor hexadecimal se rellena automáticamente en función del valor predefinido seleccionado. Cuando esté seleccionado "Personalizado", introduzca su propio 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.



Configuración de IP reservada

- URL de NSLookup: hosts nslookup personalizados opcionales (separados por comas). Máximo de 10 URL. Se consulta a cada host personalizado con todos los resolvers

configurados.

- URL de seguimiento: hosts traceroute/tracert personalizados opcionales (separados por comas). Máximo de 10 URL. La herramienta utiliza automáticamente traceroute en macOS/Linux y tracert en Windows.
- IP de resolución: IP de resolución personalizadas opcionales para consultas nslookup (separadas por comas, como 208.67.222).
- 222 de 208.67.220.220). Máximo 5 IP. Cuando se especifica, se utilizan resoluciones personalizadas además de las tres resoluciones integradas (DNS predeterminado del sistema, 127.0.0.1, 208.67.222.222).

Detalles IP reservados

El diagnóstico de IP reservada recopila estos datos de forma predeterminada:

Destinos de traceroute/tracert predeterminados (se ejecutan automáticamente con todos ellos):

Objetivo	Propósito
208.67.222.222	Route to OpenDNS primary nameserver
208.67.220.220	Route to OpenDNS secondary nameserver

146.112.255.50	Ruta a IP de infraestructura de Cisco SWG
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	Ruta al nombre de host del proxy SWG

- macOS/Linux: Utiliza el comando traceroute
- Windows: Utiliza el comando tracert

Consultas de NSLookup predeterminadas (se ejecutan en todas ellas automáticamente):

Se consulta cada destino de nslookup con cada resolución de la lista de resolución. De forma predeterminada, la lista de resolución incluye tres resoluciones integradas:

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

Si se configuran IPs de resolución personalizadas (como 208.67.222.222), se agregan a la lista de resolución y también se consultan todos los destinos de nslookup con ellos.

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 ejemplo, con los resolvers predeterminados 3, esto produce 6 consultas nslookup (2 resolvers de destinos x 3). La adición de una IP de resolución personalizada aumenta este valor a 8 consultas (2 resoluciones de destino x 4).

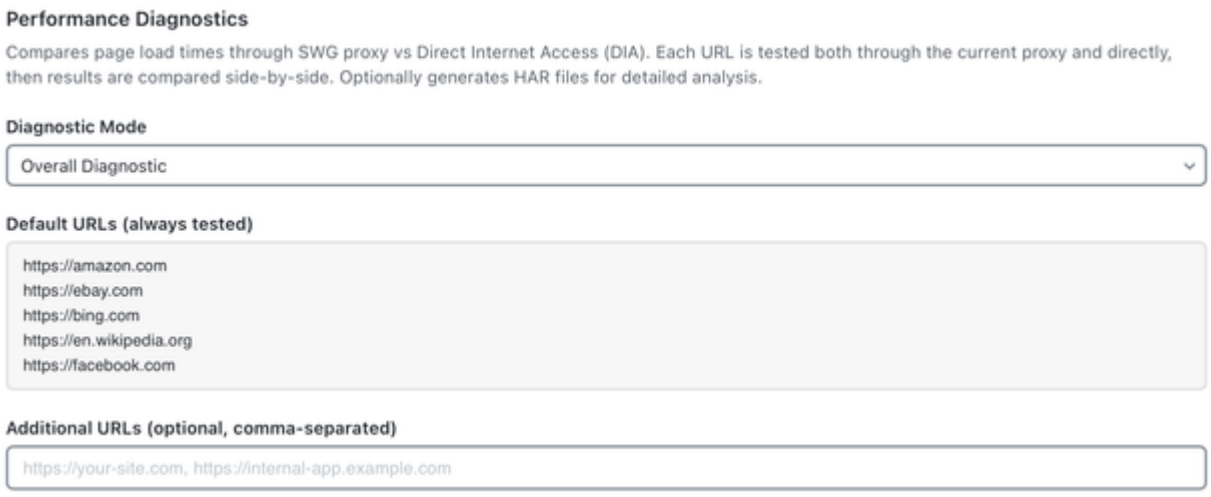
Las URL de búsqueda de NSLookup personalizadas proporcionadas por el usuario se consultan en la misma lista de resolución completa (resoluciones integradas + personalizadas).

