WINDOWS LIVE-EREIGNIS MONITOR REMOTE EDITION

IT-Service Walter

Jörn Walter
www.it-service-walter.com
02.10.2025

WINDOWS LIVE-EREIGNISMONITOR REMOTE EDITION

ÜBERBLICK

DER WINDOWS LIVE-EREIGNISMONITOR IST EIN PROFESSIONELLES WERKZEUG ZUR ÜBERWACHUNG UND ANALYSE VON WINDOWS EVENT-LOGS. DAS TOOL WURDE SPEZIELL ENTWICKELT, UM SYSTEMADMINISTRATOREN UND IT-FACHKRÄFTEN DIE ARBEIT MIT WINDOWS-EREIGNISSEN ZU ERLEICHTERN.

Warum der Windows Live-Ereignismonitor unverzichtbar ist

Das Problem ohne dieses Tool

Windows-Ereignisprotokolle sind wie ein Flugschreiber für Ihren Computer - sie zeichnen alles auf, was passiert. Aber die Standard-Windows-Ereignisanzeige ist:

- Langsam und umständlich
- Kann keine Live-Überwachung
- Kein Remote-Zugriff ohne komplizierte Einrichtung
- Keine praktischen Export-Optionen

Die Lösung: Windows Live-Ereignismonitor

Dieses Tool macht aus kryptischen Systemlogs ein mächtiges Diagnose-Werkzeug:

- **Echtzeit-Überwachung**: Sehen Sie Probleme, während sie entstehen
- **Remote-Support**: Fehlersuche auf anderen Computern ohne TeamViewer
- **Intelligente Filter**: Finden Sie die Nadel im Heuhaufen
- **Professionelle Reports**: Beweisen Sie Probleme schwarz auf weiß

Konkrete Anwendungsfälle

IT-Administratoren

- Server überwachen ohne RDP-Verbindung
- Fehler-Muster über mehrere Systeme erkennen
- Compliance-Reports für Audits erstellen

Support-Techniker

- Kundenprobleme remote diagnostizieren
- Wiederkehrende Fehler dokumentieren
- Beweise für Hardware-Defekte sammeln

Power-User

- Abstürze und Bluescreens analysieren
- Performance-Probleme aufspüren
- Software-Konflikte identifizieren

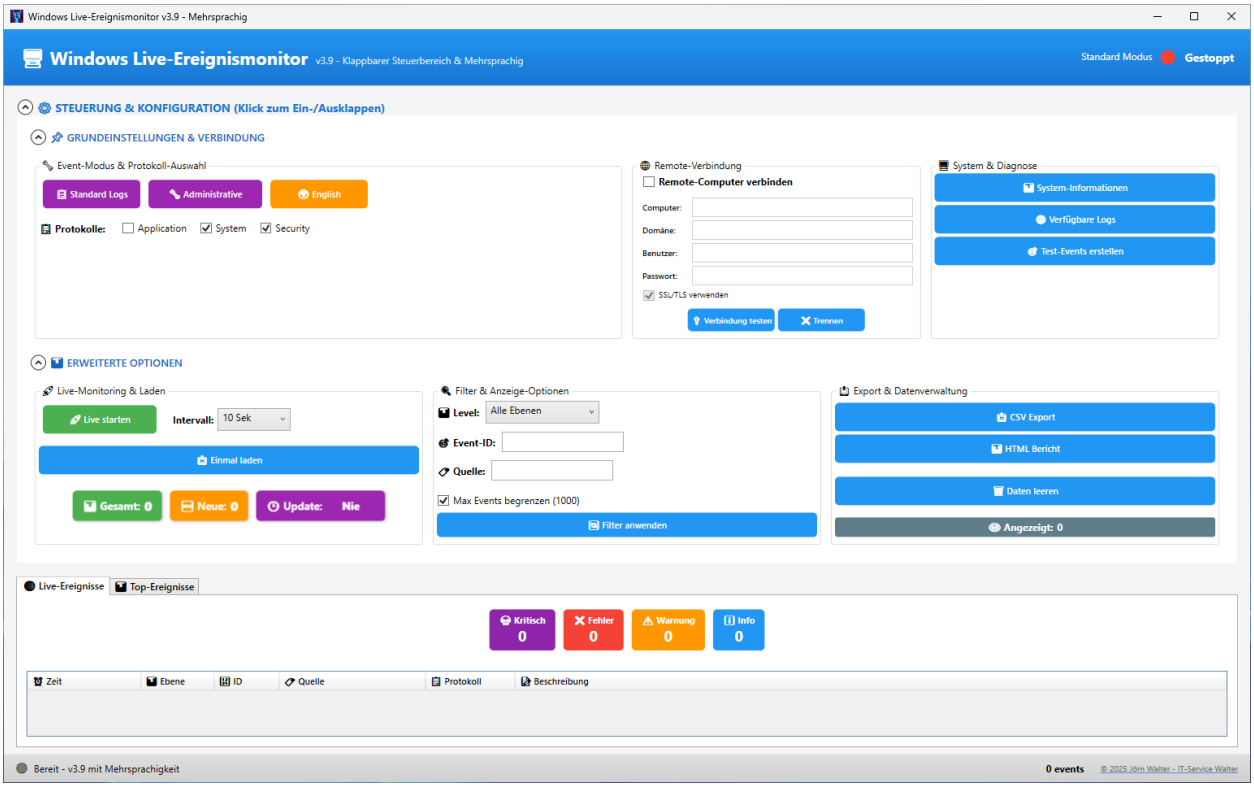
Praktisches Beispiel: Ein Kunde meldet "Der PC stürzt manchmal ab". Mit diesem Tool sehen Sie sofort: Event-ID 41 (Kernel-Power) tritt immer um 14:30 auf = Überhitzung nach Mittagssonne. Problem in 5 Minuten gefunden statt stundenlanger Suche.

