

Cisco Secure Endpoint Connector pour Mac Diagnostic Data Collection

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Générer un fichier de diagnostic avec l'outil de support](#)

[Lancer l'outil de support à l'aide de macOS Finder](#)

[Lancer l'outil de support à l'aide de macOS Terminal](#)

[Dépannage](#)

[Activer le mode débogage](#)

[Activer le mode de débogage à pulsation unique](#)

[Désactiver le mode débogage](#)

Introduction

Ce document décrit le processus utilisé afin de générer un fichier de diagnostic via l'application Support Tool qui est disponible sur le connecteur Mac Cisco Secure Endpoint et comment dépanner les problèmes de performances.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur Mac pour terminal sécurisé
- macOS

Components Used

Les informations de ce document sont basées sur le connecteur Mac Secure Endpoint.

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Le connecteur Secure Endpoint Mac regroupe une application appelée Support Tool, qui est

utilisée pour générer des informations de diagnostic sur le connecteur installé sur votre Mac. Les données de diagnostic incluent des informations sur votre Mac telles que :

- Utilisation des ressources (disque, processeur et mémoire)
- diagraphies spécifiques aux connecteurs
- information de configuration du connecteur

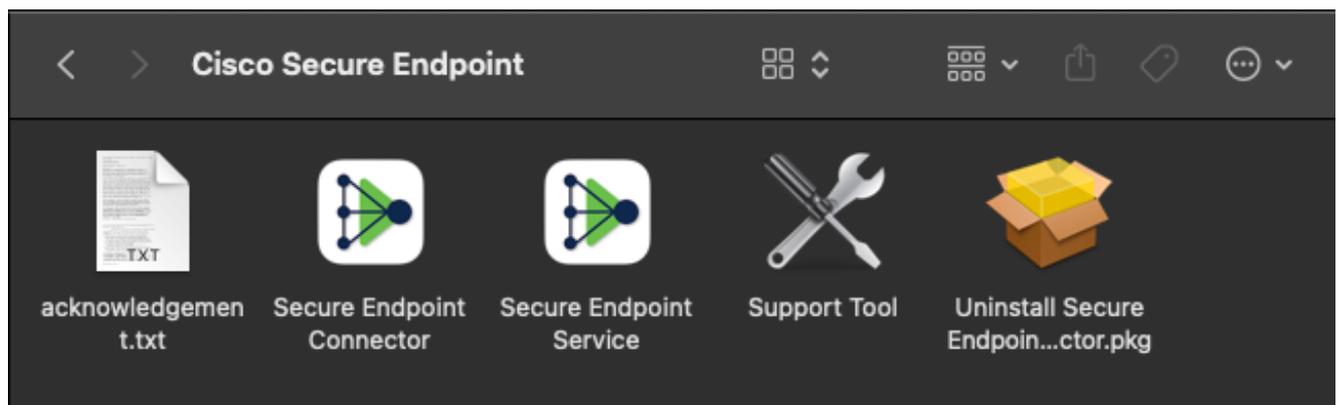
Générer un fichier de diagnostic avec l'outil de support

Cette section décrit comment lancer l'application Support Tool à partir de l'interface utilisateur graphique ou de l'interface de ligne de commande afin de générer un fichier de diagnostic.

