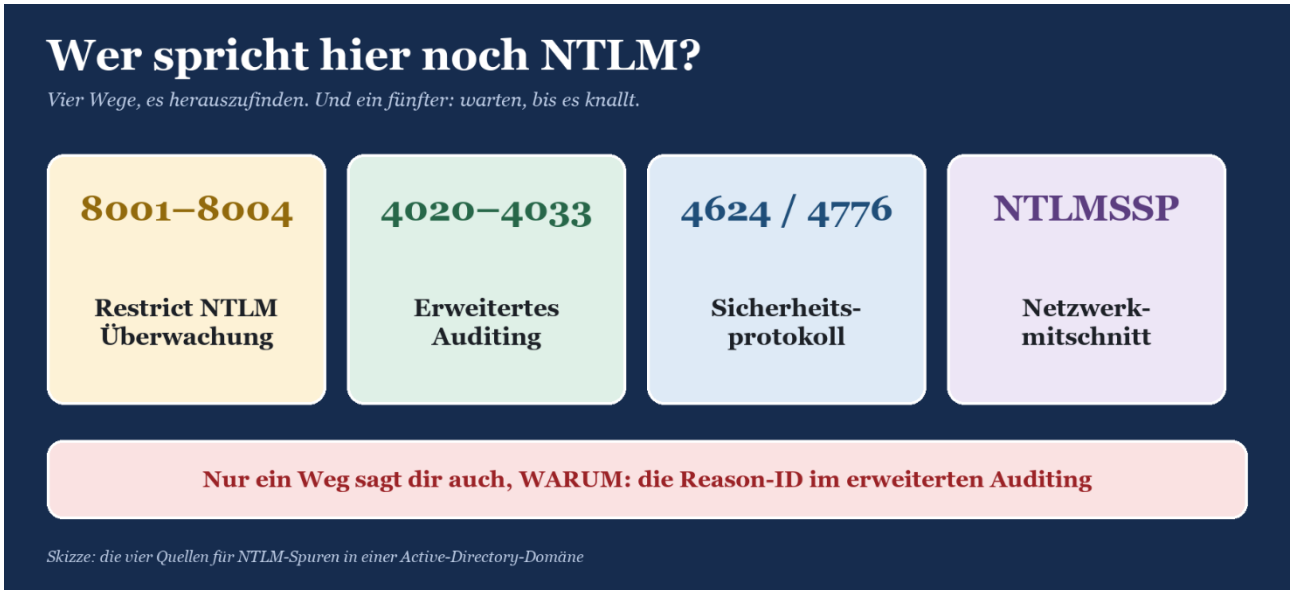
NTLM-Nutzung ermitteln: der komplette Leitfaden



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

BERATUNG
Bestandsaufnahme, Ursachenanalyse und Abschaltplan mit Begleitung.
› Beratung zur NTLM-Ablösung

SCHULUNG
NTLM-Ereignisse lesen, sammeln und bewerten: für dein ganzes Team.
› Schulung zum NTLM Diagnostiker

Frag zehn Administratoren, ob in ihrer Domäne noch NTLM läuft, und du bekommst zehnmal dieselbe Antwort: „Bestimmt, aber nicht viel." Das ist ungefähr so belastbar wie die Aussage eines Rauchers, er rauche „eigentlich kaum". NTLM steckt in Netzlaufwerken, die per IP-Adresse verbunden sind, in Dienstkonten aus dem Jahr 2011, im Scanner im Flur, in der Fachanwendung, deren Hersteller inzwischen zu einem Konzern gehört, der nicht mehr ans Telefon geht, und in Skripten, von denen niemand weiß, dass sie jede Nacht laufen.

Bisher war das ein Schönheitsfehler. Seit dem Windows-Update vom 13.10.2026 ist es ein Termin: Windows 11 ab 24H2 und Windows Server 2025 blockieren Single Sign-on mit NTLMv1-abgeleiteten Anmeldedaten standardmäßig, und mit der nächsten Windows-Server-Version will Microsoft NTLM insgesamt standardmäßig abschalten. Was das zeitlich bedeutet, steht in NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Hier geht es um die Frage davor: Wo genau wird in deiner Domäne NTLM benutzt, von wem, wohin und warum?

Die gute Nachricht: Windows bringt alles mit, was du für die Antwort brauchst. Die schlechte: Es verteilt diese Antwort auf vier verschiedene Quellen, drei Rollen, zwei Generationen von Ereignissen und ein paar Tausend Protokolleinträge pro Tag. Dieser Leitfaden sortiert das. Du erfährst, was jeder Weg zeigt und was nicht, wie du in fünf Schritten zu einem belastbaren Befund kommst und an welcher Stelle Bordmittel aufhören, Spaß zu machen.

FAKTEN · NTLM-Nutzung ermitteln: die Quellen auf einen Blick

Klassische Restrict-NTLM-Überwachung: Ereignisse 8001 bis 8004 im Protokoll Microsoft-Windows-NTLM/Operational. Funktioniert auch auf älteren Windows-Versionen, liefert aber keine Ursache.

Erweitertes NTLM-Auditing nach Microsoft KB5064479: Ereignisse 4020 bis 4023 auf Clients und Servern, 4030 bis 4033 auf Domain Controllern, im selben Protokoll. Verfügbar auf Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026.

Nur die ausgehenden Client-Ereignisse 4020 und 4021 enthalten eine Reason-ID von 0 bis 11, die erklärt, warum Kerberos nicht benutzt wurde.

Sicherheitsprotokoll: Anmeldeereignis 4624 mit Authentifizierungspaket NTLM und Paketname (NTLM V1 oder NTLM V2), auf Domain Controllern 4776 für die Anmeldedatenprüfung.

