

Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen

4024 warnt, 4025 sperrt

Zwei Ereignisse, ein Protokoll, und meistens liest sie erst jemand, wenn das WLAN schon weg ist.

4024

Warnung · Überwachung

Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten wurde erlaubt, aber notiert

4025

Fehler · Erzwingung

Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten wurde durch Richtlinie blockiert

Microsoft-Windows-NTLM/Operational · nur Windows 11 ab 24H2 und Windows Server 2025

Skizze: die beiden Ereignisse zu BlockNtlm1SSO auf einen Blick

WISSEN

Was der NTLM Diagnostiker erfasst, wie er arbeitet und was er kostet.

› [NTLM Diagnostiker](#)

BERATUNG

4024 und 4025 auswerten, Quellen umstellen, Erzwingung sauber absichern.

› [Beratung zur NTLM-Ablösung](#)

SCHULUNG

NTLM-Ereignisse lesen, filtern und zentral sammeln: für dein ganzes Team.

› [Schulung zum NTLM Diagnostiker](#)

Du bist hier, weil du nach „Ereignis 4025 NTLM“ gesucht hast. Wahrscheinlich nicht aus akademischem Interesse, sondern weil irgendwo ein Notebook nicht mehr ins WLAN kommt, ein VPN-Profil plötzlich nach dem Kennwort fragt oder ein Kiosk-Terminal im Lager seit dem Patchday beleidigt schweigt. Und dann findest du in der Ereignisanzeige einen roten Eintrag mit einem Satz, der ungefähr so beruhigend klingt wie ein Anruf vom Steuerprüfer: Ein Versuch, NTLMv1-abgeleitete Anmeldedaten für Single Sign-on zu verwenden, wurde durch eine Richtlinie blockiert.

Gute Nachricht vorweg: Das Ereignis ist kein Fehler im eigentlichen Sinn, sondern Windows macht genau das, was Microsoft angekündigt hat. Seit dem Sicherheitsupdate vom 13.10.2026 blockieren Windows 11 ab Version 24H2 und Windows Server 2025 standardmäßig Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten. Ereignis 4025 ist der Beleg dafür, Ereignis 4024 war ein Jahr lang die Vorwarnung. Die schlechte Nachricht: Ein einzelnes Ereignis auf einem einzelnen Rechner sagt dir fast nichts darüber, wie groß dein Problem ist.

In diesem Beitrag zerlegen wir beide Ereignisse: was sie bedeuten, wo sie stehen, wie du Quelle und Ziel herausliest, wie du sie mit wevtutil und Get-WinEvent filterst und warum du sie zentral sammeln musst, wenn du mehr als einen Rechner besitzt. Was die Sperre im Alltag anrichtet, beschreibt der Beitrag [NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht](#); den Registrierungswert dahinter erklärt [BlockNtlm1SSO erklärt: Überwachung, Erzwingung, Ausnahme](#).

FAKTEN · Ereignis 4024 und 4025 in 30 Sekunden

Protokoll: Microsoft-Windows-NTLM/Operational, Quelle NTLM. Zu finden in der Ereignisanzeige

unter Anwendungs- und Dienstprotokolle, Microsoft, Windows, NTLM, Operational.

4024 ist eine Warnung im Überwachungsmodus: Die Anfrage wurde erlaubt und protokolliert. 4025 ist ein Fehler im Erzwingungsmodus: Die Anfrage wurde blockiert.

Gesteuert über den Registrierungswert BlockNtlmv1SSO unter

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0: 0 = Überwachung, 1 = Erzwingung.

Fehlt der Wert, gilt seit dem 13.10.2026 die Erzwingung.

Betroffen sind nur Windows 11 24H2, 25H2, 26H1, 26H2 und Windows Server 2025. Mit aktivem Credential Guard greift die Änderung nicht, dann gibt es auch keine Ereignisse.

Beide Ereignisse enthalten dieselben Angaben: Zielsystem, übergebener Benutzer und Domäne, Prozess-ID, Name und LUID des Clientprozesses, dessen Benutzeridentität und Domäne sowie die OID des Mechanismus.

Was 4024 und 4025 bedeuten

Beide Ereignisse gehören zum selben Mechanismus und unterscheiden sich nur in einer Kleinigkeit, die für deine Anwender allerdings keine Kleinigkeit ist: ob Windows die Anfrage durchgelassen hat oder nicht. Gemeint ist immer derselbe Fall. Ein Programm, typischerweise die WLAN- oder VPN-Anmeldung mit MS-CHAPv2, möchte die Anmeldedaten des angemeldeten Benutzers automatisch weiterreichen, und zwar in einer Form, die aus NTLMv1-Kryptografie abgeleitet ist. Diese Form gilt seit Jahren als geknackt; mit genug Rechenleistung ist ein mitgeschnittener Austausch etwa so sicher wie ein Fahrradschloss aus Lakritz.

