Verbindungsabbruch in ELBA

Anleitung — Verbindungsabbruch in ELBA technisch aufzeichnen und lokalisieren

Browser-übergreifend (Firefox · Chrome · Edge)

Zielsetzung

Diese Anleitung beschreibt, wie ein lokaler IT-Techniker einen auftretenden Verbindungsabbruch auf dem ELBA-Ländermodul so aufzeichnet, dass die Ursache nachvollziehbar wird. Typische Symptome sind Browser-Meldungen wie „Reconnecting…" oder „Verbindung verloren", unterbrochene Datei-Uploads oder spürbar verzögerte Seitenwechsel. Mögliche Verursacher im lokalen Pfad zwischen Arbeitsplatz und Server: HTTPS-Inspektion durch Sicherheits-Software, Firewall-/Proxy-Regeln, ein gestörtes Browser-Profil oder zwischengeschaltete Netzwerk-Komponenten.

Voraussetzungen

- Administratorrechte am betroffenen Arbeitsplatz
- Browser am betroffenen Arbeitsplatz in der produktiv genutzten Version. Diese Anleitung enthält konkrete Menüpfade für **Mozilla Firefox**, **Google Chrome** und **Microsoft Edge**. Andere Browser (z. B. Safari, Opera, Brave) sind ebenfalls einsetzbar — die Vorgehensweise ist sinngemäß identisch, die genauen Bezeichnungen der Menüpunkte sind über die Hilfe-Funktion des jeweiligen Browsers oder eine Internet-Suche („<Browser-

Name> <Funktion>") zu ermitteln.
- Optional: Wireshark (für vertiefte Netzwerk-Analyse — nicht zwingend nötig)
- Eine Möglichkeit zur Bereitstellung mehrerer MB großer Diagnose-Dateien (z. B. E-Mail, Cloud-Ordner)

Hinweis zur Notation: *Tastenkombinationen und Menüpfade werden, soweit identisch in allen drei Browsern, einmal genannt. Wo sie sich unterscheiden, sind sie ausdrücklich pro Browser aufgeführt.*

Begriffsklärung „ELBA-Ländermodul": *Damit ist die für das jeweilige Bundesland ausgerollte ELBA-Adresse gemeint, jeweils unter der Form* `<land>.bvpi-elba.de` *— beispielsweise* `sn.bvpi-elba.de` *für Sachsen,* `bw.bvpi-elba.de` *für Baden-Württemberg,* `by.bvpi-elba.de` *für Bayern usw. In den nachfolgenden Schritten ist überall die im konkreten Bundesland produktiv genutzte Adresse einzusetzen.*

Hinweis zu Browser-Versionen: *Browser-Hersteller passen Menüstrukturen und Bezeichnungen mit jedem Update geringfügig an. Sollte ein in dieser Anleitung genannter Menüpunkt unter genau dieser Bezeichnung nicht zu finden sein, ist die Funktion in der Regel mit gleicher oder ähnlicher Benennung in einem benachbarten Menü erreichbar.*

Schritt 1 — Symptom dokumentieren

- Genauer **Zeitpunkt** (Uhrzeit auf die Minute) des Abbruchs notieren
- **Welche Aktion** war zum Zeitpunkt des Abbruchs aktiv (Datei-Upload, Seitenaufruf, Liste filtern, längere Leerlaufzeit)?
- **Screenshot** der Fehlermeldung anfertigen
- **Browser-Bezeichnung und Version** notieren:
  - Firefox: Menü → *Hilfe* → *Über Firefox*
  - Chrome: Menü → *Hilfe* → *Über Google Chrome*
  - Edge: Menü → *Hilfe und Feedback* → *Über Microsoft Edge*
- **Verwendete Firewall- oder Proxy-Lösung** im Firmennetz benennen

Installierte Endpoint-Security identifizieren (mehrere Wege, mindestens einer reicht)

1. **Schnellster Weg — Server-Zertifikat im Browser prüfen.** Das ELBA-Ländermodul im Browser öffnen, dann auf das Schloss-Symbol in der Adressleiste klicken. Der Pfad zum Zertifikat unterscheidet sich leicht:

