

Activer le débogage sur le terminal à partir d'AMP for Endpoint Console

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Configurer](#)

[Étape 1 : Identifiez le terminal à déplacer vers le débogage](#)

[Étape 2 : dupliquer la stratégie existante](#)

[Étape 3 : Configurez le niveau de journalisation pour déboguer cette stratégie](#)

[Étape 4 : Créez un nouveau groupe et liez cette nouvelle stratégie](#)

[Étape 5 : Déplacez le point de terminaison identifié vers ce nouveau groupe](#)

[Étape 6 : Vérifiez le terminal dans la page de l'ordinateur et dans l'interface utilisateur du connecteur](#)

Introduction

Ce document décrit comment activer le débogage sur le terminal à partir de Cisco Secure Endpoint Console.

Conditions préalables

Exigences

Avant de commencer, assurez-vous d'avoir :

- Accès administratif à la console Cisco Secure Endpoint for Endpoints.
- Le terminal que vous souhaitez déboguer est déjà enregistré dans Cisco Secure Endpoint

Composants utilisés

Les informations utilisées dans le document sont basées sur les versions logicielles suivantes :

- Cisco Secure Endpoint Console version 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 et versions ultérieures
- Système d'exploitation Microsoft Windows

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les données de diagnostic générées peuvent être transmises au centre d'assistance technique Cisco (TAC) pour une analyse plus approfondie.

Les données de diagnostic comprennent des informations telles que :

- Utilisation des ressources (disque, processeur et mémoire)
- Journaux spécifiques au connecteur
- Informations de configuration du connecteur

Problème

L'activation du débogage sur le terminal à partir de Cisco Secure Endpoint Console est requise dans l'un de ces scénarios.

Scénario 1 : si vous redémarrez le périphérique, activez le mode de débogage à partir de l'interface de la barre d'état IP ou il ne survit pas au redémarrage. Si des journaux de débogage de démarrage sont requis, vous pouvez activer le mode Débogage à partir de la configuration de la stratégie dans la console Secure Endpoint.

Scénario 2 : si vous rencontrez des problèmes de performances avec Cisco Secure Endpoint Connector sur un périphérique, l'activation du mode Débogage peut vous aider à collecter des journaux détaillés pour analyse.

Scénario 3 : lors du dépannage de problèmes spécifiques avec Secure Endpoint Connector, des journaux détaillés peuvent fournir des informations sur la cause première du problème.

Configurer

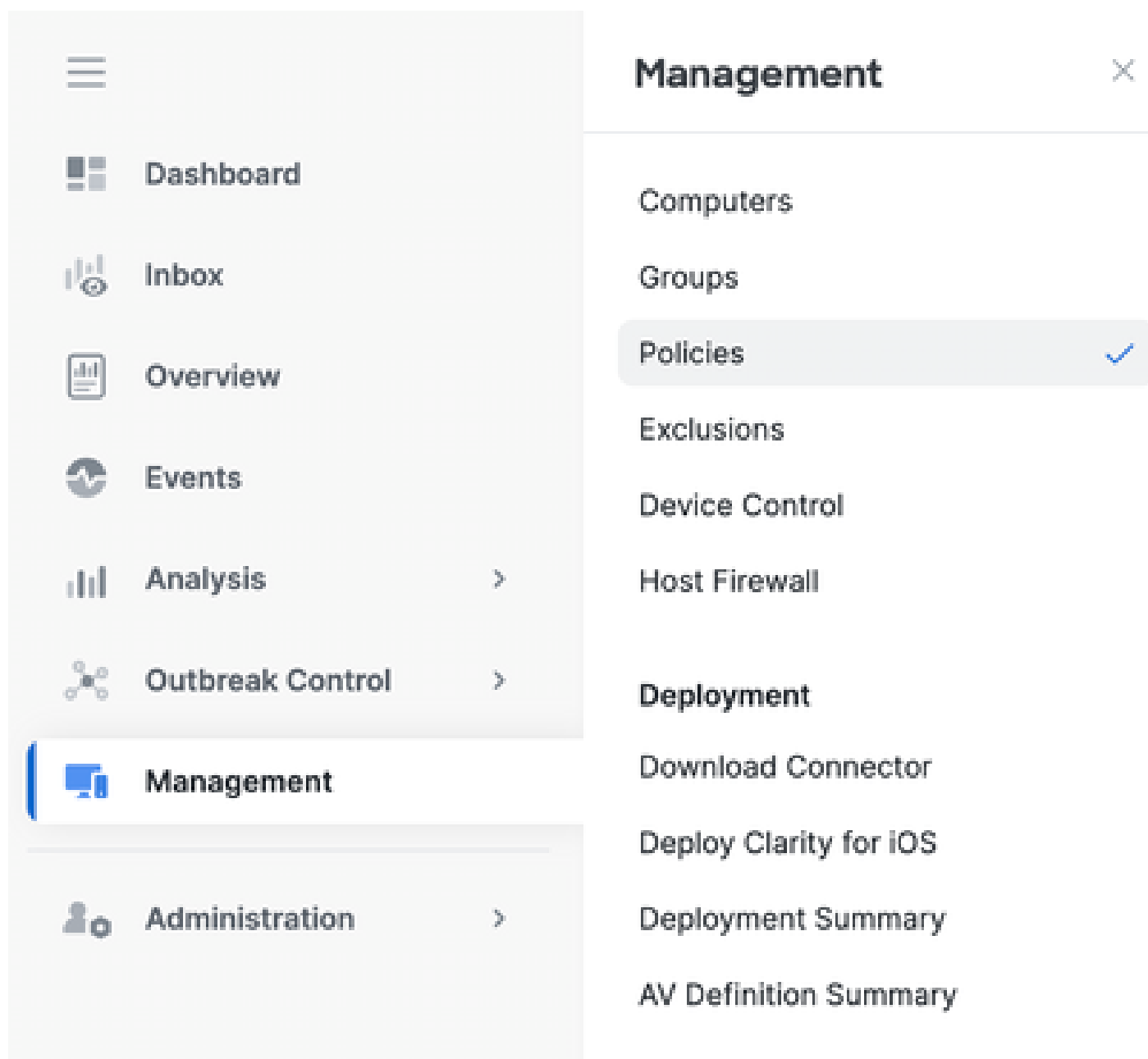
Suivez ces étapes pour activer correctement le mode de débogage sur le point de terminaison spécifié via la console Secure Endpoint.

Étape 1 : Identifiez le terminal à déplacer vers le débogage

1. Connectez-vous à la console Cisco Secure Endpoint. Dans le tableau de bord principal, accédez à la section Gestion.
2. Accédez à Gestion > Ordinateurs.
3. Identifiez et notez le point de terminaison qui nécessite le mode de débogage.

Étape 2 : dupliquer la stratégie existante

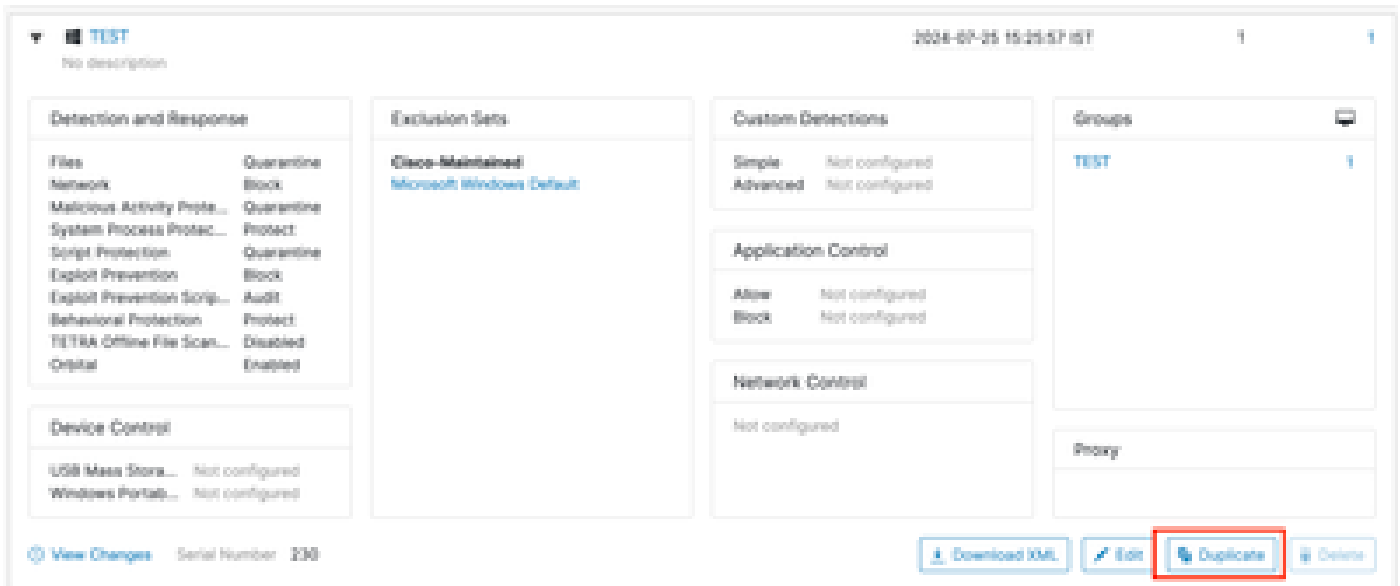
1. Accédez à Management > Politiques.



2. Localisez la stratégie actuellement appliquée au point de terminaison identifié.

3. Cliquez sur la stratégie pour développer la fenêtre de stratégie.

4. Cliquez sur Dupliquer pour créer une copie de la règle existante.



Étape 3 : Configurez le niveau de journalisation pour déboguer cette stratégie

1. Sélectionnez et développez la fenêtre Stratégie dupliquée.
2. Cliquez sur Edit et renommez la stratégie (par exemple, Debug TechZone Policy).
3. Cliquez sur Advanced Settings.
4. Sélectionnez Administrative Features dans la barre latérale.
5. Définissez à la fois Connector Log Level et Tray Log Level sur Debug.
6. Cliquez sur Save pour enregistrer les modifications.

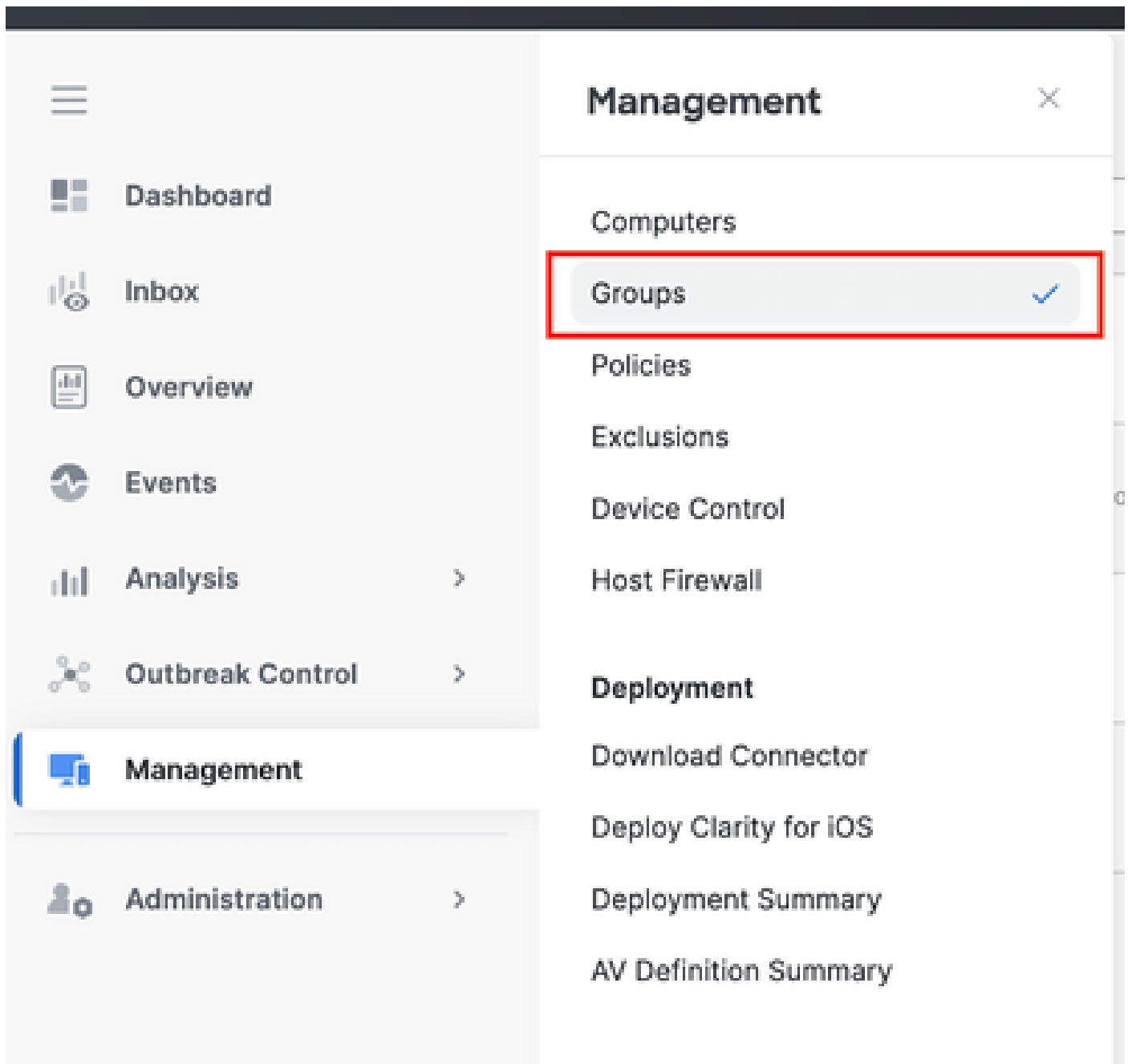
The screenshot shows the 'Edit Policy' page for a policy named 'Debug TechZone Policy'. The description is 'Taking debug on endpoint'. The left sidebar contains several categories: Modes and Engines, Exclusions, Proxy, Host Firewall, Outbreak Control, Device Control, Product Updates, Advanced Settings (highlighted), Administrative Features (highlighted with a red box), Client User Interface, File and Process Scan, Cache, Endpoint Isolation, Orbital, Engines, TETRA, Network, and Scheduled Scans. The main content area displays various settings:

- Send User Name in Events ⓘ
- Send Filename and Path Info ⓘ
- Heartbeat Interval: 15 minutes ⓘ
- Connector Log Level: Debug ⓘ (highlighted with a red box)
- Tray Log Level: Debug ⓘ (highlighted with a red box)
- Enable Connector Protection ⓘ
- Connector Protection Password: ⓘ
- Automated Crash Dump Uploads ⓘ
- Command Line Capture ⓘ
- Command Line Logging ⓘ

At the bottom right, there are 'Cancel' and 'Save' buttons.

Étape 4 : Créez un nouveau groupe et liez cette nouvelle stratégie

1. Accédez à Gestion > Groupes.



2. Cliquez sur Create Group (Créer un groupe) en haut à droite de votre écran.
3. Entrez un nom pour le groupe (par exemple, Debug TechZone Group.)
4. Remplacez la stratégie par défaut par la nouvelle stratégie de débogage.
5. Cliquez sur Enregistrer.

← Groups

New Group

Name	Debug TechZone Group
Description	This Group is used to Debug Cisco Secure Endpoint Connector
Parent Group	
Windows Policy	Debug TechZone Policy
Android Policy	Default Policy (Protect)
Mac Policy	Default Policy (Audit)
Linux Policy	Default Policy (Audit)
Network Policy	Default Policy (Default Network)
iOS Policy	Default Policy (Audit)

[Cancel](#) [Save](#)

Computers

Assign computers from the Computers page after you have saved the new group

Étape 5 : Déplacez le point de terminaison identifié vers ce nouveau groupe

1. Revenez à Gestion > Ordinateurs.



Management [X]

- Computers ✓
- Groups
- Policies
- Exclusions
- Device Control
- Deployment
- Download Connector
- Deploy Clarity for iOS
- Deployment Summary
- AV Definition Summary

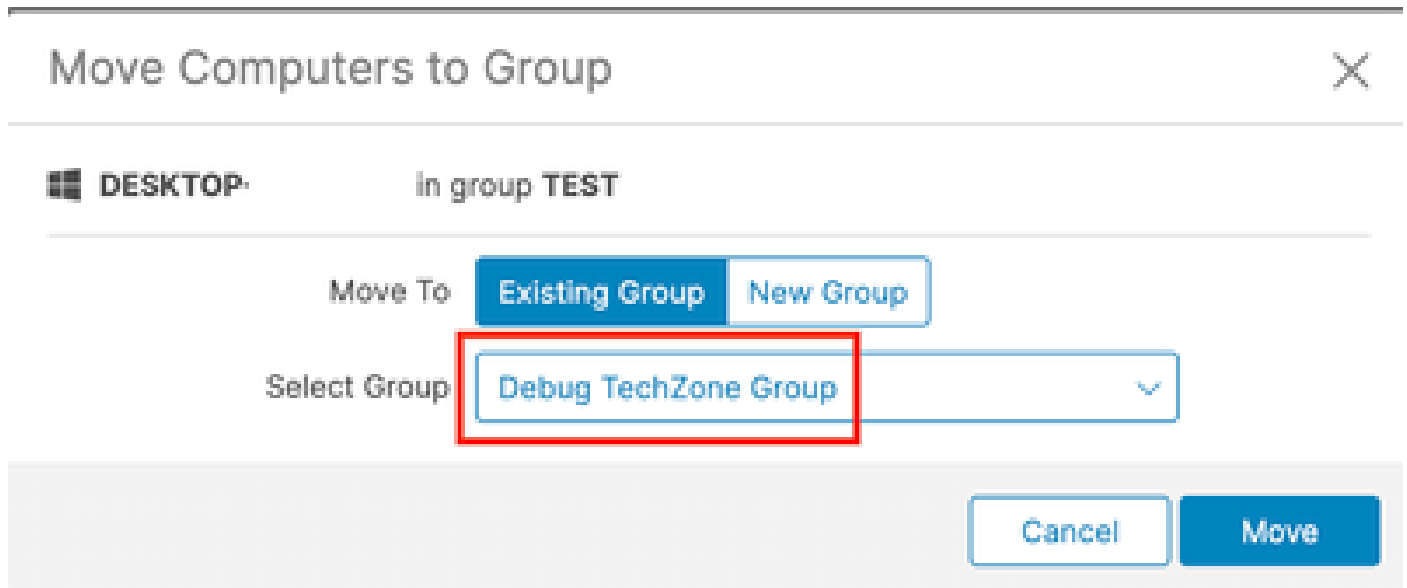
2. Sélectionnez le terminal identifié dans la liste.

3. Cliquez sur Déplacer vers le groupe.

Hostname	DESKTOP-...	Group	TEST
Operating System	Windows 10 Pro (Build 19045.4620)	Policy	TEST
Connector Version	8.4.0.20201 Show download URL	Internal IP	
Install Date	2024-07-25 15:00:13 IST	External IP	
Connector GUID	20240725-060a-4784-a0d8-c885a8884640	Last Seen	2024-07-25 15:42:55 IST
Processor ID	09a50f00000000000000000000000000	AV signature version	10004
Cisco Secure Client ID	NA	Cisco Security Risk Score	Pending...

[Take Forensic Snapshot](#) [View Snapshot](#) [Investigate in Orbital](#) [Scan...](#) [Deploy...](#) **[Move to Group...](#)** [Uninstall Connector](#) [Delete](#)

4. Sélectionnez le groupe nouvellement créé dans le menu déroulant Sélectionner un groupe.
5. Cliquez sur Déplacer pour déplacer le point de terminaison sélectionné dans le nouveau groupe.



Étape 6 : Vérifiez le terminal dans la page de l'ordinateur et dans l'interface utilisateur du connecteur

1. Assurez-vous que le point de terminaison est répertorié sous le nouveau groupe dans la page Ordinateurs.
2. Sur le point de terminaison, ouvrez l'interface utilisateur du connecteur Secure Endpoint.
3. Vérifiez que la nouvelle stratégie de débogage est appliquée en cliquant sur l'icône Secure Endpoint dans la barre de menus.



Secure Client

Secure Endpoint

Statistics Update Advanced

Agent

Status: Connected
Version: 8.4.0.30201
GUID: 202dac7b-093a-4784-ace8-cb95e8696c96
Last Scan: Today 03:03:18 PM
Isolation: Not Isolated

Policy

Name: Debug TechZone Policy
Serial Number: 229
Last Update: Today 03:52:38 PM

Cisco Secure Client



Secure Endpoint:

Connected.

Flash Scan

Start



Remarque : le mode débogage ne peut être activé que si un ingénieur du support technique Cisco demande ces données. Le fait de conserver le mode de débogage activé pendant une période prolongée peut rapidement remplir l'espace disque et empêcher la collecte des données du journal du connecteur et du journal de la barre d'état dans le fichier de diagnostic du support en raison d'une taille de fichier excessive.

Contactez l'assistance Cisco pour obtenir de l'aide.

[Coordonnées du service d'assistance Cisco à l'échelle mondiale](#)

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.