Disabling NTLM Authentication Guide – part 4 – NTLM Restrictions and Testing

willssysadmintechblog.wordpress.com/2023/09/05/disabling-ntlm-authentication-guide-part-4-testing

September 5, 2023

Part 3: Disabling NTLM Authentication Guide – part 3 – Migrating to Kerberos

Part 5: Disabling NTLM Authentication Guide – part 5 – Printers and Scanners

You have logs and know what you'll need to make Kerberos work in 99% of cases. Now you need to test disabling NTLM authentication on some systems. To do that we're going back to our logging settings in the Local Security Policy. These settings can also be set via GPO.

Client Settings

An easy and low-impact way to test disabling NTLM on a server is to disable it on a client, instead. You can do this with the setting named *Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers.* Give your client computer a restart after changing this setting to make sure it applies, although it may not need it, I can't remember.

This setting prevents your client computer from sending NTLM authentication requests. You can see if an NTLM auth request gets blocked in EventID 4001.

I wouldn't recommend using this outbound setting as your target for NTLM enforcement. You never know when a computer will need to use NTLM authentication to a server that your organization doesn't manage. The list of NTLM exceptions needed and user headaches would not be worth it.

Server Settings

You can tell a server to refuse incoming NTLM authentication requests with this setting: *Network security: Restrict NTLM: Incoming NTLM traffic*. This setting does not require a reboot to take effect.

This setting makes your server refuse incoming NTLM authentication requests. You can see if an NTLM auth request gets blocked in EventID 4002.

You can also accomplish the same task by setting this setting on domain member servers: *Network security: Restrict NTLM: Audit NTLM authentication in this domain*. That setting creates logs in EventID 4003 when NTLM is blocked, and they contain more information than the 4002 events.

Domain Controller Settings

In our case, I wanted DCs to eventually enforce NTLM being disabled. We used the client and server side settings for extended testing, but eventually the NTLM block was done on the domain controllers. This was done for 4 reasons:

1. Domain controllers generate the best logs, and they're generated all in one place (on the DCs).
2. This would ensure no systems would slip through the cracks if they don't have a certain group policy applied.
3. Changing what computers can use NTLM would require a high level change by domain admins, necessitating review of the change and approval by policy makers.
4. Similarly, an admin seeking to allow NTLM on their system would be offered domain admin help to migrate their authentication to something better before giving up and allowing NTLM.

The setting that causes DCs to restrict NTLM is: *Network security: Restrict NTLM: NTLM authentication in this domain.* Member servers may still pass DCs NTLM authentication requests, but they'll be squashed at the DC level. The DCs log these blocks in EventID 4004. This setting does not require a reboot to take effect.

Privacy Settings
For systems that will still need to process NTLM authentication, you can do this with the setting: *Network security: Restrict NTLM: Add server exceptions in this domain.* In the setting text box, add each computer (hostname or AD FQDN) per line. If you want to be careful like me, add both on separate lines. This setting does not require a reboot to take effect.

End of Project Settings Note

Once you're at the end of the project, I recommend stopping use of the local NTLM disablement settings (block Incoming, block Outgoing) and just rely on the domain wide setting on domain controllers, as I mentioned above. For clients where you've disabled NTLM locally, I'd even recommend changing those settings to *Allow NTLM*, or *Unconfigured* (See my gotcha note below to decide which). This will force servers to pass the NTLM auth requests on to the DCs where it will be blocked. You'll get the benefits of DC-side enforcement I discussed above.

Potential Gotcha

Simply changing these settings to “unconfigured” will not revert to allowing NTLM, as the underlying registry value isn’t reverted. Once you disable NTLM on a system with one of these settings you must leave it configured and change the value in the configuration. If you use GPOs to configure this setting you will need two: one to disable NTLM; one to enable NTLM.

If you configure these NTLM settings locally, the computer will remember the last local setting you set. If you later configure them via GPO, and then unlink those GPOs, the computer will revert to the last local policy you had set. This caused me to accidentally disable NTLM on a computer that needed it 1 year after I started testing with it.

Part 1: Disabling NTLM Authentication Guide – part 1 – Prerequisites

Part 2: Disabling NTLM Authentication Guide – part 2 – Logs

Part 3: Disabling NTLM Authentication Guide – part 3 – Migrating to Kerberos

Part 4: Disabling NTLM Authentication Guide – part 4 – NTLM Restrictions and Testing

Part 5: Disabling NTLM Authentication Guide – part 5 – Printers and Scanners

Part 6: Disabling NTLM Authentication Guide – part 6 – RDP

Part 7: Disabling NTLM Authentication Guide – part 7 – Kerberos Logs