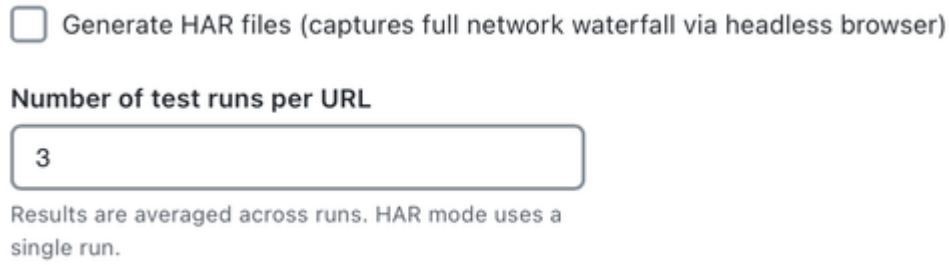
Todos los resultados se consolidan en un único archivo: reserved_ip/reserved_ip_diagnostics.txt, agrupado por sección (traceroute, nslookup) con encabezados legibles por el usuario que indican el destino y la resolución de cada entrada.

Diagnóstico de rendimiento

Compara los tiempos de carga de páginas mediante proxy SWG frente a acceso directo a Internet (DIA). Dispone de dos modos:

1 Modo de diagnóstico general: Cada URL se prueba tanto a través del proxy actual como directamente, luego los resultados se comparan uno al lado del otro. De manera opcional, genera archivos HAR para un análisis detallado.





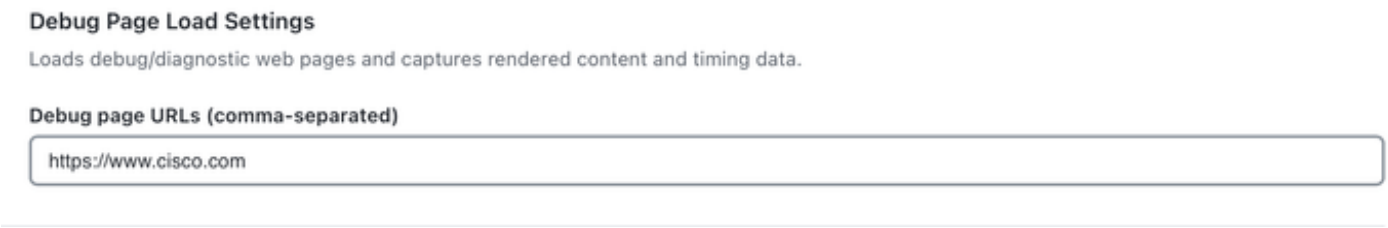
2 Modo de diagnóstico de una URL: Podemos introducir una URL específica para probarla tanto a través del proxy actual como directamente y, a continuación, los resultados se comparan uno al lado del otro. De manera opcional, genera archivos HAR para un análisis detallado.

Configuración de inventario de almacén de certificados

- Enumera certificados de almacenes de certificados configurados:
  - Sistema
  - Inicio de sesión
  - Raíz
  - Y mucho más
- Identifica rápidamente certificados que faltan, caducados o que no son fiables

Configuración de carga de página de depuración:

- Carga las URL de depuración configurables.
- Capturas:
  - Encabezados de respuesta
  - Cuerpo de respuesta
  - Información de sincronización
  - metadatos SSL



Acciones

1. Rellene o ajuste los parámetros de cada diagnóstico activado.
2. Haga clic en Iniciar diagnóstico para iniciar la ejecución del diagnóstico.
3. Haga clic en Atrás para volver al paso 1 o en Cancelar para salir

---

Nota: Los campos con errores de validación están resaltados. Debe corregirlos antes de que se pueda iniciar el diagnóstico.

