Universität zu Köln
Regionales Rechenzentrum
Abteilung Nutzer- und
Anwendungsunterstützung

Stand: Mai 2020

Sophos Anti-Virus (SAV) – Dokumentation

Inhalt

1. Allgemeine Infos und Kontakt

Kontakt

Bei Fragen oder Problemen wenden Sie sich bitte unter Angabe von Betriebssystem, Sophos-Version, eingesetzter beziehungsweise aktivierter Firewall (etwa Sophos Client Firewall) und der Fehlermeldung beziehungsweise Angabe der Protokoll-Datei per E-Mail an den RRZK-Helpdesk.

Bei lizenzrechtlichen Fragen wenden Sie sich bitte an softwaremgr@uni-koeln.de.

Laufzeit

Laufzeit des aktuellen Vertrages bis: 30.09.2024

Links zu Sophos u.a.

Download der Software:
Online-Softwareshop der Universität zu Köln
Webseite der Firma Sophos:
http://www.sophos.de/
Download der Virendefinitionen bei Sophos:
http://www.sophos.de/downloads/ide/
Download der SAV Dokumentation bei Sophos:
http://www.sophos.com/de-de/support/documentation.aspx

2. Verfügbare Produkte

Der Vertrag mit der Firma Sophos (Laufzeit bis 30.09.2024) umfasst die folgenden Produkte:

- Endpoint Protection Advanced
- Server Protection (Windows/Linux)
- Pure Message for Exchange
- Pure Message for Unix
- Secure E-Mail Gateway
- Endpoint eXploit Prevention
- Sophos Central Endpoint und Intercept X für Clients

Der Vertrag erlaubt insbesondere, Sophos Anti-Virus (SAV) auf Rechnern in der Universität und auf Privatrechnern von Angehörigen der Universität zu Köln einzusetzen.

3. Lizenzbedingungen

Mit dem Herunterladen der Software erkennen Sie die Lizenzbedingungen der Firma Sophos sowie die allgemeinen Lizenzbedingungen des RRZK (wie auf unseren Webseiten veröffentlicht) an:

- Die Software darf von Beschäftigten und Studierenden der Universität zu Köln sowohl auf privaten als auch auf dienstlichen Geräten installiert und genutzt werden.
- Die kommerzielle Nutzung der Software ist verboten.
- Eine Weitergabe der Software an Dritte ist ebenfalls untersagt.
- Es darf immer die jeweils aktuellste Version der Software eingesetzt werden.
- Das Nutzungsrecht gilt bis zum 30.09.2024 (Ende des aktuellen Vertrags) oder bis zum Ausscheiden aus der Universität (je nachdem, welches Ereignis zuerst eintritt).

4. Download der Software aus dem Online-Softwareshop des RRZK

4.1 Download

Für die lokale Installationen muss SAV aus dem Online-Softwareshop des RRZK heruntergeladen werden: https://rrzk.uni-koeln.de/software-multimedia/software/software-shop

Sie finden die entsprechenden Artikel im Shop, wenn Sie in der linken Spalte in der Rubrik „Campuslizenzen“ den Hersteller „Sophos“ auswählen.

Nach dem Abschluss der Bestellung finden Sie die Installationsdateien in Ihrem Downloadbereich (in der rechten Spalte unter „Meine Einstellungen“ → „Meine Downloads“).

4.2 Versionen

Im Softwareshop können Sie zwischen vier Versionen wählen:

- Sophos Endpoint and Server for Windows (inkl. Client Firewall)
- Sophos Endpoint and Server for Windows (nur Anti-Virus)
- Sophos Endpoint for Mac
- Sophos Endpoint for Linux

Das für Endbenutzer zentrale Programm der Firma Sophos ist Sophos Anti-Virus (SAV) zur Abwehr von Computer-Viren und anderen Schädlingen. Neben SAV kann die Sophos Client Firewall (SCF) von Interesse sein, die ein installiertes SAV voraussetzt und unerwünschte Zugriffe aus dem Internet zum Rechner oder vom Rechner in das Internet (zum Beispiel bei Trojanern) verhindern kann. Die Sophos Client Firewall blockiert standardmäßig jeglichen Datenverkehr, außer er wird explizit erlaubt. Es muss also für jedes Programm, bspw. Mozilla Firefox als Internetbrowser, eine Ausnahme hinzugefügt werden. Grundsätzlich ist der Schutz durch die Windows Firewall ausreichend, bei Interesse kann jedoch auch die Sophos Client Firewall installiert werden.

Wenn Sie eines der übrigen, im Rahmen der Landeslizenz erhältlichen Produkte nutzen möchten (siehe Punkt2), wenden Sie sich bitte an softwaremgr@uni-koeln.de.

5. Installation

5.1 Allgemeines

Vor der Installation von SAV muss jede andere Anti-Viren-Software deinstalliert werden.