- *Firefox:* Schloss → „Verbindung sicher" → „Weitere Informationen" → Schaltfläche „Zertifikat anzeigen"
- *Chrome:* Schloss → „Verbindung ist sicher" → „Zertifikat ist gültig"
- *Edge:* Schloss → „Verbindung ist sicher" → Zertifikat-Symbol oben rechts im Pop-up

Im Zertifikats-Dialog beim Feld **Aussteller** (engl. „Issued by") prüfen:

- Aussteller ist eine bekannte öffentliche CA (z. B. *Let's Encrypt, DigiCert, Sectigo, GlobalSign*) → **keine HTTPS-Inspektion aktiv**, der Datenverkehr läuft ungebrochen zwischen Arbeitsplatz und ELBA-Server.
- Aussteller ist eine **lokale CA** mit AV-Hersteller-Namen oder generischem Firmen-Namen, z. B. *ESET SSL Filter CA, Avast Web/Mail Shield Root, Kaspersky Anti-Virus Personal Root, Bitdefender Personal CA, Sophos SSL CA, F-Secure, Symantec Endpoint Protection, Zscaler Root CA, FortiGate CA, <Firmenname> Proxy CA* → **HTTPS-Inspektion ist aktiv**, der Hersteller ist direkt ablesbar. Dieses Produkt steht ab sofort an Position 1 der Verdächtigenliste.

2. **Liste installierter Programme.** Windows-Einstellungen → *Apps* → *Apps & Features*. Nach typischen AV-/Endpoint-Herstellern filtern: AVG, Avast, Avira, Bitdefender, ESET, F-Secure, G DATA, Kaspersky, McAfee, Norton, Sophos, Symantec, Trend Micro, Webroot, Windows Defender, Malwarebytes.
3. **Windows-Sicherheits-Center.** Einstellungen → *Datenschutz und Sicherheit* → *Windows-Sicherheit* → *Anbieter*. Zeigt den aktiv registrierten Virenschutz und ggf. zusätzliche Sicherheits-Produkte.
4. **Per PowerShell** (mit Administratorrechten):

   ```
   Get-CimInstance -Namespace root/SecurityCenter2 -ClassName AntivirusProduct | Select-Object displayName
     Get-CimInstance -Namespace root/SecurityCenter2 -ClassName FirewallProduct  | Select-Object displayName
   ```

   Listet alle bei Windows registrierten Virenschutz- und Firewall-Produkte mitsamt Anzeigenamen.

Schritt 2 — Browser-Aufzeichnung (HAR-Datei)

Eine HAR-Datei enthält alle Netzwerk-Anfragen einer Browser-Sitzung mit Zeitstempel, Status, Headern und Antwortzeiten. Sie ist das wertvollste Einzel-Diagnose-Artefakt.

1. Das ELBA-Ländermodul im Browser öffnen und am Login anmelden — **noch nicht arbeiten**
2. Mit `F12` (oder `Strg+Umschalt+I`) die Entwicklerwerkzeuge öffnen — in allen drei Browsern identisch

3. Den Netzwerk-Reiter wählen:
   - *Firefox:* Reiter **Netzwerkanalyse**
   - *Chrome:* Reiter **Network** bzw. **Netzwerk**
   - *Edge:* Reiter **Netzwerk**
4. Folgende Optionen aktivieren — sie verhindern, dass Diagnose-Daten beim Seitenwechsel oder durch den Browser-Cache verloren gehen:
   - *Firefox:* Zahnrad-Symbol oben rechts im Netzwerkanalyse-Reiter → **Persistente Protokolle** aktivieren und **HTTP-Cache deaktivieren**, solange das Werkzeug geöffnet ist
   - *Chrome:* Oberhalb der Anfrageliste die Optionen **Preserve log** bzw. **Protokoll beibehalten** und **Disable cache** bzw. **Cache deaktivieren** setzen
   - *Edge:* Identisch zu Chrome — **Protokoll beibehalten** und **Cache deaktivieren** setzen
5. Sicherstellen, dass die **Aufzeichnung aktiv** ist (in Chrome/Edge ein roter Kreis oben links im Netzwerk-Reiter; in Firefox läuft die Aufzeichnung automatisch, sobald der Reiter geöffnet ist)
6. Mit der gewohnten Arbeit am Anwender-Arbeitsplatz beginnen und so lange weiterarbeiten, bis der Verbindungsabbruch eintritt
7. Den genauen Zeitpunkt des Abbruchs notieren
8. Nach dem Abbruch im Netzwerk-Reiter mit Rechtsklick auf einen beliebigen Eintrag in der Anfrageliste:
   - *Firefox:* → **Alle als HAR speichern**
   - *Chrome:* → **Save all as HAR with content** bzw. **Alle als HAR-Datei mit Inhalt speichern**
   - *Edge:* → **Inhalt als HAR speichern** bzw. **Save all as HAR with content**
9. Datei mit aussagekräftigem Namen abspeichern, z. B. `elba-abbruch-2026-MM-TT-HHMM.har`

