NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet

Skizze: die drei Phasen der NTLM-Ablösung und der NTLMv1-Sonderweg

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

BERATUNG
Wir begleiten deine NTLM-Ablösung vom ersten Audit bis zur Abschaltung.
› Beratung zur NTLM-Ablösung

SCHULUNG
Ereignisse lesen, Ursachen finden, Ausnahmen pflegen: praxisnah für dein Team.
› Schulung zum NTLM Diagnostiker

NTLM ist so etwas wie der alte Kellerschlüssel, den niemand mehr braucht, den aber auch niemand wegwirft, weil irgendwo noch eine Tür ist, die nur er aufsperrt. Dreißig Jahre lang hat Windows dieses Protokoll still im Hintergrund mitlaufen lassen: als Rückfallebene, wenn Kerberos nicht wollte, als Notnagel für Geräte, die Kerberos nie gelernt haben, und als bequeme Abkürzung für jedes Skript, das auf eine IP-Adresse statt auf einen Namen zeigt.

Damit ist Schluss, und zwar nicht irgendwann, sondern in Etappen, die Microsoft inzwischen öffentlich gemacht hat. Die erste Etappe läuft längst, die zweite kommt gerade, die dritte steht mit der nächsten Windows-Server-Version an. Und als kleine Vorspeise hat das Windows-Update vom 13. Oktober 2026 auf aktuellen Systemen die Single-Sign-on-Anmeldung mit NTLMv1-abgeleiteten Anmeldedaten standardmäßig gesperrt. Wenn bei dir seitdem ein WLAN auf der Station oder ein VPN-Zugang plötzlich nach dem Passwort fragt, weißt du jetzt, warum.

In diesem Beitrag bekommst du den Fahrplan in Ruhe erklärt: was in welcher Phase passiert, was davon schon wirkt, was das für eine typische Umgebung im Mittelstand, in der Klinik oder in der Verwaltung heißt, und welche Ausreden du ab sofort nicht mehr gelten lassen solltest. Am Ende weißt du, was du in den nächsten Wochen tun solltest, damit du am Stichtag nicht der Mensch bist, der um drei Uhr nachts herausfindet, dass die Laborsoftware NTLM fest eingebaut hat.

FAKTEN · Das Wichtigste in 30 Sekunden

Phase 1: erweitertes NTLM-Auditing mit den Ereignissen 4020 bis 4023 (Client und Server) und 4030 bis 4033 (Domain Controller), inklusive Reason-ID. Verfügbar ab Windows 11 24H2 und

Windows Server 2025, für Server 2022 und 2019 mit den Updates ab 13.10.2026.

Phase 2: IAKerb und lokales KDC schließen Lücken, in denen Windows bisher auf NTLM ausweichen musste. Microsoft hat sie für die zweite Jahreshälfte 2026 angekündigt.

Phase 3: Mit der nächsten Windows-Server-Version und den zugehörigen Client-Versionen ist Netzwerk-NTLM standardmäßig deaktiviert. Entfernt ist es damit noch nicht.

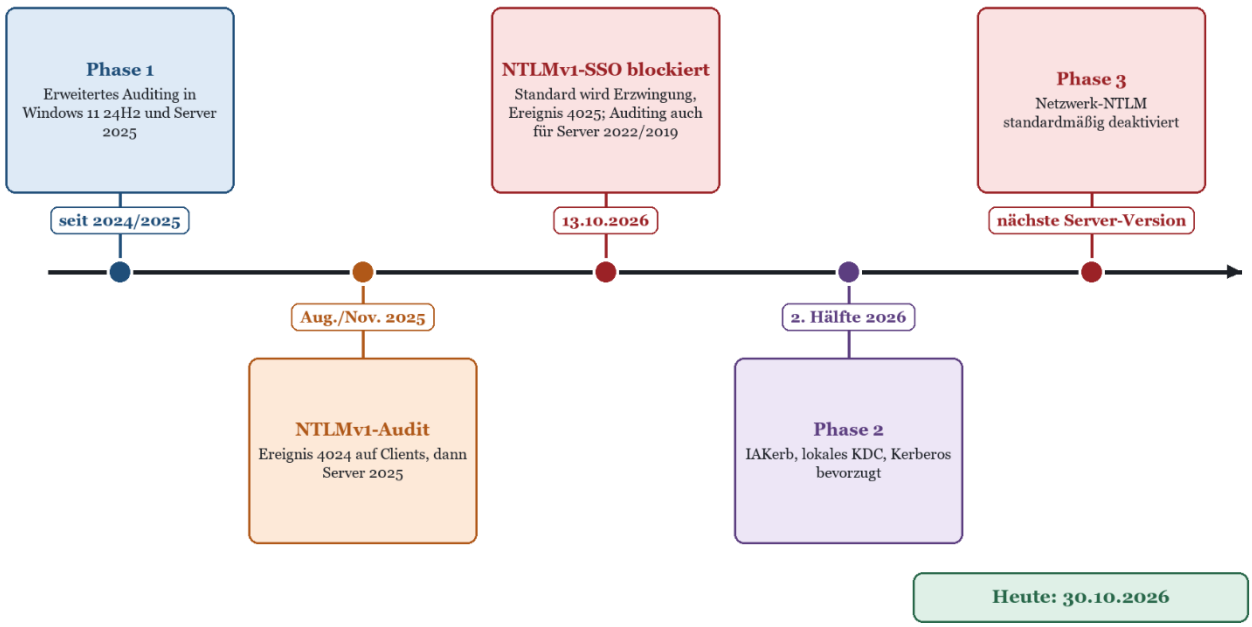
Sonderweg: Seit dem Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1-abgeleitete Anmeldedaten für Single Sign-on standardmäßig (BlockNtlmv1SSO, Ereignisse 4024 und 4025).