Pausar y continuar

Cuando se ejecuta una recopilación de diagnóstico que incluye solución de problemas avanzada (por ejemplo, ZTNA o seguimiento SWG), la herramienta de diagnóstico de terminales de Cisco puede hacer una pausa durante la ejecución y pedirle que reproduzca el problema antes de que continúe.

Esto le da tiempo para activar el problema mientras se activa el registro detallado, para que el equipo de soporte reciba datos de diagnóstico más útiles.

- Cuando aparezca la ventana Diagnostics Paused, lea el mensaje, que le indica qué funciones de registro están ahora activas.
- Reproduzca el problema que está solucionando. Por ejemplo:
    - Volver a conectar a VPN
    - Abra la aplicación interna que está fallando
    - Repita los pasos que causan el error
- Cuando haya terminado de reproducir el problema, haga clic en Continuar

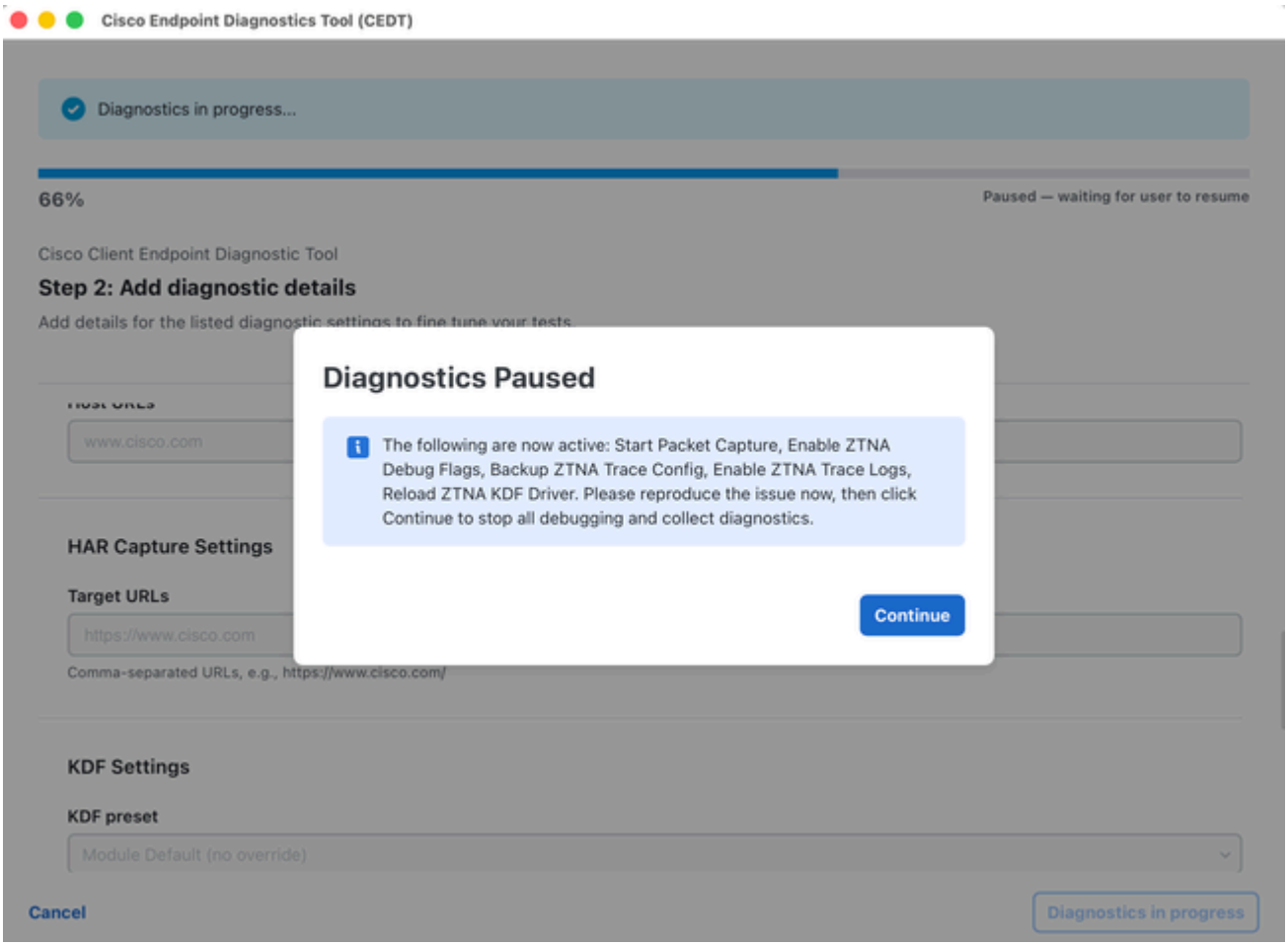
Deja que la carrera termine. A continuación, la herramienta recopila archivos, restaura la configuración normal y crea el archivo de diagnóstico.

