Configurez et gérez les exclusions dans l'AMP pour des points finaux

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
Types d'exclusion
Extension de fichier
Chemin
Masque
Menace
Processus
Prévention d'exploit
Protection d'action malveillante
Configurer
Vérifier
Dépanner
Annexe A : Exclusions recommandées
Postes Windows (génériques)
Windows Server (génériques)
Contrôleurs de domaine windows
Windows - IIS
Windows - Serveur exchange
Windows - Serveur SQL
Windows - Protection de point final de Symantec
Windows - Avast
Windows - Avira
Windows - Altiris par Symantec
Windows - Tendance
Windows - Kaspersky
Windows - McAfee
Windows Defender
Windows - Premier rang de Microsoft
Windows - Client de Sécurité de Microsoft
Windows - Sophos
Windows - VSE
MAC - Postes de travail (génériques)
MAC - Jabber
MAC - JAMF Casper

MAC - McAfee
MAC - Crashplan
MAC - Fusion
MAC - Bureau
Windows - Logiciel de Lakeside - Systrack
Windows - Applications SAS
Windows - Splunk
Windows - Diebold Warsaw
Windows - Un lecteur
Windows - Bureau

Introduction

Ce document décrit comment créer des exclusions de sorte qu'un AMP pour le connecteur des points finaux (A4E) n'analyse pas le répertoire du programme. Ceci est terminé afin d'empêcher des conflits ou des problèmes de performances entre un connecteur de FireAMP et un antivirus ou d'autres applications. C'est particulièrement important avec les signatures d'antivirus qui contiennent les chaînes que le connecteur A4E détecte en tant que malveillant ou émet avec les fichiers mis en quarantaine.

> **Note**: Le centre d'assistance technique Cisco (TAC) ne dépiste pas l'inventaire du nombre d'applications potentiellement infini. La liste d'exclusions dans l'annexe est juste une instruction. Pour information les informations complémentaires, lisez le guide utilisateur et la documentation officiels.

Conditions préalables

Exigences

Cisco recommande que vous ayez la connaissance de la console de nuage A4E, l'AMP pour les points finaux (A4E), et les Produits d'antivirus.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Types d'exclusion

Il y a cinq types d'exclusions utilisables dans la console et deux A4E qui peuvent être additionnés

par le niveau 3. Si le type inapproprié d'exclusion est utilisé, l'exclusion ne fonctionnera pas. Il est important de noter le format de chaque type afin de vérifier l'exclusion a été ajouté correctement pendant le processus de accord.

Extension de fichier

Ce type d'exclusion est utilisé pour exclure des fichiers d'une certaine extension, n'importe où il se trouve sur l'ordinateur. Exemples :

- .log
- .txt
- .db

Chemin

Cette exclusion peut être utilisée afin d'exclure un répertoire simple ou classer. Les exclusions de chemin sont récursives (tous les sous-dossiers dans ce chemin seront également exclus). Les exclusions de chemin sont les seules qui peuvent utiliser la liste spéciale constante d'ID d'élément (CSIDL) comme masque. Les deux formats de chemin sont :

- CSIDL_WINDOWS\system32
- C:\Windows\system32

  Note: L'étoile de masque « * » le caractère est non valide pour l'usage dans une exclusion de chemin. En outre, parce que ordinateurs Windows seulement (n'affecte pas le MAC/Linux) : Ajouter « \ » à la fin d'une exclusion de chemin change le comportement légèrement. C'est plus facile expliqué avec un exemple. Si vous excluez « C:\Test », l'AMP exclura des fichiers dans le _Two de « C:\Test », de « C:\Testing », « de C:\Test », etc. (et tous les sous-répertoires s'y rapportant). Si vous excluez « C:\Test\ », l'AMP exclura seulement des fichiers dans « C:\Test » (et des sous-répertoires s'y rapportant). Il n'exclura pas des fichiers dans le _Two de « C:\Testing », « de C:\Test », etc.

Masque

Ce type d'exclusion est meilleur utilisé quand vous pouvez ne pouvoir pas anticiper un répertoire ou un nom du fichier. Vous pouvez utiliser de plusieurs masques dans une exclusion simple aussi bien. Les exemples de masque sont :

- C:\Program Files\MyApplication\ *.log
- * De C:\Users\ \ MyApplication \
- C:\ProgramData\ * \ MyApplication \ * \ *.log

Menace

Cette exclusion aide à empêcher un ou plusieurs fichiers d'être balayé et détecté basé sur le nom de menace. Ceci peut être utile si vous anticipez un grand choix de noms pour un fichier donné. Quelques exemples des noms de menace sont ci-dessous :

