



Event-ID 4624 Logon Types

Windows dokumentiert unter der Ereignis-ID 4624 erfolgreiche Anmeldeversuche. Dieses Ereignis wird auf dem Computer generiert, auf dem der Zugriffsversuch stattfindet. Somit wird ersichtlich, wie der Benutzer Zugriff auf das System erlangt hat.

Insgesamt gibt es 13 verschiedene Anmeldetypen (Logon Types).

Die gebräuchlichsten Logon Types sind:

- Anmeldetyp 2
- Anmeldetyp 3
- Anmeldetyp 5

Das Pendant dazu ist die Ereignis-ID 4625. Dieses Ereignis registriert die fehlerhaften Anmeldeversuche.

Die Event-ID 4624 gilt für folgende Systeme:

- Windows 7
- Windows Server 2008 R2
- Windows 8.1
- Windows Server 2012 R2
- Windows 10
- Windows Server 2016

Ältere Systeme registrieren die Anmeldeversuche mit der Event-ID 528 und 540.

Die registrierten Ereignisse sehen je nach Windows System etwas anders aus, geben aber die gleichen Informationen her.

Fangen wir erst einmal damit an, die einzelnen Logon Types aufzuzählen und kennenzulernen.

Logon Type 0:

Wird nur vom System Account verwendet.

Logon Type 2:

Ist eine interaktive Anmeldung entweder durch die lokale Eingabe von Benutzernamen und Passwort, durch die Nutzung einer Smartcard, kann aber auch ausgelöst werden durch eine RunAS Funktion oder Remote über Terminaldienste.

Zur Authentifizierung wird die lokale Sicherheitsdatenbank oder die Active Directory Domäne abgefragt.

Logon Type 3:

Bedeutet das eine Netzwerkanmeldung stattgefunden hat. Dahinter steckt oft der Zugriff auf eine Ressource wie z.B. einem freigegebenen Ordner oder Drucker.

Die Anmeldedaten werden nicht durch LSASS verarbeitet oder auf der Festplatte gespeichert.

Logon Type 4:

Dahinter steht in der Regel die Ausführung einer geplanten Aufgabe, wobei hier die hinterlegten Anmeldeinformationen durch LSASS verarbeitet werden. Vor der Ausführung wird zuerst eine Anmeldesitzung ausgeführt, wodurch ein Anmelde- und Abmeldeereignis entsteht.



Event-ID 4624 Logon Types

Logon Type 5:

Wird in der Regel durch einen Dienst ausgeführt, wobei hier die hinterlegten Anmeldeinformationen durch LSASS verarbeitet werden.

Vor dem Starten eines Dienstes wird zuerst eine Anmeldesitzung ausgeführt, wodurch ein Anmelde- und Abmeldeereignis entsteht.

Anmeldedaten liegen auf der Festplatte oder im Speicher (LSA).

Logon Type 6:

Steht für eine Proxy Anmeldung.

Logon Type 7:

Die Arbeitsstation wurde entsperrt, z.B. nach dem Entsperren eines Bildschirmschoners. Windows protokolliert hierzu ein Logon/Logoff-Ergebnis.

Logon Type 8:

Ist eine Klartextanmeldung! Früher verwendet vom IIS (Standardauthentifizierung), sollte nicht mehr eingesetzt werden. Wenn es doch gebraucht wird dann bitte nur in einer SSL Session.

Logon Type 9:

Ist in der Regel die Ausführung durch ein RunAS Netonly. Ohne /netonly wäre das Logon Type 2. Total unsicher!

Logon Type 10:

Ist eine Standard RDP-Benachrichtigung, ausgelöst durch die Anmeldung an Terminaldiensten, Remotedesktop oder einer Remoteunterstützung.

Software von Drittherstellern können diese auch erzeugen, darunter fallen z.B. Virtualisierungskonsolen oder Bildschirmfreigaben.

Verarbeitet durch LSASS.

Logon Type 11:

Anmeldedaten wurde aus einem Cache heraus verwendet. Dahinter steckt die Windows-Funktion "zwischengespeicherte Anmeldungen". Wird verwendet, wenn z.B. kein Domänenkontroller zur Verfügung steht.

Logon Type 12:

Ist ein Ereignis des Typs 10. Die Protokollierung findet statt, wenn das System den Benutzer durch die zwischengespeicherten RDP Anmeldedaten authentifiziert.

Logon Type 13:

Zwischengespeicherte Freigabe.



Event-ID 4624 Logon Types

Sicherheitsinformation:

Jeder Zugriff auf ein System sollte geloggt und ausgewertet werden.

„Oder kannst Du mit Sicherheit sagen, dass hinter der letzten Anmeldung an einem Server keine potenzielle bössartige Aktivität steckt?“ Ich nicht.

Um den gesetzlichen Anforderungen gerecht zu werden, sind genau diese Informationen über erfolgreiche Anmeldungen notwendig.

Ereignisse:

Hier ein paar Beispiele von einem Server 2016.

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Ereignisanzeige (Lokal)' tree with 'Sicherheit' expanded. The main pane shows a list of security events. The event 'Ein Konto wurde erfolgreich angemeldet' (Event ID 4624) is selected. The details pane shows the following information:

Antragsteller:	
Sicherheits-ID:	SYSTEM
Kontoname:	DC015
Kontodomäne:	NDSEDEV
Anmelde-ID:	0x3E7

Anmeldeinformationen:	
Anmeldetyp:	2
Eingeschränkter Administratormodus:	-
Virtuelles Konto:	Nein
Token mit erhöhten Rechten:	Ja

Identitätswechselebene:	
Identitätswechsel:	

Protokollname:	
Sicherheit:	

Quelle:	
Microsoft Windows security	

Ereignis-ID:	
4624	

Ebene:	
Informationen	

Benutzer:	
Nicht zutreffend	

Vorgangscodes:	
Info	

Weitere Informationen:	
Onlinehilfe	

Event-ID 4624 Logon Types

Ereignisanzeige

Datei Aktion Ansicht ?

Ereignisanzeige (Lokal)

- > Benutzerdefinierte Ansichten
- > Windows-Protokolle
 - Sicherheit
 - Anwendung
 - Installation
 - System
 - Weitergeleitete Ereignisse
- > Anwendungs- und Dienstprotokolle
- Abonnements

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolgreich	09.07.2018 18:40:05	Microsoft Windows security auditing.	4634	Abmelden
Überwachung erfolgreich	09.07.2018 18:40:05	Microsoft Windows security auditing.	4624	Anmelden
Überwachung erfolgreich	09.07.2018 18:40:04	Microsoft Windows security auditing.	4689	Prozessbeendigung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4689	Prozessbeendigung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:03	Microsoft Windows security auditing.	4670	Authentifizierungssichtlin

Ereignis 4624, Microsoft Windows security auditing.

Allgemein Details

Ein Konto wurde erfolgreich angemeldet.

Antragsteller:

Sicherheits-ID: NULL SID
Kontoname: -
Kontodomäne: -
Anmelde-ID: 0x0

Anmeldedaten:

Anmeldetyp: 3
Eingeschränkter Administratormodus: -
Virtuelles Konto: Nein
Token mit erhöhten Rechten: Ja

Identitätswechselebene: Identitätswechsel

Protokollname: Sicherheit
Quelle: Microsoft Windows security Protokolliert: 09.07.2018 18:40:05
Ereignis-ID: 4624 Aufgabenkategorie: Anmelden
Ebene: Informationen Schlüsselwörter: Überwachung erfolgreich
Benutzer: Nicht zutreffend Computer: DC01.indesdr.de
Vorgangscod: Info
Weitere Informationen: [Onlinehilfe](#)

Ereignisanzeige

File Action Ansicht ?

Ereignisanzeige (Lokal)

Benutzerdefinierte Ansichten

Windows-Protokolle

Anwendung

Sicherheit

Installation

System

Weitergeleitete Ereignisse

Anwendungs- und Dienstprotokolle

Abonnements

Sicherheit Anzahl von Ereignissen: 154.464 (!) Neue Ereignisse sind verfügbar

Schlüsselwörter	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Überwachung erfolgreich	09.07.2018 18:40:02	Microsoft Windows security auditing.	4670	Autorisierungsrichtlin...
Überwachung erfolgreich	09.07.2018 18:40:02	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:02	Microsoft Windows security auditing.	4670	Autorisierungsrichtlin...
Überwachung erfolgreich	09.07.2018 18:40:02	Microsoft Windows security auditing.	4624	Anmelden
Überwachung erfolgreich	09.07.2018 18:40:02	Microsoft Windows security auditing.	4689	Prozessbeendigung
Überwachung erfolgreich	09.07.2018 18:40:00	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:40:00	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:39:57	Microsoft Windows security auditing.	4688	Prozesserstellung
Überwachung erfolgreich	09.07.2018 18:39:55	Microsoft Windows security auditing.	4689	Prozessbeendigung
Überwachung erfolgreich	09.07.2018 18:39:55	Microsoft Windows security auditing.	4688	Prozesserstellung

Ereignis 4624, Microsoft Windows security auditing.

Allgemein Details

Ein Konto wurde erfolgreich angemeldet.

Antragsteller:

Sicherheits-ID: SYSTEM

Kontoname: DC015

Kontodomäne: NDSEDEV

Anmelde-ID: 0x3E7

Anmeldeinformationen:

Anmeldetyp: 5

Eingeschränkter Administratormodus: -

Virtuelles Konto: Nein

Token mit erhöhten Rechten: Ja

Identitätswechselebene: Identitätswechsel

Protokollname: Sicherheit

Quelle: Microsoft Windows security

Protokolliert: 09.07.2018 18:40:02

Ereignis-ID: 4624

Aufgabenkategorie: Anmelden

Ebene: Informationen

Schlüsselwörter: Überwachung erfolgreich

Benutzer: Nicht zutreffend

Computer: DC01.ndsedv.de

Vorgangscode: Info

Weitere Informationen: [Onlinehilfe](#)

Aktionen

Sicherheit

Gespeichert...

Benutzerde...

Benutzerde...

Protokoll lö...

Aktuelles Pr...

Eigenschaft...

Suchen...

Alle Ereigni...

Aufgabe an...

Ansicht

Aktualisieren

Hilfe

Ereignis 4624, M...

Ereigniseig...

Aufgabe an...

Kopieren

Ausgewählt...

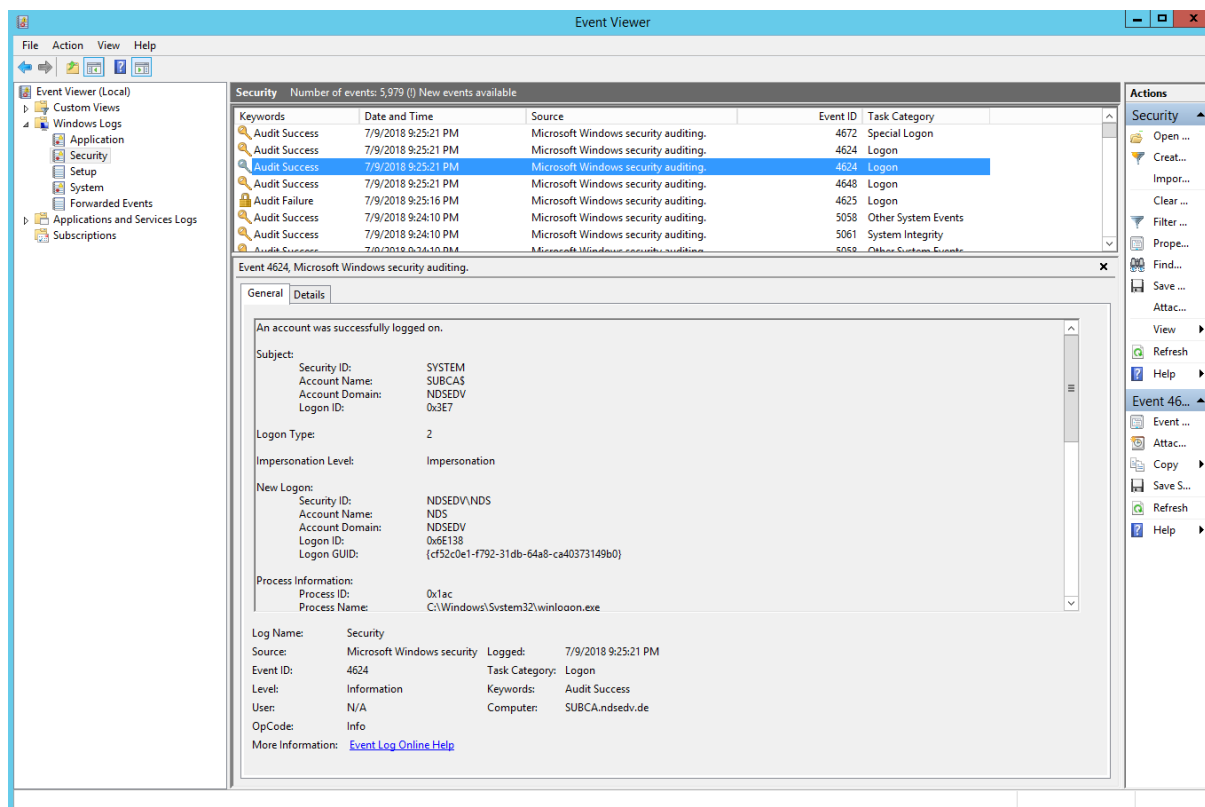
Aktualisieren

Hilfe



Event-ID 4624 Logon Types

Server 2012:



Dieses Ereignis wird beim Erstellen einer Anmeldesitzung generiert. Es wird auf dem Computer generiert, auf den zugegriffen wurde.

Die **Antragstellerfelder** geben das Konto auf dem lokalen System an, von dem die Anmeldung angefordert wurde. Dies ist meistens ein Dienst wie der Serverdienst oder ein lokaler Prozess wie "Winlogon.exe" oder "Services.exe".

Das **Anmeldetypfeld** gibt den jeweiligen Anmeldetyp an. Die häufigsten Typen sind 2 (interaktiv) und 3 (Netzwerk).

Die Felder für die **neue Anmeldung** geben das Konto an, für das die neue Anmeldung erstellt wurde, d. h. das angemeldete Konto.

Die Netzwerkfelder geben die Quelle einer Remoteanmeldeanforderung an. Der Arbeitsstationsname ist nicht immer verfügbar und kann in manchen Fällen leer bleiben.

Das Feld für die **Identitätswechselebene** gibt an, in welchem Umfang ein Prozess in der Anmeldesitzung einen Identitätswechsel vornehmen kann.

Die Felder für die **Authentifizierungsinformationen** enthalten detaillierte Informationen zu dieser speziellen Anmeldeanforderung.

- Die Anmelde-GUID ist ein eindeutiger Bezeichner, der verwendet werden kann, um dieses Ereignis mit einem KDC-Ereignis zu korrelieren.
- Die übertragenen Dienste geben an, welche Zwischendienste an der Anmeldeanforderung beteiligt waren.
- Der Paketname gibt das in den NTLM-Protokollen verwendete Unterprotokoll an.
- Die Schlüssellänge gibt die Länge des generierten Sitzungsschlüssels an. Wenn kein Sitzungsschlüssel angefordert wurde, ist dieser Wert 0.



Event-ID 4624 Logon Types

Weitere Event-IDs:

Event ID	Kategorie/Unterkategorie	Beschreibung
Windows Server 2000-2003 / Windows XP		
528	Logon/Logoff	Successful Logon
538	Logon/Logoff	User Logoff
540	Logon/Logoff	Successful Network Logon
551	Logon/Logoff	User initiated Logoff
672	Account Logon	Authentication Ticket Granted
673	Account Logon	Service Ticket Granted
680	Account Logon	Account Used for Logon by
Windows Server 2008/R2 2012/R2 2016 / Windows 7/8/10		
4624	Logon/Logoff\Logon	An account was successfully logged on
4634	Logon/Logoff\Logon	An account was logged off
4647	Logon/Logoff\Logon	User initiated logoff
4768	Account Logon\Kerberos Authentication Service	A Kerberos authentication ticket (TGT) was requested
4769	Account Logon\Kerberos Service Ticket Operations	A Kerberos service ticket was requested
4776	Account Logon\Credential Validation	The domain controller attempted to validate the credentials for an account

Event-ID alt und neu:

Event ID 528 + 4096 = 4624

Was noch interessant ist sind diese Event-IDs:

Event ID	Level	Event log	Beschreibung
1000	Error	Application	Application Error
1002	Error	Application	Application Hang
1001	Error	System	Microsoft-Windows-WER-SystemErrorReporting
1001	Informational	Application	Windows Error Reporting
1,2	Warning, Error	Application	EMET



Event-ID 4624 Logon Types

Microsoft Windows Security - Ereignisquellen

4608 – STARTUP

4609 – SHUTDOWN

4624 – LOGON

4634 – LOGOFF

4647 – BEGIN_LOGOFF

4778 – SESSION_RECONNECTED

4779 – SESSION_DISCONNECTED

4800 – WORKSTATION_LOCKED

4801 – WORKSTATION_UNLOCKED

4802 – SCREENSAVER_INVOKED

4803 – SCREENSAVER_DISMISSED

Um eine ausführliche Liste aller Ereigniseinträge zu erhalten führen wir folgenden Befehl in der CMD aus:

wevtutil gp Microsoft-Windows-Security-Auditing /ge /gm:true

```
Administrator: Eingabeaufforderung
name: Microsoft-Windows-Security-Auditing
guid: 54849625-5478-4994-a5ba-3e3b0328c30d
helpLink: http://go.microsoft.com/fwlink/events.asp?CoName=Microsoft%20Corporation&ProdName=Microsoft%20Windows%20Operating%20System&ProdVer=10.0.14393.0&FileName=adtschema.dll&FileVer=10.0.14393.0
resourceFileName: C:\Windows\system32\adtschema.dll
parameterFileName: C:\Windows\system32\msobjs.dll
messageFileName: C:\Windows\system32\adtschema.dll
message: Microsoft Windows security auditing.
channels:
  channel:
    name: Security
    id: 10
    flags: 1
    message: Sicherheit
levels:
  level:
    name: win:Informational
    value: 4
    message: Informationen
opcodes:
  opcode:
    name: win:Info
    value: 0
    task: 0
    opcode: 0
    message: Info
tasks:
  task:
    name: SE_ADT_SYSTEM_SECURITYSTATECHANGE
    value: 12288
    eventGUID: 00000000-0000-0000-0000-000000000000
    message: Sicherheitsstatusänderung
  task:
    name: SE_ADT_SYSTEM_SECURITYSUBSYSTEMEXTENSION
    value: 12289
    eventGUID: 00000000-0000-0000-0000-000000000000
    message: Sicherheitssystemerweiterung
  task:
    name: SE_ADT_SYSTEM_INTEGRITY
    value: 12290
-- Fortsetzung --
```



Event-ID 4624 Logon Types

```
Administrator: Eingabeaufforderung
eventGUID: 00000000-0000-0000-0000-000000000000
message: Systemintegrität
task:
  name: SE_ADT_SYSTEM_IPSECDRIVEREVENTS
  value: 12291
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: IPSEC-Treiber
task:
  name: SE_ADT_SYSTEM_OTHERS
  value: 12292
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Andere Systemereignisse
task:
  name: SE_ADT_LOGON_LOGON
  value: 12544
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Anmelden
task:
  name: SE_ADT_LOGON_LOGOFF
  value: 12545
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Abmelden
task:
  name: SE_ADT_LOGON_ACCOUNTLOCKOUT
  value: 12546
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Kontosperrung
task:
  name: SE_ADT_LOGON_IPSECMAINMODE
  value: 12547
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: IPsec-Hauptmodus
task:
  name: SE_ADT_LOGON_SPECIALLOGON
  value: 12548
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Spezielle Anmeldung
task:
  name: SE_ADT_LOGON_IPSECQUICKMODE
  value: 12549
-- Fortsetzung --
```

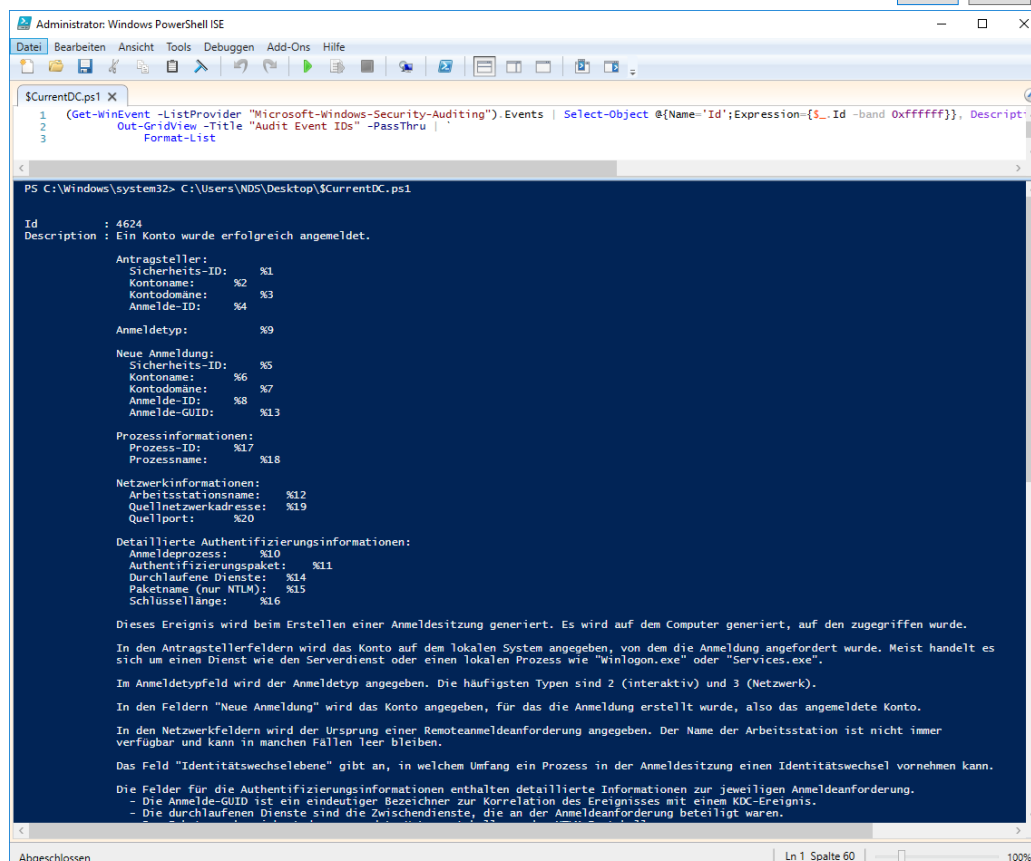
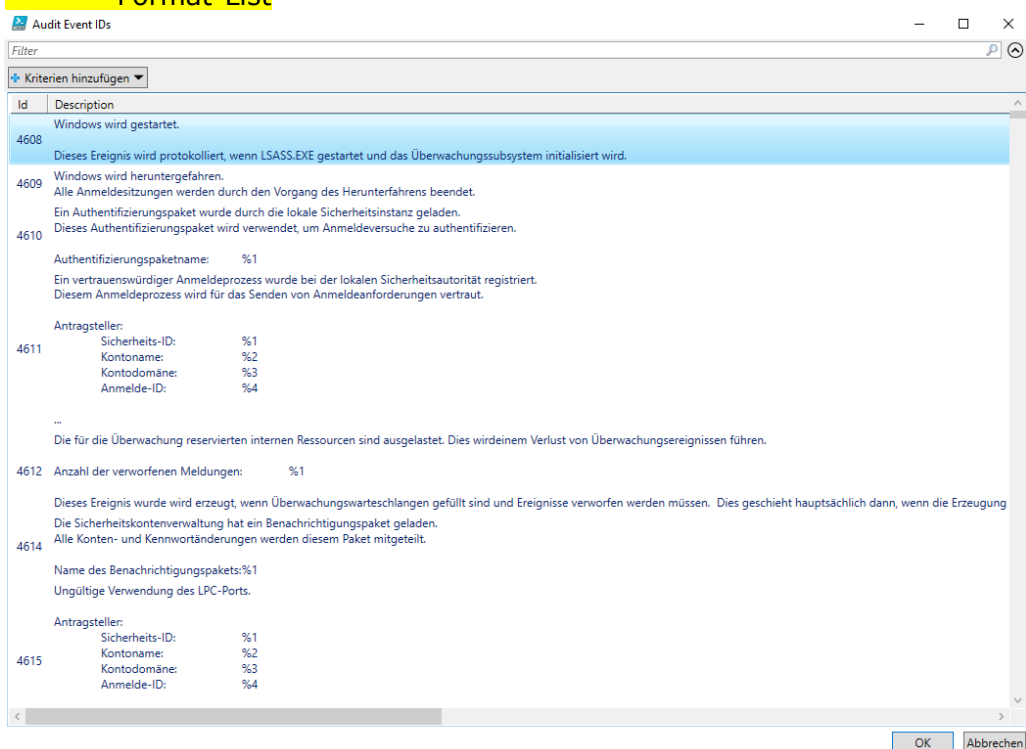
```
Administrator: Eingabeaufforderung
eventGUID: 00000000-0000-0000-0000-000000000000
message: Systemintegrität
task:
  name: SE_ADT_SYSTEM_IPSECDRIVEREVENTS
  value: 12291
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: IPSEC-Treiber
task:
  name: SE_ADT_SYSTEM_OTHERS
  value: 12292
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Andere Systemereignisse
task:
  name: SE_ADT_LOGON_LOGON
  value: 12544
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Anmelden
task:
  name: SE_ADT_LOGON_LOGOFF
  value: 12545
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Abmelden
task:
  name: SE_ADT_LOGON_ACCOUNTLOCKOUT
  value: 12546
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Kontosperrung
task:
  name: SE_ADT_LOGON_IPSECMAINMODE
  value: 12547
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: IPsec-Hauptmodus
task:
  name: SE_ADT_LOGON_SPECIALLOGON
  value: 12548
  eventGUID: 00000000-0000-0000-0000-000000000000
  message: Spezielle Anmeldung
task:
  name: SE_ADT_LOGON_IPSECQUICKMODE
  value: 12549
-- Fortsetzung --
```



Event-ID 4624 Logon Types

Per Powershell:

```
(Get-WinEvent -ListProvider "Microsoft-Windows-Security-Auditing").Events | Select-Object @{{Name='Id';Expression={$_.Id -band 0xfffff}}, Description, @{{Name='Parameters';Expression={$_.Template}.template.data}} | `Out-GridView -Title "Audit Event IDs" -PassThru | `Format-List
```





Event-ID 4624 Logon Types

Windows verwendet einen Industriestandard zum Weiterleiten von Ereignisprotokollen, sodass wir Protokolle an jedes Windows-System oder ein SIEM Produkt senden können.

<https://www.der-windows-papst.de/2018/07/10/windows-ereignisse-weiterleiten/>