

BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme

BlockNtlmv1SSO: ein DWORD, drei Zustände

Der gefährlichste Zustand ist der, den niemand gesetzt hat: Der Wert fehlt, und Windows entscheidet für dich.

Wert fehlt

seit 13.10.2026:
Erzwingung

0

Überwachung
Ereignis 4024

1

Erzwingung
Ereignis 4025

HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_o

REG_DWORD, wirkt ohne Neustart, wird vom Update nicht angelegt

Skizze: die drei Zustände von BlockNtlmv1SSO auf einen Blick

WISSEN

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

› [NTLM Diagnostiker](#)

BERATUNG

BlockNtlmv1SSO sauber einführen: messen, Ausnahmen begrenzen, erzwingen.

› [Beratung zur NTLM-Ablösung](#)

SCHULUNG

Ereignisse lesen, Gruppenrichtlinien bauen, Ausnahmen pflegen: für dein Team.

› [Schulung zum NTLM Diagnostiker](#)

Es gibt Registrierungswerte, die du einmal im Leben setzt und dann vergisst. BlockNtlmv1SSO gehört nicht dazu, obwohl er genau so aussieht: ein DWORD, zwei erlaubte Werte, kein Neustart. Das Tückische ist der dritte Zustand, den es offiziell gar nicht gibt. Der Wert fehlt. Und genau dieser Zustand hat sich am 13. Oktober 2026 still und leise von „Windows warnt“ in „Windows sperrt“ verwandelt, ohne dass auf einem einzigen Rechner auch nur ein Bit in der Registrierung geändert wurde.

Seitdem blockieren Windows 11 ab Version 24H2 und Windows Server 2025 standardmäßig Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten. Wer vorher nichts getan hat, hat damit die Erzwingung bekommen, ob er wollte oder nicht. Wer vorher den Wert auf 0 gesetzt hat, weil irgendwo ein Forumsbeitrag das empfahl, hat dagegen noch genau den Zustand von gestern, mit allen Schwächen von gestern. Beides ist keine Strategie, sondern Zufall mit Verwaltungsaufwand.

Dieser Beitrag ist die technische Referenz zum Wert: wo er liegt, was jeder Zustand bewirkt, wie du ihn per Gruppenrichtlinie steuerst, wie du Ausnahmen so setzt, dass sie wieder verschwinden, und wie du vorher misst, was die Erzwingung kaputtmachen würde. Was die Sperre im Alltag konkret anrichtet, von WLAN bis Kiosk-Terminal, steht im Schwesterbeitrag [NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht](#).

FAKTEN • BlockNtlmv1SSO in 30 Sekunden

Pfad: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_o, Typ REG_DWORD.

0 = Überwachung: SSO mit NTLMv1-abgeleiteten Anmeldedaten wird erlaubt, Windows schreibt Warnung 4024. 1 = Erzwingung: SSO wird blockiert, Windows schreibt Fehler 4025.

Wert fehlt: vor dem Oktober-Update 2026 wie 0, ab dem Update vom 13.10.2026 wie 1. Das Update legt den Wert nicht an und ändert ihn nicht.

Änderungen wirken ohne Neustart. Betroffen sind Windows 11 ab 24H2 und Windows Server 2025, und nur, wenn Credential Guard nicht aktiv ist.