NOTA:No cierre la aplicación mientras está en pausa. El registro permanecerá activo hasta que haga clic en Continuar y finalice la ejecución.

(Línea de comandos)

Si está ejecutando la herramienta desde un terminal, puede ver un mensaje de pausa en la ventana en lugar de un cuadro de diálogo.

1. Lea el mensaje de pausa que se muestra en el terminal.
2. Reproduzca el problema.
3. Vuelva a la terminal y pulse Enter para continuar.
4. Espere a que termine la carrera.

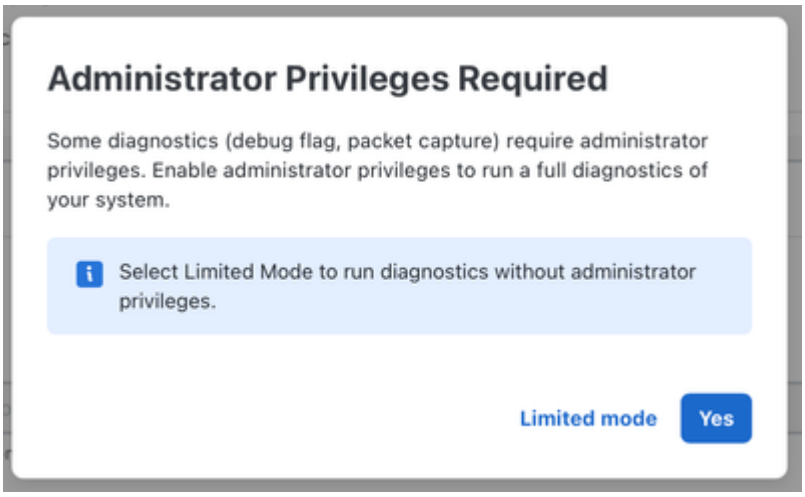


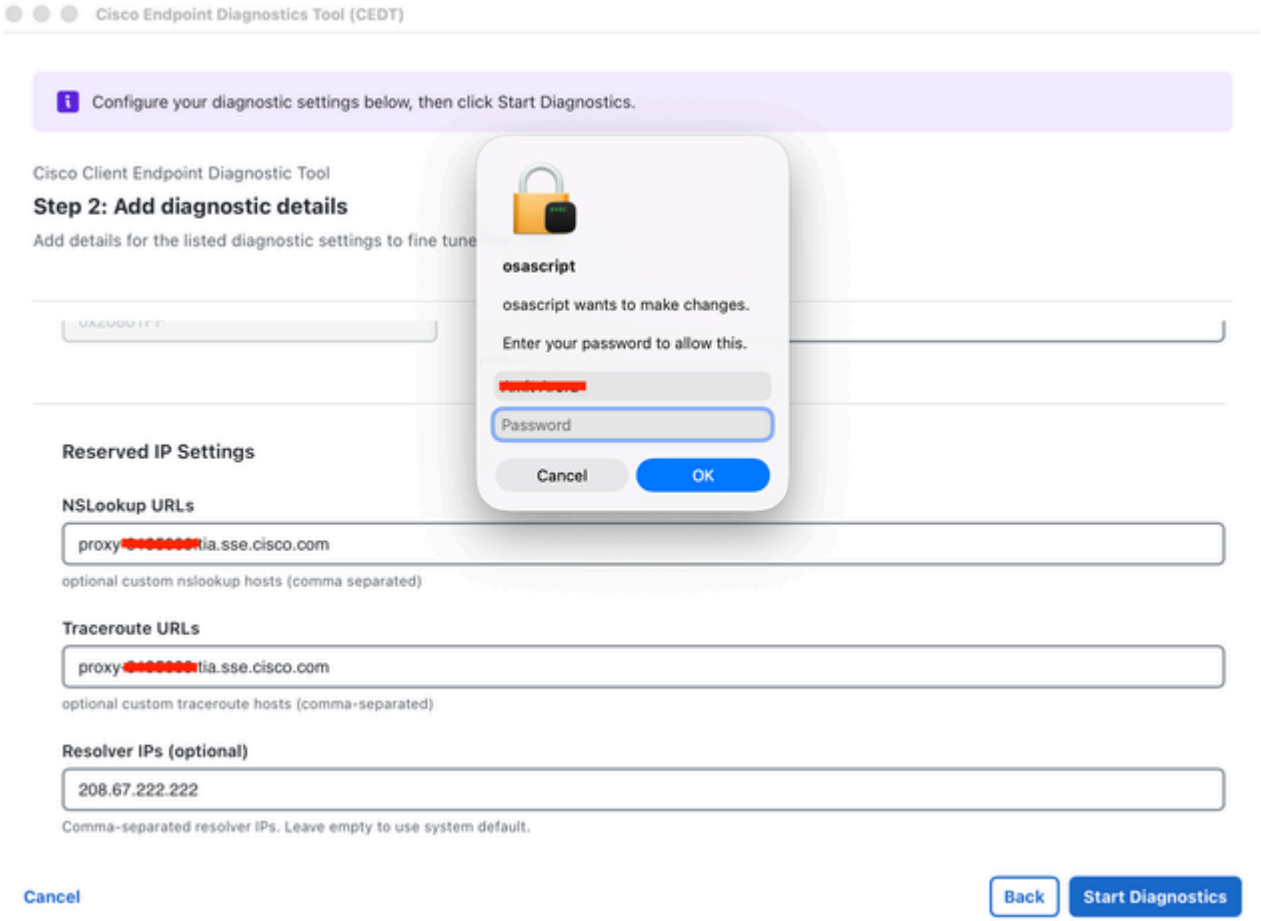
Mensaje de privilegios del administrador

Después de hacer clic en Iniciar diagnóstico, la herramienta puede solicitar privilegios de administrador si ha habilitado funciones que requieren un acceso elevado (como Captura de paquetes o Indicadores de depuración).

Aparecerá un cuadro de diálogo con el título Privilegios de administrador requeridos:

- Haga clic en Sí para otorgar privilegios de administrador. Esto activa la solicitud de credenciales nativas de macOS/Windows.
- Haga clic en Modo limitado para continuar sin elevación. Las tareas con privilegios (captura de paquetes, indicadores de depuración) se omiten.
- macOS: Puede ver el diálogo de contraseña estándar de macOS desde osascript. Introduzca la contraseña del sistema y haga clic en Aceptar.
- Windows: Aparece un mensaje de elevación estándar de UAC. Haga clic en Sí para permitir.





