Restrict-NTLM-Richtlinien erklärt: Überwachen, Ausnahmen, Verweigern



WISSEN
Wie der NTLM Diagnostiker die aktuellen Restrict-NTLM-Werte zeigt und Widersprüche zwischen Richtlinien sichtbar macht.
› NTLM Diagnostiker

BERATUNG
Richtlinien, Ausnahmen und GPO-Struktur für die NTLM-Ablösung planen, bevor das erste Verweigern scharf geschaltet wird.
› Beratung zur NTLM-Ablösung

SCHULUNG
Restrict-NTLM-Richtlinien, Ereignisse und Ausnahmen verstehen, statt sie nach Bauchgefühl zu setzen.
› Schulung zum NTLM Diagnostiker

In jeder Gruppenrichtlinienverwaltung gibt es einen Ordner, der aussieht wie ein harmloser Abstellraum: Computerkonfiguration, Richtlinien, Windows-Einstellungen, Sicherheitseinstellungen, Lokale Richtlinien, Sicherheitsoptionen. Darin stehen sieben Einträge, die alle mit „Netzwerksicherheit: NTLM einschränken" beginnen. Sie sehen unscheinbar aus. Tatsächlich ist es der Sicherungskasten des Gebäudes, nur ohne Beschriftung, und irgendwer hat vor Jahren einen Zettel „Nicht anfassen" draufgeklebt, der inzwischen abgefallen ist.

Wer heute NTLM einschränken will, per GPO und mit Plan, kommt an diesen Optionen nicht vorbei. Der Druck ist real: Seit dem Windows-Update vom 13.10.2026 blockieren Windows 11 ab 24H2 und Windows Server 2025 NTLMv1 für Single Sign-on standardmäßig. Phase 2 bringt IAKerb und ein lokales KDC, und mit der nächsten Windows-Server-Version ist NTLM standardmäßig abgeschaltet. Den gesamten Zeitplan erklärt NTLM-Abschaltung: Microsofts Fahrplan und was er für dich bedeutet. Die Restrict-NTLM-Richtlinien sind das Werkzeug, mit dem du diesen Weg selbst steuerst, statt ihn dir von einem Update diktieren zu lassen.

Dieser Beitrag ist die Referenz dazu: welche Richtlinie was tut, welche Werte es gibt, wo sie wirkt (Client, Server oder Domänencontroller), wie die beiden Ausnahmelisten funktionieren, warum Überwachen immer vor Verweigern kommt und an welchen Stellen die GPO-Rangfolge dir ein Bein stellt. Kurz: alles, was du wissen solltest, bevor du zum ersten Mal „Alle verweigern" auswählst und danach das Telefon klingelt.

FAKTEN · Restrict NTLM auf einen Blick

Pfad: Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen. Alle Optionen beginnen mit „Netzwerksicherheit: NTLM einschränken“.

Es gibt drei Verweigern-Richtlinien (ausgehend, eingehend, in dieser Domäne), zwei Überwachungs-Richtlinien (eingehend, in dieser Domäne) und zwei Ausnahmelisten (Remoteserver, Server in dieser Domäne). Ausgehend überwacht über den Wert „Alle überwachen“ der Verweigern-Richtlinie selbst.

Ein Neustart ist laut Microsoft nicht nötig, die Werte greifen nach der Gruppenrichtlinien-Aktualisierung.

Die Richtlinien „in dieser Domäne“ wirken nur auf Domänencontrollern.

Protokolliert wird im Kanal Microsoft-Windows-NTLM/Operational: klassisch mit 8001 bis 8004, mit erweitertem Auditing zusätzlich 4020 bis 4023 auf Clients und Servern sowie 4030 bis 4033 auf DCs.

Die sieben Sicherheitsoptionen im Überblick

Microsoft hat die Restrict-NTLM-Familie mit Windows 7 und Windows Server 2008 R2 eingeführt. Seitdem hat sich an Namen und Werten nichts geändert, was angesichts der sonstigen Umbenennungsfreude fast rührend ist. Geändert hat sich die Bedeutung: Was jahrelang ein Werkzeug für besonders vorsichtige Umgebungen war, wird jetzt zur Standardausrüstung jeder NTLM-Ablösung.

