

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

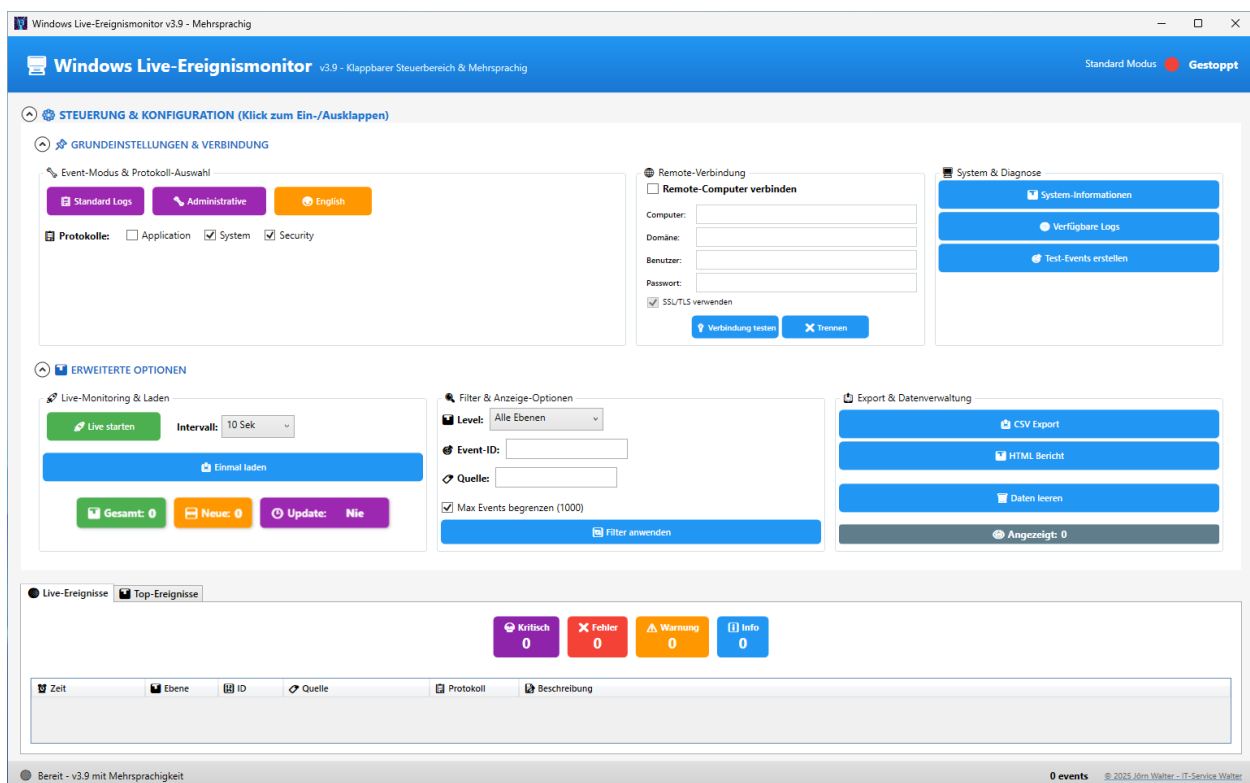
Praktisches Beispiel: Ein Kunde meldet "Der PC stürzt manchmal ab". Mit diesem Tool sehen Sie sofort: Event-ID 41 (Kernel-Power) tritt immer um 14:30 auf = Überhitzung nach Mittagssonne. Problem in 5 Minuten gefunden statt stundenlanger Suche.