Die beiden Ereignisse im Vergleich

Merkmal	Ereignis 4024	Ereignis 4025
Ebene	Warnung	Fehler
Modus	Überwachung (Audit)	Erzwingung (Enforce)
Ergebnis für den Anwender	Single Sign-on funktioniert	Single Sign-on scheitert
Meldungstext (englisch)	Auditing an attempt to use NTLMv1-derived credentials for Single Sign-On	An attempt to use NTLMv1-derived credentials for Single Sign-On was blocked due to policy.
BlockNtlmv1SSO	0, oder Wert fehlt auf einem Rechner ohne Oktober-Update 2026	1, oder Wert fehlt auf einem Rechner mit Oktober-Update 2026
Protokoll	Microsoft-Windows-NTLM/Operational	Microsoft-Windows-NTLM/Operational
Was du tun solltest	Quelle finden, bevor sie blockiert wird	Auswirkung prüfen, Quelle umstellen, nur notfalls befristete Ausnahme

Wo die Ereignisse überhaupt entstehen

Die Ereignisse gibt es nur auf Windows 11 ab Version 24H2 und auf Windows Server 2025. Ein Windows 10 schreibt sie nicht, ein Server 2022 auch nicht, selbst wenn dort fröhlich NTLMv1 im Einsatz ist. Und sie entstehen auf dem Rechner, der die Anmeldedaten weitergeben will, also in der Regel auf dem Client. Der Domain Controller bekommt von 4024 und 4025 nichts mit. Wer dort nach den Ereignissen sucht, sucht so lange wie nach dem Lichtschalter in einem Raum ohne Strom.

System	4024 und 4025?	Was stattdessen hilft
Windows 11 24H2, 25H2, 26H1, 26H2	ja, sofern Credential Guard nicht aktiv ist	–
Windows Server 2025	ja, sofern Credential Guard nicht	–

	aktiv ist	
Rechner mit aktivem Credential Guard	nein, NTLMv1-Kryptografie ist dort ohnehin gesperrt	Netzzugang trotzdem auf Zertifikate prüfen
Windows 10, Windows 11 vor 24H2	nein	klassische Restrict-NTLM-Überwachung, Ereignisse 8001 bis 8004
Windows Server 2022 und 2019	nein	erweitertes NTLM-Auditing mit Updates ab 13.10.2026 (4020 bis 4023), zusätzlich 8001 bis 8004
Domain Controller	nein, dort entstehen 4024 und 4025 nicht	erweitertes Auditing 4030 bis 4033, klassisch 8004

WARNUNG · Leeres Protokoll heißt nicht sauberes Netz

Kein 4024 und kein 4025 auf einem Rechner kann drei Dinge bedeuten: Es gab keinen Versuch, Credential Guard hat die Sache vorher erledigt, oder der Rechner läuft auf einer Windows-Version, die diese Ereignisse gar nicht kennt. Nur die erste Variante ist eine gute Nachricht. Prüfe also immer zuerst Version und Credential Guard, bevor du ein leeres Protokoll als Freispruch wertest.

Verwandte Ereignisse, die du nicht verwechseln solltest

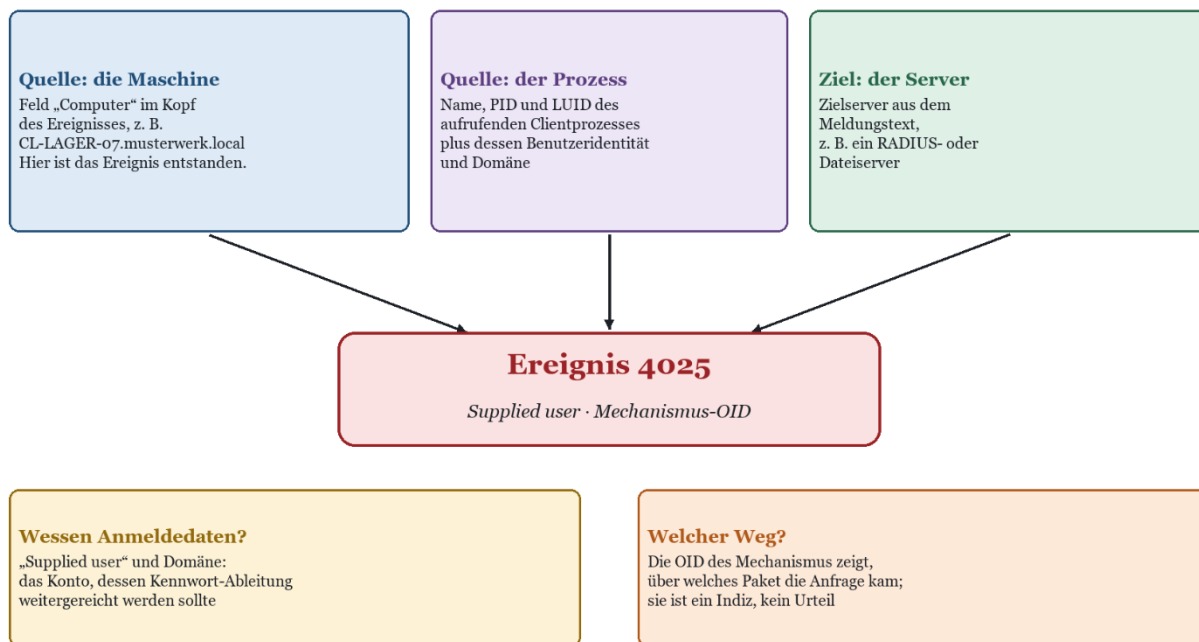
4024 und 4025 drehen sich ausschließlich um Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten. Das erweiterte NTLM-Auditing nach Microsoft KB5064479 bringt im selben Protokoll eine ganze Familie weiterer Ereignisse mit, die allgemeine NTLM-Nutzung zeigen: 4020 bis 4023 auf Clients und Servern, 4030 bis 4033 auf Domain Controllern, jeweils mit einer Reason-ID von 0 bis 11, die erklärt, warum nicht Kerberos zum Zug kam. Die ausgehende Seite beschreibt [Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen](#), die Sicht des Domain Controllers [NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004](#). Wer das erweiterte Auditing noch nicht eingeschaltet hat, findet die Anleitung in [Erweitertes NTLM-Auditing einschalten: Schritt für Schritt](#).

Quelle und Ziel aus dem Ereignis herauslesen

Ein 4025 ist im Grunde ein Polizeibericht: Tatort, Täter, Opfer, Tatwerkzeug. Man muss ihn nur lesen. Microsoft beschreibt in KB5066470, welche Angaben drinstehen, und die reichen fast immer aus, um die Ursache einzugrenzen.

Wer wollte wohin? So zerlegst du ein 4025

Musterwerk GmbH, musterwerk.local: ein Ereignis, drei Fragen, alles steht im Meldungstext



Skizze: Inhalte nach Microsoft KB5066470; Hostname frei erfunden

Die Quelle: Maschine und Prozess

Die Maschine steht nicht im Meldungstext, sondern im Kopf des Ereignisses, im Feld „Computer“. Auf dem Rechner selbst ist das trivial, beim zentralen Sammeln wird es zur wichtigsten Spalte. Spannender ist der Prozess: Name, Prozess-ID und LUID des aufrufenden Clientprozesses sowie die Identität, unter der er läuft. Steht dort ein Systemdienst, der für die Netzanmeldung zuständig ist, bist du beim WLAN oder beim kabelgebundenen 802.1X. Steht dort ein VPN-Client oder eine Fachanwendung, weißt du, bei welchem Hersteller du anrufen darfst.

Das Ziel: der Server

Der Zielserver ist das Gegenüber, an das die Anmeldedaten gehen sollten. Bei MS-CHAPv2 im Netzzugang ist das oft nicht der Dateiserver, an den du zuerst denkst, sondern die Infrastruktur dazwischen, zum Beispiel ein RADIUS-Dienst oder ein VPN-Gateway. Ein Ziel, das in vielen 4025 auf vielen Rechnern auftaucht, ist dein Hauptverdächtiger. Ein Ziel, das nur einmal auftaucht, ist vermutlich das Notebook des Geschäftsführers im Hotel-WLAN. Auch wichtig, aber anders wichtig.

Benutzer und Mechanismus

„Supplied user“ und die zugehörige Domäne nennen das Konto, dessen Anmeldedaten weitergegeben werden sollten. Das ist nicht zwingend dasselbe Konto, unter dem der Prozess läuft. Die OID des Mechanismus verrät, über welches Sicherheitspaket die Anfrage kam. Sie ist ein Indiz für die Einordnung, kein Urteil über die Schuld.

Frage	Wo du die Antwort findest	Typische Erkenntnis
Auf welchem Rechner?	Kopf des Ereignisses, Feld „Computer“	betroffene Maschine
Welches Programm?	Meldungstext: Name, PID und LUID des Clientprozesses	WLAN-Dienst, VPN-Client, Fachanwendung
Unter welcher Identität läuft es?	Meldungstext: Benutzeridentität und Domäne des Prozesses	Dienst unter SYSTEM oder Benutzersitzung
Wessen	Meldungstext: Supplied user und	betroffenes Benutzerkonto

Anmeldedaten?	Domäne	
Wohin sollte es gehen?	Meldungstext: Zielsever	RADIUS, VPN-Gateway, Server
Über welchen Weg?	Meldungstext: OID des Mechanismus	Sicherheitspaket der Anfrage

TIPP · Feldnamen nicht raten, sondern nachsehen

Die Beschriftungen im Meldungstext hängen von der Sprache des Betriebssystems ab, und die internen Namen in der XML-Ansicht sind nicht zwingend dieselben wie im Meldungstext. Öffne ein echtes 4025, wechsele in der Ereignisanzeige auf die Registerkarte „Details“ und dort auf die XML-Ansicht. Was dort unter EventData steht, ist die Grundlage für jedes Skript. Das Skript weiter unten liest die Namen deshalb aus dem Ereignis selbst aus, statt sie vorauszusetzen.

AUS DER PRAXIS · Musterwerk GmbH: 37 rote Einträge, eine Ursache

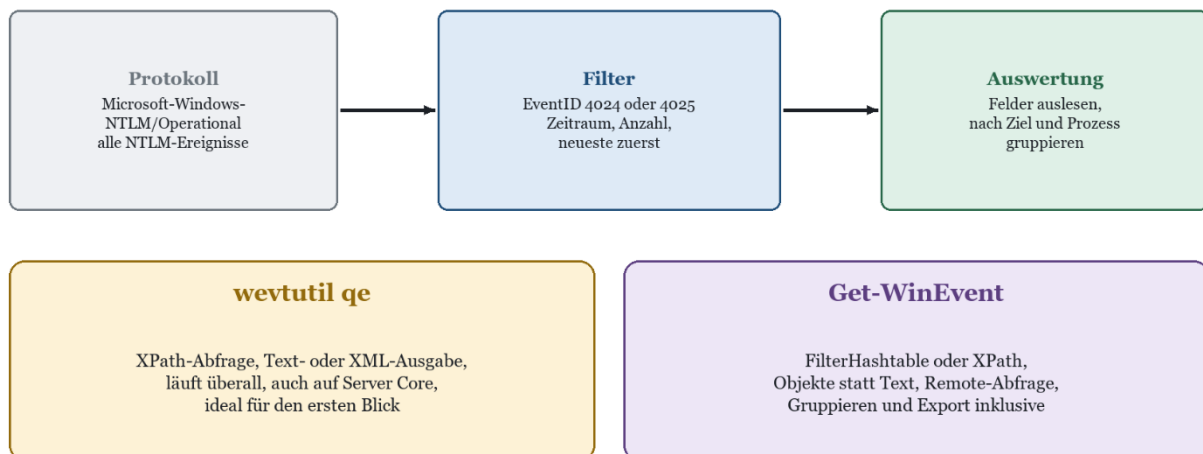
Am Mittwoch nach dem Patchday meldete das Lager in Halle 3, dass sich die Hands scanner-Stationen nicht mehr mit dem Lager-WLAN verbinden. Auf einer der Stationen fanden sich 37 Ereignisse 4025, alle mit demselben Prozess, demselben Ziel und demselben übergebenen Gerätebenutzer. Das WLAN-Profil arbeitete noch mit PEAP-MSCHAPv2 und gespeicherten Anmeldedaten. Ursache gefunden, Lösung bekannt: Umstellung auf Zertifikatsanmeldung. Das Lesen hat zehn Minuten gedauert, die Frage „Welche Stationen noch?“ hat zwei Tage gedauert. Dazu gleich mehr.

Filtern mit wevtutil und Get-WinEvent

Klicken in der Ereignisanzeige funktioniert für das erste Ereignis. Ab dem zehnten möchtest du filtern, ab dem hundertsten gruppieren. Beides geht mit Bordmitteln, und beides solltest du einmal von Hand gemacht haben, bevor du es automatisierst.

Vom Rauschen zur Liste: zwei Werkzeuge, ein Ziel

wevtutil für die schnelle Abfrage, Get-WinEvent für alles, was danach kommt



Skizze: Filterweg für 4024 und 4025 mit Bordmitteln

Zuerst: Ist das Protokoll aktiv?

Bevor du dich über ein leeres Ergebnis freust, prüf, ob das Protokoll überhaupt aufzeichnet und wie groß es ist. Ein Protokoll mit Mindestgröße überschreibt die interessanten Ereignisse schneller, als du „Montagmorgen“ sagen kannst.

```
wevtutil gl Microsoft-Windows-NTLM/Operational
```

```
REM enabled: true sollte dort stehen, maxSize zeigt die Größe in Bytes
REM Größe bei Bedarf anheben, hier auf 64 MB:
wevtutil sl Microsoft-Windows-NTLM/Operational /ms:67108864
```

wevtutil: schnell und überall

wevtutil ist das Schweizer Taschenmesser für die Kommandozeile und läuft auch dort, wo PowerShell-Remoting gerade nicht will. Die Abfrage nutzt XPath auf den System-Teil des Ereignisses, also nur auf Felder, die jedes Ereignis hat. Das ist robust und unabhängig von Sprache und Feldnamen.

```
REM die letzten 20 Ereignisse 4024 und 4025, neueste zuerst, als Text
wevtutil qe Microsoft-Windows-NTLM/Operational ^
/q:"*[System[(EventID=4024 or EventID=4025)]]" /c:20 /rd:true /f:text
```

```
REM nur 4025 der letzten 24 Stunden (86400000 Millisekunden), als XML
wevtutil qe Microsoft-Windows-NTLM/Operational ^
/q:"*[System[(EventID=4025) and TimeCreated[timediff(@SystemTime) <= 86400000]]]" /f:xml
```

```
REM von einem entfernten Rechner abfragen
wevtutil qe Microsoft-Windows-NTLM/Operational /r:CL-LAGER-07 ^
/q:"*[System[(EventID=4025)]]" /c:10 /rd:true /f:text
```

Get-WinEvent: Objekte statt Text

Sobald du zählen, gruppieren oder exportieren willst, ist Get-WinEvent das bessere Werkzeug. Mit FilterHashtable filtert bereits das Ereignisprotokoll, nicht erst PowerShell, das spart bei großen Protokollen spürbar Zeit.

```
# Überblick: wie viele 4024 und 4025 in den letzten 14 Tagen?
Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational';
    Id=4024,4025; StartTime=(Get-Date).AddDays(-14) } -ErrorAction SilentlyContinue |
    Group-Object Id | Select-Object Name, Count

# Ein Ereignis vollständig ansehen
Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational'; Id=4025 } `
    -MaxEvents 1 | Format-List TimeCreated, MachineName, Id, LevelDisplayName, Message
```

Für die Gruppierung nach Ziel oder Prozess brauchst du die einzelnen Datenfelder. Statt Feldnamen zu raten, liest das folgende Skript sie aus dem XML jedes Ereignisses aus und baut daraus Objekte. Mit dem ersten Aufruf siehst du, welche Namen es auf deinen Systemen gibt; mit dem zweiten gruppierst du nach dem Feld, das dich interessiert.

```
function Get-NtlmV1SsoEvent {
    param([string]$ComputerName = $env:COMPUTERNAME, [int]$Days = 14)
    Get-WinEvent -ComputerName $ComputerName -ErrorAction SilentlyContinue -FilterHashtable @{
        LogName='Microsoft-Windows-NTLM/Operational'; Id=4024,4025
        StartTime=(Get-Date).AddDays(-$Days) } |
    ForEach-Object {
        $o = [ordered]@{ Zeit=$_ .TimeCreated; Rechner=$_ .MachineName; Id=$_ .Id }
        foreach ($f in ([xml]$_ .ToXml()).Event.EventData.Data) { $o[$f.Name] = $f.'#text' }
        [pscustomobject]$o
    }
}

# 1. Welche Felder gibt es? Einmal ansehen:
Get-NtlmV1SsoEvent | Select-Object -First 1 | Format-List *

# 2. Gruppieren, Feldname aus Schritt 1 einsetzen:
$feld = '<Feldname für den Zielservers>'
Get-NtlmV1SsoEvent | Group-Object Id, $feld | Sort-Object Count -Descending |
```

Select-Object Count, Name -First 20

WICHTIG · 4024 schweigt seit dem 13.10.2026 meistens

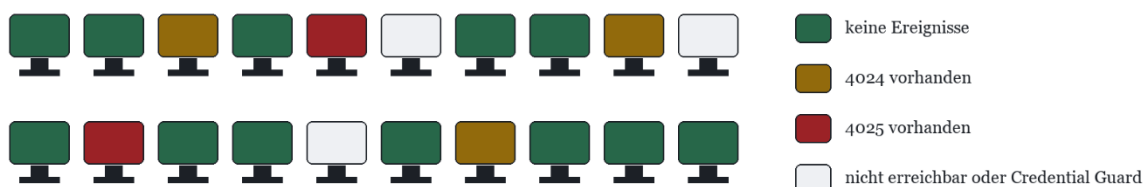
Ein 4024 entsteht nur im Überwachungsmodus, also bei BlockNtlmv1SSO = 0 oder auf Rechnern, die das Oktober-Update noch nicht haben. Wenn deine Rechner aktuell sind und niemand den Wert gesetzt hat, siehst du nur noch 4025. Eine Abfrage, die bloß nach 4024 sucht, liefert dann ein beruhigendes Nichts, und das ist die gefährlichste Art von Nichts.

Der Haken mit dem einzelnen Client

Alles bis hierhin funktioniert hervorragend, solange du genau weißt, welchen Rechner du fragen musst. In der Realität kennst du den einen, der sich beschwert hat. Die zwanzig anderen mit demselben WLAN-Profil haben sich noch nicht gemeldet, weil ihre Benutzer im Urlaub sind, im Homeoffice per Kabel arbeiten oder das Problem stillschweigend mit dem Hotspot ihres Diensthandys gelöst haben. Herzlichen Glückwunsch, du hast gerade eine Schatten-IT entdeckt.

Warum ein einzelner Client nichts beweist

Sparfuchs & Partner Steuerberatungs GmbH: 20 Clients, und jeder schreibt nur für sich



Du schaust auf einen grünen Rechner und denkst: alles gut.

Nur lokal

4024 und 4025 entstehen auf dem Client, nicht auf dem Domain Controller

Nur bei Bedarf

Ereignisse kommen nur, wenn SSO tatsächlich versucht wird

Nur begrenzt

Das Protokoll rotiert; alte Spuren werden überschrieben

Skizze: Verteilung frei erfunden, Prinzip leider nicht

- **Die Ereignisse sind lokal.** 4024 und 4025 entstehen auf dem Client, kein Domain Controller sammelt sie für dich ein.
- **Sie entstehen nur bei Bedarf.** Ein Notebook, das diese Woche nicht im Firmen-WLAN war, schreibt diese Woche kein Ereignis, das Problem ist trotzdem da.
- **Das Protokoll rotiert.** Bei kleiner Protokollgröße sind die Spuren nach ein paar Tagen überschrieben, vor allem auf Rechnern mit viel NTLM-Verkehr.
- **Remote-Abfragen scheitern leise.** Was nicht erreichbar ist, taucht im Ergebnis nicht auf, und eine fehlende Zeile sieht genauso aus wie ein sauberer Rechner.

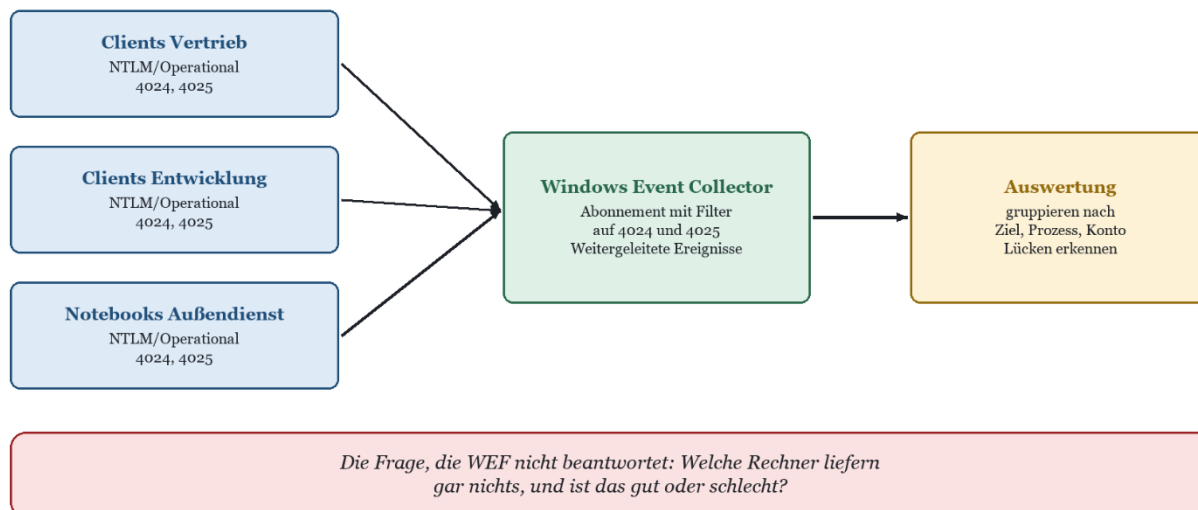
Zentral sammeln statt Rechner abklappern

Die Antwort auf die Frage „Welche Rechner noch?“ steht nicht auf einem Rechner, sondern nur in der Summe aller Rechner. Der Bordmittel-Weg dorthin heißt Windows Event Forwarding: Die Clients leiten ausgewählte Ereignisse per Abonnement an einen Windows Event Collector weiter,

der sie im Protokoll „Weitergeleitete Ereignisse“ ablegt. Für 4024 und 4025 reicht ein Abonnement auf Microsoft-Windows-NTLM/Operational mit dem bekannten XPath-Filter.

Zentral sammeln: vom Einzelprotokoll zur Gesamtsicht

Trendforge Digital GmbH, trendforge.local: Clients liefern, ein Collector empfängt



Skizze: Architekturprinzip Windows Event Forwarding; Namen frei erfunden

```

<QueryList>
  <Query Id="0" Path="Microsoft-Windows-NTLM/Operational">
    <Select Path="Microsoft-Windows-NTLM/Operational">
      *[System[(EventID=4024 or EventID=4025)]]
    </Select>
  </Query>
</QueryList>
    
```

Wie du Collector, Abonnement, Gruppenrichtlinie und Berechtigungen sauber aufsetzt, beschreibt der Beitrag [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#) Schritt für Schritt. Wenn du ohnehin dabei bist, nimm die Ereignisse 4020 bis 4023 des erweiterten Audittings gleich mit in den Filter, dann siehst du mit demselben Aufwand auch die allgemeine NTLM-Nutzung. Die passende Überwachungsrichtlinie legt dir das [NTLM-Audit-GPO-Skript](#) an, statt dass du sie von Hand zusammenklickst.

Auf dem Collector auswerten

Auf dem Collector landen die Ereignisse mit ihrem ursprünglichen Rechnernamen. Damit funktioniert dieselbe Auswertung wie oben, nur eben über alle Rechner auf einmal:

```

Get-WinEvent -FilterHashtable @{ LogName='ForwardedEvents'; Id=4024,4025;
  StartTime=(Get-Date).AddDays(-30) } |
  Group-Object MachineName, Id | Sort-Object Count -Descending |
  Select-Object Count, Name | Export-Csv .\ntlmv1-sso-rechner.csv -NoTypeInformation -Encoding
UTF8
    
```

WARNUNG · WEF zeigt dir, wer etwas schickt, nicht wer schweigt

Event Forwarding liefert, was ankommt. Ein Rechner, dessen Abonnement nie aktiv wurde, weil der Netzwerkdienst keinen Zugriff auf das Protokoll hat oder die Richtlinie nicht greift, erscheint einfach nicht. Ohne Abgleich gegen die Liste der aktiven Computerkonten im Active Directory hältst du Lücken für Sauberkeit. Prüfe auf dem Collector regelmäßig mit `wecutil gr <Abonnement>`, welche Quellen aktiv sind, und vergleiche das mit dem Bestand.

Wo Bordmittel mühsam werden

Bis hierhin bist du ohne einen Euro Lizenzkosten gekommen, und für eine Umgebung mit fünfzig Rechnern und einem WLAN-Profil ist das auch völlig in Ordnung. Ab einer gewissen Größe kippt das Verhältnis aber. Dann hast du Tausende Ereignisse im Collector, Hunderte Rechner im Bestand, einige stille Geräte ohne Abonnement und eine CSV-Datei, die zwar zählt, aber nicht erklärt. Die eigentliche Arbeit beginnt erst danach: herausfinden, welche fünf Ursachen hinter den Tausenden Einträgen stecken, und welche Rechner du nicht siehst.

Aufgabe	Bordmittel	Aufwand bei 500 Rechnern
Ereignis lesen	Ereignisanzeige	gering
Ereignisse auf einem Rechner filtern	wevtutil, Get-WinEvent	gering
Ereignisse zentral sammeln	Windows Event Forwarding	einmalig mittel, dann gering
Stille Rechner erkennen	Abgleich mit Active Directory, eigenes Skript	hoch
Nach Ursache gruppieren	XML auslesen, Group-Object, Excel	hoch
Ergebnis für die IT-Leitung aufbereiten	Handarbeit in Word und Excel	hoch, jedes Mal

Genau an dieser Stelle setzt der [NTLM Diagnostiker](#) an. Er sammelt die NTLM-Ereignisse aus deinen Quellen, gruppiert sie automatisch und arbeitet dabei ausschließlich lesend: Er ändert keinen Registrierungswert, keine Richtlinie und kein Konto. Was du mit den Ergebnissen machst, entscheidest weiterhin du.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Von 4025-Rauschen zur Hitliste

Ereignisquellen: Der Diagnostiker liest die Ereignisse wahlweise direkt vom Domain Controller, von einem vorhandenen Windows Event Collector oder per Direktabfrage der Rechner. Wenn du Event Forwarding schon eingerichtet hast, ist die Arbeit also nicht verloren.

Sammeln und gruppieren: Die NTLMv1-Hitliste fasst die Quellen nach Häufigkeit zusammen, die Kommunikationsmatrix und die Konten-Sicht zeigen, welches Konto von welchem Rechner zu welchem Ziel spricht. Die Ursachen-Engine prüft dazu SPN und DNS, Sicherheitsflaggen markieren auffällige Muster.

Lücken sehen: Der Abdeckungsmonitor und die OS-Landkarte zeigen, welche Rechner liefern, welche schweigen und auf welchen Windows-Versionen 4024 und 4025 überhaupt entstehen können. Die Readiness-Ampel fasst das je Maschine zusammen; die Abschalt-Simulation zeigt, was eine Erzwingung treffen würde.

Ergebnisse: Word-Bericht für die IT-Leitung, Excel- oder CSV-Export für das Ticket, Wireshark-Import für Geräte, die gar kein Ereignisprotokoll haben. Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund; die Vollversion kannst du 7 Tage testen, lizenziert wird pro aktivem Computerkonto. Ein Ausnahmelisten- und Skript-Generator, ein Phasenplan und ein Verlauf sind geplant, aber noch nicht enthalten.

› [NTLM Diagnostiker](#)

AUS DER PRAXIS · Sparfuchs & Partner: der Abgleich, der den Unterschied machte

In der Kanzlei lieferte Event Forwarding nach einer Woche 4025 von 14 Rechnern, alle mit demselben VPN-Gateway als Ziel. Der Abgleich mit dem Bestand ergab zusätzlich neun Notebooks,

die gar nichts geliefert hatten. Sechs davon waren in der Woche schlicht nicht im Netz, drei hatten ein defektes Abonnement. Ohne diesen Abgleich wäre die Umstellung des VPN-Profiles bei 14 Rechnern als erledigt markiert worden, und der Montag nach den Herbstferien hätte drei sehr schlecht gelaunte Steuerberaterinnen und Steuerberater produziert.

Wenn du die Auswertung nicht allein stemmen willst, unterstützen wir dich in der [Beratung zur NTLM-Ablösung](#) von der ersten Abfrage bis zur umgestellten Quelle. Und wenn dein Team die Ereignisse künftig selbst lesen und bewerten soll, ist die [Schulung zum NTLM Diagnostiker](#) der kürzere Weg. Einen Vergleich der Wege, von Bordmitteln über Skripte bis zum Diagnostiker, findest du in [NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker](#).

FAQ zu Ereignis 4024 und 4025

Was bedeutet Ereignis 4025 im NTLM-Protokoll?

Windows hat einen Versuch blockiert, NTLMv1-abgeleitete Anmeldedaten für Single Sign-on zu verwenden. Ursache ist der Erzwingungsmodus von BlockNtlmv1SSO, der seit dem Update vom 13.10.2026 auch dann gilt, wenn der Wert nicht gesetzt ist. Für den Anwender heißt das: Die automatische Anmeldung, oft im WLAN oder VPN, funktioniert nicht mehr.

Und was ist Ereignis 4024?

Dieselbe Situation im Überwachungsmodus: Die Anfrage wurde erlaubt, aber als Warnung protokolliert. Ein 4024 ist also die Ankündigung eines 4025, sobald der Rechner in die Erzwingung wechselt.

Warum finde ich die Ereignisse nicht im Sicherheitsprotokoll?

Weil sie dort nicht stehen. Beide Ereignisse landen in Microsoft-Windows-NTLM/Operational, in der Ereignisanzeige unter Anwendungs- und Dienstprotokolle, Microsoft, Windows, NTLM.

Warum gibt es auf meinem Domain Controller keine 4025?

Weil die Ereignisse auf dem Rechner entstehen, der die Anmeldedaten weitergeben will, also auf dem Client. Für den Überblick musst du die Clients abfragen oder ihre Ereignisse zentral sammeln.

Mein Windows-10-Rechner zeigt keine 4024 oder 4025. Ist er sauber?

Nicht unbedingt. Die Ereignisse gibt es nur auf Windows 11 ab 24H2 und Windows Server 2025. Für ältere Systeme brauchst du die klassische Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8004; einen Überblick über alle Wege gibt [NTLM-Nutzung ermitteln: der komplette Leitfaden](#).

Kann ich 4025 einfach abstellen?

Technisch ja, mit BlockNtlmv1SSO = 0. Dann bekommst du statt 4025 wieder 4024 und die Anmeldung funktioniert, allerdings ohne Schutz. Microsoft beschreibt das als befristete Ausnahme für kritische Abhängigkeiten. Wie du so eine Ausnahme gezielt und mit Ablaufdatum setzt, steht in [BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme](#).

Darf ich die Ereignisse zentral sammeln, ohne den Betriebsrat zu fragen?

Die Ereignisse enthalten Benutzernamen und Zeitstempel, damit sind es personenbezogene Daten. Was du dabei beachten solltest, beschreibt [NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst](#).

Wo steht das bei Microsoft?

Im Supportartikel [Manage NTLMv1 changes and prevent network authentication issues in Windows](#). Dort findest du Ereignisse, Registrierungswert, betroffene Windows-Versionen und den Zeitplan.

Fazit: Ein Ereignis ist ein Hinweis, hundert sind ein Befund

4024 und 4025 sind zwei der ehrlichsten Ereignisse, die Windows je geschrieben hat. Sie sagen dir, welcher Prozess auf welchem Rechner wessen Anmeldedaten an welches Ziel schicken wollte, und ob Windows das zugelassen hat. Mit wevtutil und Get-WinEvent liest du sie auf einem Rechner in Minuten. Der Haken liegt nicht im Lesen, sondern im Zählen: Die Ereignisse entstehen verteilt, nur bei Bedarf, und sie verschwinden, wenn das Protokoll rotiert.

Wer die Lage wirklich kennen will, sammelt zentral, gleicht gegen den Bestand ab und gruppiert nach Ursache. Das geht mit Event Forwarding und etwas Skriptarbeit, oder eben mit einem Werkzeug, das genau dafür gebaut ist. Wichtig ist nur, dass du nicht beim ersten roten Eintrag aufhörst. Der erste ist selten der letzte. Er ist nur der, der als Erster Krach gemacht hat.

WEITERLESEN • Weiter in dieser Serie

- › [NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht](#)
- › [BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme](#)
- › [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#)
- › [Erweitertes NTLM-Auditing einschalten: Schritt für Schritt](#)
- › [Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen](#)
- › [NTLM-Nutzung ermitteln: der komplette Leitfaden](#)
- › [NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll](#)
- › [NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet](#)