Der Fahrplan: drei Phasen und ein Sonderweg

Microsoft geht bei NTLM ungewöhnlich behutsam vor, und das hat einen Grund: Kaum ein Protokoll steckt so tief in so vielen Ecken, an die sich niemand mehr erinnert. Statt eines großen Knalls gibt es deshalb drei Phasen. Erst sollst du sehen können, wo NTLM benutzt wird. Dann baut Microsoft die Lücken zu, in denen Kerberos bisher technisch gar nicht konnte. Und erst danach wird der Schalter umgelegt. Parallel dazu läuft die NTLMv1-Sperre, die einen eigenen, schnelleren Weg geht.

Die Zeitleiste der NTLM-Ablösung

Stand 30.10.2026. Termine ab Phase 3 nennt Microsoft ausdrücklich unter Vorbehalt



Skizze: vereinfachte Zeitleiste nach den Ankündigungen von Microsoft

Etappe	Was passiert	Betroffene Systeme	Stand Ende Oktober 2026
Phase 1: Auditing	Erweiterte NTLM-Ereignisse mit Reason-ID, Prozess, Ziel und NTLM-Version	Windows 11 ab 24H2, Server 2025; Server 2022/2019 mit Updates ab 13.10.2026	Verfügbar und standardmäßig aktiv
Phase 2: Lückenschluss	IAKerb, lokales KDC, Windows-Komponenten bevorzugen Kerberos	Aktuelle Windows-Versionen	Angekündigt für die zweite Jahreshälfte 2026, teils Vorabversion
Phase 3:	Netzwerk-NTLM ist ab Werk	Nächste Windows-Server-	Angekündigt, ohne

Standard-Abschaltung	deaktiviert, per Richtlinie wieder einschaltbar	Version und zugehörige Clients	festes Datum
Sonderweg NTLMv1-SSO	NTLMv1-abgeleitete Anmeldedaten für Single Sign-on gesperrt	Windows 11 ab 24H2, Server 2025 (ohne Credential Guard)	Seit 13.10.2026 standardmäßig erzwungen

Phase 1: Erst hinschauen, dann handeln

Die erste Phase ist die unspektakulärste und zugleich die wichtigste. Windows protokolliert NTLM jetzt deutlich genauer als früher. Auf Clients erscheinen die Ereignisse 4020 und 4021 für ausgehende NTLM-Anmeldungen, auf Servern 4022 und 4023 für eingehende. Domain Controller schreiben 4030 bis 4033, getrennt nach Anmeldungen innerhalb der eigenen Domäne und über Domänengrenzen hinweg. Die ungeraden Nummern sind jeweils die Warnungen: Sie tauchen auf, wenn die Anmeldung mit verringerter Sicherheit lief, etwa mit NTLMv1 oder ohne MIC.

Der eigentliche Fortschritt steckt in einem einzigen Feld: „Reason ID“. Zum ersten Mal sagt dir Windows nicht nur, dass NTLM benutzt wurde, sondern auch, warum Kerberos nicht zum Zug kam. Die Werte reichen von 0 bis 11, von „Anwendung ruft NTLM direkt auf“ über „Zielname enthält eine IP-Adresse“ bis „keine Sichtverbindung zum Domain Controller“. Dazu kommen Felder wie „Process Name“, „Target Machine“ und „NTLM Version“. Alles zusammen steht im Protokoll Microsoft-Windows-NTLM/Operational. Was jede einzelne Reason-ID bedeutet und was du dagegen tust, erklärt NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

Die neuen Ereignisse gibt es ab Windows 11 24H2 und Windows Server 2025, für Windows Server 2022 und 2019 mit den Updates ab dem 13. Oktober 2026. Auf älteren Systemen bleibt dir die klassische Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8004, die zwar weniger erzählt, aber immerhin überhaupt etwas erzählt. Die Details zu beiden Welten findest du in der Microsoft-Dokumentation Microsoft-Support: Überblick zu den erweiterten NTLM-Überwachungsereignissen (KB5064479).

TIPP · Die Gruppenrichtlinien heißen anders, als du suchst

Das erweiterte Logging steuerst du über die Richtlinie „NTLM Enhanced Logging“ unter Administrative Vorlagen, System, NTLM sowie auf den Domain Controllern über „Log Enhanced Domain-wide NTLM Logs“ unter Administrative Vorlagen, System, Netlogon.

Wenn du dir das Zusammenklicken sparen willst, legt dir das NTLM-Audit-GPO-Skript die passenden Richtlinien an. Die ausführliche Anleitung steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt.

Phase 2: IAKerb und lokales KDC stopfen die technischen Löcher

Es gibt Situationen, in denen Kerberos bisher schlicht nicht konnte, egal wie sauber deine SPNs gepflegt sind. Der Klassiker: Der Client hat keine direkte Verbindung zu einem Domain Controller, etwa weil er in einem abgeschotteten Netz steht oder über ein Gateway kommt. Kerberos braucht den Kontakt zum KDC, NTLM nicht, also fiel Windows auf NTLM zurück. Das ist Reason-ID 9. IAKerb löst das, indem der Zielserver die Kerberos-Kommunikation stellvertretend an den Domain Controller weiterreicht.