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

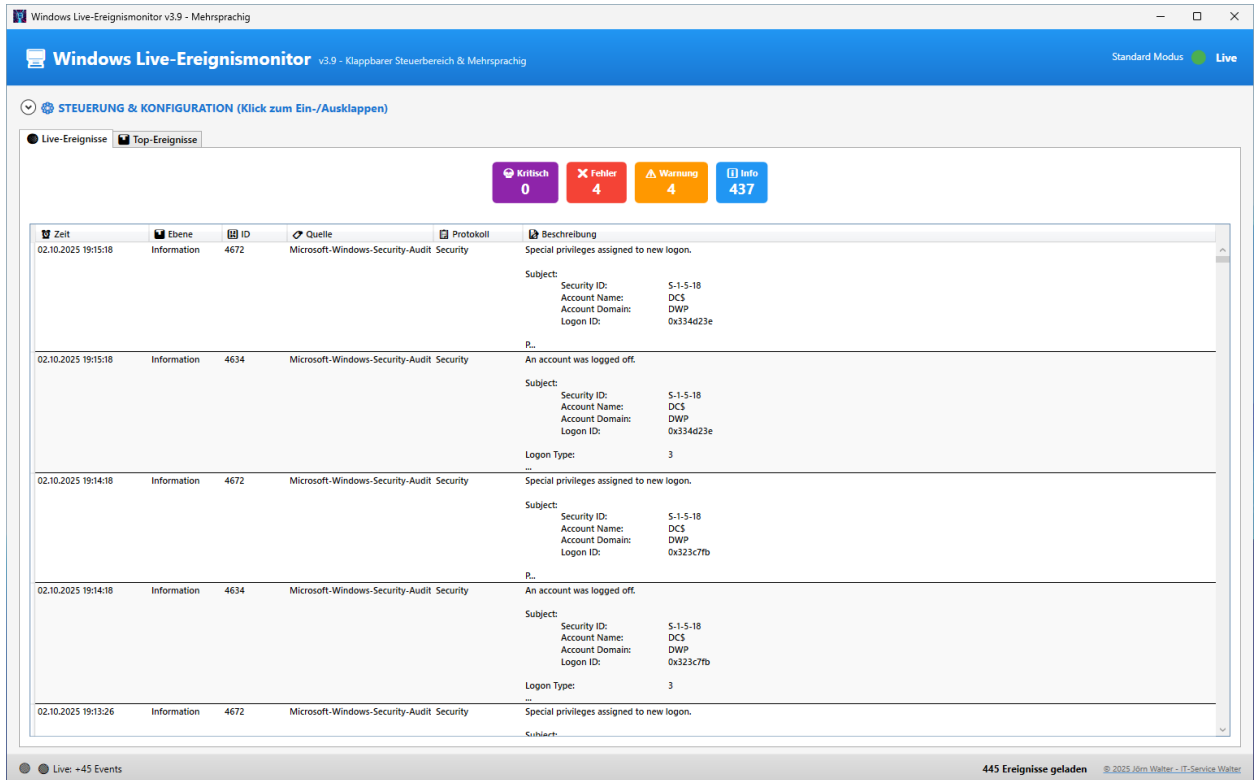
📄 Einmal laden

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!



The screenshot displays the Windows Live-Ereignismonitor v3.9 interface. The top bar shows the application name and version, along with a 'Standard Modus' button and a 'Live' indicator. Below this is a 'STEUERUNG & KONFIGURATION' section with a 'Live-Ereignisse' tab selected. A summary bar shows event counts: 0 Critical, 4 Errors, 4 Warnings, and 437 Info. The main area is a table of events with columns for Time, Level, ID, Source, Protocol, and Description. The events listed are related to user logon and logoff activities, including special privileges assigned to new logon and account logoff events. The bottom status bar indicates 'Live: +45 Events' and '445 Ereignisse geladen'.

