Comprendre l'outil CEDT (Endpoint Diagnostics Tool)

Table des matières

- Introduction
- Conditions préalables
- Données système collectées
  - Informations générales sur le système
  - Configuration du réseau
  - Informations sur le produit
- Procédure pas à pas
  - Écran de bienvenue
    - Actions
  - Étape 1: Collecte des données de diagnostic
    - Diagnostic du réseau
    - Collecte des données
    - Déboguer
    - Spécifique À La Plateforme
    - Actions
  - Étape 2: Ajouter des détails de diagnostic
    - Paramètres de recherche DNS
    - Paramètres de capture de paquets
    - Outils de capture de paquets par plate-forme
    - Fichiers de sortie de capture de paquets
    - Paramètres Ping
    - Paramètres d'accessibilité URL
    - Paramètres de test de stratégie
    - Paramètres de capture HAR
    - Paramètres KDF
    - Paramètres IP réservés
    - Détails IP réservés
    - Diagnostics des performances
    - Actions
  - Suspendre et continuer
  - Invite Privilèges administrateur
  - Diagnostics en cours
  - Diagnostics terminés - Téléchargement vers le TAC
  - Téléchargement terminé - Écran final
    - Actions
- Emplacement de sortie
- Dépannage
- FAQ

Introduction

Ce document décrit le CEDT pour collecter des données de diagnostic de votre système et les télécharger vers un dossier d'assistance du TAC Cisco.

Conditions préalables

Cet outil est disponible pour MacOS et Windows.

Vous devez comprendre ces sujets :

- MacOS : Double-cliquez sur Cisco Endpoint Diagnostics Tool (CEDT).app pour le lancer.
- Fenêtres: Double-cliquez sur CEDT.exe pour démarrer.
- Une connexion Internet active.
- Un ID de dossier et un jeton du centre d'assistance technique Cisco (requis uniquement si vous souhaitez télécharger les résultats directement).

Données système collectées

L'outil collecte ces données système, classées par catégorie. Aucune donnée personnelle n'est saisie.

Informations générales sur le système

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

Configuration du réseau

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`

Informations sur le produit

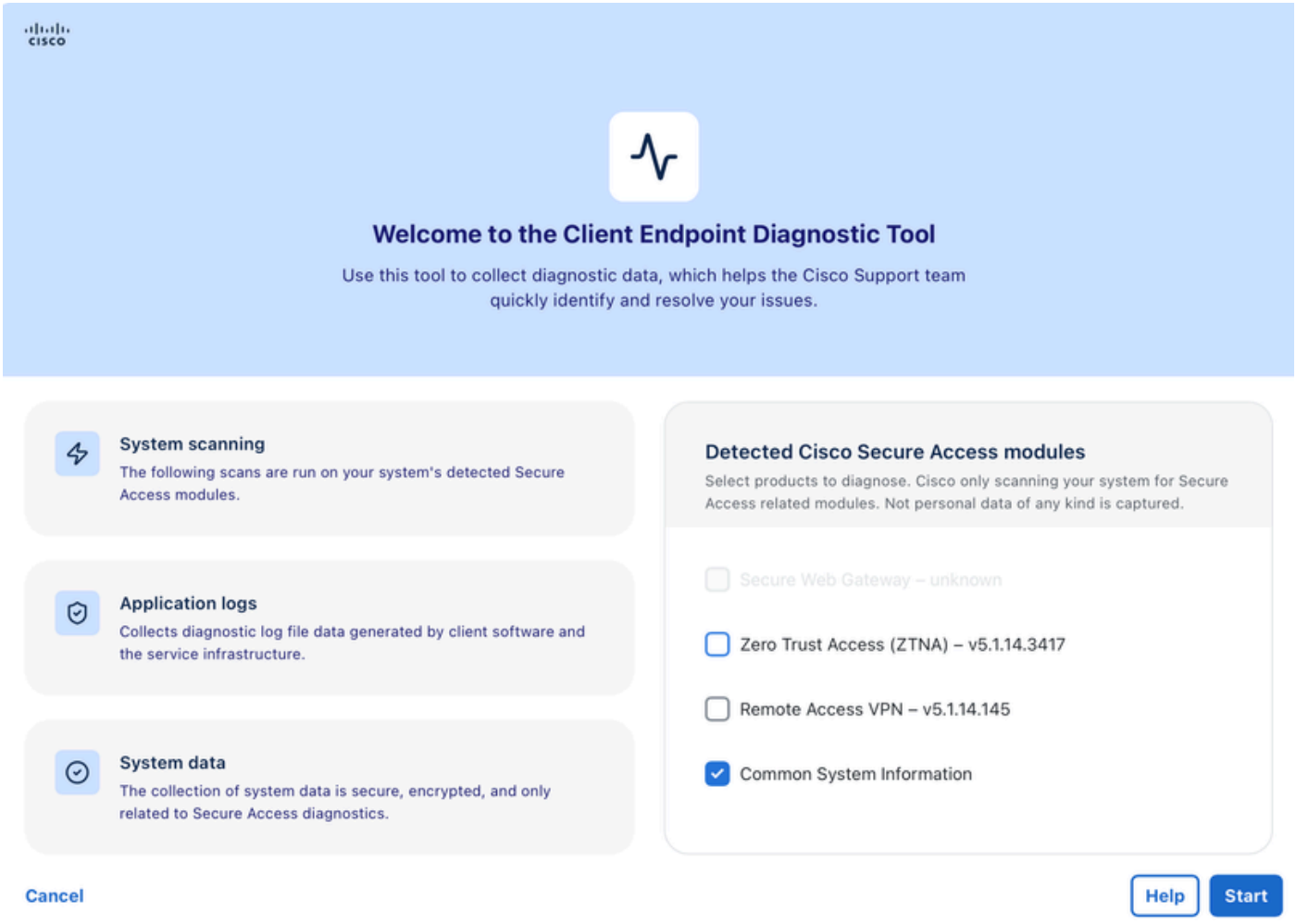
Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco.*`	Registry exports (`HKLM\SOFTWARE\Cisco`, `HKCU\SOFTWARE\Cisco`, `acsock` service)
Installation directories	`ls -laR /opt/cisco`	`%ProgramFiles%\Cisco`, `%ProgramFiles(x86)%\Cisco`, `%ProgramData%\Cisco`
Running Cisco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

Procédure pas à pas

Écran de bienvenue

Lorsque vous lancez CEDT, l'écran Welcome (Bienvenue) s'affiche. Il fournit un aperçu de ce que l'outil fait :

- Analyse du système : analyse votre système à la recherche de modules Cisco Secure Access détectés.
- Journaux d'application : collecte les données du fichier journal de diagnostic générées par le logiciel client et l'infrastructure de service.
- Données système : la collecte des données système est sécurisée, chiffrée et uniquement liée aux diagnostics d'accès sécurisé.