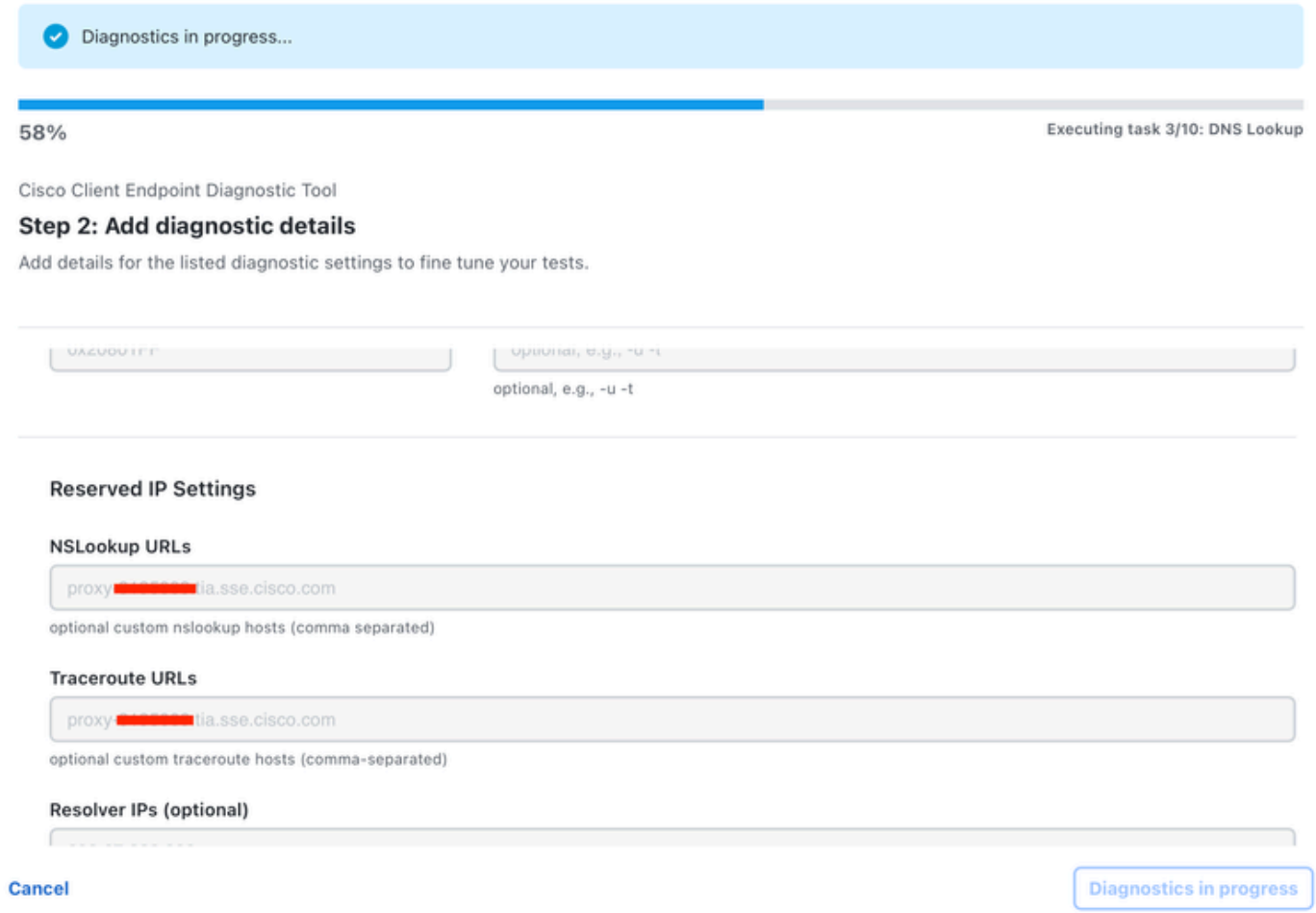
Diagnóstico en curso

Una vez iniciada, la herramienta ejecuta todas las tareas de diagnóstico seleccionadas:

- Una barra de progreso muestra la finalización general (como 59% — Ejecución de la tarea 3/9: Búsqueda de DNS).

- Un diagnóstico en curso... se muestra en la parte superior.
- Todos los campos de configuración están desactivados o atenuados durante la ejecución.
- El pie de página muestra un botón Diagnóstico en curso (deshabilitado) para indicar que la herramienta está ocupada.

Espere mientras se completa el diagnóstico. No cierre la aplicación.



1.

Diagnóstico completado: carga en TAC

Cuando todos los diagnósticos terminan, aparece un cuadro de diálogo de finalización:

Diagnóstico finalizado. Cargue el archivo en un caso del TAC.

El cuadro de diálogo muestra:

- Archive: nombre de archivo del archivo de diagnóstico generado (como cisco_diagnostics.tar.gz).
- Tamaño de archivo: el tamaño del archivo (por ejemplo, 7,72 MB).
- SHA256: suma de comprobación del archivo de almacenamiento para la verificación de integridad.

