# Konfiguration von SOPHOS Antivirenprogrammen für den JURA KI Assistenten

(Stand: 19.03.2026)

# Anleitung für Sophos Endpoint Protection

Der JURA KI Assistent verwendet bestimmte Systemfunktionen, die von Sicherheitssoftware wie **Sophos Endpoint Protection** gelegentlich als verdächtig eingestuft werden können. Um eine reibungslose Nutzung zu gewährleisten, sind entsprechende Konfigurationen in Sophos erforderlich. Dies beinhaltet das Hinzufügen von Ausnahmen für die ausführbaren Dateien und spezifische Sicherheitsfunktionen, die blockierende Ereignisse verursachen könnten.

Der JURA KI Assistent nutzt eine Prozess-ID (PID). Eine PID ist eine normale und unvermeidbare Eigenschaft eines jeden Prozesses, und alle laufenden Programme erhalten eine PID vom Betriebssystem. Sophos oder andere Antivirenprogramme blockieren in der Regel keine Prozesse basierend auf ihrer PID. Stattdessen prüfen sie auf andere Kriterien, um Bedrohungen zu erkennen, wie:

**Verhaltensbasierte Analysen:** Antivirenprogramme wie Sophos analysieren das Verhalten eines Programms.

**Heuristik und Machine Learning:** Sophos verwendet heuristische Analysen und maschinelles Lernen, um verdächtige Muster zu erkennen. Selbst legitime Programme könnten aufgrund bestimmter Verhaltensweisen blockiert werden, wenn sie denen von Malware ähneln.

**Signaturbasierte Erkennung:** Antivirenprogramme überprüfen Programme gegen eine Datenbank bekannter Malware-Signaturen. Wenn der JURA KI Assistent fälschlicherweise als Bedrohung eingestuft wird (False Positive), könnte er blockiert werden. Potentiell unerwünschte Anwendungen (PUA): Der JURA KI Assistent könnte als PUA erkannt werden, wenn Sophos ihn als potenziell unerwünschte Software einstuft, basierend auf dessen Verhalten oder Funktionen.

Nachstehend finden Sie eine Methode, wie der JURA KI Assistent als Anwendung in **Sophos Endpoint Protection** eingerichtet werden kann, dass er nicht mehr blockiert wird. Diese Anleitung basiert auf den gängigen Methoden, die von Sophos unterstützt werden, um legitime Programme von der Blockierung auszunehmen:

# Schritte zur Konfiguration von Ausnahmen

## Schritt 1: Globale Ausnahmen hinzufügen

1. Öffnen Sie die **Sophos Central Admin Console** und navigieren zu **Global Exclusions.**
2. Wählen Sie hier **Global Settings** und scrollen zu **Global Exclusion.**
3. Fügen Sie die folgenden Dateien/Pfade des JURA KI Assistenten zur Liste der Ausnahmen hinzu:
   - ✓ C:\anonym\anonymer.exe (Hauptanwendung)
   - ✓ C:\anonym\anonymer.update.exe (Update-Prozess)
   - ✓ Optional -empfohlen!-: Das gesamte Verzeichnis C:\anonym\, um zukünftige Änderungen zu berücksichtigen
   - ✓ C:\ProgramData\JuraSoft\ (benutzerbezogene Daten/Sessions)

- ✓ C:\Users\<username>\Dokumente\jura-ki\ (Logs und weitere Anwendungsdaten)
- ✓ C:\Users\<username>\Dokumente\jura-ki\ssl\ (SSL-Zertifikate für HTTPS)

  Dieses Verzeichnis enthält die automatisch generierten SSL-Zertifikate (cert.pem, key.pem) des HTTPS-Servers (bei aktivierter Integration des JURA KI Assistenten in RA-MICRO Essentials). Einige Antivirenprogramme überwachen Verzeichnisse mit .pem-Schlüsseldateien oder blockieren den Zugriff darauf.

4. Zusätzliche Ausnahmen für **temporäre Sandbox-Prozesse (Turbo.net)**
   Der JURA KI Assistent nutzt eine virtualisierte Umgebung über Turbo.net. Dabei werden Prozesse und temporäre Dateien in dynamisch erzeugten Verzeichnissen innerhalb der Sandbox ausgeführt. Durch aktuelle Sicherheitsmechanismen wie HTTPS-/TLS-Verifizierung kann es vorkommen, dass Antiviren- oder Endpoint-Security-Lösungen nicht nur einzelne Hilfsprozesse, sondern auch weitere Bestandteile dieser virtualisierten Umgebung fälschlich blockieren.

   Bitte ergänzen Sie daher folgenden Pfad in Ihre Ausnahmeliste:

   - ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Assistent*

   Diese Ausnahme stellt sicher, dass alle durch die Anwendung innerhalb der Turbo.net-Sandbox gestarteten Prozesse und erzeugten Dateien korrekt ausgeführt bzw. verarbeitet werden.

   **Hinweis:**

   Falls Ihre Sicherheitslösung mit einer enger gefassten Ausnahme zuverlässig funktioniert, kann alternativ weiterhin nur der folgende Pfad freigegeben werden:

   - ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Assistent*\local\stubexe**.exe

Bei der Festlegung, welche Scans und Schutzmechanismen für diese Dateien / diese Verzeichnisse ausgenommen werden sollen, empfehlen wir mindestens die **Ausnahmen für den Echtzeitscan und die Verhaltensanalyse,** um sicherzustellen, dass die Prozesse nicht mehr blockiert werden.

