Konfiguration von 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/

Schritte zur Konfiguration der Firewall

A. Windows Defender Firewall konfigurieren

Schritte zur Freigabe der lokalen Ports 5050 bzw. 5051

1. Öffnen Sie die **Systemsteuerung** und navigieren Sie zu:
   System und Sicherheit > Windows Defender Firewall > Erweiterte Einstellungen
2. Navigieren Sie zu **Eingehende Regeln** und wählen **Neue Regel**.
3. Wählen Sie **Port** und klicken Sie auf **Weiter**.
4. Geben Sie **die TCP-Ports 5050 und 5051** ein und klicken Sie auf **Weiter**.
   Dabei wird **Port 5050** für die **HTTP- Kommunikation** und **Port 5051** für die **HTTPS-Kommunikation** freigegeben.
5. Wählen Sie **Verbindung zulassen** und klicken auf **Weiter**.
6. **Aktivieren** Sie die gewünschten Netzwerkprofile (Privat, Domäne, Öffentlich).

7. **Benennen Sie die Regel,** z. B. „JURA KI Assistent – Lokale Ports 5050 und 5051“.
8. Wiederholen Sie den Vorgang für **Ausgehende Regeln**, um sicherzustellen, dass auch der Datenverkehr von Ihrem PC aus über **Port 5050** sowie über **Port 5051 für HTTPS-Verbindungen** erlaubt ist.

Schritte zur Whitelist-Erstellung für externe URLs

Da Windows Defender externe URLs nicht direkt whitelisten kann, arbeiten Sie mit Domänen- oder Anwendungsregeln:

1. Öffnen Sie **Windows Defender Firewall > Erweiterte Einstellungen.**
2. Navigieren Sie zu **ausgehende Regeln** und wählen **Neue Regel.**
3. Wählen Sie **Benutzerdefiniert** und bestätigen mit **Weiter.**
4. Unter **Programme** wählen Sie **Alle Programme** und klicken auf **Weiter.**
5. Im Abschnitt **Protokolle und Ports** wählen Sie **TCP** und geben die **Ports 80 (HTTP)** und **443 (HTTPS)** ein.
6. Im Abschnitt **Bereich** geben Sie die **IP-Adressen oder Domänennamen** der **externen URLs** ein:

   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/

7. Wählen Sie **Verbindung zulassen** und bestätigen mit **Weiter.**
8. **Benennen Sie die Regel,** z.B. *„JURA KI Assistent – externe URLs“.*

Optional: Regel für spezifische Anwendungen

Falls der Datenverkehr über bestimmte Programme, wie **python.exe,** läuft:

1. Erstellen Sie eine Regel für die Anwendung.
2. Geben Sie den Pfad zum Programm an und erlauben Sie den Datenverkehr über die Ports 80 und 443.

Protokollprüfung

1. **Aktivieren** Sie die **Protokollierung** der **Windows Defender Firewall** unter:
   Windows Defender Firewall > Erweiterte Einstellungen > Protokollierung.

2. Überprüfen Sie die Firewall-Protokolle, um sicherzustellen, dass keine relevanten Verbindungen blockiert werden.

Verzeichniserkennung

Sollte die Firewall eine Bedrohung oder eine Aktivität in einem der folgenden Ordner erkennen:

- ✓ C:\anonym\
- ✓ C:\anonym\ProgramData\JuraSoft
- ✓ C:\Users\<username>\Dokumente\jura-ki

dann müssen diese Dateien/Ordner als **Ausnahme in der Firewall-Konfiguration** festgelegt werden, um sicherzustellen, dass der JURA KI Assistent korrekt funktioniert.

B. Konfiguration in Drittanbieter-Firewalls

Für andere Firewall-Programme wie **Sophos, Fortinet** oder **Check Point** folgen Sie ähnlichen Schritten. Beachten Sie hierbei die spezifische Benutzeroberfläche und Konfigurationsmöglichkeiten der jeweiligen Software:

1. **Lokale Port 5050 und 5051 freigeben**:
   Erstellen Sie eine neue Regel für **eingehenden und ausgehenden TCP-Datenverkehr** über die Ports 5050 bzw. 5051.

2. **Externe URLs whitelisten**:
   Erstellen Sie Regeln für den Zugriff auf die oben genannten URLs. Stellen Sie sicher, dass die Kommunikation über die Ports 80 und 443 erlaubt ist.

Domänen- oder Anwendungsregel:
Je nach Firewall können Sie spezifische Domänen oder Anwendungen konfigurieren.

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.

Hinweise zu HTTPS, SSL-Inspektion und alternativer Proxy-Nutzung

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

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

SSL/TLS-Inspektion

Sicherheitslösungen mit aktiver **HTTPS- bzw. SSL/TLS-Inspektion** (z. B. Kaspersky, ESET, Avast Business oder Bitdefender GravityZone) können die Verbindung zu **localhost:5051** unterbrechen. Ursache ist, dass das vom JURA KI Assistenten verwendete selbstsignierte Zertifikat im Rahmen der Inspektion nicht mehr als vertrauenswürdig erkannt wird.

Daher sind in solchen Umgebungen **Ausnahmen für localhost und 127.0.0.1 von der SSL/TLS-Inspektion** zu definieren. Zusätzlich sind HTTPS-Verbindungen an **https://localhost:5051** im jeweiligen Webschutzmodul ausdrücklich zuzulassen.

Cross-Origin-Anfragen bei aktivierter 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 Webschutz- oder Endpoint-Security-Module blockieren solche Anfragen als Schutz vor sogenanntem **„localhost-Probing“**. Damit die Integration ordnungsgemäß funktioniert, müssen **HTTPS-Anfragen an https://localhost:5051 auch dann zugelassen werden, wenn sie aus einem externen Ursprung stammen**.

Alternative bei Zertifikatsproblemen: Proxy-Nutzung

Sollten trotz angepasster Firewallregeln und definierter Ausnahmen weiterhin Zertifikatsprobleme auftreten, liegt dies häufig an einer weiterhin 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 die Firewall blockiert oder manipuliert wird,
- ✓ eine zentrale Zertifikatsprüfung über einen vertrauenswürdigen Unternehmens-Proxy erfolgen soll,
- ✓ ein firmeneigenes Root-Zertifikat verwendet wird, das in den lokalen Zertifikatsspeicher aufgenommen wurde.

Wichtig: 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.