Der entscheidende Vorteil

Während andere noch in der Windows-Ereignisanzeige blättern, haben Sie bereits:

- Alle kritischen Fehler der letzten Woche gefiltert
- Die Problemquelle identifiziert
- Einen HTML-Report für den Kunden erstellt

Kurz gesagt: Dieses Tool verwandelt Windows-Ereignisse von einem unübersichtlichen Datenberg in ein strukturiertes Diagnose-System, das Zeit spart und Probleme schneller löst.



🚀 Erste Schritte

1. Programm starten

Starten Sie die Anwendung **als Administrator** für vollen Zugriff:

- Rechtsklick auf die .exe
- "Als Administrator ausführen"

2. Sprache wählen

Klicken Sie auf den 🌐 **English/Deutsch** Button oben links, um die Sprache zu wechseln.

3. Modus auswählen

Sie haben zwei Modi zur Auswahl:

📋 Standard Logs

- Überwacht die wichtigsten Windows-Protokolle
- Application, System, Security
- Ideal für normale Fehlersuche

🔧 Administrative

- Sammelt ALLE kritischen Ereignisse
- Aus diversen Logs (Windows Default)
- Für tiefgreifende Systemanalyse

💡 Hauptfunktionen

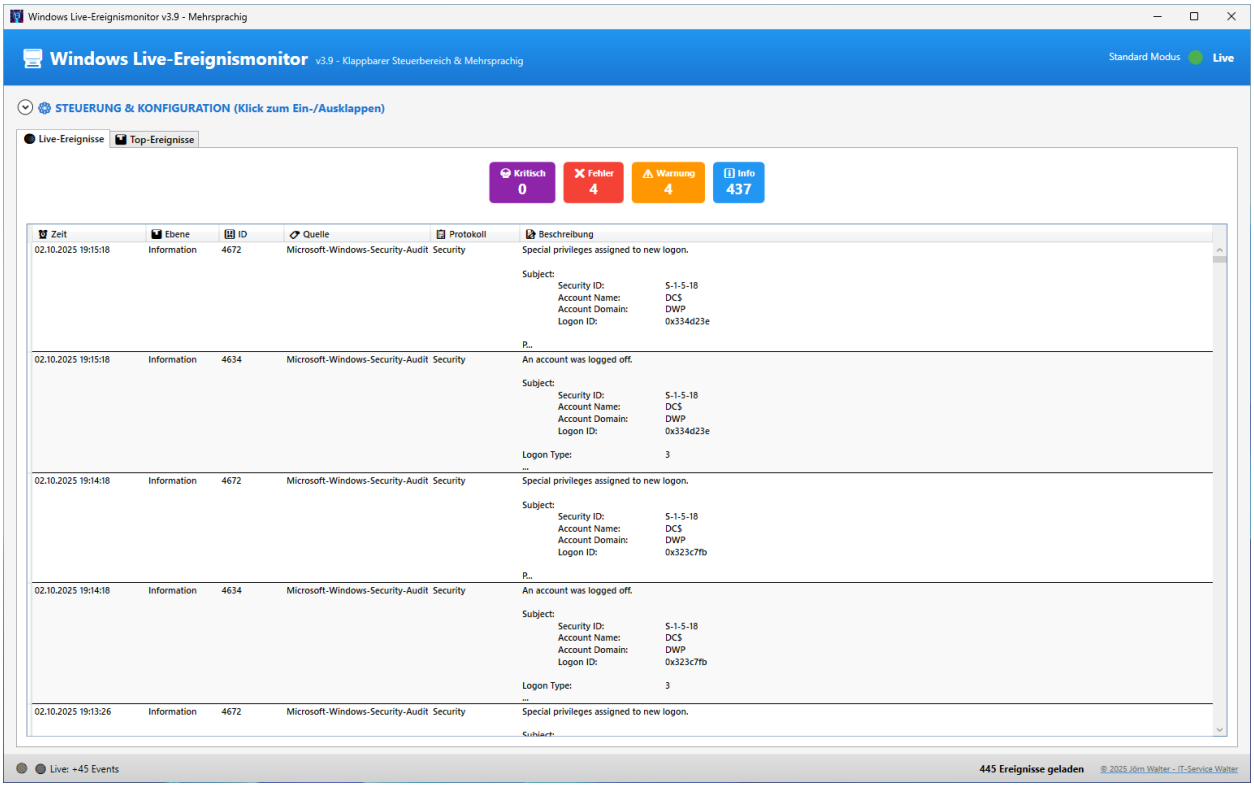
📥 Einmal laden

Zweck: Lädt aktuelle Ereignisse einmalig

So geht's:

1. Wählen Sie Ihren Modus (Standard/Administrative)
2. Im Standard-Modus: Wählen Sie die gewünschten Logs aus
3. Klicken Sie auf " 📥 **Einmal laden"**
4. Warten Sie, bis die Daten geladen sind

Tipp: Beginnen Sie immer mit "Einmal laden", bevor Sie Live-Monitoring starten!



🚀 Live-Monitoring

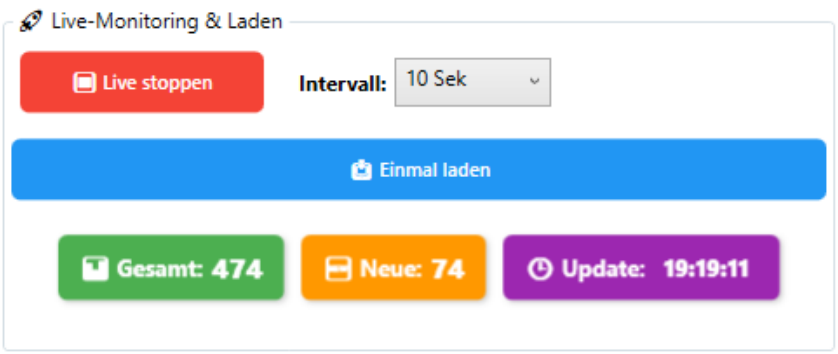
Zweck: Überwacht kontinuierlich neue Ereignisse

So geht's:

1. Laden Sie zuerst Daten mit "Einmal laden"
2. Wählen Sie ein Intervall (5, 10, 30 oder 60 Sekunden)
3. Klicken Sie auf **"🚀 Live starten"**
4. Neue Events werden automatisch hinzugefügt

Status-Anzeigen:

- 📊 **Gesamt**: Alle geladenen Ereignisse
- 🆕 **Neue**: Ereignisse seit Live-Start
- 🕐 **Update**: Zeitpunkt der letzten Prüfung



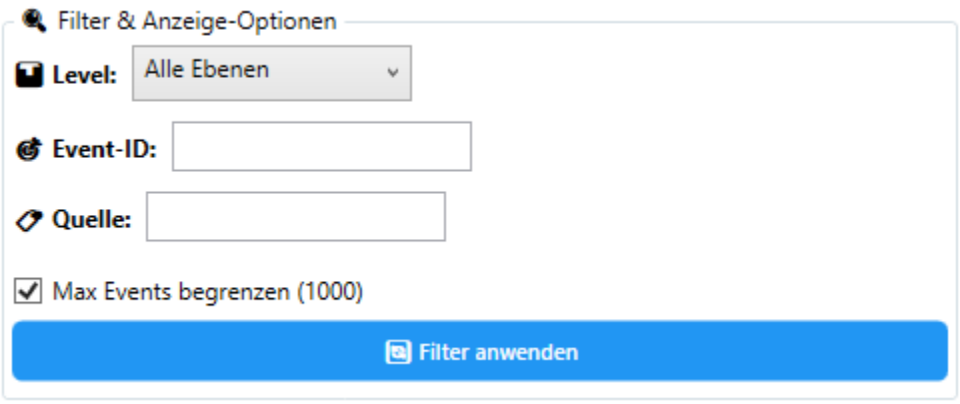
🔍 Filter anwenden

Zweck: Zeigt nur relevante Ereignisse

Filter-Optionen:

Level-Filter

- **Alle Ebenen**: Zeigt alles
- **Kritisch + Fehler**: Nur schwerwiegende Probleme
- **Nur Fehler**: Fehler ohne Warnungen
- **Nur Warnungen**: Potenzielle Probleme
- **Nur Information**: Systemmeldungen



Event-ID Filter

Geben Sie spezifische IDs ein, z.B.: 1000,1001,4625

Quellen-Filter

Suchen Sie nach bestimmten Programmen/Diensten

Anwendung:

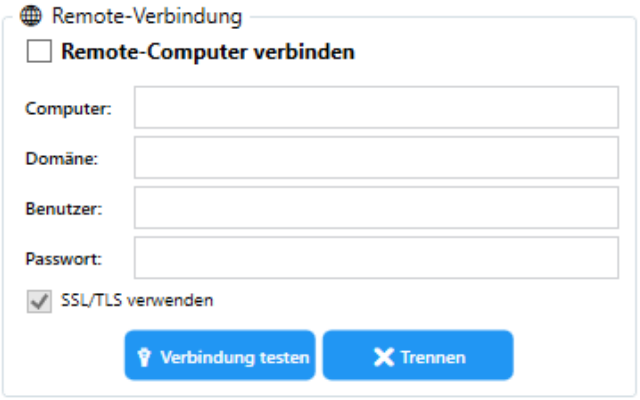
1. Filter einstellen
2. **"🔄 Filter anwenden"** klicken

