Konfiguration von SOPHOS Firewalls für den JURA KI Assistenten

(Stand 12.03.2026)

Der **JURA KI Assistent** benötigt Zugriff auf bestimmte lokale und externe Ressourcen, um ordnungsgemäß zu funktionieren. Firewalls oder Webfilter können Verbindungen blockieren, die für den Betrieb des Assistenten erforderlich sind.

Um sicherzustellen, dass der JURA KI Assistent korrekt funktioniert, müssen die folgenden Konfigurationen vorgenommen werden.

Erforderliche Whitelist-Einträge

Der JURA KI Assistent benötigt Zugriff auf folgende Ressourcen.

Lokale Verbindung

- ✓ http://localhost:5050
- ✓ https://localhost:5051 *(bei aktivierter RA-MICRO Essentials Integration)*

Diese lokalen Ports müssen für **eingehenden und ausgehenden Datenverkehr freigegeben** werden.

Externe Verbindungen

- ✓ https://huggingface.co/
- ✓ https://cdn-lfs.hf.co/
- ✓ https://voice-lab.dictanet.com/downloads/
- ✓ https://jurasoft-dev.ra-micro.de/dictanet/
- ✓ https://dictanet.raupdate3.de/
- ✓ https://ra-micro-online.de/
- ✓ https://recht.ra-micro.de/

Anleitung für die Sophos XG Firewall

Schritt 1: Anmeldung an der Sophos XG Firewall

Melden Sie sich an der Admin-Konsole Ihrer Sophos XG Firewall an.

Schritt 2: Erstellen einer Web-Filter-Policy

1. Navigieren Sie zu **Web → Policies**.
2. Wählen Sie die entsprechende **Web-Filter-Policy**, in der die Whitelist konfiguriert werden soll, oder erstellen Sie eine neue Policy.
3. Öffnen Sie die Policy mit **Bearbeiten**.

Schritt 3: Erstellen einer URL-Whitelist

1. Navigieren Sie im Bereich **Web Filtering** zu **URL Groups** oder **Custom Web Categories.**
2. Klicken Sie auf **Add / Create New,** um eine neue URL-Gruppe zu erstellen.
3. **Benennen** Sie die Gruppe (z. B. "*JURA KI Whitelist*") und **fügen** die folgenden **URLs hinzu:**
    - ✓ http://localhost:5050
    - ✓ https://localhost:5051 (bei aktivierter RA-MICRO Essentials Integration)
    - ✓ https://huggingface.co/
    - ✓ https://cdn-lfs.hf.co/
    - ✓ https://voice-lab.dictanet/downloads/
    - ✓ https://jurasoft-dev.ra-micro.de/DictaNet/
    - ✓ https://dictanet.raupdate3.de/
    - ✓ https://ra-micro-online.de/
    - ✓ https://recht.ra-micro.de/

Schritt 4: Zuweisen der Whitelist zu einer Web-Filter-Policy

1. Gehen Sie zurück zur **Web-Filter-Policy**.
2. Fügen Sie die neue URL-Gruppe im Bereich der **erlaubten URL-Kategorien** hinzu.
3. Speichern Sie die Änderungen.

Schritt 5: SSL/TLS-Ausnahme hinzufügen

Falls auf der Sophos XG Firewall **SSL/TLS-Inspection** aktiviert ist, müssen bestimmte Verbindungen von der Entschlüsselung ausgenommen werden, um Kommunikationsprobleme mit dem JURA KI Assistenten zu vermeiden.

1. Navigieren Sie zu **Rules and Policies → SSL/TLS Inspection Rules.**
2. Klicken Sie auf **Add Exception,** um eine neue Ausnahme zu erstellen.
3. Fügen Sie die folgenden Domains als Ausnahmen hinzu:
    - ✓ api.openai.com
    - ✓ files.openai.com
    - ✓ openaipublic.blob.core.windows.net
4. Aktivieren Sie die Option **SSL/TLS Decryption Bypass** für diese Einträge.
5. Speichern Sie die Regel.

Diese Einstellung stellt sicher, dass die HTTPS-Kommunikation mit den OpenAI-Diensten **nicht durch SSL/TLS-Inspection verändert wird,** wodurch Zertifikatsfehler vermieden werden.

Schritt 6: Lokale Kommunikation über localhost zulassen

Der **JURA KI Assistent** verwendet lokale Dienste auf den folgenden Ports:

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

Damit die Anwendung ordnungsgemäß funktioniert, müssen Verbindungen zu **localhost (127.0.0.1)** erlaubt sein.

Schritt 7: Testen und Überprüfen

1. Nachdem alle Einstellungen gespeichert wurden, testen Sie den JURA KI Assistenten, um sicherzustellen, dass die Anwendung jetzt korrekt funktioniert.
2. Überwachen Sie die Firewall-Protokolle, um sicherzustellen, dass keine der URLs blockiert wird.

