

NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht

NTLMv1 blockiert: der Montag nach dem Patchday

Das WLAN fragt nach dem Passwort, das Helpdesk-Telefon klingelt, und irgendwo schreibt Windows still Ereignis 4025.

13.10.2026

Update installiert,
Standard: Erzwingung

Symptom

Anmeldefenster
statt Single Sign-on

Beweis

Ereignis 4025 in
NTLM/Operational

Ausweg

Quelle finden,
sauber umstellen

Blockiert wird Single Sign-on, nicht die Anmeldung an sich

Wer das Passwort von Hand eintippt, kommt weiterhin rein. Das ist ein Trost, aber kein Betriebskonzept.

Skizze: vom Update zum Ausweg in vier Schritten

WISSEN

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

› [NTLM Diagnostiker](#)

BERATUNG

NTLMv1-Soforthilfe: Quelle finden, Notlösung begrenzen, sauber umstellen.

› [Beratung zur NTLM-Ablösung](#)

SCHULUNG

Ereignisse lesen, Ursachen finden, Ausnahmen pflegen: praxisnah für dein Team.

› [Schulung zum NTLM Diagnostiker](#)

Es gibt diese besonderen Montage. Am Wochenende sind die Oktober-Updates durchgelaufen, die Wartungsfenster waren ruhig, die Überwachung grün. Und dann, um 7:12 Uhr, ruft die Station 3 an: Das WLAN will plötzlich ein Passwort. Um 7:20 Uhr der Außendienst: Das VPN fragt nach Benutzername und Kennwort, das hat es noch nie getan. Um 7:45 Uhr meldet die Buchhaltung, der Scanner im Flur scanne nicht mehr in den Ordner, und das sei bestimmt auch das Update. Ist es vielleicht. Vielleicht aber auch nicht.

Seit dem Windows-Update vom 13. Oktober 2026 blockieren Windows 11 ab Version 24H2 und Windows Server 2025 standardmäßig Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten. Microsoft hatte das über ein Jahr lang angekündigt und in dieser Zeit fleißig Warnungen protokolliert, nämlich Ereignis 4024. Gelesen hat sie kaum jemand. Jetzt steht im selben Protokoll Ereignis 4025, und dieses Mal ist es keine Warnung mehr, sondern eine Sperre.

In diesem Beitrag sortieren wir das Chaos. Du erfährst, was genau gesperrt wird und was nicht, welche Symptome wirklich auf die NTLMv1-Sperre zurückgehen und welche nur zufällig zur selben Zeit auftauchen, warum der schnelle Griff in die Registrierung eine Notlösung bleibt und wie du die Quelle findest: mit Bordmitteln, mit Geduld und, wenn die Geduld endlich ist, mit Werkzeugunterstützung.

FAKTEN • Die NTLMv1-Sperre in 30 Sekunden

Seit 13.10.2026: Fehlt der Registrierungswert BlockNtlmv1SSO, gilt Erzwingung statt Überwachung. Das Update legt den Wert nicht an und ändert ihn nicht.

Betroffen: Windows 11 24H2, 25H2, 26H1 und 26H2 sowie Windows Server 2025, jeweils nur ohne aktiviertes Credential Guard.

Gesperrt: Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten, typischerweise MS-CHAPv2 in WLAN-, LAN- und VPN-Anmeldungen (PEAP-MSCHAPv2, EAP-MSCHAPv2).

Weiter erlaubt: manuell eingegebene Anmeldedaten.

Protokoll: Microsoft-Windows-NTLM/Operational, Ereignis 4024 (Warnung, Überwachung) und 4025 (Fehler, Sperre). Ein Neustart ist nach Änderung des Werts nicht nötig.

Die Symptome: Was seit dem Oktober-Update klemmt

Die NTLMv1-Sperre ist heimtückisch, weil sie nicht krachend ausfällt, sondern höflich nachfragt. Statt einer Fehlermeldung erscheint ein Anmeldedialog. Viele Anwenderinnen und Anwender tippen brav ihr Kennwort ein, es funktioniert, und das Ticket lautet am Ende „WLAN will manchmal Passwort“. Genau so bleiben solche Probleme monatelang unentdeckt, bis jemand das Kennwort ändert und alle Geräte gleichzeitig nachfragen.

Anmeldeaufforderungen statt Single Sign-on

Das klassische Bild: Ein Notebook verbindet sich morgens mit dem Firmen-WLAN oder baut das VPN auf. Bisher hat Windows dafür automatisch die Anmeldedaten des angemeldeten Benutzers verwendet. Wenn die Netzwerkanmeldung per PEAP-MSCHAPv2 oder EAP-MSCHAPv2 läuft, braucht sie dafür NTLMv1-abgeleitete Anmeldedaten, also genau das, was seit dem 13. Oktober gesperrt ist. Ergebnis: ein Dialog, der nach Benutzername und Kennwort fragt. Wer tippt, kommt rein. Wer nicht tippt, steht ohne Netz da, und das betrifft vor allem Geräte, an denen niemand sitzt, der tippen könnte.

