



## Das Microsoft Tool wevtutil einsetzen

Wer über die Kommandozeile mal schnell ein Ereignis auslesen möchte geht wie folgt vor.

Hier einige Beispiele für den Umgang mit dem Tool wevtutil.exe.

Eine Erklärung zu den gängigen Parametern:

- /f: formatiert die Ausgabe in Text
- /e: aktiviert oder deaktiviert ein Protokoll über true oder false
- qe liest Ereignisse aus
- /rd: bestimmt die Richtung der Ereignisse. True sind die neusten und False die älteren
- epl exportiert Logs

**Liest den letzten Eintrag aus Anwendungen aus und gibt diesen als Text aus.**

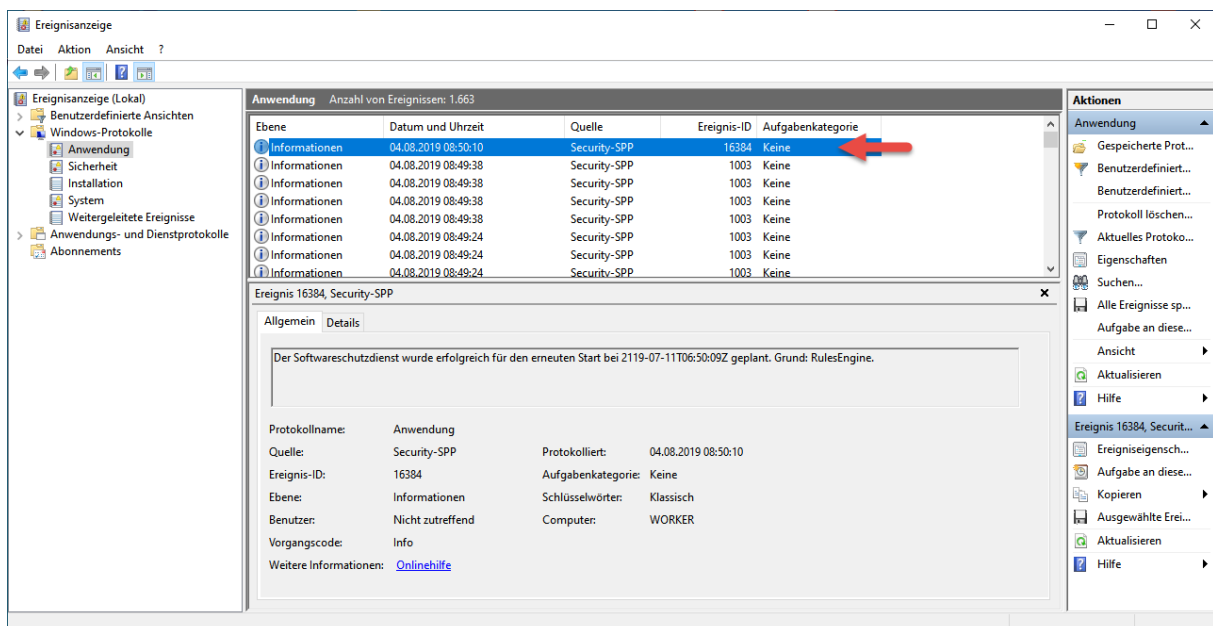
**wevtutil qe Application /c:1 /f:text /rd:true**

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>winevtutil
Der Befehl "winevtutil" ist entweder falsch geschrieben oder
konnte nicht gefunden werden.

C:\Windows\system32>wevtutil qe Application /c:1 /f:text /rd:true
Event[0]:
  Log Name: Application
  Source: Microsoft-Windows-Security-SPP
  Date: 2019-08-04T08:50:10.016
  Event ID: 16384
  Task: N/A
  Level: Informationen
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: WORKER
  Description:
  Der Softwareschutzdienst wurde erfolgreich für den erneuten Start bei 2119-07-11T06:50:09Z geplant. Grund: RulesEngine.