Sur le côté droit, l'outil détecte automatiquement tous les modules Cisco Secure Access installés sur votre système. Vous pouvez voir les cases à cocher pour chaque module détecté avec son numéro de version :

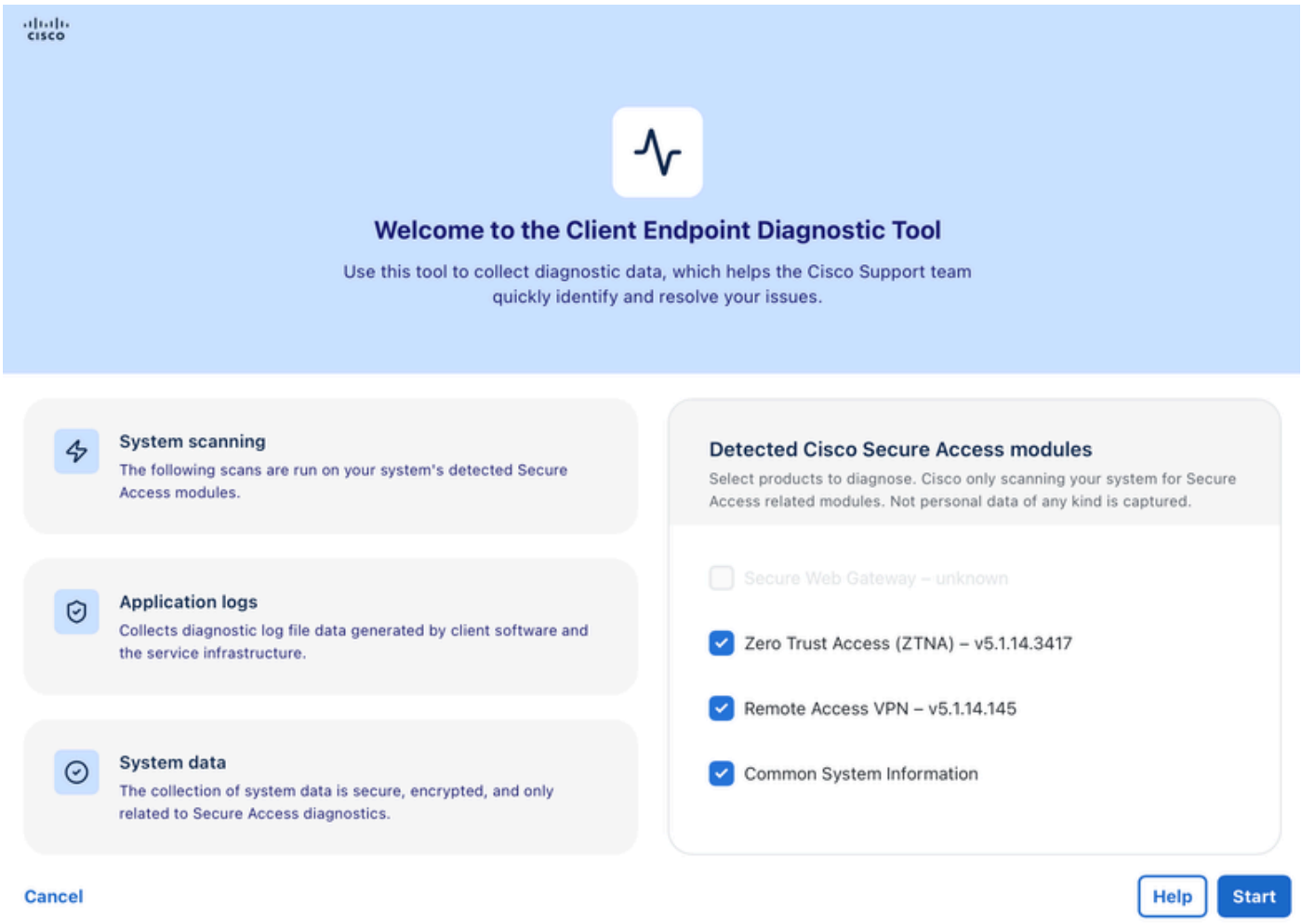
- ZTNA (Zero Trust Access)
- Passerelle Web sécurisée (SWG)
- VPN d'accès à distance (RAVPN)

- Informations système communes (toujours disponibles)

Actions

1. Sélectionnez ou désélectionnez les produits que vous souhaitez diagnostiquer.
2. Cliquez sur Let's Start pour continuer ou cliquez sur Help pour plus d'informations.

Remarque : Cet outil collecte uniquement des données pour les modules associés à Secure Access. Aucune donnée personnelle n'est saisie.



Étape 1: Collecte des données de diagnostic

Cet écran vous permet de choisir les tests de diagnostic et les modules de collecte de données à inclure.

Diagnostic du réseau

Sélectionnez les tests de connectivité à exécuter :

- Recherche DNS : effectue des tests de résolution DNS sur les hôtes spécifiés. Prend en charge les adresses IP de résolution personnalisées pour les recherches ciblées. Tous les résultats sont consolidés dans un seul fichier de sortie (dns/dns_lookups.txt) avec des délimiteurs de section structurés.
- Capture de paquets : capture les paquets réseau pour une durée spécifiée (nécessite des privilèges d'administrateur).
- Ping Hosts - Envoie une requête ping aux hôtes spécifiés pour vérifier la connectivité.
- Résultats des tests de stratégie - Teste l'application des stratégies par rapport aux URL spécifiées à l'aide du point de terminaison de test de stratégie Cisco (policy.test.sse.cisco.com). Prend en charge plusieurs hôtes séparés par des virgules (10 au maximum). Les résultats incluent les données HAR capturées automatiquement lors de la navigation du test de stratégie.
- Network Speed Test : mesure la vitesse de chargement/téléchargement et la latence par rapport au terminal de test de vitesse Cisco (speed.test.sse.cisco.com). Collecte la vitesse de téléchargement (6 flux parallèles), la vitesse de téléchargement (3 flux parallèles) et la latence/gigue des requêtes ping (10 échantillons ICMP). Les résultats sont enregistrés au format JSON et au format texte résumé.
- Accessibilité des URL : vérifie si les URL spécifiées sont accessibles à l'aide des requêtes HTTP GET. Prend en charge HTTP (port 80) et HTTPS (port 443) par défaut. Les ports non standard peuvent être spécifiés dans l'URL (par exemple, https://)example.com:8443). 20 URL maximum par vérification avec un délai d'attente de 30 secondes par URL. Les données collectées par URL incluent : URL, état d'accessibilité, code d'état HTTP, temps de réponse (ms), longueur du contenu, adresse IP résolue, version TLS et horodatage. Les résultats sont enregistrés dans reachability/reachability_results.json et reachability/reachability_summary.txt.

Collecte des données

Sélectionnez les modules pour collecter les données de performances et de connectivité :

- Capture HAR : enregistre les données d'archive HTTP (HAR) d'une session de navigateur. Actuellement prend en charge Google Chrome seulement (utilise le Chrome DevTools Protocol via l'automatisation du navigateur sans en-tête). L'outil détecte automatiquement l'installation de Chrome sur votre système. Firefox et Safari ne sont pas pris en charge pour le moment. La sortie HAR est conforme à la spécification HAR 1.2 et inclut des traces réseau complètes (y compris les appels XHR/fetch déclenchés par JS).
- Collection d'offres groupées DART : collecte une offre groupée de diagnostic DART auprès du client sécurisé Cisco. Cela inclut tous les journaux de module, y compris les journaux ZTA (Zero Trust Access) (tels que flowlog.db sous Windows à l'adresse