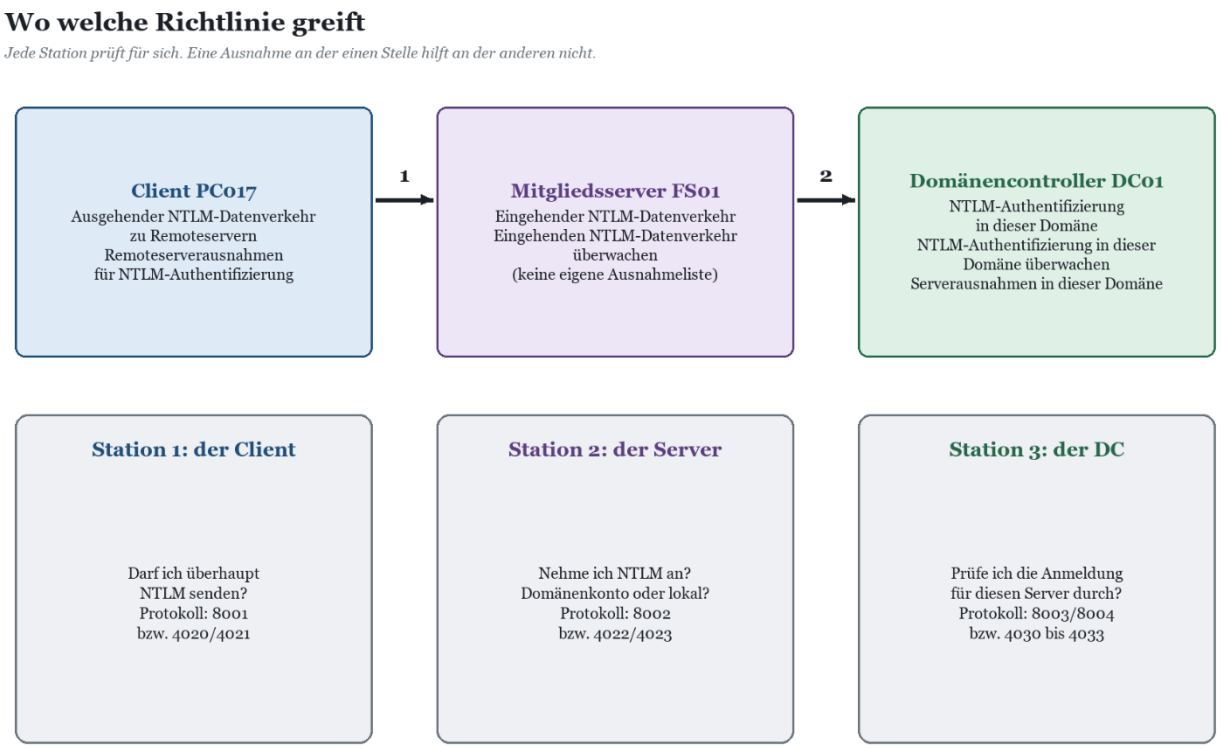
Werte, Registrierung und Wirkungsort

Die folgende Tabelle fasst alle sieben Optionen zusammen. Die deutschen Bezeichnungen stehen so in der Gruppenrichtlinienverwaltung, die Registrierungswerte helfen dir beim Prüfen auf einzelnen Geräten.

Richtlinie (NTLM einschränken: …)	Werte	Registrierungswert	Wirkt auf
Ausgehender NTLM-Datenverkehr zu Remoteservern	Alle zulassen (0) · Alle überwachen (1) · Alle verweigern (2)	MSV1_0\RestrictSendingNTLMTraffic	jedes Gerät, das sich als Client anmeldet, also auch Server und DCs
Remoteserverausnahmen für die NTLM-Authentifizierung hinzufügen	Liste von Servernamen, ein Name pro Zeile, Platzhalter *	MSV1_0\ClientAllowedNTLMServers	Client, nur zusammen mit der ausgehenden Richtlinie
Eingehender NTLM-Datenverkehr	Alle zulassen (0) · Alle Domänenkonten verweigern (1) · Alle Konten verweigern (2)	MSV1_0\RestrictReceivingNTLMTraffic	jedes Gerät, das NTLM annimmt: Server, aber auch Clients und DCs
Eingehenden NTLM-Datenverkehr überwachen	Deaktivieren (0) · Überwachung für Domänenkonten (1) · Überwachung	MSV1_0\AuditReceivingNTLMTraffic	jedes Gerät, das NTLM annimmt

	für alle Konten (2)		
NTLM-Authentifizierung in dieser Domäne	Deaktivieren (0) · Für Domänenkonten zu Domänenservern verweigern (1) · Für Domänenkonten verweigern (3) · Für Domänenserver verweigern (5) · Alle verweigern (7)	Netlogon\Parameters\RestrictNTLMInDomain	nur Domänencontroller
NTLM-Authentifizierung in dieser Domäne überwachen	Deaktivieren (0) · für Domänenkonten zu Domänenservern (1) · für Domänenkonten (3) · für Domänenserver (5) · Alle aktivieren (7)	Netlogon\Parameters\AuditNTLMInDomain	nur Domänencontroller
Serverausnahmen in dieser Domäne hinzufügen	Liste von Servernamen, ein Name pro Zeile, Platzhalter *	Netlogon\Parameters\DCAllowedNTLMServers	nur Domänencontroller, nur zusammen mit einer Verweigern-Option der Domänenrichtlinie

MSV1_0 steht für HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0, Netlogon\Parameters für HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters. Nicht konfiguriert entspricht in allen Fällen „Alle zulassen“ beziehungsweise „Deaktivieren“, und die Standardwerte sind auf Clients, Mitgliedsservern und DCs identisch: nicht definiert.



Skizze: Domänenkonto, NTLM-Durchreichung über den DC; Namen fiktiv

Eingehend: der Türsteher am Server

„Eingehender NTLM-Datenverkehr“ entscheidet auf dem Gerät, das eine NTLM-Anmeldung entgegennimmt. Das ist meist ein Dateiserver, ein Anwendungsserver oder ein Webserver, aber eben nicht nur: Auch ein Client mit administrativer Freigabe nimmt NTLM an, und ein DC sowieso. Mit „Alle Domänenkonten verweigern“ lehnt der Server NTLM für Domänenkonten ab, erlaubt aber weiterhin lokale Konten. „Alle Konten verweigern“ macht die Tür komplett zu, auch für den lokalen Administrator, mit dem jemand vor sechs Jahren ein Skript gebaut hat, das heute noch jede Nacht läuft. Welche Altlasten dieser Art typischerweise auftauchen, zeigt Lokale Konten und NTLM: Dienste, Aufgaben und Altlasten finden.