Das ist der Fall, den Microsoft ausdrücklich nennt, und er ist in der Praxis der häufigste. Er betrifft die Clients selbst, nicht die Server. Der RADIUS-Server, bei Windows meist der Netzwerkrichtlinienserver, bekommt einfach keine Anfrage mehr oder eine, die nach manueller Eingabe wieder funktioniert.

AUS DER PRAXIS · Musterwerk GmbH, Montag nach dem Patchday

In der Fertigung der Musterwerk GmbH hängen zwölf Bedienterminals mit Windows 11 24H2 im Produktions-WLAN. Die Anmeldung läuft seit Jahren per PEAP-MSCHAPv2 mit den Daten des Schichtkontos. Am Montag nach dem Update stehen alle zwölf mit einem Anmeldedialog da, den niemand beantworten kann, weil das Kennwort des Schichtkontos nur die IT kennt.

Auf jedem Terminal steht im Protokoll Microsoft-Windows-NTLM/Operational ein Ereignis 4025.

Die Notebooks in der Verwaltung sind nicht betroffen: Auf ihnen ist Credential Guard aktiv, und dort hatte NTLMv1-abgeleitetes Single Sign-on ohnehin nie eine Chance.

Scanner, Multifunktionsgeräte und NAS

Jetzt wird es unbequem, denn hier muss man ehrlich sein: Ein Multifunktionsgerät, das per „Scan to Folder“ in eine Freigabe schreibt, benutzt kein Single Sign-on. Es meldet sich mit einem fest hinterlegten Konto am Dateiserver an. BlockNtlmv1SSO wirkt auf dem Windows-Rechner, der sich anmelden will, nicht auf dem Server, der eine Anmeldung annimmt. Ein Scanner, der NTLMv1 spricht, scheitert deshalb nicht an dieser Sperre, sondern an etwas anderem: an einem Dateiserver oder Domain Controller, der NTLMv1 per LAN-Manager-Authentifizierungsebene ablehnt, an einer SMB-Härtung oder an einer Restrict-NTLM-Richtlinie.

Warum das trotzdem in diesem Beitrag steht? Weil diese Störungen in denselben Wochen auftauchen. Viele Häuser haben im Zuge des Oktober-Updates gleich noch die Gelegenheit genutzt, NTLMv1 per Gruppenrichtlinie zu verbieten, Server-Härtungen nachzuziehen oder SMB-

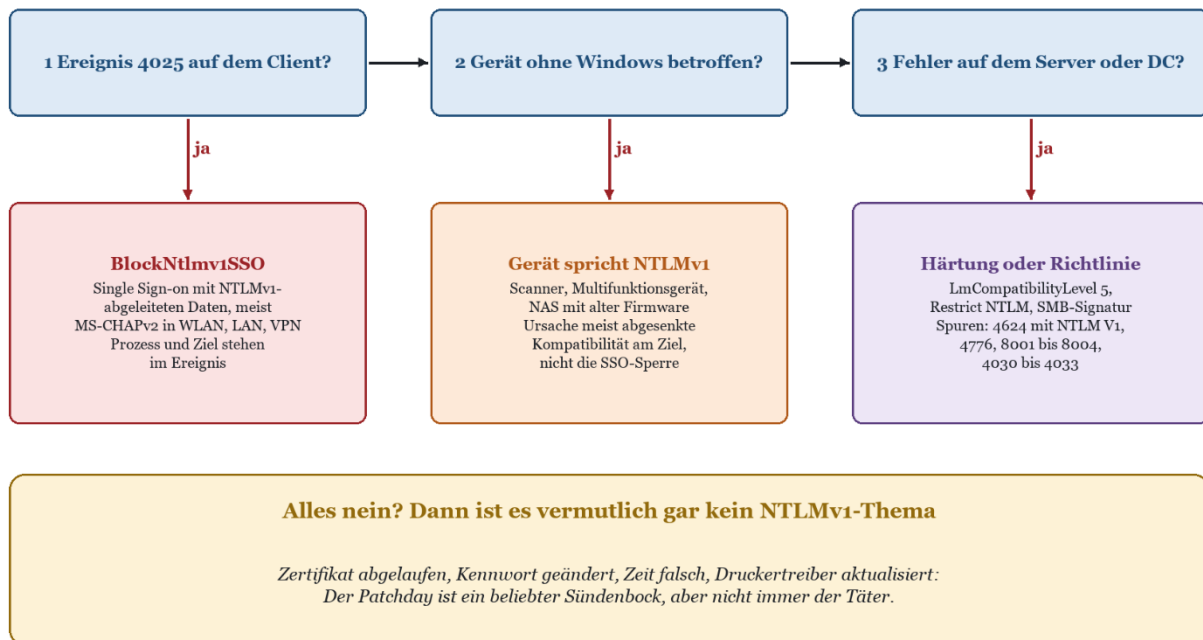
Einstellungen zu verschärfen. Und dann landet alles im selben Ticket. Wenn du ein Gerät ohne Windows im Verdacht hast, lohnt der Blick in [NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll](#).

