Configurer une liste de détection personnalisée simple sur le portail AMP for Endpoints

Contenu

Introduction

Ce document décrit les étapes de création d'une liste de détection personnalisée simple pour détecter, bloquer et mettre en quarantaine des fichiers spécifiques afin d'empêcher les fichiers d'être autorisés sur les périphériques qui ont installé les connecteurs AMP (Advanced Malware Protection) pour les terminaux.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès au portail AMP
- Compte avec privilèges d'administrateur
- Taille de fichier maximale de 20 Mo

Components Used

Les informations de ce document sont basées sur la console Cisco AMP for Endpoints version 5.4.20190709.

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.

Flux de travail

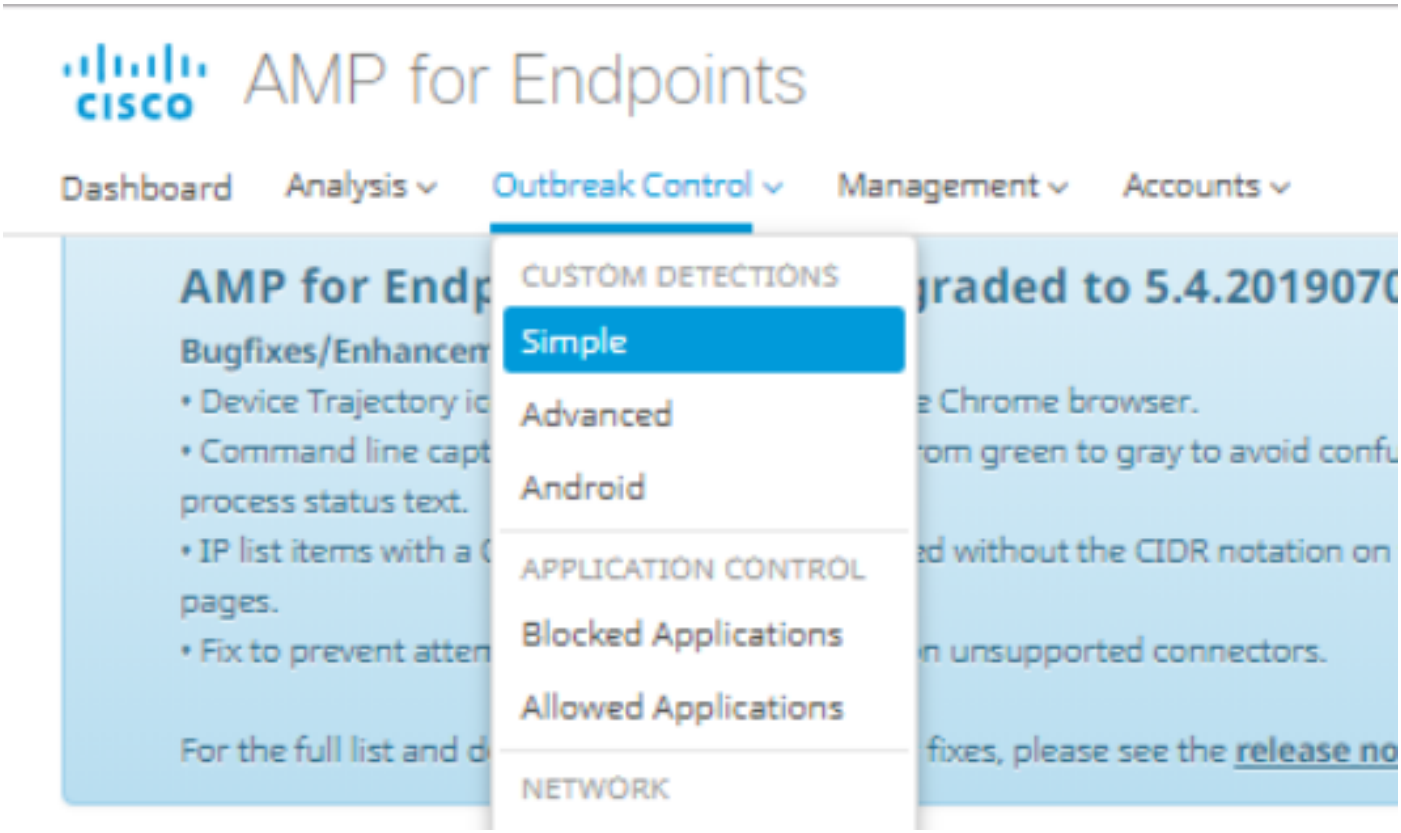
L'option de liste Détection personnalisée simple utilise ce workflow :

