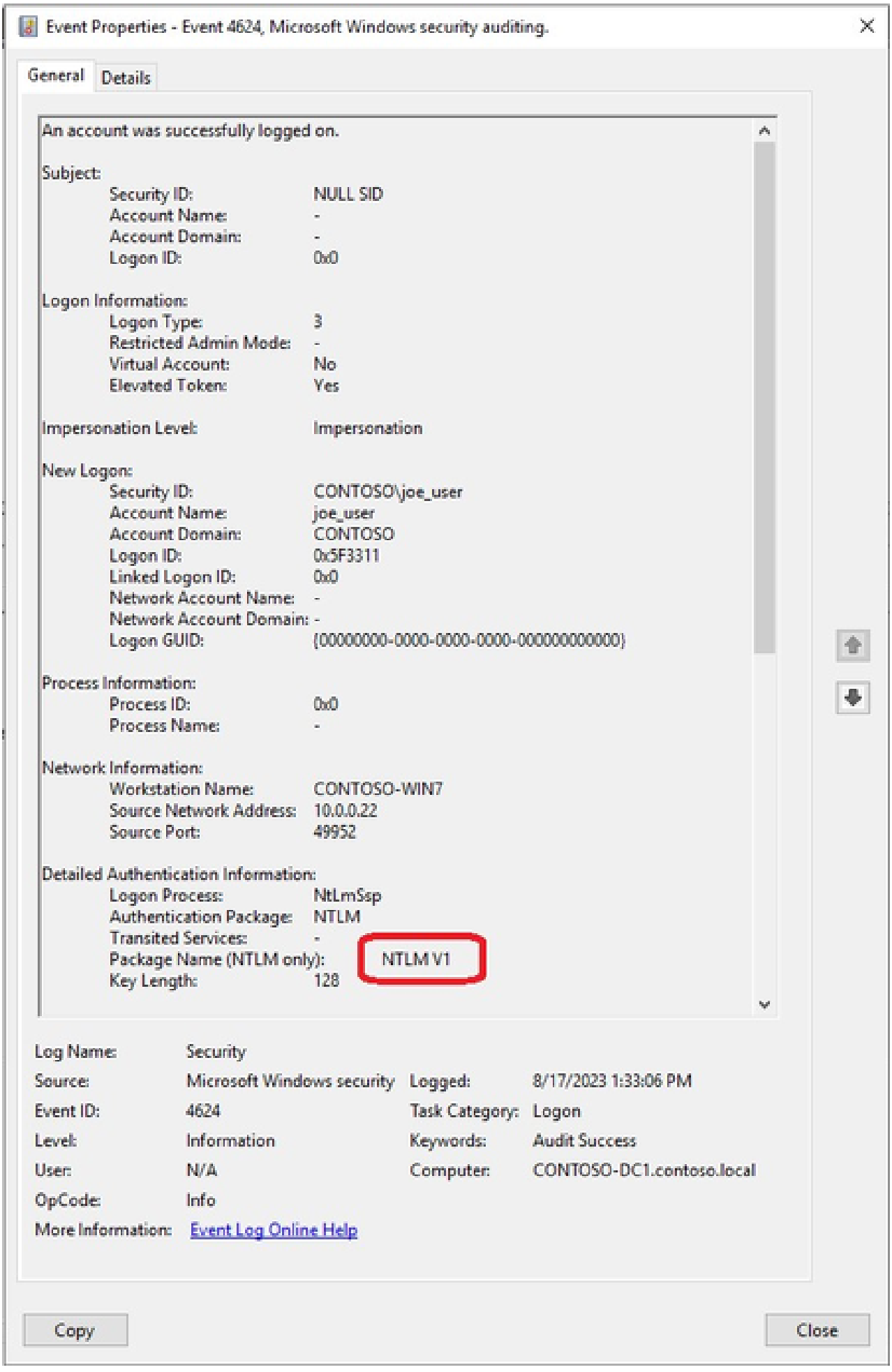
Active Directory Hardening Series - Part 1 – Disabling NTLMv1

techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-1—-disabling-ntlmv1/3934787


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Information:
Logon Type: 3
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: Yes
Impersonation Level: Impersonation
New Logon:
Security ID: CONTOSO\joe_user
Account Name: joe_user
Account Domain: CONTOSO
Logon ID: 0x5F3311
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}
Process Information:
Process ID: 0x0
Process Name: -
Network Information:
Workstation Name: CONTOSO-WIN7
Source Network Address: 10.0.0.22
Source Port: 49952
Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V1
Key Length: 128
Log Name: Security
Source: Microsoft Windows security
Logged: 8/17/2023 1:33:06 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: CONTOSO-DC1.contoso.local
OpCode: Info
More Information: Event Log Online Help
Copy
Close

Blog Post

Active Directory Hardening Series - Part 1 – Disabling NTLMv1

Hello everyone, Jerry Devore back again after to along break from blogging to talk about Active Directory hardening. In my role at Microsoft, I have found every organization has room to improve when it comes to hardening Active Directory. Many times, customers are aware of issues but are afraid of unintended impacts if they make a change. In other words, organizations are getting stuck in the "analysis paralysis" stage. In this series my goal is to help you understand how to move forward with confidence by better understanding the changes along with how to perform proper due diligence.

Before we jump into the first topic it's worth discussing why it is important to invest effort into Active Directory security given Microsoft considers it a legacy technology. After all, it is very compelling to prioritize moving to modern features offered by Entra ID rather than spending time on Active Directory. The simple explanation is cyber adversaries are continuing to have much success accessing privileged credentials by targeting Active Directory. As a result, they are able to gain control of critical data and systems. From there they often pivot to cloud resources as a secondary target.

We are often asked why Microsoft cannot simply harden Active Directory with a security update. While it would be nice if an "easy button" was an option, the reality is nearly all Microsoft customers are carrying a significant amount of "technical debt", which has complex dependencies on Active Directory. Microsoft moves the needle with Active Directory security where possible, but for the most part this must be a joint effort to avoid significant impacts to production environments. While pursuing Active Directory hardening can be a time and resource intensive initiative, bear in mind the checklist to proactively secure your Active Directory is often similar to the one required for compromised recovery. Having witnessed it performed both ways I can assure you it is better to tackle this effort proactively rather than in the midst of a crisis.

Enforcing NTLMv2

For the first topic in this series, I would like to address is the enforcement of NTLMv2. NTLMv2 has been around since Windows NT 4.0 SP4 and we have been talking about enforcing its use for well over 10 years now. There has been plenty written on how NTLM works and why NTLMv1 is no longer secure. Rather than recreating that content I will just stress these key concepts.

- Using NTLM does not send the account's clear password or even the password hash of over the wire. Instead, it uses a challenge / response protocol where the server sends the client a challenge (random number called a nonce), which the client will encrypt using the password hash as one of the inputs, then returns it to the server. In a domain environment the response is forwarded to a domain controller which verifies the challenge response. With NTLMv1 the encryption is based on DES (bad, bad, bad). When using NTLMv2 the encryption has more inputs and uses HMAC-MD5 (not great by today's standards but significantly better than DES).
- NTLMv1 is far more susceptible to man-in-the-middle and relay attacks due to weaker session security and weaker encryption used to generate challenge responses. As a result, adversaries can brute force captured packets to determine hashes or gain access to resources without even having the account's password hash.
- The version of NTLM and other options are negotiated between the client and server. Windows will always use the highest mutually supported version. When reading documentation keep in mind "client device" refers to the device that initiated the authentication request. It is not a reflection of the OS version.
- While Windows since NT 4.0 has been capable of NTLMv2, older operating systems did not attempt to negotiate NTLMv2 by default. Additionally, it is possible for an old GPO to downgrade the NTLM settings on current OS versions.
- Since 2008R2 Windows has supported disabling NTLM (except for local accounts), but as Steve Syfuhs pointed out Killing NTLM is Hard. If you have not enforced NTLMv2 in your environment yet, put the effort there rather than attempting to eliminate the protocol completely. At the same time look for opportunities to reduce NTLM by giving Kerberos every chance to work. The common culprits for NTLM fall back are missing Service Principal names (SPNs), duplicate SPNs or accessing resources using an IP address instead of a FQDN. To start tracking such issues begin by reviewing the failure codes in 4769 events. If you do want to take a swing at disabling NTLM, focus on individual servers rather than domain wide.