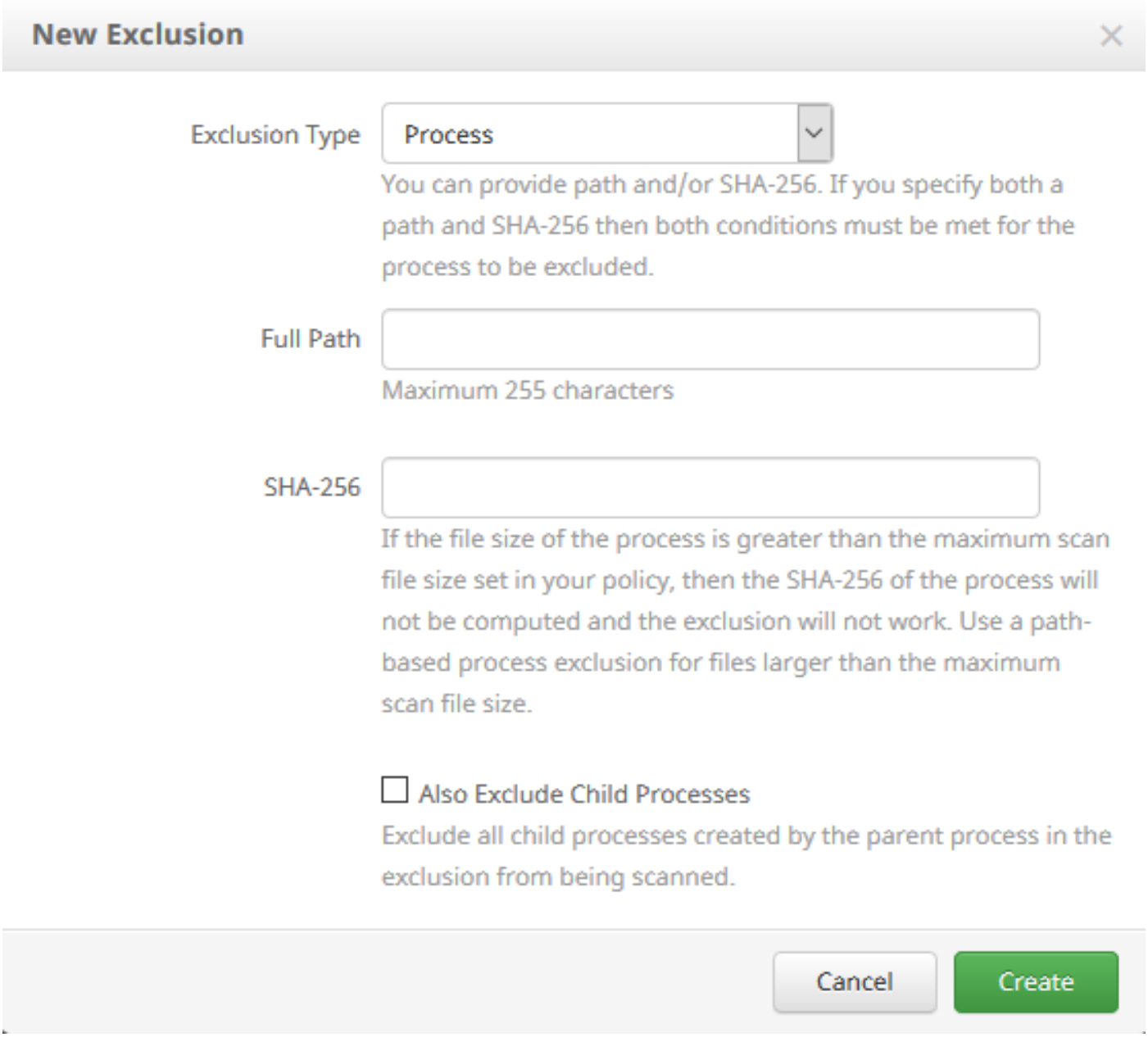
- W32.B76344BA43-95.SBX.TG

- W32.Auto:dfd99f89d2.in05.Talos

Processus

Des exclusions de processus peuvent être utilisées pour empêcher A4E de balayer tous les fichiers et sous-processus basés sur un processus. Vous pouvez utiliser les informations parasites SHA256 du chemin de fichier de processus ou plein, ou SHA256 et chemin de fichier ensemble. Si vous utilisez les deux parties de données puis les deux conditions doivent être remplies pour que l'exclusion fonctionne. Vous pouvez également choisir d'exclure des sous-processus. Les exemples sont ci-dessous :

- C:\Program Files\MyApplication.exe
- SHA256 du MyApplication.exe
- Chacun des deux ce qui précède



Note: v5.1.13 ou plus élevé est exigé pour utiliser des exclusions de processus avec des exclusions de processus fils activées.

Prévention d'exploit

Les exclusions de prévention d'exploit sont utiles pour exclure DLLs incompatible jusqu'à ce qu'une mise à jour à l'engine puisse être terminée pour résoudre le problème. Pour déterminer l'exclusion appropriée, entrez en contact avec s'il vous plaît le TAC.

> **Note**: Le connecteur v6.0.1 de Windows ou plus élevé est exigé pour utiliser des exclusions de prévention d'exploit.

Protection d'action malveillante

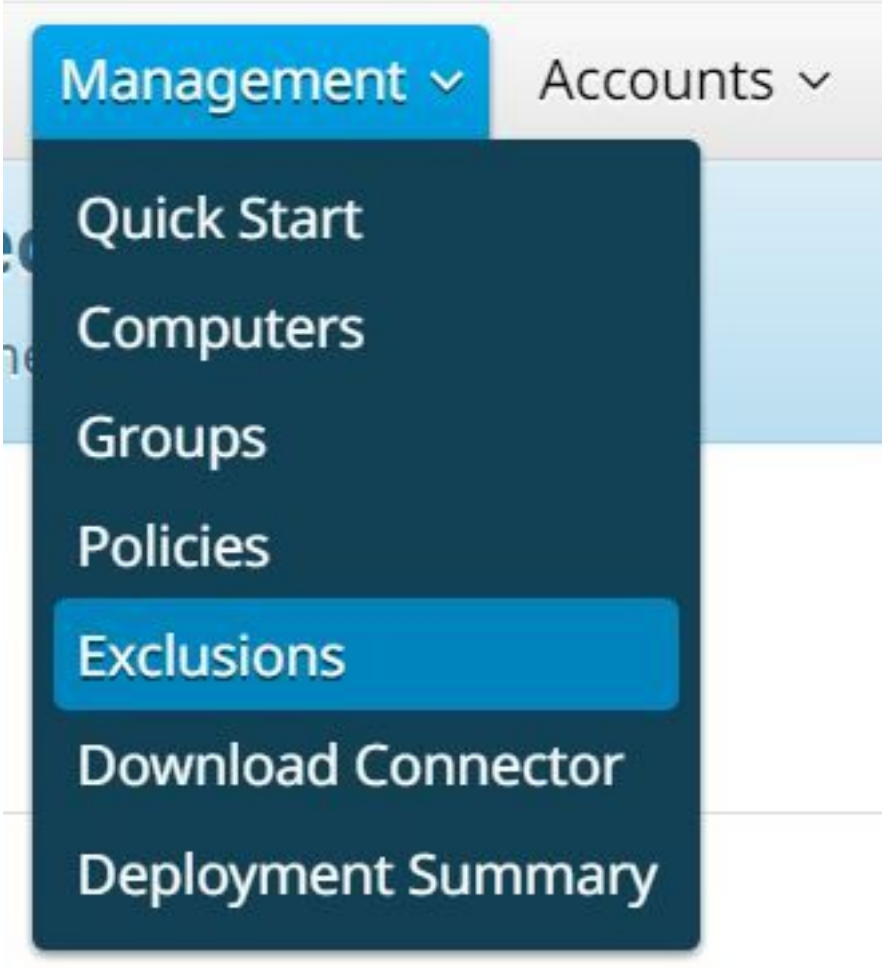
Des exclusions de MAP peuvent être utilisées si un processus est signalé comme malveillant basé sur ses comportements malveillants connus de ressemblance de comportement. Si une exclusion est exigée pour la MAP, entrez en contact avec s'il vous plaît le TAC

> **Note**: Le connecteur v6.1.1 de Windows ou plus élevé est exigé pour utiliser des exclusions de processus avec des exclusions de processus fils activées.

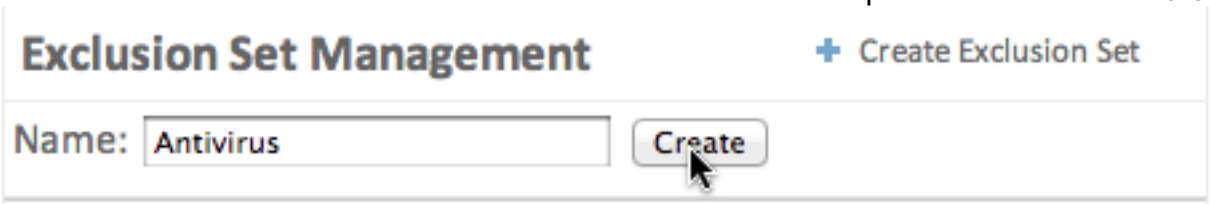
Configurer

Afin de créer des exclusions, terminez-vous ces étapes :

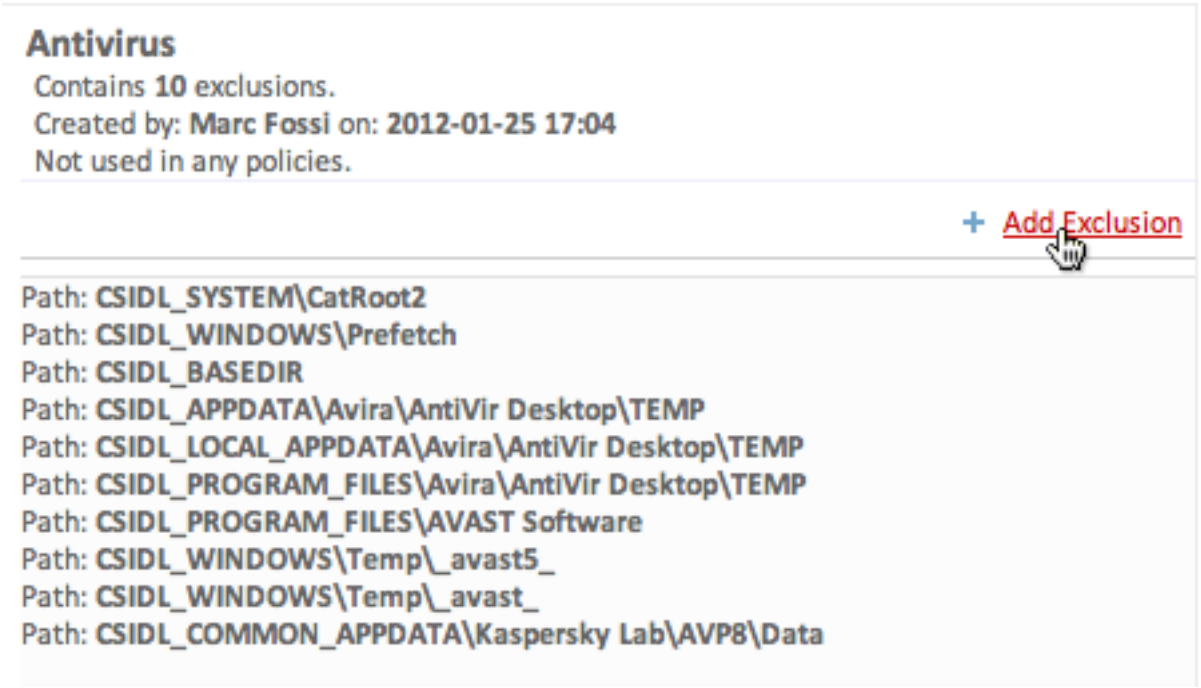
1. Choisissez la **Gestion > les exclusions** sur la console de nuage A4E.



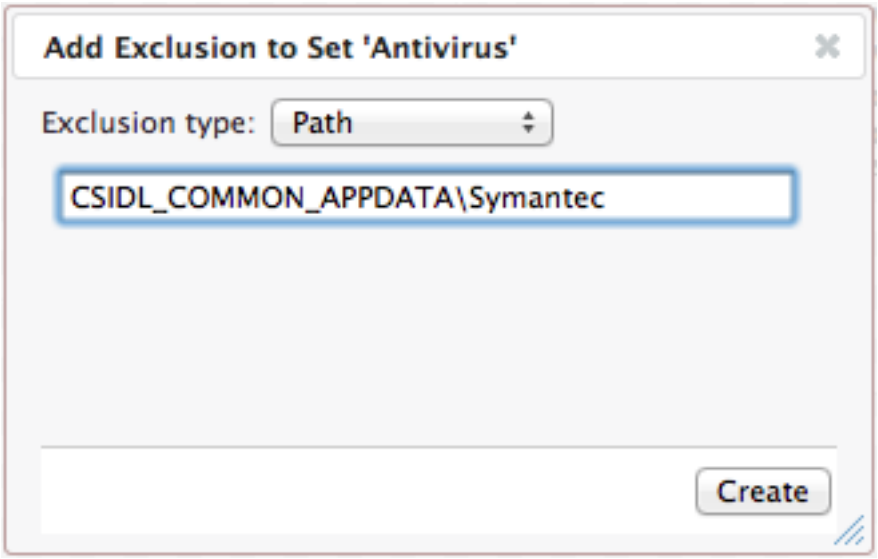
2. Ou éditez un positionnement existant d'exclusion (préféré) ou le clic **créent l'exclusion réglée** afin de créer une nouvelle liste d'exclusions. Écrivez un nom pour la liste et le clic **créent**.



3. Cliquez sur Add l'**exclusion** afin d'ajouter une exclusion à votre liste. Vous serez incité à entrer dans un chemin pour l'exclusion.



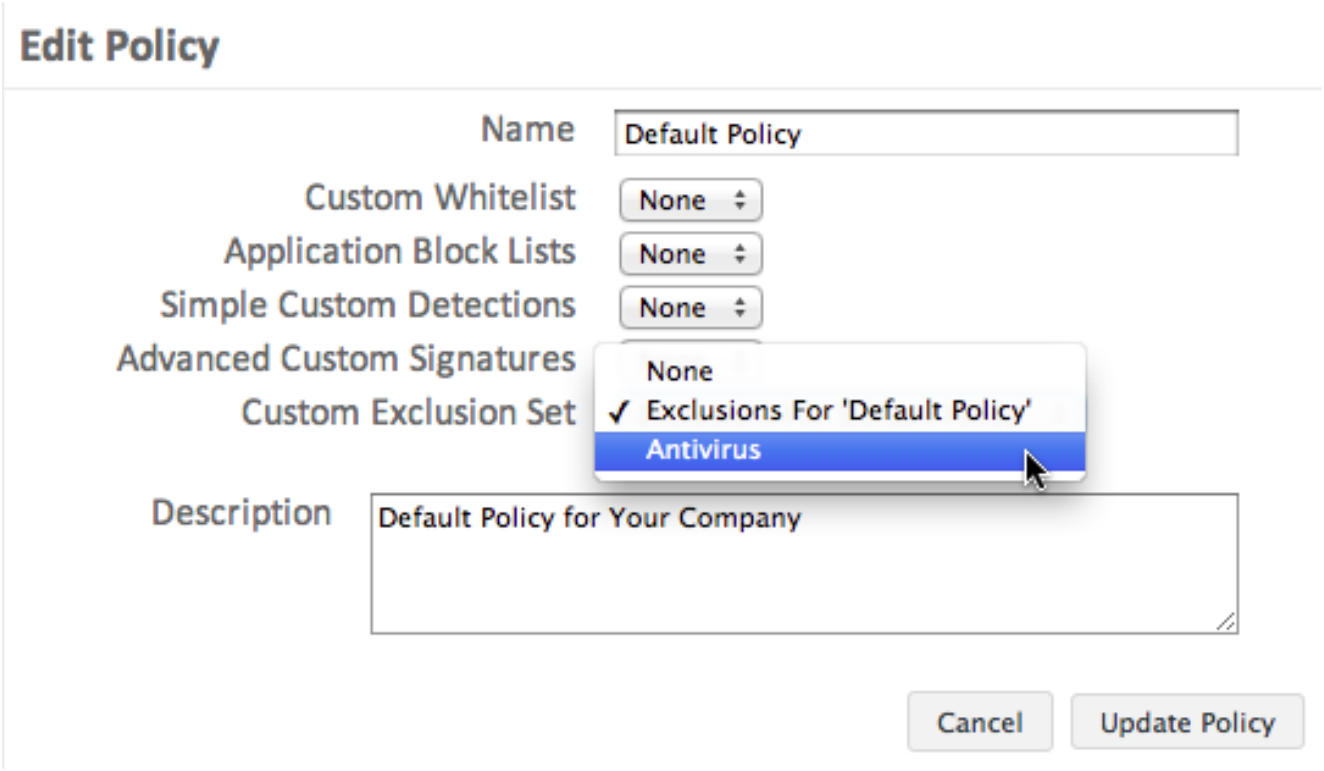
4. Écrivez le CSIDL des logiciels que vous avez installés sur vos points finaux et puis cliquez sur **créez**. **Note**: Une valeur CSIDL identifie des dossiers spéciaux utilisés par une application. C'est système-indépendant et indépendant de n'importe quel nom du fichier ou emplacement du système.



Note: Dans le tir d'écran précédent, le nom du répertoire est exclu pour Symantec. Une fois que le CSIDL est chargé sur l'ordinateur qui exécute le connecteur de FireAMP, le CSIDL le résout au chemin d'accès complet, `C:\ProgramData\Symantec`.

5. Choisissez la **Gestion > les stratégies**. Cliquez sur Edit à côté de la stratégie appropriée. De la liste déroulante **réglée d'exclusion de coutume**, choisissez l'exclusion vous placent créé.

SOUVENEZ-VOUS TOUJOURS QU'UNE STRATÉGIE PEUT SEULEMENT AVOIR UNE EXCLUSION RÉGLÉE ASSOCIÉE AVEC LE SERVICE INFORMATIQUE.**Note**: Une fois que vous avez créé un positionnement d'exclusion, vous devez l'ajouter à toutes les stratégies que vous avez
créées.



6. Cliquez sur la **stratégie de mise à jour** et répétez les étapes pour toutes les autres stratégies que vous voulez l'appliqué réglé d'exclusion à. **Note**: Il y a un retard entre une mise à jour de stratégie et le prochain intervalle de pulsation, quand un connecteur reçoit un changement de politique mis à jour.**Conseil** : Afin de déterminer le CSIDLs pour votre produit ou application en cours de Sécurité, entrez en contact avec le fabricant. Pour une liste complète de CSIDLs, référez-vous à Microsoft Dev Center - appareil de bureau.

Vérifiez

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

Dépanner

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

Annexe A : Exclusions recommandées

Basé sur la liste d'exclusion d'antivirus de Microsoft, Cisco recommande que vous excluiez :

Postes Windows (génériques)

- Extension : .db-journal
- Extension : .db-wal

- Extension : .db-shm
- Extension : .pst
- Extension : .log
- Chemin : CSIDL_BASEDIR
- Chemin : CSIDL_SYSTEM \ emptyregdb.dat
- Chemin : CSIDL_SYSTEM\CatRoot2
- Chemin : CSIDL_WINDOWS \ Prefetch
- Chemin : CSIDL_PROGRAM_FILES \ Windows Defender
- Chemin : Defender CSIDL_PROGRAM_FILESX86\Windows
- Chemin : CSIDL_COMMON_APPDATA \ Microsoft \ Windows Defender
- Chemin : CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb.chk
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ tmp.edb
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.chk
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.edb
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.jrs
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.log
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.sdb
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ *.log
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ \ logs \ edb*.log
- Masque : * \ les informations volume de système \ tracking.log$

Windows Server (génériques)

- Chemin : CSIDL_BASEDIR
- Chemin : CSIDL_SYSTEM \ emptyregdb.dat
- Chemin : CSIDL_SYSTEM\CatRoot2
- Chemin : CSIDL_WINDOWS \ Prefetch
- Chemin : CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb.chk
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ tmp.edb
- Chemin : Fichiers compressés provisoires de C:\inetpub\temp\IIS
- Chemin : Fichiers compressés provisoires CSIDL_WINDOWS \ IIS
- Chemin : CSIDL_WINDOWS\system32\inetsrv
- Chemin : CSIDL_WINDOWS\system32\inetsrv\w3wp.exe
- Chemin : CSIDL_WINDOWS\SysWOW64\inetsrv\w3wp.exe
- Chemin : CSIDL_COMMON_APPDATA \ ntuser.pol

- Chemin : CSIDL_WINDOWS\System32\LogFiles
- Chemin : CSIDL_WINDOWS\SysWow64\LogFiles
- Chemin : CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\SQLServr.exe
- Chemin : CSIDL_PROGRAM_FILES \ services de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting \ ReportServer \ coffre \ ReportingServicesService.exe
- Chemin : CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- Chemin : CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- Chemin : CSIDL_PROGRAM_FILES \ services de Microsoft SQL Server\MSSQL.3\Reporting \ ReportServer \ coffre \ ReportingServicesService.exe
- Chemin : CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.chk
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.edb
- Masque : \ CSIDL_WINDOWS \ Sécurité \ base de données \ *.log
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.sdb
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.jrs
- Masque : * \ les informations volume de système \ tracking.log$
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ *.log
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb*.log
- Extension : .bak
- Extension : .ldf
- Extension : .mdf
- Extension : .trn
- Extension : .abf
- Extension : .ctl
- Extension : .dbf
- Extension : .rdo
- Extension : .arc
- Extension : .ndf

Remarque: Des exclusions supplémentaires suggérées par Microsoft sont fréquemment mises à jour ici

Contrôleurs de domaine windows

- Chemin : CSIDL_COMMON_APPDATA \ ntuser.pol
- Chemin : CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb.chk
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Chemin : CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Chemin : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ tmp.edb
- Chemin : CSIDL_WINDOWS \ ntds \ ntds.dit

- Chemin : CSIDL_WINDOWS \ ntds \ EDB.chk
- Chemin : CSIDL_WINDOWS \ ntds \ TEMP.edb
- Chemin : CSIDL_WINDOWS \ SYSVOL \ domaine \ DO_NOT_REMOVE_NtFrs_PreInstall_Directory
- Chemin : CSIDL_WINDOWS \ SYSVOL \ mise en place
- Chemin : CSIDL_WINDOWS \ SYSVOL \ zones de transit
- Chemin : CSIDL_WINDOWS \ SYSVOL \ sysvol
- Chemin : CSIDL_WINDOWS\System32\ntfrs.exe
- Chemin : CSIDL_WINDOWS\System32\dfsr.exe
- Chemin : CSIDL_WINDOWS\System32\dfsrs.exe
- Chemin : CSIDL_WINDOWS\System32\dns.exe
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.edb
- Masque : \ CSIDL_WINDOWS \ Sécurité \ base de données \ *.log
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.sdb
- Masque : CSIDL_WINDOWS \ Sécurité \ base de données \ *.jrs
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ *.log
- Masque : CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb*.log
- Masque : CSIDL_WINDOWS \ ntds \ EDB*.log
- Masque : CSIDL_WINDOWS \ ntds \ Edbres*.jrs
- Masque : CSIDL_WINDOWS \ ntds \ *.pat
- Masque : CSIDL_WINDOWS\System32\DNS*.dns
- Masque : CSIDL_WINDOWS\System32\DNS*.scc

Windows - IIS

- Chemin : *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Chemin : *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Chemin : *Fichiers compressés provisoires de C:\inetpub\temp\IIS*
- Chemin : *Fichiers compressés provisoires CSIDL_WINDOWS \ IIS*
- Chemin : *CSIDL_WINDOWS\system32\inetsrv*
- Chemin : *CSIDL_WINDOWS\system32\inetsrv\w3wp.exe*
- Chemin : *CSIDL_WINDOWS\SysWOW64\inetsrv\w3wp.exe*
- Chemin : *CSIDL_WINDOWS\System32\LogFiles*
- Chemin : *CSIDL_WINDOWS\SysWow64\LogFiles*

Windows - Serveur exchange

- Chemin : CSIDL_PROGRAM_FILES \ Microsoft \ serveur exchange \
- Chemin : CSIDL_SYSTEM \ inetsrv

Windows - Serveur SQL

- Extension : *.bak*
- Extension : *.ldf*
- Extension : *.mdf*
- Extension : *.trn*
- Extension : *.abf*

- Extension : *.ctl*
- Extension : *.dbf*
- Extension : *.rdo*
- Extension : *.arc*
- Extension : *.ndf*
- Chemin : *CSIDL_COMMON_APPDATA* \ *ntuser.pol*
- Chemin : *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Chemin : *CSIDL_WINDOWS\System32\LogFiles*
- Chemin : *CSIDL_WINDOWS\SysWow64\LogFiles*
- Chemin : *CSIDL_PROGRAM_FILES* \ *Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\SQLServr.exe*
- Chemin : *CSIDL_PROGRAM_FILES* \ *services de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting* \ *ReportServer* \ *coffre* \ *ReportingServicesService.exe*
- Chemin : *CSIDL_PROGRAM_FILES* \ *Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe*
- Chemin : *CSIDL_PROGRAM_FILES* \ *Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe*
- Chemin : *CSIDL_PROGRAM_FILES* \ *services de Microsoft SQL Server\MSSQL.3\Reporting* \ *ReportServer* \ *coffre* \ *ReportingServicesService.exe*
- Chemin : *CSIDL_PROGRAM_FILES* \ *Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe*

Remarque: Les exclusions supplémentaires suggérées par Microsoft sont fréquemment updatedHere

Windows - Protection de point final de Symantec

- Chemin : CSIDL_COMMON_APPDATA \ Symantec
- Chemin : Protection CSIDL_PROGRAM_FILES \ Symantec \ point final de Symantec
- Chemin : Protection de point final CSIDL_PROGRAM_FILESX86\Symantec\Symantec
- Masque : CSIDL_WINDOWS \ Temp \ musdmys_*
- Masque : CSIDL_WINDOWS \ Temp \ content.zip.tmp \ *.diff
- Masque : CSIDL_WINDOWS \ Temp \ content.zip.tmp \ SymDeltaDecompressOptions.xml
- Masque : CSIDL_WINDOWS \ Temp \ content.zip.tmp \ cur.scr
- Masque : CSIDL_WINDOWS \ Temp \ TMP*.tmp

Windows - Avast

- Chemin : CSIDL_WINDOWS\Temp_avast5_
- Chemin : CSIDL_WINDOWS \ Temp \ _avast_

Windows - Avira

- Chemin : Appareil de bureau CSIDL_APPDATA \ Avira \ AntiVir \ température
- Chemin : Appareil de bureau CSIDL_LOCAL_APPDATA \ Avira \ AntiVir \ température
- Chemin : Appareil de bureau CSIDL_PROGRAM_FILES \ Avira \ AntiVir \ température

Windows - Altiris par Symantec

- Chemin : CSIDL_PROGRAM_FILES \ Altiris \ agent \ TaskManagement d'Altiris
- Chemin : CSIDL_PROGRAM_FILES \ Altiris \ inventaire \ Outbox
- Masque : * \ Windows \ Temp \ AltirisScript*.cmd

Windows - Tendance

- Chemin : CSIDL_PROGRAM_FILES \ Trend Micro
- Chemin : Micro CSIDL_PROGRAM_FILESX86\Trend

Windows - Kaspersky

- Chemin : CSIDL_COMMON_APPDATA \ Kaspersky Lab

Windows - McAfee

- Chemin : CSIDL_PROGRAM_FILES \ McAfee
- Chemin : CSIDL_PROGRAM_FILESX86\McAfee
- Chemin : CSIDL_COMMON_APPDATA \ McAfee
- Chemin : CSIDL_PROGRAM_FILES \ fichiers communs \ McAfee

Windows Defender

- Chemin : CSIDL_PROGRAM_FILES \ Windows Defender
- Chemin : Defender CSIDL_PROGRAM_FILESX86\Windows
- Chemin : CSIDL_COMMON_APPDATA \ Microsoft \ Windows Defender

Windows - Premier rang de Microsoft

- Chemin : CSIDL_PROGRAM_FILES \ premier rang de Microsoft
- Chemin : Premier rang CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Client de Sécurité de Microsoft

- Chemin : CSIDL_PROGRAM_FILES \ client Sécurité de Microsoft
- Chemin : Client de Sécurité CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Sophos

- Chemin : CSIDL_PROGRAM_FILES \ Sophos
- Chemin : CSIDL_PROGRAM_FILESX86\Sophos
- Chemin : CSIDL_COMMON_APPDATA \ Sophos \ antivirus de Sophos
- Chemin : CSIDL_COMMON_APPDATA \ Sophos

Vista/Win7 et plus nouveau exige également ce chemin.

