

SOPHOS

Sophos Enterprise Console 3.1 Anleitung zur Entfernung von Fremdsoftware

Dokumentdatum: April 2008



Inhalt

1	Einleitung.....	3
2	Systemanforderungen.....	4
3	Was ist das Third-Party Security Software Removal Tool?.....	5
4	Befehlszeilenparameter.....	7
5	Konfigurationsoptionen.....	8
6	Copyright.....	11

1 Einleitung

Diese Anleitung beschreibt Folgendes:

- Erkennung von Sicherheitssoftware von Fremdherstellern
- Entfernung von Sicherheitssoftware von Fremdherstellern
- Konfiguration des Removal Tools

2 Systemanforderungen

Das Dienstprogramm zur Entfernung von Fremdsoftware (kurz: *Removal-Tool*) lässt sich auf folgenden Plattformen einsetzen:

- Windows 98/Me
- Windows NT
- Windows 2000/XP
- Windows Vista
- Windows 2003 Server

Folgende Plattformen betrachtet das Removal-Tool als Server-Plattformen (siehe [Konfigurationsoptionen](#) auf Seite 8):

- Windows NT Server 4.0
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows Server 2003
- Windows Server 2008

3 Was ist das Third-Party Security Software Removal Tool?

Es gibt zwei Versionen des Removal-Tools. 1) Das **Standard-Tool** wird als Komponente der Sophos Installationspakete in einem Ordner namens „CRT“ im zentralen Installationsverzeichnis (CID) installiert. 2) Das **Standalone-Tool** ist optional auf der Sophos Website als Download erhältlich.

Beide Tools bestehen aus zwei Programmen:

- dem im Hintergrund laufenden Tool „AVRemoveW.exe“
- dem interaktiven Tool „AVRemove.exe“, das Meldungen bei Ausführung an die Konsole ausgibt

Diese Tools können automatisch Sicherheitssoftware von Fremdherstellern erkennen und entfernen.

Eine aktuelle Liste der Software, die das Tool entdecken kann, erhalten Sie durch Eingabe des Parameters `-l` oder `--listproducts` an der Befehlszeile. Weitere Informationen finden Sie unter [Befehlszeilenparameter](#) auf Seite 7.

3.1 Das Standard-Tool

Das Standard-Tool kann die gängigsten Sicherheitsprodukte anderer Hersteller entfernen. Die Liste der erkannten Sicherheitsprodukte lässt sich jedoch nicht ändern. Dieses Tool ist in folgenden Paketen enthalten:

- EEXP
- EESCP
- EENT
- EE9X

Wenn Sie eins dieser Pakete abonnieren, wird das Standard-Tool nach dem Herunterladen automatisch im CID gespeichert. Bevor der RMS-Agent und die Sophos Sicherheitssoftware auf Ihrem Computer installiert wird, startet der Installer das Removal-Tool. Im Assistenten **Computer schützen** von Enterprise Console können Sie bestimmen, ob Sicherheitssoftware von Fremdherstellern automatisch entfernt werden soll. Wenn automatische Entfernung nicht erwünscht ist, unternimmt das Tool trotzdem einen Erkennungsversuch auf Fremdsoftware, deinstalliert sie jedoch nicht. Bei Erkennung von Sicherheitssoftware wird eine Meldung an Enterprise Console gesendet und die Installation abgebrochen. Die Konfigurationsoptionen werden unter [Konfigurationsoptionen](#) auf Seite 8 beschrieben.

3.2 Das Standalone-Tool

Mit dem Standalone-Tool können Sie eine größere Auswahl an Sicherheitssoftware entfernen als mit dem Standard-Tool. Für diese Version ist in der Regel die Unterstützung durch Sophos Professional Services erforderlich.

Dieses Tool kann als eigenständiges Tool über die Befehlszeile ausgeführt werden. Es kann jedoch auch in ein CID verschoben werden, sodass der Installer statt des Standard-Tools das Standalone-Tool ausführt.

Wenn Letzteres erwünscht ist, verschieben Sie den *Remover*-Ordner in das CID (auf gleicher Ebene mit dem *CRT*-Ordner). Der Installer sucht nun im *Remover*-Ordner nach dem Removal-Tool.

