FORESTALL

Modern Kurumlar için Kimlik Güvenliği #01

NTLMv1'i Devre Dışı Bırakma Yol Haritası

Version 1.0 - 14.04.2026

Serdal Tarkan Altun

Özet

NTLMv1, DES tabanlı zayıf kriptografisi nedeniyle yakalanan hash'lerin saniyeler içinde kırılmasına olanak tanımaktadır. Ayrıca NTLM Relay saldırısını engellemek için geliştirilen bazı güvenlik ayarlarını desteklememektedir. Bu nedenle kurumsal altyapılarda kullanılmamalıdır.

Microsoft, Haziran 2024 itibarıyla NTLM ailesini deprecated olarak işaretlemiştir; NTLMv1 ise Windows 11 24H2 ve Windows Server 2025 ile varsayılan olarak kullanılmamaktadır.

NTLMv1'i kapatma süreci için güvenli yaklaşım, tek seferde giderme işlemlerini uygulamak değil; discover → remediate → enforce → monitor sırasını izlemektir.

LmCompatibilityLevel = 5 (GPO) ayarı ile NTLMv1 tamamen engellenebilir; ancak öncelikle tüm istemcilerin NTLMv2'ye geçirilmesi gerekmektedir.

Uzun vadeli hedef yalnızca NTLMv1'i kapatmak değil, **NTLM bağımlılığını azaltıp Kerberos kullanımını genişletmektir**.

Bu dokümanın ana hedefi, NTLMv1'i kesinti yaşamadan kapatmak için **uygulanabilir** bir geçiş modeli sunmaktır.

Okuyucu Kitlesi

Bu doküman özellikle aşağıdaki ekipler için hazırlanmıştır.

- Active Directory / IAM ekipleri
- Windows platform ve endpoint ekipleri
- Blue team / SOC ekipleri
- Legacy bağımlılık temizliği yapan altyapı ekipleri
- AD hardening projesi yöneten güvenlik mimarları

Dokümanın Amacı

Bu dokümanın amacı NTLMv1'in neden riskli olduğunu tekrar etmekten çok, güvenli biçimde nasıl kapatılacağını aktarmaktır.

İçerikte risk özeti, en sık problem yaşanan alanlar, uygulanabilir geçiş modeli ve enforcement detayları yer almaktadır.

İçindekiler

- Giriş
  - NTLM Protokolü Nasıl Çalışır?
    - LM Hash ve LM Protokolü Neden Bu Kadar Zayıf?
    - NTLMv1 ve NTLMv2 Karşılaştırması
  - Olası Güvenlik Etkileri
    - Örnek Saldırı Senaryosu
- Giderme Adımları için Dikkat Edilmesi Gereken Noktalar
- Güvenli Geçiş Modeli
- Uygulama Adımları
  - 1. Discovery
  - 2. Remediation
  - 3. Enforcement
    - Rollback Planı
  - 4. Monitoring
  - 5. Uygulama Kontrol Listesi
  - 6. Proje Zaman Planı
  - 7. Başarı Metrikleri ve KPI
- Yeni NTLM Denetim Kayıtları
- Kaynaklar

Giriş

Modern kurumsal ağlarda kimlik doğrulama güvenliği, saldırı yüzeyini doğrudan etkileyen kritik bir güvenlik katmanıdır. Microsoft Active Directory altyapılarında uzun yıllar boyunca kullanılan NTLM protokolü, günümüzde hâlâ çeşitli gereksinimler nedeniyle kolaylıkla kaldırılamamaktadır.

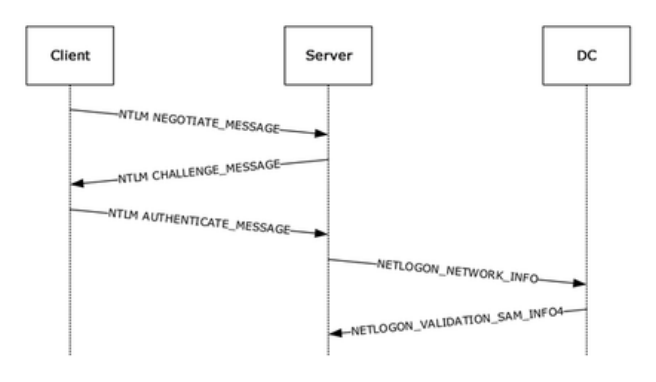
Ancak NTLM protokolünün eski sürümü olan NTLMv1, modern saldırı tekniklerine karşı oldukça zayıf kabul edilmektedir. Bu nedenle Active Directory güvenlik sıkılaştırma çalışmalarının önemli bir parçası **NTLMv1 protokolünün devre dışı bırakılmasıdır.**

NTLM Protokolü Nasıl Çalışır?

NTLM, Microsoft tarafından geliştirilen ve challenge-response tabanlı bir kimlik doğrulama mekanizmasıdır.

Protokolün temel akışı şu şekildedir:

Client → Authentication Request -> Server
Server → Challenge -> Client
Client → Response (Hash) -> Server



1. İstemci, sunucuya düz metin olarak kullanıcı adını gönderir.
2. Sunucu rastgele bir sayı (challenge/nonce) üretir ve istemciye gönderir.
3. İstemci, kullanıcının parola hash'ini kullanarak challenge üzerinden bir response üretir ve sunucuya geri gönderir.
    a. NTLMv1 kullanılıyorsa: Kimlik doğrulama temelde server challenge ve DES tabanlı response üretimine dayanır. Bazı Extended Session Security (ESS) senaryolarında istemci taraflı ek değerler sürece girse de kimlik doğrulamanın kendisi hâlâ NTLMv1 olarak kalır.
    b. NTLMv2 kullanılıyorsa: İstemci challenge'a client challenge + timestamp + target bilgileri ekler ve HMAC-MD5 tabanlı daha güçlü bir response üretir. Bu yapı replay'a karşı korumayı ve doğrulamayı güçlendirir.

4. Sunucu; kullanıcı adı, challenge ve response bilgilerini Domain Controller'a doğrulama için iletir.
5. Domain Controller, SAM veritabanından kullanıcının parola hash'ini alarak aynı challenge'ı şifreler.
6. DC'nin hesapladığı sonuç ile istemciden gelen response eşleşiyorsa kimlik doğrulama başarılıdır.

Versiyon	Durum	Güvenlik
LM	Legacy	Çok zayıf
NTLMv1	Deprecated	Zayıf
NTLMv2	Deprecated fakat Aktif	Görece güvenli ama kullanılmamalı

LM Hash ve LM Protokolü Neden Bu Kadar Zayıf?

Temel zayıflıkları:

- Büyük/küçük harf ayrımı yoktur: Parola hash'lenmeden önce tüm karakterler büyük harfe dönüştürülmektedir. Bu durum brute-force saldırılarının arama uzayını önemli ölçüde daraltmaktadır.

- Parola iki yarıya bölünür: Parola 7+7 byte olarak iki bağımsız yarıya ayrılmakta ve her yarı ayrı ayrı DES ile şifrelenmektedir. Saldırgan 14 karakterlik bir parolayı kırmak yerine iki adet 7 karakterlik yarıyı bağımsız olarak kırabilmektedir.

- Kısa parolalar tespit edilebilir: Parola 8 karakterden kısaysa ikinci yarı tamamen NULL ile doldurulmakta ve her zaman aynı hash değerini üretmektedir (AAD3B435B51404EE). Saldırgan bu sabit hash'i gördüğünde parolanın 7 karakter veya daha kısa olduğunu doğrudan anlayabilmektedir.

- Hızlı kırılır: 7 byte'lık bir DES hash'i modern donanımlarla 6 saatten kısa sürede brute-force ile kırılabilmektedir.

LM Hash, 1987 yılında tasarlanmış ve günümüzde kırılması son derece **kolay** bir mekanizmadır.

NTLMv1 ve NTLMv2 Karşılaştırması

Özellik	NTLMv1	NTLMv2
Hash Algoritması	DES (56-bit)	HMAC-MD5
Challenge	Yalnızca server challenge (8 byte)	Server challenge + client challenge
Salt	Yok	Client challenge salt olarak kullanılır
Replay Koruması	Zayıf	Client challenge ile güçlendirilmiş
Brute-Force Direnci	Düşük / DES tabanlı hash hızlı kırılır	Daha yüksek / HMAC-MD5 yapısı direnci artırır

NTLMv1'de kullanılan DES algoritması tasarım gereği daha hızlı çalışmaktadır; bu da saldırganların yakalanan paketlerden hash değerlerini kısa sürede elde etmesine olanak tanımaktadır.

NTLMv2 ise HMAC-MD5 kullanarak daha güçlü bir kriptografik yapı sunmakta ve challenge içeriğine eklenen ek parametreler (timestamp, username, target) sayesinde replay saldırılarına karşı koruma sağlamaktadır.

HMAC-MD5 günümüz standartlarına göre ideal olmasa da DES'e kıyasla önemli ölçüde daha güvenlidir.

Bu versiyonlar arasında güvenlik açısından ciddi farklar bulunmaktadır.

Olası Güvenlik Etkileri

NTLMv1'in; zayıf kriptografik yapısı, Pass-the-Hash / relay saldırılarına açıklığı ve modern güvenlik standartlarıyla uyumsuzluğu nedeniyle güncel altyapılarda kullanılmaması önerilmektedir. Kurumsal ağlarda NTLMv1 kullanımının devam etmesi aşağıdaki riskleri doğurmaktadır:

- Credential dumping sonrası hızlı parola kırma
- Pass-the-hash saldırıları
- NTLM relay saldırıları; saldırganın kimlik doğrulama trafiğini üçüncü bir sisteme yönlendirerek yetkisiz erişim elde etmesi
- Man-in-the-Middle (MitM) saldırıları; NTLMv1'in zayıf session security yapısı nedeniyle araya girme saldırılarına açıklık
- Yetki yükseltme (Privilege Escalation)
- Lateral movement saldırıları
- Domain ortamında kimlik doğrulama güvenliğinin zayıflaması

Kısacası, NTLMv1'in ortamda bulunması eski ama çalışıyor kategorisinde değil, gereksiz ve ölçülebilir bir kimlik riski kategorisindedir.