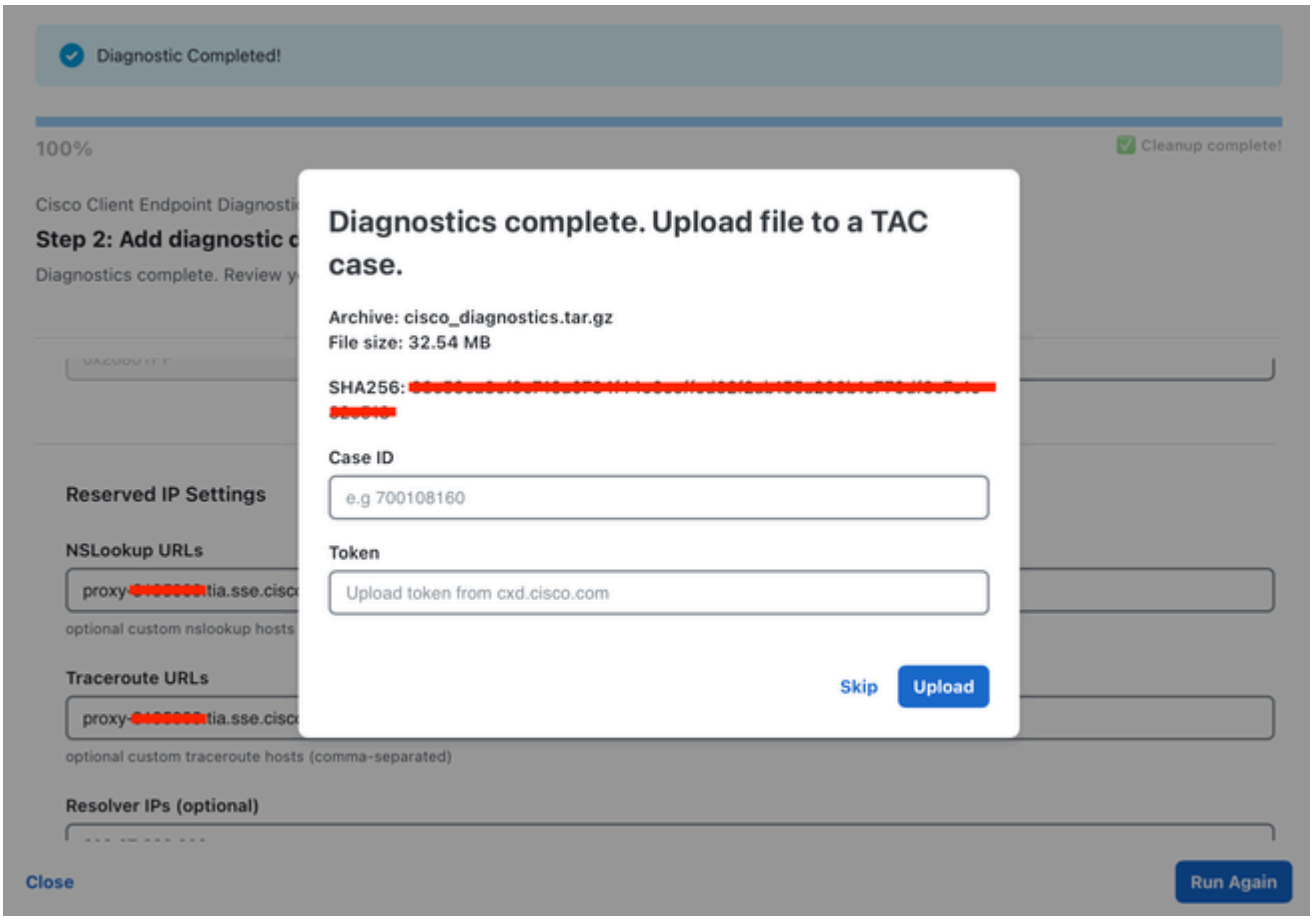
Para cargar en un caso de TAC:

1. Introduzca su ID de caso (como 698746730).
2. Ingrese su Token (proporcionado por el soporte de Cisco).
3. Haga clic en Abrir caso TAC para iniciar la carga.