Altanwendungen und Dienste ohne Benutzer

Die dritte Gruppe sind Anwendungen, die im Hintergrund eine Anmeldung aufbauen und dabei auf NTLMv1-abgeleitete Anmeldedaten angewiesen sind. Das ist seltener als der WLAN-Fall, aber unangenehmer, weil hier kein Dialog erscheint, den jemand ausfüllen könnte. Die Anwendung meldet nur „Zugriff verweigert“ oder, im schlechtesten Fall, gar nichts und arbeitet einfach nicht mehr. In Ereignis 4025 steht dann der Clientprozess, und damit hast du wenigstens einen Namen, den du beim Hersteller anbringen kannst. Wie du das Gespräch dort führst, ohne mit einem „Das unterstützen wir nicht“ abgespeist zu werden, steht in [Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen](#).

Triage: Ist es wirklich die NTLMv1-Sperre?

Nicht jede Störung seit dem Patchday hat dieselbe Ursache. Drei Fragen sortieren die meisten Fälle



Skizze: Triage-Schema; stark vereinfacht, ohne Anspruch auf Vollständigkeit

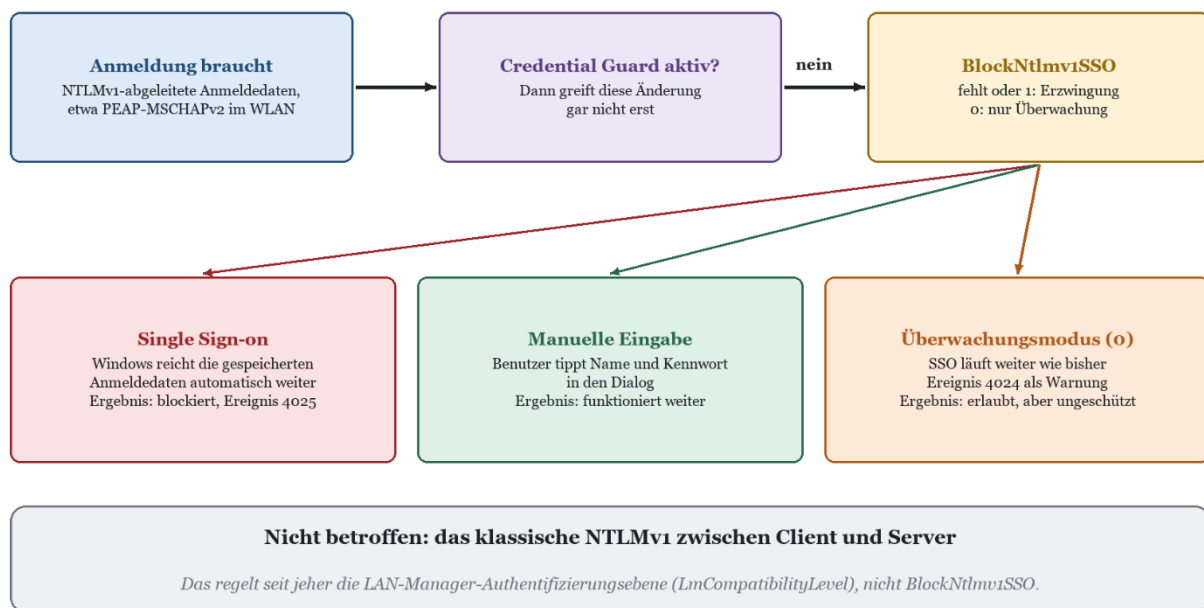
Symptom	Wahrscheinliche Ursache	Erster Prüfpunkt
WLAN, LAN oder VPN fragt nach Kennwort	BlockNtlmv1SSO mit MS-CHAPv2	Ereignis 4025 auf dem Client
Terminal oder Kiosk ohne Netz nach Neustart	BlockNtlmv1SSO, niemand gibt Kennwort ein	Ereignis 4025, Profil der Netzwerkverbindung
Scanner kann nicht mehr in Freigabe schreiben	NTLMv1 am Ziel abgelehnt, SMB-Härtung	Sicherheitsprotokoll des Dateiservers, Firmware des Geräts
Fachanwendung meldet Zugriff verweigert	NTLMv1-Pfad in der Anwendung oder Restrict NTLM	Ereignis 4025 mit Prozessname, sonst 4020/4021 und 8001
Nur einzelne Notebooks betroffen	Unterschiedlicher Credential-Guard-Status	Credential Guard in msinfo32 vergleichen
Alles betroffen, auch ältere Windows-Versionen	Vermutlich keine NTLMv1-Sperre	Zertifikate, Kennwortänderungen, Zeit, RADIUS-Protokoll

Was genau blockiert wird und was nicht

Der Name des Registrierungswerts sagt es eigentlich schon, man muss ihn nur langsam lesen: Block NTLMv1 SSO. Gesperrt wird nicht NTLMv1 im Allgemeinen, sondern die Verwendung NTLMv1-abgeleiteter Anmeldedaten für Single Sign-on. Single Sign-on heißt: Windows nimmt die Anmeldedaten, die bei der Anmeldung am Rechner im Speicher gelandet sind, und reicht sie automatisch weiter. Genau diese automatische Weitergabe ist der Teil, den Angreifer seit Jahren lieben, denn NTLMv1-Antworten lassen sich mit vertretbarem Aufwand knacken oder weiterverwenden.