C:\Windows\system32>
```





## Das Microsoft Tool wevtutil einsetzen

### Exportiert alle Ereignisse aus Anwendungen

`wevtutil epl Application C:\Temp\App.evtx`

Administrator: Eingabeaufforderung

```
C:\Windows\system32>wevtutil epl Application C:\Temp\App.evtx  
C:\Windows\system32>
```

Temp

Dieser PC > WIN10ENT (C:) > Temp

Name	Änderungsdatum	Typ	Größe
App.evtx	04.08.2019 09:40	Ereignisprotokoll	2.116 KB

1 Element

### Setzt die maximale Größe für Anwendungen auf 10 MB fest.

`wevtutil sl Application /ms:10485760`

Administrator: Eingabeaufforderung

```
C:\Windows\system32>wevtutil sl Application /ms:10485760  
C:\Windows\system32>
```

Protokolleigenschaften - Anwendung (Typ Verwaltung)

Allgemein Abonnements

Vollständiger Name: Application

Protokollpfad: %SystemRoot%\System32\Winevt\Logs\Application.evtx

Protokollgröße: 2,07 MB(2.166.784 Bytes)

Erstellt: Donnerstag, 23. Mai 2019 09:34:33

Geändert: Sonntag, 4. August 2019 09:41:54

Letzter Zugriff: Sonntag, 4. August 2019 09:41:54

Protokollierung

Max. Protokollgröße (KB): 10240

Bei Erreichen der maximalen Ereignisprotokollgröße:

- Ereignisse bei Bedarf überschreiben (älteste Ereignisse zuerst)
- Volles Protokoll archivieren, Ereignisse nicht überschreiben
- Ereignisse nicht überschreiben (Protokoll manuell löschen)

Protokoll löschen

OK Abbrechen Übernehmen



## Das Microsoft Tool wevtutil einsetzen

Gibt die Ereignisse der letzten 24 Stunden aus, die neusten zuerst.

```
wevtutil qe Application "/q:*[System[TimeCreated[@SystemTime>='2019-08-03T09:00:00' and @SystemTime<'2019-08-04T09:00:00']]]" /f:text /rd:true
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>wevtutil qe Application "/q:*[System[TimeCreated[@SystemTime>='2019-08-03T09:00:00' and @SystemTime<'2019-08-04T09:00:00']]]" /f:text /rd:true
Event[0]:
  Log Name: Application
  Source: Microsoft-Windows-Security-SPP
  Date: 2019-08-04T09:28:08.357
  Event ID: 16384
  Task: N/A
  Level: Informationen
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: WORKER
  Description:
  Der Softwareschutzdienst wurde erfolgreich für den erneuten Start bei 2119-07-11T07:28:08Z geplant. Grund: RulesEngine.

Event[1]:
  Log Name: Application
  Source: Microsoft-Windows-Security-SPP
  Date: 2019-08-04T09:27:37.359
  Event ID: 1003
  Task: N/A
  Level: Informationen
  Opcode: N/A
  Keyword: Klassisch
  User: N/A
  User Name: N/A
  Computer: WORKER
  Description:
  Der Softwareschutzdienst hat die Überprüfung des Lizenzierungsstatus abgeschlossen.
  Anwendungs-ID=0ff1ce15-a989-479d-af46-f275c6370663
  Lizenzierungsstatus=
  1: 6755c7a7-4dfe-46f5-bce8-427be8e9dc62, 1, 1 [(0 [0x00000000, 1, 0], [(?) (1 0x00000000)(?) (2 0x00000000 3 0 msft:rm/algorithm/hwid/4.0 0x00000000 0)(?) (2)(?) (1)(2)(3) ]]
```

**Ereignisanzeige**

Windows-Protokolle > Anwendung > Informationen

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	04.08.2019 09:28:08	Security-SPP	16384	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:36	Security-SPP	16394	Keine
Informationen	04.08.2019 08:50:10	Security-SPP	16384	Keine
Informationen	04.08.2019 08:10:29	Security-SPP	1002	Keine

**Ereignis 1003, Security-SPP**

Allgemein Details

Der Softwareschutzdienst hat die Überprüfung des Lizenzierungsstatus abgeschlossen.

Anwendungs-ID=0ff1ce15-a989-479d-af46-f275c6370663  
Lizenzierungsstatus= 1: 6755c7a7-4dfe-46f5-bce8-427be8e9dc62, 1, 1 [(0 [0x00000000, 1, 0], [(?) (1 0x00000000)(?) (2 0x00000000 3 0

Protokollname: Anwendung  
Quelle: Security-SPP  
Ereignis-ID: 1003  
Ebene: Informationen  
Benutzer: Nicht zutreffend  
Vorgangscodename: Info  
Weitere Informationen: [Onlinehilfe](#)

Protokolliert: 04.08.2019 09:27:37  
Aufgabenkategorie: Keine  
Schlüsselwörter: Klassisch  
Computer: WORKER



## Das Microsoft Tool wevtutil einsetzen

### Archiviert Ereignisse aus einem Ereignisprotokoll

**wevtutil epl Application C:\Temp\AppArchive.evtx**