Die passende Überwachung heißt „Eingehenden NTLM-Datenverkehr überwachen“. Sie hat dieselbe Logik in zwei Stufen: nur Domänenkonten oder alle Konten. Wichtig ist der Satz, den man beim ersten Lesen überspringt: Für die eingehende Richtlinie gibt es keine Ausnahmeliste. Der Server lehnt ab, egal wer anklopft. Ausnahmen musst du hier über die GPO-Struktur abbilden, also indem du den betroffenen Server schlicht nicht in die Verweigern-GPO aufnimmst.

Ausgehend: der Client, der nicht mehr fragen darf

„Ausgehender NTLM-Datenverkehr zu Remoteservern“ wirkt auf der anderen Seite der Leitung. Mit „Alle überwachen“ protokolliert das Gerät jede NTLM-Anmeldung, die es an einen Remoteserver schickt, ohne sie zu blockieren. Mit „Alle verweigern“ schickt es gar keine mehr, außer an Server auf der Liste „Remoteserverausnahmen für die NTLM-Authentifizierung hinzufügen“. Der Vorteil: Du kannst NTLM auf den Clients abdrehen, auch wenn ein Teil der Ziele nicht unter deiner Kontrolle steht, etwa ein NAS, ein Drucker mit Scan-to-Folder oder ein Linux-System mit Samba. Wie du solche stillen Geräte überhaupt findest, steht in NAS, Drucker und Scanner: NTLM bei Geräten ohne Ereignisprotokoll.

Für das erweiterte Auditing liefern Clients ab Windows 11 24H2 außerdem die Ereignisse 4020 und 4021 mit Reason ID und Zielangaben; was darin steht, erklärt Ereignis 4020 und 4021:

ausgehende NTLM-Anmeldungen lesen. Die Restrict-Überwachung mit 8001 funktioniert dagegen auch auf älteren Systemen.

In dieser Domäne: das Hausrecht des Domänencontrollers

Die beiden Richtlinien „NTLM-Authentifizierung in dieser Domäne“ und die zugehörige Überwachung gelten nur auf Domänencontrollern. Sie greifen bei der NTLM-Durchreichung: Ein Mitgliedsserver bekommt eine NTLM-Anmeldung mit einem Domänenkonto, kann sie selbst nicht prüfen und reicht sie über den sicheren Kanal an einen DC weiter. Der DC entscheidet dann anhand dieser Richtlinie, ob er mitspielt. Interaktive Anmeldungen direkt am DC sind nach Microsoft-Dokumentation nicht betroffen.

Wert	Was der DC verweigert	Typischer Einsatz
Für Domänenkonten zu Domänenservern verweigern	NTLM-Anmeldungen mit Konten dieser Domäne an Server dieser Domäne	der klassische erste Schritt im eigenen Haus
Für Domänenkonten verweigern	NTLM-Anmeldungen mit Konten dieser Domäne, egal an welchem Server	wenn auch Server in vertrauten Domänen erfasst werden sollen
Für Domänenserver verweigern	NTLM-Anmeldungen an Server dieser Domäne, egal mit welchem Konto	Server schützen, auch vor Konten aus vertrauten Domänen
Alle verweigern	alle NTLM-Durchreichungen von seinen Servern und für seine Konten	Endzustand, nur mit gepflegter Serverausnahmeliste

Die Überwachungsrichtlinie spiegelt diese Werte exakt. Microsoft empfiehlt ausdrücklich, zuerst die Überwachung auf denselben Wert zu setzen, den du später verweigern willst. Dann zeigt das Protokoll genau die Anmeldungen, die es treffen würde. Wie du die Ereignisse 8004 und 4030 bis 4033 auf dem DC liest, beschreibt NTLM auf dem Domain Controller: Ereignisse 4030 bis 4033 und 8004.

WARNUNG · Eine Richtlinie pro DC ist keine Richtlinie für die Domäne

Die Domänenrichtlinien wirken auf genau dem DC, auf dem sie angewendet werden. Hat nur ein Teil der DCs den Wert, hängt das Ergebnis davon ab, welchen DC ein Server gerade über seinen sicheren Kanal erreicht. Das ergibt Fehler, die am Dienstag auftreten und am Mittwoch nicht, und die niemand reproduzieren kann. Verknüpfe die Domänenrichtlinien deshalb an der OU Domain Controllers und prüfe, dass wirklich alle DCs darin stehen, auch der in der Außenstelle.

Ausnahmen: Remoteserver und Server in dieser Domäne

Ausnahmen sind der Teil der Restrict-NTLM-Familie, an dem sich gute von schlechten Projekten unterscheiden. Eine Ausnahme ist ein bewusst offen gelassenes Fenster. Das ist in Ordnung, solange du weißt, welches Fenster es ist, warum es offen steht und wann es wieder zugeht. Es ist nicht in Ordnung, wenn die Liste irgendwann „*“ enthält, weil das am Freitagnachmittag am schnellsten ging.