Netzwerkmitschnitt: NTLMSSP-Nachrichten im Datenverkehr, die einzige Quelle für Geräte, die selbst kein Windows-Ereignisprotokoll führen.

Warum NTLM so schwer zu finden ist

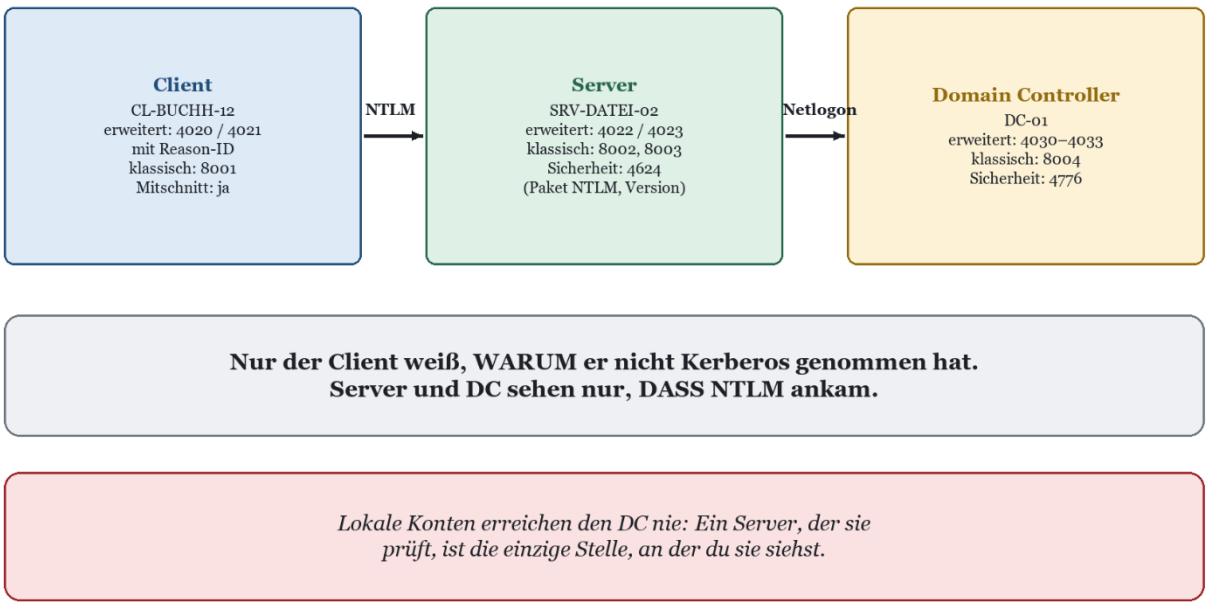
NTLM ist kein Dienst, den du in einer Liste abhakst. Es ist ein Rückfallverfahren. Windows versucht bei einer Domänenanmeldung zuerst Kerberos, und nur wenn das nicht klappt, verhandelt das Paket Negotiate still und leise auf NTLM herunter. Niemand bekommt eine Meldung, niemand wartet länger, alles funktioniert. Genau das ist das Problem: Was funktioniert, fällt nicht auf. NTLM ist der Mitbewohner, der nie Miete zahlt, aber auch nie Lärm macht. Bis der Vermieter vor der Tür steht.

Drei Rollen, drei Blickwinkel

An einer NTLM-Anmeldung in der Domäne sind drei Systeme beteiligt: der Client, der sich anmelden will, der Server, auf den er zugreift, und der Domain Controller, der für den Server die Anmeldedaten prüft. Jeder dieser drei sieht etwas anderes und schreibt etwas anderes ins Protokoll. Wer nur auf den Domain Controllern schaut, verpasst alles, was mit lokalen Konten passiert. Wer nur auf Servern schaut, sieht nicht, welcher Prozess auf dem Client die Anmeldung ausgelöst hat. Und wer nur auf Clients schaut, hat hinterher sehr viele Clients.

Eine NTLM-Anmeldung, drei Tatorte

Musterwerk GmbH, musterwerk.local: Client, Server und Domain Controller schreiben jeweils ihre Sicht



Skizze: Ereignis-IDs nach Microsoft KB5064479; Hostnamen frei erfunden

Was du am Ende wissen willst

Bevor du anfängst, Ereignisse zu sammeln, lohnt sich ein Blick auf das Ziel. Eine brauchbare NTLM-Bestandsaufnahme beantwortet fünf Fragen. Jede Quelle beantwortet davon nur einen Teil, deshalb kombinierst du sie.

Frage	Warum sie wichtig ist	Beste Quelle
Wer? (Quellrechner, Konto)	Ohne Quelle keine Umstellung	4020/4021 auf dem Client, 4022/4023 auf dem Server, 8001 bis 8004
Wohin? (Zielsystem, Dienst)	Zeigt, welche Server Ausnahmen brauchen würden	4020/4021 (Target Machine), 4022/4023, 8004 auf dem DC
Warum? (Ursache)	Entscheidet zwischen DNS-Eintrag, SPN-Korrektur und Herstelleranruf	nur 4020/4021 mit Reason ID
Welche Version?	NTLMv1 ist das dringendere Problem	erweitertes Auditing (NTLM Version), 4624 (Paketname), Mitschnitt
Was fehlt?	Stille Rechner und Geräte sind die Ausfälle von morgen	Abgleich mit dem Bestand, Netzwerkmitschnitt

WICHTIG · Erst messen, dann abschalten

Die Richtlinie „Netzwerksicherheit: NTLM einschränken“ kennt neben Überwachen auch Verweigern. Wer sie ohne Bestandsaufnahme auf Verweigern stellt, ermittelt die NTLM-Nutzung auch, nur eben über das Ticketsystem und den Flurfunk. Das ist die teuerste Messmethode, die es gibt. Wie die Richtlinien zusammenspielen, steht weiter unten.