Zeit	Ebene	ID	Quelle	Protokoll	Beschreibung
02.10.2025 19:15:18	Information	4672	Microsoft-Windows-Security-Audit	Security	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DCS Account Domain: DWP Logon ID: 0x334d23e
02.10.2025 19:15:18	Information	4634	Microsoft-Windows-Security-Audit	Security	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: DCS Account Domain: DWP Logon ID: 0x334d23e Logon Type: 3
02.10.2025 19:14:18	Information	4672	Microsoft-Windows-Security-Audit	Security	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DCS Account Domain: DWP Logon ID: 0x323c7fb
02.10.2025 19:14:18	Information	4634	Microsoft-Windows-Security-Audit	Security	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: DCS Account Domain: DWP Logon ID: 0x323c7fb Logon Type: 3
02.10.2025 19:13:26	Information	4672	Microsoft-Windows-Security-Audit	Security	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: DCS Account Domain: DWP Logon ID: 0x323c7fb

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

 Live-Monitoring & Laden

 Live stoppen

Intervall: 10 Sek 

 Einmal laden

 Gesamt: 474

 Neue: 74

 Update: 19:19:11

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



Filter & Anzeige-Optionen

Level: Alle Ebenen

Event-ID:

Quelle:

☒ Max Events begrenzen (1000)

 Filter anwenden

Event-ID Filter

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

Quellen-Filter

Suchen Sie nach bestimmten Programmen/Diensten

Anwendung:

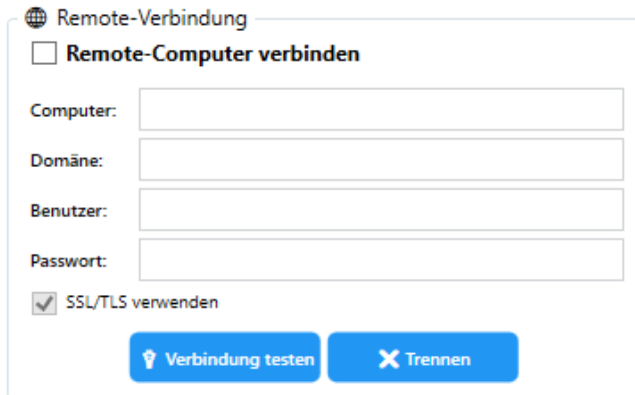
1. Filter einstellen
2. " Filter anwenden" klicken