🌐 Remote-Verbindungen

Verbindung einrichten

Voraussetzungen:

- WinRM muss auf dem Zielcomputer aktiviert sein
- Benutzer muss in "Event Log Readers" Gruppe sein
- Firewall-Ports: 5985 (HTTP) oder 5986 (HTTPS)



Schritte:

1. Aktivieren Sie **"Remote-Computer verbinden"**
2. Füllen Sie aus:
    - **Computer**: Name oder IP-Adresse
    - **Domäne**: Nur bei Active Directory
    - **Benutzer**: Windows-Benutzername
    - **Passwort**: Windows-Passwort
3. Optional: **"SSL/TLS verwenden"** für verschlüsselte Verbindung
4. Klicken Sie **" 📌 Verbindung testen"**

Wichtige Hinweise:

- 🔓 Port 5985: Schneller, aber unverschlüsselt (internes Netzwerk)
- 🔒 Port 5986: Verschlüsselt, benötigt SSL-Zertifikat

Verbindung trennen

Klicken Sie "❌ **Trennen**" um zur lokalen Ansicht zurückzukehren.

📊 Datenanalyse

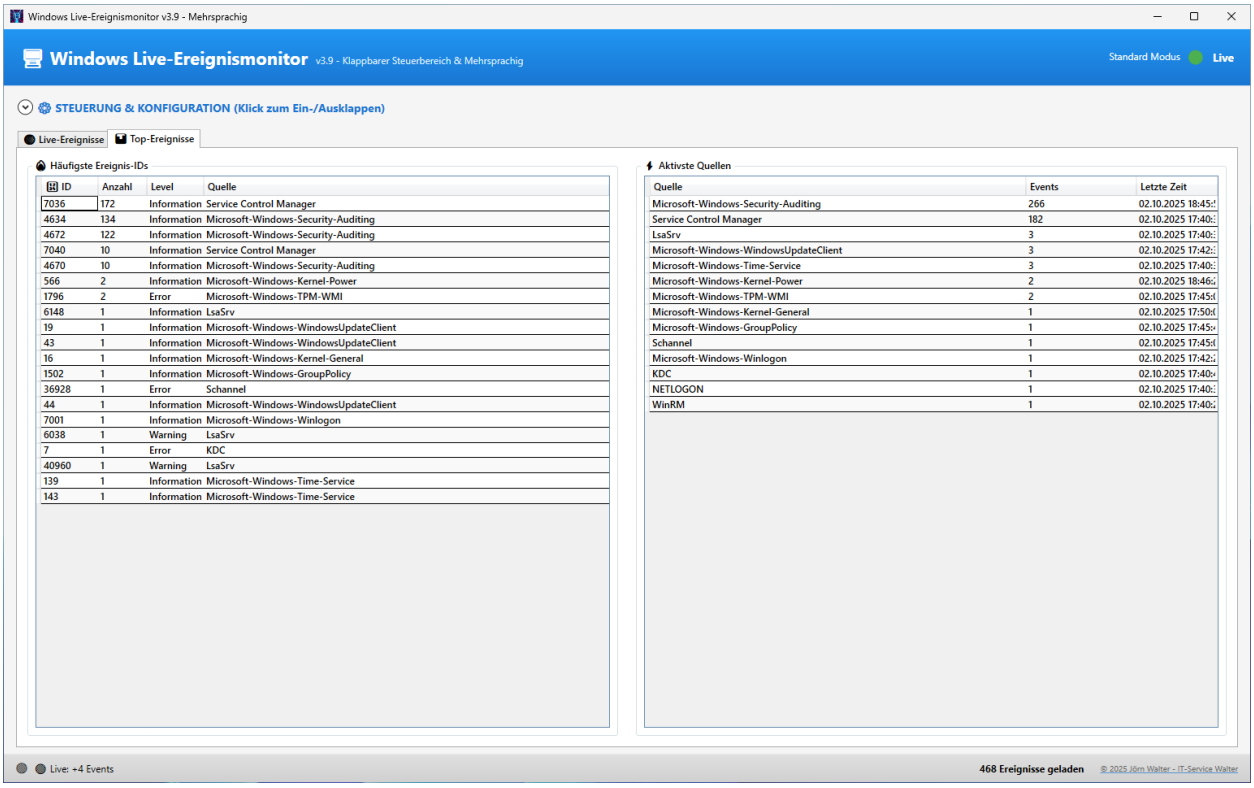
Live-Ereignisse Tab

Hauptansicht mit allen Events:

- **Doppelklick** auf eine Zeile zeigt vollständige Details
- Farbcodierte Level für schnelle Übersicht
- Sortierbar nach allen Spalten