## Schritt 2: Application Control Policy (Anwendungssteuerung) anpassen

Wenn Sophos die Prozesse blockiert, weil sie als **unerwünschte Anwendungen (PUAs)** eingestuft werden, müssen Sie eventuell die **Application Control Policy (Anwendungssteuerungsrichtlinie)** anpassen:

1. Navigieren Sie zurück zu **Endpoint Protection > Policies.**
2. Suchen Sie nach der **Application Control Policy.**
3. Fügen Sie die folgenden Prozesse zur **Allow List** hinzu, falls sie dort aufgeführt sind:
   - ✓ anonymer.exe
   - ✓ anonymer.update.exe
   - ✓ certutil.exe

4. **Integration JURA KI Assistent in RA-MICRO Essentials**

   Beim Start installiert anonymer.update.exe automatisch ein selbstsigniertes HTTPS-Zertifikat in den Windows-Stammzertifikatsspeicher. Dies geschieht über folgenden Systemaufruf mit erhöhten Rechten (UAC):

   - ✓ certutil -addstore Root "C:\Users\<username>\Dokumente\jura-ki\ssl\cert.pem"

   Einige Antivirenlösungen blockieren Schreibzugriffe auf den Stammzertifikatsspeicher. Die Anwendung certutil.exe sollte daher in Verbindung mit dem Aufruf durch anonymer.update.exe als vertrauenswürdig eingestuft werden.

5. **Hinweis zur Anwendungserkennung von Sandbox-Prozessen:**

   Einige Antivirenlösungen erkennen python.exe oder cmd.exe, wenn sie über die Sandbox gestartet werden, als potenziell unerwünschte Anwendung (PUA). In diesem Fall sollten Sie auch diese temporären Pfade zur **„Allow List“** hinzufügen, sofern Ihre Software diese pfadbasiert erlaubt.

   - ✓ Empfohlener Pfad für die Zulassung: C:\Users*\AppData\Local\Turbo.net\Sandbox\Anonymer*\local\stubexe**.exe

## Schritt 3: HTTPS und SSL-Inspektion

Der JURA KI Assistent verwendet **HTTPS** für die lokale Kommunikation, sofern die **Integration in RA-MICRO Essentials** aktiviert wird. Die Anwendung läuft auf zwei lokalen Ports:

- ✓ http://localhost:5050 — Kompatibilitäts-/Weiterleitungsserver
- ✓ https://localhost:5051 — HTTPS-Hauptserver

**SSL/TLS-Inspektion:** Antivirenlösungen mit HTTPS-Inspektion können die Verbindung zu localhost:5051 unterbrechen, da das selbstsignierte Zertifikat dabei nicht mehr als vertrauenswürdig erkannt wird. Daher sind **Ausnahmen** für **localhost** und **127.0.0.1 von der SSL/TLS-Inspektion** zu setzen.

**Cross-Origin-Anfragen (Essentials-Integration):** Im Rahmen der RA-MICRO Essentials-Integration wird der JURA KI Assistent als iFrame innerhalb von ***.es.ra-micro.**de geöffnet. Der Browser stellt dabei **Cross-Origin-Anfragen** an **https://localhost:5051.** Einige Webschutzmodule blockieren solche Anfragen als Schutz vor „localhost-Probing". HTTPS-Anfragen an https://localhost:5051 sind im Webschutzmodul zuzulassen, auch wenn diese aus einem externen Ursprung stammen.

## Schritt 4: Zusätzliche Ausnahmen für Exploit-Erkennung

Ggf. müssen folgende zusätzliche Schritte ausgeführt werden:

1. Öffnen Sie in der **Sophos Central Console** den Bereich **Global Settings.**
2. Navigieren Sie zu **Exploit Mitigation > Exclusions.**
3. Um Fehlalarme zu vermeiden und eine stabile Ausführung zu ermöglichen, sollte folgender Pfad bei Bedarf als Ausnahme hinterlegt werden – insbesondere für den Exploit-Typ **DynamicShellcode,** der bei Ausführung von ***python.exe*** in der Sandbox des JURA KI Assistenten auftreten kann:

   - ✓ C:\Users*\AppData\Local\Turbo.net\Sandbox\Anonymer*\local\stubexe**.exe

Diese Freigabe stellt sicher, dass dynamisch erzeugte Hilfsprozesse korrekt ausgeführt werden können, ohne vom Exploit-Schutz blockiert zu werden.

## Schritt 5: Umgang mit False Positives

Falls Sophos den JURA KI Assistent weiterhin blockiert:

1. **Dateien zur Überprüfung einreichen:**

   Melden Sie die betroffenen Dateien direkt an Sophos, insbesondere:

   - ✓ *anonymer.exe, anonymer.update.exe*
   - ✓ sowie temporäre Prozesse wie *python.exe* oder *cmd.exe,* sofern sie aus der Turbo.net Sandbox (stubexe) stammen.

2. **Protokolle überprüfen:**

   Analysieren Sie die Sophos-Protokolle (z. B. Exploit Reports, Event Logs), um weitere Details zur Blockierung zu erhalten. Achten Sie dabei insbesondere auf „Dynamic Shellcode“- oder „Memory Protection“-Ereignisse.

3. **Support kontaktieren:**

   Wenden Sie sich bei anhaltenden Problemen an den Sophos-Support. Geben Sie idealerweise die vollständigen Pfade, Dateihashes und betroffenen Exploit-Typen mit an.

# Wichtige Hinweise

Die genauen Menüpunkte und Begriffe können variieren. Konsultieren Sie die Dokumentation Ihrer Software, um die relevanten Einstellungen zu finden. Stellen Sie sicher, dass die Ausnahmen nur für bekannte und vertrauenswürdige Programme wie den JURA KI Assistenten konfiguriert werden, um die Systemsicherheit nicht zu gefährden.