Örnek Saldırı Senaryosu

Hash Yakalama

Saldırgan, ağ üzerinde Responder veya ntlmrelayx gibi bir araç çalıştırarak NTLMv1 challenge-response trafiğini yakalar. Bunun için LLMNR/NBT-NS poisoning veya farklı bir MITM saldırısı kullanılabilir.

Hash Kırma

Yakalanan NTLMv1 hash'i, DES tabanlı yapısı nedeniyle crack.sh gibi çevrimiçi servisler veya hashcat ile saniyeler içinde kırılabilir. NTLMv1 hash'leri için rainbow table saldırıları da son derece etkilidir.

Lateral Movement

Kırılan parola ile saldırgan, kullanıcının erişim yetkisine sahip olan diğer sistemlere yatay hareketle ilerler.

Privilege Escalation

Eğer yakalanan hesap bir servis hesabı veya yönetici hesabıysa, saldırgan doğrudan yüksek yetkili erişim elde eder.

Not: NTLMv2 hash'leri de yakalanabilir ancak kriptografik yapısı (HMAC-MD5 + timestamp + client challenge) nedeniyle kırılması çok daha zor ve zaman almaktadır. NTLMv1'den NTLMv2'ye geçiş, bu saldırı zincirinin en kritik adımını (hash kırma) önemli ölçüde zorlaştırmaktadır.

Giderme Adımları için Dikkat Edilmesi Gereken Noktalar

Microsoft'un Verdiği Temel Mesajlar

- Microsoft, NTLMv1'i legacy ve modern kimlik doğrulama mimarileriyle uyumsuz bir mekanizma olarak konumlandırmaktadır.
- Haziran 2024 itibarıyla Microsoft, NTLM ailesinin tamamını deprecated olarak işaretlemiştir.
- NTLMv1, Windows 11 24H2 ve Windows Server 2025 ile varsayılan olarak kapatılmıştır.
- Microsoft, denetim (audit), kademeli kısıtlama ve yeni Kerberos yetenekleriyle NTLM bağımlılığını azaltan bir geçiş stratejisi izlemektedir.
- Microsoft, NTLM'i gelecek Windows sürümlerinde default olarak devre dışı bırakılmış hale getirmeye doğru ilerlemektedir.
- Uzun vadeli hedef, NTLM bağımlılığını azaltarak Kerberos tabanlı kimlik doğrulamayı genişletmektir.

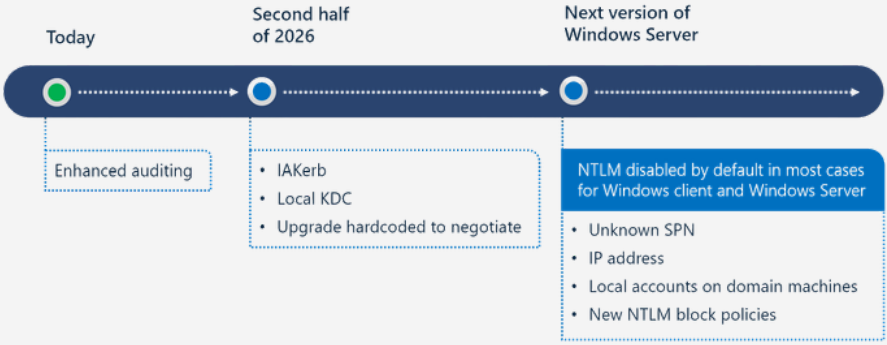
Microsoft'un NTLM Geçiş Yol Haritası

Microsoft, NTLM bağımlılığını bir anda değil, aşamalı şekilde azaltmayı hedeflemektedir. Bugün görünen ana yönelim şöyledir:

Faz	Dönem	Kapsam
Faz 1	Aktif	NTLM denetimlerinin güçlendirilmesi, NTLM ailesinin deprecated ilan edilmesi, NTLMv1'in yeni platformlardan kaldırılması
Faz 2	2026 ve sonrası	**IAKerb** ve **Local KDC** gibi yeteneklerle Kerberos kapsamasının genişletilmesi, NTLM bağımlılıklarının azaltılması
Faz 3	Gelecek sürümler	NTLM'in **default olarak devre dışı** geldiği daha güvenli varsayılanların yaygınlaşması

Bu yol haritasında dikkat çeken iki önemli teknoloji bulunmaktadır:

- IAKerb (Initial and Pass Through Authentication Using Kerberos): Domain Controller'a doğrudan erişimi olmayan istemcilerin Kerberos kullanabilmesini sağlamaktadır.
- Local KDC: Yerel hesaplar için Kerberos desteği sunarak NTLM bağımlılığını azaltmaktadır.



Not: NTLMv2'ye geçiş bir ara adımdır. Microsoft'un uzun vadeli yönü, NTLM kullanımını olabildiğince azaltıp Kerberos tabanlı kimlik doğrulamayı genişletmektir.

Uyumluluk ve Regülasyonlar

NTLMv1 kapatma çalışması yalnızca teknik bir sıkılaştırma değil, aynı zamanda çeşitli regülasyon ve uyumlulukların da gereksinimidir:

Regülasyon/Uyumluluk	İlgili Gereksinim	NTLMv1 İlişkisi
CIS Benchmarks	Windows Server / Workstation Level 1	LmCompatibilityLevel = 5 zorunlu
Microsoft Security Baselines	Tüm Windows sürümleri	LmCompatibilityLevel = 5 önerilen
NIST SP 800-53	IA-5 (Authenticator Management), SC-8 (Transmission Confidentiality)	Zayıf kimlik doğrulama mekanizmalarının kullanım dışı bırakılması
ISO 27001:2022	A.8.5 (Secure Authentication)	Güvenli kimlik doğrulama gereksinimi
PCI-DSS v4.0	Requirement 8.3 (Strong Authentication)	Zayıf kriptografinin kaldırılması
KVKK / Kişisel Verileri Koruma Kanunu	Teknik Tedbirler — Yetkilendirme ve Kimlik Doğrulama	Kişisel verilere erişimde güvenli kimlik doğrulama zorunluluğu

Credential Guard ile NTLMv1 İlişkisi

Windows Credential Guard, LSASS belleğindeki sırları izole ederek özellikle NTLM hash ve diğer oturum bilgilerini korumaktadır. Etkin olduğunda NTLMv1, MS-CHAPv2, Digest ve CredSSP ile signed-in credential kullanımı / SSO çalışmamaktadır. Bu durum, uç nokta tarafında NTLMv1 maruziyetini önemli ölçüde azaltmaktadır.

Ancak bu durum, ortam genelinde NTLMv1'in merkezi olarak kapatıldığı anlamına gelmemektedir. Credential Guard bir uç nokta korumasıdır; LmCompatibilityLevel ise istemci/sunucu/DC davranışını yöneten kurumsal politika katmanıdır. Bu nedenle Credential Guard destekleyen ortamlarda etkinleştirilmesi güçlü bir tamamlayıcı kontroldür, fakat GPO/Intune tabanlı merkezi enforcement'ın yerini tek başına almamaktadır.

Alan	Tipik Problem
Eski NAS cihazları	SMB / scan-to-folder senaryolarında NTLMv1 bağımlılığı
Yazıcı / MFP cihazları	SMB share veya eski auth yöntemiyle klasöre tarama
Eski Samba sürümleri	Varsayılan veya yanlış yapılandırılmış NTLM davranışı
SQL Server 2008 ve öncesi	Named Pipes veya eski client davranışları
Eski IIS / intranet uygulamaları	Kerberos başarısız olunca sessiz NTLM fallback
SCCM / MECM	Bazı client push ve legacy communication senaryoları
IP ile erişilen dosya paylaşımları	Kerberos yerine NTLM fallback
Trust / multi-forest ortamları	SPN, trust veya farklı policy seviyeleri nedeniyle fallback

Kapatma Aşamasında En Sık Problem Yaşanan Alanlar

Kurumlar genelde NTLMv1'i GPO ile kolaylıkla kapatabilmektedir; ancak zor olan kısım, hangi legacy bağımlılıklarda erişim problemi oluşabileceğini önceden tespit etmektir.

En Sık Gözden Kaçan Nedenler

Aşağıda bahsedilen durumlar, enforcement yapılmadan önce göz önünde bulundurulmalıdır. Bu tip durumlar mevcutsa enforcement yapıldığı anda erişim kesintileri yaşanabilmektedir.

- Eksik SPN (Service Principal Name): Hedef servis için SPN tanımlanmamışsa Kerberos başarısız olur ve NTLM kullanılır.
- Duplicate SPN: Aynı SPN birden fazla hesaba atanmışsa Kerberos doğrulaması başarısız olur.
- IP adresi ile erişim: Kaynaklara FQDN yerine IP adresi ile erişilmesi durumunda Kerberos kullanılamaz ve NTLM kullanılır.

> Bu nedenlerle NTLM bağımlılıklarını azaltmak için 4769 (A Kerberos service ticket was requested) ve ilişkili Kerberos olayları da incelenmeli, özellikle başarısız istekler ve SPN sorunları analiz edilmelidir.

- Eski GPO'ların modern cihazlarda NTLMv1 versiyonunu aktif etmesi
- Windows dışı cihazların varsayılan kimlik doğrulama ayarları
- VPN dışındaki uzak cihazlarda Kerberos erişim sorunları

Güvenli Geçiş Modeli

NTLMv1 kapatma işlemi tek adımlı bir güvenlik ayarı değildir. Bu nedenle kurumların NTLMv1 kullanımını tespit ederek kontrollü şekilde devre dışı bırakmaları önerilmektedir. Süreç aşağıdaki aşamalarla ilerlemelidir:

- Discovery — NTLMv1 kullanımını tespit etme
- Remediation — Uygulama, cihaz ve yapılandırmaların düzeltilmesi
- Enforce — NTLMv1 protokolünün adım adım kapatılması
- Monitor — Periyodik izleme ile kalıcı bir süreç oluşturulması

Uygulama Adımları

Aşağıdaki adımlar, NTLMv1 devre dışı bırakma sürecinin kontrollü ve güvenli şekilde yürütülmesi için izlenmesi gereken temel aşamaları kapsamaktadır.