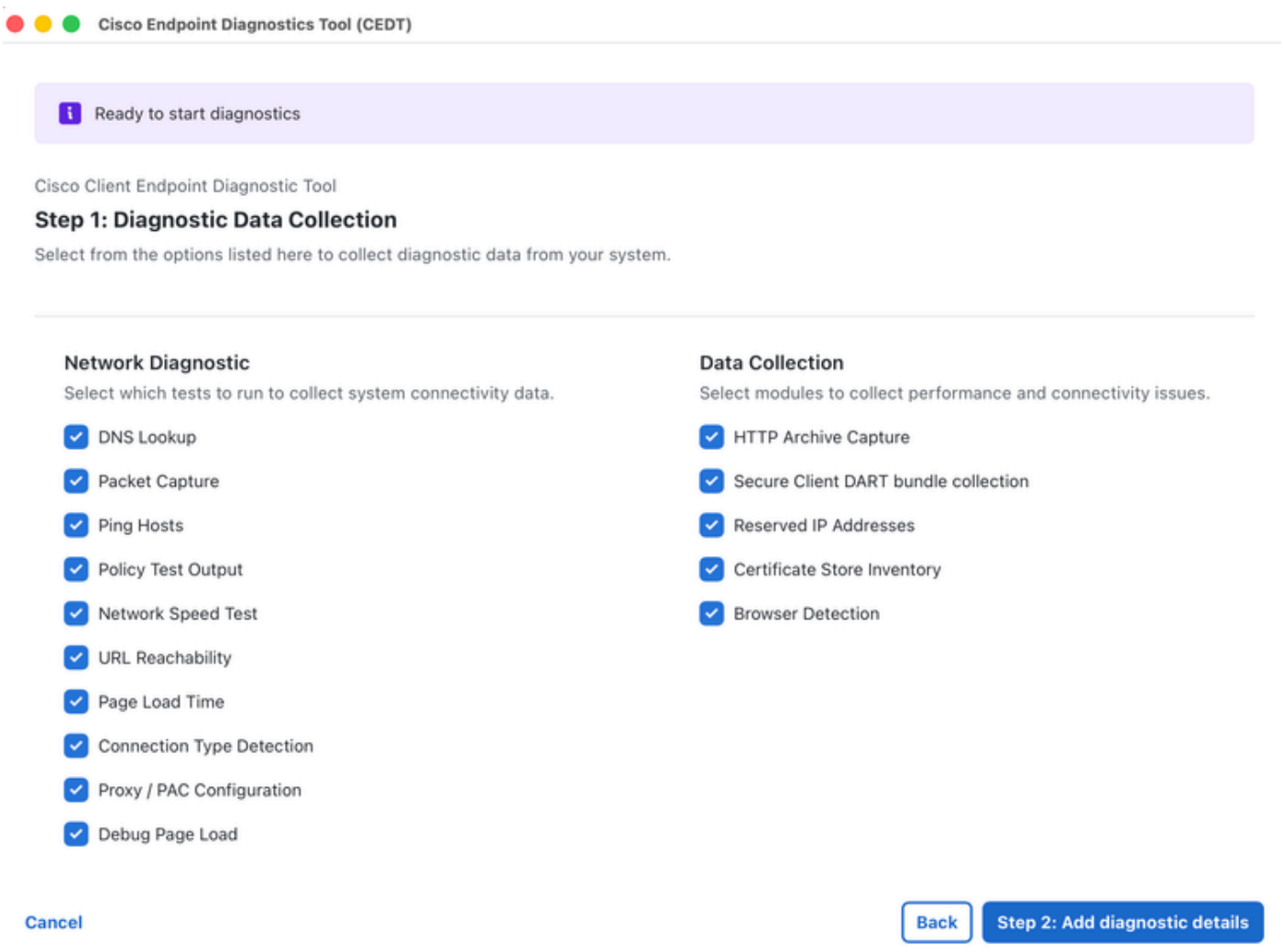
C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\).
- Reserved IP : exécute les vérifications de diagnostic IP réservées. Reportez-vous à la section suivante pour obtenir la liste complète des diagnostics collectés.

Déboguer

- Enable Debug Flags : collecte des journaux détaillés des activités des terminaux pour diagnostiquer les problèmes de terminaux. Cette option n'est disponible que lorsqu'au moins un produit Cisco Secure Access est détecté et sélectionné.

Spécifique À La Plateforme

- DebugView Capture (Windows) : active la journalisation du débogage sur le connecteur Secure Endpoint de Windows. Cette option n'est disponible que sur les systèmes Windows.



Actions

1. Cochez ou décochez les options de diagnostic souhaitées.
2. Cliquez sur Étape 2 : Ajoutez des détails de diagnostic pour continuer.
3. Cliquez sur Back pour revenir à l'écran Welcome (Bienvenue) ou sur Cancel pour quitter.

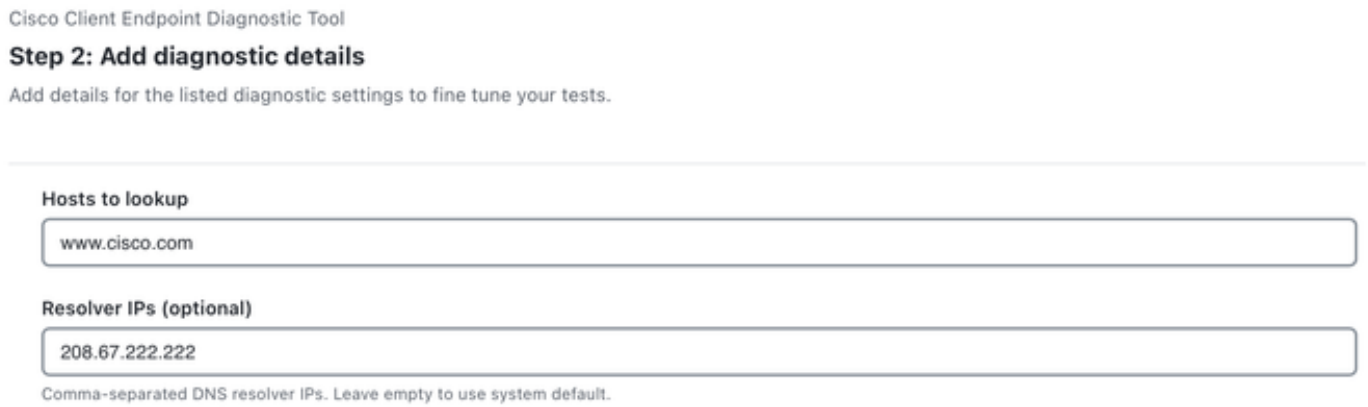
Étape 2: Ajouter des détails de diagnostic

Cet écran vous permet de configurer les paramètres spécifiques de chaque test de diagnostic activé. Seuls les paramètres des tests que vous avez activés à l'étape 1 sont affichés.

Paramètres de recherche DNS

- Hôtes à rechercher : saisissez un ou plusieurs noms d'hôte (séparés par des virgules). Exemple : cisco.com
- Adresses IP du résolveur (facultatif) : saisissez les adresses IP du résolveur DNS personnalisé (séparées par des virgules). Exemple : 208.67.222.222, 208.67.220.220. Laissez vide pour utiliser le résolveur DNS par défaut du système. Une fois spécifié, chaque hôte est interrogé par rapport à chaque résolveur, fournissant des résultats de résolution DNS comparative sur différents serveurs DNS.

Tous les résultats de la recherche DNS sont consolidés dans un seul fichier de sortie : dns/dns_lookups.txt, avec des délimiteurs de section TextFSM structurés pour chaque combinaison hôte/résolveur.



Paramètres de capture de paquets

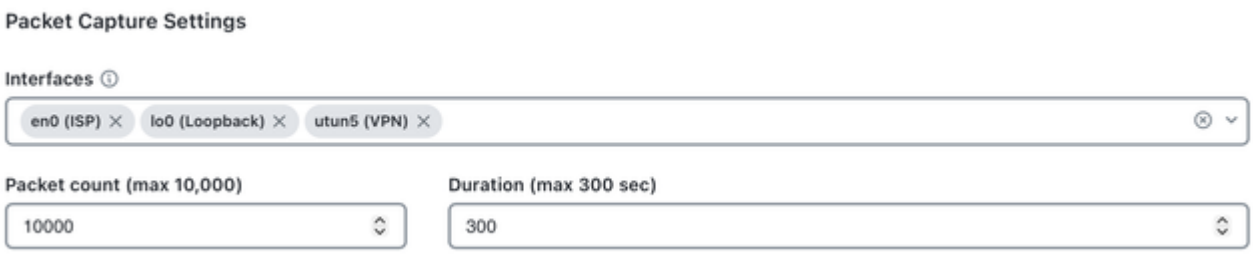
- Interfaces : sélectionnez l'interface réseau sur laquelle effectuer la capture (ou conservez la valeur All).
    - Lorsque cette option est définie sur All (mode auto) :
        - macOS/Linux : L'outil exécute tcpdump -D pour énumérer toutes les interfaces

disponibles, puis filtre les interfaces qui sont actives et en cours d'exécution (à l'exception des interfaces déconnectées). Si aucune interface active n'est trouvée, elle revient à l'interface spéciale any. Les captures s'exécutent sur toutes les interfaces correspondantes en parallèle.
    - Fenêtres: Effectue des captures sur toutes les cartes réseau en utilisant le moteur de capture sélectionné (voir les outils dans la section suivante). Lors de l'utilisation de dumpcap sans interface sélectionnée, jusqu'aux 3 premières interfaces détectées sont capturées simultanément.
- Packet count : nombre de paquets à capturer par interface. Par défaut : 100. Maximum : 10,000.
- Durée (s) - Durée maximale de capture en secondes. Par défaut : 20 secondes sous macOS/Linux, 5 secondes sous Windows. Maximum : 300 secondes La capture s'arrête lorsque le nombre de paquets ou la limite de durée est atteint, selon la première éventualité.