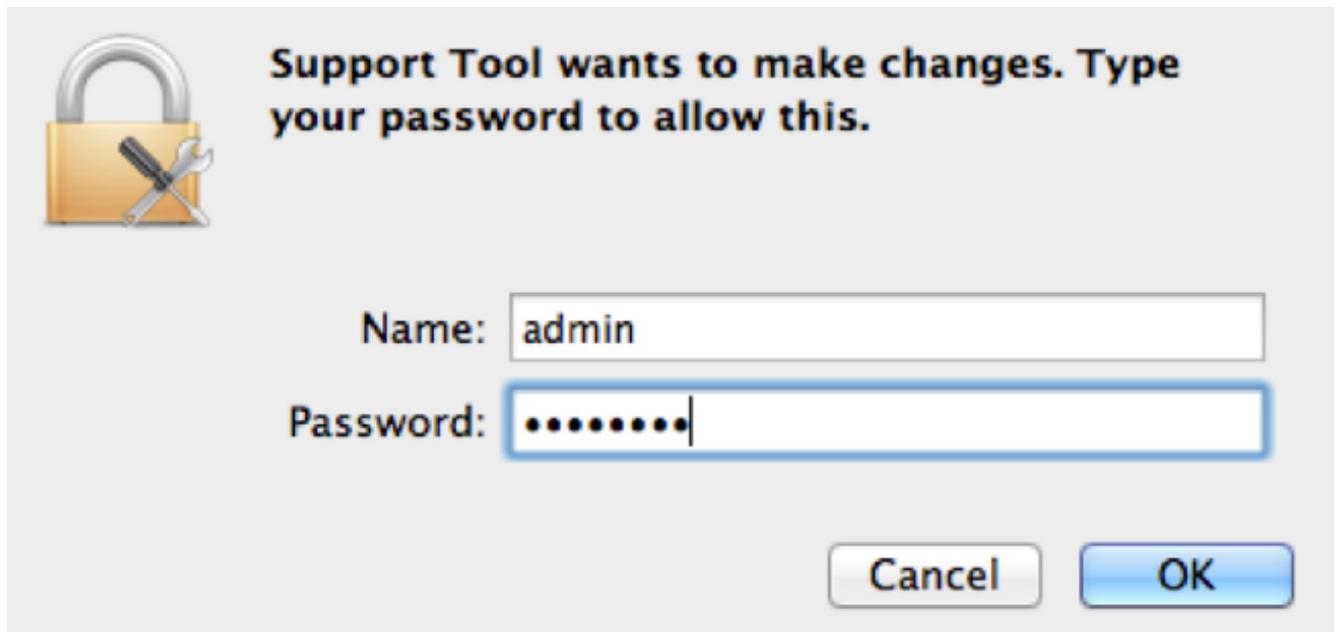
Lancer l'outil de support à l'aide de macOS Finder

Complétez ces étapes afin de lancer l'outil de support du connecteur Mac Secure Endpoint à l'aide du Finder macOS :

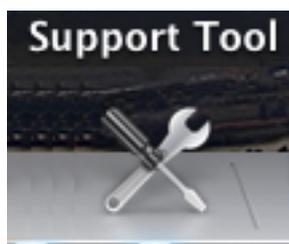
1. Accédez au répertoire Cisco Secure Endpoint dans votre dossier Applications et localisez le lanceur de l'outil de support :



2. Double-cliquez sur le lanceur de l'outil de support et vous êtes invité à saisir les informations d'identification d'administration :

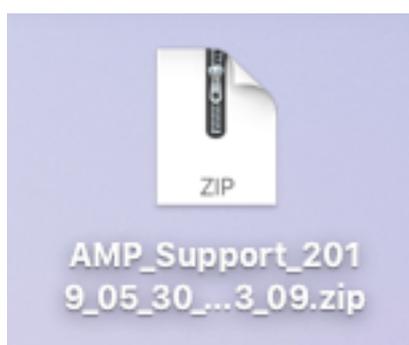


3. Une fois que vous avez saisi vos informations d'identification, l'icône Support Tool devrait apparaître dans votre dock :