Details zu Überwachen, Ausnahmen und Verweigern findest du in Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern; wie du daraus einen sanften Abschaltpfad baust, zeigt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

Vier Wege, NTLM sichtbar zu machen

Jetzt wird es konkret. Es gibt vier Quellen, und keine davon ist überflüssig. Die Reihenfolge hier folgt dem Alter, nicht der Wichtigkeit.

Weg 1: klassische Restrict-NTLM-Überwachung (8001 bis 8004)

Seit Windows 7 und Windows Server 2008 R2 gibt es in den Sicherheitsoptionen der Gruppenrichtlinie die Familie „Netzwerksicherheit: NTLM einschränken“. Drei dieser Richtlinien haben einen Überwachungsmodus, und genau den nutzt du zur Bestandsaufnahme. Sie verweigern nichts, sie schreiben nur auf, was sie verweigern würden.

Ereignis	Wo	Auslösende Richtlinie (Überwachungsmodus)	Was es zeigt
8001	Client	NTLM einschränken: Ausgehender NTLM-Datenverkehr zu Remoteservern = Alle überwachen	Ausgehende NTLM-Anmeldung, Zielserver, Konto, Prozess
8002	Server	NTLM einschränken: Eingehenden NTLM-Datenverkehr überwachen	Eingehende NTLM-Anmeldung, auch mit lokalen Konten
8003	Server	NTLM einschränken: Eingehenden NTLM-Datenverkehr überwachen	Eingehende NTLM-Anmeldung mit Domänenkonten
8004	Domain Controller	NTLM einschränken: NTLM-Authentifizierung in dieser Domäne überwachen	Vom DC geprüfte NTLM-Anmeldung, Server, Konto, Quellrechner

Der große Vorteil: Das funktioniert praktisch überall, auch auf Windows 10, Server 2016 und der Maschine im Keller, deren Update-Stand du lieber nicht wissen willst. Der große Nachteil: Die Ereignisse sagen dir, dass NTLM benutzt wurde, aber nie, warum. Ob dahinter ein fehlender SPN, eine IP-Adresse im Laufwerkspfad oder eine Anwendung steckt, die NTLM fest einprogrammiert hat, musst du selbst herausfinden. Mit Detektivarbeit, Kaffee und gelegentlich Tränen.

TIPP · 8004 ist der beste Einstieg

Wenn du nur an einer Stelle anfangen willst, dann bei 8004 auf den Domain Controllern. Ein Gruppenrichtlinienobjekt, wenige Maschinen, und du siehst jede NTLM-Anmeldung mit Domänenkonto, die über einen DC geprüft wird. Lokale Konten fehlen allerdings, und die Ursache auch. Was in 8004 und den neuen DC-Ereignissen steht, beschreibt NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

Weg 2: erweitertes NTLM-Auditing (4020 bis 4033)

Mit KB5064479 hat Microsoft das NTLM-Auditing grundlegend erweitert. Die neuen Ereignisse landen ebenfalls in Microsoft-Windows-NTLM/Operational und sind deutlich gesprächiger als ihre Vorgänger. Gesteuert werden sie über zwei administrative Vorlagen: „NTLM Enhanced Logging“ unter System, NTLM für Clients und Server sowie „Log Enhanced Domain-wide NTLM Logs“ unter System, Netlogon für Domain Controller. Wie du beides per Gruppenrichtlinie ausrollst, zeigt Erweitertes NTLM-Auditing einschalten: Schritt für Schritt; wer nicht klicken will, nimmt das NTLM-Audit-GPO-Skript.

Ereignis	Ebene	Rolle	Bedeutung
4020	Information	Client	Ausgehende NTLM-Anmeldung an eine entfernte Ressource
4021	Warnung	Client	wie 4020, aber als Sicherheitsabstufung markiert, etwa NTLMv1
4022	Information	Server	Ein entfernter Client hat sich per NTLM angemeldet
4023	Warnung	Server	wie 4022, als Abstufung markiert
4030	Information	Domain Controller	Weitergeleitete NTLM-Anfrage aus einer anderen Domäne
4031	Warnung	Domain Controller	wie 4030, als Abstufung markiert
4032	Information	Domain Controller	Weitergeleitete NTLM-Anfrage aus derselben Domäne
4033	Warnung	Domain Controller	wie 4032, als Abstufung markiert

Der eigentliche Schatz steckt in den Client-Ereignissen 4020 und 4021. Dort stehen neben Process Name, Username und Target Machine auch „Reason ID“ und „Reason“, also der Grund, warum Windows nicht Kerberos genommen hat. Dazu kommen in allen Ereignissen Sicherheitsangaben wie „NTLM Version“, „Channel Binding“ und „MIC Status“. Was die ausgehende Seite im Detail verrät, steht in Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen, die Serverseite in Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern.

Die Reason-IDs: endlich ein Warum

Zwölf Werte, und jeder davon führt zu einer anderen Baustelle. Das ist der Unterschied zwischen „Da ist NTLM“ und „Da ist NTLM, weil das Laufwerk über eine IP-Adresse verbunden ist“. Der erste Satz erzeugt ein Meeting, der zweite ein Ticket.