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

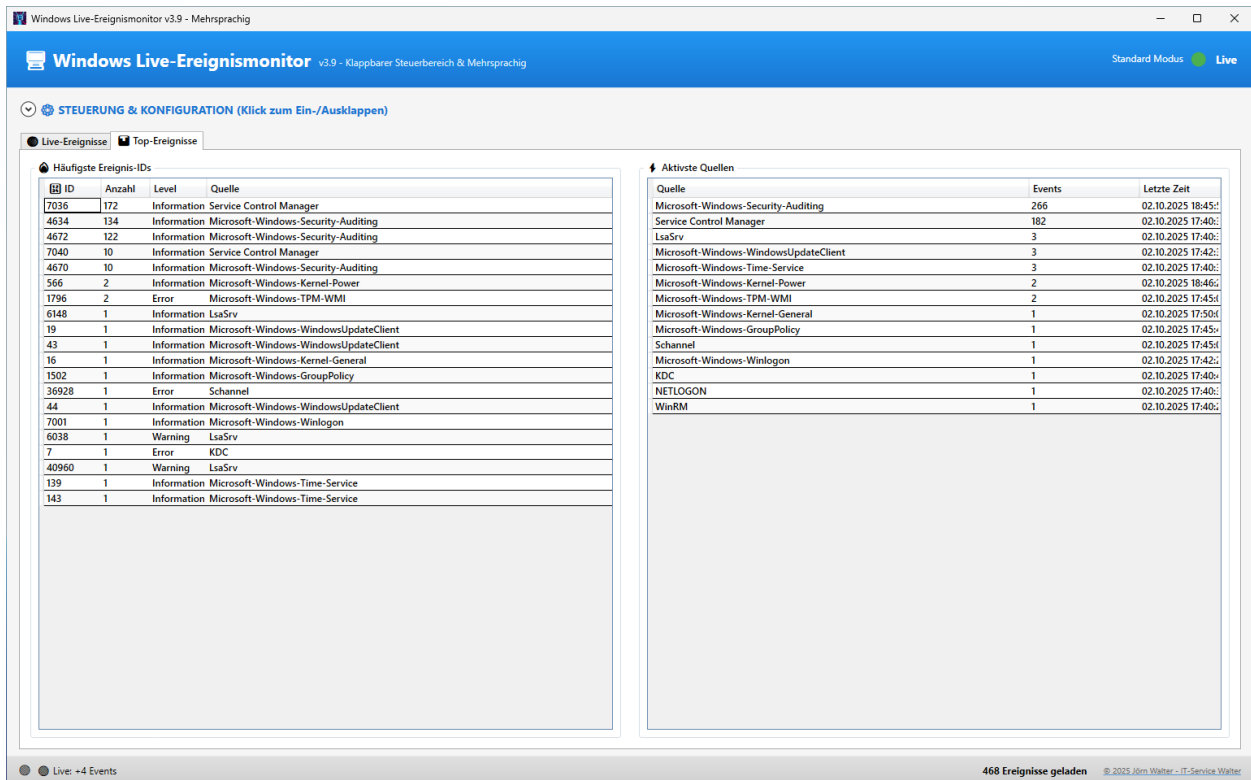
Live-Ereignisse Tab

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:



The screenshot displays the Windows Live-Ereignismonitor v3.9 interface. The main window is titled "Windows Live-Ereignismonitor v3.9 - Klappbarer Steuerbereich & Mehrsprachig". It features a blue header bar with the application name and a "Standard Modus" button. Below the header, there's a "STEUERUNG & KONFIGURATION (Klick zum Ein-/Ausklappen)" section. The main content area is divided into two panels: "Live-Ereignisse" (selected) and "Top-Ereignisse". The "Live-Ereignisse" panel shows a table of "Häufigste Ereignis-IDs" with columns for ID, Anzahl, Level, and Quelle. The "Top-Ereignisse" panel shows a table of "Aktivste Quellen" with columns for Quelle, Events, and Letzte Zeit. The status bar at the bottom indicates "Live: +4 Events" and "468 Ereignisse geladen".

ID	Anzahl	Level	Quelle
7036	172	Information	Service Control Manager
4634	134	Information	Microsoft-Windows-Security-Auditing
4672	122	Information	Microsoft-Windows-Security-Auditing
7040	10	Information	Service Control Manager
4670	10	Information	Microsoft-Windows-Security-Auditing
566	2	Information	Microsoft-Windows-Kernel-Power
1796	2	Error	Microsoft-Windows-TPM-WMI
6148	1	Information	LsaSrv
19	1	Information	Microsoft-Windows-UpdateClient
43	1	Information	Microsoft-Windows-UpdateClient
16	1	Information	Microsoft-Windows-Kernel-General
1502	1	Information	Microsoft-Windows-GroupPolicy
36928	1	Error	Schannel
44	1	Information	Microsoft-Windows-UpdateClient
7001	1	Information	Microsoft-Windows-Winlogon
6038	1	Warning	LsaSrv
7	1	Error	KDC
40960	1	Warning	LsaSrv
139	1	Information	Microsoft-Windows-Time-Service
143	1	Information	Microsoft-Windows-Time-Service

Quelle	Events	Letzte Zeit
Microsoft-Windows-Security-Auditing	266	02.10.2025 18:45:1
Service Control Manager	182	02.10.2025 17:40:1
LsaSrv	3	02.10.2025 17:40:1
Microsoft-Windows-UpdateClient	3	02.10.2025 17:42:1
Microsoft-Windows-Time-Service	3	02.10.2025 17:40:1
Microsoft-Windows-Kernel-Power	2	02.10.2025 18:46:1
Microsoft-Windows-TPM-WMI	2	02.10.2025 17:45:1
Microsoft-Windows-Kernel-General	1	02.10.2025 17:50:1
Microsoft-Windows-GroupPolicy	1	02.10.2025 17:45:1
Schannel	1	02.10.2025 17:45:1
Microsoft-Windows-Winlogon	1	02.10.2025 17:42:1
KDC	1	02.10.2025 17:40:1
NETLOGON	1	02.10.2025 17:40:1
WinRM	1	02.10.2025 17:40:1