Outils de capture de paquets par plate-forme

Remarque : (Windows) : L'outil sélectionne automatiquement le meilleur moteur de capture disponible. pktmon est préférable (intégré à Windows 10 v2004+), en revenant à dumpcap (si Wireshark est installé), puis netsh trace en dernier recours.

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



Fichiers de sortie de capture de paquets

La capture de chaque interface est enregistrée dans un fichier distinct selon la convention d'attribution de noms : tcpdump/{nom_interface}_capture.pcap (comme en0_capture.pcap, eth0_capture.pcap). Un fichier manifeste de métadonnées (tcpdump/packet_capture_manifest.txt) est également généré, enregistrant la plate-forme, le nombre de paquets, la durée, les interfaces capturées et le moteur de capture utilisé.

Paramètres Ping

- Hôtes à envoyer une requête ping : saisissez les hôtes à envoyer une requête ping (séparés par des virgules). Exemple : www.cisco.com.



Paramètres d'accessibilité URL

URL à vérifier : saisissez les URL à tester (séparées par des virgules). Exemple : https://github.com

- Utilise les requêtes HTTP GET pour tester l'accessibilité.
- Ports par défaut : 80 (HTTP) / 443 (HTTPS). Incluez le port dans l'URL des ports non standard (par exemple, https:///)example.com:8443).
- Maximum de 20 URL par vérification.
- timeout : 30 secondes par URL.
- Données collectées par URL : URL, état d'accessibilité, code d'état HTTP, temps de réponse (ms), longueur du contenu, adresse IP résolue, version TLS et horodatage.
- Les résultats sont enregistrés dans reachability/reachability_results.json et reachability/reachability_summary.txt.



Paramètres de test de stratégie

- URL d'hôte : saisissez les hôtes pour le test des stratégies (séparées par des virgules, 10 au

maximum). Exemple : www.cisco.com.
- Les tests de stratégie sont exécutés par rapport au terminal de test de stratégie Cisco : policy.test.sse.cisco.com
- Les résultats incluent les résultats du test de stratégie structurée et les données HAR automatiquement capturées lors de la navigation du test.



Paramètres de capture HAR

- URL cibles : saisissez les URL de capture HAR (séparées par des virgules). Exemple : https://www.cisco.com/.

Conseil : La capture HAR prend actuellement en charge Google Chrome uniquement. L'outil utilise le protocole Chrome DevTools Protocol (via chromedp) pour automatiser une session Chrome sans tête et capturer le trafic réseau. Assurez-vous que Google Chrome est installé sur votre système. Firefox et Safari ne sont pas pris en charge pour le moment.



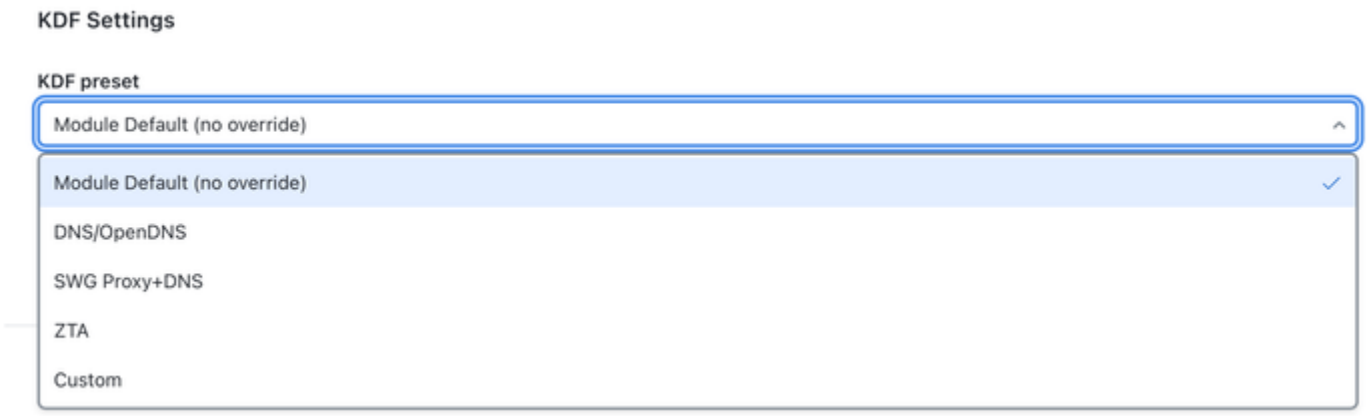
Paramètres KDF

Configurez les indicateurs de fonction de dérivation de clé utilisés lors de la collecte de diagnostics. Les indicateurs KDF contrôlent les catégories de débogage activées dans Cisco Secure Client :

- Préréglage KDF : sélectionnez un préréglage Fonction de dérivation de clé.
- KDF HEX - La valeur hexadécimale est automatiquement renseignée en fonction du préréglage sélectionné. Lorsque l'option Personnalisé est sélectionnée, entrez votre propre valeur hexadécimale.

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.





Paramètres IP réservés

- URL NSLookup : hôtes nslookup personnalisés facultatifs (séparés par des virgules). 10 URL maximum. Chaque hôte personnalisé est interrogé sur tous les résolveurs configurés.
- URL de suivi : hôtes traceroute/tracert personnalisés facultatifs (séparés par des virgules). 10 URL maximum. L'outil utilise automatiquement traceroute sur macOS/Linux et tracert sur Windows.
- Adresses IP de résolution : adresses IP de résolution personnalisées facultatives pour les requêtes nslookup (séparées par des virgules, telles que 208.67.222).
- 222, 208.67.220.220). 5 adresses IP maximum. Lorsqu'ils sont spécifiés, les résolveurs personnalisés sont utilisés en plus des trois résolveurs intégrés (DNS par défaut du système, 127.0.0.1, 208.67.222.222).



Détails IP réservés

Le diagnostic de l'adresse IP réservée collecte ces données par défaut :

Cibles Traceroute/Tracert par défaut (exécutées automatiquement sur toutes ces cibles) :

208.67.222.222Route vers le serveur de noms principal OpenDNS

Target	Objectif
208.67.220.220	Route vers le serveur de noms secondaire OpenDNS
146.112.255.50	Route vers IP d'infrastructure Cisco SWG
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	Route vers le nom d'hôte proxy SWG

- macOS/Linux : Utilise la commande traceroute
- Fenêtres: Utilise la commande tracert

Requêtes NSLookup par défaut (exécutées automatiquement sur toutes ces requêtes) :

Chaque cible nslookup est interrogée sur chaque résolveur de la liste. Par défaut, la liste des résolveurs inclut trois résolveurs intégrés :

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 des adresses IP de résolution personnalisées sont configurées (par exemple 208.67.222.222), elles sont ajoutées à la liste de résolution et chaque cible nslookup est également interrogée.

Cibles 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

Par exemple, avec les 3 résolveurs par défaut, cela produit 6 requêtes nslookup (2 cibles x 3 résolveurs). L'ajout d'une adresse IP de résolveur personnalisé porte ce nombre à 8 requêtes (2 cibles x 4 résolveurs).