- Liste de détection personnalisée simple créée à partir du portail AMP.
- Liste de détection personnalisée simple appliquée dans une stratégie précédemment créée.
- Connecteur AMP installé sur le périphérique et appliqué dans la stratégie.

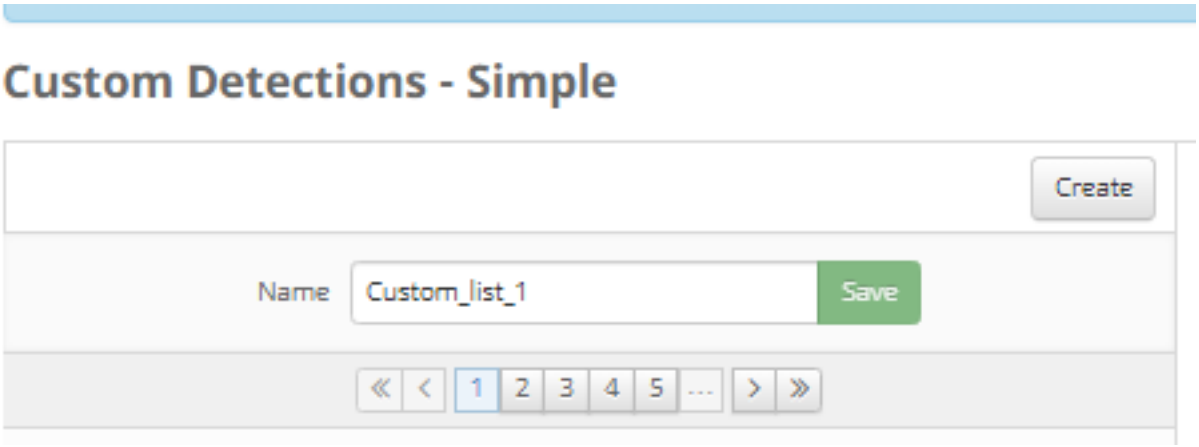
Configuration

Afin de créer une liste de détection personnalisée simple, procédez comme suit :

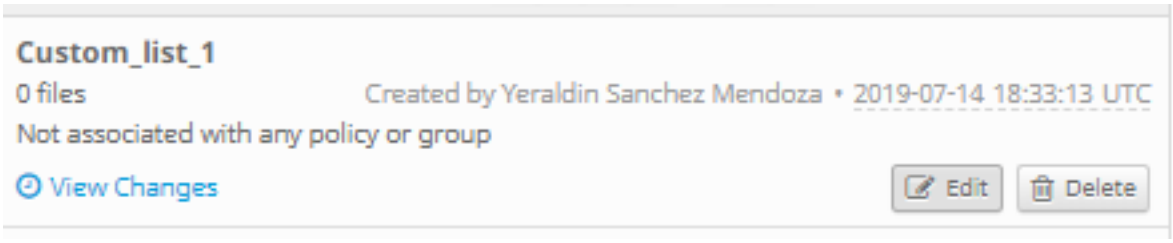
Étape 1. Sur le portail AMP, accédez à l'option **Contrôle des attaques > Simple**, comme illustré dans l'image.