```
Administrator: Eingabeaufforderung
C:\Windows\system32>wevtutil epl Application C:\AppArchive.evtx
C:\Windows\system32>
```

**Ereignisanzeige** (Lokal)

- Benutzerdefinierte Ansichten
- Windows-Protokolle
- Anwendungs- und Dienstprotokolle
- Gespeicherte Protokolle**
  - AppArchive** (rot markiert)
  - Abonnements

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	04.08.2019 09:28:08	Security-SPP	16384	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:37	Security-SPP	1003	Keine
Informationen	04.08.2019 09:27:36	Security-SPP	16394	Keine
Informationen	04.08.2019 08:50:10	Security-SPP	16384	Keine

**Ereignis 1003, Security-SPP**

Allgemein Details

Der Softwareschutzdienst hat die Überprüfung des Lizenzierungsstatus abgeschlossen.  
Anwendungs-ID=0ff1ce15-a989-479d-af46-f275c6370663

Protokollname: Anwendung  
Quelle: Security-SPP Protokolliert: 04.08.2019 09:27:37  
Ereignis-ID: 1003 Aufgabenkategorie: Keine  
Ebene: Informationen Schlüsselwörter: Klassisch  
Benutzer: Nicht zutreffend Computer: WORKER  
Vorgangscod: Info  
Weitere Informationen: [Onlinehilfe](#)

**Aktionen**

- AppArchive
  - Gespeichert...
  - Benutzerdef...
  - Benutzerdef...
  - Aktuelles Pr...
  - Eigenschaft...
  - Suchen...
  - Alle Ereigni...
  - Ansicht
  - Löschen
  - Umbenennen
  - Aktualisieren
  - Hilfe
- Ereignis 1003, Se...
  - Ereigniseige...
  - Kopieren
  - Ausgewählt...
  - Aktualisieren
  - Hilfe

### Protokoll löschen aber vorher sichern

**wevtutil cl Application /bu:C:\Temp\AppBackup.evt oder evtx**

```
Administrator: Eingabeaufforderung
C:\Windows\system32>wevtutil cl Application /bu:C:\Temp\AppBackup.evt
C:\Windows\system32>
```



## Das Microsoft Tool wevtutil einsetzen

The screenshot shows the Windows Event Viewer window. The left pane shows the tree view with 'Windows-Protokolle' expanded. The main pane shows a table with one entry:

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	04.08.2019 10:06:01	Security-SPP	16384	Keine

Below the table, the details for 'Ereignis 16384, Security-SPP' are shown:

Allgemein Details

Der Softwareschutzdienst wurde erfolgreich für den erneuten Start bei 2119-07-11T08:06:01Z geplant. Grund: RulesEngine.

Protokollname: Anwendung  
Quelle: Security-SPP  
Protokolliert: 04.08.2019 10:06:01  
Ereignis-ID: 16384  
Aufgabenkategorie: Keine  
Ebene: Informationen  
Schlüsselwörter: Klassisch  
Benutzer: Nicht zutreffend  
Computer: WORKER  
Vorgangscod: Info

The screenshot shows a Windows File Explorer window for the 'Temp' folder. The file list contains one item:

Name	Änderungsdatum	Typ	Größe
AppBackup.evt	04.08.2019 10:05	Klassische Ereignisanzeige	2.116 KB

A red arrow points to the 'Typ' column for 'AppBackup.evt'.

## Ein Protokoll aktivieren

wevtutil set-log Microsoft-Windows-PrintService/Admin /e:true /q:true

The screenshot shows a Windows Command Prompt window with the following text:

```
Administrator: Eingabeaufforderung  
C:\Windows\system32>wevtutil set-log Microsoft-Windows-PrintService/Admin /e:true /q:true  
C:\Windows\system32>
```

The screenshot shows the Windows Event Viewer window. The left pane shows the tree view with 'PrintService' expanded and 'Administrator' selected. The main pane shows a table with one entry:

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie

Below the table, the details for 'Administrator' are shown:

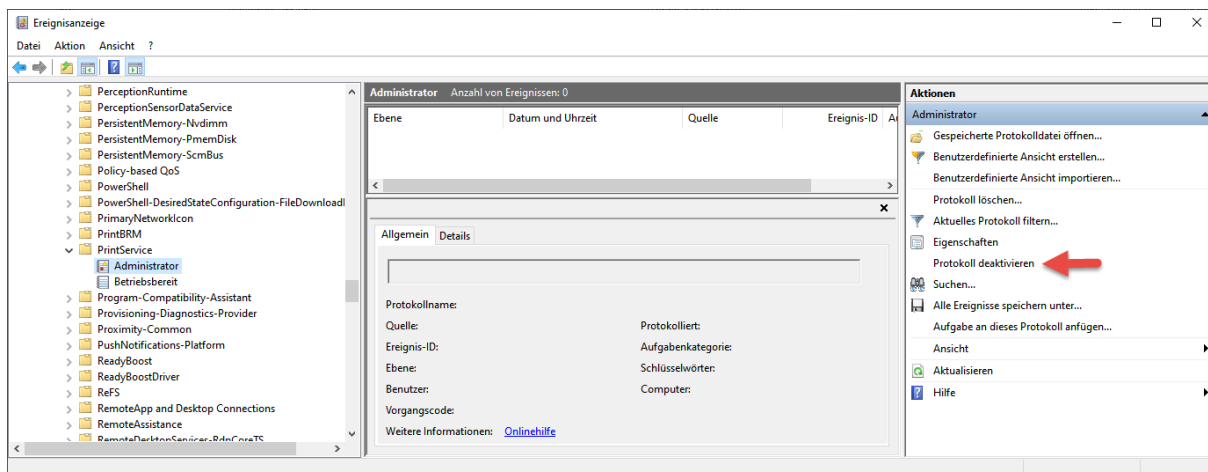
Allgemein Details

Protokollname: Administrator  
Quelle: Administrator  
Protokolliert:   
Ereignis-ID:   
Aufgabenkategorie:   
Ebene:   
Schlüsselwörter:   
Benutzer:   
Computer:   
Vorgangscod:

A red arrow points to the 'Protokoll aktivieren' option in the 'Aktionen' pane.

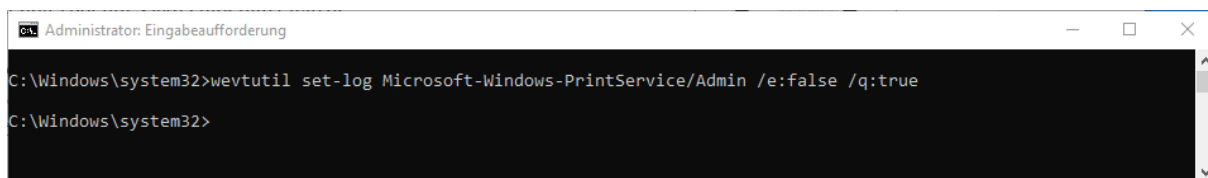


# Das Microsoft Tool wevtutil einsetzen



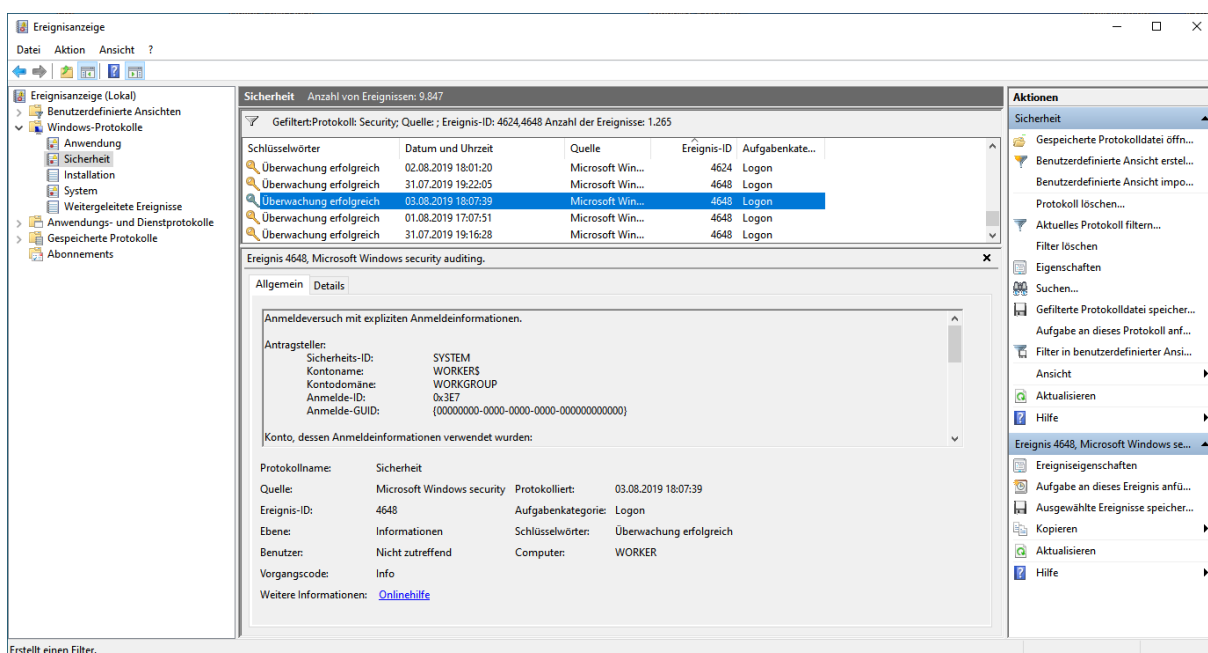
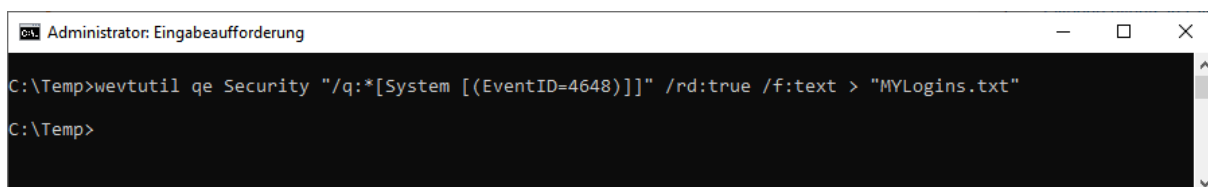
## Ein Protokoll wieder deaktivieren

wevtutil set-log Microsoft-Windows-PrintService/Admin /e:false /q:true



## Eine Abfrage nach einer ID filtern

wevtutil qe Security "/q:\*[System [(EventID=4648)]]" /rd:true /f:text > "MYLogins.txt"  
wevtutil qe Security "/q:\*[System [(EventID=4624)]]" /rd:true /f:text > "MYLogins.txt"





## Das Microsoft Tool wevtutil einsetzen

Abfrage

### Die Basics:

- wevtutil el
  - gibt eine Liste aller Ereignisprotokolle aus
- wevtutil ep
  - gibt eine Liste aller Event-Publisher aus