Configuration settings

The setting used to control NTLM negotiation behavior is referred to as LmCompatibilityLevel. When managed by the policy setting **Network security: LAN Manager authentication level** the registry key **HKLM\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel** will be created and configured.

The table below describes a description of the various levels (0-5). A few concepts that help explain the levels are:

- NTLM by itself is referring to NTLMv1.
- Windows stopped generating the LM Hash (by default) with Vista and Windows Server 2008 so unless the NoLMHash value has been changed, you don't need to worry about level 1 and 2 using the LM Hash instead of the NTLM hash

- Levels 0-3 control what the clients will request (NEGOTIATE_MESSAGE). Once at level 3 clients will **only** request NTLMv2.
- Levels 4-5 control what the server (recipient of the request) will accept during the negotiation which communicated back to the client in the CHALLENGE_MESSAGE.
- Anything less than level 3 means **NTLMv1 will be requested by the client**. Level 2 benefits from improved session security but it is still NTLMv1.
- Once the domain controllers are at level 5, only NTLMv2 is allowed for domain accounts. That is the goal, but it is the **last step** in the process.
- Enabling Credential Guard on a device disables NTLMv1 and the LmCompatibilityLevel setting is pretty much ignored. If you are not using Credential Guard, please give it serious consideration. It is a key feature for protecting credentials stored in LSASS memory.

Setting	**Description**	**Registry setting**
Send LM & NTLM responses	Client devices use LM and NTLM authentication, and they never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	0
Send LM & NTLM – use NTLMv2 session security if negotiated	Client devices use LM and NTLM authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	1
Send NTLM response only	Client devices use NTLMv1 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	2
Send NTLMv2 response only	Client devices use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication.	3
Send NTLMv2 response only. Refuse LM	Client devices use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM authentication, and they'll accept only NTLM and NTLMv2 authentication.	4

Send NTLMv2 response only. Refuse LM & NTLM	Client devices use NTLMv2 authentication, and they use NTLMv2 session security if the server supports it. Domain controllers refuse to accept LM and NTLM authentication, and they'll accept only NTLMv2 authentication.	5

The registry key HKLM\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel does not exist by default. When it is missing the OS version will determine the behavior. The table below shows the native behavior by OS.

OS	**Default LmCompatibilityLevel**
Sever 2000 \ XP	1 - NTLMv1
Server 2003	2 - NTLMv1 with v2 Session Security
Vista \ 2008 and higher	3 - NTLMv2

There is one more key consideration when working with this setting. The registry key outside the typical path for group policies (HKLM\SOFTWARE\Policies). As a result, the registry will become tattooed if the policy has a value set and then configured to "not defined". In that situation it will be necessary to clear the registry key from every device that has processed the policy if you want to remove the tattoo. Some documentation indicates it is necessary to reboot a device after modifying LmCompatibilityLevel. That is not correct. A change via policy or registry modification will be effective immediately.

Auditing for NTLMv1

If your environment has no legacy devices or old GPOs downgrading LmCompatibilityLevel, you should be ready to configure a domain wide policy to level 5 and call this project done. Before you pull that trigger it is highly recommended that you use auditing to confirm there are no unexpected dependencies on NTLMv1. For that you will need to focus on the **Package Name** field in **4624** Events.