Una barra de progreso muestra el estado de la carga (como Cargando... 85,0% (6,56 MB / 7,72 MB).

Para omitir la carga:

- Haga clic en Skip para cerrar el diálogo sin cargar. El archivo de almacenamiento aún se guarda localmente.



Carga finalizada: pantalla final

Después de una carga correcta, el banner de finalización se actualiza a:

Archivo de diagnóstico cargado correctamente en el caso [Case ID]

La barra de progreso muestra 100% con el estado Limpieza completa.

Acciones

- Haga clic en Ejecutar de nuevo para iniciar una nueva ejecución de diagnóstico.
- Haga clic en Cerrar para salir de la aplicación.

Ubicación de salida

El resultado del diagnóstico se guarda en:

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

El archivo de salida (cisco_diagnostics.tar.gz) contiene todos los datos de diagnóstico recopilados en un formato estructurado.

Resolución de problemas

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.

Preguntas frecuentes

A: ¿Qué datos recopila esta herramienta?
R: La herramienta recopila información del sistema (SO, hardware, configuración de red), registros de aplicaciones, datos de la configuración de productos y módulos instalados de Cisco, y datos de diagnóstico de red relacionados únicamente con los módulos Cisco Secure Access. Consulte la sección Qué datos del sistema se recopilan en la sección anterior para obtener un

desglose detallado. No se capturan datos personales.

A: ¿Necesito acceso de administrador/raíz?
R: El acceso de administrador es opcional, pero se recomienda. Sin ella, se omiten algunos diagnósticos (captura de paquetes, indicadores de depuración). La herramienta le solicita y le permite elegir.

A: ¿Puedo ejecutar la herramienta varias veces?
R: Yes. Una vez finalizada cada ejecución, puede hacer clic en "Ejecutar de nuevo" para iniciar una nueva sesión de diagnóstico.

A: ¿Dónde se guarda la salida?
R: El archivo de diagnóstico se guarda en el escritorio en la carpeta cisco_diagnostics.

A: ¿Qué sucede si no tengo una ID de caso de TAC?
R: Puede hacer clic en "Omitir" en el cuadro de diálogo de carga. El archivo de almacenamiento aún se guarda localmente. Puede cargarlo manualmente en un caso del TAC más adelante o compartirlo con su ingeniero de soporte.

A: ¿Están cifrados los datos?
R: El archivo de diagnóstico se comprime (tar.gz) y los datos confidenciales se eliminan automáticamente antes de empaquetarlos.

A: ¿Qué navegadores admite la captura de HAR?
R: HAR captura actualmente es compatible con Google Chrome solo. La herramienta utiliza el Chrome DevTools Protocol para la automatización del navegador sin cabeza. Asegúrese de que Chrome esté instalado antes de ejecutar la captura HAR.

P La pantalla de pausa nunca apareció. ¿Pasa algo?

R: No necesariamente. El paso de pausa solo aparece cuando el registro detallado se ha habilitado correctamente para su escenario. Compruebe el registro de ejecución en la aplicación: si se omitieron los pasos de activación, la herramienta continúa sin pausar.

P La carrera parece atascada. ¿Qué debo hacer?

R: Busque la ventana Diagnóstico en pausa; puede estar detrás de otras ventanas. La ejecución no avanzará hasta que haga clic en Continuar (o presione Intro en la línea de comandos).

P El mensaje enumera características que no esperaba. ¿Es normal?

R: Yes. El mensaje muestra las funciones de registro que la herramienta haya activado para la plataforma y las opciones de diagnóstico que haya seleccionado.

P Cerré la aplicación durante la pausa. ¿Ahora qué?

R: Ejecute de nuevo la recopilación de diagnóstico y déjela terminar. Si no está seguro de si el inicio de sesión se ha dejado encendido, póngase en contacto con el ingeniero de soporte técnico para obtener ayuda.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).