Die zweite Lücke sind lokale Konten. Wer sich mit einem lokalen Administratorkonto an einem anderen Rechner anmeldet, hatte bisher keinen KDC, der dafür ein Ticket ausstellen konnte. Das lokale KDC gibt jedem Rechner einen eigenen kleinen Ticketschalter für seine lokalen Konten. Zusätzlich stellt Microsoft Windows-Komponenten, die NTLM bisher fest verdrahtet hatten, auf Kerberos um. Wie IAKerb und lokales KDC im Detail funktionieren und wo sie (noch) nicht helfen,

steht in Keine Sichtverbindung zum DC: Reason-ID 9, IAKerb und lokales KDC. Wer bei Kerberos selbst noch Lücken hat, findet die Grundlagen im Kompetenzbereich Microsoft Kerberos.

WICHTIG · Phase 2 repariert nicht deine Altlasten

IAKerb und lokales KDC helfen bei Reason-ID 9 und bei lokalen Konten. Sie helfen nicht bei Laufwerken, die auf IP-Adressen zeigen, bei fehlenden oder doppelten SPNs und erst recht nicht bei Anwendungen, die NTLM direkt aufrufen. Microsoft nennt die Funktionen zudem teilweise noch Vorabversion. Plane also nicht darauf, dass sich das Problem von selbst erledigt.

Phase 3: NTLM ist aus, außer du schaltest es wieder ein

Mit der nächsten Windows-Server-Version und den zugehörigen Client-Versionen wird Netzwerk-NTLM standardmäßig deaktiviert. Microsoft betont ausdrücklich zwei Dinge: Erstens ist NTLM damit nicht aus Windows entfernt, sondern nur ab Werk abgeschaltet. Zweitens kannst du es per Richtlinie wieder einschalten, wenn es gar nicht anders geht. Ein festes Datum gibt es nicht, und Microsoft stellt den gesamten Zeitplan unter den Vorbehalt, dass er sich ändern kann.

Das klingt entspannt, ist es aber nur auf den ersten Blick. Denn „per Richtlinie wieder einschaltbar“ heißt im Alltag: Am Tag, an dem der erste neue Server in Betrieb geht, musst du wissen, welche Clients, Dienste und Geräte ihn per NTLM ansprechen. Sonst merkst du es an den Tickets. Und wer NTLM pauschal wieder einschaltet, hat sich einen neuen Server mit altem Sicherheitsniveau gekauft. Herzlichen Glückwunsch.

Der Sonderweg: NTLMv1 für Single Sign-on ist seit dem 13.10.2026 gesperrt

Während die drei Phasen gemächlich vorankommen, hat Microsoft bei NTLMv1 kürzeren Prozess gemacht. Seit dem Sicherheitsupdate vom 13. Oktober 2026 erzeugen Windows 11 ab 24H2 und Windows Server 2025 standardmäßig keine NTLMv1-abgeleiteten Anmeldedaten mehr für Single Sign-on. Gesteuert wird das über den Registrierungswert BlockNtlmv1SSO unter HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0: 0 bedeutet Überwachung, 1 bedeutet Erzwingung. Fehlt der Wert, gilt seit Oktober die Erzwingung. Das Update legt den Wert übrigens nicht an, du siehst also in der Registrierung nichts und wirst trotzdem blockiert.

Im Überwachungsmodus schreibt Windows das Ereignis 4024 (Warnung), im Erzwingungsmodus 4025 (Fehler), beide in Microsoft-Windows-NTLM/Operational. Typisch betroffen sind WLAN-, LAN- und VPN-Anmeldungen mit MS-CHAPv2, also PEAP-MSCHAPv2 und EAP-MSCHAPv2. Manuell eingegebene Anmeldedaten funktionieren weiter, nur das automatische Durchreichen nicht mehr. Auf Geräten mit aktiviertem Credential Guard war dieses Verhalten ohnehin schon gesperrt, dort ändert sich nichts. Microsoft beschreibt die Details Microsoft-Support: Änderungen an NTLMv1 in Windows 11 24H2 und Windows Server 2025 (KB5066470).

WARNUNG · Zurück auf 0 ist eine Ausnahme, kein Zustand

BlockNtlmv1SSO auf 0 zu setzen, holt dir das alte Verhalten zurück und senkt den Schutz. Microsoft empfiehlt das nur als befristete, eng begrenzte Ausnahme für kritische Abhängigkeiten, die du nicht sofort umstellen kannst. Die dauerhafte Lösung für WLAN und VPN ist eine zertifikatsbasierte Anmeldung wie EAP-TLS oder PEAP-TLS.