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



```
Events_20251002_192335.csv - Notepad
File Edit Format View Help
TimeCreated;Level;Id;Source;LogName;FullMessage
02.10.2025 19:23:18;Information;4672;Microsoft-Windows-Security-Auditing;Security;"Special privileges assigned to new logon.

Subject:
    Security ID:          S-1-5-18
    Account Name:         DC$
    Account Domain:       DWP
    Logon ID:             0xa5fc28c

Privileges:
    SeSecurityPrivilege
    SeBackupPrivilege
    SeRestorePrivilege
    SeTakeOwnershipPrivilege
    SeDebugPrivilege
    SeSystemEnvironmentPrivilege
    SeLoadDriverPrivilege
    SeImpersonatePrivilege
    SeDelegateSessionUserImpersonatePrivilege
    SeEnableDelegationPrivilege"
02.10.2025 19:23:18;Information;4634;Microsoft-Windows-Security-Auditing;Security;"An account was logged off.

Subject:
    Security ID:          S-1-5-18
    Account Name:         DC$
    Account Domain:       DWP
    Logon ID:             0xa5fc28c

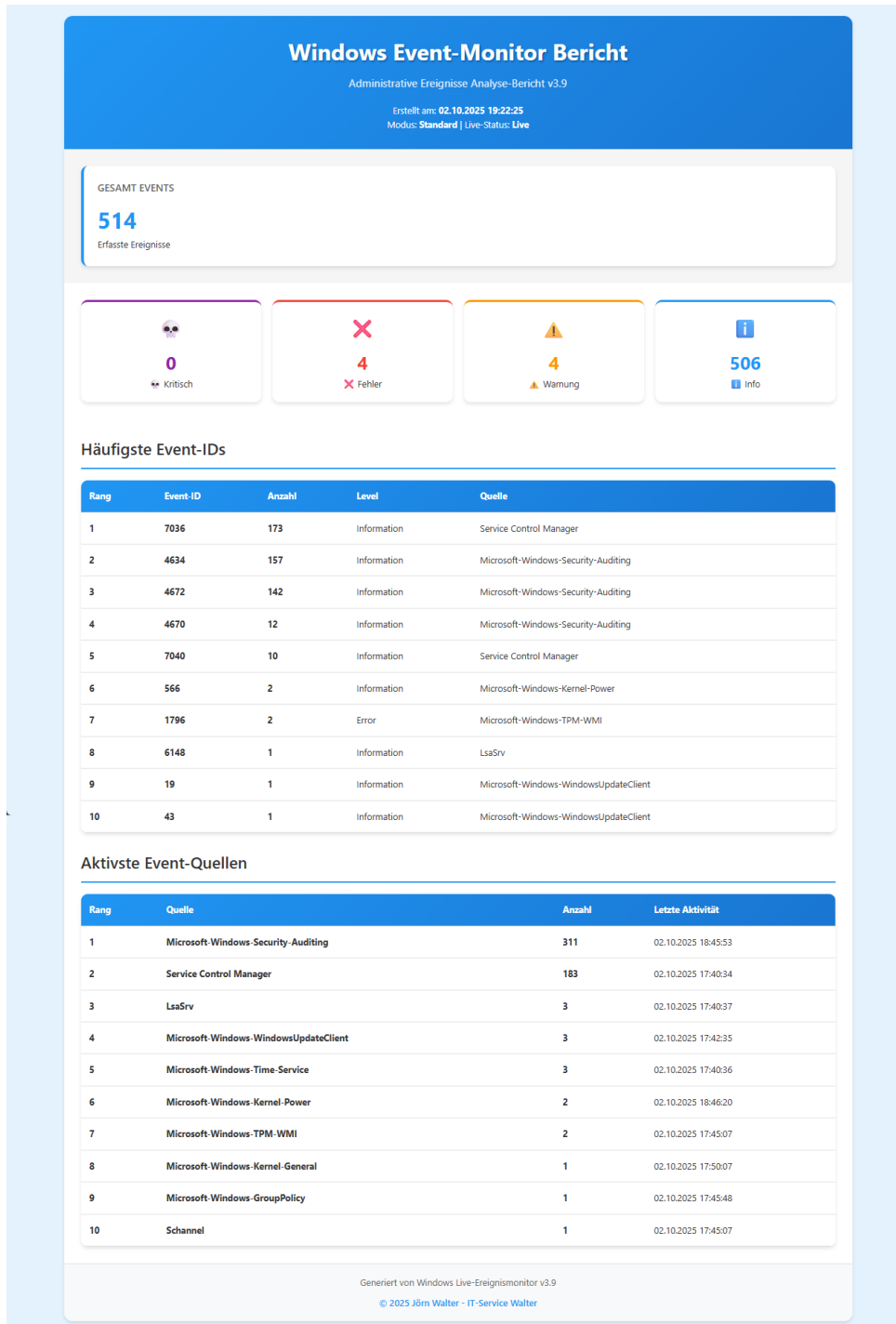
Logon Type:              3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon ID:
02.10.2025 19:22:18;Information;4672;Microsoft-Windows-Security-Auditing;Security;"Special privileges assigned to new logon.
```