Top-Ereignisse Tab

Statistiken über häufigste Probleme:



Häufigste Ereignis-IDs

- Zeigt die Top 20 Event-IDs
- Mit Anzahl und Quelle
- Hilft Muster zu erkennen

Aktivste Quellen

- Programme/Dienste mit meisten Events
- Zeigt letzte Aktivität
- Identifiziert Problemverursacher

💾 Export-Funktionen

📤 CSV Export

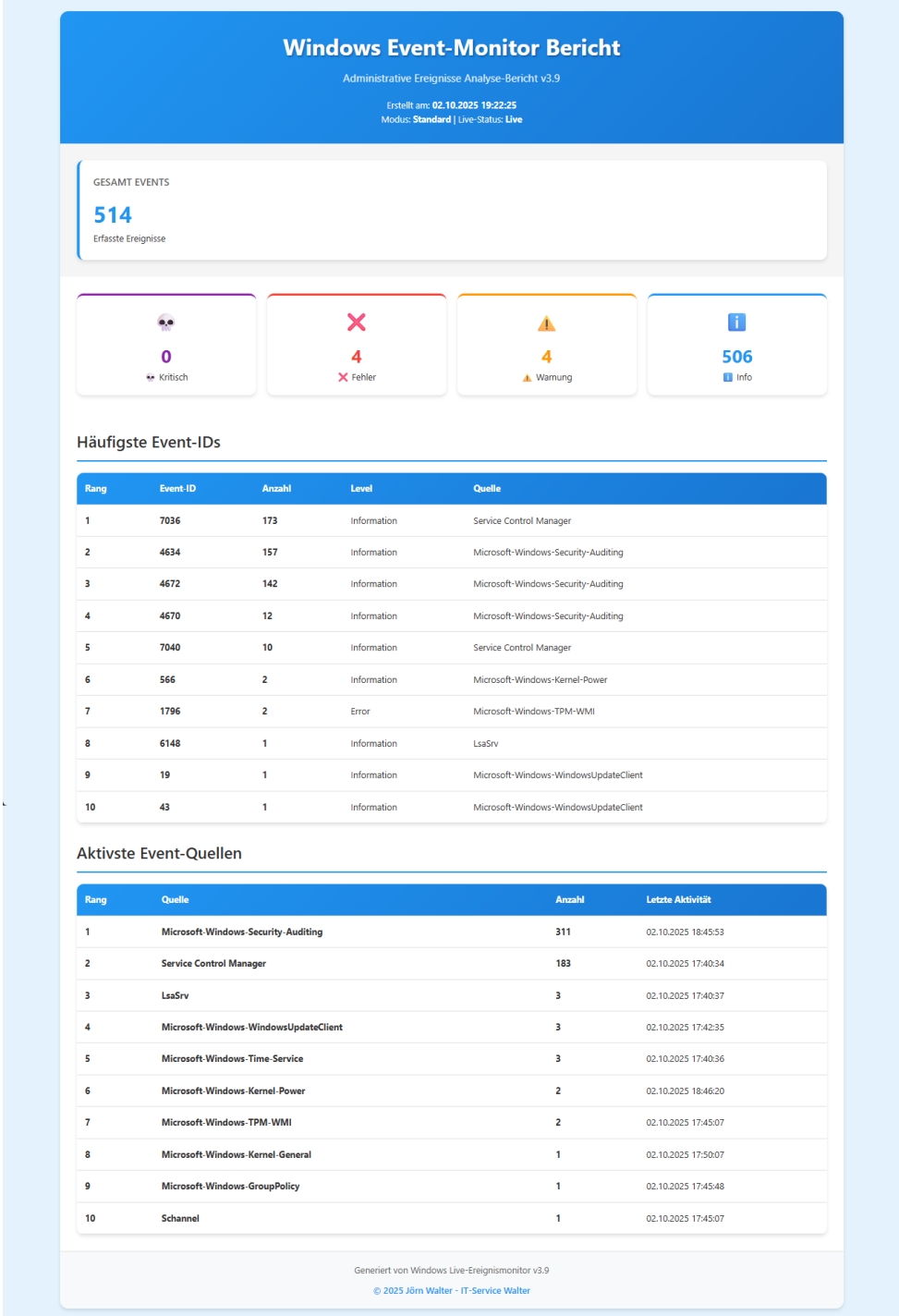
Für: Excel-Analyse, Archivierung

Format: Semikolon-getrennt (;)