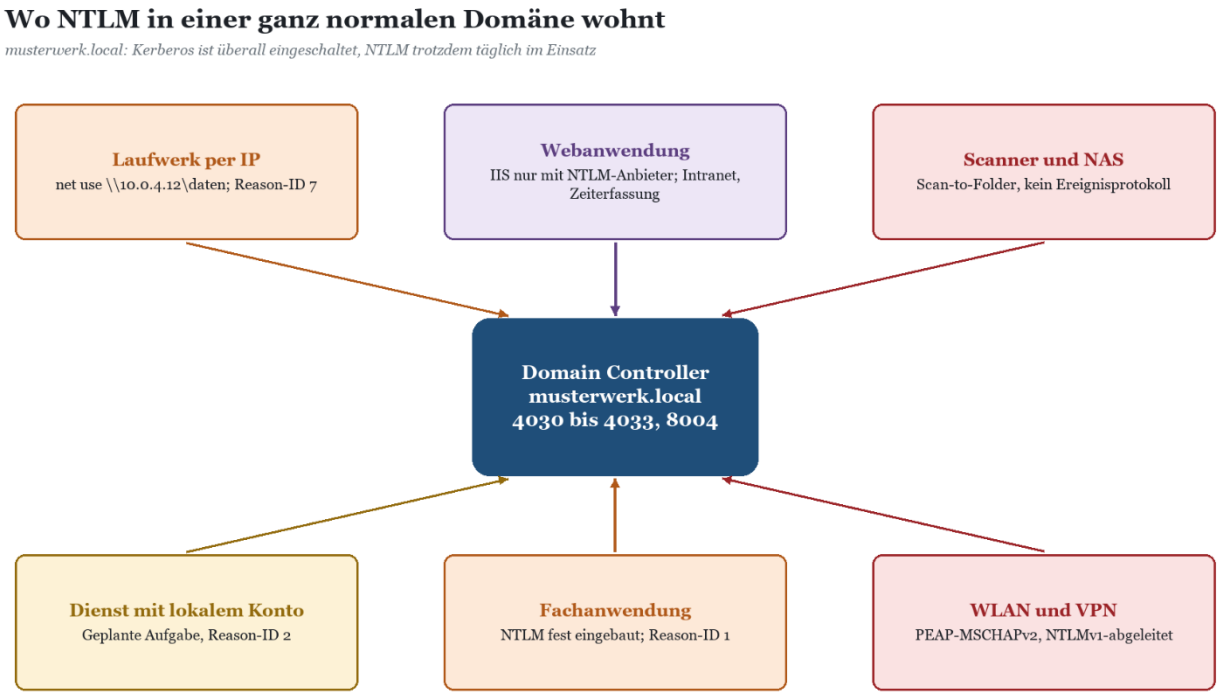
WEITERLESEN · Alles zur NTLMv1-Sperre

› NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht
› BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme

› Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen

Was das für deine Umgebung heißt

Die gute Nachricht zuerst: In den meisten Active-Directory-Umgebungen läuft der weit überwiegende Teil der Anmeldungen längst über Kerberos. Die schlechte: Der Rest ist genau der Teil, den niemand dokumentiert hat. NTLM versteckt sich nicht in den großen, gut gepflegten Systemen, sondern in den Ritzen dazwischen.



Skizze: typische NTLM-Quellen; Adressen und Namen frei erfunden

Mittelstand: der Scanner, das NAS und das Skript von 2011

Bei der Musterwerk GmbH sieht es aus wie in Tausenden anderen Betrieben: eine Domäne musterwerk.local, zwei Domain Controller, ein Dateiserver, ein ERP-System, Multifunktionsgeräte mit Scan-to-Folder und ein NAS für die Datensicherung. Kerberos funktioniert tadellos. Trotzdem zählt das erste Audit einige Tausend NTLM-Anmeldungen pro Tag. Die Quellen: ein Anmeldeskript, das Laufwerke per IP-Adresse verbindet, ein Dienst auf dem ERP-Server mit einem lokalen Konto, die Multifunktionsgeräte und eine Zeiterfassung im Intranet, deren IIS nur den NTLM-Anbieter kennt.

Nichts davon ist exotisch, und das meiste davon lässt sich mit überschaubarem Aufwand umstellen, sobald man es gefunden hat. Für die Skripte hilft NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen, für die Webanwendung NTLM in IIS und Webanwendungen: Negotiate statt NTLM und für die Geräte ohne eigenes Ereignisprotokoll NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

Kliniken: Medizintechnik hat einen langen Atem

In Krankenhäusern kommt eine Besonderheit hinzu: Viele Systeme dürfen gar nicht beliebig verändert werden. Medizinprodukte, Laborgeräte, Bildarchive und Fachanwendungen sind zertifiziert, gewartet vom Hersteller und oft mit Betriebssystemständen unterwegs, die älter sind

als manche Assistenzärztin und mancher Assistenzarzt. Wenn hier NTLM fest eingebaut ist, entscheidest nicht du über den Zeitplan, sondern der Hersteller.

Dazu kommt das WLAN. Stationen, Visitenwagen und mobile Geräte melden sich in vielen Häusern noch per PEAP-MSCHAPv2 an. Genau das trifft die NTLMv1-Sperre seit dem 13. Oktober. Wer hier nicht rechtzeitig auf Zertifikate umgestellt hat, erlebt gerade Pflegekräfte, die morgens um sechs ihr Passwort in ein WLAN-Fenster tippen. Wie man in dieser Lage priorisiert, zeigt NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen. Und wie du Herstellern die richtigen Fragen stellst, statt ein „wir prüfen das“ zu kassieren, steht in Wenn die Anwendung NTLM fest eingebaut hat: Hersteller richtig fragen.