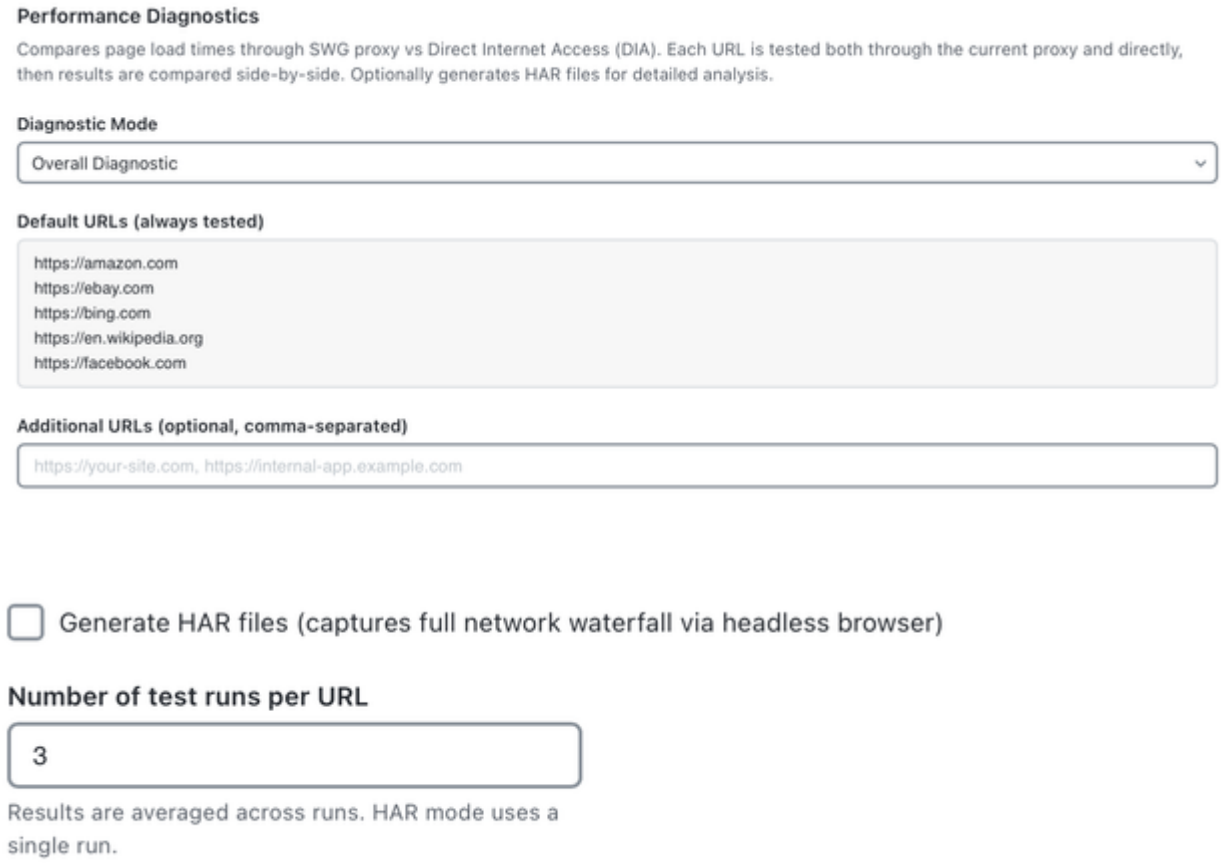
Les URL NSLookup personnalisées fournies par l'utilisateur sont interrogées sur la même liste de résolution complète (résolutions intégrées + résolutions personnalisées).

Tous les résultats sont consolidés dans un seul fichier : reserved_ip/reserved_ip_diagnostics.txt, regroupés par section (traceroute, nslookup) avec des en-têtes lisibles par l'utilisateur indiquant la cible et le résolveur pour chaque entrée.

Diagnostics des performances

Compare les temps de chargement des pages via le proxy SWG et l'accès direct à Internet (DIA). Il dispose de deux modes :

1. Mode de diagnostic global : Chaque URL est testée à la fois via le proxy actuel et directement, puis les résultats sont comparés côte à côte. Génère éventuellement des fichiers HAR pour une analyse détaillée.



2. Un mode de diagnostic d'URL : Nous pouvons entrer l'URL spécifique à tester à la fois via le proxy actuel et directement, puis les résultats sont comparés côte à côte. Génère éventuellement des fichiers HAR pour une analyse détaillée.



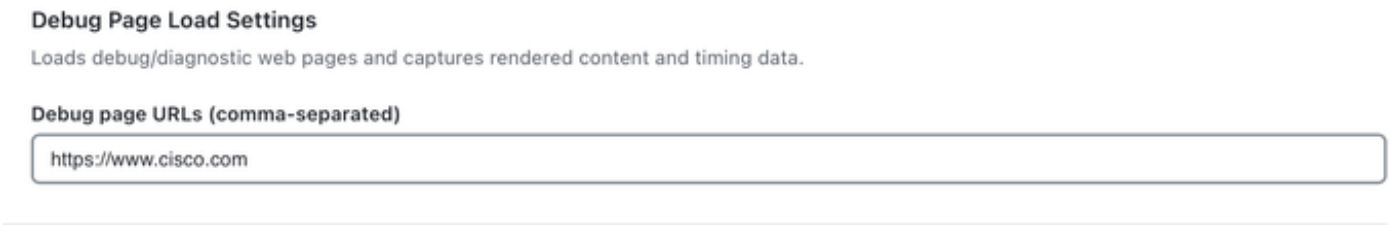
Paramètres du prix fixe du magasin de certificats

- Énumère les certificats des magasins de certificats configurés :
  - système
  - Connexion
  - Racine
  - Et plus encore
- Identifie rapidement les certificats manquants, expirés ou non fiables



Paramètres de chargement de la page de débogage :

- Charge les URL de débogage configurables.
- Captures:
  - En-têtes de réponse
  - Organisme de réaction
  - Informations de synchronisation
  - Métadonnées SSL



Actions

1. Complétez ou ajustez les paramètres de chaque diagnostic activé.
2. Cliquez sur Start Diagnostics pour commencer l'exécution du diagnostic.
3. Cliquez sur Back pour revenir à l'étape 1 ou sur Cancel pour quitter

---

Remarque : Les champs contenant des erreurs de validation sont mis en surbrillance. Vous devez les corriger avant que les tests de diagnostic puissent démarrer.

Suspendre et continuer

Lorsque vous exécutez une collection de diagnostics qui inclut un dépannage avancé (par exemple, le suivi ZTNA ou SWG), l'outil de diagnostic de point de terminaison Cisco peut marquer une pause au cours de l'exécution et vous demander de reproduire le problème avant qu'il ne se poursuive.

Cela vous donne le temps de déclencher le problème lorsque la journalisation détaillée est activée, de sorte que l'équipe d'assistance reçoit des données de diagnostic plus utiles.