Was BlockNtlmv1SSO tatsächlich sperrt

Windows 11 ab 24H2 und Windows Server 2025 mit dem Update vom 13.10.2026, Credential Guard aus



Skizze: vereinfachte Wirkung nach Microsoft KB5066470

Der Registrierungswert und seine drei Zustände

Gesteuert wird alles über den DWORD-Wert BlockNtlmv1SSO unter HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_o. Entscheidend ist dabei weniger, was drinsteht, sondern ob überhaupt etwas drinsteht. Denn das Oktober-Update hat nicht den Wert geändert, sondern das Verhalten bei fehlendem Wert.

Zustand von BlockNtlmv1SSO	Verhalten	Ereignis
Nicht vorhanden, vor dem 13.10.2026	Überwachung: SSO erlaubt, Warnung	4024
Nicht vorhanden, ab dem 13.10.2026	Erzwingung: SSO blockiert	4025
0	Überwachung: SSO erlaubt, Warnung	4024
1	Erzwingung: SSO blockiert	4025
Beliebig, Credential Guard aktiv	Änderung greift nicht; Credential Guard schützt ohnehin	keines

Alle Einzelheiten zum Wert, zur Verteilung per Gruppenrichtlinie und zum Umgang mit Ausnahmen findest du in [BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme](#).

Microsoft selbst beschreibt die Änderung im Artikel [Microsoft-Support: Änderungen an NTLMv1 in Windows 11 24H2 und Windows Server 2025 \(KB5066470\)](#).

Manuell eingegebene Anmeldedaten gehen weiter

Das ist die gute Nachricht, und sie erklärt, warum viele Umgebungen die Sperre erst Tage später bemerken. Wer das Kennwort im Dialog eintippt, wird weiterhin angemeldet. Für einen Arbeitsplatz mit einem Menschen davor ist das lästig, aber überlebbbar. Für ein Bedienterminal, eine Anzeigetafel oder einen Laborrechner, an dem morgens niemand sitzt, ist es ein Ausfall.

WARNUNG · Kennwort eintippen ist kein Workaround

Wenn das Helpdesk jetzt anfängt, Kennwörter von Funktionskonten an Stationen oder in der Fertigung herauszugeben, damit jemand sie in den WLAN-Dialog tippt, hast du ein neues Problem geschaffen: gemeinsam genutzte Kennwörter, die bald auf einem Zettel am Monitor kleben. Lieber ein paar Tage gezielte Ausnahme als ein Jahr Zettelwirtschaft.

Credential Guard: Wer ihn hat, hat das Problem nicht

Die Änderung gilt nur auf Systemen ohne aktiviertes Credential Guard. Wo Credential Guard läuft, gab es NTLMv1-abgeleitetes Single Sign-on schon vorher nicht. Das erklärt das häufige Muster, dass dieselbe WLAN-Konfiguration auf einem Teil der Geräte seit Jahren nach dem Kennwort fragt und auf dem anderen Teil erst seit Oktober. Microsoft empfiehlt Credential Guard ausdrücklich dort, wo die Voraussetzungen erfüllt sind, weil er weit mehr schützt als nur diesen einen Weg. Die MS-CHAPv2-Abhängigkeit löst er allerdings nicht, er macht sie nur sichtbar.

Was nicht unter BlockNtlmv1SSO fällt

Ältere Windows-Versionen wie Windows 10 oder Windows Server 2022 sind von dieser Sperre nicht betroffen. Ebenso wenig die klassische Frage, ob ein Client gegenüber einem Server NTLMv1 oder NTLMv2 spricht: Die regelt seit jeher die Richtlinie „Netzwerksicherheit: LAN Manager-Authentifizierungsebene“, technisch LmCompatibilityLevel. Und die allgemeine NTLM-Abschaltung, die Microsoft für die nächste Windows-Server-Version angekündigt hat, ist noch einmal ein eigenes Thema. Wie die Etappen zusammenhängen, erklärt [NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet](#).

Warum „Registrierungswert zurück auf Überwachung“ eine Notlösung ist

Natürlich gibt es den schnellen Weg, und natürlich kennt ihn inzwischen jeder: BlockNtlmv1SSO auf 0 setzen, per Gruppenrichtlinie an alle Clients verteilen, fertig. Kein Neustart, kein Anmeldedialog, das Telefon wird ruhig. Microsoft beschreibt diesen Weg sogar selbst, allerdings mit dem Zusatz, dass er als begrenzte, vorübergehende Ausnahme gedacht ist und den Schutz senkt.

Die Ausweg-Leiter: von der Notlösung zur Lösung

Je weiter oben, desto weniger Aufwand heute und desto mehr Ärger beim nächsten Audit



Skizze: Bewertung der Auswege; je weiter unten, desto dauerhafter die Lösung

Das Problem an der Notlösung ist nicht, dass sie nicht funktioniert. Das Problem ist, dass sie zu gut funktioniert. Sobald das Telefon ruhig ist, verschwindet das Thema von der Liste. Der Wert bleibt auf o, und in zwei Jahren weiß niemand mehr, warum er dort steht. Bis dahin bleibt genau der Angriffsweg offen, den Microsoft schließen wollte: NTLMv1-Antworten, die sich mitschneiden und mit überschaubarem Rechenaufwand auswerten lassen.

Weg	Aufwand heute	Wirkung	Bewertung
BlockNtlmv1SSO = o für alle Clients	Minuten	Alle Geräte wieder ungeschützt	Nur als Erste Hilfe für Stunden, nicht Wochen
BlockNtlmv1SSO = o nur für betroffene Geräte	Stunden	Schutz bleibt dort, wo er nicht stört	Vertretbar mit Ablaufdatum und Verantwortlichem
Credential Guard einschalten	Tage bis Wochen	Breiter Schutz gegen Diebstahl von Anmeldedaten	Empfehlenswert, ersetzt aber nicht die Umstellung
WLAN, LAN, VPN auf Zertifikate umstellen	Wochen	Keine NTLMv1-Abhängigkeit mehr	Die eigentliche Lösung
Altanwendung beim Hersteller klären	Offen	Ursache beseitigt	Ohne Alternative bleibt nur die gezielte Ausnahme

WICHTIG · Wenn schon Ausnahme, dann richtig

Setze den Wert nicht domänenweit, sondern nur per gefilterter Gruppenrichtlinie für eine benannte Gerätegruppe. Gib jeder Ausnahme ein Ablaufdatum, einen Verantwortlichen und ein Ticket. Und lass die Überwachung laufen: Im Modus o schreibt Windows weiter Ereignis 4024, du siehst also jeden Tag, ob die Ausnahme noch gebraucht wird.

Wenn bei dir gerade alles gleichzeitig brennt und du jemanden brauchst, der die Notlösung sauber eingrenzt und parallel die eigentliche Ursache abstellt: Genau dafür gibt es unsere NTLMv1-

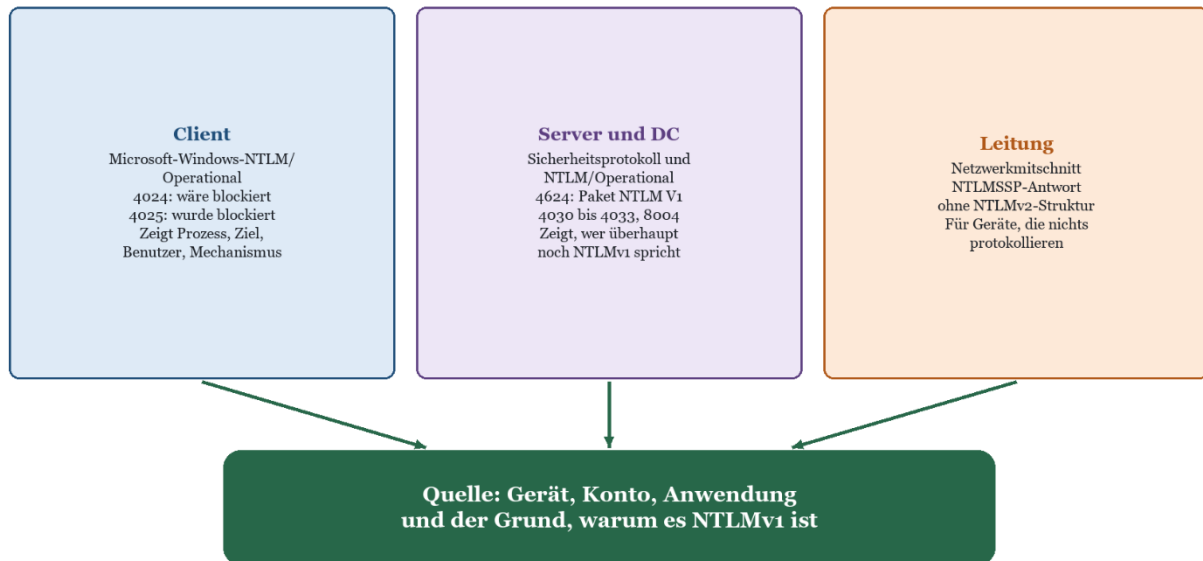
Soforthilfe im Rahmen der [Beratung zur NTLM-Ablösung](#). Wir machen das nicht zum ersten Mal, und wir sind bei Notlösungen ziemlich pingelig, was das Ablaufdatum angeht.

Die Quellen finden: mit Bordmitteln

Bevor du irgendetwas umstellst, brauchst du eine Liste: Welche Geräte, welche Benutzer, welche Prozesse, welches Ziel. Dafür gibt es drei Perspektiven, die sich ergänzen. Der Client weiß, was gesperrt wurde. Server und Domain Controller wissen, wer überhaupt noch NTLMv1 spricht. Und die Leitung weiß Bescheid über Geräte, die gar nichts protokollieren.

Drei Wege zur NTLMv1-Quelle

musterwerk.local: Jede Perspektive sieht etwas anderes. Erst zusammen ergeben sie das Bild



Skizze: Perspektiven der Ursachensuche; Namen frei erfunden

Ereignis 4024 und 4025 auf den Clients

Beide Ereignisse stehen im Protokoll Microsoft-Windows-NTLM/Operational mit der Quelle NTLM. 4024 ist die Warnung aus dem Überwachungsmodus: Diese Anmeldung wäre blockiert worden, wurde aber durchgelassen. 4025 ist der Fehler aus dem Erzwingungsmodus: Diese Anmeldung wurde blockiert. Beide nennen den Zielserver, den Benutzer, die Domäne, Angaben zum aufrufenden Prozess und die OID des Mechanismus. Damit weißt du in der Regel sofort, ob es das WLAN-Profil, der VPN-Client oder eine Anwendung war.

```
# Die letzten blockierten NTLMv1-SSO-Versuche (4025) im Klartext
wevtutil qe Microsoft-Windows-NTLM/Operational /q:"*[System[(EventID=4025)]]" /c:20 /rd:true /f:text

# Warnungen und Sperren der letzten 14 Tage zählen
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

# Ist BlockNtlmv1SSO gesetzt? Kein Wert bedeutet seit 13.10.2026: Erzwingung
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0' -Name BlockNtlmv1SSO -ErrorAction SilentlyContinue

# Mehrere Clients abfragen (WinRM erforderlich)
Invoke-Command -ComputerName PC-0815, PC-0816 -ScriptBlock {
    Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational'; Id=4025 } -MaxEvents 5 -ErrorAction SilentlyContinue } | Select-Object PSComputerName,
```

TimeCreated, Message

Wie du die Meldungstexte im Detail liest und welche Angaben dich zur Ursache führen, zeigt [Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen](#).

TIPP · Die Warnungen von gestern sind die Sperren von heute

Das Protokoll Microsoft-Windows-NTLM/Operational ist ab Werk nicht besonders groß. Wenn du noch alte 4024-Ereignisse aus der Zeit vor dem 13. Oktober findest, sind sie Gold wert: Sie zeigen dir, was seitdem blockiert wird, auch auf Geräten, die gerade niemand benutzt. Sichere sie, bevor sie überschrieben werden, und vergrößere das Protokoll per Gruppenrichtlinie.

LmCompatibilityLevel und die Spuren auf Servern und DCs

Die Clientereignisse zeigen nur die SSO-Sperre. Für das größere Bild willst du wissen, wer in deiner Domäne überhaupt noch NTLMv1 spricht. Zwei Stellschrauben gehören dazu. Auf den Clients bestimmt LmCompatibilityLevel, was sie senden; auf den Domain Controllern, was sie annehmen. Ab Wert 3, der auf aktuellen Windows-Versionen als Standard gilt, senden Clients nur NTLMv2. Erst Wert 5 lässt den Domain Controller LM und NTLMv1 ablehnen. Wer dort noch 1 oder 2 findet, sollte wissen, warum, und es aufschreiben.

Wert	Client sendet	DC nimmt an	Einordnung
0 bis 2	LM und NTLMv1 möglich	LM, NTLMv1, NTLMv2	Altlast, dringend prüfen
3	Nur NTLMv2	LM, NTLMv1, NTLMv2	Üblicher Standard auf aktuellem Windows
4	Nur NTLMv2	NTLMv1, NTLMv2 (kein LM)	Zwischenschritt
5	Nur NTLMv2	Nur NTLMv2	Ziel; vorher Quellen von NTLMv1 abstellen

```
# Aktuellen Wert prüfen (kein Wert: Betriebssystem-Standard)
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa' `
    -Name LmCompatibilityLevel -ErrorAction SilentlyContinue

# Auf dem DC: erfolgreiche Anmeldungen mit NTLM V1 im Sicherheitsprotokoll finden
Get-WinEvent -FilterHashtable @{ LogName='Security'; Id=4624 } -MaxEvents 20000 |
    Where-Object { $_.Message -match 'NTLM V1' } |
    Select-Object TimeCreated, Message -First 50
```

Das Ereignis 4624 enthält im Abschnitt mit den detaillierten Authentifizierungsinformationen den Paketnamen, und dort steht bei den Übeltätern „NTLM V1“. Auf Systemen mit erweitertem Auditing, also ab Windows 11 24H2 und Server 2025 sowie Server 2022 und 2019 mit den Updates ab 13.10.2026, liefern zusätzlich die Ereignisse 4020 bis 4023 auf Clients und Servern sowie 4030 bis 4033 auf den Domain Controllern das Feld „NTLM Version“; die ungeraden IDs sind die Warnungen bei verringerter Sicherheit. Auf älteren Systemen bleibt die klassische Restrict-NTLM-Überwachung mit 8001 bis 8004. Wie du das einschaltest, steht in [Erweitertes NTLM-Auditing einschalten: Schritt für Schritt](#); die passenden Richtlinien legt dir das [NTLM-Audit-GPO-Skript](#) an. Was die DC-Ereignisse im Einzelnen verraten, erklärt [NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004](#).

Netzwerkmitschnitt für Geräte ohne Protokoll

Scanner, NAS und Medizingeräte schreiben kein Windows-Ereignisprotokoll. Bei ihnen hilft nur der Blick auf die Leitung, am besten am Dateiserver mit Wireshark oder dem integrierten pktmon.

NTLM-Anmeldungen findest du mit dem Anzeigefilter ntlmssp. Die Unterscheidung zwischen v1 und v2 steckt in der dritten Nachricht, der Authenticate-Nachricht: Bei NTLMv2 zerlegt Wireshark die NT-Antwort in eine NTLMv2-Struktur mit Zeitstempel und Client-Challenge, bei NTLMv1 bleibt eine nackte Antwort von 24 Byte.

```
# Wireshark-Anzeigefilter: Authenticate-Nachrichten ohne NTLMv2-Antwort
ntlmssp.message_type == 0x00000003 && !ntlmssp.ntlmv2_response

# Mitschnitt auf einem Windows-Server ohne Zusatzsoftware (als Administrator)
pktmon start --capture --pkt-size 0 --file-name C:\Temp\smb.etl
pktmon stop
pktmon etl2pcap C:\Temp\smb.etl --out C:\Temp\smb.pcapng
```

WARNUNG • Was der Mitschnitt nicht sieht

MS-CHAPv2 innerhalb von PEAP läuft in einem TLS-Tunnel. Den WLAN-Fall findest du deshalb nicht in Wireshark, sondern in den Clientereignissen 4024/4025 und im Protokoll deines RADIUS-Servers. Der Mitschnitt ist das Werkzeug für SMB, HTTP und andere Protokolle, in denen NTLM offen transportiert wird.

Und bevor du in der Klinik oder in der Verwaltung mitschneidest: Ein Mitschnitt enthält Benutzernamen und unter Umständen Inhalte. Kläre Zweck und Umfang vorher.

Welche Filter, Mitschnittpunkte und Fallstricke es noch gibt, beschreibt [NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen](#).

Wo es mühsam wird, und wie es leichter geht

Auf einem einzelnen Notebook ist das alles ein überschaubarer Vormittag. Bei der Sparfuchs & Partner Steuerberatungs GmbH mit 60 Arbeitsplätzen auch noch. Spätestens bei einer Klinik mit 1.800 Clients, drei Domain Controllern, einem Dutzend WLAN-Profilen und einer Labor-IT, die seit 2014 niemand mehr angefasst hat, wird aus dem Vormittag ein Projekt. Die Gründe sind immer dieselben.

- **Die Ereignisse liegen verteilt.** 4024 und 4025 entstehen auf jedem einzelnen Client. Ohne Windows Event Forwarding oder Direktabfrage kommst du nicht heran, und bei Geräten im Außendienst schon gar nicht.
- **Die Menge erschlägt.** Ein Domain Controller schreibt am Tag Zehntausende 4624-Ereignisse. Die zwölf mit „NTLM V1“ darin findest du mit Where-Object, aber nicht nebenbei.
- **Stille Geräte bleiben unsichtbar.** Was kein Protokoll schreibt, siehst du nur von der Gegenseite oder im Mitschnitt, und den macht man nicht auf Hunderten Ports gleichzeitig.
- **Die Ursache fehlt.** Das Ereignis sagt, dass NTLMv1 benutzt wurde. Es sagt nicht, welches WLAN-Profil, welche Firmware oder welche Gruppenrichtlinie dahintersteckt.
- **Die Leitung will eine Antwort.** „Wie viele Geräte sind betroffen, und wann sind wir durch?“ ist eine berechtigte Frage, und 30.000 Zeilen CSV sind keine Antwort darauf.

Das Sammeln selbst lässt sich mit Bordmitteln lösen, [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#) zeigt den Weg. Das Verdichten, Zuordnen und Erklären ist der Teil, an dem die meisten Teams hängenbleiben, und der Teil, für den wir den [NTLM Diagnostiker](#) gebaut haben. Er liest NTLM-Ereignisse dort, wo sie entstehen, und macht daraus eine Liste, mit der man arbeiten kann. Er arbeitet ausschließlich lesend: Er ändert keinen Registrierungswert, keine Gruppenrichtlinie und kein Konto. Gerade während einer Störung ist das beruhigend, denn das Letzte, was du jetzt brauchst, ist ein Werkzeug, das auch noch eigene Ideen hat.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Die NTLMv1-Quellen in einer Liste

Die NTLMv1-Hitliste fasst zusammen, welche Clients, Server, Konten und Ziele noch NTLMv1 benutzen, sortiert nach Häufigkeit. Damit weißt du, mit welchem Gerät du anfängst. Sicherheitsflaggen markieren zusätzlich Anmeldungen mit NTLMv1 oder ohne MIC.

Für Geräte ohne Ereignisprotokoll importierst du einen Wireshark-Mitschnitt. Der Diagnostiker erkennt darin NTLMv1-Anmeldungen und führt sie in derselben Liste wie die Ereignisse aus dem Protokoll. Der Scanner im Flur steht dann neben dem Dateiserver, an dem er scheitert.

Als Ereignisquellen dienen die Domain Controller direkt, ein vorhandener Windows Event Collector oder die Direktabfrage einzelner Rechner. Der Abdeckungsmonitor und die OS-Landkarte zeigen, welche Systeme Daten liefern und welche überhaupt betroffen sein können. Kommunikationsmatrix und Konten-Sicht zeigen, wer mit wem und unter welchem Konto spricht; die Ursachen-Engine prüft dazu SPN und DNS.

Für die Leitung gibt es einen Word-Bericht, für das Team den Excel- oder CSV-Export. Die kostenlose Express-Edition liefert einen Fünf-Minuten-Befund mit Readiness-Ampel, die Vollversion kannst du sieben Tage testen, lizenziert wird pro aktivem Computerkonto.

Ein Generator für Ausnahmelisten und Skripte ist geplant, aber noch nicht enthalten. Die Ausnahme für BlockNtlmv1SSO setzt du also weiterhin selbst, dafür aber mit einer Liste, die stimmt.

AUS DER PRAXIS · Trendforge Digital GmbH: vom Ticketberg zur Liste

Bei der Trendforge Digital GmbH, Domäne trendforge.local, kamen in der Woche nach dem Update 43 Tickets zu „Anmeldeproblemen“. Nach dem Zusammenführen der Client- und DC-Ereignisse blieben drei Ursachen übrig: ein VPN-Profil mit EAP-MSCHAPv2 auf 31 Notebooks, ein WLAN-Profil für Besprechungsraumgeräte und ein Multifunktionsgerät mit alter Firmware, das mit der SSO-Sperre gar nichts zu tun hatte, sondern an einer Server-Härtung aus derselben Woche scheiterte. Drei Ursachen, drei Maßnahmen, eine befristete Ausnahme für die Besprechungsraumgeräte.

FAQ zur NTLMv1-Sperre

Betrifft die Sperre auch Windows 10 oder Windows Server 2022?

Nein. Die Änderung an BlockNtlmv1SSO gilt für Windows 11 ab 24H2 und für Windows Server 2025. Ältere Systeme verhalten sich wie bisher. NTLMv1 kann dort trotzdem scheitern, etwa wenn der Domain Controller per LmCompatibilityLevel 5 nur noch NTLMv2 annimmt.

Muss ich nach dem Ändern von BlockNtlmv1SSO neu starten?

Nein. Laut Microsoft wirkt die Änderung ohne Neustart. Das ist praktisch für die Erste Hilfe und genauso praktisch für das Zurückdrehen, wenn die Ursache behoben ist.

Wir haben NTLMv1 per Gruppenrichtlinie längst verboten. Warum sehen wir trotzdem 4025?

Weil die Richtlinie zur LAN-Manager-Authentifizierungsebene regelt, was ein Client einem Server als Antwort schickt. MS-CHAPv2 in WLAN, LAN oder VPN braucht NTLMv1-abgeleitete Anmeldedaten unabhängig davon. Genau diesen Weg sperrt BlockNtlmv1SSO.

Ist Credential Guard die Lösung?

Für den Schutz der Anmeldedaten ja, Microsoft empfiehlt ihn ausdrücklich. Für die Netzwerkanmeldung nein: Auch unter Credential Guard funktioniert MS-CHAPv2-SSO nicht. Die dauerhafte Lösung ist eine zertifikatsbasierte Anmeldung am Netz.

Warum scannt unser Multifunktionsgerät nicht mehr in den Ordner?

Mit hoher Wahrscheinlichkeit nicht wegen BlockNtlmv1SSO, denn das Gerät nutzt kein Single Sign-on eines Windows-Clients. Prüfe das Sicherheitsprotokoll des Zielservers, die LAN-Manager-Authentifizierungsebene auf Server und DC, SMB-Einstellungen und die Firmware des Geräts.

Wie lange darf eine Ausnahme mit BlockNtlmv1SSO = 0 bestehen bleiben?

So kurz wie möglich und nur für benannte Geräte. Gib ihr ein Ablaufdatum und lass die Ereignisse 4024 weiterlaufen, dann siehst du, wann sie nicht mehr gebraucht wird.

Was hat die NTLMv1-Sperre mit der NTLM-Abschaltung zu tun?

Sie ist ein Vorgeschmack. Die allgemeine Abschaltung von Netzwerk-NTLM kommt laut Microsoft mit der nächsten Windows-Server-Version als Standard. Wer jetzt die NTLMv1-Quellen sauber findet, hat dafür schon die halbe Inventur erledigt.

Fazit: Die Sperre ist richtig, die Notlösung nur geliehen

Die NTLMv1-Sperre vom 13. Oktober 2026 ist kein Betriebsunfall, sondern ein überfälliger Schritt, mit über einem Jahr Vorlauf und Tausenden Warnungen, die niemand lesen wollte. Sie sperrt einen eng umrissenen Weg: Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten auf Windows 11 ab 24H2 und Server 2025 ohne Credential Guard. Wer das versteht, sortiert die Tickets schneller und verschwendet keine Zeit mit Scannern, die ein ganz anderes Problem haben.

Der Registrierungswert auf 0 ist erlaubt, aber geliehen: gezielt, befristet und überwacht. Die eigentliche Arbeit ist, die Quellen zu finden und abzustellen, vor allem MS-CHAPv2 im Netzzugang. Mit Ereignisanzeige, PowerShell und Wireshark kommst du dahin; mit einer NTLMv1-Hitliste kommst du schneller dahin. Und wenn dein Team das künftig selbst sicher beherrschen soll, ist die [Schulung zum NTLM Diagnostiker](#) der passende nächste Schritt.

WEITERLESEN · Weiter in dieser Serie

- › [BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme](#)
- › [Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen](#)
- › [NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet](#)
- › [NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll](#)
- › [NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen](#)
- › [NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen](#)