Verwaltungen und Systemhäuser: viele Fachverfahren, wenig Zeit

Kommunalverwaltungen kämpfen mit Fachverfahren, die über Jahrzehnte gewachsen sind und teilweise von Rechenzentren oder Zweckverbänden betrieben werden. Systemhäuser kämpfen mit dem gleichen Problem, nur mal zwanzig Kunden. Für Trendforge Digital GmbH, ein Systemhaus mit rund dreißig betreuten Domänen, ist die NTLM-Ablösung keine technische, sondern eine organisatorische Herausforderung: Wie bekomme ich ein einheitliches Lagebild, ohne bei jedem Kunden drei Tage im Ereignisprotokoll zu verbringen? Darauf geht NTLM-Ablösung im Systemhaus: viele Kunden, ein Vorgehen ein. Und weil NTLM-Protokolle Benutzernamen und Rechnernamen enthalten, gehört auch die Frage nach Datenschutz und Mitbestimmung auf die Liste: NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Umgebung	Typische NTLM-Quellen	Häufige Reason-IDs	Wer entscheidet
Mittelstand	Laufwerke per IP, Scanner, NAS, IIS-Intranet, lokale Dienstkonten	7, 2, 1	Du selbst, meist schnell
Klinik	Medizintechnik, Labor, PACS, WLAN mit PEAP-MSCHAPv2, Fachanwendungen	1, 9, 2	Oft der Hersteller
Verwaltung	Fachverfahren, externe Rechenzentren, alte Druckerumgebungen	1, 6, 7	Fachamt, Dienstleister, Hersteller
Systemhaus	Alles oben, multipliziert mit der Kundenzahl	alle	Kunde und Systemhaus gemeinsam

AUS DER PRAXIS · Sparfuchs & Partner und der Drucker im Flur

Bei der Sparfuchs & Partner Steuerberatungs GmbH lief nach dem Oktober-Update alles, bis auf eine Kleinigkeit: Das Scan-to-Folder des Multifunktionsgeräts legte keine Dateien mehr ab. Das Gerät selbst schreibt kein Windows-Ereignisprotokoll, der Dateiserver aber schon. Die Ereignisse 4022 und 4023 auf dem Dateiserver zeigten die IP-Adresse des Geräts, eine NTLM-Anmeldung mit einem Dienstkonto und eine Warnung zur NTLM-Version. Ursache gefunden in zwanzig Minuten. Ohne die Serverseite wäre es ein Nachmittag mit dem Druckerdienstleister geworden.

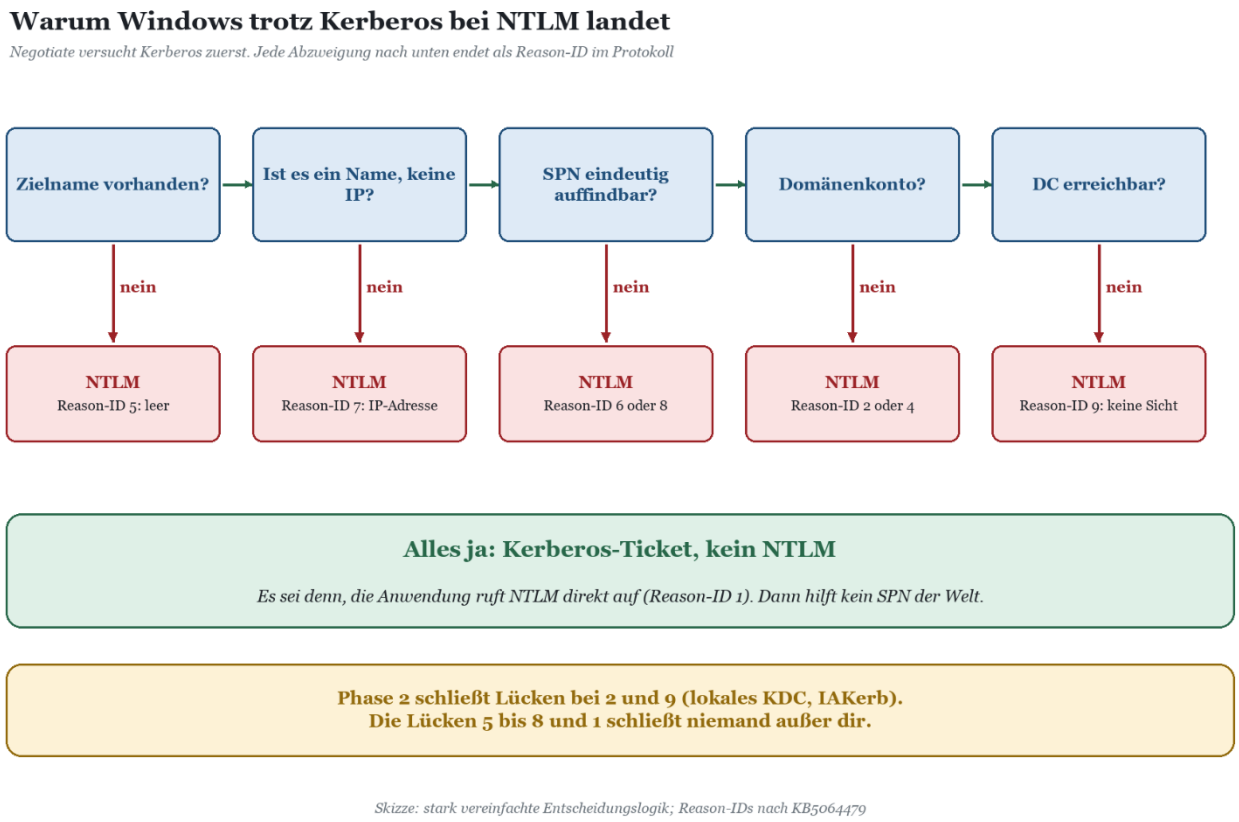
Mythen, die du ab heute nicht mehr gelten lässt

Jede Infrastrukturänderung bringt ihre eigenen Beruhigungssätze mit. Bei NTLM sind sie besonders hartnäckig, weil sie meistens halb stimmen. Und halb stimmt bei Authentifizierung ungefähr so beruhigend wie halb schwanger.

„Betrifft uns nicht, wir haben Kerberos“

Der Klassiker, und er ist fast immer falsch. Kerberos ist in jeder Domäne seit Windows 2000 eingeschaltet. NTLM aber auch. Windows nutzt Negotiate, versucht zuerst Kerberos und fällt

lautlos auf NTLM zurück, sobald irgendetwas nicht passt: ein Ziel per IP-Adresse, ein fehlender SPN, ein doppelter SPN, ein lokales Konto, kein Domain Controller in Sicht. Oder die Anwendung fragt Kerberos gar nicht erst. Kein Benutzer merkt davon etwas, und genau das ist das Problem: NTLM fällt erst auf, wenn es nicht mehr da ist.



Skizze: stark vereinfachte Entscheidungslogik; Reason-IDs nach KB5064479

Zwei dieser Abzweigungen kannst du mit Bordmitteln sehr gezielt prüfen. Für fehlende Namen und SPNs lohnt Reason-ID 6: wenn der Zielname nicht auflösbar ist, für doppelte SPNs Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten. Für lokale Konten und Dienstkonten gibt es eigene Wege: Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden und Dienstkonten als NTLM-Quelle: finden, prüfen, umstellen.

Die übrigen Mythen im Schnelldurchlauf

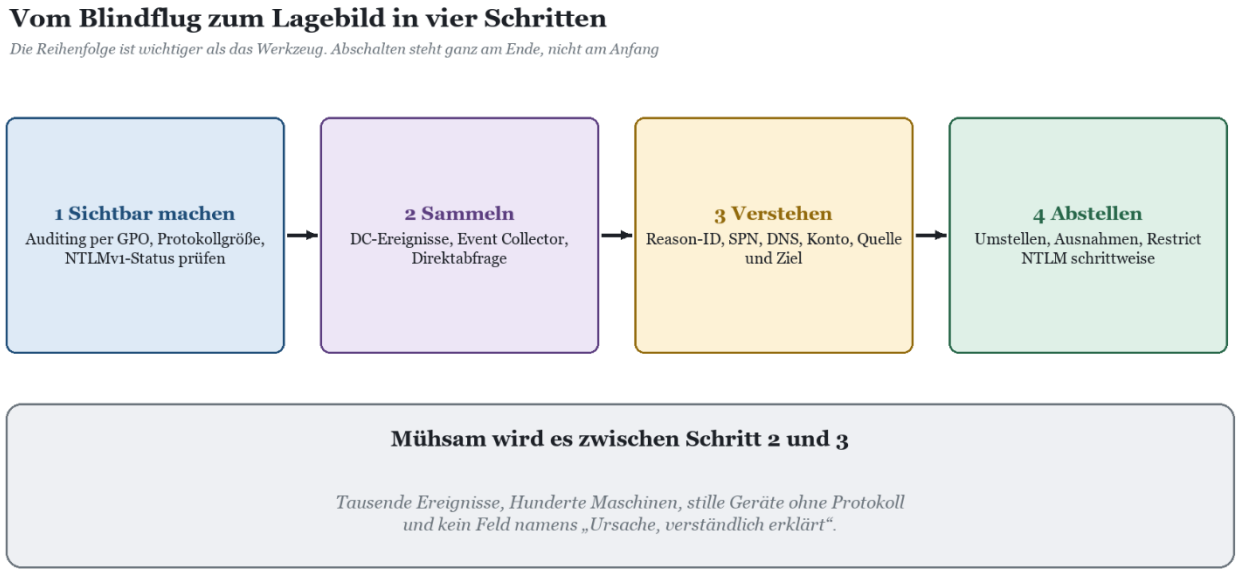
Mythos	Was wirklich stimmt
„NTLMv1 haben wir längst nicht mehr.“	Vielleicht nicht als Anmeldeprotokoll im Netz. Aber MS-CHAPv2 im WLAN und VPN nutzt NTLMv1-abgeleitete Anmeldedaten. Genau das blockiert BlockNtlmv1SSO seit dem 13.10.2026.
„Microsoft löscht NTLM, dann ist es eben weg.“	In Phase 3 wird NTLM standardmäßig deaktiviert, nicht entfernt. Du kannst es per Richtlinie wieder einschalten, mit allen Sicherheitsfolgen.
„Das betrifft nur den neuen Server.“	Die Ereignisse und die NTLMv1-Sperre wirken schon heute auf Windows 11 24H2 und Server 2025. Und der neue Server ist das Ziel, das deine alten Clients per NTLM ansprechen.
„Phase 2 repariert das schon.“	IAKerb und lokales KDC helfen bei fehlender DC-Sicht und lokalen Konten. IP-Adressen, SPN-Fehler und fest eingebautes NTLM bleiben deine Aufgabe.
„Wir schalten einfach per GPO ab und schauen, was passiert.“	Das ist kein Test, das ist ein Ausfall mit Ansage. Erst überwachen, dann Ausnahmen, dann schrittweise verweigern.
„Auditing frisst Leistung und	Die erweiterten Ereignisse sind standardmäßig aktiv. Was knapp werden

Speicherplatz.“	kann, ist die Protokollgröße. Die stellst du größer, das kostet dich ein paar Megabyte.

Wie ein schrittweises Vorgehen konkret aussieht, beschreiben Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern und NTLM schrittweise abschalten, ohne dass etwas ausfällt. Und weil NTLM nicht nur ein Kompatibilitäts-, sondern vor allem ein Sicherheitsthema ist, lohnt bis zur endgültigen Abschaltung auch ein Blick auf NTLM-Relay verhindern: MIC, Kanalbindung und erweiterter Schutz.

Jetzt erfassen: mit Bordmitteln, und wo es mühsam wird

Das Vorgehen ist für alle Umgebungen das gleiche, egal ob zwanzig oder zweitausend Rechner. Erst sichtbar machen, dann sammeln, dann verstehen, dann abstellen. Wer die Reihenfolge umdreht, bekommt das Verstehen gratis, allerdings in Form von Störungsmeldungen.



Skizze: Vorgehensmodell für die NTLM-Ablösung

Der erste Blick mit Bordmitteln

Für einen ersten Eindruck reichen PowerShell und wevtutil völlig aus. Die folgenden Befehle laufen lesend, verändern nichts und zeigen dir auf einem einzelnen Rechner, ob und wie viel NTLM dort unterwegs ist:

```
# NTLM-Ereignisse der letzten Zeit nach ID zählen
Get-WinEvent -LogName 'Microsoft-Windows-NTLM/Operational' -MaxEvents 2000 |
    Group-Object Id | Sort-Object Count -Descending | Select-Object Name, Count

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

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

# Doppelte SPNs im Forest finden (Reason-ID 8)
setspn -X -F
```

Auf einem Domain Controller zeigen dir die Ereignisse 4030 bis 4033 dazu, welche Server NTLM-Anmeldungen mit welchen Konten durchreichen. Was in den einzelnen Feldern steht und wie du sie liest, erklären Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen, Ereignis 4022

und 4023: eingehende NTLM-Anmeldungen auf Servern und NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004. Den kompletten Weg mit allen Varianten zeigt NTLM-Nutzung ermitteln: der komplette Leitfaden.

Wo es mühsam wird

Auf einem Rechner ist das ein netter Nachmittag. In einer echten Umgebung wird es schnell unübersichtlich. Ein einziger Dateiserver erzeugt am Tag leicht Tausende Ereignisse, die sich zu einer Handvoll Ursachen verdichten. Die Ereignisse liegen verteilt auf Hunderten Maschinen, also brauchst du Windows Event Forwarding oder einen anderen Sammelweg (NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding). Geräte wie Drucker, NAS und Medizintechnik schreiben gar nichts, die siehst du nur von der Gegenseite oder im Mitschnitt (NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen). Und die Reason-ID sagt dir zwar, dass der SPN fehlte, aber nicht, ob der DNS-Eintrag falsch ist, der Alias nie registriert wurde oder das Skript eine IP-Adresse aus dem Jahr 2011 benutzt.

Dazu kommt die Frage, die dir die Geschäftsführung oder die Krankenhausleitung stellen wird: „Sind wir bereit?“ Die Antwort „Ich habe 48.000 Ereignisse in einer CSV-Datei“ ist ehrlich, aber nicht hilfreich. Einen ausführlichen Vergleich der Wege findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

Der kurze Weg zum Lagebild

Genau für diese Lücke zwischen Sammeln und Verstehen haben wir den NTLM Diagnostiker gebaut. Er liest die NTLM-Ereignisse dort, wo sie entstehen, ordnet sie Ursachen zu und macht daraus ein Bild, das auch jemand versteht, der nicht jeden Tag im Ereignisprotokoll wohnt. Er arbeitet ausschließlich lesend: Er ändert keine Richtlinie, keinen Registrierungswert und kein Konto. Das ist kein Detail, sondern die Voraussetzung dafür, dass du ihn in einer Klinik oder einer Verwaltung überhaupt einsetzen darfst.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Fünf Minuten bis zum ersten Befund

Mit der kostenlosen Express-Edition bekommst du einen Fünf-Minuten-Befund: eine Readiness-Ampel, die dir sagt, wie weit deine Umgebung von einer NTLM-Abschaltung entfernt ist, und eine NTLMv1-Hitliste, die zeigt, wer seit dem Oktober-Update Probleme hat oder haben wird.

Ereignisquellen sind wahlweise die Domain Controller direkt, ein vorhandener Windows Event Collector oder die Direktabfrage einzelner Rechner. Der Abdeckungsmonitor und die OS-Landkarte zeigen dir, von welchen Systemen Daten kommen und welche überhaupt die erweiterten Ereignisse liefern können.

Die Ursachen-Engine prüft zu jeder NTLM-Anmeldung SPN und DNS und sagt dir, warum Kerberos nicht gegriffen hat. Kommunikationsmatrix und Konten-Sicht zeigen, wer mit wem und unter welchem Konto spricht, Sicherheitsflaggen markieren Anmeldungen ohne MIC oder mit NTLMv1. Für Geräte ohne Protokoll gibt es den Wireshark-Import.