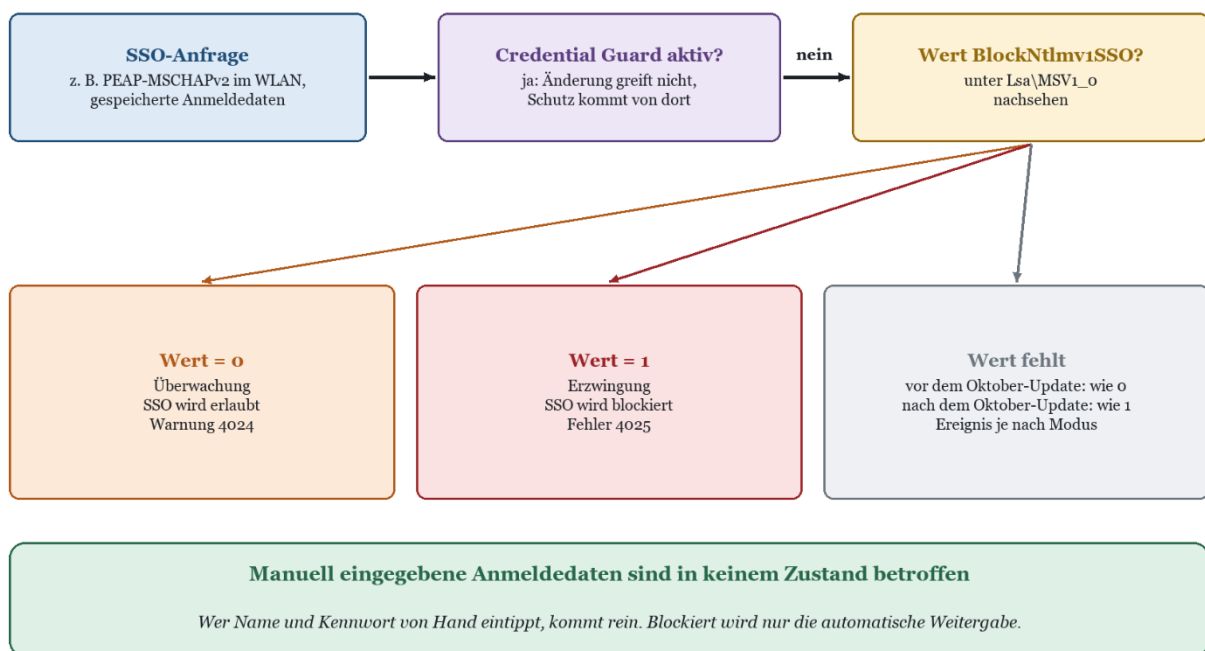
Beide Ereignisse landen in Microsoft-Windows-NTLM/Operational.

Der Wert im Detail: Pfad, Typ, Zustände

Der Name ist Programm, wenn man ihn langsam liest: Block NTLMv1 SSO. Der Wert sperrt nicht NTLMv1 im Allgemeinen, sondern die automatische Weitergabe NTLMv1-abgeleiteter Anmeldedaten für Single Sign-on. Das klassische Beispiel ist der Netzzugang mit MS-CHAPv2, also PEAP-MSCHAPv2 oder EAP-MSCHAPv2 im WLAN, am kabelgebundenen Port mit 802.1X oder im VPN. Windows nimmt dort die Anmeldedaten, die bei der Anmeldung am Rechner im Speicher gelandet sind, und rechnet daraus eine Antwort, deren Kryptografie aus einer Zeit stammt, in der Modems noch gepfiffen haben.

Wie Windows über BlockNtlmv1SSO entscheidet

Windows 11 ab 24H2 und Windows Server 2025, Anfrage mit NTLMv1-abgeleiteten Anmeldedaten für Single Sign-on



Skizze: vereinfachte Entscheidungslogik nach Microsoft KB5066470

Wo der Wert liegt und wie er aussieht

Eigenschaft	Inhalt
Schlüssel	HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_o
Name	BlockNtlmv1SSO (Microsoft schreibt ihn teils auch BlockNTLMv1SSO; die Registrierung unterscheidet bei Namen nicht nach Groß- und Kleinschreibung)
Typ	REG_DWORD
Gültige Werte	0 = Überwachung, 1 = Erzwingung
Neustart	nicht erforderlich
Vom Update angelegt?	nein, der Wert bleibt fehlend, solange du ihn nicht setzt
Betroffene Systeme	Windows 11 24H2, 25H2, 26H1, 26H2 und Windows Server 2025

Wirkungslos bei	aktivem Credential Guard
------------------------	--------------------------

Die drei Zustände und ihre Ereignisse

Entscheidend ist weniger, was im Wert steht, sondern ob überhaupt etwas drinsteht. Das Oktober-Update hat keinen einzigen Wert geändert, sondern nur die Bedeutung von „nichts“. Genau deshalb sieht ein Registrierungsvergleich vor und nach dem Patchday völlig harmlos aus.