Reason ID	Bedeutung nach KB5064479	Typische Abhilfe
0	Unbekannter Grund	Mitschnitt oder Prozessanalyse
1	Anwendung ruft NTLM direkt auf	Hersteller fragen, Negotiate verlangen

2	Anmeldung mit lokalem Konto	Domänen- oder Dienstkonto verwenden
3	reserviert, nicht verwendet	–
4	Anmeldung mit Cloud-Konto	Szenario prüfen
5	Zielname fehlt oder ist leer	Anwendung bzw. Aufruf korrigieren
6	Zielname weder per Kerberos noch anders auflösbar	SPN und DNS prüfen
7	Zielname enthält eine IP-Adresse	auf DNS-Namen umstellen
8	Zielname in Active Directory doppelt vorhanden	doppelten SPN bereinigen
9	keine Sichtverbindung zu einem Domain Controller	Netzpfad, künftig IAKerb und lokales KDC
10	Aufruf über die Loopback-Schnittstelle	lokalen Zugriff prüfen
11	Aufruf mit Nullsitzung	anonymen Zugriff abschaffen

Zu den häufigsten Fällen gibt es eigene Beiträge: NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen, Reason-ID 6: wenn der Zielname nicht auflösbar ist, Doppelte SPNs im NTLM-Audit: Reason-ID 8 richtig deuten und Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden. Die Gesamtschau aller Werte liefert NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat. Und weil Reason-ID 6 und 8 fast immer bei Kerberos enden, lohnt bei der Fehlersuche ein Blick in den Kompetenzbereich Microsoft Kerberos.

WARNUNG · Kein Update, keine Reason-ID

Das erweiterte Auditing gibt es nur auf Windows 11 24H2, 25H2, 26H1 und 26H2, auf Windows Server 2025 und auf Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026. Ein Windows 10, ein Server 2016 oder ein Server 2019 ohne aktuelle Updates schreibt kein einziges 4020. Dort bleibt dir nur 8001 bis 8004, und damit keine Ursache. Ein leeres Protokoll auf so einem System ist kein Freispruch, sondern Schweigen aus Unvermögen.

Weg 3: das Sicherheitsprotokoll

Das Sicherheitsprotokoll protokolliert NTLM schon seit Ewigkeiten mit, man muss nur wissen, wo. Auf dem Server zeigt Ereignis 4624 (erfolgreiche Anmeldung) im Feld „Authentifizierungspaket“ den Wert NTLM und im Feld „Paketname (nur NTLM)“ die Version, also NTLM V1 oder NTLM V2. Auf dem Domain Controller zeigt 4776, dass er Anmeldedaten für ein Konto geprüft hat. Voraussetzung ist eine Überwachungsrichtlinie, die Anmeldungen und Anmeldeinformationsüberprüfung erfasst; in den meisten Domänen ist das ohnehin der Fall.

```
# NTLMv1-Anmeldungen der letzten 24 Stunden auf diesem Server
$xp = "*[System[EventID=4624]] and *[EventData[Data[@Name='LmPackageName']='NTLM V1']]"
Get-WinEvent -LogName Security -FilterXPath $xp -MaxEvents 500 |
  Where-Object TimeCreated -gt (Get-Date).AddDays(-1) |
  Select-Object TimeCreated, @{n='Text';e={$_.Message.Split("`n")[0]}}
```

Das Sicherheitsprotokoll ist der Weg für alte Server, die weder erweitertes Auditing noch gepflegte Restrict-NTLM-Richtlinien haben, und für die schnelle NTLMv1-Prüfung. Seine Schwächen: Es ist laut, es rotiert schnell, es kennt keine Ursache und keinen Clientprozess, und es ist voll mit Dingen, die nichts mit NTLM zu tun haben. Auf einem Domain Controller mit ein paar Hundert Benutzern hält es manchmal keine sechs Stunden durch.

Weg 4: der Netzwerkmitschnitt

Und dann gibt es noch die Geräte, die einfach nichts protokollieren: das NAS aus dem Elektronikmarkt, der Multifunktionsdrucker, der Scans per SMB in eine Freigabe schiebt, die Laborsteuerung mit eingebettetem Linux. Die siehst du nur auf dem Server, auf den sie zugreifen, oder im Netzwerkverkehr. In Wireshark filterst du mit „ntlmssp“ auf die NTLM-Nachrichten; die dritte Nachricht (AUTHENTICATE) enthält Benutzer, Domäne und Rechnername der Gegenstelle, und an der Länge der Antwort erkennst du NTLMv1 oder NTLMv2.

Der Mitschnitt ist der einzige Weg, der wirklich alles sieht, was über das Kabel geht, aber nur an dieser einen Stelle und nur in diesem einen Zeitraum. Für eine flächendeckende Bestandsaufnahme ist er ungeeignet, als Lupe für die letzten Unbekannten unschlagbar. Wie du ihn sauber aufsetzt, steht in NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen; welche Geräteklassen typischerweise auffallen, in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

Die vier Wege im direkten Vergleich

Was sieht welcher Weg?

grün = vollständig, gelb = teilweise, rot = gar nicht

	Restrict NTLM 8001–8004	Erweitert 4020–4033	Sicherheit 4624 / 4776	Mitschnitt Wireshark
Dass NTLM benutzt wurde	ja	ja	ja	ja
NTLM-Version (v1 oder v2)	nein	ja	ja	ja
Ursache (Reason-ID)	nein	teils	nein	nein
Prozess auf dem Client	teils	ja	nein	nein
Alte Systeme ohne Updates	ja	nein	ja	ja
Geräte ohne Windows	teils	teils	teils	ja
Aufwand im Großen	teils	teils	teils	nein

Skizze: vereinfachte Bewertung; Reason-ID gibt es nur in 4020 und 4021 auf dem Client