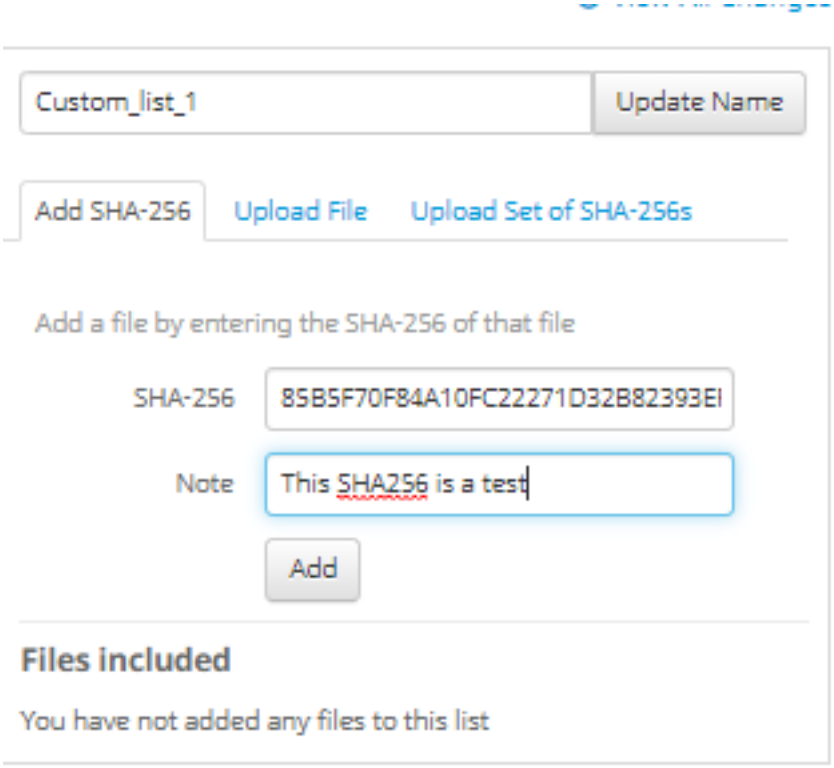
Étape 2. Dans l'option Détections personnalisées - Simple, cliquez sur le bouton **Créer** pour ajouter une nouvelle liste, choisissez un nom pour identifier la liste Détection personnalisée simple et enregistrez-la, comme indiqué dans l'image.



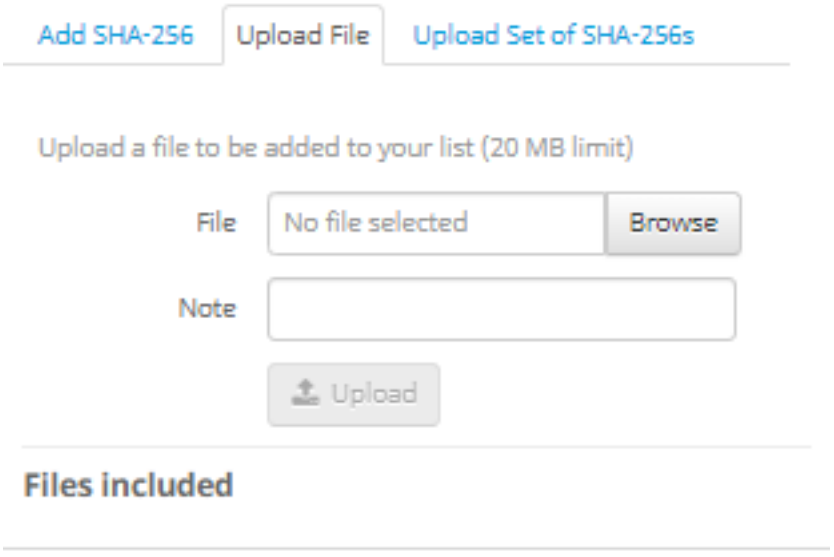
Étape 3. Une fois la liste créée, cliquez sur le bouton **Modifier** pour ajouter la liste des fichiers à bloquer, comme l'illustre l'image.