Unter Windows kann es vorkommen, dass trotz Deinstallation anderer Antivirus-Software die Installation von SAV mit der Meldung "Installation konnte nicht fortgesetzt werden, da ein anderes Anti-Viren-Programm auf diesem Computer existiert." abgebrochen wird. Suchen Sie in diesem Fall bitte mit Administratorrechten im Verzeichnis C:\Windows\Temp (im Windows-Installations-Verzeichnis\Temp) nach der Datei „Sophos AntiVirus Competitorlist.txt“. Dort wird normalerweise protokolliert, welcher Registry-Eintrag die Installation verhindert. Dieser Eintrag muss dann gelöscht werden.

Startup-Anleitungen für die Installation und Handbücher für die Konfiguration und Benutzung finden Sie auf den Webseiten der Firma Sophos.

In allen Fällen muss während oder auch nach der Installation die "AutoUpdate-Funktion" von SAV konfiguriert werden (vergleiche Abschnitt 6).

5.2 Lokale Installation

Nach dem Download und Entpacken des Archivs wird SAV entsprechend der üblichen Installation von Software auf Ihrem Betriebssystem installiert. Hierbei kann zuerst einmal das Konfigurieren der AutoUpdate-Funktion übersprungen und später nachgeholt werden.

Nach der Installation muss SAV (im Startmenü) aufgerufen und das Verhalten beim Überprüfen von Dateien konfiguriert werden (Menü Konfigurieren, On-Access-Überprüfung oder Konfigurieren, On-Demand-Erweiterungen und -Ausnahmen), wobei u.a. die Maßnahmen (Umbenennen, Verschieben, Löschen) beim Entdecken eines Virus festgelegt werden (siehe Abschnitt 6).

Die einzelnen Arbeitsschritte für die lokale Installation und Konfiguration von SAV:

- Herunterladen des Installationspakets.
- Starten dieser Datei mit Administratorrechten und Installieren von SAV, dabei Vorgaben akzeptieren.

- Sobald der Dialog "Eigenschaften von Sophos AutoUpdate" erscheint, die Adresse des Servers eingeben:

  Windows:

  Primary Server: http://rzk-adsec5.ad.uni-koeln.de/Bootstrap-Verzeichnisse-3/SAVSCFXP/

  Mac:

  http://sophosupdate.rrz.uni-koeln.de/ESCOSX/

  (weitere Update-Server siehe Abschnitt 6).

- "Benutzername" und "Passwort" sind nicht erforderlich.
- Mit Klick auf [OK] bestätigen (die restlichen (Vor-) Einstellungen werden damit übernommen).
- Erste Aktualisierung durch Doppelklick auf den blau-weißen Sophos-Schild in der Windows-Symbolleiste starten.

Das lokal installierte SAV ist so konfiguriert, dass es sich automatisch in festen Zeitintervallen (60 Minuten) über einen unserer Update-Server aktualisiert und keine manuellen Eingriffe mehr notwendig sind.

Bitte beachten Sie, dass aus lizenzrechtlichen Gründen ein Update der Virendefinitionen nur innerhalb des Uninetzes UKLAN möglich ist. Für Geräte, die sich nicht dauerhaft im Netz der Universität befinden, ist die Installation von Sophos daher nur dann sinnvoll, wenn Sie regelmäßig eine VPN-Verbindung zur Universität aufbauen. Ohne regelmäßige Updates ist der Schutz vor Schadsoftware nicht gewährleistet.

6. Konfiguration der automatischen Updates

6.1 Allgemeines

Das Programm Sophos Anti-Virus selbst (die Detection Engine) und vor allem die Virenkennungen (Virendefinitionen, Virensignaturen, ide-Dateien) müssen regelmäßig aktualisiert werden, um möglichst großen Schutz zu erhalten. Ein absoluter Schutz ist nicht möglich. Am sinnvollsten ist es, in festen Zeitabständen von z.B. 60 Minuten automatisch überprüfen zu lassen[1], ob neue Virenkennungen oder neue Programmversionen installiert werden können. In manchen Fällen muss

[1] Das Zeitintervall von 60 Minuten ist bei der Installation bereits voreingestellt und sollte nicht verändert werden.

nach dem Update auf eine neue Programmversion unter Windows ein Neustart des Systems durchgeführt werden. Ohne aktuelle Updates ist der Computer nicht ausreichend geschützt.

Der Dialog zur Konfiguration der AutoUpdate-Funktion wird unter Windows durch den Aufruf von Sophos Endpoint Security and Control über das Startmenü, dann Befehl "Updates konfigurieren" geöffnet. Für andere Betriebssysteme beachten Sie bitte die ausführlichen Dokumentationen des Herstellers.

Wichtig bei der Konfiguration ist die Angabe der Server, von denen die Updates bezogen werden sollen. Es können bis zu zwei Server angegeben werden, ein Primary Server und ein Secondary Server. Beim Updateversuch fragt SAV zuerst den Primary Server ab und anschließend, falls kein Kontakt zustande kommt, den Secondary Server. Ausreichend ist prinzipiell die Angabe eines funktionsfähigen Primary Servers.