Discovery

TLMv1'i devre dışı bırakmadan önce hangi sistemlerin ve sistemler içerisindeki hangi uygulama ve servislerin bu versiyonu kullandığı tespit edilmelidir.

Önerilen aksiyonlar:

Mevcut LmCompatibilityLevel Envanterinin Çıkarılması

NTLM protokolüne dair versiyon LmCompatibilityLevel isimli değer üzerinden konfigüre edilmektedir. Bu değer manuel olarak Registry ile veya merkezi olarak Group Policy objeleri ile ayarlanabilmektedir.

LmCompatibilityLevel ayarının alabileceği değerler ve davranışları aşağıdaki tabloda özetlenmiştir.

Level	İstemci Davranışı	Sunucu / DC Davranışı
0	LM ve NTLMv1 gönderir; NTLMv2 session security kullanmaz	DC: LM, NTLM ve NTLMv2 kabul eder
1	LM ve NTLMv1 gönderir; sunucu destekliyorsa NTLMv2 session security kullanır	DC: LM, NTLM ve NTLMv2 kabul eder
2	Yalnızca NTLMv1 gönderir; NTLMv2 session security kullanır	DC: LM, NTLM ve NTLMv2 kabul eder
3	Yalnızca NTLMv2 gönderir	DC: LM, NTLM ve NTLMv2 kabul eder
4	Yalnızca NTLMv2 gönderir	DC: LM'i reddeder; NTLM ve NTLMv2 kabul eder
5	Yalnızca NTLMv2 gönderir	DC: LM ve NTLMv1'i reddeder; yalnızca NTLMv2 kabul eder

Uyarı: Level 0-2 arasındaki değerler istemcinin NTLMv1 kullanmasına izin vermektedir. Özellikle Level 2, session security'yi iyileştirmesine rağmen kimlik doğrulamanın kendisi hâlâ NTLMv1 olarak kalmakta ve yeterli güvenlik sağlamamaktadır. Minimum hedef Level 3 olmalıdır.

Uyarı: NTLMv1 + ESS Yanılgısı: Level 2'de etkinleştirilen Extended Session Security (ESS/NTLMv2 Session Security), NTLMv1 üzerinde ek koruma sağlıyor gibi görünse de kimlik doğrulama mekanizmasının kendisi hâlâ DES tabanlı NTLMv1 olarak kalmaktadır. ESS yalnızca session key üretimini güçlendirmekte; challenge-response yapısını ise değiştirmemektedir. Bu nedenle "NTLMv1 + ESS kullanıyoruz, güvendeyiz" varsayımı yanlıştır. Hash yakalama ve kırma saldırılarına karşı korunmak için NTLMv2'ye (Level 3+) geçiş şarttır.

Not: Level 0-3 istemcinin NEGOTIATE_MESSAGE içinde ne göndereceğini kontrol ederken, Level 4-5 sunucunun/DC'nin CHALLENGE_MESSAGE aşamasında neyi kabul edeceğini kontrol etmektedir.

LmCompatibilityLevel registry anahtarı varsayılan olarak sistemde bulunmayabilir. Bu anahtar mevcut değilse, sistemin davranışı kullanılan Windows sürümüne göre belirlenmektedir:

İşletim Sistemi	Varsayılan Değer	Davranış
Windows 2000 / XP	1	NTLMv1 kullanılır
Windows Server 2003	2	NTLMv1 + NTLMv2 session security
Windows Vista / Server 2008 ve üzeri	3	Yalnızca NTLMv2

Bu tabloda görüldüğü gibi, Vista/Server 2008 öncesi işletim sistemleri varsayılan olarak NTLMv1 kullanmaktadır. Ortamda eski bir GPO'nun olması durumunda güncel Windows sürümlerinin NTLM ayarları da düşürülebilmektedir. Eski GPO'ların modern sistemleri downgrade etmediğinden emin olmak için mevcut politikalar mutlaka gözden geçirilmelidir.

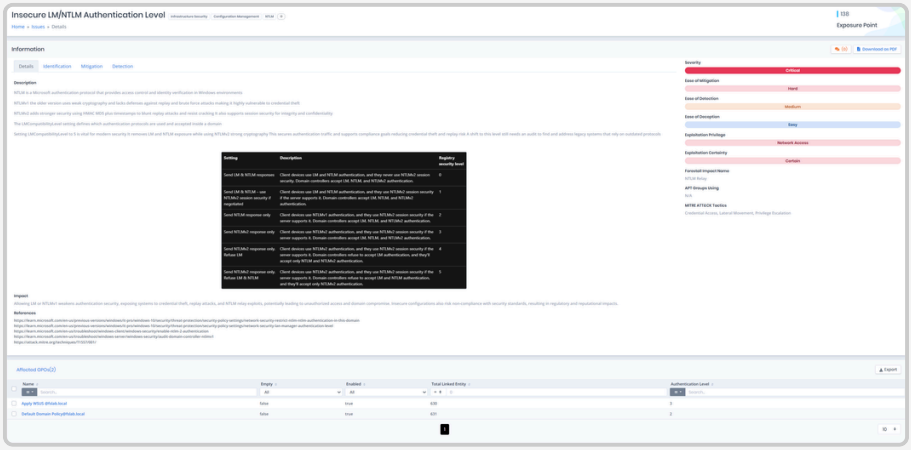
NTLMv1 kapatma sürecinin ilk adımı, ortamdaki tüm sistemlerin mevcut LmCompatibilityLevel değerlerinin toplu olarak raporlanmasıdır. Bu değeri tüm sistemlerden toplayabilmek için aşağıdaki yöntemler uygulanabilmektedir.

- İlgili ayarı konfigüre eden tüm Group Policy objeleri ve bu objelerin hangi bilgisayarlara uygulandığı tespit edilir.
- Bilgisayarlar üzerinde hali hazırda kurulu olan bir ajan üzerinden registry değeri merkezi olarak sorgulanır.
- Powershell script ile tüm bilgisayarlara ağ üzerinden erişim sağlanarak registry değerleri sorgulanır.

Bu adımlar çoğu zaman manuel efor gerektirdiği için hızlı bir şekilde gerçekleştirilememekte ve tüm sistemleri kapsayamamaktadır.

Bu işlemlerin yanı sıra Forestall ISPM'in Identity Risk Assessment, GPO Audit ve Search & Report modülleri kullanılarak ilgili tespit adımı hızlıca gerçekleştirilebilmektedir.

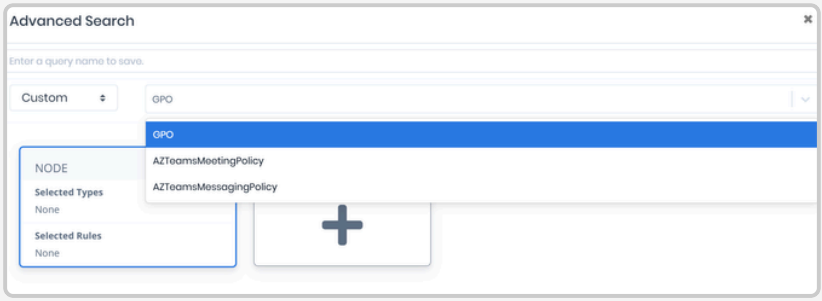
1. Forestall ISPM, güvensiz NTLM versiyon konfigürasyonlarını barındıran Group Policy objelerini ve bu objelerin hangi cihazları etkilediklerini otomatize bir şekilde tespit etmektedir. İlgili çıktıya ulaşmak adına öncelikle Issues sayfasına gidilir ve Insecure LM/NTLM Authentication Level zafiyeti kontrol edilir. Zafiyet içerisinde hangi Group Policy objesinin, hangi güvensiz ayarı kaç farklı bilgisayara uyguladığı görülebilmektedir.



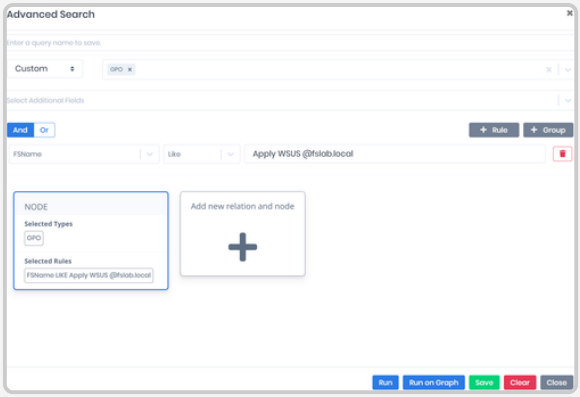
Örnek olarak zafiyet detayında, Apply WSUS isimli GPO'nun LmCompatibilityLevel değerini 630 farklı objeye 3 olarak uyguladığı görülebilmektedir.

2. Bir sonraki aşamada Search & Reports sayfasına gidilerek, güvensiz GPO'ların hangi bilgisayarlara uygulandığı tespit edilir. Bu tespiti yapabilmek adına aşağıdaki adımlar uygulanarak gerekli sorgu yazılır.

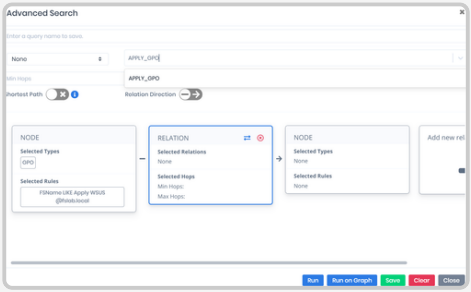
a. Bir sonraki aşamada Search & Reports sayfasına gidilerek, güvensiz GPO'ların hangi bilgisayarlara uygulandığı tespit edilir. Bu tespiti yapabilmek adına aşağıdaki adımlar uygulanarak gerekli sorgu yazılır.