- Lorsque la fenêtre Diagnostics Paused s'affiche, lisez le message - il vous indique quelles fonctionnalités de journalisation sont désormais actives.
- Reproduisez le problème que vous êtes en train de résoudre. Exemple :
  - Reconnecter au VPN
  - Ouvrez l'application interne défaillante
  - Répétez les étapes qui provoquent l'erreur
- Lorsque vous avez terminé de reproduire le problème, cliquez sur Continuer

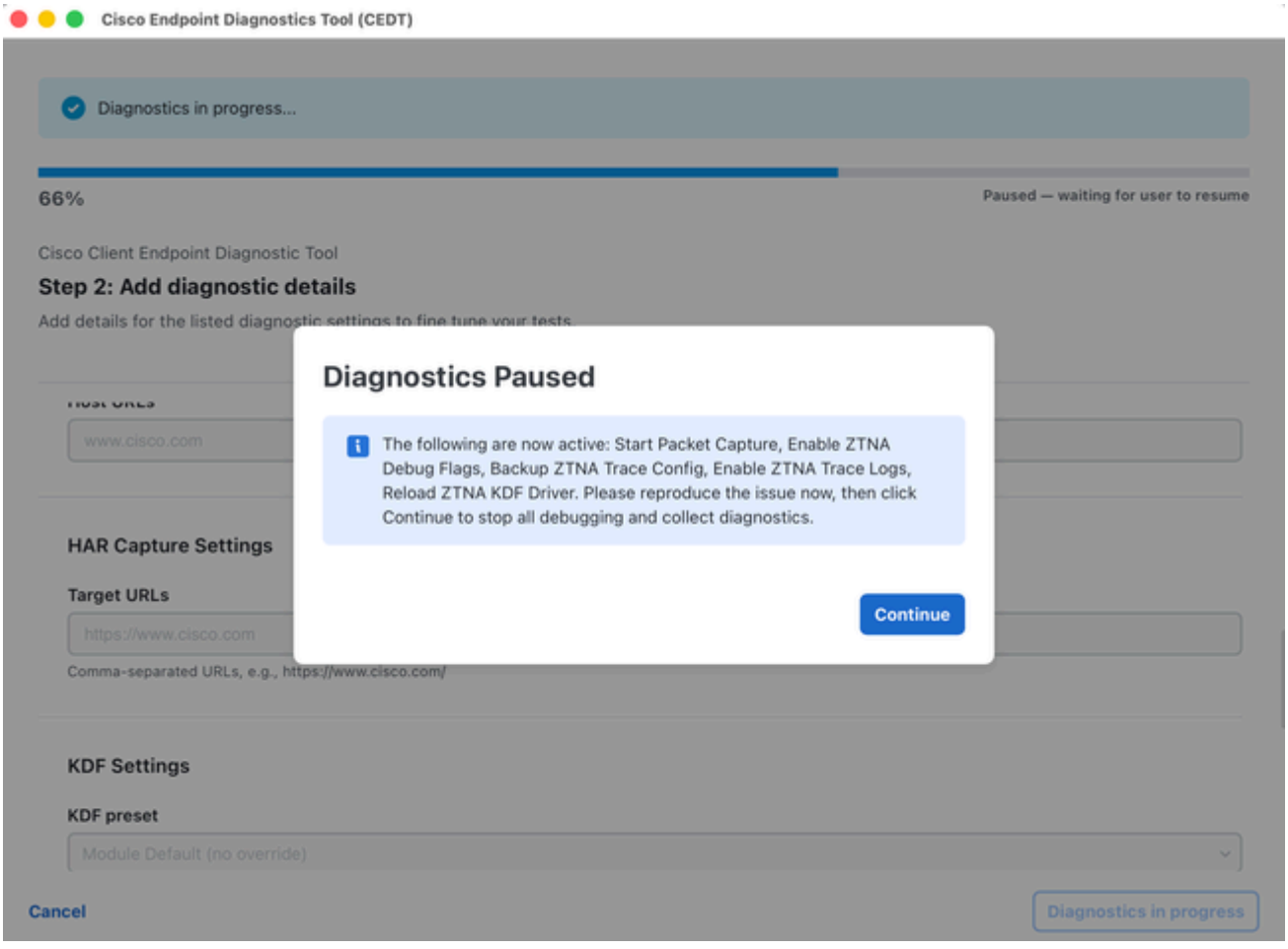
Laisse la course se terminer. L'outil collecte ensuite les fichiers, restaure vos paramètres normaux et crée l'archive de diagnostic.

Ne fermez pas l'application en pause. La journalisation reste active jusqu'à ce que vous cliquiez sur Continue et que l'exécution se termine.

(Ligne de commande)

Si vous exécutez l'outil à partir d'un terminal, vous pouvez voir un message de pause dans la fenêtre au lieu d'une boîte de dialogue.

1. Lisez le message de pause affiché dans le terminal.
2. Reproduisez le problème.
3. Retournez au terminal et appuyez sur Entrée pour continuer.
4. Attendez la fin de l'exécution.



Invite Privilèges administrateur

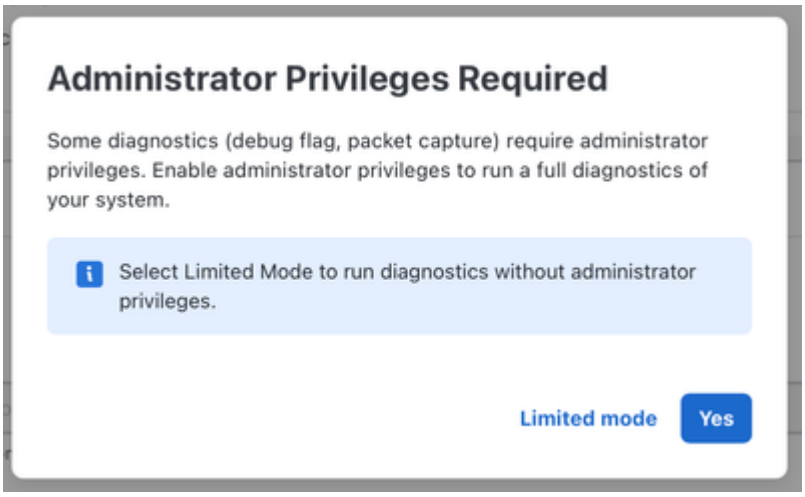
Après avoir cliqué sur Démarrer les diagnostics, l'outil peut vous demander des privilèges d'administrateur si vous avez activé des fonctionnalités qui nécessitent un accès élevé (telles que la capture de paquets ou les indicateurs de débogage).

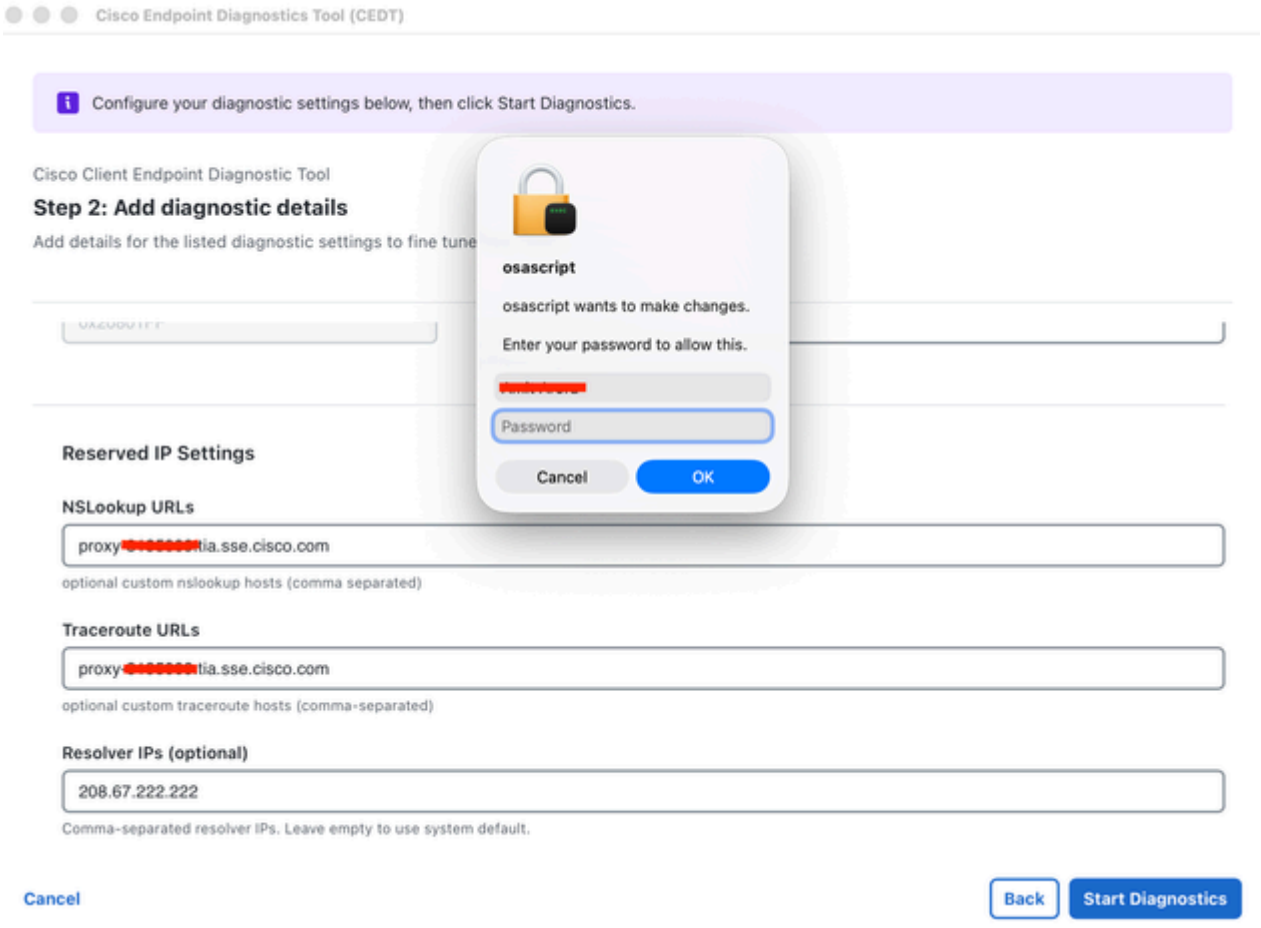
Une boîte de dialogue s'affiche avec le titre Privilèges administrateur requis :