Die Auto-Update-Funktion aktualisiert Programm und ide-Dateien.

6.2 Rechner im UKLAN

SAV mit AutoUpdate-Funktion kann sich automatisch aktualisieren, wenn der Rechner über eine Netzwerk- oder Internet-Verbindung verfügt. Die Funktion muss bei der Installation oder später z.B. so konfiguriert werden, dass sie in einem festen Zeitintervall auf den eingerichteten Update-Servern des RRZK nach Updates sucht. Anzugeben ist hierbei ein Primary Server, falls vorhanden, sollte zur Sicherheit auch ein Secondary Server angegeben werden. Verwenden Sie dazu bitte die folgenden Daten:

Windows

Primary Server: http://rzk-adsec5.ad.uni-koeln.de/Bootstrap-Verzeichnisse-3/SAVSCFXP/
Secondary Server: http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse-3/SAVSCFXP/

MacOS-X

Primary Server: http://rzk-adsec5.ad.uni-koeln.de/Bootstrap-Verzeichnisse-3/ESCOSX/
Secondary Server: http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse-3/ESCOSX/

Linux

Primary Server: http://rzk-adsec5.ad.uni-koeln.de/Bootstrap-Verzeichnisse-3/savlinux/
Secondary Server: http://rzk-efms4.ef.uni-koeln.de/Bootstrap-Verzeichnisse-3/savlinux/

6.3 Mobile Rechner und Rechner außerhalb des UKLAN

Bitte beachten Sie, dass aus lizenzrechtlichen Gründen ein Update der Virendefinitionen nur innerhalb des Uninetzes UKLAN möglich ist. Um die Aktualisierungen auch von außerhalb der Universität empfangen zu können, muss daher zunächst eine VPN-Verbindung hergestellt werden. Daher ist der Betrieb der Software auf mobilen Geräten nicht empfehlenswert, sofern nicht regelmäßig eine Verbindung zum Netz der Universität aufgebaut wird, da die Sicherheit des Gerätes sonst nicht gewährleistet werden kann.

7. Hinweise zur Benutzung

Erkennen unter Windows, ob Sophos AV aktiv ist

Sophos AV besteht aus zwei Komponenten:

- On-Access-Scanner (prüfen beim Zugriff)
- On-Demand-Scanner (prüfen auf Befehl)

Der On-Access-Scanner prüft als Windows-Dienst jede Datei, die geöffnet wird, etwa beim Lesen einer E-Mail oder beim Bearbeiten einer Textdatei. Der On-Demand-Scanner kann z.B. über das Tray Icon (ein weißes Schild mit einem blauen S) aufgerufen werden, um die Dateien der Festplatte oder eines Ordners gezielt zu prüfen (zu "scannen"), ohne jede einzelne Datei öffnen zu müssen.

Der On-Access-Scanner sollte immer aktiv sein. Zu erkennen ist dies am Sophos-Symbol in der Taskleiste: SAV ist aktiv, wenn das Schild-Symbol blau ist. Ist das Symbol grau, so ist der Dienst deaktiviert worden und sollte – notfalls durch einen Neustart von Windows – unbedingt aktiviert werden, um den Schutz des Rechners wiederherzustellen. Kann er nicht aktiviert werden, könnte ein Virus die Ursache sein und der Rechner sollte bis zur Klärung oder Beseitigung vom Netz genommen werden.

Aktualisieren

Der mögliche Schutz ist nur gegeben, wenn SAV regelmäßig automatisch aktualisiert wird (siehe Abschnitt 6). Dies bezieht sich insbesondere auf neue Virendefinitionen. Absolute Sicherheit vor Viren ist aber nicht möglich.

Entfernen von Malware

Ist ein Rechner von einem Virus befallen, so kann in vielen Fällen SAV je nach Konfiguration (siehe Befehl "Konfigurieren, On-Access-Überprüfung" in SAV) den Virus melden, verschieben, umbenennen oder auch löschen.

Einige Viren unter Windows können nur mit speziellen Programmen im "geschützten Modus" von Windows beseitigt werden. In solchen Fällen finden Sie spezielle Programme sowie Informationen zum Säubern des Rechners bei den Herstellern von Anti-Viren-Programmen, unter anderem auch bei Sophos. In schwierigen Fällen hilft auch der Helpdesk des RRZK. (Notieren Sie für die Suche nach den passenden Informationen oder Fragen an den Helpdesk den von SAV gemeldeten Namen des Virus.)

8. Problem-Meldungen

Probleme mit Sophos Produkten melden Sie bitte per E-Mail an den RRZK-Helpdesk unter Angabe von:

- Betriebssystem
- SAV-Version (etwa 10.8)

  Sie finden diese Information in Sophos Endpoint Security and Control unter Hilfe -> Information zu Sophos Endpoint Security and Control
- eingesetzter bzw. aktivierter Firewall (Windows Firewall oder Sophos Client Firewall?)
- Fehlermeldung bzw. Angaben der Log-Datei