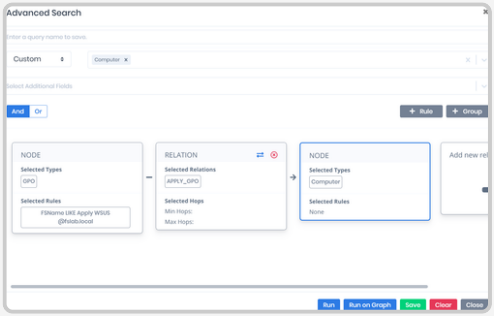
b. Ardından +Rule alanına tıklanır ve açılan Select Your Option ekranından FSName filtresi seçilir. Ardından Like veya Equal operatörü seçilerek zafiyetli olarak tespit edilen GPO adı yazılır.



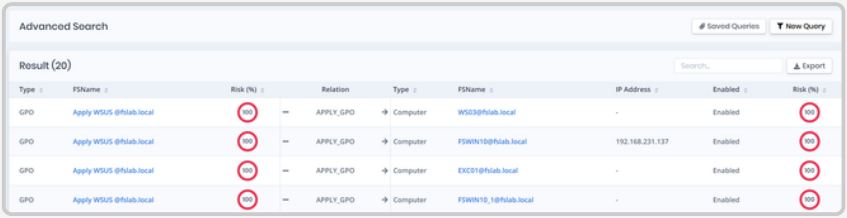
c. Sonraki adımda **Relation** alanına (Add new relation and node) tıklanır ve ilişki türü olarak **Apply_GPO** seçilir. Bu seçim ile belirlenen GPO'ların hangi varlıklara uygulandığı ilişki bazlı olarak sorguya dahil edilir.



d. Sağ tarafta bulunan Node alanına tıklanır. Ardından üst bölümde yer alan Entity Type listesinden Computer seçilir ve Run butonuna tıklanarak sorgu çalıştırılır. Bu sayede sorgu, zafiyetli GPO'ların uygulandığı hedef sistemleri bilgisayar bazında gösterecek şekilde tamamlanır.

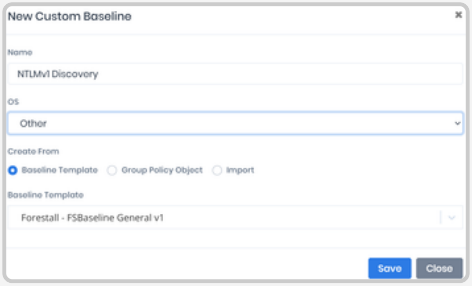


e. Bu sorgu yapısı sayesinde, LmCompatibilityLevel değerini güvensiz olarak uygulayan (NTLMv1 Protokolüne İzin Veren) GPO'ların bu ayarı hangi bilgisayarlara uyguladığı net biçimde görüntülenebilir. Ayrıca Export fonksiyonu üzerinden ilgili liste Excel formatında elde edilebilir.

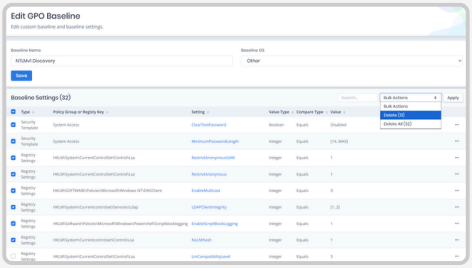


3. GPO Audit modülü içerisinde sadece LmCompatibilityLevel ayarının durumunu kontrol eden bir Baseline oluşturulur. Ardından RSOP Audit sayfasına gidilerek bu Baseline ile tüm bilgisayarlar üzerinde karşılaştırma yapılarak güvensiz konfigürasyon barındıran bilgisayarlar tespit edilebilir. Ayrıca bu arayüz üzerinden güvensiz konfigürasyonun hangi Group Policy objesinden kaynaklandığı da görülebilmektedir.

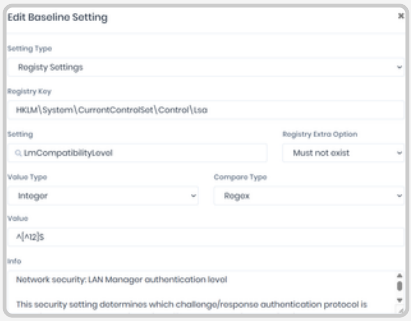
a. GPO Audit modülü altındaki Custom Baselines sayfasına gidilir. New Baseline butonuna tıklanır, yeni oluşturulacak baseline'a bir isim (NTLMv1 Discovery) verilir. OS alanı bu senaryoda önemsiz olduğundan Other seçilir. Süreci kolaylaştırmak adına Baseline Template olarak Forestall - FSBaseline General v1 seçilir. Save butonuna tıklanarak yeni baseline oluşturulur.



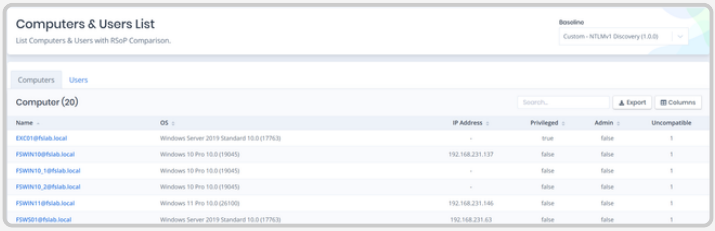
b. Custom Baselines sayfasından oluşturulan yeni baseline'a tıklanarak detay sayfasına gidilir. Öncelikle tabloda gösterilen satır sayısı arttırılır, en sol sütunda bulunan tümünü seç kutucuğu işaretlenir. Ardından sadece LmCompatibilityLevel ayarı için kutucuktaki işaret kaldırılır. Sağ üst kısımda bulunan Bulk Actions üzerinden Delete seçeneği seçilir ve Apply butonuna tıklanır. Bu işlemden sonra ilgili baseline sadece LmCompatibilityLevel ayarını kontrol edecektir.



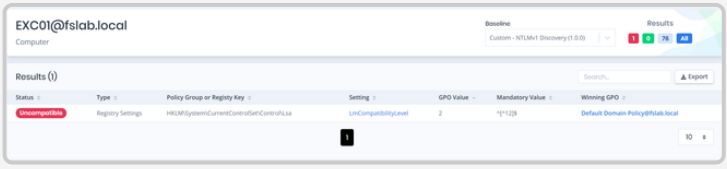
c. LmCompatibilityLevel ayarı ve 1 veya 2 olarak tanımlanmış bilgisayarları tespit edebilmek için, ilgili satırda en sağdaki üç noktaya ardından da Edit butonuna tıklanır. Açılan sayfada Compare Type değeri Regex olarak seçilir, Value alanına ise ^[^12]$ regex değeri girilir. Save butonuna tıklanarak ayar kayıt edilir. Regex kısmına farklı değerler girilerek farklı kontroller de gerçekleştirilebilir.



d. Karşılaştırma işlemini yapmak için RSOP Comparison sayfasına gidilir. Sağ üst kısımdaki Baseline seçeneğinden yeni oluşturan baseline seçilir. Baseline seçildiği anda kontrol otomatikman gerçekleştirilir ve oluşturulan baselinea uyumlu olmayan bilgisayarların Uncompatible sütunu 1 olarak görülebilmektedir.



e. Detayları görmek için istenilen bir bilgisayar detayına tıklanır. Sağ üst kısımda kırmızı olarak işaretlenen Uncompatible filtresine tıklanır, bu filtre sonucunda LmCompatibilityLevel değerinin nasıl konfigüre edildiği GPO Value sütununda, hangi GPO tarafından bu bilgisayara ulaştığı ise Winning GPO sütununda görülebilmektedir.



Bu yöntemlere alternatif olarak aşağıdaki Powershell scripti ile tüm sunucu ve istemcilerden ilgili değerin sorgusu yapılabilmektedir.

Not: Bu scriptin çalıştırılabilmesi için komutun çalıştırıldığı bilgisayarda RSAT veya Powershell ActiveDirectoryModule yüklü olmalıdır.

Not: Bu scriptin sağlıklı bir şekilde çalışabilmesi için kullanıcının hedef bilgisayarlarda en az Registry okuma yetkisine sahip olması gerekmektedir.

Not Set (OS Default) olarak görünen sistemlerde davranış işletim sistemi sürümüne bağlıdır (Vista/2008+ için varsayılan Level 3). Bu sonuçlar, ortamda eski GPO'lar tarafından downgrade edilmiş sistemlerin hızlıca tespit edilmesini sağlamaktadır.

@forestall

```
# Ortamdaki tüm bilgisayarların LmCompatibilityLevel değerlerini raporlama
$Computers = Get-ADComputer -Filter * -Properties OperatingSystem |
Select-Object Name, OperatingSystem

$Results = foreach ($Computer in $Computers) {
 $Level = Invoke-Command -ComputerName $Computer.Name -ErrorAction SilentlyContinue -
ScriptBlock {
 $RegPath = 'HKLM:\System\CurrentControlSet\Control\Lsa'
 $Value = Get-ItemProperty -Path $RegPath -Name 'LmCompatibilityLevel' -ErrorAction
SilentlyContinue
 if ($Value) { $Value.LmCompatibilityLevel } else { 'Not Set (OS Default)' }
 }
 [PSCustomObject]@{
 ComputerName = $Computer.Name
 OperatingSystem = $Computer.OperatingSystem
 LmCompatLevel = $Level
 }
}

$Results | Sort-Object LmCompatLevel |
Format-Table -AutoSize
$Results |
Export-Csv -Path "LmCompatibilityLevel_Inventory.csv" -NoTypeInformation -Encoding UTF8

# Özet rapor
$Results |
Group-Object LmCompatLevel |
Sort-Object Count -Descending |
Select-Object Count, Name |
Format-Table -AutoSize
```

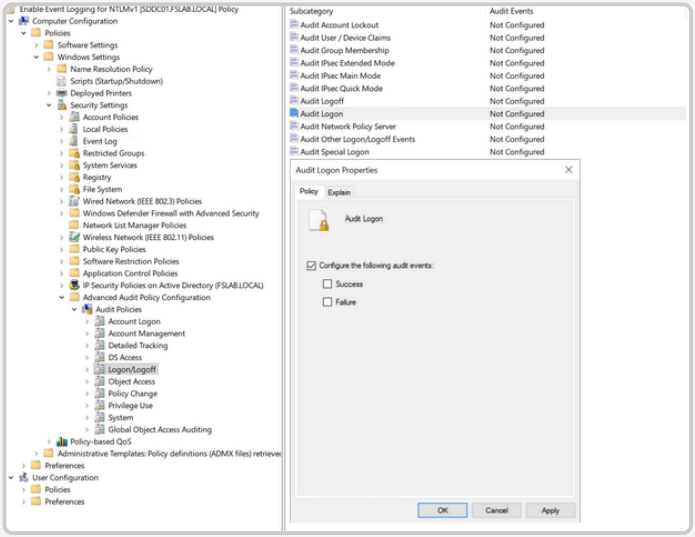
NTLMv1 Trafiğinin Event Loglar ile Tespit Edilmesi

NTLM tabanlı kimlik doğrulamalarını analiz edebilmek için ortamda **4624 (Logon) güvenlik olaylarının toplanması gerekmektedir**. Bir kullanıcı veya servis bir **sunucuya veya kaynak barındıran endpoint'e kimlik doğrulaması yaptığında**, ilgili **4624 olayı o sistemin Security log'una kaydedilmektedir**.

