User name:
Password:
Login / Forgot?
Register

Security Log | Windows | SharePoint | SQL Server | Exchange | | | Training | Tools | Newsletter | Webinars | Blog

WinSecWiki | Patch Analysis | Webinars

Network Security

- Do not store LAN Manager hash value on next password change
- Force log off when logon hours expire
- LAN Manager authentication level
- LDAP client signing requirements
- Minimum session security for NTLM SSP based (including secure RPC) clients
- Minimum session security for NTLM SSP based (including secure RPC) servers

WinSecWiki > Security Settings > Local Policies > Security Options > Network Security > Minimum session security for NTLM SSP based (including secure RPC) servers

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

This value impacts applications, from the point of view of the server, that use the NTLM SSP or secure RPC and specifies session security requirements for communication between the client and server.

Hex value	Check box	Meaning
0x0	None checked	None. No security is used for session security.
0x10	Require message integrity	Message integrity. If the value of either this entry or the NtlmMinClientSec entry is 0x10, then the connection will fail unless message integrity is negotiated.
0x20	Require message confidentiality	Message confidentiality. If the value of either this entry or the NtlmMinClientSec entry is 0x20, then the connection will fail unless message confidentiality is negotiated.
0x80000	Require NTLMv2 session security	NTLMv2 session security. If the value of either this entry or the NtlmMinClientSec entry is 0x80000, then the connection will fail unless NTLMv2 session security is negotiated.
0x20000000	Require 128-bit encryption	128-bit encryption. If the value of either this entry or the NtlmMinClientSec entry is 0x20000000, then the connection will fail unless 128-bit encryption is negotiated

As best I can tell, this setting will primarily impact secure RBC communications such as between Outlook and Exchange when authenticating via NTLM.

Unanswered questions: how do these settings affect SMB traffic or do they? Do these setting apply to all RPC traffic, only secure RPC traffic or just secure RPC traffic authenticated via NTLM instead of Keberos? How do these setting affect traffic sent via the Kerberos SSP? If they don't, how do you set similar requirements for Kerberos SSP?

Underlying registry key and value

NtlmMinServerSec HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0

Data type	Range	Default value
REG_DWORD	0x0 | 0x10 | 0x20 | 0x80000 | 0x20000000	0x0

Excellent sources for more information on NTLM: http://davenport.sourceforge.net/ntlm.html by Eric Glass and http://www.microsoft.com/technet/technetmag/issues/2006/08/SecurityWatch/

Back to top

About | Newsletter | Contact

Terms of Use | Privacy |