- Alle Events mit vollständigen Details
- Importierbar in Excel/LibreOffice

HTML Bericht

Für: Präsentationen, Dokumentation



Windows Event-Monitor Bericht

Administrative Ereignisse Analyse-Bericht v3.9

Erstellt am: **02.10.2025 19:22:25**
Modus: **Standard** | Live-Status: **Live**

GESAMT EVENTS

514

Erfasste Ereignisse

Kritisch	Fehler	Warnung	Info
0	4	4	506

Häufigste Event-IDs

Rang	Event-ID	Anzahl	Level	Quelle
1	7036	173	Information	Service Control Manager
2	4634	157	Information	Microsoft-Windows-Security-Auditing
3	4672	142	Information	Microsoft-Windows-Security-Auditing
4	4670	12	Information	Microsoft-Windows-Security-Auditing
5	7040	10	Information	Service Control Manager
6	566	2	Information	Microsoft-Windows-Kernel-Power
7	1796	2	Error	Microsoft-Windows-TPM-WMI
8	6148	1	Information	LsaSrv
9	19	1	Information	Microsoft-Windows-WindowsUpdateClient
10	43	1	Information	Microsoft-Windows-WindowsUpdateClient

Aktivste Event-Quellen

Rang	Quelle	Anzahl	Letzte Aktivität
1	Microsoft-Windows-Security-Auditing	311	02.10.2025 18:45:53
2	Service Control Manager	183	02.10.2025 17:40:34
3	LsaSrv	3	02.10.2025 17:40:37
4	Microsoft-Windows-WindowsUpdateClient	3	02.10.2025 17:42:35
5	Microsoft-Windows-Time-Service	3	02.10.2025 17:40:36
6	Microsoft-Windows-Kernel-Power	2	02.10.2025 18:46:20
7	Microsoft-Windows-TPM-WMI	2	02.10.2025 17:45:07
8	Microsoft-Windows-Kernel-General	1	02.10.2025 17:50:07
9	Microsoft-Windows-GroupPolicy	1	02.10.2025 17:45:48
10	Schannel	1	02.10.2025 17:45:07

Generiert von Windows Live-Ereignismonitor v3.9

© 2025 Jörn Walter - IT-Service Walter

Enthält:

- Übersichtliche Zusammenfassung
- Farbcodierte Statistiken
- Top 10 häufigste Probleme
- Professionelles Design

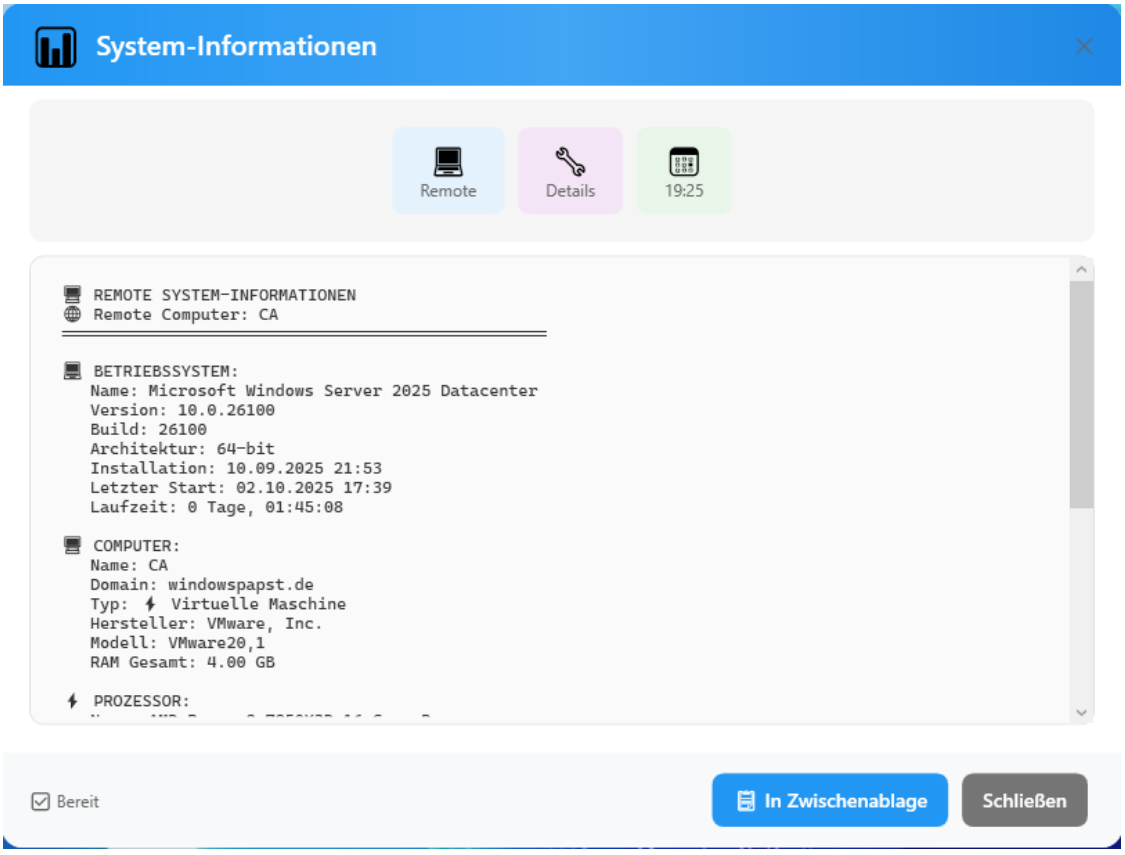
Nach Export: Option zum direkten Öffnen im Browser

