

Configurar e controle exclusões no AMP para valores-limite

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Tipos da exclusão](#)

[Extensão de arquivo](#)

[Caminho](#)

[Convite](#)

[Ameaça](#)

[Processo](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

[Apêndice A: Exclusões recomendadas](#)

[Estações de trabalho do Windows \(genéricas\)](#)

[Windows Server \(genéricos\)](#)

[Controladores do domínio do Windows](#)

[Windows - IIS](#)

[Windows - Servidor SQL](#)

[Windows - Proteção do valor-limite de Symantec](#)

[Windows - Avast](#)

[Windows - Avira](#)

[Windows - Altiris por Symantec](#)

[Windows - Tendência](#)

[Windows - Kaspersky](#)

[Windows - McAfee](#)

[Windows Defender](#)

[Windows - Pelotão da frente de Microsoft](#)

[Windows - Cliente da Segurança de Microsoft](#)

[Windows - Sophos](#)

[Windows - VSE](#)

[Mac - Estações de trabalho \(genéricas\)](#)

[Mac - Jabber](#)

[Mac - JAMF Casper](#)

[Mac - McAfee](#)

[Mac - Crashplan](#)

[Mac - Fusão](#)

[Mac - Escritório](#)

[Windows - Software da beira do lago - Systrack](#)

[Windows - Aplicativos SAS](#)

[Windows - Splunk](#)

[Windows - Diebold Varsóvia](#)

[Windows - Uma movimentação](#)

[Windows - Escritório](#)

Introdução

Este documento descreve como criar exclusões de modo que um AMP para o conector dos valores-limite (A4E) não faça a varredura do diretório do programa. Isto é terminado a fim impedir conflitos ou problemas de desempenho entre um conector de FireAMP e uns aplicativos anti-vírus ou outros. Isto é especialmente importante com assinaturas anti-vírus que contêm as cordas que o conector A4E detecta como malicioso ou emite com arquivos quarantined.

Note: O centro de assistência técnica da Cisco (TAC) não segue o inventário do número potencialmente infinito de aplicativos. A lista de exclusões no apêndice é apenas uma diretriz. Para a informação adicional, leia o Guia do Usuário e a documentação oficiais.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do console da nuvem A4E, o AMP para os valores-limite (A4E), e o Produtos anti-vírus.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Tipos da exclusão

Há cinco tipos de exclusões úteis no console A4E. Se o tipo errado da exclusão é usado, a exclusão não funcionará. É importante notar o formato de cada tipo a fim verificar que a exclusão esteve adicionada corretamente durante o processo de ajustamento.

Extensão de arquivo

Este tipo da exclusão é usado para excluir arquivos de uma determinada extensão, não importa onde é ficado situado na máquina. Exemplos:

- .log
- .txt
- .db

Caminho

Esta exclusão pode ser usada a fim excluir um único dobrador ou arquivá-lo. As exclusões do trajeto são recursivos (todas as subpastas dentro desse trajeto serão excluídas igualmente). As exclusões do trajeto são únicas que podem usar a lista especial constante do artigo ID (CSIDL) como um convite. Os dois formatos do trajeto são:

- CSIDL_WINDOWS\system32
- C:\Windows\system32

Note: “Do fim \” é opcional. Adicionalmente, a estrela do convite “*” o caráter é inválido para o uso dentro de uma exclusão do trajeto.

Convite

Este tipo da exclusão é melhor usado quando você pode ser incapaz de antecipar um dobrador ou um nome de arquivo. Você pode usar convites múltiplos em uma única exclusão também. Os exemplos do convite são:

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

Ameaça

Esta exclusão ajuda a impedir que uns ou vários arquivos estejam feitos a varredura e detectars baseado no nome da ameaça. Isto pode ser útil se você antecipa uma variedade de nomes para um arquivo dado. Alguns exemplos de nomes da ameaça estão abaixo:

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

Processo

As exclusões do processo podem ser usadas para impedir que A4E faça a varredura de todos os arquivos e subprocesses baseados em um processo. Você pode usar a mistura SHA256 do processo ou o caminho de arquivo completo, ou SHA256 e caminho de arquivo junto. Se você usa ambas as partes de dados então ambas as circunstâncias devem ser estadas conformes para que a exclusão trabalhe. Você pode igualmente escolher excluir subprocesses. Os exemplos estão abaixo:

- C:\Program Files\MyApplication.exe

- SHA256 do MyApplication.exe
- Ambos o acima

New Exclusion ✕

Exclusion Type

You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.

Full Path

Maximum 255 characters

SHA-256

If the file size of the process is greater than the maximum scan file size set in your policy, then the SHA-256 of the process will not be computed and the exclusion will not work. Use a path-based process exclusion for files larger than the maximum scan file size.

Also Exclude Child Processes

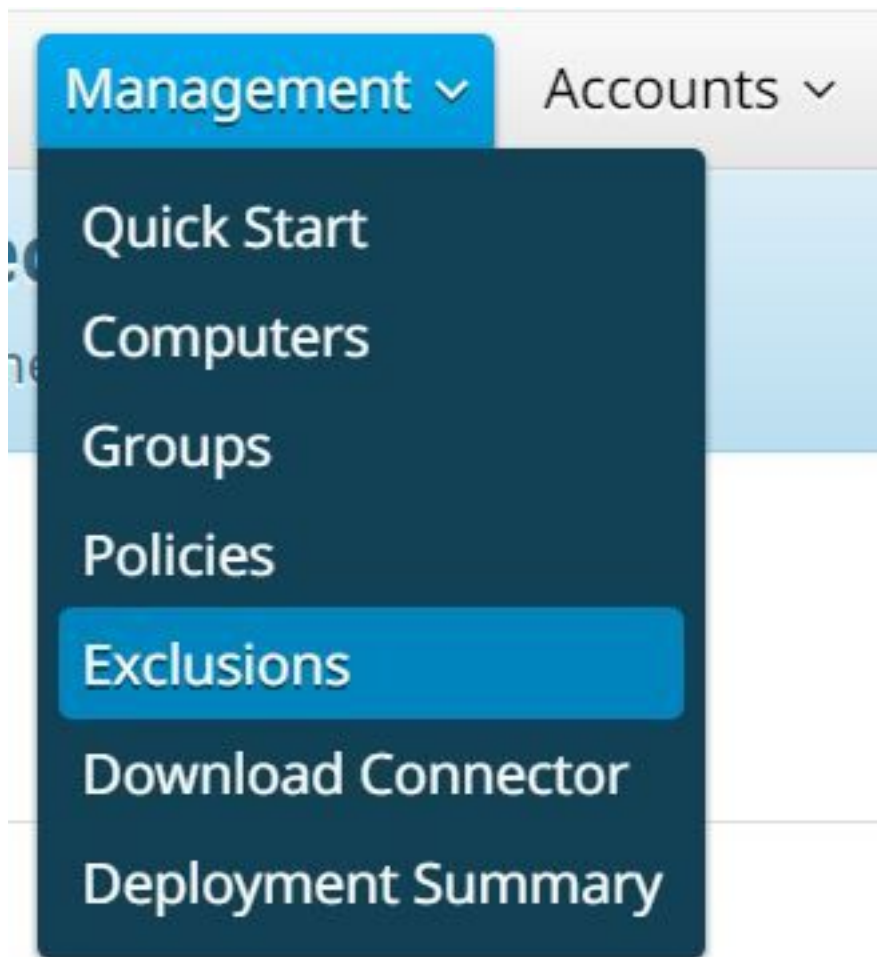
Exclude all child processes created by the parent process in the exclusion from being scanned.

Note: v5.1.13 ou é exigido mais altamente para usar exclusões do processo com as exclusões do processo filho permitidas.

Configurar

A fim criar exclusões, termine estas etapas:

1. Escolha o **Gerenciamento > as exclusões no console da nuvem A4E.**



2. Ou edite um grupo existente da exclusão (preferido) ou o clique **cria a exclusão ajustada** a fim criar uma lista nova de exclusões. Dê entrada com um nome para a lista e o clique **cria**.

Exclusion Set Management [+ Create Exclusion Set](#)

Name:

3. O clique **adiciona a exclusão** a fim adicionar uma exclusão a sua lista. Você será alertado entrar em um trajeto para a exclusão.

Antivirus

Contains 10 exclusions.

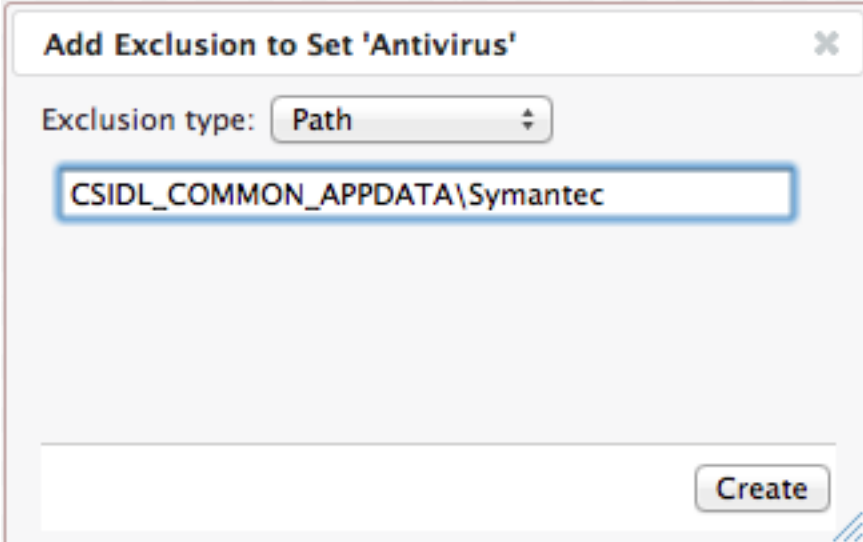
Created by: Marc Fossi on: 2012-01-25 17:04

Not used in any policies.

[+ Add Exclusion](#)

Path: CSIDL_SYSTEM\CatRoot2
Path: CSIDL_WINDOWS\Prefetch
Path: CSIDL_BASEDIR
Path: CSIDL_APPDATA\Avira\AntiVir Desktop\TEMP
Path: CSIDL_LOCAL_APPDATA\Avira\AntiVir Desktop\TEMP
Path: CSIDL_PROGRAM_FILES\Avira\AntiVir Desktop\TEMP
Path: CSIDL_PROGRAM_FILES\AVAST Software
Path: CSIDL_WINDOWS\Temp_avast_
Path: CSIDL_WINDOWS\Temp_avast_
Path: CSIDL_COMMON_APPDATA\Kaspersky Lab\AVP8\Data

- Incorpore o CSIDL dos produtos de software que você instalou em seus valores-limite e clique então **cria**. **Note:** Um valor CSIDL identifica os dobradores especiais usados por um aplicativo. Este é sistema-independente e independente de todo o nome de arquivo ou lugar



The screenshot shows a dialog box titled "Add Exclusion to Set 'Antivirus'". It has a close button (X) in the top right corner. Below the title, there is a label "Exclusion type:" followed by a dropdown menu currently showing "Path". Underneath is a text input field containing the text "CSIDL_COMMON_APPDATA\Symantec". At the bottom right of the dialog is a button labeled "Create".

do sistema. **Note:** No tiro de tela precedente, o nome de diretório é excluído para Symantec. Uma vez que o CSIDL é carregado no computador que executa o conector de FireAMP, o CSIDL resolve ao máximo o trajeto, C:\ProgramData\Symantec.

- Escolha o **Gerenciamento > as políticas**. O clique **edita** ao lado da política apropriada. Da lista de drop-down **ajustada da exclusão do costume**, escolha a exclusão ajustam-no criado. **RECORDE SEMPRE QUE UMA POLÍTICA PODE SOMENTE TER UMA EXCLUSÃO AJUSTADA ASSOCIADA COM ELA.** **Note:** Uma vez que você criou um grupo da exclusão, você deve adicioná-lo a todas as políticas que você criar.

Edit Policy

Name	Default Policy
Custom Whitelist	None
Application Block Lists	None
Simple Custom Detections	None
Advanced Custom Signatures	None
Custom Exclusion Set	None ✓ Exclusions For 'Default Policy' Antivirus
Description	Default Policy for Your Company

Cancel Update Policy

6. Clique a **política da atualização** e repita as etapas para todas as outras políticas que você quiser o aplicativo ajustado da exclusão a. **Note:** Há um atraso entre uma atualização da política e o intervalo de batimento cardíaco seguinte, quando um conector recebe uma alteração de política atualizado. **Tip:** A fim determinar o CSIDLs para seu produtos de segurança ou aplicativo atual, contacte o fabricante. Para uma lista completa de CSIDLs, refira [Microsoft Dev Center - Desktop](#).

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

[Apêndice A: Exclusões recomendadas](#)

Baseado na [lista anti-vírus da exclusão de Microsoft](#), Cisco recomenda que você exclui:

Estações de trabalho do Windows (genéricas)

- Extensão: .db-journal
- Extensão: .db-wal
- Extensão: .db-shm
- Extensão: .pst
- Extensão: .log
- Caminho: CSIDL_BASEDIR

- Caminho: CSIDL_SYSTEM \ emptyregdb.dat
- Caminho: CSIDL_SYSTEM\CatRoot2
- Caminho: CSIDL_WINDOWS \ Prefetch
- Caminho: CSIDL_PROGRAM_FILES \ Windows Defender
- Caminho: Defensor CSIDL_PROGRAM_FILESX86\Windows
- Caminho: CSIDL_COMMON_APPDATA \ Microsoft \ Windows Defender
- Caminho: CSIDL_WINDOWS\system32\GroupPolicy\registry.pol
- Caminho: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb
- Caminho: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb.chk
- Caminho: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs
- Caminho: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs
- Caminho: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log
- Caminho: CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log
- Caminho: CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ tmp.edb
- Convite: * \ informação do volume de sistema \ tracking.log\$
- Convite: * \ Windows \ Segurança \ base de dados \ *.chk
- Convite: * \ Windows \ Segurança \ base de dados \ *.edb
- Convite: * \ Windows \ Segurança \ base de dados \ *.jrs
- Convite: * \ Windows \ Segurança \ base de dados \ *.log
- Convite: * \ Windows \ Segurança \ base de dados \ *.sdb
- Convite: * \ Windows \ SoftwareDistribution \ Datastore \ logs \ *.log
- Convite: * \ Windows \ SoftwareDistribution \ Datastore \ \ logs \ edb*.log

Windows Server (genéricos)

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

- Caminho: CSIDL_PROGRAM_FILES \ serviços de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting \ ReportServer \ escaninho \ ReportingServicesService.exe
- Caminho: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe
- Caminho: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- Caminho: CSIDL_PROGRAM_FILES \ serviços de Microsoft SQL Server\MSSQL.3\Reporting \ ReportServer \ escaninho \ ReportingServicesService.exe
- Caminho: CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe
- Convite: * \ Windows \ Segurança \ base de dados \ *.chk
- Convite: * \ Windows \ Segurança \ base de dados \ *.edb
- Convite: * \ de Windows \ Segurança \ base de dados \ *.log
- Convite: * \ Windows \ Segurança \ base de dados \ *.sdb
- Convite: * \ Windows \ Segurança \ base de dados \ *.jrs
- Convite: * \ informação do volume de sistema \ tracking.log\$
- Convite: * \ Windows \ SoftwareDistribution \ Datastore \ logs \ *.log
- Convite: * \ de Windows \ SoftwareDistribution \ Datastore \ logs \ edb*.log
- Extensão: .bak
- Extensão: .ldf
- Extensão: .mdf
- Extensão: .trn
- Extensão: .abf
- Extensão: .ctl
- Extensão: .dbf
- Extensão: .rdo
- Extensão: .arc
- Extensão: .ndf

Nota: As exclusões adicionais sugeridas por Microsoft são atualizadas frequentemente [aqui](#)

Controladores do domínio do Windows

- Caminho: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Caminho: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Caminho: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ Datastore.edb*
- Caminho: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ edb.chk*
- Caminho: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00001.jrs*
- Caminho: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Edbres00002.jrs*
- Caminho: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res1.log*
- Caminho: *CSIDL_WINDOWS\SoftwareDistribution\Datastore\Logs\Res2.log*
- Caminho: *CSIDL_WINDOWS \ SoftwareDistribution \ Datastore \ logs \ tmp.edb*
- Caminho: *CSIDL_WINDOWS \ ntds \ ntds.dit*
- Caminho: *CSIDL_WINDOWS \ ntds \ EDB.chk*
- Caminho: *CSIDL_WINDOWS \ ntds \ TEMP.edb*
- Caminho: *CSIDL_WINDOWS \ SYSVOL \ domínio \ DO_NOT_REMOVE_NtFrs_PreInstall_Directory*

- Caminho: *CSIDL_WINDOWS \ SYSVOL \ plataforma*
- Caminho: *CSIDL_WINDOWS \ SYSVOL \ áreas de staging*
- Caminho: *CSIDL_WINDOWS \ SYSVOL \ sysvol*
- Caminho: *CSIDL_WINDOWS\System32\ntfrs.exe*
- Caminho: *CSIDL_WINDOWS\System32\dfs.exe*
- Caminho: *CSIDL_WINDOWS\System32\dfsrs.exe*
- Caminho: *CSIDL_WINDOWS\System32\dns.exe*
- Convite: ** \ Windows \ Segurança \ base de dados \ *.edb*
- Convite: ** \ \ de Windows \ Segurança \ base de dados \ *.log*
- Convite: ** \ Windows \ Segurança \ base de dados \ *.sdb*
- Convite: ** \ Windows \ Segurança \ base de dados \ *.jrs*
- Convite: ** \ Windows \ SoftwareDistribution \ Datastore \ logs \ *.log*
- Convite: ** \ \ de Windows \ SoftwareDistribution \ Datastore \ logs \ edb*.log*
- Convite: ** \ Windows \ ntds \ EDB*.log*
- Convite: ** \ Windows \ ntds \ Edbres*.jrs*
- Convite: ** \ Windows \ ntds \ *.pat*
- Convite: **\Windows\System32\DNS*.dns*
- Convite: **\Windows\System32\DNS*.scc*

Windows - IIS

- Caminho: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Caminho: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Caminho: *Arquivos compactados provisórios de C:\inetpub\temp\IIS*
- Caminho: *Arquivos compactados provisórios CSIDL_WINDOWS \ IIS*
- Caminho: *CSIDL_WINDOWS\system32\inetsrv*
- Caminho: *CSIDL_WINDOWS\system32\inetsrv\w3wp.exe*
- Caminho: *CSIDL_WINDOWS\SysWOW64\inetsrv\w3wp.exe*
- Caminho: *CSIDL_WINDOWS\System32\LogFiles*
- Caminho: *CSIDL_WINDOWS\SysWow64\LogFiles*

Windows - Servidor SQL

- Extensão: *.bak*
- Extensão: *.ldf*
- Extensão: *.mdf*
- Extensão: *.trn*
- Extensão: *.abf*
- Extensão: *.ctl*
- Extensão: *.dbf*
- Extensão: *.rdo*
- Extensão: *.arc*
- Extensão: *.ndf*
- Caminho: *CSIDL_COMMON_APPDATA \ ntuser.pol*
- Caminho: *CSIDL_WINDOWS\system32\GroupPolicy\registry.pol*
- Caminho: *CSIDL_WINDOWS\System32\LogFiles*
- Caminho: *CSIDL_WINDOWS\SysWow64\LogFiles*

- Caminho: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Binn\SQLServr.exe*
- Caminho: *CSIDL_PROGRAM_FILES \ serviços de Microsoft SQL Server\MSRS10.MSSQLSERVER\Reporting \ ReportServer \ escaninho \ ReportingServicesService.exe*
- Caminho: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\Bin\MSMDSrv.exe*
- Caminho: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe*
- Caminho: *CSIDL_PROGRAM_FILES \ serviços de Microsoft SQL Server\MSSQL.3\Reporting \ ReportServer \ escaninho \ ReportingServicesService.exe*
- Caminho: *CSIDL_PROGRAM_FILES \ Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe*

Nota: As exclusões adicionais sugeridas por Microsoft são frequentemente [updatedHere](#)

Windows - Proteção do valor-limite de Symantec

- Caminho: *CSIDL_COMMON_APPDATA \ Symantec*
- Caminho: *Proteção CSIDL_PROGRAM_FILES \ Symantec \ ponto final de Symantec*
- Caminho: *Proteção do valor-limite CSIDL_PROGRAM_FILESX86\Symantec\Symantec*
- Convite: ** \ Windows \ Temp \ musdmys_**
- Convite: ** \ Windows \ Temp \ content.zip.tmp \ *.diff*
- Convite: ** \ Windows \ Temp \ content.zip.tmp \ SymDeltaDecompressOptions.xml*
- Convite: ** \ Windows \ Temp \ content.zip.tmp \ cur.scr*
- Convite: ** \ Windows \ Temp \ TMP*.tmp*

Windows - Avast

- Caminho: *CSIDL_WINDOWS\Temp_avast5_*
- Caminho: *CSIDL_WINDOWS \ Temp \ _avast_*

Windows - Avira

- Caminho: *Desktop CSIDL_APPDATA \ Avira \ AntiVir \ TEMP*
- Caminho: *Desktop CSIDL_LOCAL_APPDATA \ Avira \ AntiVir \ TEMP*
- Caminho: *Desktop CSIDL_PROGRAM_FILES \ Avira \ AntiVir \ TEMP*

Windows - Altiris por Symantec

- Caminho: *CSIDL_PROGRAM_FILES \ Altiris \ agente \ TaskManagement de Altiris*
- Caminho: *CSIDL_PROGRAM_FILES \ Altiris \ inventário \ Outbox*
- Convite: ** \ Windows \ Temp \ AltirisScript*.cmd*

Windows - Tendência

- Caminho: *CSIDL_PROGRAM_FILES \ Trend Micro*
- Caminho: *Micro CSIDL_PROGRAM_FILESX86\Trend*

Windows - Kaspersky

- Caminho: CSIDL_COMMON_APPDATA \ Kaspersky Lab

Windows - McAfee

- Caminho: CSIDL_PROGRAM_FILES \ McAfee
- Caminho: CSIDL_PROGRAM_FILESX86\McAfee
- Caminho: CSIDL_COMMON_APPDATA \ McAfee
- Caminho: CSIDL_PROGRAM_FILES \ arquivos comuns \ McAfee

Windows Defender

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

Windows - Pelotão da frente de Microsoft

- Caminho: CSIDL_PROGRAM_FILES \ pelotão da frente de Microsoft
- Caminho: Pelotão da frente CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Cliente da Segurança de Microsoft

- Caminho: CSIDL_PROGRAM_FILES \ cliente Segurança de Microsoft
- Caminho: Cliente da Segurança CSIDL_PROGRAM_FILESX86\Microsoft

Windows - Sophos

- Caminho: CSIDL_PROGRAM_FILES \ Sophos
- Caminho: CSIDL_PROGRAM_FILESX86\Sophos
- Caminho: CSIDL_COMMON_APPDATA \ Sophos \ Sophos anti-vírus
- Caminho: CSIDL_COMMON_APPDATA \ Sophos

Vista/Win7 e mais novo igualmente exigem este trajeto.

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

Windows - VSE

- Caminho: CSIDL_PROGRAM_FILES \ VSE
- Caminho: CSIDL_COMMON_APPDATA \ VSE

Mac - Estações de trabalho (genéricas)

- Caminho: /private/var/vm
- Caminho: ght-V100
- Caminho: /.MobileBackups
- Caminho: /Volumes/MobileBackups/
- Caminho: /Quarantine
- Caminho: Apoios da máquina de /Volumes/Time
- Convite: /Volumes/*.Spotlight-V100
- Convite: /Volumes/*.Spotlight-V100*
- Convite: /Volumes/ */Backups.backupdb
- Convite: dados do usuário de /Users/ */Documents/Microsoft/escritório 2011 Identities/*
- Convite: escritório/probabilidade/probabilidade 15 Profiles/* de /Users/ */Library/Group Containers/*
- Convite: /Users/ */Library/Caches/Outlook/*
- Convite: /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kclB*

Mac - Jabber

- Caminho: /bin/ps
- Caminho: /usr/bin/grep
- Convite: /Users/ */Library/Logs/Jabber

Mac - JAMF Casper

- Caminho: /usr/bin/sw_vers
- Convite: /Library/Application Support/JAMF/Usage/201*-*/.dat*

Mac - McAfee

- Caminho: /Library/McAfee/
- Caminho: Apoio de /Library/Application/McAfee/

Mac - Crashplan

- Caminho: /Library/Caches/CrashPlan/
- Convite: *.log de /Library/Logs/CrashPlan/

Mac - Fusão

- Caminho: /Library/Logs/VMware/

Mac - Escritório

- Convite: dados do usuário de /Users/ */Documents/Microsoft/escritório 2011 Identities/*
- Convite: escritório/probabilidade/probabilidade 15 Profiles/* de /Users/ */Library/Group Containers/*
- Convite: /Users/ */Library/Caches/Outlook/*
- Convite: /Users/ */Library/Caches/TemporaryItems/Outlook Temp/*kclB*

Windows - Software da beira do lago - Systrack

- Convite: * \ arquivos de programa (x86)\SysTrack\LsiAgent\Condense**.tmp
- Convite: * \ arquivos de programa (x86)\SysTrack\LsiAgent\Condense**.hld

Windows - Aplicativos SAS

- Extensão: .lck
- Extensão: .sd2
- Extensão: .sc2
- Extensão: .SPDS
- Extensão: .utl
- Convite: *.sas* (veja a nota na seção do convite.)

Igualmente o lugar do trabalho SAS precisa de ser excluído, mas o dobrador pôde ser diferente em versões diferentes SAS.

Windows - Splunk

- Caminho: CSIDL_PROGRAM_FILES \ Splunk
- Caminho: CSIDL_PROGRAM_FILESX86\Splunk
- Caminho: CSIDL_PROGRAM_FILES \ Splunk \ var \ liberal \ splunk
- Caminho: CSIDL_PROGRAM_FILESX86\Splunk\var\lib\splunk
- Caminho: CSIDL_PROGRAM_FILES \ SplunkUniversalForwarder
- Caminho: CSIDL_PROGRAM_FILESX86\SplunkUniversalForwarder

Windows - Diebold Varsóvia

Estas são as exclusões exigidas para o software de operação bancária de Diebold Varsóvia. Sem estas exclusões no lugar o aplicativo não instalará corretamente. Se o software é instalado antes da instalação AMP sem estas exclusões no lugar o sistema pôde tornar-se sem resposta.

Exclusões do trajeto

- Caminho: C:\Program arquivos (x86)\Diebold\Warsaw
- Caminho: C:\Program Files\Diebold\Warsaw
- Caminho: C:\Windows\System32\drivers\wsddfacs.sys

Umhas versões mais novas puderam exigir:

- Caminho: C:\Windows\System32\drivers\gbpddfacs64.sys
- Caminho: C:\Program arquivos (x86)\GAS Tecnologia \ Varsóvia
- Caminho: C:\Windows\Temp\Diebold\Warsaw

Exclusões do convite

- Convite: *_de C:\Windows\Temp\warsaw
- Convite: * de C:\Users\ \ AppData \ Local \ Temp \ warsaw_*
- Convite: * De C:\Users\ \ AppData \ Local \ Temp \ *-*.tmp
- Convite: C:\Windows\System32\drivers*-*.tmp

Windows - Uma movimentação

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

Windows - Escritório

- Convite: C:\Users\ * \ AppData \ Local \ Microsoft \ escritório \ * \ OfficeFileCache