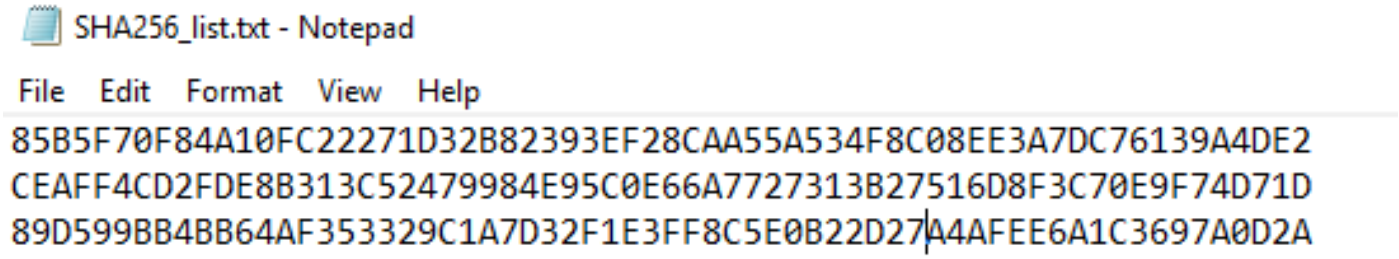
Étape 4. Dans l'option Add SHA-256, collez le code SHA-256 précédemment collecté à partir du fichier spécifique à bloquer, comme illustré dans l'image.

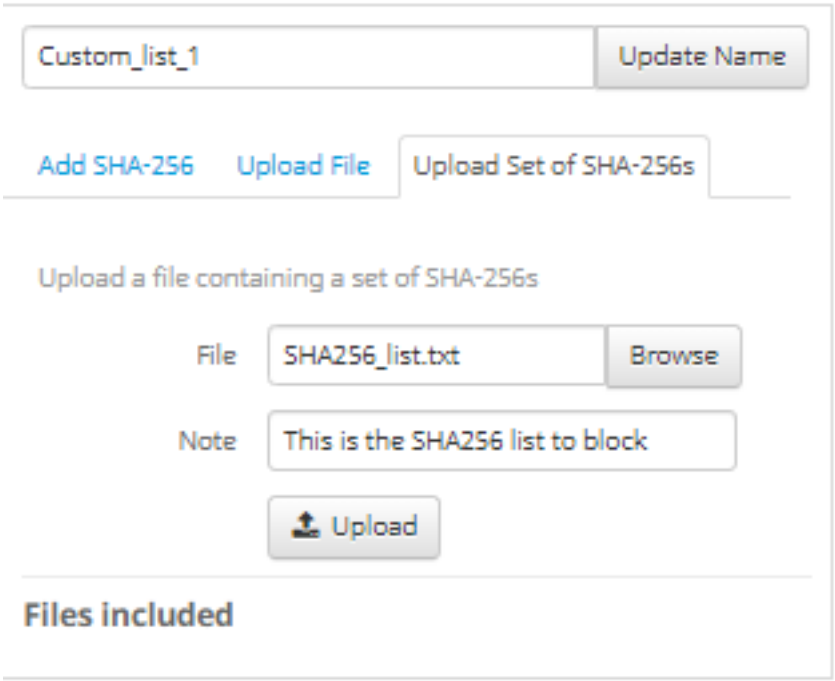


Étape 5. Dans l'option Upload File (Télécharger le fichier), recherchez le fichier spécifique à bloquer, une fois le fichier téléchargé, le SHA-256 de ce fichier est ajouté à la liste, comme l'illustre l'image.