Schritt 3 — Browser-Konsole sichern

Parallel zum Netzwerkmitschnitt die Konsolenmeldungen sichern — dort erscheinen WebSocket- und JavaScript-spezifische Fehler im Klartext.

1. In den Entwicklerwerkzeugen den Reiter **Konsole** (engl. *Console*) öffnen — in allen drei Browsern identisch benannt
2. Filter so einstellen, dass **alle Meldungstypen** sichtbar sind (Fehler, Warnungen, Informationen, Debug)
3. Den Inhalt komplett markieren und in eine Textdatei kopieren — z. B. `elba-konsole-2026-MM-TT-HHMM.txt`

Schritt 4 — Gegenprobe mit mobilem Datennetz

Dieser Test isoliert das Firmennetzwerk und ist diagnostisch hochwertig:

1. Smartphone als WLAN-Hotspot konfigurieren (Mobilfunknetz, **nicht** Firmen-WLAN)
2. Den Arbeitsplatz vom Firmennetz trennen und ausschließlich über den mobilen Hotspot verbinden
3. Mit demselben Browser und Profil dieselbe Tätigkeit ausführen
4. **Ergebnis A:** Verbindungsabbruch tritt im Hotspot-Betrieb **nicht** mehr auf → Ursache liegt im Firmen-Netzwerkpfad (Firewall, Proxy, HTTPS-Inspektion am Gateway)
5. **Ergebnis B:** Verbindungsabbruch tritt auch im Hotspot-Betrieb auf → Ursache liegt im Arbeitsplatz selbst (Browser-Profil, Endpoint-Security, lokale Antivirus-Lösung)

Schritt 5 — Browser-Profil isolieren

Wenn Ergebnis B (Schritt 4) eintritt, gezielt das Browser-Profil eingrenzen:

1. Ein **privates Fenster** öffnen und dort am ELBA-Ländermodul anmelden — Erweiterungen sind dabei standardmäßig deaktiviert:
   - *Firefox:* `Strg+Umschalt+P` (Privates Fenster)
   - *Chrome:* `Strg+Umschalt+N` (Inkognito-Fenster)
   - *Edge:* `Strg+Umschalt+N` (InPrivate-Fenster)

   Läuft es im privaten Fenster sauber → Ursache ist eine Browser-Erweiterung oder ein gestörter Profilzustand (Cookies, Cache).
2. Ein **neues, sauberes Browser-Profil** anlegen und dort ohne Erweiterungen testen:
   - *Firefox:* Adressleiste `about:profiles` → „Neues Profil erstellen"
   - *Chrome:* Profil-Symbol oben rechts → „Hinzufügen" / „Weitere Person hinzufügen", oder `chrome://settings/manageProfile`
   - *Edge:* Profil-Symbol oben rechts → „Profil hinzufügen", oder `edge://settings/profiles`

   Läuft es im neuen Profil sauber → das alte Profil ist gestört; sauberer Neuaufbau empfohlen.
3. Browser-Erweiterungen **einzeln deaktivieren** (Werbeblocker, Tracking-Schutz, Cookie-Manager, NoScript) und Verhalten beobachten. Pfad zur Erweiterungs-Verwaltung:
   - *Firefox:* `about:addons`
   - *Chrome:* `chrome://extensions`
   - *Edge:* `edge://extensions`

Schritt 6 — Endpoint-Security testweise deaktivieren

Antivirus- und Endpoint-Security-Lösungen können WebSocket-Verbindungen durch **HTTPS-Inspektion / Web-Schutz / Deep Packet Inspection** stören. Häufig betroffen: Avast, Bitdefender, ESET, F-Secure, Kaspersky, Norton, Sophos.