Keep in mind that when the authentication occurs against a member server, the 4624 event will be logged in the security log of that server. The validating domain controller will log a 4776 event (The computer attempted to validate the credentials for an account) which does not capture the NTLM version. Therefore, you will need to collect the events from all servers in order to have a comprehensive understanding of the environment. If you are concerned about endpoint devices hosting resources, you will need to collect their 4624 events as well.

Hopefully your organization already has a SEIM solution that centrally collects security events and can help filter and visualize the data. If that is not the case, you can leverage the Windows Event Forwarding feature to forward all 4624 events into a centralized log file. Once the events are in a central log you could use some PowerShell code like this which will read the security log and export key details about NTLMv1 authentications.

```
Get-WinEvent -FilterXml @"

<QueryList>

<Query Id="0" Path="Security">

<Select Path="Security">

*[System[(EventID=4624)]]

[EventData[Data[@Name='LmPackageName'] and (Data='NTLM V1')]]

</Select>

</Query>

</QueryList>

"@ | Where-Object {$_.Properties[5].Value -ne "ANONYMOUS LOGON"} | Select-Object TimeCreated, @{Name='Account Name';Expression={$_.Properties[5].Value}}, @{Name='Account Domain';Expression={$_.Properties[6].Value}}, @{Name='Logon Type';Expression={$_.Properties[8].Value}}, @{Name='Workstation Name';Expression={$_.Properties[11].Value}}, @{Name='Source Network Address';Expression={$_.Properties[18].Value}} | Export-Csv -Path C:\NTLMv1Events.csv -NoTypeInformation
```

You may have noticed that my filter excludes Anonymous Logons. This is because they are not true NTLMv1 authentications as explained in this article.

Do's and Don'ts for disabling NTLMv1 in a domain

Hopefully this information will help give you confidence to take action in your environment. Just keep the following points in mind and you will be well on your way.

- **Don't** configure your domain controllers to level 5 until all devices in the domain are at level 3 or higher. At level 5, domain controllers will treat NTLMv1 requests as bad password attempts which will quickly lock out accounts due to clients retrying multiple times. In my testing a single NTLMv1 connection using SMB resulted in 46 failed logon attempts.
- **Don't** let the fear of breaking something keep you from addressing this security concern. Perform auditing and take action now rather than as part of a compromise recovery.

- **Don't** forget about 3rd party devices. Work with the device vendor if NTLMv1 authentications are discovered. If remediation is not possible the device should be retired or replaced.
- **Do** focus on getting all devices to level 3 as the first phase. That will ensure NTLMv2 is the only version requested by clients. Moving to level 5 is just a way to ensure a downgrade attack is not possible.
- **Do** consider managing LmCompatibilityLevel centrally (GPO\Intune\etc). Doing so will ensure there is no intentional or accidental configuration drift.
- **Do** spot check the registry of old devices to ensure an old policy has not created a tattooed value for LmCompatibilityLevel.
- **Do** know that CIS and Microsoft baselines recommend setting Windows devices to level 5 (refuse anything but NTLMv2).
- **Do** share any lessons you have learned from removing NTLMv1 in the comments section.
- **Do** check out the following excellent resources if you want to understand NTLM better.
    - Purging Old NT Security Protocols | Microsoft Learn
    - Stop using LAN Manager and NTLMv1! | Microsoft Learn
    - Audit event shows authentication package as NTLMv1 instead of NTLMv2 - Windows Server | Microsoft Learn
    - [MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol | Microsoft Learn
    - Security Watch: The Most Misunderstood Windows Security Setting of All Time | Microsoft Learn
    - Security guidance for NTLMv1 and LM network authentication - Microsoft Support
    - Auditing and restricting NTLM usage guide | Microsoft Learn
    - NTLM Overview | Microsoft Learn

Disclaimer

Updated Jan 15, 2025