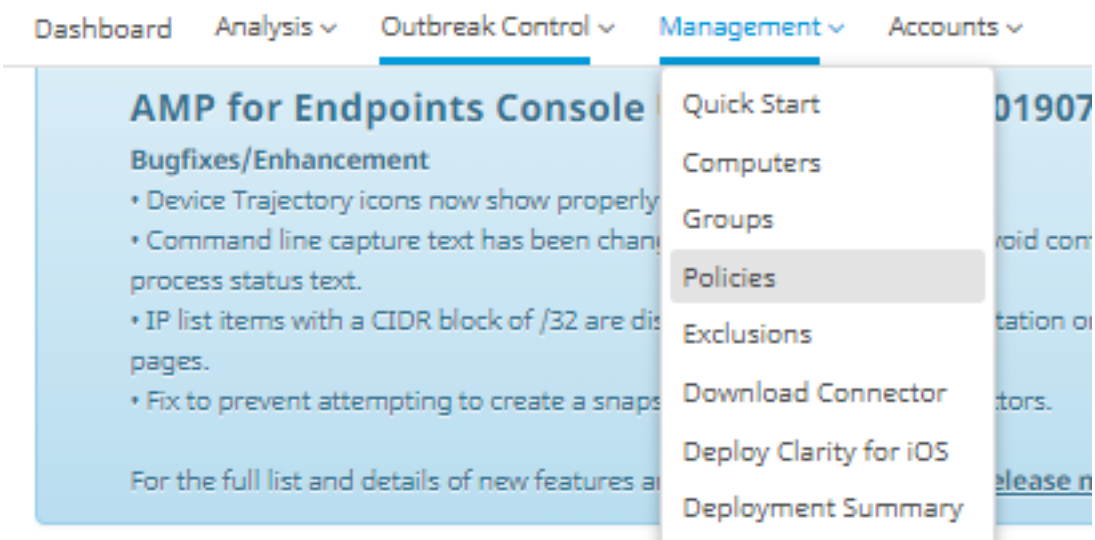


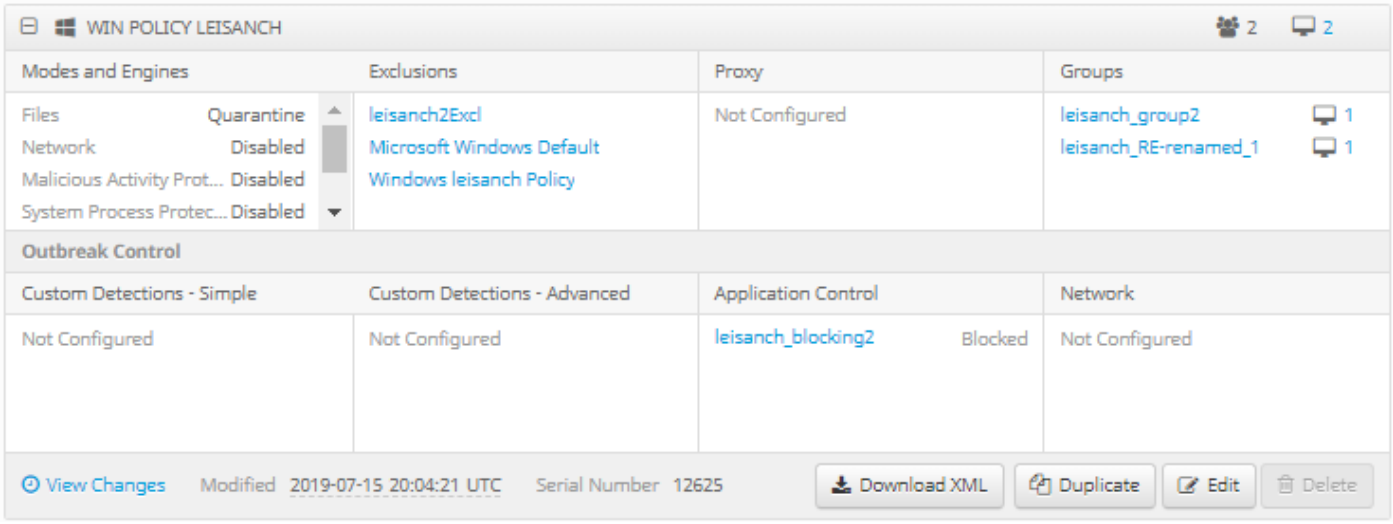
Étape 6. L'option Upload Set of SHA-256s permet d'ajouter un fichier avec une liste de plusieurs codes SHA-256 précédemment acquis, comme le montrent les images.