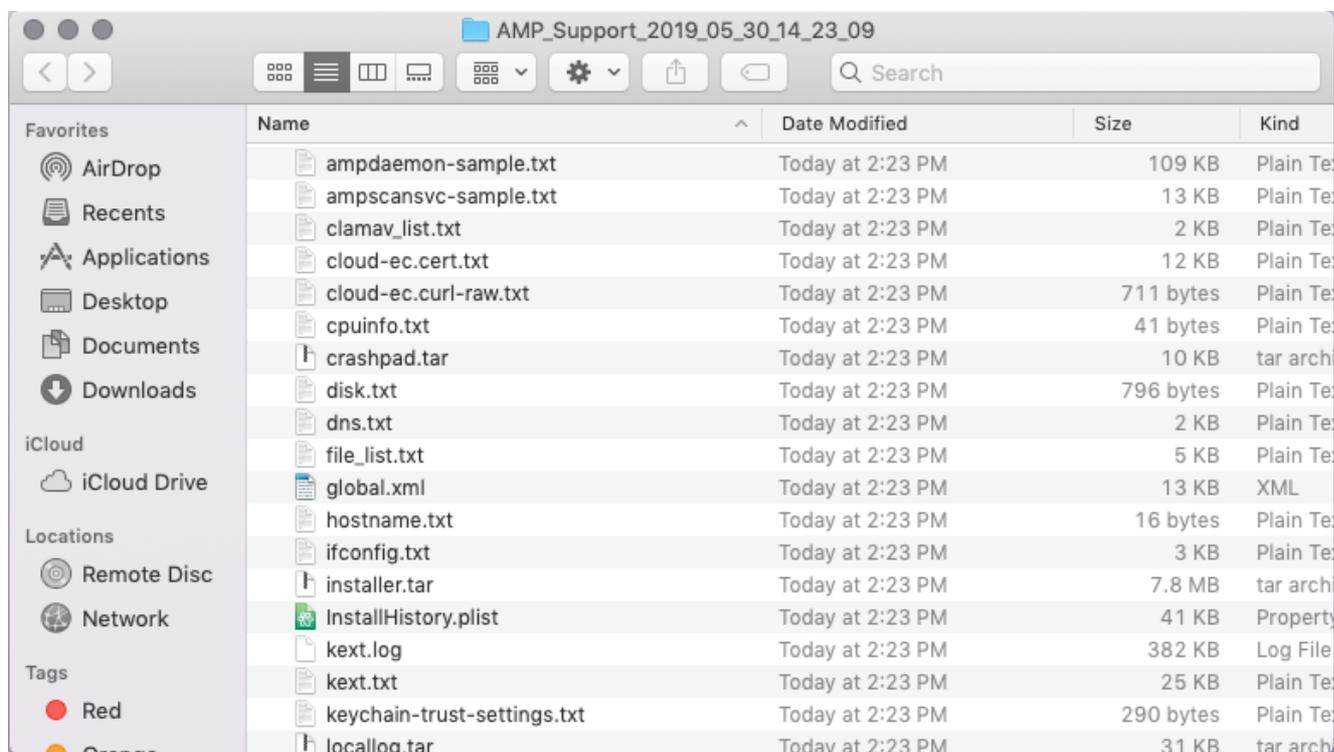


Note: L'application Support Tool s'exécute en arrière-plan et prend un certain temps (environ 20 à 30 minutes).

4. Une fois l'application Support Tool terminée, un fichier est généré et placé sur votre bureau :



Voici un exemple de sortie non compressée :



5. Afin d'analyser les données, fournissez ce fichier à l'équipe d'assistance technique de Cisco.

Lancer l'outil de support à l'aide de macOS Terminal

Le lanceur de l'outil de support se trouve dans le répertoire suivant :

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

Pour lancer l'application Support Tool, entrez la commande suivante :

Note: Vous devez exécuter cette commande en tant que root, donc assurez-vous que vous basculez vers root ou préfacez la commande avec **sudo**.