Kriterium	8001–8004	4020–4033	Sicherheitsprotokoll	Mitschnitt
Systemvoraussetzung	ab Windows 7 / Server 2008 R2	Windows 11 ab 24H2, Server 2025, Server 2022/2019 mit Updates ab 13.10.2026	alle Windows-Versionen	Spiegelport oder Mitschnitt auf dem Server
Einrichtung	Gruppenrichtlinie, Sicherheitsoptionen	Gruppenrichtlinie, administrative Vorlagen	Überwachungsrichtlinie	Wireshark oder pktmon
Ursache	nein	ja, Reason-ID auf dem Client	nein	nur indirekt
NTLM-Version	nein	ja	ja (4624)	ja
Clientprozess	teilweise	ja (Process Name)	nein	nein
Lokale Konten	ja, auf dem Server	ja	ja, auf dem Server	ja

	(8002)			
Geräte ohne Windows	nur als Ziel- oder Quelladresse	nur als Gegenstelle	nur als Gegenstelle	ja
Datenmenge	mittel	hoch	sehr hoch	sehr hoch, punktuell

WICHTIG · Personenbezogene Daten im Spiel

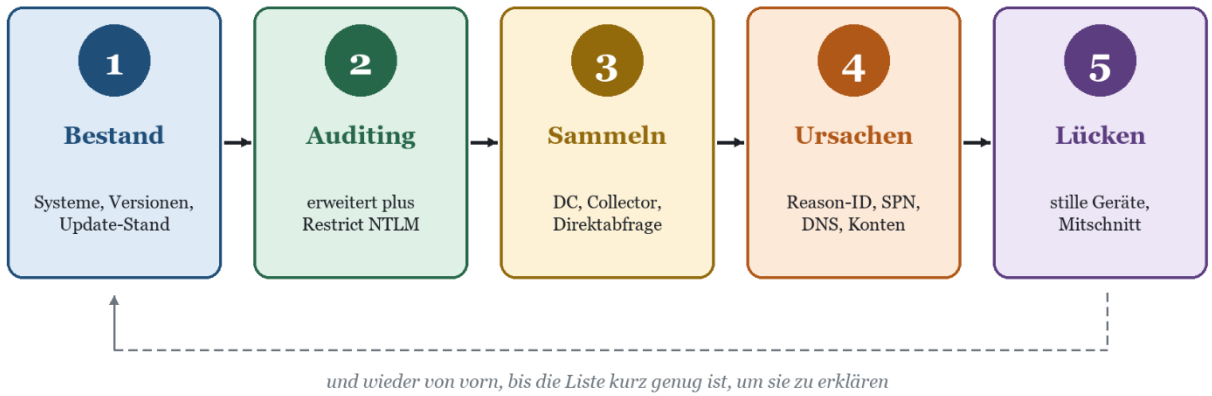
Alle vier Wege erfassen Benutzernamen, Rechnernamen und Zeitstempel. Bevor du flächendeckend sammelst, kläre Zweck, Aufbewahrungsdauer und Zugriff, und sprich bei Bedarf mit dem Betriebsrat. Worauf es dabei ankommt, beschreibt NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

NTLM-Nutzung ermitteln in fünf Schritten

Genug Theorie. So kommst du in einer realistischen Umgebung vom Bauchgefühl zu einem Befund, den du einer IT-Leitung vorlegen kannst, ohne rot zu werden.

Fünf Schritte vom Bauchgefühl zum Befund

Trendforge Digital GmbH, trendforge.local: so sah der Ablauf nach drei Wochen aus



Skizze: Ablauf der NTLM-Bestandsaufnahme; Firmenname frei erfunden

Schritt 1: Bestand und Versionen erfassen

Bevor du ein einziges Ereignis liest, musst du wissen, welche Rechner überhaupt welche Ereignisse schreiben können. Die Betriebssystemversion steht im Computerkonto, der Update-Stand leider nicht. Für die Version reicht eine Zeile:

```
Get-ADComputer -Filter 'Enabled -eq $true' -Properties OperatingSystem, OperatingSystemVersion,
  LastLogonTimestamp | Group-Object OperatingSystem | Sort-Object Count -Descending |
  Select-Object Count, Name
```

Aus dieser Liste ergibt sich, wo du dich auf erweitertes Auditing verlassen kannst und wo du 8001 bis 8004 brauchst. Die Rechner mit uraltem LastLogonTimestamp sortierst du gleich mit aus: Sie verfälschen sonst später jede Abdeckungsquote.

Schritt 2: Auditing per Gruppenrichtlinie einschalten

Aktiviere beides parallel: das erweiterte Auditing für die Systeme, die es können, und die Restrict-NTLM-Überwachung für alle. Die Kombination kostet nichts außer Protokollplatz und schließt die

Lücke bei alten Systemen. Vergrößere bei der Gelegenheit das Protokoll Microsoft-Windows-NTLM/Operational, sonst rotiert es dir unter den Händen weg:

```
wevtutil gl Microsoft-Windows-NTLM/Operational
wevtutil sl Microsoft-Windows-NTLM/Operational /ms:104857600
```

TIPP · Erst DC, dann Server, dann Clients

Fang auf den Domain Controllern an, dann die Server, dann eine Pilotgruppe von Clients. So hast du nach einem Tag einen ersten Eindruck, ohne gleich auf 800 Rechnern das Protokoll vollzuschreiben. Die Reason-IDs aus 4020 kommen aber nur von Clients; ohne Clients bleibt das Warum offen.