Zustand	Verhalten	Ereignis	Typ
0	Überwachung: SSO erlaubt	4024	Warnung
1	Erzwingung: SSO blockiert	4025	Fehler
fehlt, vor dem 13.10.2026	wie 0: Überwachung	4024	Warnung
fehlt, ab dem 13.10.2026	wie 1: Erzwingung	4025	Fehler
beliebig, Credential Guard aktiv	Änderung greift nicht	keines	–

Vom Warnen zum Sperren: die Zeitleiste

Was ein fehlender Wert zu welchem Zeitpunkt bedeutet hat



Skizze: Zeitleiste nach Microsoft KB5066470, Monatsangaben gerundet

Was in 4024 und 4025 drinsteht

Beide Ereignisse stammen aus der Quelle NTLM und landen im Protokoll Microsoft-Windows-NTLM/Operational. Laut Microsoft nennt der Meldungstext unter anderem den Zielserver, den übergebenen Benutzer und die Domäne, Prozess-ID, Name und LUID des aufrufenden Clientprozesses, die Identität, unter der dieser Prozess läuft, sowie die OID des Mechanismus. Mit anderen Worten: Du erfährst, wer wohin wollte und welches Programm es versucht hat. Das ist mehr, als viele Fachanwendungen in ihr eigenes Fehlerprotokoll schreiben. Wie du die Ereignisse im Einzelnen liest und filterst, steht in [Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen](#).

WARNUNG · Credential Guard ist kein Freibrief für die Inventur

Auf Rechnern mit aktivem Credential Guard greift BlockNtlmv1SSO nicht, weil Credential Guard NTLMv1-Kryptografie ohnehin nicht zulässt. Das ist gut für die Sicherheit, aber es heißt auch: Diese Rechner schreiben keine 4024 und keine 4025. Wenn in deinem Fuhrpark Geräte mit und ohne Credential Guard gemischt sind, wirkt die Sperre nur auf einem Teil, und die Statistik ist entsprechend lückenhaft. Ob Credential Guard läuft, zeigt dir msinfo32 oder die WMI-Klasse Win32_DeviceGuard im Namespace root\Microsoft\Windows\DeviceGuard.

Den aktuellen Stand mit Bordmitteln prüfen

Für einen einzelnen Rechner reichen drei Zeilen PowerShell. Die erste liest den Wert, die zweite zeigt, ob Credential Guard läuft, die dritte zählt die Ereignisse der letzten sieben Tage. Ein fehlender Wert ergibt keine Fehlermeldung, sondern schlicht nichts, und genau dieses Nichts ist seit dem 13.10.2026 die Erzwingung.

```
# Wert lesen (leer = nicht gesetzt)
Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0' `
  -Name BlockNtlmv1SSO -ErrorAction SilentlyContinue | Select-Object BlockNtlmv1SSO

# Credential Guard: 1 in SecurityServicesRunning = läuft
(Get-CimInstance -Namespace root\Microsoft\Windows\DeviceGuard `
  -ClassName Win32_DeviceGuard).SecurityServicesRunning

# 4024 und 4025 der letzten sieben Tage zählen
Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational';
  Id=4024,4025; StartTime=(Get-Date).AddDays(-7) } -ErrorAction SilentlyContinue |
  Group-Object Id | Select-Object Name, Count
```

Wer lieber mit wevtutil arbeitet, etwa in einem Anmeldeskript oder auf einem Server Core, kommt mit einer XPath-Abfrage zum selben Ziel:

```
wevtutil qe Microsoft-Windows-NTLM/Operational ^
  /q:"*[System[(EventID=4024 or EventID=4025)]]" /c:20 /rd:true /f:text
```

Per Gruppenrichtlinie steuern statt von Hand

Eine administrative Vorlage mit einem hübschen Kontrollkästchen für BlockNtlmv1SSO beschreibt Microsoft in der Supportdokumentation nicht. Dort ist nur vom Registrierungswert die Rede. Der saubere Weg in der Domäne führt deshalb über die Gruppenrichtlinien-Einstellungen, also Computerkonfiguration, Einstellungen, Windows-Einstellungen, Registrierung. Ein Registrierungselement mit Aktion „Aktualisieren“, Struktur HKEY_LOCAL_MACHINE, Schlüsselpfad SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0, Wertname BlockNtlmv1SSO, Typ REG_DWORD, Daten 0 oder 1. Mehr ist es nicht.