Vorab-Indikator aus Schritt 1: Wenn der Zertifikats-Check ergeben hat, dass ein lokaler AV-/Proxy-Aussteller das ELBA-Zertifikat ersetzt, ist HTTPS-Inspektion *nachweisbar* aktiv — der Test in diesem Schritt zielt dann gezielt auf dieses identifizierte Produkt.

1. Nach Rücksprache mit dem Anwender den HTTPS-/Web-Schutz **kurzzeitig deaktivieren** oder eine Ausnahme für die ELBA-Domain `*.bvpi-elba.de` einrichten (deckt alle Ländermodule ab)
2. Mit derselben Aktion das Verhalten erneut testen
3. Nach dem Test den Schutz **wieder aktivieren** — Ausnahmen für die ELBA-Domain bei Bedarf dauerhaft eintragen

Schritt 7 — Firewall / Proxy prüfen

Im Firmennetz mit Firewall oder Web-Proxy folgende Aspekte prüfen lassen:

- **WebSocket-Protokoll** (HTTP-Upgrade auf `wss://`) ist für die ELBA-Domain (`*.bvpi-elba.de`) dauerhaft freigegeben
- **Idle-Timeouts** für WebSocket-Verbindungen sind nicht kürzer als 5 Minuten konfiguriert
- **Request Body Size Limit** ist nicht unterhalb der größten ELBA-Upload-Datei gesetzt
- **SSL-/TLS-Inspektion** am Gateway: entweder Ausnahme für die ELBA-Domain (`*.bvpi-elba.de`) oder testweise deaktivieren
- **HTTP/2 oder HTTP/3:** einige Proxies brechen HTTP/2-Streams nach kurzer Zeit ab — Verhalten mit HTTP/1.1 testen

Schritt 8 — Optional: Netzwerk-Mitschnitt (Wireshark)

Falls Schritte 4–7 die Ursache nicht eindeutig eingrenzen, ein paralleler Wireshark-Mitschnitt während eines weiteren Abbruchs:

1. Wireshark auf dem Arbeitsplatz starten, Aufzeichnung auf dem produktiv genutzten Netzwerkinterface beginnen
2. Capture-Filter (optional, zur Reduktion): `host <land>.bvpi-elba.de` — also den im jeweiligen Bundesland verwendeten Hostnamen einsetzen (z. B. `host sn.bvpi-elba.de` für Sachsen)
3. Während des Abbruchs weiter aufzeichnen, danach Aufzeichnung stoppen
4. Mitschnitt als `.pcapng` speichern
5. Relevante Pakete unmittelbar vor dem Abbruch interpretieren:
   - **TCP RST** vom Client → lokale Software (AV, Firewall) hat die Verbindung gekappt
   - **TCP RST** vom Server → serverseitig oder durch zwischengeschaltete NAT/Proxy-Box
   - **TLS close_notify Alert** → ordentlicher Verbindungsabbau, vermutlich durch HTTPS-Inspektion
   - **Stille — kein Paket vor dem Abbruch** → reine Idle-Timeout-Trennung (Firewall-Stateful-Inspection)

Zu sammelnde Artefakte für die Auswertung

- HAR-Datei aus Schritt 2
- Konsolen-Mitschnitt aus Schritt 3
- Ergebnis des Hotspot-Tests aus Schritt 4 (Ergebnis A oder B)
- Ergebnis der Profil-Isolation aus Schritt 5
- Ergebnis des HTTPS-Inspektions-Tests aus Schritt 6
- Notizen aus Schritt 7 zu Firewall-/Proxy-Konfiguration
- Optional: `.pcapng` aus Schritt 8
- Allgemeine Notizen aus Schritt 1 (Uhrzeit, Aktion, Browser-Bezeichnung und Version, Endpoint-Security-Produkt)

Das ist vollständiges HTML mit: -

/

/

für die Überschriften-Hierarchie - **für Fettschrift,** ***für Kursiv -*** `*für Pfade, Dateinamen und PowerShell-Befehle*` `-`

```
für den mehrzeiligen PowerShell-Block
 -  für Tastenkombinationen
 - Verschachtelte
```

- /

1. -Listen entsprechend der Original-Struktur

Revision #2
Created 2024-01-16 13:32:08 UTC by Sebastian Langwald
Updated 2026-06-09 10:22:32 UTC by Sebastian Langwald