Schritt 3: Ereignisse sammeln

Für einen einzelnen Rechner genügt die Ereignisanzeige oder eine PowerShell-Abfrage. Die folgenden Zeilen zählen die Ereignisse des erweiterten und klassischen Auditings der letzten sieben Tage:

```
Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational';
  Id=4020,4021,4022,4023,4030,4031,4032,4033,8001,8002,8003,8004;
  StartTime=(Get-Date).AddDays(-7) } -ErrorAction SilentlyContinue |
  Group-Object Id | Sort-Object Name | Select-Object Name, Count
```

Für eine ganze Domäne brauchst du eine zentrale Sammlung. Der Standardweg ist Windows Event Forwarding mit einem Collector, der die Ereignisse per Abonnement einsammelt. Wie das geht, beschreibt NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding. Alternativ fragst du die Domain Controller direkt ab und holst Client-Ereignisse gezielt per Remote-Abfrage, was bei wenigen Hundert Rechnern noch geht, bei Notebooks im Homeoffice aber zur Geduldsprobe wird.

Schritt 4: nach Ursache verdichten

Jetzt hast du Tausende Zeilen. Daraus wird erst ein Befund, wenn du sie nach Quelle, Ziel und Grund gruppierst. Bei 4020 und 4021 stehen „Reason ID“ und „Target Machine“ im Meldungstext; mit etwas Textverarbeitung kommst du an beides heran:

```
Get-WinEvent -FilterHashtable @{ LogName='Microsoft-Windows-NTLM/Operational'; Id=4020,4021 } |
  ForEach-Object {
    $m = $_.Message
    [pscustomobject]@{
      Rechner = $_.MachineName
      Ziel    = ([regex]::Match($m, 'Target Machine:\s*(\S+)')).Groups[1].Value
      Reason  = ([regex]::Match($m, 'Reason ID:\s*(\d+)')).Groups[1].Value
    } } | Group-Object Reason, Ziel | Sort-Object Count -Descending | Select-Object -First 25
```

Die Musterzeilen gehen von englischem Meldungstext aus; auf deutsch lokalisierten Systemen passt du die Suchmuster an. Und dann beginnt die eigentliche Arbeit: Für jede Reason-ID 6 prüfst du mit setspn -Q und nslookup, ob SPN und DNS-Eintrag stimmen. Für jede 8 suchst du mit setspn -X den doppelten SPN. Für jede 7 suchst du das Laufwerk, die Verknüpfung oder das Skript mit der IP-Adresse. Für jede 1 rufst du einen Hersteller an.

```
setspn -Q cifs/srv-datei-02.musterwerk.local
setspn -X -F
nslookup srv-datei-02.musterwerk.local
```

Schritt 5: Lücken schließen

Der gefährlichste Teil deines Befunds ist der, der fehlt. Gleiche die Liste der Rechner, die Ereignisse geliefert haben, mit dem aktiven Bestand aus Schritt 1 ab. Jeder Rechner ohne

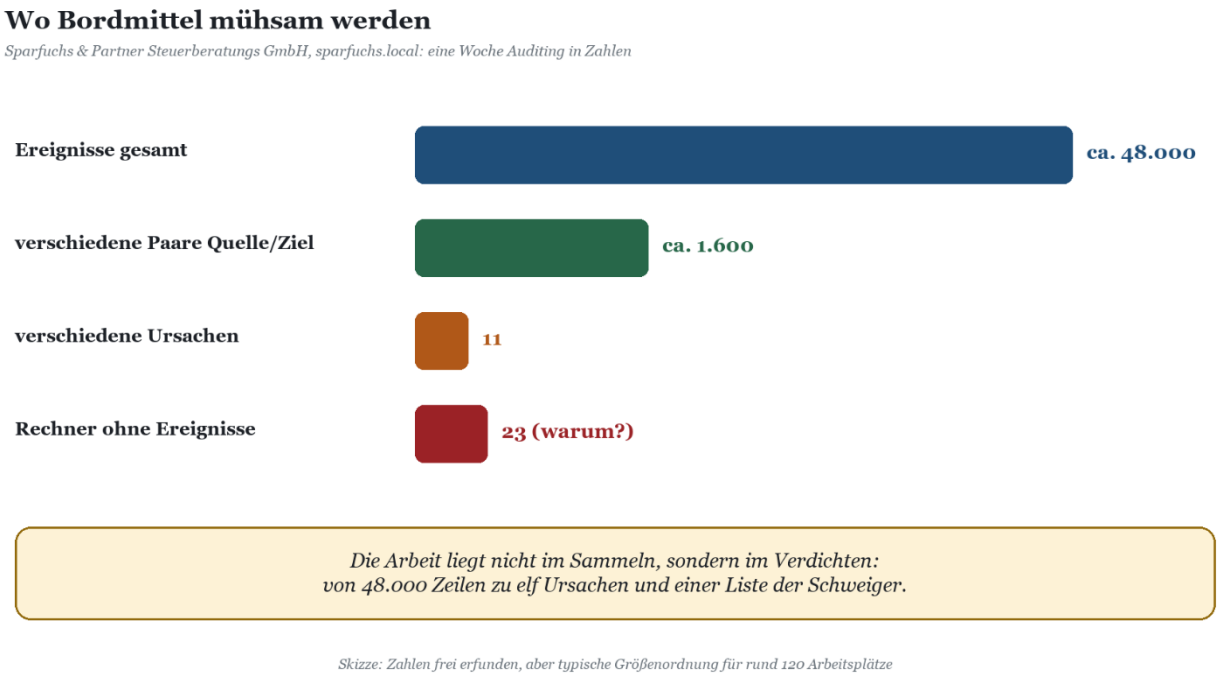
Ereignisse ist entweder sauber, ausgeschaltet, falsch konfiguriert oder zu alt für das erweiterte Auditing. Nur die erste Variante ist erfreulich, und sie ist seltener, als man hofft. Für Geräte ohne Windows nimmst du dir die Server vor, auf die sie zugreifen (4022, 8002, 4624), und wo das nicht reicht, den Mitschnitt.