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#  
./SupportTool
```

Note: Cette commande s'exécute verbalement. Une fois terminé, un fichier de diagnostic est généré et placé sur votre bureau.

Dépannage

Cette section décrit comment activer et désactiver le mode de débogage sur le connecteur Mac Secure Endpoint afin de résoudre les problèmes de performances.

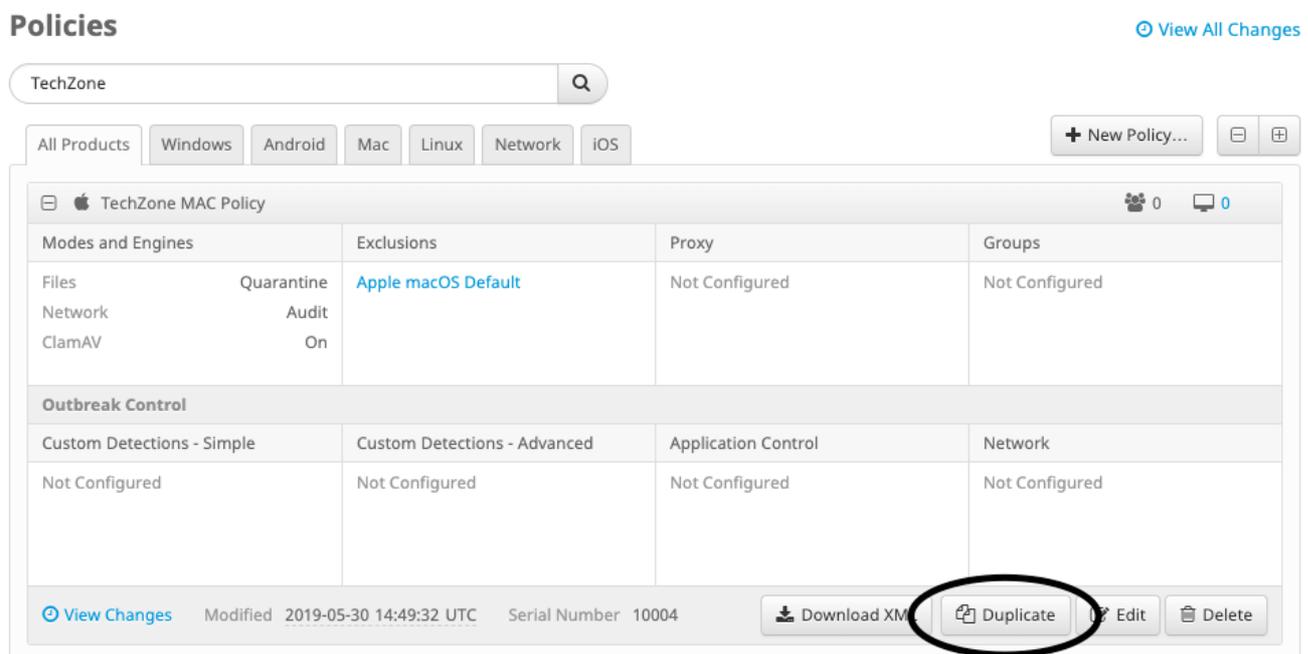
Activer le mode débogage

Avertissement : le mode débogage ne doit être activé que si un ingénieur du support technique Cisco demande ces données. Si vous maintenez le mode de débogage activé

pendant une période prolongée, il peut remplir l'espace disque très rapidement et peut 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 de la taille excessive du fichier.

Le mode débogage est utile pour tenter de résoudre les problèmes de performances sur un connecteur Secure Endpoint. Complétez ces étapes afin d'activer le mode de débogage et de recueillir des données de diagnostic ;

1. Connectez-vous à la console Secure Endpoint.
2. Accédez à **Management > Politiques**.
3. Recherchez une stratégie appliquée à un ordinateur, cliquez sur la stratégie qui développera la fenêtre de stratégie, puis cliquez sur **Dupliquer**. Secure Endpoint Console se met à jour avec la stratégie dupliquée :



Policies View All Changes

TechZone

All Products Windows Android Mac Linux Network iOS + New Policy...

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	Apple macOS Default	Not Configured	Not Configured
Network	Audit			
ClamAV	On			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

View Changes Modified 2019-05-30 14:49:32 UTC Serial Number 10004 Download XML **Duplicate** Edit Delete

4. Sélectionnez et développez la fenêtre de stratégie en double, puis cliquez sur **Modifier** et modifiez le nom de la stratégie. Par exemple, vous pouvez utiliser *Debug TechZone MAC Policy*.
5. Cliquer **Paramètres avancés**, sélectionnez **Fonctions administratives** dans la barre latérale et sélectionnez **Débugger** pour les menus déroulants Log Level et Tray Log Level du connecteur :

Name

Description

Modes and Engines

Exclusions
1 exclusion set

Proxy

Outbreak Control

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

ClamAV

Network

Scheduled Scans

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

6. Cliquez sur le bouton **Enregistrer** afin d'enregistrer les modifications.
7. Naviguez jusqu'à **Gestion > Groupes** et cliquez sur **Créer un groupe** près du côté supérieur droit de votre écran.
8. Entrez un nom pour le groupe. Par exemple, vous pouvez *utiliser Debug TechZone Mac Group*.

< **New Group** ?

Name

Description

Parent Group

Windows Policy

Android Policy

Mac Policy

Linux Policy

Network Policy

iOS Policy

Computers

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

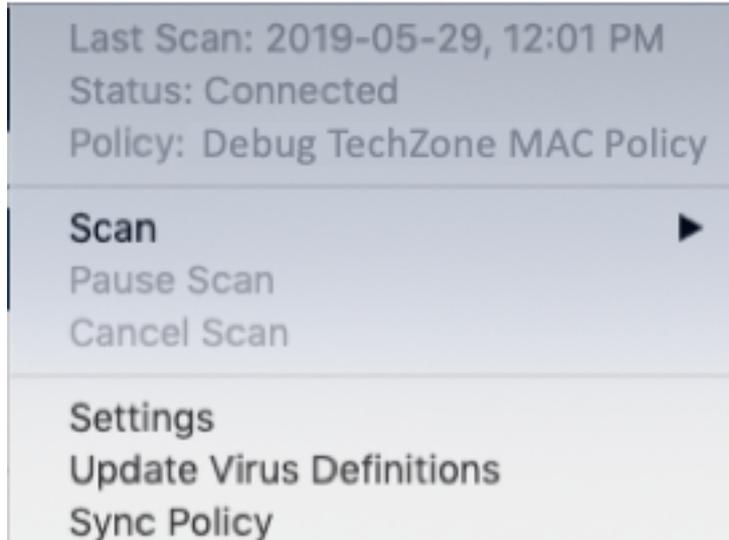
9. Modifier la stratégie Mac de *Stratégie Mac par défaut* à la nouvelle stratégie dupliquée que vous venez de créer, qui est **Debug TechZone Mac Policy** dans cet exemple.

Cliquer **Enregistrer**.

10. Naviguez jusqu'à **Gestion > Ordinateurs** et identifiez votre ordinateur dans la liste.

Sélectionnez-le et cliquez sur **Déplacer vers le groupe....**

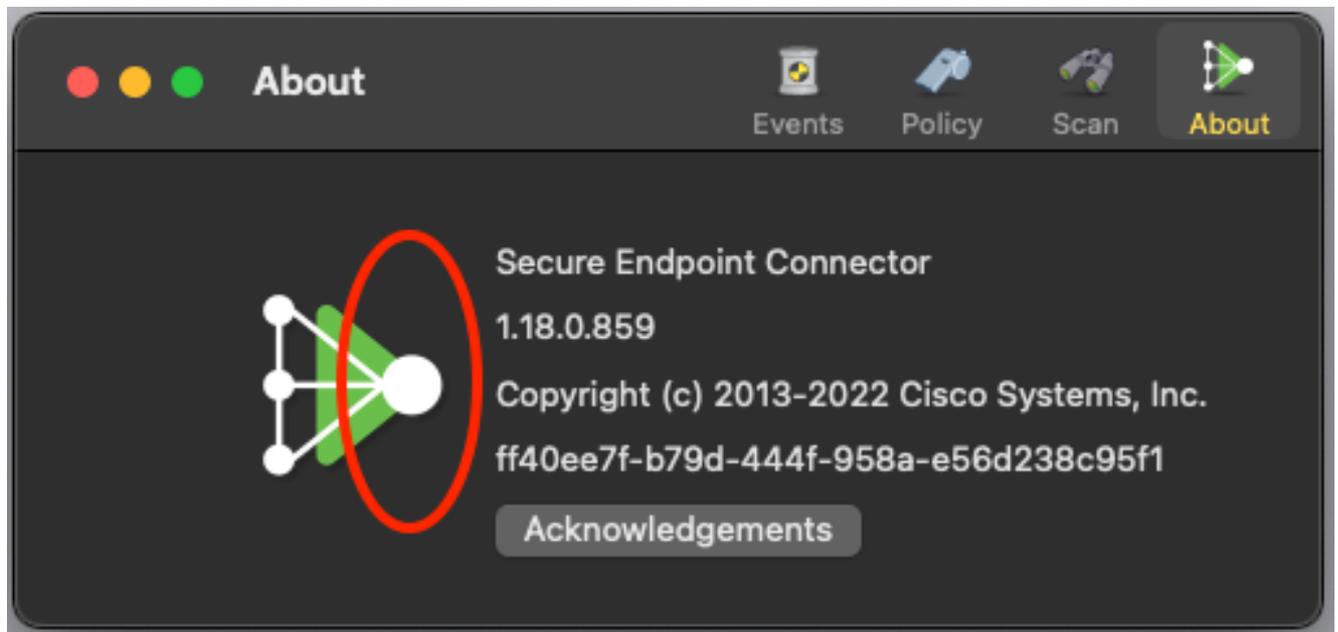
11. Sélectionnez le groupe que vous venez de créer dans la liste **Sélectionner un groupe** menu déroulant. Cliquez **Déplacer** pour déplacer l'ordinateur sélectionné dans votre nouveau groupe. Votre Mac doit maintenant avoir une stratégie de débogage fonctionnelle. Vous pouvez sélectionner l'icône Secure Endpoint qui apparaît dans la barre de menus et vous assurer que la nouvelle stratégie est appliquée :



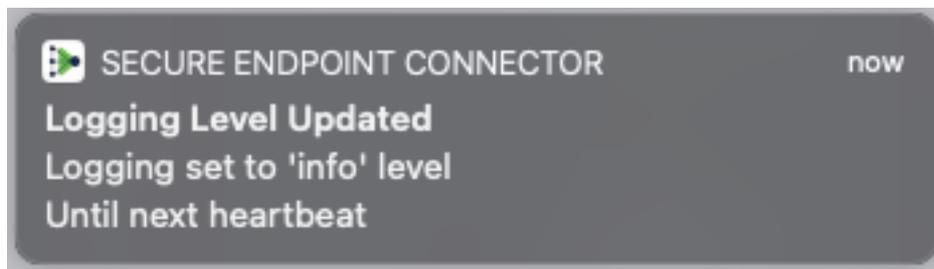
Activer le mode de débogage à pulsation unique

Cette procédure est uniquement disponible pour le connecteur 1.0.4 et versions ultérieures. Cela permet de mettre un seul connecteur en mode de débogage jusqu'au prochain battement de coeur. Selon la situation, cela peut fournir suffisamment d'informations pour nos développeurs, mais en fonction de la durée du battement de coeur, risque de ne pas capter tous les processus nécessaires pour effectuer une analyse diagnostique complète. Voici les étapes à suivre pour activer le débogage d'une pulsation unique :