Bu nedenle kapsamlı bir analiz için 4624 loglarının yalnızca üye sunuculardan değil, **kaynak barındıran tüm sunucu ve endpoint'lerden** toplanması gerekmektedir.

Not: Domain Controller tarafında oluşan 4776 olayı ise NTLM doğrulama girişimini göstermekte, ancak kullanılan NTLM sürümünü içermemektedir. Bu nedenle NTLMv1 kullanımını analiz etmek için özellikle 4624 logları kritik öneme sahiptir.

4624 loglarının üretilebilmesi için **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy > Audit Policy > Logon/Logoff > Audit Logon** politikasının etkinleştirilmesi gerekmektedir:



Bu politika aktif edildiğinde sistemler 4624 loglarını üretmeye başlayacaktır. Bu loglar üzerinden NTLMv1 kullanılan oturum açma işlemleri tespit edilebilecektir.

SIEM çözümü yardımıyla, 4624 olayları merkezi olarak toplanarak NTLMv1 trafiğini tespit eden kurallar yazılabilmektedir. Böylece hangi sistemlerin, uygulamaların veya servis hesaplarının NTLMv1 kullandığı merkezi olarak analiz edilebilmektedir. Aşağıdaki SIGMA kuralı bu amaçla kullanılabilir.

@forestall

```
title: NTLMv1 Authentication Detected
id: b4efd38b-7a7a-45ad-9914-f677f9071f34
description: Alert triggers when the NTLM request is made with insecure version 1.
version: 1
ttp: T1550 # custom field – not part of the official Sigma specification
status: experimental
performance: high # custom field – not part of the official Sigma specification
author:
 - linkedin: serdal-tarkan-altun
 - twitter: TarkanSerdal
date: 2026/03/09
references:
 - https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-
10/security/threat-protection/auditing/event-4624
 - https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-
directory-hardening-series---part-1-%E2%80%93-disabling-ntlmv1/3934787
tags:
 - attack.credential_access
 - attack.t1550
logsource:
 product: windows
 service: security
 definition: "Requires Audit Logon policy enabled (Computer Configuration > Policies >
Windows Settings > Security Settings > Advanced Audit Policy > Logon/Logoff > Audit
Logon)"
detection:
 selection:
 EventID: 4624
 AuthenticationPackageName: NTLM
 LmPackageName|contains: 'NTLM V1'
 filter_anonymous:
 TargetUserName: 'ANONYMOUS LOGON'
 condition: selection and not filter_anonymous
falsepositives:
 - Anonymous Logon sessions (filtered by rule)
 - Some environments where 4624 field interpretation is misleading without correlation
level: high
```

Önemli: NTLMv1 kullanımını doğru tespit edebilmek için 4624 olaylarının yalnızca DC'lerden değil, tüm üye sunucular ve istemcilerden toplanması gerekmektedir. Bir sunucuya yapılan kimlik doğrulamada 4624 olayı ilgili sunucunun kendi loguna yazılmaktadır.

Önemli: Eğer ortamınızdaki tüm Domain Controller'lar Windows Server 2025 ise daha gelişmiş loglar aktif edilebilmektedir. Bu loglar (4020, 4021, 4022, 4023, 4030, 4031, 4032, 4033) sayesinde NTLM kimlik doğrulama trafiği daha görünür hale gelmekte ve NTLMv1 bağımlılıklarının tespiti kolaylaşmaktadır. Ayrıca 4032 logu sayesinde 4624 logunu tüm istemci ve sunucularda aktif etmeye gerek kalmamaktadır. Bu durum da süreci hızlandırabilmektedir.

Uyarı — False Positive: 4624 loglarında ANONYMOUS LOGON oturumları NTLMv1 olarak görülebilmektedir, ancak bunlar gerçek NTLMv1 kullanıcı kimlik doğrulamaları değildir. Bu kayıtlar filtrelenmelidir.

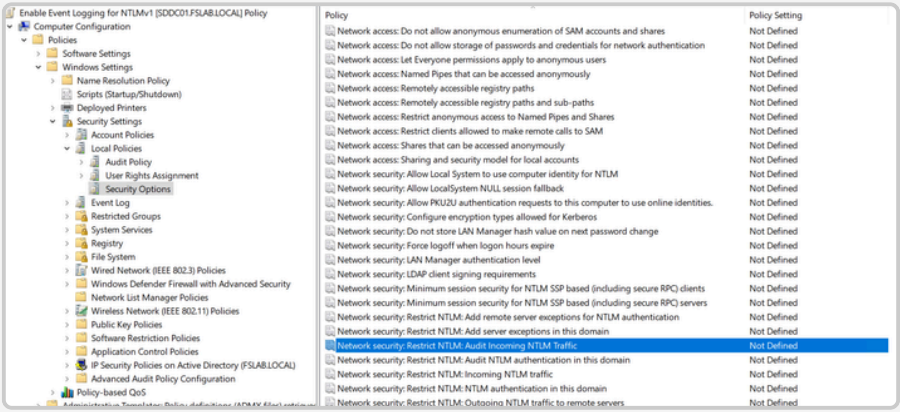
Uyarı: Microsoft, bazı senaryolarda 4624 üzerindeki LmPackageName = NTLM V1 bilgisinin tek başına kesin kanıt olarak yorumlanmaması gerektiğini belirtmektedir. Kritik kararlar için bu sinyal; ağ trafiği, Restrict NTLM event'leri (8001-8004) veya ek DC telemetry'si ile korele edilmelidir.

LmCompatibilityLevel ayarı dışında Microsoft, NTLM kullanımını daha granüler seviyede denetlemek ve kısıtlamak için ek GPO politikaları sunmaktadır. Bu politikalar audit fazında hangi sistemlerin NTLM kullandığını tespit etmek için 4624 loglarından daha detaylı veri sağlar:

Politika	Açıklama	Event ID
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Domain içindeki tüm NTLM kimlik doğrulamalarını denetler	8004
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Sunucuya gelen NTLM trafiğini denetler	8001, 8002
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	İstemciden çıkan NTLM trafiğini denetler/engeller	8003
Network security: Restrict NTLM: NTLM authentication in this domain	Domain seviyesinde NTLM kullanımını engeller	8004

Bu politikalar önce "Audit" modunda etkinleştirilmeli ve üretilen 8001-8004 Event ID'leri analiz edilmelidir. Bu loglar hangi uygulamanın, hangi sunucuya, hangi kullanıcı hesabıyla NTLM kullandığını gösterecektir.

Belirtilen logların üretilebilmesi için **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options** yolundaki ilgili konfigürasyonların etkinleştirilmesi gerekmektedir.



İlgili loglar **Event Viewer** ile **Event Viewer > Applications and Services Logs > Microsoft > Windows > NTLM > Operational** yolunda görülebilecektir.

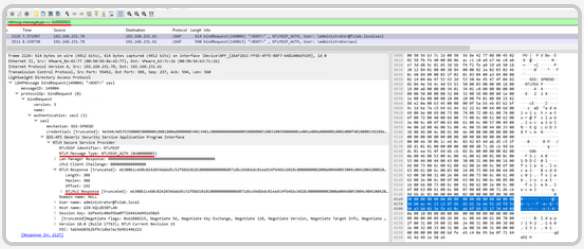
Not: Bu politikalar NTLMv1'e özel değil, tüm NTLM kullanımını (v1 ve v2) kapsar. NTLMv1 kapatma çalışmasının ötesinde, uzun vadeli NTLM eliminasyonu için de bu politikalar kritik öneme sahiptir.

Farklı Kaynaklar ile NTLMv1 Trafiğinin Tespit Edilmesi

Event log'lara ek olarak, ağ seviyesinde de NTLMv1 trafiği tespit edilebilmektedir. Bu yöntem özellikle log toplanamayan legacy sistemler veya SIEM kapsamı dışındaki ağ segmentleri için kritik önem taşımaktadır.

Wireshark veya benzer bir ürün ile ağ üzerindeki NTLMSSP paketleri analiz edilebilir:

- Filtre: ntlmssp.messagetype == 0x00000003 (AUTHENTICATE_MESSAGE)
- NTLMSSP paketinde NtlmV1Response alanının varlığı NTLMv1 kullanımını göstermektedir.
- NtlmV2Response alanı ise NTLM versiyonunu belirtmektedir.



NDR (Network Detection and Response) Çözümleri: Kurumsal ortamlarda ağ trafiğini sürekli izleyen NDR çözümleri NTLM sürüm tespitini otomatik olarak yapabilir.

Bu araçlar:

- NTLMv1 kullanımını gerçek zamanlı olarak tespit etmekte ve alarm üretebilmektedir.
- Hangi istemcinin hangi sunucuya NTLMv1 ile kimlik doğrulaması yaptığını görselleştirebilmektedir.
- Event log toplanamayan sistemlerdeki NTLM trafiğini de yakalayabilmektedir.

Bahsedilen mekanizmalar üzerinden tespit süreci başlatıldıktan sonra belli bir süre (örn 1 Ay) analiz devam ettirilmelidir. Bu süre içerisinde NTLMv1 trafiği üreten sunucular, uygulamalar, cihazlar ve bu istemcilerin neden **NTLMv1** trafiği ürettiği tespit edilmelidir.

Remediation

Discovery ardından adım adım bağımlıkların gerekli yollarla (Örn, sürüm güncelleme, kaynak kodda değişiklik, konfigürasyon değişikliği vb) kaldırılması gerekmektedir.

NTLMv1 bağımlılıkları çoğu zaman Windows dışı sistemlerde veya eski Microsoft servislerinde bulunur. Aşağıda bağımlılıklara dair bazı örnekler verilmiştir.
Windows dışı sistemler:

- NAS cihazları (Synology, QNAP vb.)
- Yazıcı ve MFP cihazları (scan-to-folder, SMTP relay)
- Legacy uygulamalar
- Linux / Samba sistemleri (eski Samba sürümleri varsayılan olarak NTLMv1 kullanabilir)

Microsoft servisleri ve uygulamalar:

Servis	**NTLMv1 Risk Alanı**
SQL Server	Eski sürümlerde (2008 ve öncesi) veya Named Pipes üzerinden bağlantılarda NTLM fallback
IIS	Windows Authentication modülü ile çalışan eski web uygulamaları
Exchange	OWA, ActiveSync, Autodiscover — özellikle eski CAS sunucularında
SCCM/MECM	Client push installation ve site-to-site iletişiminde NTLM kullanımı
Print Services	Point and Print sürücü yüklemelerinde NTLMv1 fallback
ADFS	Intranet authentication senaryolarında NTLM kullanımı
DFS	DFS referral ve namespace erişiminde NTLM fallback

Önemli Not: Eğer ortamda NTLMv1 kullanması gereken sunucu ve sistemler varsa bunlar da dokümante edilmeli ve exclusion sürecine tabi tutulmalıdır. Fakat bu sistemler DC sunucularına erişiyorsa, NTLMv1 kapatma süreci tamamlanamayacaktır. Bu nedenle, böyle bir durumla karşılaşıldığı anda ilgili sistemler için farklı senaryolar üretilmeli ve DC'ye erişim ihtiyacı bir şekilde ortadan kaldırılmalıdır.

Enforcement

Bu adımda NTLMv1 bağımlılıkları kaldırılan sistemler için gerekli konfigürasyon değişiklikleri adım adım uygulanmalıdır.

Domain Controller üzerinde NTLMv1'i doğrudan engellemek bazı uygulama ve servislerde kimlik doğrulama sorunlarına neden olabilir. Bu nedenle değişiklikler istemci, sunucu ve Domain Controller sırasıyla dikkatli ve kademeli şekilde uygulanmalıdır.

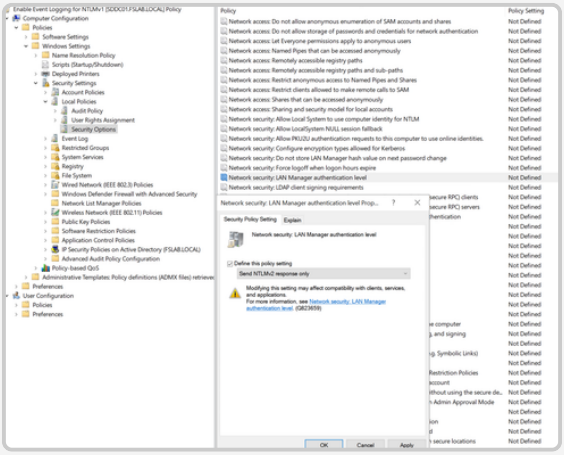
Kritik Uyarı — Hesap Kilitleme Riski: DC LmCompatibilityLevel = 5 olarak yapılandırıldığında, NTLMv1 ile gelen istekler hatalı parola girişimi olarak değerlendirilmektedir. İstemci tarafındaki yeniden deneme davranışı nedeniyle bu durum hızlı hesap kilitlenmelerine yol açmaktadır. Microsoft'un testlerinde, tek bir NTLMv1 SMB bağlantısının 46 başarısız oturum açma denemesi ürettiği gözlemlenmiştir. Bu nedenle DC'lerde Level 5 uygulanması, tüm istemcilerin Level 3 veya üstüne geçirilmesinden sonra yapılmalıdır.

NTLMv1 devre dışı bırakma sürecinde doğru uygulama sırası:

- İstemcilerin NTLMv2 kullanacak şekilde yapılandırılması (LmCompatibilityLevel = 3)
- Sunucuların NTLMv1 kabul etmesinin engellenmesi (LmCompatibilityLevel = 5)
- Domain Controller tarafında tam engelleme uygulanması (LmCompatibilityLevel = 5)
- İstemcilerin NTLMv1 kabul etmesinin engellenmesi (LmCompatibilityLevel = 5)

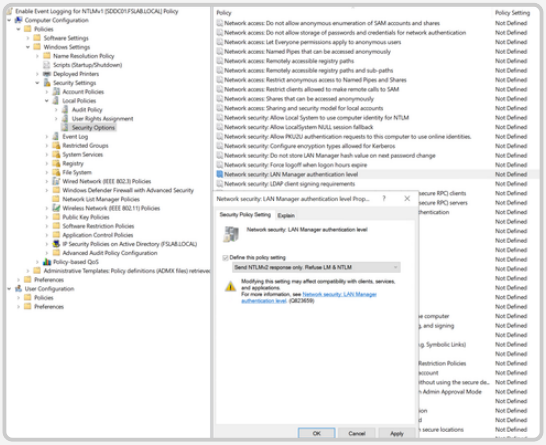
NTLMv1 devre dışı bırakma işleminin Group Policy (GPO) üzerinden aşağıdaki şekilde yapılması önerilmektedir.

- İstemcilere uygulanan ve güvensiz konfigürasyon barındıran (LmCompatibilityLevel 3'ten küçük) Group Policy objeleri bulunuyorsa, bu objeler üzerinde aşağıdaki işlemler gerçekleştirilir.
- Grup İlkesi Yönetim Konsolu (GPMC) yönetici ayrıcalıklarıyla açılır.
- Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Network Security: LAN Manager Authentication Level politikası detayları açılır.
- Send NTLMv2 response only politikası ayarlanır.
- Güncellenen GPO ilgili istemcilere uygulanır



Bu ayar uygulandıktan sonra belli bir süre de daha analiz yapılması gerekmektedir. Bu analiz süresi sonucunda herhangi bir erişim kesintisi yaşanmadığı takdirde bu ayarlar diğer istemcilere genişletilir.

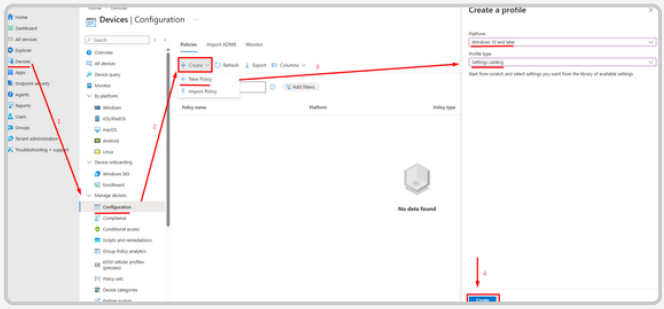
Tüm istemcilere ilgili uygulama yapıldıktan sonra aynı ayar sunuculara LmCompatibilityLevel = 5 şeklinde uygulanır, yine belli bir süre analiz yapıldıktan sonra herhangi bir erişim problemi olmazsa Domain Controller sunucularında da LmCompatibilityLevel = 5 olarak konfigüre edilir.



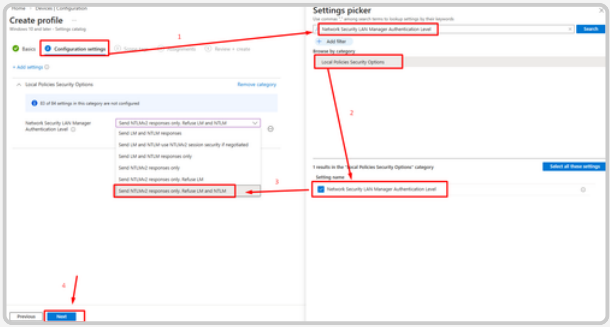
GPO ile yönetilmeyen, Microsoft Intune veya diğer MDM çözümleriyle yönetilen cihazlar için LmCompatibilityLevel aşağıdaki yöntemlerle yapılandırılabilir:

Settings Catalog (Önerilen):

1. Intune yönetim merkezinde Devices > Configuration > Create > New Policy yolu izlenir.
2. Platform olarak Windows 10 and later, profil tipi olarak Settings Catalog seçilir ve Create edilir.



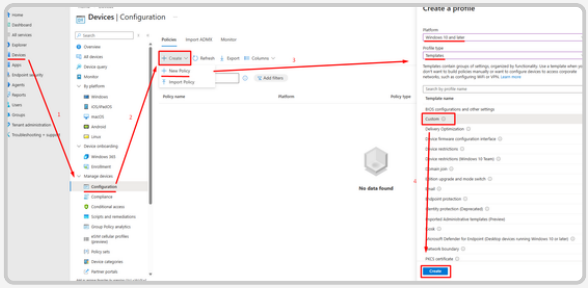
3. Network Security LAN Manager Authentication Level ayarı tespit edilir.
4. Değeri Send NTLMv2 response only. Refuse LM & NTLM olarak ayarlanır ve diğer adımlar Next diyerek tamamlanır.



Custom OMA-URI:

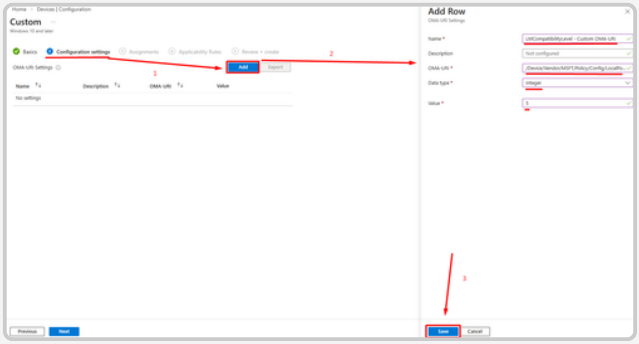
Alternatif olarak, custom profil ile doğrudan registry ayarı uygulanabilir:

1. Intune yönetim merkezinde Devices > Configuration > Create > New Policy yolu izlenir.
2. Platform olarak Windows 10 and later, profil tipi olarak Template ve ardından Custom seçilir.



3. Configuration Settings adımında Add Row yolu izlenir. Çıkan ekranda aşağıdaki değerler girilir. Doğrudan registry ayarı uygulanmış olur.

- Name: LmCompatibilityLevel
- OMA-URI: ./Device/Vendor/MSFT/Policy/Config/LocalPoliciesSecurityOptions/NetworkSecurity_LANManagerAuthenticationLevel
- Veri tipi: Integer
- Değer: 5



Hybrid Azure AD Join / Entra ID Join Senaryoları: Cloud-managed cihazlar Kerberos için DC erişimine ihtiyaç duymaktadır. VPN veya Always On VPN olmadan çalışan uzak cihazlarda Kerberos kullanılamayacağı için NTLM fallback yaşanabilmektedir. Bu durumda IAKerb veya cloud trust yapılandırması değerlendirilmelidir.

Birden fazla forest veya domain trust'ı bulunan ortamlarda NTLMv1 kapatma ek dikkat gerektirir:

- Cross-forest NTLM: Forest trust üzerinden yapılan kimlik doğrulamalar Kerberos yerine NTLM'e düşebilmektedir. Bu durum özellikle selective authentication kullanılan trust'larda yaygındır.
- Farklı LmCompatibilityLevel değerleri: Trust edilen forest'ta LmCompatibilityLevel düşük bir değerde olabilmekte, bu durumda da cross-forest NTLM trafiği NTLMv1 olarak gerçekleşebilmektedir.
- SID Filtering: Trust'larda SID filtering aktifken bazı Kerberos ticket'ları reddedilmekte ve NTLM kullanılmaktadır.

Önerilen yaklaşım:

- Tüm trust edilen forest/domain'lerdeki LmCompatibilityLevel değerleri doğrulanmalıdır.
- Cross-forest 4624 logları analiz edilerek NTLM kullanımı tespit edilmelidir.
- Trust'lar üzerinden gelen NTLMv1 trafiğini engellemek için hem kaynak hem hedef forest'ta Level 5 uygulanmalıdır.

Rollback Planı

Enforcement sonrasında beklenmeyen kimlik doğrulama sorunları yaşanabilir. Bu durumda hızlı geri alma yapılabilmesi için aşağıdaki adımlar hazır tutulmalıdır:

- **GPO ayarları geri alınır:** LAN Manager Authentication Level politikası önceki değerine (Send NTLMv2 response only) döndürülür veya Not Configured olarak ayarlanır.
- **Registry temizliği:** GPO Not Configured yapılsa bile HKLM\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel değeri sistemde kalabilir. Gerekirse bu anahtar manuel olarak kaldırılır veya önceki değerine geri döndürülür.
- **Forced gpupdate:** Geri alma sonrası etkilenen sistemlerde gpupdate /force çalıştırılarak politikanın hemen uygulanması sağlanır.
- **Log takibi:** Geri alma sonrasında 4624, 4776 ve 8001-8004 olayları izlenerek kimlik doğrulama akışının normale döndüğü doğrulanır.

Monitoring

Enforcement süreci de tamamlandıktan sonra daha önce oluşturulan kurallar ile izleme süreci devam ettirilmelidir. Bu sayede NTLMv1 kullanmaya çalışan farklı bir sistem tespit edilebilir veya NTLMv1 denemesi yapan saldırganlar ortaya çıkarılabilir.

Uygulama Kontrol Listesi

NTLMv1 kapatma sürecinin eksiksiz takibi için aşağıdaki kontrol listesi kullanılabilir:

Audit Fazı:
- 4624 logları tüm sunucu ve endpoint'lerden toplanıyor mu?
- Restrict NTLM audit politikaları etkinleştirildi mi? (8001-8004 Event ID'leri)
- NTLMv1 kullanan kullanıcılar, servis hesapları ve sistemler tespit edildi mi?
- Cross-forest / trust üzerinden gelen NTLM trafiği analiz edildi mi?
- Kerberos fallback nedenleri (eksik SPN, duplicate SPN, IP erişimi) araştırıldı mi?

Remediation Fazı:
- NTLMv1 kullanan uygulamalar güncellendi veya alternatifle değiştirildi mi?
- Üçüncü taraf cihazlar (NAS, yazıcı, Linux/Samba) NTLMv2 desteğine geçirildi mi?
- SPN sorunları giderildi mi?
- Geçirilemeyen sistemler için istisna kaydı oluşturuldu mu?

Enforcement Fazı:
- Rollback planı hazır ve test edilmiş durumda mı?
- İstemcilerde LmCompatibilityLevel = 3 (veya üstü) uygulandı mı?
- Sunucularda LmCompatibilityLevel = 5 uygulandı mı?
- DC'lerde LmCompatibilityLevel = 5 uygulandı mı?
- İstemcilerde LmCompatibilityLevel = 5 uygulandı mı?
- Intune/MDM ile yönetilen cihazlar yapılandırıldı mı?
- Credential Guard etkinleştirildi mi?

Monitoring Fazı:
- SIEM'de sürekli izleme dashboard'u oluşturuldu mu?
- Enforcement sonrası 4624 loglarında NTLMv1 trafiği sıfırlandı mı?
- Eski GPO'ların modern sistemleri downgrade etmediği doğrulandı mı?

Proje Zaman Planı

Aşağıdaki zaman planı, orta-büyük ölçekli bir kurumsal ortam için NTLMv1 kapatma projesinin referans çerçevesidir. Ortam büyüklüğüne, legacy sistem sayısına ve ekip kapasitesine göre sürelerin uyarlanması gerekebilir.

Faz 0 — Proje Başlangıcı ve Hazırlık (Hafta 1-2)

Görev	Sorumlu	Süre
Proje paydaşlarının belirlenmesi	Proje Yöneticisi	1. hafta
Proje kapsamının tanımlanması (domain, forest sayısı, trust yapısı)	AD Ekibi	1. hafta
Rollback planının oluşturulması ve dokümante edilmesi	AD Ekibi	1-2. hafta
İletişim planının hazırlanması (etkilenen ekipler, duyuru takvimi)	Proje Yöneticisi	2. hafta
Mevcut LmCompatibilityLevel ve NTLM GPO'larının envanterinin çıkarılması	AD Ekibi	2. hafta

Faz 1 — Audit ve Keşif (Hafta 3-6)

Görev	Sorumlu	Süre
4624 Audit Logon politikasının tüm sistemlerde etkinleştirilmesi	AD Ekibi	3. hafta
Restrict NTLM audit politikalarının tüm sistemlerde etkinleştirilmesi	AD Ekibi	3. hafta
Logların merkezi toplama altyapısına aktarılması	SIEM Ekibi	3-4. hafta
NTLMv1 kullanım raporunun oluşturulması (kullanıcı, sistem, uygulama bazında)	Güvenlik Ekibi	4-5. hafta
Cross-forest / trust NTLM trafiğinin analizi	AD Ekibi	5. hafta
SPN sorunlarının tespiti ve Kerberos fallback nedenlerinin analizi	AD Ekibi	5-6. hafta
Ağ seviyesinde NTLMv1 taraması (Wireshark/NDR)	Ağ Güvenliği Ekibi	5-6. hafta

Faz 2 — Remediation (Hafta 7-14)

Görev	Sorumlu	Süre
NTLMv1 kullanan uygulamaların güncellenmesi veya alternatif çözüme geçirilmesi	Uygulama Ekipleri	7-12. hafta
Üçüncü taraf cihazların (NAS, yazıcı, Samba vb.) NTLMv2 uyumluluğunun sağlanması	Altyapı Ekibi	7-10. hafta
SPN düzeltmelerinin uygulanması	AD Ekibi	7-8. hafta
NTLMv2'ye geçirilemeyen sistemler için istisna kayıtlarının oluşturulması	Güvenlik Ekibi	10-12. hafta
İstisna kapsamındaki sistemlerin ağ izolasyonu ve kompansasyon kontrollerinin uygulanması	Ağ / Güvenlik Ekibi	11-14. hafta
Eski / çakışan GPO'ların temizlenmesi	AD Ekibi	8-9. hafta

Faz 3 — Pilot Enforcement (Hafta 15-18)

Görev	Sorumlu	Süre
Pilot OU/grup seçimi (düşük riskli sunucu ve istemci grubu)	AD Ekibi	15. hafta
Pilot grupta istemcilere LmCompatibilityLevel = 3 uygulanması	AD Ekibi	15. hafta
Pilot grupta sunuculara LmCompatibilityLevel = 5 uygulanması	AD Ekibi	16. hafta
1 hafta izleme — 4624 logları ve kullanıcı geri bildirimleri	Güvenlik Ekibi	16-17. hafta
Sorun varsa remediation, yoksa genişletme onayı	Tüm Ekipler	17-18. hafta

Faz 4 — Üretim Geneli Enforcement (Hafta 19-24)

Görev	Sorumlu	Süre
Tüm istemcilere LmCompatibilityLevel = 3 uygulanması (dalga dalga)	AD Ekibi	19-20. hafta
Tüm üye sunuculara LmCompatibilityLevel = 5 uygulanması (dalga dalga)	AD Ekibi	20-21. hafta
DC'lere LmCompatibilityLevel = 5 uygulanması	AD Ekibi	22. hafta
Tüm istemcilere LmCompatibilityLevel = 5 uygulanması (dalga dalga)	AD Ekibi	22. hafta
Intune / MDM ile yönetilen cihazların yapılandırılması	Endpoint Ekibi	19-21. hafta
Credential Guard etkinleştirilmesi (destekleyen sistemlerde)	Güvenlik Ekibi	20-22. hafta
Her dalga sonrası izleme ve eskalasyon	Güvenlik Ekibi	Sürekli

Faz 5 — Stabilizasyon ve Sürekli İzleme (Hafta 25+)

Görev	Sorumlu	Süre
SIEM'de kalıcı NTLMv1 monitoring dashboard'u oluşturulması	SIEM Ekibi	25. hafta
Haftalık NTLMv1 kullanım raporu otomasyonu	Güvenlik Ekibi	25. hafta
İstisna listesinin ilk periyodik gözden geçirmesi	Güvenlik Ekibi	25-26. hafta
Proje kapanış raporu ve lessons learned dokümantasyonu	Proje Yöneticisi	26. hafta

Not: Bu zaman planı bir referans çerçevesidir. Küçük ortamlarda kısaltılabilirken, büyük ve karmaşık ortamlarda doğal olarak uzayabilmektedir. Kritik olan, her fazın bir önceki fazın çıktılarına dayanması ve hiçbir fazın atlanmamasıdır.

Başarı Metrikleri ve KPI

NTLMv1 kapatma projesinin başarısını ölçmek ve ilerlemeyi yönetim katmanına raporlamak için aşağıdaki metrikler izlenmelidir:

Birincil Metrikler (Zorunlu):

Metrik	Hedef	Ölçüm Yöntemi
NTLMv1 Event Sayısı	0 (sıfır)	Loglarda NTLM V1 kayıt sayısı
Enforce Edilen Sistem Oranı	%100	LmCompatibilityLevel ≥ 3 olan sistem / toplam sistem
DC Enforcement Oranı	%100	LmCompatibilityLevel = 5 olan DC / toplam DC
Aktif İstisna Sayısı	Azalan trend	İstisna listesindeki kayıt sayısı

İkincil Metrikler (Önerilen):

Metrik	Hedef	Ölçüm Yöntemi
Ortalama Tespit Süresi (MTTD)	< 24 saat	Yeni NTLMv1 kaynağının SIEM'de tespit edilme süresi
İstisna Çözüm Oranı	Artan trend	Çözülen istisna / toplam istisna (üç aylık)
Kerberos Fallback Oranı	Azalan trend	4769 içindeki başarısız / anomali gösteren isteklerin trendi
Remediation Tamamlanma Oranı	%100	Düzeltilen bağımlılık / tespit edilen bağımlılık

Önemli: Enforcement sonrasında NTLMv1 event sayısının sürekli olarak sıfır kalması beklenir. Herhangi bir artış, yeni bir bağımlılığın ortaya çıktığını, konfigürasyon sapması yaşandığını veya istisna kapsamında olmayan bir sistemin NTLMv1 kullandığını gösterir ve derhal araştırılmalıdır.

Yeni NTLM Denetim Kayıtları

Windows 11 24H2 ve Windows Server 2025 ile birlikte NTLM audit kabiliyetleri geliştirilmiştir. İstemciler, sunucular ve Domain Controller'lar için daha ayrıntılı loglama imkânı sunulmuştur. Bu loglar (4020, 4021, 4022, 4023, 4030, 4031, 4032, 4033) sayesinde NTLM kimlik doğrulama trafiği daha görünür hale gelmekte ve NTLMv1 bağımlılıklarının tespiti kolaylaşmaktadır.

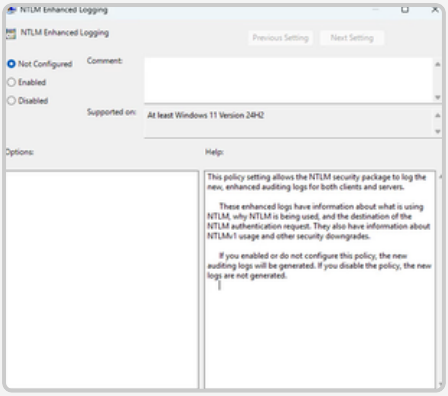
Önemli Not: Domain Controller'larda oluşan 4032 event logu NTLMv1 analiz sürecini hızlandırabilmektedir. Bu log sayesinde tüm istemci ve sunucularda 4624 logunu aktif etmeden analiz yapılabilmektedir.

Yeni log kayıtları, mevcut loglama yapısına kıyasla güvenlik ekiplerinin aşağıdaki sorulara daha net yanıt verebilmesini sağlar:

- Kim NTLM kullanıyor; Kullanılan hesap, ilgili makine ve süreci görünür hale getirir.
- Neden NTLM tercih ediliyor; Kerberos gibi modern protokoller yerine NTLM kullanımının gerekçesini ortaya koyar.
- Nerede NTLM kimlik doğrulaması gerçekleşiyor; İlgili makine adı ve IP adresi gibi bağlantı detaylarını sağlar.

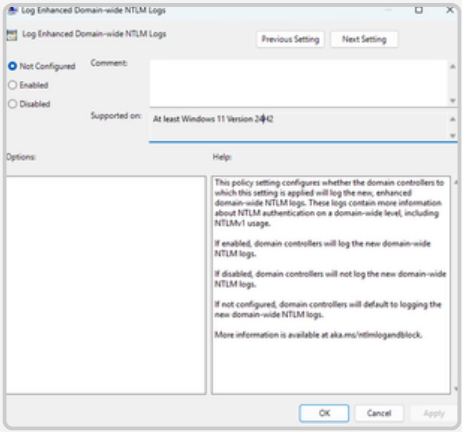
Gelişmiş log kayıtları ayrıca istemci ve sunucu tarafında NTLMv1 kullanımı hakkında bilgi üretirken, Domain Controller'lar üzerinde de etki alanı genelindeki NTLMv1 kullanımının izlenmesine imkân tanır.

İlgili loglar Event Viewer uygulamasında Event Viewer > Applications and Services Logs > Microsoft > Windows > NTLM > Operational yolunda görülebilmektedir.
İstemci ve sunucu tarafındaki gelişmiş NTLM logları Computer Configuration > Policies > Administrative Templates > System > NTLM > NTLM Enhanced Logging yolundaki ayarlar ile yönetilmektedir.



Tüm domain genelindeki gelişmiş NTLM logları ise domain controller üzerinde aşağıdaki policy ile kontrol edilir.

Domain genelindeki NTLM logları Computer Configuration > Policies > Administrative Templates > System > Netlogon > Log Enhanced Domain-wide NTLM Logs yolundaki ayarlar ile yönetilmektedir.



Event ID	Event Adı	Artıları	Eksileri
4776	Credential Validation	Yalnızca etki alanı denetleyicilerinden log toplanmasını gerektirir. Etki alanındaki NTLM kimlik doğrulama miktarını baz almak için kullanılabilir. "NTLM'yi en çok kullanan" hesapları tespit etmek için kullanılabilir.	Yalnızca istemciyi (workstation alanı) ve kimlik doğrulayan kullanıcı adını sağlar. Olay, erişilen kaynağı göstermez.NTLM versiyonuna ilişkin herhangi bir bilgi barındırmaz.
4624	An account successfully logged on	Kimlik doğrulayan kullanıcıyı, istemci adını ve erişilen sunucuyu kaydeder. Ayrıca müzakere edilen NTLM sürümünü de kaydeder.	Kaynak barındıran etki alanına bağlı tüm cihazlardan olay toplanmasını gerektirir. NTLM kullanan süreç veya uygulama hakkında bilgi sağlamaz.
8001-8006	An account used NTLM for either inbound or outbound authentication	Kimlik doğrulayan kullanıcıyı, istemci adını, sunucu adını ve NTLM kullanan süreçlerin adlarını kaydeder. Giden veya gelen NTLM kimlik doğrulamasına bağımlılığı olmayan hesap ve cihazları tespit etmek için kullanılabilir.	Etki alanındaki NTLM kullanımını kapsamlı şekilde anlayabilmek için etki alanına bağlı tüm cihazlardan olay toplanmasını gerektirir. Ancak yalnızca etki alanı denetleyicisi olaylarının (8004) toplanması bile, etki alanı kimlik doğrulaması için kimlik doğrulayan kullanıcıyı, istemci adını ve sunucu adını sağlayacaktır.
4001-4006	NTLM authentication was blocked	NTLM'nin ne zaman engellendiğini kaydeder; böylece istenmeyen bir etkinin farkına varabilirsiniz.	Engellenen NTLM kimlik doğrulamalarını kapsamlı şekilde anlayabilmek için etki alanına bağlı tüm cihazlardan olay toplanmasını gerektirir.
4020,4022, 4030,4032	An account used NTLM for either inbound or outbound authentication	Süreç adı, müzakere edilen flag'ler ve NTLM fallback oluşma nedeni dahil olmak üzere NTLM kimlik doğrulamaları hakkında çok ayrıntılı bilgi sağlar.	Yalnızca 24H2 / 2025 ve üzeri sürümlerde desteklenecektir. Etki alanındaki NTLM kullanımını kapsamlı şekilde anlayabilmek için etki alanına bağlı tüm cihazlardan olay toplanmasını gerektirir.
4021,4023, 4031,4033	NTLM authentication was blocked	NTLM engellendiğinde, 4001-4006 olaylarına göre daha ayrıntılı bilgi içerir.	Yalnızca 24H2 / 2025 ve üzeri sürümlerde desteklenecektir. Engellenen NTLM kimlik doğrulamalarını kapsamlı şekilde anlayabilmek için etki alanına bağlı tüm cihazlardan olay toplanmasını gerektirir.

MODERN KURUMLAR İÇİN
KİMLİK GÜVENLİĞİ **#01**

FORESTALL

Make identity risk visible across every identity - and actionable.