AUS DER PRAXIS · Musterwerk GmbH: der Scanner, den keiner kannte

Nach zwei Wochen Auditing war die Liste bei Musterwerk überschaubar: 14 Ursachen, die meisten Reason-ID 7 aus einem Anmeldeskript mit einer IP-Adresse. Erst der Abgleich der Serverereignisse 4022 auf dem Dateiserver zeigte eine Gegenstelle, die in keinem Client-Ereignis auftauchte: ein Multifunktionsgerät in der Versandhalle, das Scans mit einem lokalen Konto und NTLMv1 in eine Freigabe schob. Der Mitschnitt bestätigte es in fünf Minuten. Ohne Schritt 5 hätte das Gerät am Tag der Abschaltung als Erstes aufgegeben, und zwar vor dem Versand der Monatsrechnungen.

Wo Bordmittel an ihre Grenzen kommen

Alles bis hierher geht mit Bordmitteln. Ehrlich, ohne Haken. Bei 30 Rechnern und einem Dateiserver bist du damit an einem Nachmittag fertig. Bei 300 Rechnern, vier Standorten und einer Klinik-IT mit Medizintechnik ändern sich die Verhältnisse. Dann ist nicht das Sammeln schwierig, sondern das Verdichten, das Abgleichen und das Erklären.



Die typischen Stolpersteine

- **Tausende Ereignisse:** Ein Dateiserver erzeugt pro Tag schnell fünfstellige Mengen. Wer sie per Regex aus Meldungstexten zieht, baut sich ein Skript, das bei der nächsten Sprachversion bricht.
- **Hunderte Maschinen:** Ereignisse entstehen verteilt. Ohne funktionierendes Event Forwarding fehlen dir genau die Notebooks, die nie im Büro sind.
- **Stille Geräte:** Was nichts protokolliert, steht in keiner Auswertung. Ohne Abgleich gegen den Bestand hältst du Schweigen für Sauberkeit.
- **Fehlende Ursache:** 8001 bis 8004 und das Sicherheitsprotokoll sagen nur „NTLM“. Die Ursache musst du für jede Kombination aus Quelle und Ziel von Hand ermitteln, mit setspn, nslookup und Geduld.

- **Bericht für die Leitung:** Eine CSV-Datei mit 1.600 Zeilen überzeugt niemanden. Eine Ampel pro Maschine schon.

Bordmittel und NTLM Diagnostiker im Vergleich

Genau für diese Verdichtungsarbeit ist der NTLM Diagnostiker gebaut. Er nutzt dieselben Quellen wie du, also die Ereignisse 4020 bis 4033 und 8001 bis 8004, und erspart dir das Kleben. Wichtig: Er arbeitet ausschließlich lesend. Er setzt keine Richtlinie, ändert keinen SPN und fasst kein Konto an. Die Entscheidungen bleiben bei dir.

Aufgabe	Mit Bordmitteln	Mit dem NTLM Diagnostiker
Ereignisse sammeln	WEF einrichten oder Skript je Rechner	DC direkt, vorhandener Windows Event Collector oder Direktabfrage
Abdeckung prüfen	eigener Abgleich mit Get-ADComputer	Abdeckungsmonitor und OS-Landkarte
Ursache bestimmen	Reason-ID per Regex, setspn und nslookup von Hand	Ursachen-Engine mit SPN- und DNS-Prüfung
NTLMv1 finden	4624-Filter, 4021/4023 einzeln auswerten	NTLMv1-Hitliste
Wer mit wem?	Group-Object und Excel-Pivot	Kommunikationsmatrix und Konten-Sicht
Auffällige Sicherheitsmerkmale	Felder wie MIC Status einzeln lesen	Sicherheitsflaggen
Geräte ohne Ereignisprotokoll	Wireshark und Handarbeit	Wireshark-Import
Was passiert beim Abschalten?	Pilotgruppe und hoffen	Abschalt-Simulation
Ergebnis für die Leitung	Word und Excel von Hand	Readiness-Ampel, Word-Bericht, Excel/CSV-Export
Kosten	keine Lizenz, viel Zeit	Express kostenlos, sonst Lizenz pro aktivem Computerkonto

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Die NTLM-Bestandsaufnahme in einem Durchgang

Fünf-Minuten-Befund: Die kostenlose Edition Express verschafft dir einen ersten Überblick, ohne dass du vorher ein Projekt aufsetzen musst. Die Vollversion kannst du 7 Tage testen.

Quellen wählen: Ereignisse direkt von den Domain Controllern, von einem vorhandenen Windows Event Collector oder per Direktabfrage der Rechner. Schon eingerichtetes Event Forwarding wird also weiterverwendet.

Lücken sehen: Abdeckungsmonitor und OS-Landkarte zeigen, welche Rechner liefern, welche schweigen und welche wegen ihrer Windows-Version gar keine erweiterten Ereignisse schreiben können.

Ursachen verstehen: Die Ursachen-Engine wertet die Reason-IDs aus und prüft SPN und DNS. Die NTLMv1-Hitliste, die Kommunikationsmatrix und die Konten-Sicht zeigen, wer mit wem spricht, Sicherheitsflaggen markieren Auffälligkeiten. Für stille Geräte liest der Wireshark-Import Mitschnitte ein.

