Configure y maneje las exclusiones en el AMP para los puntos finales

Contenido

Introducción

Este documento describe cómo crear las exclusiones de modo que un AMP para el conector de los puntos finales (A4E) no analice el directorio del programa. Esto se completa para prevenir los conflictos o los problemas de rendimiento entre un conector de FireAMP y un contra virus u otras aplicaciones. Esto es especialmente importante con las firmas del contra virus que contienen las cadenas que el conector A4E detecta como malévolo o publica con los archivos quarantined.

> **Note**: El Centro de Asistencia Técnica de Cisco (TAC) no sigue el inventario del número potencialmente infinito de aplicaciones. La lista de exclusiones en el apéndice es apenas una guía de consulta. Para la información adicional, lea el guía del usuario y la documentación oficiales.

Prerequisites

Requisitos

Cisco recomienda que usted tiene el conocimiento de la consola de la nube A4E, el AMP para los puntos finales (A4E), y Productos del contra virus.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Tipos de la exclusión

Hay cinco tipos de exclusiones usables en la consola A4E. Si utilizan al tipo incorrecto de la exclusión, la exclusión no funcionará. Es importante observar el formato de cada tipo para verificar la exclusión fue agregado correctamente durante el proceso que ajusta.

Extensión de Archivo

Utilizan a este tipo de la exclusión para excluir los archivos de cierta extensión, no importa dónde está situada en la máquina. Ejemplos:

- .log
- .txt
- .db

Trayecto:

Esta exclusión se puede utilizar para excluir una sola carpeta o clasifiar. Las exclusiones de la trayectoria son recurrentes (cualquier subfolders dentro de esa trayectoria también será excluido). Las exclusiones de la trayectoria son las únicas que pueden utilizar la lista especial constante de elemento ID (CSIDL) como comodín. Los dos formatos de la trayectoria son:

- CSIDL_WINDOWS\system32
- C:\Windows\system32

  Note: "\" Del final es opcional. Además, la estrella del comodín "*" el carácter es inválido para el uso dentro de una exclusión de la trayectoria.

Comodín

Este tipo de la exclusión es mejor usado cuando usted puede no poder anticipar una carpeta o un nombre del archivo. Usted puede utilizar a los comodines múltiples en una sola exclusión también. Los ejemplos del comodín son:

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

Amenaza

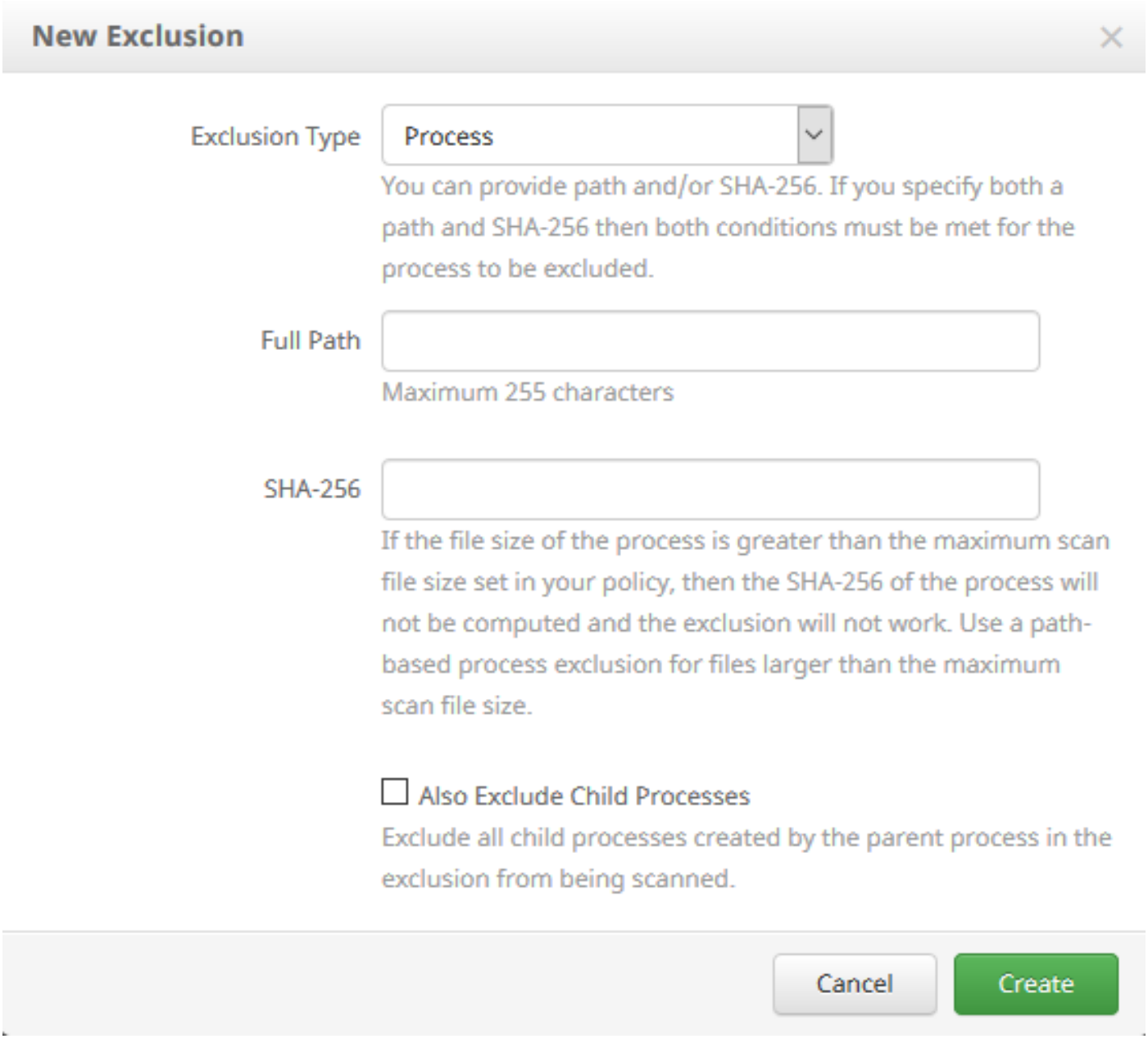
Esta exclusión ayuda a evitar que uno o más archivos sean analizados y que detectados basado en el nombre de la amenaza. Esto puede ser útil si usted anticipa una variedad de nombres para un archivo dado. Algunos ejemplos de los nombres de la amenaza están abajo:

- W32.B76344BA43-95.SBX.TG
- W32.Auto:dfd99f89d2.in05.Talos

Proceso

Las exclusiones de proceso se pueden utilizar para evitar que A4E analice cualesquiera archivos y subproceso basados en un proceso. Usted puede utilizar el hash SHA256 del trayecto del archivo de proceso o lleno, o SHA256 y trayecto del archivo junto. Si usted utiliza ambos pedazos de datos entonces ambas condiciones se deben cumplir para que la exclusión trabaje. Usted puede también elegir excluir los subprocesos. Los ejemplos están abajo:

- C:\Program Files\MyApplication.exe
- SHA256 del MyApplication.exe
- Ambos antedicho

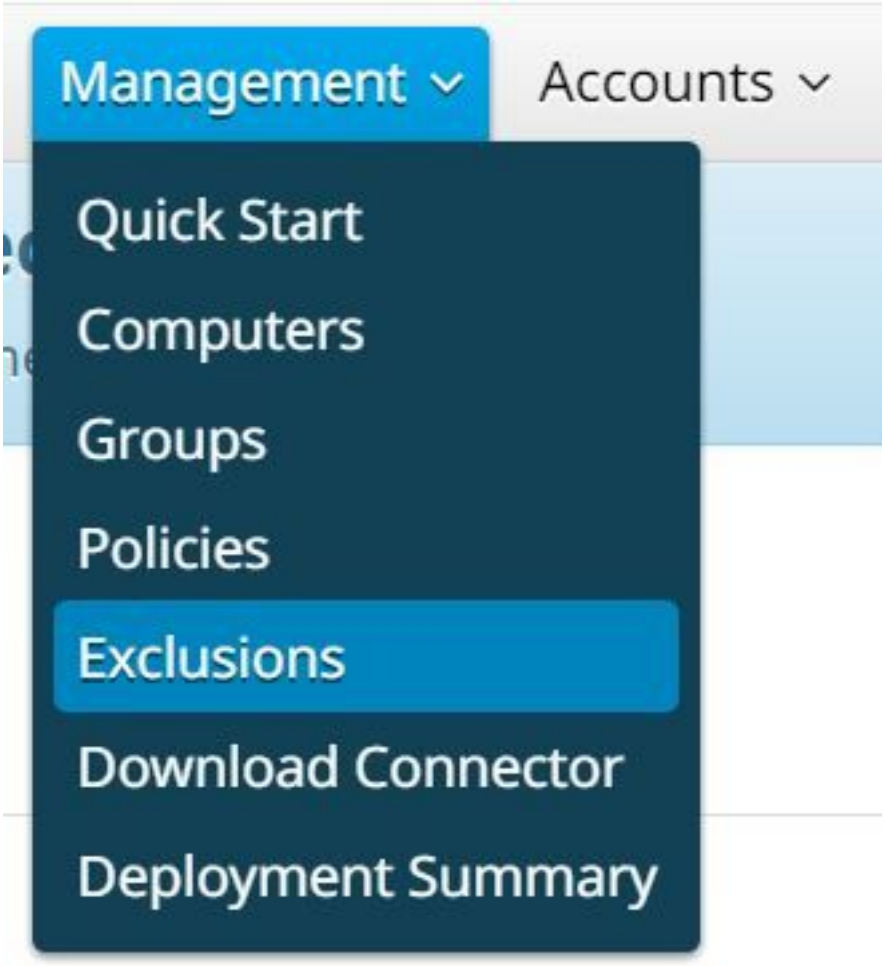


Note: v5.1.13 o más arriba se requiere para utilizar las exclusiones de proceso con las exclusiones del proceso hijo habilitadas.

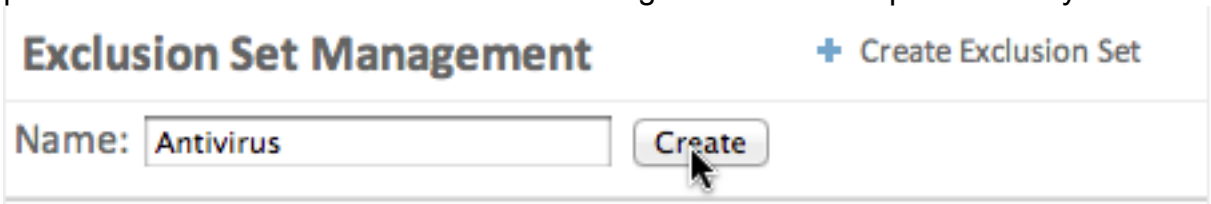
Configurar

Para crear las exclusiones, complete estos pasos:

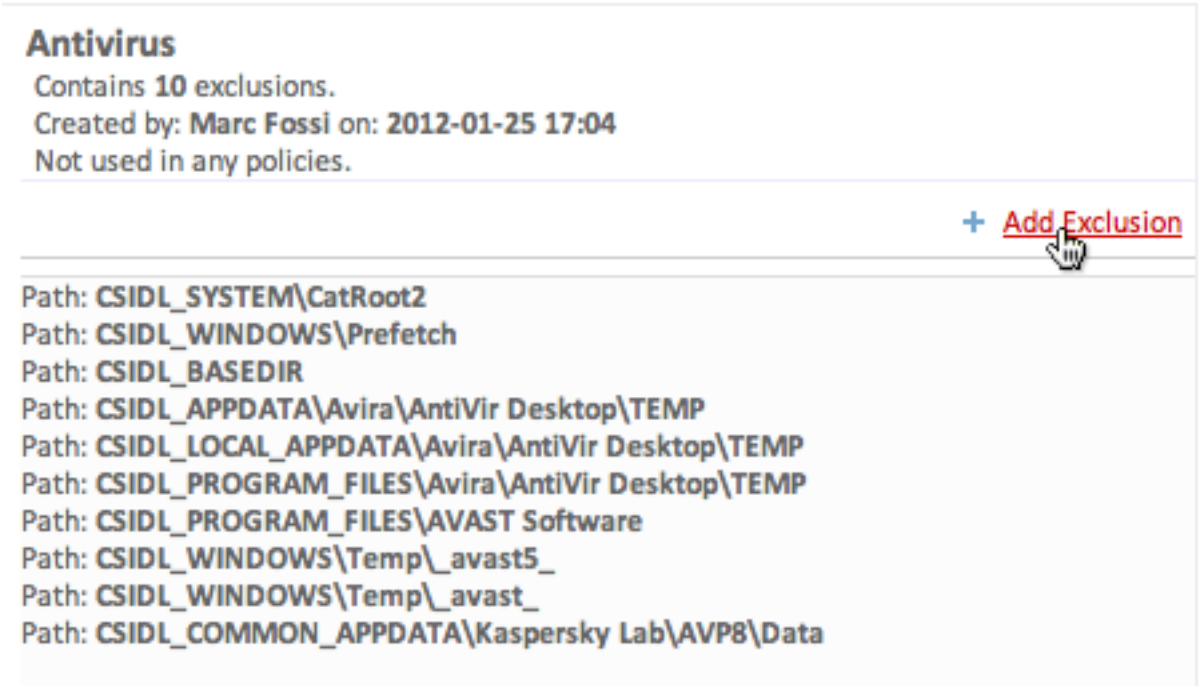
1. Elija la **Administración > las exclusiones** en la consola de la nube A4E.

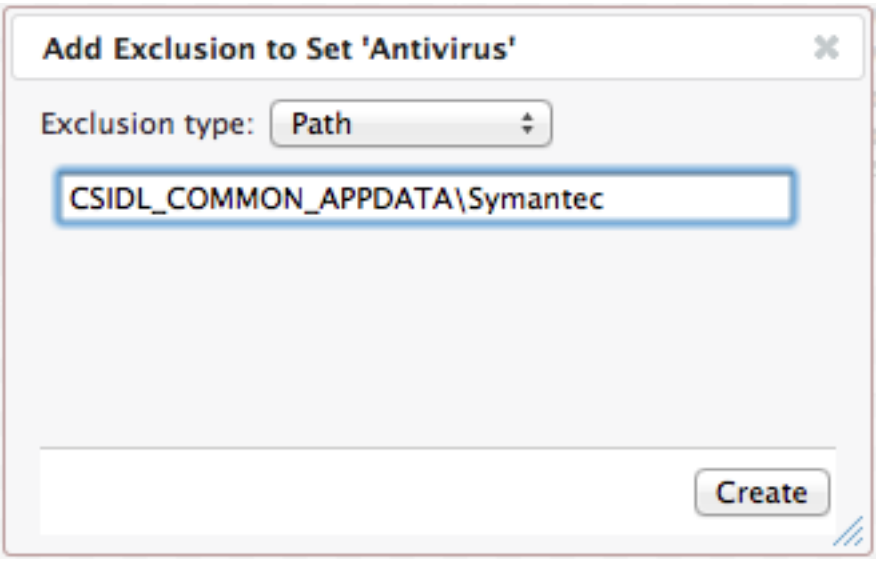


2. O edite un conjunto existente de la exclusión (preferido) o el tecleo **crea la exclusión fijada** para crear una nueva lista de exclusiones. Ingrese un nombre para la lista y el tecleo **crea**.

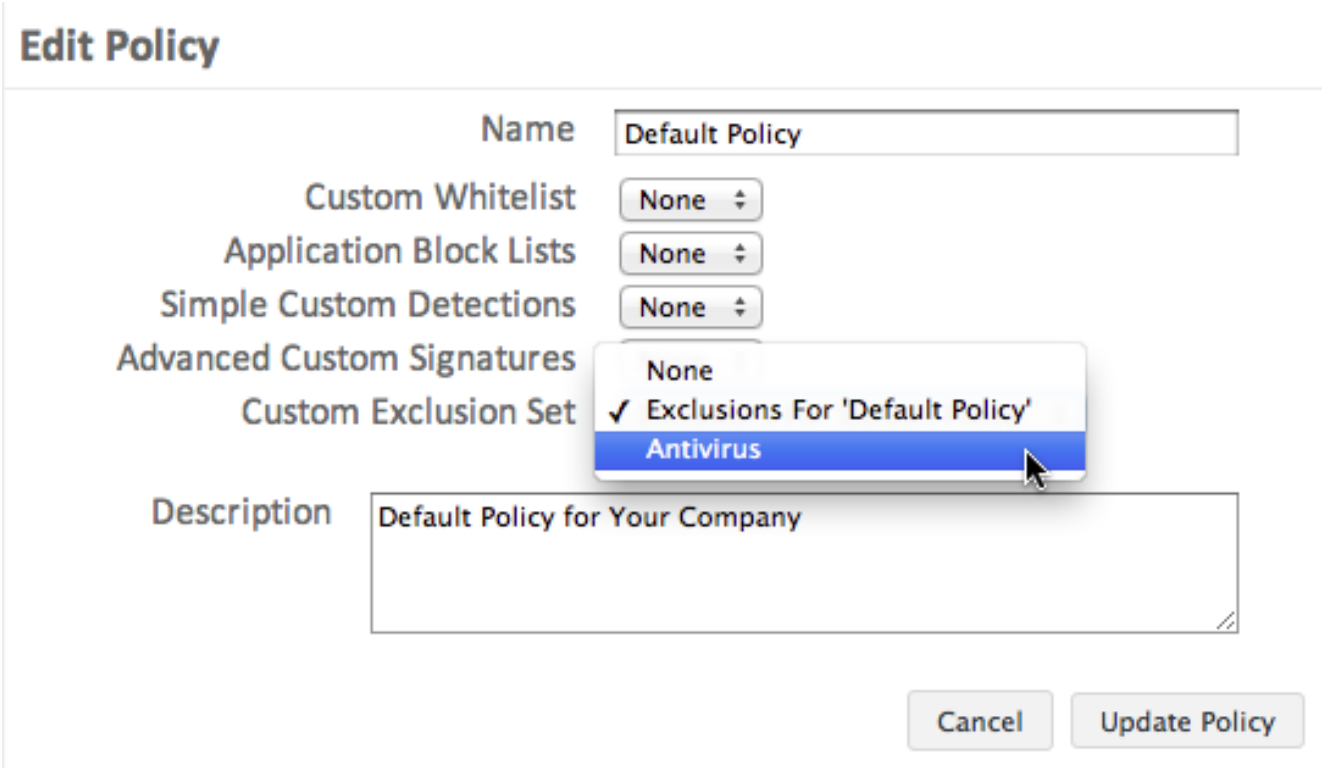


3. El tecleo **agrega la exclusión** para agregar una exclusión a su lista. A le indicarán que ingrese una trayectoria para la exclusión.



4. Ingrese el CSIDL de los productos de software que usted instaló en sus puntos finales y después que hace clic **crea**. **Note**: Un valor CSIDL identifica las carpetas especiales usadas por una aplicación. Ésta es sistema-independiente y independiente de cualquier nombre de fichero o ubicación del sistema. 

Note: En el tiro de pantalla anterior, Directory Name (Nombre de directorio) se excluye para Symantec. Una vez que el CSIDL se carga en el ordenador que funciona con el conector de FireAMP, el CSIDL resuelve a la ruta completa, `C:\ProgramData\Symantec`.
5. Elija la **Administración > las directivas**. El tecleo **edita** al lado de la directiva apropiada. De la lista desplegable **determinada de la exclusión de la aduana**, elija la exclusión le fijan creado. **RECUERDE SIEMPRE QUE UNA DIRECTIVA PUEDE SOLAMENTE TENER UNA EXCLUSIÓN FIJADA ASOCIADA A ELLA.Note**: Una vez que usted ha creado un conjunto de la exclusión, usted debe agregarlo a cualquier directiva que usted haya creado.



6. Haga clic la **directiva de la actualización** y relance los pasos para cualquier otra directiva que usted quiera el aplicado determinado de la exclusión a. **Note**: Hay un retardo entre una actualización de la directiva y el intervalo de latido siguiente, cuando un conector recibe un cambio de política actualizado.**Tip**: Para determinar el CSIDLs para su producto de seguridad o aplicación actual, entre en contacto el fabricante. Para una lista completa de CSIDLs, refiera a Microsoft Dev Center - escritorio.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Apéndice A: Exclusiones recomendadas

De acuerdo con la lista de la exclusión del contra virus de Microsoft, Cisco recomienda que usted excluye:

Estaciones de trabajo con Windows (genéricas)

- Extensión: .db-journal
- Extensión: .db-wal
- Extensión: .db-shm
- Extensión: .pst
- Extensión: .log
- Ruta: CSIDL_BASEDIR

- Ruta: CSIDL_SYSTEM \ emptyregdb.dat
- Ruta: CSIDL_SYSTEM\CatRoot2
- Ruta: CSIDL_WINDOWS \ Prefetch
- Ruta: CSIDL_PROGRAM_FILES \ Windows Defender
- Ruta: Defensor CSIDL_PROGRAM_FILESX86\Windows
- Ruta: CSIDL_COMMON_APPDATA \ Microsoft \ Windows Defender
- Ruta: CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ edb.chk
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ tmp.edb
- Comodín: * \ System Volume (Volumen del sistema) información \ tracking.log$
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.chk
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.edb
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.jrs
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.log
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.sdb
- Comodín: * \ Windows \ SoftwareDistribution \ Datastore \ registros \ *.log
- Comodín: * \ Windows \ SoftwareDistribution \ Datastore \ \ registros \ edb*.log

Servidores Windows (genéricos)

- Ruta: CSIDL_BASEDIR
- Ruta: CSIDL_SYSTEM \ emptyregdb.dat
- Ruta: CSIDL_SYSTEM\CatRoot2
- Ruta: CSIDL_WINDOWS \ Prefetch
- Ruta: CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ edb.chk
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Ruta: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Ruta: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ tmp.edb
- Ruta: Archivos comprimidos temporales de C:\inetpub\temp\IIS
- Ruta: Archivos comprimidos temporales CSIDL_WINDOWS \ IIS
- Ruta: CSIDL_WINDOWS\system32\inetsrv
- Ruta: CSIDL_WINDOWS\system32\inetsrv\w3wp.exe
- Ruta: CSIDL_WINDOWS\SysWOW64\inetsrv\w3wp.exe
- Ruta: CSIDL_COMMON_APPDATA \ ntuser.pol
- Ruta: CSIDL_WINDOWS\System32\LogFiles
- Ruta: CSIDL_WINDOWS\SysWow64\LogFiles
- Ruta: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\SQLServr.exe

- Ruta: Servicios \ ReportServer \ compartimiento \ ReportingServicesService.exe CSIDL_PROGRAM_FILES \ de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting
- Ruta: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- Ruta: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- Ruta: Servicios \ ReportServer \ compartimiento \ ReportingServicesService.exe CSIDL_PROGRAM_FILES \ de Microsoft SQL Server\MSSQL.3\Reporting
- Ruta: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.chk
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.edb
- Comodín: * \ \ \ base de datos \ *.log de Windows \ de la Seguridad
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.sdb
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.jrs
- Comodín: * \ System Volume (Volumen del sistema) información \ tracking.log$
- Comodín: * \ Windows \ SoftwareDistribution \ Datastore \ registros \ *.log
- Comodín: * \ \ \ SoftwareDistribution \ Datastore \ registros \ edb*.log de Windows
- Extensión: .bak
- Extensión: .ldf
- Extensión: .mdf
- Extensión: .trn
- Extensión: .abf
- Extensión: .ctl
- Extensión: .dbf
- Extensión: .rdo
- Extensión: .arc
- Extensión: .ndf

Nota: Las exclusiones adicionales sugeridas por Microsoft se ponen al día con frecuencia aquí

Reguladores del Dominio de Windows

- Ruta: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Ruta: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Ruta: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb*
- Ruta: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ edb.chk*
- Ruta: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs*
- Ruta: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs*
- Ruta: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log*
- Ruta: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log*
- Ruta: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ registros \ tmp.edb*
- Ruta: *CSIDL_WINDOWS \ ntds \ ntds.dit*
- Ruta: *CSIDL_WINDOWS \ ntds \ EDB.chk*
- Ruta: *CSIDL_WINDOWS \ ntds \ TEMP.edb*
- Ruta: *CSIDL_WINDOWS \ SYSVOL \ dominio \ DO_NOT_REMOVE_NtFrs_PreInstall_Directory*
- Ruta: *CSIDL_WINDOWS \ SYSVOL \ estacionamiento*
- Ruta: *CSIDL_WINDOWS \ SYSVOL \ áreas de montaje*

- Ruta: *CSIDL_WINDOWS \ SYSVOL \ sysvol*
- Ruta: *CSIDL_WINDOWS\System32\ntfrs.exe*
- Ruta: *CSIDL_WINDOWS\System32\dfsr.exe*
- Ruta: *CSIDL_WINDOWS\System32\dfsrs.exe*
- Ruta: *CSIDL_WINDOWS\System32\dns.exe*
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.edb
- Comodín: * \ \ \ base de datos \ *.log de Windows \ de la Seguridad
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.sdb
- Comodín: * \ Windows \ Seguridad \ base de datos \ *.jrs
- Comodín: * \ Windows \ SoftwareDistribution \ Datastore \ registros \ *.log
- Comodín: * \ \ \ SoftwareDistribution \ Datastore \ registros \ edb*.log de Windows
- Comodín: * \ Windows \ ntds \ EDB*.log
- Comodín: * \ Windows \ ntds \ Edbres*.jrs
- Comodín: * \ Windows \ ntds \ *.pat
- Comodín: *\Windows\System32\DNS*.dns
- Comodín: *\Windows\System32\DNS*.scc

Windows - IIS

- Ruta: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Ruta: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Ruta: *Archivos comprimidos temporales de C:\inetpub\temp\IIS*
- Ruta: *Archivos comprimidos temporales CSIDL_WINDOWS \ IIS*
- Ruta: *CSIDL_WINDOWS\system32\inetsrv*
- Ruta: *CSIDL_WINDOWS\system32\inetsrv\w3wp.exe*
- Ruta: *CSIDL_WINDOWS\SysWOW64\inetsrv\w3wp.exe*
- Ruta: *CSIDL_WINDOWS\System32\LogFiles*
- Ruta: *CSIDL_WINDOWS\SysWow64\LogFiles*

Windows - SQL Server

- Extensión: *.bak*
- Extensión: *.ldf*
- Extensión: *.mdf*
- Extensión: *.trn*
- Extensión: *.abf*
- Extensión: *.ctl*
- Extensión: *.dbf*
- Extensión: *.rdo*
- Extensión: *.arc*
- Extensión: *.ndf*
- Ruta: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Ruta: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Ruta: *CSIDL_WINDOWS\System32\LogFiles*
- Ruta: *CSIDL_WINDOWS\SysWow64\LogFiles*
- Ruta: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\SQLServr.exe*

- Ruta: *Servicios \ ReportServer \ compartimiento \ ReportingServicesService.exe CSIDL_PROGRAM_FILES \ de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting*
- Ruta: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe*
- Ruta: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe*
- Ruta: *Servicios \ ReportServer \ compartimiento \ ReportingServicesService.exe CSIDL_PROGRAM_FILES \ de Microsoft SQL Server\MSSQL.3\Reporting*
- Ruta: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe*

Nota: Las exclusiones adicionales sugeridas por Microsoft son con frecuencia updatedHere

Windows - Protección del punto final de Symantec

- Ruta: CSIDL_COMMON_APPDATA \ Symantec
- Ruta: Protección CSIDL_PROGRAM_FILES \ de Symantec \ del punto extremo de Symantec
- Ruta: Protección del punto final CSIDL_PROGRAM_FILESX86\Symantec\Symantec
- Comodín: * \ Windows \ temporero \ musdmys_*
- Comodín: * \ Windows \ temporero \ content.zip.tmp \ *.diff
- Comodín: * \ Windows \ temporero \ content.zip.tmp \ SymDeltaDecompressOptions.xml
- Comodín: * \ Windows \ temporero \ content.zip.tmp \ cur.scr
- Comodín: * \ Windows \ temporero \ TMP*.tmp

Windows - Avast

- Ruta: CSIDL_WINDOWS\Temp_avast5_
- Ruta: CSIDL_WINDOWS \ temporeros \ _avast_

Windows - Avira

- Ruta: CSIDL_APPDATA \ Avira \ escritorio \ TEMPOREROS de AntiVir
- Ruta: CSIDL_LOCAL_APPDATA \ Avira \ escritorio \ TEMPOREROS de AntiVir
- Ruta: CSIDL_PROGRAM_FILES \ Avira \ escritorio \ TEMPOREROS de AntiVir

Windows - Altiris por Symantec

- Ruta: CSIDL_PROGRAM_FILES \ Altiris \ agente \ TaskManagement de Altiris
- Ruta: CSIDL_PROGRAM_FILES \ Altiris \ inventario \ bandeja de salida
- Comodín: * \ Windows \ temporero \ AltirisScript*.cmd

Windows - Tendencia

- Ruta: CSIDL_PROGRAM_FILES \ Trend Micro
- Ruta: Micrófono CSIDL_PROGRAM_FILESX86\Trend

Windows - Kaspersky

- Ruta: CSIDL_COMMON_APPDATA \ Kaspersky Lab

Windows - McAfee

- Ruta: CSIDL_PROGRAM_FILES \ McAfee
- Ruta: CSIDL_PROGRAM_FILESX86\McAfee
- Ruta: CSIDL_COMMON_APPDATA \ McAfee
- Ruta: CSIDL_PROGRAM_FILES \ archivos comunes \ McAfee

Windows Defender

- Ruta: CSIDL_PROGRAM_FILES \ Windows Defender
- Ruta: Defensor CSIDL_PROGRAM_FILESX86\Windows
- Ruta: CSIDL_COMMON_APPDATA \ Microsoft \ Windows Defender

Windows - Vanguardia de Microsoft

- Ruta: Vanguardia CSIDL_PROGRAM_FILES \ de Microsoft
- Ruta: Vanguardia CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Cliente de la Seguridad de Microsoft

- Ruta: Cliente de la Seguridad CSIDL_PROGRAM_FILES \ de Microsoft
- Ruta: Cliente de la Seguridad CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Sophos

- Ruta: CSIDL_PROGRAM_FILES \ Sophos
- Ruta: CSIDL_PROGRAM_FILESX86\Sophos
- Ruta: CSIDL_COMMON_APPDATA \ Sophos \ contra virus de Sophos
- Ruta: CSIDL_COMMON_APPDATA \ Sophos

Vista/Win7 y más nuevo también requiere esta trayectoria.

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

Windows - VSE

- Ruta: CSIDL_PROGRAM_FILES \ VSE
- Ruta: CSIDL_COMMON_APPDATA \ VSE

Mac - Puestos de trabajo (genéricos)

- Ruta: /private/var/vm
- Ruta: ght-V100
- Ruta: /.MobileBackups

- Ruta: /Volumes/MobileBackups/
- Ruta: /Quarantine
- Ruta: Salvaguardias de la máquina de /Volumes/Time
- Comodín: /Volumes/*/.Spotlight-V100
- Comodín: /Volumes/*/.Spotlight-V100*
- Comodín: /Volumes/ */Backups.backupdb
- Comodín: datos del usuario de /Users/ */Documents/Microsoft/oficina 2011 Identities/*
- Comodín: oficina/perspectiva/perspectiva 15 Profiles/* de /Users/ */Library/Group Containers/*
- Comodín: /Users/ */Library/Caches/Outlook/*
- Comodín: /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kcIB*

Mac - Jabber

- Ruta: /bin/ps
- Ruta: /usr/bin/grep
- Comodín: /Users/ */Library/Logs/Jabber

Mac - JAMF Casper

- Ruta: /usr/bin/sw_vers
- Comodín: /Library/Application Support/JAMF/Usage/201*-*-*/.dat*

Mac - McAfee

- Ruta: /Library/McAfee/
- Ruta: Soporte/McAfee/de /Library/Application

Mac - Crashplan

- Ruta: /Library/Caches/CrashPlan/
- Comodín: *.log de /Library/Logs/CrashPlan/

Mac - Fusión

- Ruta: /Library/Logs/VMware/

Mac - Oficina

- Comodín: datos del usuario de /Users/ */Documents/Microsoft/oficina 2011 Identities/*
- Comodín: oficina/perspectiva/perspectiva 15 Profiles/* de /Users/ */Library/Group Containers/*
- Comodín: /Users/ */Library/Caches/Outlook/*
- Comodín: /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kcIB*

Windows - Software de la orilla del lago - Systrack

- Comodín: * \ archivos de programa (x86)\SysTrack\LsiAgent\Condense***.tmp
- Comodín: * \ archivos de programa (x86)\SysTrack\LsiAgent\Condense**.hld

Windows - Aplicaciones SAS

- Extensión: .lck
- Extensión: .sd2
- Extensión: .sc2
- Extensión: .SPDS
- Extensión: .utl
- Comodín: *.sas* (véase la nota en la sección del comodín.)

También la ubicación del trabajo SAS necesita ser excluida, pero la carpeta pudo ser diferente en diversas versiones SAS.

Windows - Splunk

- Ruta: CSIDL_PROGRAM_FILES \ Splunk
- Ruta: CSIDL_PROGRAM_FILESX86\Splunk
- Ruta: CSIDL_PROGRAM_FILES \ Splunk \ var \ liberación \ splunk
- Ruta: CSIDL_PROGRAM_FILESX86\Splunk\var\lib\splunk
- Ruta: CSIDL_PROGRAM_FILES \ SplunkUniversalForwarder
- Ruta: CSIDL_PROGRAM_FILESX86\SplunkUniversalForwarder

Windows - Diebold Varsovia

Éstas son las exclusiones requeridas para el software de actividades bancarias de Diebold Varsovia. Sin estas exclusiones en el lugar la aplicación no instalará correctamente. Si el software está instalado antes de la instalación AMP sin estas exclusiones en el lugar el sistema pudo llegar a ser insensible.

Exclusiones de la trayectoria

- Ruta: C:\Program clasifía (x86)\Diebold\Warsaw
- Ruta: C:\Program Files\Diebold\Warsaw
- Ruta: C:\Windows\System32\drivers\wsddfac.sys

Las versiones más recientes pudieron requerir:

- Ruta: C:\Windows\System32\drivers\gbpddfac64.sys
- Ruta: C:\Program clasifía (x86)\GAS Tecnologia \ Varsovia
- Ruta: C:\Windows\Temp\Diebold\Warsaw

Exclusiones del comodín

- Comodín: _*de C:\Windows\Temp\warsaw
- Comodín: * \ AppData \ Local \ temporero \ warsaw_* de C:\Users\
- Comodín: * \ AppData \ Local \ temporero \ *-*.tmp de C:\Users\
- Comodín: C:\Windows\System32\drivers*-*.tmp

Windows - Una unidad

- Comodín: * \ OneDrive de C:\Users\

Windows - Oficina

- Comodín: C:\Users\ * \ AppData \ Local \ Microsoft \ oficina \ * \ OfficeFileCache