Warum du den Wert 1 explizit setzen solltest

Ja, ein fehlender Wert bedeutet heute schon Erzwingung. Trotzdem lohnt es sich, die 1 per Gruppenrichtlinie aktiv zu verteilen. Erstens ist dann dokumentiert, dass jemand diese Entscheidung getroffen hat, und nicht, dass sie zufällig passiert ist. Zweitens überschreibt die Richtlinie alte Nullen, die irgendwer irgendwann mal per Skript, Image oder Forumsrezept hinterlassen hat. Drittens kannst du bei der nächsten Prüfung mit einem Blick in die Gruppenrichtlinienergebnisse belegen, wie der Stand ist. Im Audit klingt „Die 1 ist per GPO gesetzt“ deutlich besser als „Das ist halt der Standard, glaube ich“.

Vorgehen	Vorteil	Nachteil	Einordnung
Wert fehlt, nichts tun	kein Aufwand	alte Nullen bleiben, nichts dokumentiert	Zufall
1 per GPO für alle	einheitlich, belegbar, räumt Altlasten ab	keine Ausnahme ohne zweite GPO	Zielbild
0 per GPO für alle	keine Tickets heute	Schutz überall weg, Ausnahme wird Dauerzustand	Notbremse, nur kurz
1 für alle, 0 für	Schutz bleibt, Ausfälle	Gruppe braucht Pflege	Empfehlung

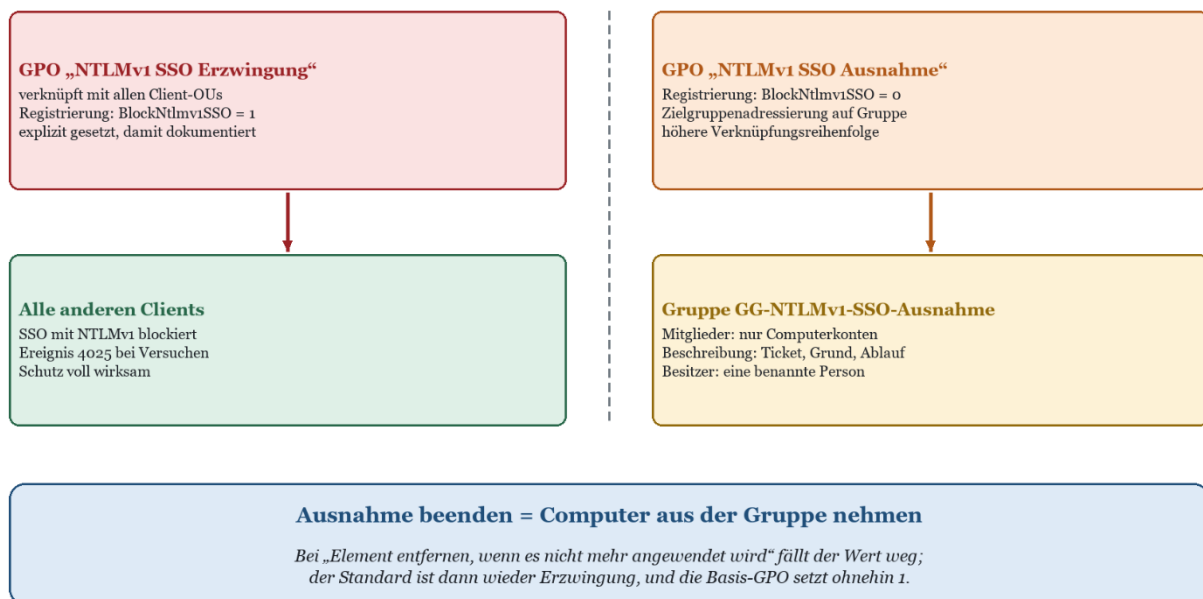
Gruppe	gezielt abgefangen		
von Hand per regedit	schnell am Einzelplatz	nicht nachvollziehbar, wird vergessen	nur zum Testen

Die Ausnahme: gezielt und befristet

Microsoft beschreibt den Wert 0 ausdrücklich als befristete, eng begrenzte Ausnahme für kritische Abhängigkeiten, die sich noch nicht umstellen lassen, mit dem Hinweis, dass der Schutz dabei sinkt. Das ist die freundliche Formulierung für: Jede Null ist ein Loch, und du solltest wissen, wo es ist und wann du es wieder zumachst.

Die gezielte Ausnahme per Gruppenrichtlinie

musterwerk.local: Wert 1 für alle, Wert 0 nur für eine Computergruppe mit Ablaufdatum



Skizze: Ausnahme über Gruppenrichtlinien-Einstellungen; Namen frei erfunden

Bewährt hat sich eine zweite Richtlinie, die nur den Wert 0 setzt und per Zielgruppenadressierung auf eine Sicherheitsgruppe mit Computerkonten zielt. In der Beschreibung der Gruppe stehen Ticketnummer, Grund und Ablaufdatum; die Gruppe hat eine benannte Person als Besitzer. Wichtig ist im Registrierungselement das Kontrollkästchen „Element entfernen, wenn es nicht mehr angewendet wird“ auf der Registerkarte „Gemeinsam“. Ohne dieses Häkchen bleibt die 0 auf dem Rechner stehen, auch wenn du ihn längst aus der Gruppe genommen hast. Gruppenrichtlinien-Einstellungen tätowieren nämlich gern.

- **Nur Computerkonten in die Gruppe.** Der Wert gilt pro Maschine, nicht pro Benutzer.
- **Gruppenmitgliedschaft braucht ein frisches Ticket.** Nach dem Hinzufügen hilft ein Neustart oder `klist -li 0x3e7 purge` mit anschließendem `gpupdate /force`.
- **Ablaufdatum in die Beschreibung.** Und einen Kalendereintrag für die Person, die die Gruppe verantwortet. Ein Ablaufdatum, das niemand prüft, ist Dekoration.
- **Verknüpfungsreihenfolge prüfen.** Die Ausnahme-GPO muss die Basis-GPO überstimmen, sonst gewinnt die 1 und die Ausnahme existiert nur auf dem Papier.

WICHTIG · Die domänenweite Null ist die teuerste Abkürzung

Am Montag nach dem Patchday ist die Versuchung groß: eine GPO, Wert 0, Domänenstamm, fertig. Die Tickets verschwinden, und mit ihnen der Schutz auf jedem einzelnen Client. Ein halbes Jahr

später weiß niemand mehr, warum die Richtlinie existiert, und beim nächsten Penetrationstest steht sie als Befund im Bericht. Wenn es wirklich brennt, dann die Null mit Sicherheitsgruppe und Ablaufdatum, nicht mit dem Domänenstamm als Ziel.

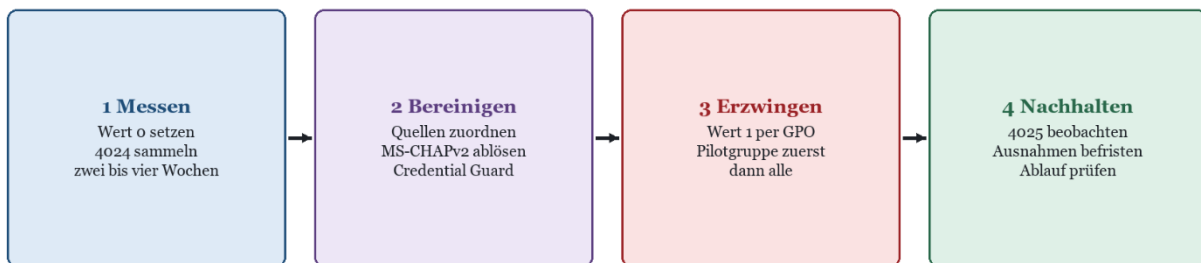
Dasselbe Prinzip, Ausnahmen klein, benannt und befristet, gilt übrigens auch für die Server-Ausnahmen der Restrict-NTLM-Richtlinien. Wie du die pflegst, ohne dass sie zum Schweizer Käse werden, steht in [Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren](#).

Erst messen, dann erzwingen

Der Zweck der Überwachung war nie, dass Windows ein Jahr lang Warnungen in ein Protokoll schreibt, das niemand öffnet. Der Zweck war, dir die Liste zu liefern, bevor die Sperre kommt. Wer heute noch Rechner im Überwachungsmodus hat, sei es über eine Ausnahme oder weil das Oktober-Update dort noch nicht installiert ist, sitzt auf genau dieser Liste.

Erst messen, dann erzwingen

Vier Schritte, die aus einem Patchday-Schreck einen geplanten Vorgang machen



Schon nach dem 13.10.2026? Dann beginnst du bei Schritt 3

und misst rückwärts: Die 4025 zeigen dir, was gerade ausfällt. Schritt 1 gibt es nur noch als gezielte Ausnahme.

Skizze: Vorgehensmodell; Zeiträume als Richtwert, nicht als Norm

Was du messen musst

Für die Entscheidung je Maschine brauchst du drei Dinge: den aktuellen Wert von BlockNtlmv1SSO, den Status von Credential Guard und die Ereignisse 4024 und 4025 aus einem aussagekräftigen Zeitraum, also mindestens über einen Monatsabschluss, eine Schicht am Wochenende und den einen Laptop, der nur im Außendienst ins VPN geht. Wer nur drei Tage misst, findet die Quellen von drei Tagen.

Befund auf der Maschine	Bedeutung	Nächster Schritt
kein 4024, kein 4025	keine SSO-Versuche mit NTLMv1 gesehen	Wert 1, fertig
4024 vorhanden	würde bei Erzwingung blockiert	Prozess und Ziel klären, Quelle umstellen
4025 vorhanden	wird gerade blockiert	Auswirkung prüfen, ggf. befristete Ausnahme
keine Ereignisse, Credential Guard aktiv	Sperre greift dort ohnehin nicht	Netzzugang trotzdem auf Zertifikate prüfen
Windows 10, Server 2022 oder älter	BlockNtlmv1SSO wirkt dort nicht	klassisches NTLM-Auditing nutzen, 8001 bis 8004

Ein Rechner ist leicht, zweihundert sind Arbeit

Auf einem Rechner zählt Get-WinEvent in Sekunden. Auf zweihundert wird daraus ein Invoke-Command über eine Liste, die nie ganz vollständig ist, weil die Hälfte der Notebooks gerade im Zug sitzt. Dazu kommt, dass 4024 und 4025 nur auf dem Client entstehen. Der Domain Controller sieht davon nichts, denn bei MS-CHAPv2 im WLAN ist es der RADIUS-Server, der die Antwort prüft. Du sammelst also von vielen Maschinen und musst wissen, von welchen du gerade nichts gehört hast, weil sie sauber sind, und von welchen, weil sie schlicht nicht erreichbar waren.

Der klassische Weg ist Windows Event Forwarding: Abonnement auf Microsoft-Windows-NTLM/Operational, Filter auf 4024 und 4025, ein Collector, fertig. Wie das geht, steht in [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#). Wenn du parallel das erweiterte NTLM-Auditing nach KB5064479 einschaltetest, also die Ereignisse 4020 bis 4023 auf Clients und Servern und 4030 bis 4033 auf Domain Controllern, siehst du zusätzlich, wo außerhalb von Single Sign-on noch NTLM läuft. Die Gruppenrichtlinie dafür musst du nicht von Hand zusammenklicken; das [NTLM-Audit-GPO-Skript](#) legt sie dir an.

```
# Stand auf vielen Rechnern einsammeln (Liste: computers.txt)
$pcs = Get-Content .\computers.txt
Invoke-Command -ComputerName $pcs -ErrorAction SilentlyContinue -ScriptBlock {
    $v = (Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0' `
        -Name BlockNtlmv1SSO -ErrorAction SilentlyContinue).BlockNtlmv1SSO
    $e = Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational';
        Id=4024,4025 } -ErrorAction SilentlyContinue
    [pscustomobject]@{ Wert = if ($null -eq $v) { 'fehlt' } else { $v }
        E4024 = ($e | Where-Object Id -eq 4024).Count
        E4025 = ($e | Where-Object Id -eq 4025).Count }
} | Select-Object PSComputerName, Wert, E4024, E4025 | Export-Csv .\sso-stand.csv -NoType
```

TIPP · Die stillen Rechner zählen extra

Das Skript liefert nur die Rechner, die geantwortet haben. Vergleiche die Ergebnisliste immer mit der Liste der aktiven Computerkonten im Active Directory. Die Differenz ist nicht „sauber“, sondern „unbekannt“, und unbekannt ist bei einer Sperre die unangenehmste Kategorie.