- Chemin : C:\ProgramData\Sophos\AutoUpdate\Cache
- Chemin : C:\Program Files\Sophos\AutoUpdate\Cache
- Chemin : C:\ProgramData\Sophos
- Masque : C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\Sophos *
- Masque : C:\Windows\Temp\Sophos *

Windows - VSE

- Chemin : CSIDL_PROGRAM_FILES \ VSE
- Chemin : CSIDL_COMMON_APPDATA \ VSE

MAC - Postes de travail (génériques)

- Chemin : /private/var/vm
- Chemin : /.Spotlight-V100
- Chemin : /.MobileBackups
- Chemin : /Volumes/MobileBackups/
- Chemin : /Quarantine
- Chemin : Copies de sauvegarde d'ordinateur de /Volumes/Time
- Masque : /Volumes/*/.Spotlight-V100
- Masque : /Volumes/*/.Spotlight-V100*
- Masque : /Volumes/ */Backups.backupdb
- Masque : données d'utilisateur de /Users/ */Documents/Microsoft/bureau 2011 Identities/*
- Masque : bureau de /Users/ */Library/Group Containers/*/Outlook/Outlook 15 Profiles/*
- Masque : /Users/ */Library/Caches/Outlook/*
- Masque : /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kcIB*

MAC - Jabber

- Chemin : /bin/ps
- Chemin : /usr/bin/grep
- Masque : /Users/ */Library/Logs/Jabber

MAC - JAMF Casper

- Chemin : /usr/bin/sw_vers
- Masque : /Library/Application Support/JAMF/Usage/201*-*-*/.dat*

MAC - McAfee

- Chemin : /Library/McAfee/
- Chemin : Support de /Library/Application/McAfee/

MAC - Crashplan

- Chemin : /Library/Caches/CrashPlan/
- Masque : /Library/Logs/CrashPlan/ *.log

MAC - Fusion

- Chemin : /Library/Logs/VMware/

MAC - Bureau

- Masque : données d'utilisateur de /Users/ */Documents/Microsoft/bureau 2011 Identities/*
- Masque : bureau de /Users/ */Library/Group Containers/*/Outlook/Outlook 15 Profiles/*
- Masque : /Users/ */Library/Caches/Outlook/*
- Masque : /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kcIB*

Windows - Logiciel de Lakeside - Systrack

- Masque : * \ fichiers de programme (x86)\SysTrack\LsiAgent\Condense***.tmp
- Masque : * \ fichiers de programme (x86)\SysTrack\LsiAgent\Condense**.hld

Windows - Applications SAS

- Extension : .lck
- Extension : .sd2
- Extension : .sc2
- Extension : .SPDS
- Extension : .utl
- Masque : *.sas* (voyez la note dans la section de masque.)

Également l'emplacement de travail SAS doit être exclu, mais le répertoire pourrait être différent dans différentes versions SAS.

Windows - Splunk

- Chemin : CSIDL_PROGRAM_FILES \ Splunk
- Chemin : CSIDL_PROGRAM_FILESX86\Splunk
- Chemin : CSIDL_PROGRAM_FILES \ Splunk \ distributeur intégrant son logiciel au matériel \ bibliothèque \ splunk
- Chemin : CSIDL_PROGRAM_FILESX86\Splunk\var\lib\splunk
- Chemin : CSIDL_PROGRAM_FILES \ SplunkUniversalForwarder
- Chemin : CSIDL_PROGRAM_FILESX86\SplunkUniversalForwarder

Windows - Diebold Warsaw

Ce sont les exclusions exigées pour le logiciel bancaire de Diebold Warsaw. Sans ces exclusions en place l'application n'installera pas correctement. Si le logiciel est installé avant l'installation d'AMP sans ces exclusions en place le système pourrait devenir insensible.

Exclusions de chemin

- Chemin : C:\Program classe (x86)\Diebold\Warsaw
- Chemin : C:\Program Files\Diebold\Warsaw

- Chemin : C:\Windows\System32\drivers\wsddfac.sys

De plus nouvelles versions pourraient exiger :

- Chemin : C:\Windows\System32\drivers\gbpddfac64.sys
- Chemin : C:\Program classe (x86)\GAS Tecnologia \ Warsaw
- Chemin : C:\Windows\Temp\Diebold\Warsaw

Exclusions de masque

- Masque : _*de C:\Windows\Temp\warsaw
- Masque : * de C:\Users\ \ AppData \ gens du pays \ Temp \ warsaw_*
- Masque : * De C:\Users\ \ AppData \ gens du pays \ Temp \ *-*.tmp
- Masque : C:\Windows\System32\drivers*-*.tmp

Windows - Un lecteur

- Masque : * De C:\Users\ \ OneDrive

Windows - Bureau

- Masque : C:\Users\ * \ AppData \ gens du pays \ Microsoft \ bureau \ * \ OfficeFileCache