🛠️ System-Funktionen

📊 System-Informationen

Zeigt detaillierte Hardware- und Software-Infos:

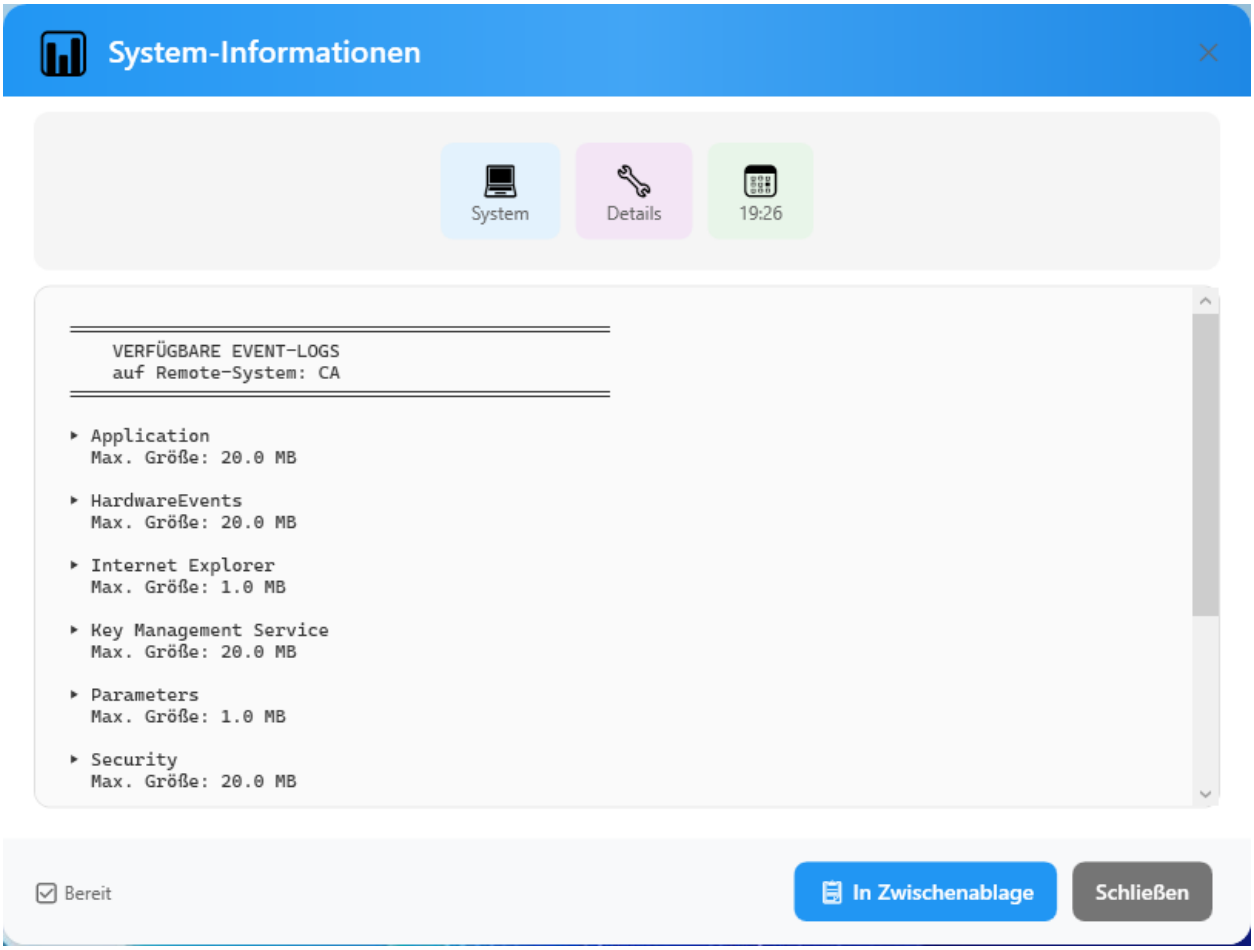
- Betriebssystem-Version
- CPU und RAM
- Festplatten
- Netzwerk
- Laufzeit



🌐 Verfügbare Logs

Listet alle Event-Logs auf dem System:

- Mit Größenangaben
- Überlaufverhalten
- Hilfreich für Administrative Mode



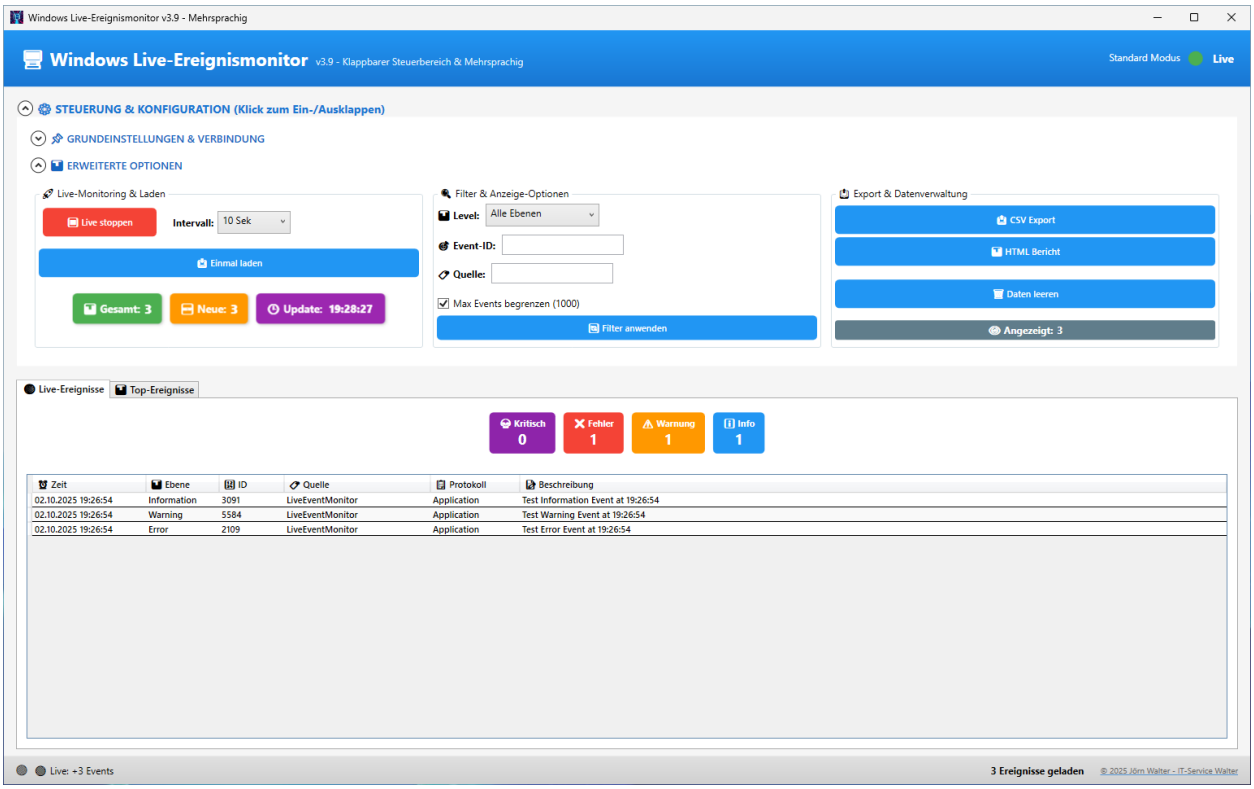
🎯 Test-Events erstellen

Zweck: Testet die Funktionalität

Erstellt 3 Test-Ereignisse:

- Information
- Warnung
- Fehler

Hinweis: Benötigt Administrator-Rechte!



❓ Häufige Probleme

"Keine Daten zum Exportieren"

Lösung: Erst "Einmal laden" ausführen

"Remote-Verbindung fehlgeschlagen"

Prüfen Sie:

1. WinRM-Dienst läuft auf Zielcomputer
2. Firewall-Ports sind offen
3. Benutzer hat Berechtigungen
4. Bei nur Port 5986: SSL-Checkbox aktivieren

"Test-Events fehlgeschlagen"

Lösung: Als Administrator ausführen

Zu viele Events (langsam)

Lösung:

1. "Max Events begrenzen" aktiviert lassen
2. Spezifische Filter verwenden
3. Kürzeres Zeitintervall wählen

💡 Tipps & Tricks

Für Administratoren

1. **Administrative Mode** für Server-Überwachung
2. **HTML-Reports** für Management-Berichte
3. **Event-ID 4625** = Fehlgeschlagene Anmeldungen
4. **Live-Monitoring** während Wartungsarbeiten

Für Fehlersuche

1. Filtern Sie nach **"Kritisch + Fehler"**
2. Sortieren Sie nach **Zeit** (neueste zuerst)
3. Prüfen Sie **Top-Quellen** für wiederkehrende Probleme
4. Exportieren Sie relevante Events für Hersteller-Support

Performance

1. Begrenzen Sie Events auf 1000 (Standard)
2. Verwenden Sie spezifische Filter
3. Größere Intervalle bei Remote-Verbindungen
4. Administrative Mode nur wenn nötig

Technische Details

- Programmiersprache: C# mit WPF
- Anforderungen: Windows 7 oder höher, .NET Framework
- Remote: WinRM-Protokoll über Port 5985/5986
- Sprachen: Deutsch und Englisch

📞 Support

Bei Problemen:

1. Screenshot der Fehlermeldung
2. Export der relevanten Events
3. System-Informationen (aus dem Tool)

Copyright © 2025 Jörn Walter - IT-Service Walter

Verkauf

Das Tool kostet für den Einzelplatz 39,00 € inkl. 19% MwSt. Als Firmenlizenz einmalig 199,00 € inkl. 19% MwSt.