- Cliquez sur Yes pour accorder des privilèges d'administrateur. Cela déclenche l'invite

d'informations d'identification macOS/Windows native.

- Cliquez sur Limited mode pour continuer sans élévation. Les tâches privilégiées (capture de paquets, indicateurs de débogage) sont ignorées.
- macOS : La boîte de dialogue de mot de passe macOS standard s'affiche dans osascript. Entrez votre mot de passe système et cliquez sur OK.
- Fenêtres: Une invite d'élévation UAC standard apparaît. Cliquez sur Yes pour autoriser.



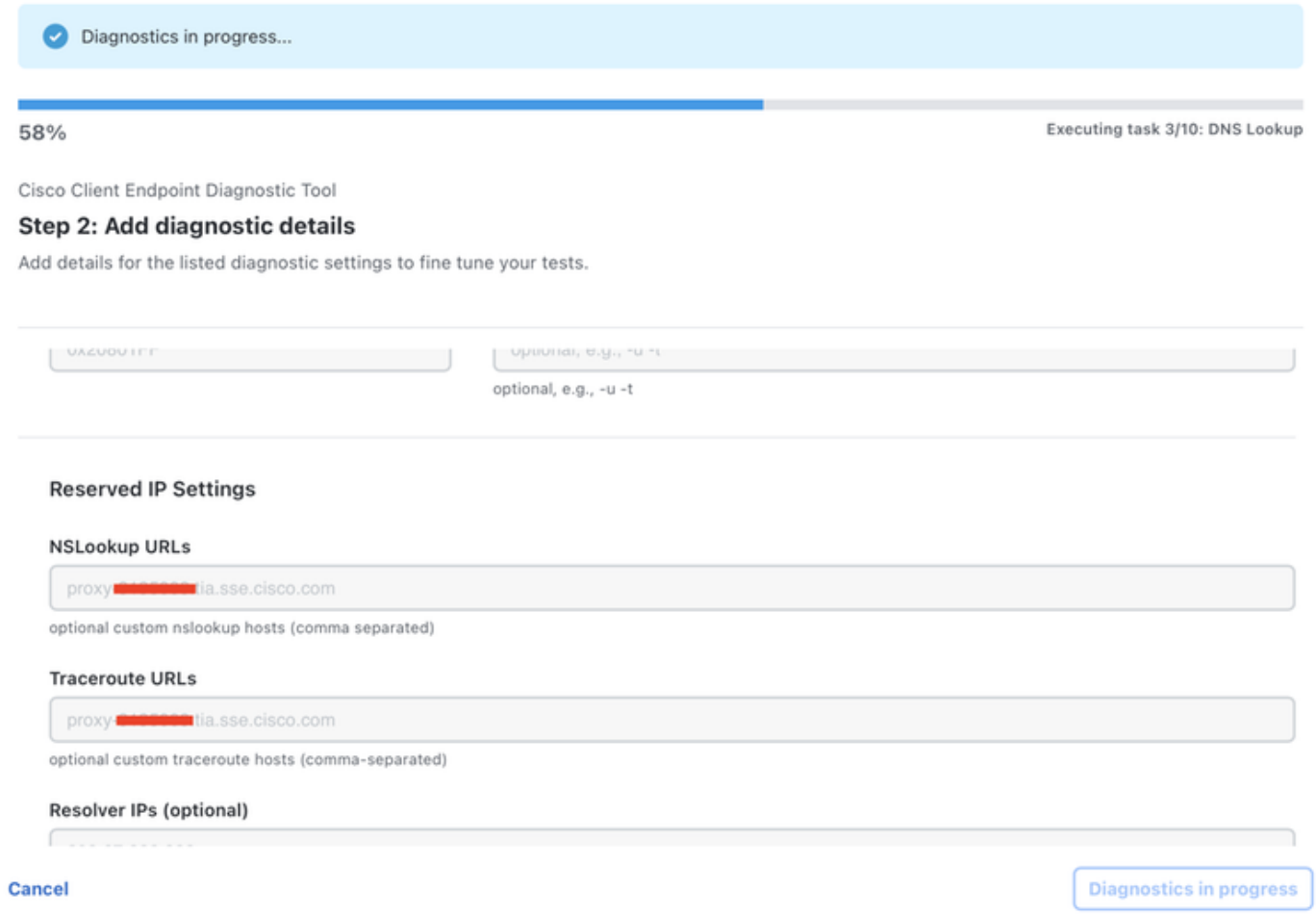


Diagnostics en cours

Une fois démarré, l'outil exécute toutes les tâches de diagnostic sélectionnées :

- Une barre de progression indique l'achèvement global (par exemple, 59 % - Exécution de la tâche 3/9 : Recherche DNS).
- Une bannière Diagnostics en cours... s'affiche en haut.
- Tous les champs de paramètres sont désactivés/grisés pendant l'exécution.
- Le pied de page affiche un bouton Diagnostics en cours (désactivé) pour indiquer que l'outil est occupé.

Patientez pendant la fin des tests de diagnostic. Ne fermez pas l'application.



Diagnostics terminés - Téléchargement vers le TAC

Lorsque tous les diagnostics sont terminés, une boîte de dialogue de fin apparaît :

Diagnostic terminé. Téléchargez le fichier dans un dossier TAC.

La boîte de dialogue affiche :

- Archive : nom de fichier de l'archive de diagnostic générée (par exemple, cisco_diagnostics.tar.gz).
- Taille du fichier : taille de l'archive (par exemple, 7,72 Mo).
- SHA256 - Somme de contrôle du fichier d'archive pour la vérification de l'intégrité.

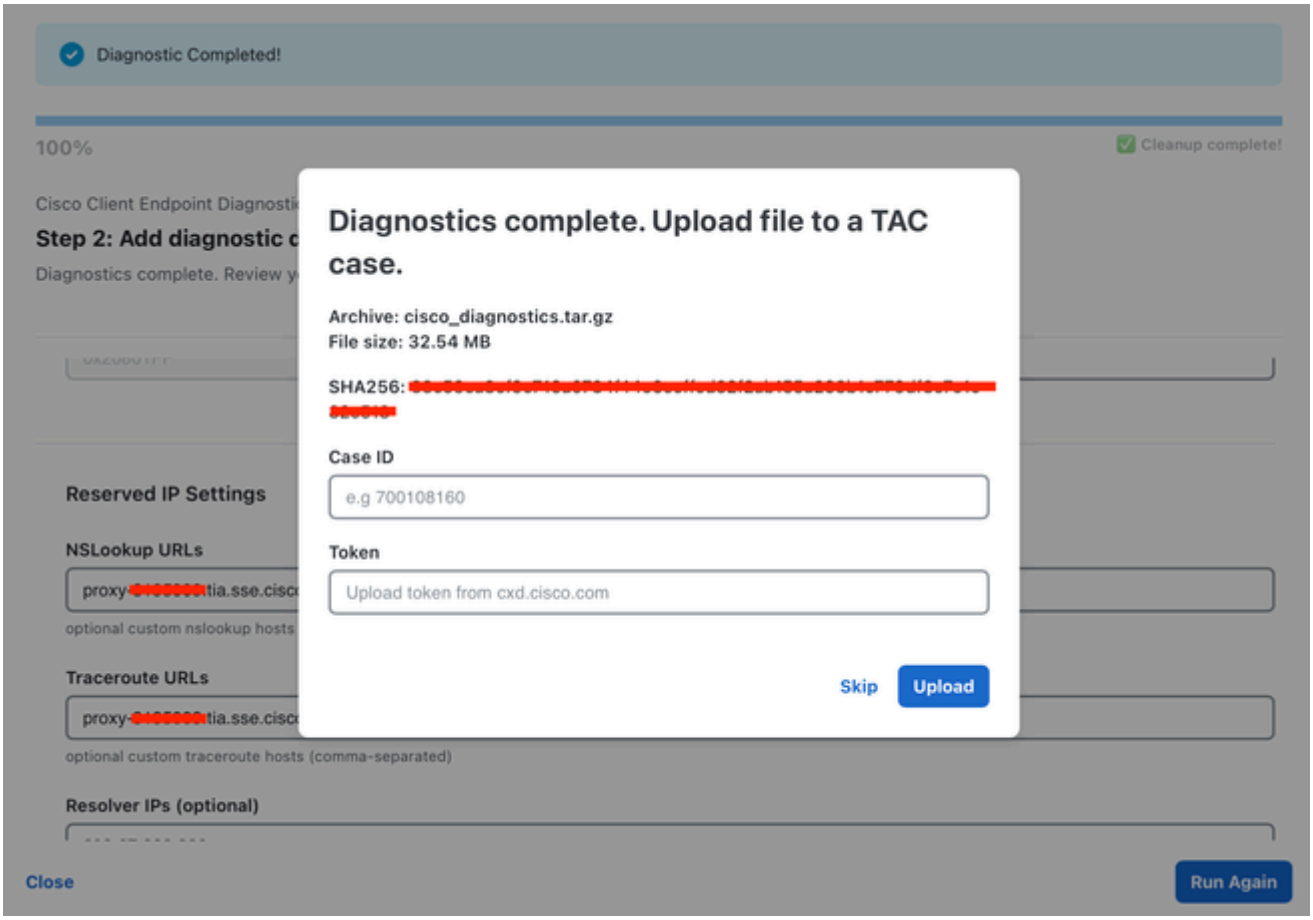
Pour effectuer un téléchargement vers un dossier TAC :

1. Saisissez votre ID de dossier (par exemple 698746730).
2. Saisissez votre jeton (fourni par l'assistance Cisco).
3. Cliquez sur Open TAC Case pour démarrer le téléchargement.

Une barre de progression indique l'état du téléchargement (par exemple, Téléchargement... 85,0 % (6,56 Mo / 7,72 Mo).

Pour ignorer le téléchargement :

- Cliquez sur Ignorer pour fermer la boîte de dialogue sans télécharger. Le fichier d'archive est toujours enregistré localement.



Téléchargement terminé - Écran final

Après un téléchargement réussi, la bannière de fin est mise à jour vers :

Archive de diagnostic téléchargée vers le dossier [ID du dossier]

La barre de progression affiche 100 % avec l'état Nettoyage terminé.

Actions

- Cliquez sur Exécuter à nouveau pour démarrer une nouvelle exécution de diagnostic.
- Cliquez sur Close pour quitter l'application.

Emplacement de sortie

Le résultat du diagnostic est enregistré dans :

- macOS : ~/Bureau/diagnostics_cisco/
- Fenêtres: %USERPROFILE%\Desktop\cisco_diagnostics\

Le fichier d'archive de sortie (cisco_diagnostics.tar.gz) contient toutes les données de diagnostic collectées dans un format structuré.

Dépannage

Issue	Resolution
No products detected	Ensure Cisco Secure Client is installed and running on your system.
Packet Capture greyed out	Enable it in Step 1, and grant administrator privileges when prompted.
Debug Flags greyed out	At least one Cisco Secure Access product must be detected and selected.
DebugView greyed out	This option is only available on Windows.
Upload fails	Verify your Case ID and Token are correct. Check your internet connection.
"Administrator credentials could not be obtained"	You cancelled the password prompt or entered an incorrect password. Click Start Diagnostics again to retry.
Limited mode warning	Some privileged tasks were skipped. Re-run with administrator privileges for a full diagnostic.

FAQ

Q : Quelles données cet outil collecte-t-il ?
A : L'outil collecte des informations système (système d'exploitation, matériel, configuration réseau), des journaux d'applications, des données de configuration des produits et des modules installés Cisco, ainsi que des données de diagnostic du réseau relatives aux modules d'accès sécurisé Cisco uniquement. Reportez-vous à la section Quelles données système sont collectées dans la section précédente pour une répartition détaillée. Aucune donnée personnelle n'est capturée.

Q : Ai-je besoin d'un accès administrateur/racine ?
A : L'accès administrateur est facultatif mais recommandé. Sans elle, certains diagnostics (capture de paquets, indicateurs de débogage) sont ignorés. L'outil vous invite et vous permet de choisir.

Q : Puis-je exécuter l'outil plusieurs fois ?
A : Oui. Une fois chaque exécution terminée, vous pouvez cliquer sur « Exécuter à nouveau » pour lancer une nouvelle session de diagnostic.

Q : Où est enregistré le résultat ?
A : L'archive de diagnostic est enregistrée sur votre Bureau dans le dossier cisco_diagnostics.

Q : Que faire si je n'ai pas d'ID de dossier TAC ?
A : Cliquez sur Ignorer dans la boîte de dialogue de téléchargement. Le fichier d'archive est toujours enregistré localement. Vous pouvez le télécharger manuellement sur un dossier TAC ultérieurement ou le partager avec votre ingénieur du support technique.

Q : Les données sont-elles chiffrées ?
A : L'archive de diagnostic est compressée (tar.gz) et les données sensibles sont automatiquement effacées avant l'empaquetage.

Q : Quels navigateurs la capture HAR prend-elle en charge ?
A : La capture HAR prend actuellement en charge Google Chrome uniquement. L'outil utilise le Chrome DevTools Protocol pour l'automatisation du navigateur sans tête. Assurez-vous que Chrome est installé avant d'exécuter la capture HAR.

Q L'écran de pause n'est jamais apparu. Quelque chose ne va pas ?

A : Pas nécessairement. L'étape de pause apparaît uniquement lorsque la journalisation détaillée a été correctement activée pour votre scénario. Vérifiez le journal d'exécution dans l'application ; si les étapes enable ont été ignorées, l'outil continue sans s'arrêter.

Q La course semble bloquée. Que dois-je faire ?

A : Recherchez la fenêtre Diagnostics Paused - elle peut se trouver derrière d'autres fenêtres. L'exécution n'avance pas tant que vous n'avez pas cliqué sur Continue (ou appuyé sur Enter dans la ligne de commande).

A : Oui. Le message indique les fonctions de journalisation activées par l'outil pour votre plate-forme et les options de diagnostic que vous avez sélectionnées.

A : Réexécutez la collection de diagnostics et laissez-la se terminer. Si vous ne savez pas si la journalisation a été laissée, contactez votre ingénieur du support technique pour obtenir des conseils.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.