AUS DER PRAXIS · Trendforge Digital GmbH: Messung im Rückwärtsgang

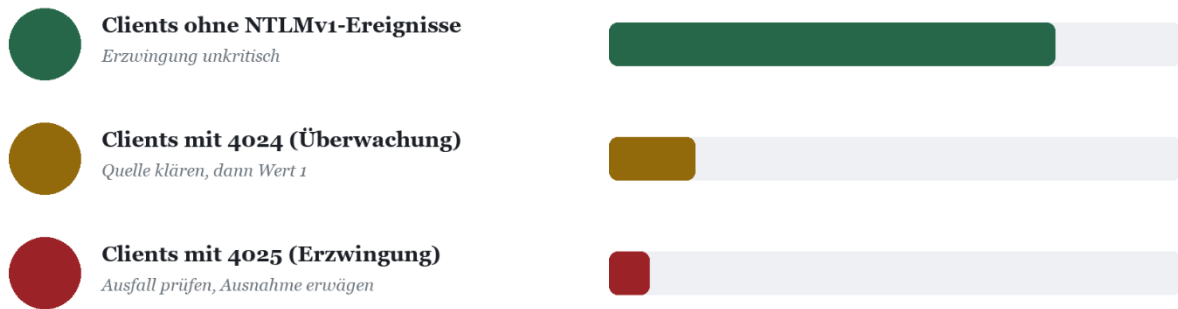
Bei Trendforge war das Oktober-Update schon auf allen Notebooks, als die ersten VPN-Tickets kamen. Statt die Null domänenweit zu verteilen, hat das Team die betroffenen Geräte per 4025 identifiziert, genau elf Stück, in eine Ausnahmegruppe gesteckt und ein Ablaufdatum von vier Wochen eingetragen. In dieser Zeit wurde das VPN-Profil von MS-CHAPv2 auf Zertifikatsanmeldung umgestellt. Die Gruppe war nach drei Wochen leer, die Ausnahme-GPO wurde gelöscht. Unspektakulär, und genau so soll es sein.

Den Stand je Maschine im Blick behalten

Mit PowerShell, wevtutil und Event Forwarding kommst du zum Ziel, das ist keine Frage. Mühsam wird es an drei Stellen: wenn aus elf Rechnern dreihundert werden, wenn dieselbe Quelle an fünfzig Stellen Hunderte Ereignisse erzeugt und du die eine Ursache dahinter suchst, und wenn du der IT-Leitung bis Freitag sagen sollst, ob die Erzwingung „passt“. Eine CSV-Datei mit Zählern beantwortet keine dieser Fragen, sie verschiebt sie nur in Excel.

Stand je Maschine statt Bauchgefühl

Sparfuchs & Partner Steuerberatungs GmbH: fiktive Auswertung, drei Ampelzustände



*Wichtig ist nicht die grüne Mehrheit, sondern die rote Minderheit:
Dort sitzt das Ticket von morgen früh.*

Skizze: Prinzip einer Readiness-Ampel; Anteile frei erfunden

Genau für diese Lage haben wir den [NTLM Diagnostiker](#) gebaut. Er sammelt die NTLM-Ereignisse wahlweise direkt vom Domain Controller, über einen Windows Event Collector oder per Direktabfrage, und arbeitet dabei ausschließlich lesend: Er setzt keinen Registrierungswert, ändert keine Richtlinie und fasst keine Gruppe an. Die Entscheidung, wo die 1 hingehört und wo vorerst die 0, bleibt bei dir, aber du triffst sie mit Daten statt mit Hoffnung.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · BlockNtlmv1SSO-Bereitschaft je Maschine

Die Readiness-Ampel zeigt den Stand je Maschine: Wo ist die Erzwingung unkritisch, wo gibt es noch NTLMv1-Spuren, wo wird bereits blockiert. Der Abdeckungsmonitor und die OS-Landkarte zeigen dir, welche Rechner überhaupt Ereignisse liefern und auf welchen Windows-Versionen BlockNtlmv1SSO wirkt, sodass stille Geräte nicht als sauber durchgehen.

Die NTLMv1-Hitliste sortiert die Quellen nach Häufigkeit, die Ursachen-Engine prüft dazu SPN und DNS, und die Kommunikationsmatrix mit Konten-Sicht zeigt, welches Konto von wo nach wo spricht. Mit der Abschalt-Simulation siehst du vorab, was eine Erzwingung treffen würde. Ergebnisse gehen als Word-Bericht an die IT-Leitung und als Excel- oder CSV-Export ins Ticket.

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 sowie ein Verlauf sind geplant, aber noch nicht enthalten.

› [NTLM Diagnostiker](#)

Wenn du die Umstellung nicht allein stemmen willst oder eine zweite Meinung zu deiner Ausnahmeliste suchst, unterstützen wir dich in der [Beratung zur NTLM-Ablösung](#), von der Messung bis zur letzten gelöschten Ausnahme-GPO.

FAQ zu BlockNtlmv1SSO

Muss ich nach dem Ändern von BlockNtlmv1SSO neu starten?

Nein. Laut Microsoft wirkt die Änderung ohne Neustart. Wenn du den Wert per Gruppenrichtlinie verteilst, brauchst du nur die nächste Richtlinienaktualisierung; bei einer frisch geänderten Gruppenmitgliedschaft allerdings ein neues Computerticket.

Legt das Oktober-Update den Wert an?

Nein. Das Update vom 13.10.2026 ändert nur das Standardverhalten bei fehlendem Wert. Ein Blick in die Registrierung zeigt also nach dem Update dasselbe wie vorher, nämlich nichts, obwohl sich das Verhalten von Überwachung zu Erzwingung geändert hat.

Betrifft der Wert auch Windows 10 oder Windows Server 2022?

Nein. BlockNtlmv1SSO gilt für Windows 11 ab 24H2 und für Windows Server 2025. Auf älteren Systemen setzt du für den NTLM-Überblick auf das klassische Restrict-NTLM-Auditing mit den Ereignissen 8001 bis 8004, bei Server 2022 und 2019 mit den aktuellen Updates zusätzlich auf das erweiterte Auditing. Einzelheiten dazu in [Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern](#).

Hilft die LAN-Manager-Authentifizierungsebene an dieser Stelle?

Sie regelt, welche NTLM-Varianten ein Rechner sendet und annimmt, und bleibt wichtig. BlockNtlmv1SSO ist aber ein eigener Schalter für Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten. Das eine ersetzt das andere nicht.

Kann ich die Ausnahme pro Benutzer setzen?

Nein. Der Wert liegt unter HKLM und gilt für die ganze Maschine. Deshalb gehören in die Ausnahmegruppe Computerkonten, keine Benutzer.

Ist Credential Guard die bessere Lösung?

Für den Schutz der Anmeldedaten ja, Microsoft empfiehlt ihn, wo die Voraussetzungen erfüllt sind. Die Abhängigkeit von MS-CHAPv2 im Netzzugang löst er aber nicht: Mit Credential Guard funktioniert das SSO dort ebenfalls nicht. Die eigentliche Lösung ist eine Anmeldung per Zertifikat statt MS-CHAPv2.

Wo steht das bei Microsoft?

Im Supportartikel [Manage NTLMv1 changes and prevent network authentication issues in Windows](#). Dort findest du Pfad, Werte, Ereignisse und die Liste der betroffenen Windows-Versionen.

Fazit: Die 1 gehört dir, nicht dem Zufall

BlockNtlmv1SSO ist ein unscheinbarer Wert mit einer unbequemen Eigenschaft: Sein wichtigster Zustand ist der, in dem er gar nicht existiert. Seit dem 13.10.2026 heißt dieser Zustand Erzwingung. Wer das weiß, setzt die 1 bewusst per Gruppenrichtlinie, fängt echte Abhängigkeiten mit einer kleinen, befristeten Ausnahmegruppe ab und misst vorher, statt hinterher Tickets zu zählen.

Die Bordmittel reichen für den Anfang, und dieser Beitrag hat gezeigt, wie. Ab einer gewissen Zahl Maschinen wird aus der Messung allerdings eine Fleißarbeit, bei der die stillen Geräte und die eigentliche Ursache gern durchrutschen. Dann lohnt der Blick auf eine Ampel je Maschine. Und die Null? Die darfst du ausleihen. Aber bitte mit Rückgabedatum.

WEITERLESEN • Weiter in dieser Serie

- › [NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht](#)
- › [Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen](#)
- › [NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet](#)
- › [Erweitertes NTLM-Auditing einschalten: Schritt für Schritt](#)
- › [NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding](#)
- › [NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll](#)

› [NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen](#)