Entscheiden: Die Abschalt-Simulation zeigt, was eine Sperre treffen würde, die Readiness-Ampel fasst den Stand je Maschine zusammen. Word-Bericht und Excel/CSV-Export liefern die Unterlagen. Ein Anwendungskatalog, ein Ausnahmelisten- und Skript-Generator, ein Phasenplan, ein Kerberos-Gegencheck und ein Verlauf sind geplant, aber noch nicht enthalten.

Und das Wichtigste: Alles passiert lesend. Der Diagnostiker ändert nichts an deiner Domäne.

› NTLM Diagnostiker

Wenn du die Bestandsaufnahme nicht allein stemmen willst oder einen zweiten Blick auf die Ergebnisse brauchst, begleiten wir dich in der Beratung zur NTLM-Ablösung. Wie du das Ganze als Projekt mit Rollen und Zeitplan aufziehst, beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand. Einen ausführlicheren Werkzeugvergleich findest du in NTLM-Analyse im Vergleich: Bordmittel, Skripte und NTLM Diagnostiker.

FAQ: NTLM-Nutzung ermitteln

Wie kann ich die NTLM-Nutzung in meiner Domäne am schnellsten ermitteln?

Schalte auf den Domain Controllern die Überwachung „NTLM-Authentifizierung in dieser Domäne überwachen“ ein und werte Ereignis 8004 aus. Das liefert in kurzer Zeit einen Überblick über Domänenkonten. Für Ursachen brauchst du zusätzlich das erweiterte Auditing auf den Clients.

Wo finde ich die NTLM-Ereignisse in der Ereignisanzeige?

Unter Anwendungs- und Dienstprotokolle, Microsoft, Windows, NTLM, Operational. Dort landen sowohl 8001 bis 8004 als auch 4020 bis 4033. Das Sicherheitsprotokoll enthält zusätzlich 4624 und 4776.

Warum sehe ich keine Reason-ID?

Weil die Reason-ID nur in den Client-Ereignissen 4020 und 4021 steht und nur auf Systemen mit erweitertem Auditing: Windows 11 ab 24H2, Windows Server 2025 sowie Windows Server 2022 und 2019 mit Updates ab dem 13.10.2026. Server- und DC-Ereignisse enthalten keine Reason-ID.

Reicht es, nur die Domain Controller zu überwachen?

Für einen ersten Eindruck ja, für eine Abschaltung nein. Anmeldungen mit lokalen Konten erreichen den Domain Controller nie, und die Ursache steht nur auf dem Client.

Bremst das NTLM-Auditing meine Systeme aus?

Spürbar in der Regel nicht. Das eigentliche Thema ist die Datenmenge: Vergrößere das Protokoll Microsoft-Windows-NTLM/Operational und sammle zentral, bevor die Einträge rotieren.

Wie finde ich NTLMv1 gezielt?

Über die Warnungen 4021, 4023, 4031 und 4033 mit dem Feld „NTLM Version“, über 4624 mit Paketname NTLM V1 und auf Windows 11 ab 24H2 über die Ereignisse 4024 und 4025, beschrieben in Ereignis 4024 und 4025: NTLMv1 im Protokoll erkennen. Was seit Oktober 2026 konkret blockiert wird, steht in NTLMv1 blockiert: was seit Oktober 2026 nicht mehr geht.

Was mache ich mit Geräten, die kein Windows-Protokoll haben?

Du suchst sie auf den Servern, auf die sie zugreifen, und im Netzwerkmitschnitt. Ein Filter auf „ntlmssp“ in Wireshark zeigt die NTLM-Nachrichten samt Benutzer und Rechnername.

Wo beschreibt Microsoft das erweiterte Auditing?

Im Supportartikel Overview of NTLM auditing enhancements in Windows 11 and Windows Server 2025. Dort stehen Ereignisse, Reason-IDs, Felder und Systemvoraussetzungen.

Darf ich NTLM-Ereignisse einfach zentral speichern?

Sie enthalten Benutzer- und Rechnernamen, also personenbezogene Daten. Was du mit Datenschutz und Betriebsrat klären solltest, steht in NTLM-Audit, Datenschutz und Betriebsrat: was du beachten musst.

Fazit: Wer NTLM abschalten will, muss es erst finden

NTLM-Nutzung ermitteln ist keine Raketenwissenschaft, sondern Fleißarbeit mit System. Die klassische Restrict-NTLM-Überwachung zeigt dir, dass NTLM benutzt wird, auch auf alten Systemen. Das erweiterte Auditing zeigt dir, warum, aber nur dort, wo es verfügbar ist. Das Sicherheitsprotokoll füllt Lücken bei alten Servern und bei NTLMv1, der Mitschnitt die Lücken bei Geräten ohne eigenes Protokoll. Keine Quelle allein reicht, alle zusammen schon.

Der eigentliche Feind ist nicht NTLM, sondern die Liste der Dinge, die du nicht siehst. Gleiche deshalb immer gegen den Bestand ab, und rechne damit, dass der letzte NTLM-Nutzer der ist, an den niemand gedacht hat. Er meldet sich nämlich garantiert. Am Tag nach der Abschaltung, um 7:45 Uhr, per Telefon, aus der Buchhaltung.

WEITERLESEN · Weiter in dieser Serie

› Erweitertes NTLM-Auditing einschalten: Schritt für Schritt
› Ereignis 4020 und 4021: ausgehende NTLM-Anmeldungen lesen
› Ereignis 4022 und 4023: eingehende NTLM-Anmeldungen auf Servern
› NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004
› NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat
› NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding
› NTLM im Netzwerkmitschnitt finden: Wireshark richtig einsetzen
› Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern
› NTLM schrittweise abschalten, ohne dass etwas ausfällt
› NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet