

Configurer une exclusion

Lien vers la ressource :

[Exclusions générales - Sophos Central Admin](#)

Allez dans paramètres > global exclusions

General

Tamper Protection

Manage permission for local admins so they can change settings for on-access scanning, HIPS, Sophos Live Protection, and more.

Website Management

Manage, categorize, and tag websites for use with Web Control.

Proxy Configuration

Enable devices to connect to Sophos Central or download Sophos software updates through a proxy server.

Global Exclusions

Manage exclusions for known files, websites, and applications in order to improve performance.

Les exclusions générales s'appliquent à tous vos utilisateurs (et à leurs appareils) et serveurs.

Si vous voulez que ces exclusions s'appliquent uniquement à un certain nombre d'utilisateurs ou de serveurs, veuillez plutôt utiliser les exclusions de stratégie.

Vous pouvez configurer les types d'exclusion suivants :

- Exclure des fichiers ou des dossiers du contrôle.
Si vous excluez les fichiers du contrôle, nous continuerons à vérifier toute présence de failles d'exploitation dans les éléments exclus.
- Exclure tous les processus exécutés à partir d'une application (Windows).
- Exclure les sites Web de la vérification (Windows/Mac).
- Exclure des applications de la protection contre les Exploits de sécurité (Windows/Mac).
- Exclure des applications généralement détectées comme spyware et des Exploits détectés par le passé du contrôle et de la détection (Windows/Mac).
- Exclure les Exploits de comportement malveillant détectés précédemment (Windows).
- Exclure les dossiers ou les applications de la protection antiransomware (Windows/Mac).

Vous pouvez également utiliser les exclusions pour autoriser les appareils isolés à communiquer avec d'autres appareils sous restrictions.

Exemple d'exclusion pour un fichier de mise à jour régulièrement détecté et mis en quarantaine sur les postes.

Exclude	Active for	Comment
C:\as2013\maj_as2010.exe File or folder (Windows)	Real-time and scheduled	X

Pour voir les détections provenant des postes, il faut aller dans la partie Endpoint, et récupérer le nom du poste.

Il est possible de récupérer un mot de passe pour passer admin depuis la console SOPHOS sur le poste client et désactiver l'analyse de Traffic en temps réel.

Endpoint

Dashboard

Reports

People

Computers

Policies

Settings

Installers

Tamper Protection

Tamper Protection

On Turn off tamper protection

Hide password details

Tamper Protection Password Details

CURRENT PASSWORD

JPnxgm5dZYGvhARK

Generate New Password

Revision #1

Created 12 February 2025 15:49:20 by Johann

Updated 12 February 2025 15:54:48 by Johann