Vor dem Umschalten zeigt dir die Abschalt-Simulation, was bei einer Abschaltung ausfallen würde. Ergebnisse gehen als Word-Bericht an die Leitung und als Excel- oder CSV-Export an das Team. Die Vollversion kannst du sieben Tage testen, lizenziert wird pro aktivem Computerkonto.

Geplant, aber noch nicht enthalten, sind unter anderem ein Anwendungskatalog, ein Generator für Ausnahmelisten und Skripte, ein Phasenplan, ein Kerberos-Gegencheck und eine Verlaufsansicht.

Wenn du die Analyse lieber gemeinsam mit jemandem machst, der solche Umgebungen schon häufiger auseinandergenommen hat, hilft die Beratung zur NTLM-Ablösung. Und wenn du das Projekt intern aufsetzen musst, mit Zeitplan, Rollen und realistischem Aufwand, lies zuerst NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand.

FAQ zur NTLM-Abschaltung

Wann genau schaltet Microsoft NTLM ab?

Ein festes Datum gibt es nicht. Standardmäßig deaktiviert wird Netzwerk-NTLM mit der nächsten Windows-Server-Version und den zugehörigen Client-Versionen. Microsoft stellt den Zeitplan ausdrücklich unter Vorbehalt. Fest steht dagegen die NTLMv1-SSO-Sperre: Sie wirkt seit dem 13.10.2026.

Kann ich NTLM nach Phase 3 wieder einschalten?

Ja, per Richtlinie. NTLM wird in Phase 3 nicht entfernt, sondern nur ab Werk deaktiviert. Pauschal wieder einschalten solltest du es trotzdem nicht, sondern gezielt über Ausnahmen. Wie das sauber geht, steht in Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren.

Betrifft mich die NTLMv1-Sperre, wenn ich NTLMv1 per GPO längst verboten habe?

Möglicherweise trotzdem. Die Sperre betrifft NTLMv1-abgeleitete Anmeldedaten für Single Sign-on, wie sie MS-CHAPv2 im WLAN, im kabelgebundenen 802.1X und im VPN nutzt. Das ist eine andere Baustelle als die Einstellung für die LAN-Manager-Authentifizierungsebene. Prüfe die Ereignisse 4024 und 4025.

Ich habe noch Windows Server 2016. Sehe ich dort überhaupt etwas?

Die erweiterten Ereignisse mit Reason-ID sind für Windows 11 ab 24H2, Server 2025 sowie Server 2022 und 2019 mit den Updates ab 13.10.2026 beschrieben. Auf älteren Systemen nutzt du die klassische Restrict-NTLM-Überwachung mit den Ereignissen 8001 bis 8004. Die liefern weniger Details, zeigen aber, dass und wohin NTLM läuft.

Muss ich für das Auditing etwas installieren?

Nein. Die erweiterten Ereignisse sind auf unterstützten Systemen standardmäßig aktiv und werden über Gruppenrichtlinien gesteuert. Sinnvoll ist, die Protokollgröße von Microsoft-Windows-NTLM/Operational zu erhöhen und die Ereignisse zentral zu sammeln.

Darf ich NTLM-Ereignisse einfach auswerten?

Technisch ja, organisatorisch kommt es darauf an. Die Ereignisse enthalten Benutzer- und Rechnernamen. Kläre Zweck, Aufbewahrung und gegebenenfalls die Mitbestimmung vorher, dann gibt es hinterher keine Diskussion.

Wie lange dauert eine NTLM-Ablösung?

Das hängt weniger von der Größe als von der Zahl der Altlasten ab. Das Erfassen dauert Tage bis wenige Wochen, das Umstellen kann bei Fachanwendungen und Medizintechnik Monate dauern, weil Hersteller beteiligt sind. Deshalb lohnt es sich, jetzt mit dem Erfassen anzufangen.

Fazit: Wer jetzt erfasst, hat am Stichtag Ruhe

Microsofts Fahrplan ist kein Überfall, sondern eine Ansage mit langem Vorlauf. Phase 1 gibt dir die Werkzeuge, um zu sehen, wo NTLM steckt. Phase 2 nimmt dir ein paar technische Ausreden ab. Phase 3 macht aus dem Rückfall-Protokoll eine bewusste Ausnahme. Und die NTLMv1-Sperre vom 13. Oktober hat gezeigt, wie sich das anfühlt, wenn man den Vorlauf verschlafen hat.

Der wichtigste Schritt kostet dich am wenigsten: hinschauen. Prüfe, ob das Auditing läuft, sammle die Ereignisse und verschaffe dir ein ehrliches Lagebild, bevor jemand anders den Stichtag für dich setzt. Den schnellsten Einstieg bietet die Express-Edition des NTLM Diagnostikers mit ihrem Fünf-Minuten-Befund. Danach weißt du, ob du ein Wochenendprojekt oder ein Jahresvorhaben vor dir hast. Beides ist in Ordnung. Nicht in Ordnung ist nur, es erst am Montag nach dem Server-Update zu erfahren.

Wenn dein Team die Ereignisse selbst sicher lesen und die Ursachen eigenständig abstellen soll, ist die Schulung zum NTLM Diagnostiker der passende nächste Schritt.

WEITERLESEN · Weiter in dieser Serie

› NTLM-Nutzung ermitteln: der komplette Leitfaden
› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM in der Klinik: Medizintechnik, Labor und Fachanwendungen