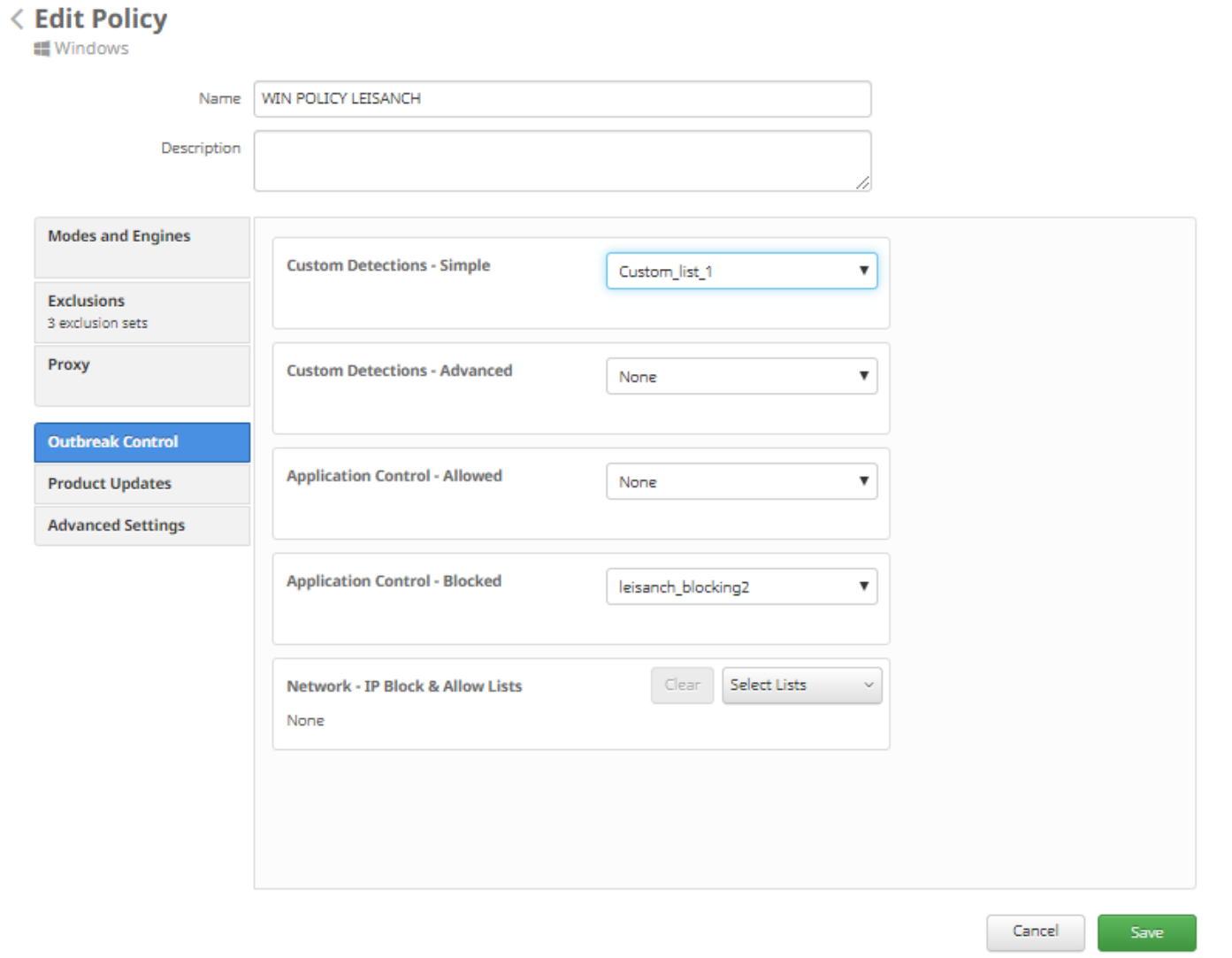


Étape 7. Une fois la liste Détection personnalisée simple générée, accédez à **Management > Policies** et choisissez la stratégie dans laquelle vous voulez appliquer la liste précédemment créée, comme le montrent les images.





Étape 8. Cliquez sur le bouton **Modifier** et naviguez jusqu'à **Contrôle des attaques > Détections personnalisées - Simple,** sélectionnez la liste précédemment générée dans le menu déroulant et enregistrez les modifications, comme indiqué dans l'image.



Une fois toutes les étapes effectuées et les connecteurs synchronisés aux dernières modifications de stratégie, la détection personnalisée simple prend effet.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

> **Avertissement :** Si un fichier est ajouté à une liste de détection personnalisée simple, le temps de cache doit expirer avant que la détection ne prenne effet.

> **Note**: Lorsque vous ajoutez une détection personnalisée simple, elle peut être mise en cache. La durée de mise en cache d'un fichier dépend de sa disposition, comme indiqué dans cette liste :
> ·Nettoyer les fichiers : 7 jours
> ·Fichiers inconnus : 1 heure
> ·fichiers malveillants : 1 heure