*Skizze: Namen fiktiv; Platzhalter * an beliebiger Stelle zulässig*

Syntax: Namen, Platzhalter, ein Eintrag pro Zeile

Beide Listen sind mehrzeilige Werte. Microsoft nennt als Format den NetBIOS-Namen des Servers, einen Eintrag pro Zeile, und erlaubt einen Stern als Platzhalter an beliebiger Stelle. Entscheidend ist der Hinweis bei den Remoteserverausnahmen: Es müssen die Namen eingetragen werden, die die Anwendungen tatsächlich verwenden. Ruft eine Anwendung den Server per vollqualifiziertem Namen oder per Alias auf, gehört genau diese Schreibweise in die Liste. Im Zweifel trägst du beide Varianten ein und prüfst im Protokoll, welche gegriffen hat.

```
FS01
fs01.musterwerk.local
scan*
ERP01
```

Ein Zugriff per IP-Adresse ist übrigens fast nie ein Fall für die Ausnahmeliste, sondern ein Fall für den Rotstift: Mit IP-Adresse gibt es kein Kerberos-Ticket, also landet der Zugriff bei NTLM. Wie du Laufwerke und Skripte umstellst, zeigt NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen.

Welche Liste wofür gilt

Merkmal	Remoteserverausnahmen	Serverausnahmen in dieser Domäne
Wo konfiguriert	auf Clients und allen Geräten, die als Client auftreten	auf Domänencontrollern
Gehört zu	Ausgehender NTLM-Datenverkehr zu Remoteservern	NTLM-Authentifizierung in dieser Domäne
Eintrag meint	das Ziel, zu dem der Client NTLM senden darf	den Server, dessen NTLM-Durchreichung der DC weiter annimmt
Hilft bei Eingehend-Verweigern am Server?	nein	nein
Wirkung ohne Verweigern	keine, solange ausgehend nicht verweigert	keine, solange die Domänenrichtlinie nicht verweigert

TIPP · Jede Ausnahme braucht drei Angaben

Halte zu jedem Eintrag fest: wer ihn verantwortet, warum er nötig ist (Anwendung, Gerät, Reason ID) und bis wann er gelten soll. Die Gruppenrichtlinie selbst kennt keine Kommentare, also gehört die Begründung in eine Tabelle neben der GPO. Ohne Ablaufdatum wird aus der Übergangslösung zuverlässig ein Denkmal.

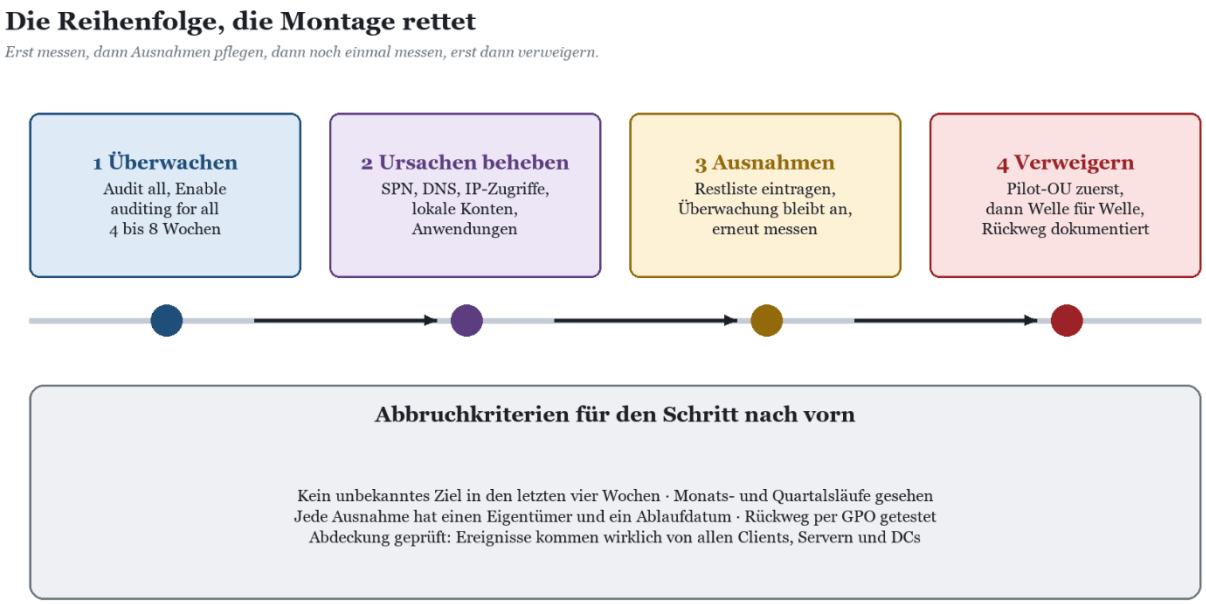
AUS DER PRAXIS · Sparfuchs & Partner: der Scanner, der nur Montags scannt

Bei der Sparfuchs & Partner Steuerberatungs GmbH lief die ausgehende Überwachung sechs Wochen. Danach stand die Ausnahmeliste: zwei Server, sauber begründet. Am ersten Montag nach dem Verweigern meldete sich die Poststelle. Der Multifunktionsdrucker legt Scans auf einer Freigabe ab und holt sich wöchentlich eine Adressliste vom Dateiserver, und zwar per IP-Adresse. Weil das nur montags passiert und die Überwachung genau in einer Urlaubswoche zwei Montage verpasst hatte, fehlte es im Protokoll. Lösung: DNS-Name statt IP im Gerät, kein neuer Listeneintrag. Lehre: Ein Messzeitraum ohne Abdeckungsprüfung ist ein Ratespiel mit Tabellenkalkulation.

Wie du Ausnahmelisten langfristig pflegst, mit Eigentümern, Fristen und regelmäßiger Rezertifizierung, beschreibt Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren ausführlich.

Die Reihenfolge: Überwachen vor Verweigern, immer

Microsoft schreibt es in jede einzelne Referenzseite der Restrict-NTLM-Richtlinien: zuerst überwachen, dann das Protokoll auswerten, dann Ausnahmen eintragen, dann erneut überwachen, erst dann verweigern. Das klingt nach Bürokratie, ist aber schlicht der Unterschied zwischen einem geplanten Wartungsfenster und einem ungeplanten Krisenstab.



Skizze: Vorgehen nach Microsoft-Empfehlung „zuerst überwachen", Zeiträume als Richtwert

Phase	Client	Server	Domänencontroller
1 Überwachen	Ausgehend: Alle überwachen	Eingehend überwachen: alle Konten	In dieser Domäne überwachen: Alle aktivieren

2 Ursachen beheben	IP-Zugriffe, Aliasse, Anwendungen	SPNs, lokale Konten, Dienste	Auswertung 8004 bzw. 4030 bis 4033
3 Ausnahmen	Remoteserverausnahmen pflegen	Server ggf. aus Verweigern-GPO herausnehmen	Serverausnahmen in dieser Domäne pflegen
4 Verweigern	Ausgehend: Alle verweigern (Pilot-OU zuerst)	Eingehend: Alle Domänenkonten verweigern	Erst Für Domänenkonten zu Domänenservern, später weiter

Was im Protokoll landet

Alle Restrict-NTLM-Richtlinien schreiben in denselben Kanal: Anwendungs- und Dienstprotokolle, Microsoft, Windows, NTLM, Operational. Die klassischen Überwachungsereignisse sind 8001 (Client, ausgehend), 8002 (Server, eingehend) sowie 8003 und 8004 auf Domänencontrollern. Sie funktionieren auch auf älteren Systemen. Seit dem Microsoft-Artikel KB5064479 gibt es zusätzlich das erweiterte Auditing: 4020 bis 4023 auf Clients und Servern, 4030 bis 4033 auf DCs, mit Reason ID 0 bis 11, die verrät, warum nicht Kerberos benutzt wurde. Das erweiterte Auditing läuft ab Windows 11 24H2 und Windows Server 2025, auf Windows Server 2022 und 2019 mit den Updates ab 13.10.2026. Wie du es einschaltest, steht in Erweitertes NTLM-Auditing einschalten: Schritt für Schritt, was die Reason IDs bedeuten, in NTLM-Reason-IDs erklärt: warum Windows nicht Kerberos benutzt hat.

Eine schnelle Abfrage mit Bordmitteln auf einem einzelnen Gerät sieht so aus:

```
# Restrict-NTLM-Überwachung der letzten 7 Tage auf diesem Gerät
Get-WinEvent -FilterHashtable @{
  LogName   = 'Microsoft-Windows-NTLM/Operational'
  Id        = 8001, 8002, 8003, 8004
  StartTime = (Get-Date).AddDays(-7)
} | Group-Object Id | Select-Object Name, Count

# Protokollgröße prüfen und anheben (hier 64 MB)
wevtutil gl Microsoft-Windows-NTLM/Operational
wevtutil sl Microsoft-Windows-NTLM/Operational /ms:67108864
```

WICHTIG · Das Protokoll ist klein, die Überwachung ist laut

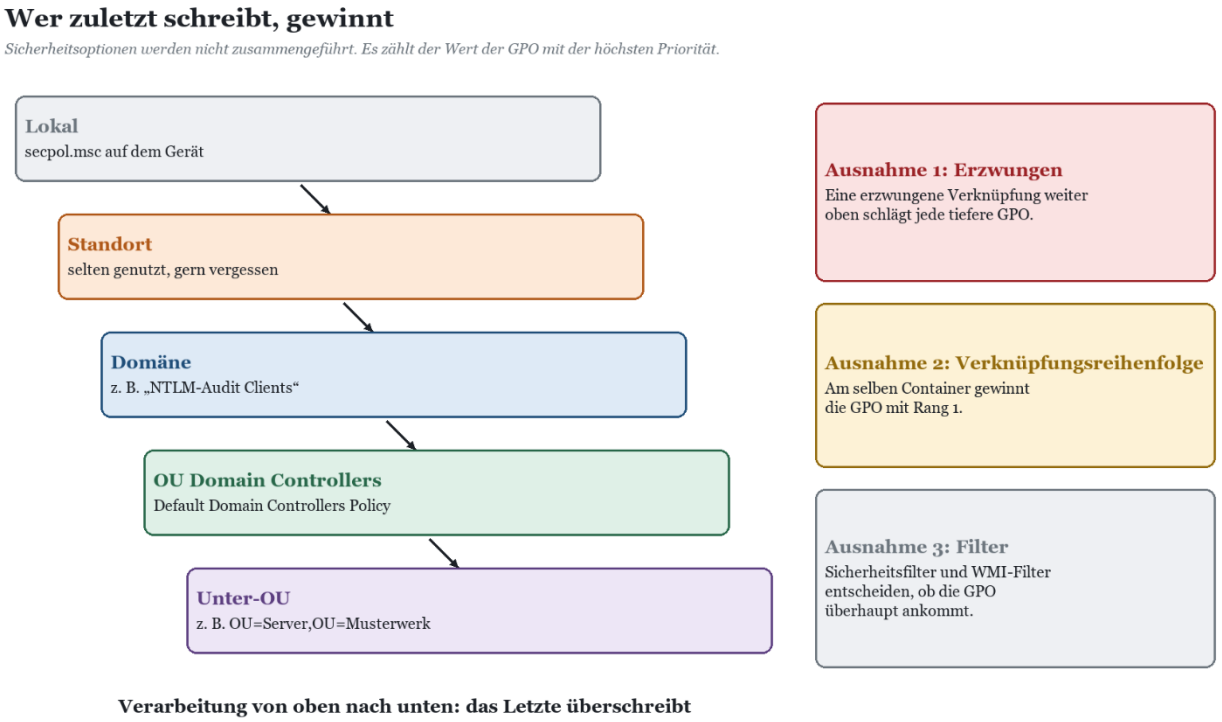
Microsoft weist bei der Domänenüberwachung ausdrücklich darauf hin, die Größe des Operational-Protokolls im Blick zu behalten. Auf einem DC mit „Alle aktivieren“ läuft der Kanal schnell voll, und ältere Einträge werden überschrieben. Wer nach vier Wochen auswertet, sieht dann die letzten paar Stunden. Hebe die Größe an und sammle zentral, etwa wie in NTLM-Ereignisse zentral sammeln mit Windows Event Forwarding beschrieben. Die passenden Überwachungs-GPOs legt das NTLM-Audit-GPO-Skript reproduzierbar an.

Wie lange überwachen?

Eine Woche reicht nie. Vier Wochen sind das Minimum, wenn ein Monatsabschluss darin liegt. In Kliniken und Verwaltungen mit Quartalsläufen, Abrechnungszyklen und Fachverfahren, die einmal im Jahr den Jahreswechsel verarbeiten, ist mehr besser. Wichtiger als die Dauer ist aber die Abdeckung: Kommen die Ereignisse tatsächlich von allen Maschinen? Ein Laptop, der sechs Wochen im Homeoffice ohne VPN stand, hat in deinem Protokoll keine Meinung, aber am Tag nach dem Verweigern sehr wohl eine.

Fallstricke bei der GPO-Rangfolge

Die Restrict-NTLM-Optionen sind Sicherheitsoptionen. Für sie gilt die normale Gruppenrichtlinien-Verarbeitung: lokal, Standort, Domäne, OU, und innerhalb der OU-Hierarchie von oben nach unten. Bei widersprüchlichen Werten gewinnt die GPO, die zuletzt angewendet wird. Das klingt banal und ist trotzdem die häufigste Ursache dafür, dass ein sorgfältig geplantes „Alle überwachen“ auf der Hälfte der Clients nie ankommt.



Skizze: Gruppenrichtlinien-Verarbeitung Lokal, Standort, Domäne, OU; Beispielnamen fiktiv

Listen werden nicht zusammengeführt

Der gemeinste Fallstrick betrifft die Ausnahmelisten. Konfigurieren zwei GPOs die Remoteserverausnahmen, ergibt das nicht die Summe beider Listen. Es gewinnt eine Liste vollständig, die andere ist wirkungslos. Bei der Musterwerk GmbH pflegte die Abteilung Produktion eine eigene GPO mit drei Maschinensteuerungen, die zentrale IT eine GPO mit zwei Dateiservern. Auf den Rechnern in der Produktion gewann die Abteilungsliste, weil sie tiefer verknüpft war, und die Dateiserver standen dort plötzlich nicht mehr auf der Liste. Die Regel daraus: Jede Ausnahmeliste wird an genau einer Stelle gepflegt.

Die typischen Stolperstellen

Fallstrick	Was passiert	Gegenmittel
Domänen-GPO trifft auch DCs und Server	„Alle verweigern“ für Clients landet auf Servern und DCs, die als Client auftreten	Client-GPOs nur an Client-OUs verknüpfen, Sicherheitsfilter prüfen
Default Domain Controllers Policy mit Altwert	Ein alter Eintrag in der DC-Standardrichtlinie überschreibt die neue Domänen-GPO	Restrict-NTLM nur in einer eigenen GPO an der OU Domain Controllers
Erzwungene Verknüpfung weiter oben	Eine erzwungene GPO auf Domänenebene schlägt die Pilot-GPO in der Unter-OU	gpresult /h auf einem Pilotgerät, Spalte „Gewinnendes GPO“ lesen
Vererbung deaktiviert	Eine OU mit blockierter Vererbung bekommt die Überwachung nie	Gruppenrichtlinienvererbung je OU prüfen, Lücken gezielt schließen

Zwei Ausnahmelisten-GPOs	Nur eine Liste wirkt, die andere wird ignoriert	eine Liste, ein Ort, ein Eigentümer
Rückbau durch Entfernen der GPO	Sicherheitseinstellungen können nach dem Entfernen in der Registrierung stehen bleiben	Rückweg aktiv setzen: Wert auf „Alle zulassen“ bzw. „Deaktivieren“, dann entfernen
Lokale Richtlinie	Ohne GPO-Wert gilt der lokale Wert aus secpol.msc	lokale Werte bei Bestandsgeräten auslesen, nicht unterstellen

WARNUNG · „Nicht definiert“ heißt nicht „zurückgesetzt“

Wenn du eine Restrict-NTLM-Option in der GPO wieder auf „Nicht definiert“ stellst, bleibt der zuletzt geschriebene Wert auf vielen Geräten in der Registrierung stehen. Für den Rückweg aus einem Verweigern ist das tückisch: Die GPO sieht sauber aus, das Gerät verweigert trotzdem weiter. Plane den Rückweg deshalb als aktive Einstellung „Alle zulassen“ und prüfe ihn im Pilot, bevor du ihn im Ernstfall brauchst.

Prüfen mit Bordmitteln

Auf einem einzelnen Gerät ist die Prüfung schnell gemacht. gpresult zeigt, welche GPO gewonnen hat, die Registrierung zeigt, was tatsächlich gilt. Beides gehört zusammen, denn das zweite kann wegen lokaler Werte oder Reste vom ersten abweichen.

```
gpresult /h C:\Temp\rsop.html /f

reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v RestrictSendingNTLMTraffic
reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v RestrictReceivingNTLMTraffic
reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v ClientAllowedNTLMServers

# auf einem DC
reg query HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters /v RestrictNTLMInDomain
reg query HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters /v AuditNTLMInDomain
```

Fehlt ein Wert, ist die Option nicht gesetzt, also wird zugelassen beziehungsweise nicht überwacht. Auf einem Gerät ist das eine Minute Arbeit. Auf 800 Geräten in sechs Standorten, von denen ein Viertel gerade ausgeschaltet ist, ist es ein Wochenende mit Remoting-Fehlern.

Wenn Hunderte Maschinen mitreden: Werte und Widersprüche sichtbar machen

Mit Bordmitteln bekommst du jede einzelne Antwort. Was du nicht bekommst, ist das Gesamtbild: Auf welchen Clients steht ausgehend wirklich „Alle überwachen“? Welcher Server verweigert eingehend, während seine Clients noch NTLM zu ihm schicken? Welcher DC hat die Domänenüberwachung, welcher nicht? Und welche Maschinen liefern überhaupt keine Ereignisse, sodass ihr Schweigen keine Entwarnung ist, sondern eine Lücke? Diese Fragen entstehen nicht auf einem Gerät, sondern zwischen den Geräten. Genau dort wird es mühsam: Tausende Ereignisse, Hunderte Maschinen, Registrierungswerte in zwei Pfaden, dazu die Frage nach der Ursache jeder einzelnen NTLM-Anmeldung.

Für diese Zusammenschau gibt es den NTLM Diagnostiker. Seine Readiness-Ampel zeigt die aktuellen Werte der Restrict-NTLM-Richtlinien und macht Widersprüche sichtbar, bevor sie zu Ausfällen werden, etwa einen Server mit verweigerter eingehender Richtlinie, zu dem laut Protokoll noch NTLM-Anmeldungen laufen.

SO GEHT'S MIT DEM NTLM DIAGNOSTIKER · Restrict-NTLM-Werte prüfen, bevor du verweigerst

Der NTLM Diagnostiker arbeitet ausschließlich lesend. Er setzt keine Gruppenrichtlinie, ändert keinen Registrierungswert und legt keine Ausnahme an. Er zeigt dir, wo du stehst.

Die Readiness-Ampel zeigt die aktuellen Restrict-NTLM-Werte und Widersprüche zwischen Richtlinien und tatsächlichem Verkehr. Abdeckungsmonitor und OS-Landkarte zeigen, welche Maschinen Ereignisse liefern, welche schweigen und auf welchen Systemen das erweiterte Auditing überhaupt verfügbar ist.

Ereignisse holt er direkt vom DC, über einen vorhandenen Windows Event Collector oder per Direktabfrage. Die Ursachen-Engine mit SPN- und DNS-Prüfung erklärt, warum eine Anmeldung bei NTLM gelandet ist, die Kommunikationsmatrix und die Konten-Sicht zeigen, wer mit wem NTLM spricht. Dazu kommen NTLMv1-Hitliste, Sicherheitsflaggen und Wireshark-Import für Geräte ohne Ereignisprotokoll.

Die Abschalt-Simulation beantwortet die entscheidende Frage vor jedem Verweigern: Was würde jetzt ausfallen? Ergebnisse gehen als Word-Bericht an die IT-Leitung und als Excel/CSV-Export an die Fachabteilungen.

Ein Ausnahmelisten- und Skript-Generator ist für eine spätere Ausbaustufe geplant, ebenso ein Phasenplan. Heute pflegst du die Listen selbst, mit den Befunden als Grundlage.

Zum Einstieg liefert die kostenlose Edition Express einen Fünf-Minuten-Befund, der volle Umfang lässt sich sieben Tage testen. Lizenziert wird pro aktivem Computerkonto.

Bei der Trendforge Digital GmbH zeigte die Ampel im ersten Lauf zwei Widersprüche, die niemand gesucht hatte: Auf einem Teil der Clients galt noch eine alte lokale Einstellung „Alle zulassen“ statt der geplanten Überwachung, weil die betroffene OU die Vererbung blockierte. Und ein Entwicklungsserver verweigerte eingehend bereits alle Domänenkonten, ein Überbleibsel eines Härtungstests, während ein Build-Dienst ihn nachts per NTLM ansprach. Beides war mit Bordmitteln auffindbar, aber nur, wenn man gewusst hätte, wo man suchen muss.

Wenn du die Restrict-NTLM-Einführung lieber mit Begleitung planst, von der GPO-Struktur bis zu den Abbruchkriterien, unterstützt dich die Beratung zur NTLM-Ablösung. Wie du die Ablösung insgesamt als Projekt aufziehst, beschreibt NTLM-Ablösung als Projekt: Zeitplan, Rollen, Aufwand; die Einführung Schritt für Schritt bis zum Verweigern zeigt NTLM schrittweise abschalten, ohne dass etwas ausfällt.

FAQ: Restrict-NTLM-Richtlinien

Muss ich nach dem Ändern einer Restrict-NTLM-Option neu starten?

Nein. Laut Microsoft greifen die Werte ohne Neustart, sobald die Gruppenrichtlinie angewendet ist. Mit gpupdate /force beschleunigst du das auf einem Testgerät.

Gibt es eine eigene Richtlinie zum Überwachen von ausgehendem NTLM?

Nein. Ausgehend überwachst du über den Wert „Alle überwachen“ der Richtlinie „Ausgehender NTLM-Datenverkehr zu Remoteservern“. Eingehend und in der Domäne gibt es jeweils eine eigene Überwachungsrichtlinie.

Kann ich für den eingehenden Datenverkehr eine Ausnahme eintragen?

Nein, die eingehende Richtlinie hat keine Ausnahmeliste. Einen Server nimmst du aus, indem du ihn nicht in den Wirkungsbereich der Verweigern-GPO aufnimmst, etwa über eine eigene OU oder einen Sicherheitsfilter.

Hilft die Remoteserverausnahme auf dem Client, wenn der DC verweigert?

Nein. Jede Station prüft für sich. Die Client-Liste lässt den Client NTLM senden; ob der DC die Durchreichung annimmt, entscheidet allein seine Richtlinie mit der Liste „Serverausnahmen in dieser Domäne“.

Was hat BlockNtlmv1SSO mit den Restrict-NTLM-Richtlinien zu tun?

Nichts direkt. BlockNtlmv1SSO steuert seit dem Update vom 13.10.2026 die Blockade von NTLMv1 für Single Sign-on, die Restrict-NTLM-Richtlinien steuern NTLM insgesamt. Die Einzelheiten zu BlockNtlmv1SSO stehen in BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme.

Soll ich zuerst auf Clients, auf Servern oder auf DCs verweigern?

Die Überwachung schaltest du überall gleichzeitig ein. Beim Verweigern beginnen viele Umgebungen mit der ausgehenden Richtlinie auf einer Pilot-OU mit Clients, weil die Ausnahmeliste dort Spielraum lässt. Eingehend am Server und die Domänenrichtlinie folgen, wenn das Protokoll ruhig ist.

Ist ein Stern allein in der Ausnahmeliste eine gute Idee?

Nein. Ein einzelner Stern erlaubt NTLM zu jedem Server und hebt das Verweigern faktisch auf. Platzhalter sind für Namensmuster wie scan* gedacht, nicht als Generalschlüssel.

Ändert der NTLM Diagnostiker meine Richtlinien?

Nein. Er arbeitet ausschließlich lesend, zeigt in der Readiness-Ampel die aktuellen Werte und Widersprüche und überlässt jede Änderung dir. Ein Ausnahmelisten-Generator ist geplant, aber noch nicht vorhanden.

Was hat das alles mit Kerberos zu tun?

Alles, was du per Restrict NTLM verweigerst, muss danach per Kerberos funktionieren. Fehlende oder doppelte SPNs, Zugriffe per IP-Adresse und fehlende Sichtverbindung zum DC sind die häufigsten Gründe, warum das nicht klappt. Hintergründe zu Kerberos findest du im Kompetenzbereich Microsoft Kerberos.

Fazit: Erst zählen, dann zumachen

Die Restrict-NTLM-Richtlinien sind kein Hexenwerk. Sieben Optionen, drei Wirkungsorte, zwei Ausnahmelisten, eine klare Reihenfolge: überwachen, Ursachen beheben, Ausnahmen pflegen, erneut überwachen, verweigern. Gefährlich werden sie nicht durch ihre Komplexität, sondern durch das Drumherum: GPOs, die sich gegenseitig überschreiben, Ausnahmelisten, die nicht zusammengeführt werden, DCs mit unterschiedlichem Stand und Geräte, die im Messzeitraum einfach nicht da waren.

Wer das sauber aufsetzt, schaltet NTLM in seinem eigenen Tempo ab und nicht im Tempo des nächsten Windows-Server-Release. Wer es überspringt, lernt die Abhängigkeiten seiner Umgebung auch kennen, nur eben montags um halb acht, live und mit Publikum. Für das Team, das diese Zusammenhänge selbst sicher lesen will, gibt es die Schulung zum NTLM Diagnostiker.

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
› Server-Ausnahmen für NTLM: sauber pflegen statt Löcher bohren
› NTLM schrittweise abschalten, ohne dass etwas ausfällt

› NTLM wegen IP-Adresse: Laufwerke und Skripte auf DNS-Namen umstellen
› BlockNtlmv1SSO erklärt: Überwachung, Erzwingung, Ausnahme