4 Befehlszeilenparameter

Hinweis: Bei den Befehlszeilenparametern muss nicht auf Groß- und Kleinschreibung geachtet werden. Sowohl das Standard-Tool als auch das Standalone-Tool unterstützt die folgenden Optionen.

Um die Befehlszeilenparameter verwenden zu können, öffnen Sie eine Befehlszeile (über **Start** > **Ausführen** und Eingabe von **cmd.exe**), suchen Sie den CRT-Ordner im Sophos Central Installation Directory und geben Sie **avremove** gefolgt vom gewünschten Parameter (siehe Tabelle) ein.

Befehl	Funktion
<code>-d</code> oder <code>--detectOnly</code>	Ausführung nur im Erkennungsmodus. Erkannte Fremdsoftware wird nicht entfernt. In Kombination mit dem Parameter <code>--firewalls</code> bleiben auch Firewalls von der Deaktivierung verschont.
<code>-f</code> oder <code>--firewalls</code>	Erkennung und Entfernung von Firewalls und Software-Suites.
<code>-h</code> oder <code>--help</code>	Anzeige der Hilfe zu den Befehlszeilenparametern.
<code>-l</code> oder <code>--listproducts</code>	Anzeige der Liste von Software, die das Tool erkennen kann.
<code>-v</code> oder <code>--version</code>	Anzeige der Versionsnummer des Tools.

5 Konfigurationsoptionen

Mit der Konfigurationsdatei, die mit dem Removal-Tool geliefert wird, können Sie das Verhalten des Removal-Tools bestimmen.

Suchen Sie zunächst im CID die Archivdatei „data.zip“. Extrahieren Sie aus diesem Archiv die Datei „crt.cfg“ und öffnen Sie sie in einem Texteditor. Speichern Sie die geänderte Datei im gleichen Verzeichnis wie „data.zip“. Wenn das Removal-Tool aufgerufen wird, zieht es nun statt der Standarddatei stets diese Datei heran.

Falls nicht anders angegeben, stehen die im Folgenden aufgeführten Optionen sowohl dem Standard-Tool als auch dem Standalone-Tool zur Verfügung.

Die Konfigurationsdatei bietet folgende Optionen:

5.1 DetectOnly

Vorgabe: `DetectOnly=0`

Dieser Parameter legt fest, ob das Removal-Tool nur im Erkennungsmodus gestartet werden soll. Standardmäßig versucht das Tool, erkannte Virenschutzsoftware oder Firewalls zu entfernen. `DetectOnly=0` kann in der Befehlszeile durch den Parameter `-d` ignoriert werden.

`DetectOnly=1` bedeutet, dass erkannte Sicherheitssoftware **nicht** entfernt wird.

`DetectOnly` setzt andere Optionen, die in Konflikt stehen könnten, außer Kraft, so z.B. [RemoveSuites](#) auf Seite 9. Wenn `DetectOnly` gesetzt ist (Wert = 1), wird die Software unabhängig von der `RemoveSuites`-Option nur erkannt, jedoch nicht entfernt.

5.2 RemoveFirewalls

Vorgabe: `RemoveFirewalls=0`

Hinweis: Diese Option kann bei der Installation von Sophos Produkten in der Benutzeroberfläche außer Kraft gesetzt werden. Wenn bei der Installation von Sophos Client Firewall die Entfernung von Fremdsoftware ausgewählt wurde, werden alle anderen auf Ihrem System erkannten Firewalls entfernt. Die Option in dieser Datei hat in diesem Fall keine Wirkung.

Dies sagt dem Tool, ob Firewalls erkannt oder entfernt werden sollen. Standardmäßig erkennt oder entfernt das Tool keine Firewalls. `RemoveFirewalls=0` kann in der Befehlszeile durch den Parameter `-f` ignoriert werden.

`RemoveFirewall=1` bedeutet, dass erkannte Firewalls anderer Hersteller entfernt werden.

Hinweis: Über diese Option werden außerdem erkannte Software-Suites entfernt. Durch das Setzen dieser Option (Wert = 1) wird die `RemoveSuites`-Option außer Kraft gesetzt.

5.3 RemoveSuites

Vorgabe: `RemoveSuites=0`

Hinweis: Diese Option kann bei der Installation von Sophos Produkten in der Benutzeroberfläche außer Kraft gesetzt werden. Wenn bei der Installation von Sophos Client Firewall die Entfernung von Fremdsoftware ausgewählt wurde, werden alle anderen auf Ihrem System erkannten Firewalls entfernt. Die Option in dieser Datei hat in diesem Fall keine Wirkung.

Diese Option bestimmt, ob Software-Suites entfernt werden sollen. Software-Suites umfassen Produkte, die sich aus einer Virenschutz- und einer Firewall-Komponente zusammensetzen. Standardmäßig erkennt oder entfernt das Tool keine erkannten Software-Suites.

`RemoveSuites=1` bedeutet, dass erkannte Software-Suites anderer Hersteller entfernt werden.

Hinweis: Da Software-Suites ein Virenschutzprodukt enthalten, werden sie standardmäßig erkannt. Diese Option bestimmt, ob Suites nach der Erkennung entfernt werden sollen.

5.4 RemoveUpdateTools

Vorgabe: `RemoveUpdateTools=0`

Diese Option bestimmt, ob erkannte Update-Tools zu Sicherheitssoftware von Fremdherstellern entfernt werden sollen. Standardmäßig erkennt oder entfernt das Tool keine Update-Tools.

`RemoveUpdateTools=1` bedeutet, dass erkannte Update-Tools anderer Hersteller entfernt werden.

5.5 RunOnServers

Vorgabe: `RunOnServers=1`

Diese Option bestimmt, ob das Removal-Tool auf Server-Plattformen ausgeführt werden soll. Standardmäßig läuft das Tool problemlos auf Server-Plattformen.

`RunOnServers=0` bedeutet, dass ein Fehler ausgegeben wird, wenn das Removal-Tool auf einem Server ausgeführt wird.

5.6 TraceLogging

Vorgabe: `TraceLogging=1`

Diese Option veranlasst das Removal-Tool, alle Daten, darunter Debug-Informationen, zu protokollieren. Standardmäßig ist die Protokollierung aktiviert.

`TraceLogging=0` bedeutet, dass nur Fehler protokolliert werden.

5.7 ProductCatalog

Hinweis: Diese Option steht nur dem Standalone-Tool zur Verfügung.

Diese Option gibt an, welche ProductCatalog-Datei das Removal-Tool verwenden soll. Dabei handelt es sich um die Datei, in der die Software aufgelistet ist, die das Removal-Tool erkennen und entfernen kann.

Standardmäßig befindet sich die Datei „ProductCatalog.xml“ in der Archivdatei „data.zip“, die mit dem Removal-Tool geliefert wird. Wenn Sie weitere Produkte in die Liste aufnehmen möchten, müssen Sie die ProductCatalog-Datei aus dem Archiv extrahieren und den Pfad darauf in der Datei „crt.cfg“ festlegen.

Beispiel: `ProductCatalog=C:\ProductCatalog.xml`

Hinweis: Das Removal-Tool muss von dem Computer, der geschützt werden soll, auf den angegebenen Pfad zugreifen können. Bei dem Pfad kann es sich um ein lokales Verzeichnis auf der Festplatte des Clients handeln, um ein Netzwerkverzeichnis (UNC-Pfad), um ein zugeordnetes Netzlaufwerk oder um den *Remover*-Ordner, in dem sich das Removal-Tool befindet.

5.8 LogFilePath

Diese Option bestimmt, in welchem Verzeichnis die Protokolldatei angelegt werden soll.

Die Vorgabe `LogFilePath=` bedeutet, dass die Protokolldatei im temporären Verzeichnis des Benutzers angelegt wird. Wenn Sie dies ändern möchten, geben Sie hier einfach das gewünschte Verzeichnis für die Protokolldatei an.

Beispiel: `LogFilePath=C:\LoggingCRT`

6 Copyright

Copyright © 2008 Sophos Group. Alle Rechte vorbehalten. Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Sophos und Sophos Anti-Virus sind eingetragene Marken der Sophos Plc und der Sophos Group. Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

6.1 Technischer Support

Technischen Support erhalten Sie auf <http://www.sophos.de/support/>.

Wenn Sie sich an den Technischen Support wenden, halten Sie möglichst folgende Informationen bereit:

- Sophos Software-Versionsnummer(n)
- Betriebssystem(e) und Patch-Level(s)
- Die genauen Fehlermeldungen