1. Accédez à la barre de menus du connecteur et accédez à **Paramètres** .
2. Cliquez sur **A propos**.
3. Cliquez sur la moitié droite du logo Secure Endpoint.



4. Si cela a été fait correctement, l'avertissement suivant s'affiche sur le côté droit de l'écran :



Debug se désactive automatiquement après le prochain heartbeat.

Désactiver le mode débogage

Une fois les données de diagnostic en mode débogage obtenues, vous devez rétablir le connecteur Secure Endpoint en mode normal. Complétez ces étapes afin de désactiver le mode de débogage :

1. Connectez-vous à la console Secure Endpoint.
2. Accédez à **Gestion > Groupes**.
3. Recherchez le nouveau groupe, *Debug TechZone Mac Group*, que vous avez créé en mode debug.
4. Cliquez sur **Edit**.
5. Dans la fenêtre Ordinateurs située en haut à droite de votre écran, localisez votre ordinateur dans la liste. Sélectionnez-le pour accéder à la page Ordinateurs. Une fois de plus, sélectionnez votre ordinateur dans la liste et **cliquez sur Déplacer vers le groupe....**
6. Sélectionnez votre groupe précédent dans le menu déroulant **Sélectionner un groupe**. Cliquez sur Déplacer pour déplacer l'ordinateur sélectionné vers le groupe précédent.
7. Cliquez sur l'icône Secure Endpoint dans la barre de menus. **Sélectionnez Synchroniser** la stratégie dans le menu.
8. Vérifiez que la stratégie est maintenant rétablie à la valeur par défaut précédente. Cochez cette option dans la barre de menus. La stratégie aurait dû maintenant revenir à la stratégie

d'origine qui était utilisée avant que vous ne la changiez en *Debug TechZone Mac Group* :

Last Scan: 2019-05-29, 12:01 PM
Status: Connected
Policy: Desktop Mac Protect

Scan ▶
Pause Scan
Cancel Scan

Settings
Update Virus Definitions
Sync Policy

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.