Ln 1, Col 1 100% Windows (CRLF) UTF-8 with BOM

HTML Bericht

Für: Präsentationen, Dokumentation



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

 System-Informationen ✕

 Remote

 Details

 19:25

 REMOTE SYSTEM-INFORMATIONEN
 Remote Computer: CA

 BETRIEBSSYSTEM:

Name: Microsoft Windows Server 2025 Datacenter
Version: 10.0.26100
Build: 26100
Architektur: 64-bit
Installation: 10.09.2025 21:53
Letzter Start: 02.10.2025 17:39
Laufzeit: 0 Tage, 01:45:08

 COMPUTER:

Name: CA
Domain: windowspapst.de
Typ: ⚡ Virtuelle Maschine
Hersteller: VMware, Inc.
Modell: VMWare20,1
RAM Gesamt: 4.00 GB

 PROZESSOR:

Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.50GHz

☒ Bereit

 In Zwischenablage

Schließen

Verfügbare Logs

Listet alle Event-Logs auf dem System:

- Mit Größenangaben
- Überlaufverhalten
- Hilfreich für Administrative Mode

 **System-Informationen** 

 System

 Details

 19:26

VERFÜGBARE EVENT-LOGS
auf Remote-System: CA

▶ Application
Max. Größe: 20.0 MB

▶ HardwareEvents
Max. Größe: 20.0 MB

▶ Internet Explorer
Max. Größe: 1.0 MB

▶ Key Management Service
Max. Größe: 20.0 MB

▶ Parameters
Max. Größe: 1.0 MB

▶ Security
Max. Größe: 20.0 MB

☒ Bereit

 In Zwischenablage

Schließen