Anleitung für die Sophos UTM Firewall

Schritt 1: Anmeldung an der Sophos UTM Firewall

1. Melden Sie sich an der **WebAdmin-Oberfläche** der **Sophos UTM Firewall** an.

Schritt 2: Erstellen einer URL-Whitelist

2. Navigieren Sie zu **Web Protection > URL Filtering > Exceptions.**

3. Klicken Sie auf **Add Exception Rule,** um eine neue Ausnahme zu erstellen.
4. **Geben Sie der Ausnahme einen Namen** (z. B. "JURA KI Whitelist").
5. Aktivieren Sie die Option **Matching URLs/Domains** und fügen Sie die folgenden URLs hinzu:
   - ✓ http://localhost:5050/anon
   - ✓ https://localhost:5051 (bei aktivierter RA-MICRO Essentials Integration)
   - ✓ https://huggingface.co/
   - ✓ https://cdn-lfs.hf.co/
   - ✓ https://voice-lab.dictanet/downloads/
   - ✓ https://jurasoft-dev.ra-micro.de/DictaNet/
   - ✓ https://dictanet.raupdate3.de/
   - ✓ https://ra-micro-online.de/
   - ✓ https://recht.ra-micro.de/

Schritt 3: Ausnahmen festlegen

1. Wählen Sie die gewünschten **Ausnahmen** für diese URLs aus, z. B.:
    - ✓ **URL-Filter deaktivieren**
    - ✓ **Antivirus deaktivieren**
    - ✓ **SSL-Scanning deaktivieren** (falls aktiviert)
2. Speichern Sie die Ausnahmeregel.

Diese Einstellung verhindert, dass Webfilter oder SSL-Inspection die Kommunikation des **JURA KI Assistenten** blockieren.

Schritt 4: Firewall-Regel für den lokalen Zugriff (localhost)

Der **JURA KI Assistent** verwendet lokale Dienste auf den folgenden Ports:

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

Damit die Anwendung korrekt funktioniert, darf der lokale Zugriff auf **localhost (127.0.0.1)** nicht durch Firewall-Regeln blockiert werden.

1. Navigieren Sie zu **Network Protection → Firewall.**
2. Klicken Sie auf **New Rule.**
3. Erstellen Sie eine Firewall-Regel mit folgenden Einstellungen:
    - ✓ **Source:** Internal (oder Any)
    - ✓ **Service:** TCP **5050** und TCP **5051**
    - ✓ **Destination: Local Host (127.0.0.1)**
    - ✓ **Action: Allow**
4. Speichern Sie die Regel.

Diese Regel stellt sicher, dass lokale HTTP- und HTTPS-Verbindungen des JURA KI Assistenten nicht durch Firewallrichtlinien blockiert werden.

Schritt 5: Testen und Überprüfen

3. Nachdem alle Einstellungen gespeichert wurden, testen Sie den JURA KI Assistenten, um sicherzustellen, dass die Anwendung jetzt korrekt funktioniert.
4. Überwachen Sie die Firewall-Protokolle, um sicherzustellen, dass keine der URLs blockiert wird.

Hinweis zur RA-MICRO Essentials Integration

Bei aktivierter **RA-MICRO Essentials Integration** wird der JURA KI Assistent als **iFrame** innerhalb von ***.es.ra-micro.de** geladen. Der Browser stellt dabei **Cross-Origin-Anfragen** an: **https://localhost:5051.** Einige Webschutz- oder Sicherheitsmodule blockieren solche Zugriffe als Schutz vor **„localhost-Probing“**.

Stellen Sie daher sicher, dass **HTTPS-Anfragen an localhost:5051 auch dann zugelassen werden, wenn sie aus einem externen Ursprung stammen.**

Hinweis zur SSL-Inspektion und alternativen Proxy-Nutzung

Sollten trotz angepasster Firewallregeln weiterhin **Zertifikatsprobleme** auftreten, liegt dies häufig an einer aktiven **SSL-Inspection.**

In diesem Fall kann alternativ die Nutzung eines **HTTP-Proxys innerhalb des JURA KI Assistenten** eine geeignete Lösung darstellen.

Proxy-Konfiguration in der Anwendung

Der JURA KI Assistent unterstützt die manuelle Konfiguration eines Proxyservers unter:

Einstellungen → Allgemein → Proxy

Diese Option ist insbesondere geeignet, wenn:

- ✓ der direkte Internetzugriff durch Sophos oder andere Sicherheitsrichtlinien blockiert oder manipuliert wird,
- ✓ eine zentrale Zertifikatsprüfung über einen Unternehmens-Proxy erfolgen soll,
- ✓ ein firmeneigenes Root-Zertifikat verwendet wird, das bereits im lokalen Zertifikatsspeicher installiert ist.

Anforderungen an den Proxy

Der konfigurierte Proxy muss den Zugriff auf folgende Domains ohne SSL-Interception ermöglichen:

- ✓ api.openai.com
- ✓ openaipublic.blob.core.windows.net
- ✓ files.openai.com

Wichtige Hinweise

- ✓ **Netzwerkprofile beachten:** Stellen Sie sicher, dass die Regeln für die richtigen Netzwerkprofile (Privat, Domäne, Öffentlich) gelten.
- ✓ **Sicherheitsrichtlinien:** Whitelisting sollte nur für vertrauenswürdige Anwendungen und URLs erfolgen.

- ✓ **Regelmäßige Überprüfung**: Überprüfen Sie regelmäßig, ob Änderungen an den URLs oder Ports erforderlich sind.
- ✓ **Protokollanalyse:** Bei fortdauernden Problemen analysieren Sie die Firewall-Protokolle, um blockierte Verbindungen zu identifizieren.

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.