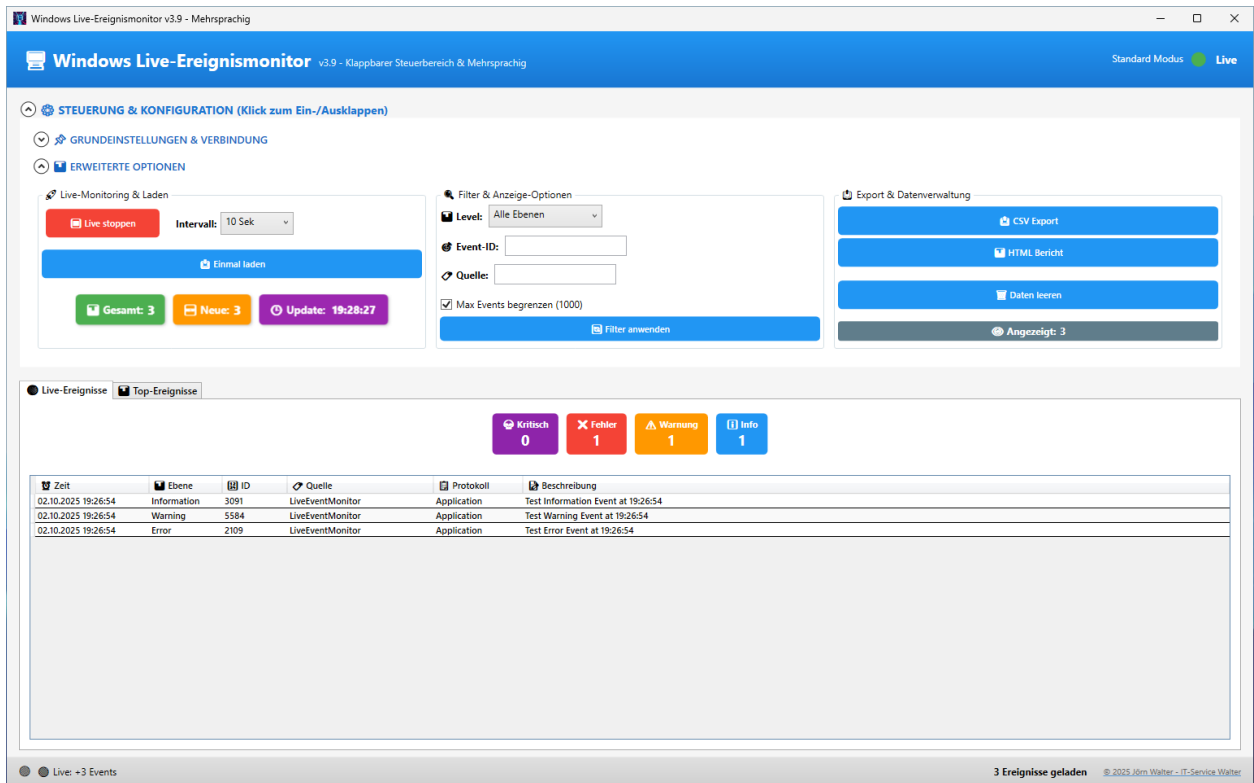
Test-Events erstellen

Zweck: Testet die Funktionalität

Erstellt 3 Test-Ereignisse:

- Information
- Warnung
- Fehler

Hinweis: Benötigt Administrator-Rechte!



Windows Live-Ereignismonitor v3.9 - Mehrsprachig

Standard Modus **Live**

STEUERUNG & KONFIGURATION (Klick zum Ein-/Ausklappen)

GRUNDEINSTELLUNGEN & VERBINDUNG

ERWEITERTE OPTIONEN

Live-Monitoring & Laden

Live stoppen Intervall: 10 Sek

Einmal laden

Gesamt: 3 Neue: 3 Update: 19:28:27

Filter & Anzeige-Optionen

Level: Alle Ebenen

Event-ID:

Quelle:

☒ Max Events begrenzen (1000)

Filter anwenden

Export & Datenverwaltung

CSV Export

HTML Bericht

Daten leeren

Angezeigt: 3

Live-Ereignisse Top-Ereignisse

Kritisch 0 Fehler 1 Warnung 1 Info 1

Zeit	Ebene	ID	Quelle	Protokoll	Beschreibung
02.10.2025 19:26:54	Information	3091	LiveEventMonitor	Application	Test Information Event at 19:26:54
02.10.2025 19:26:54	Warning	5584	LiveEventMonitor	Application	Test Warning Event at 19:26:54
02.10.2025 19:26:54	Error	2109	LiveEventMonitor	Application	Test Error Event at 19:26:54

Live: +3 Events 3 Ereignisse geladen © 2025 Jörn Walter - IT-Service Walter

? 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.