Article ID: 954387 - Last Review: July 14, 2008 - Revision: 1.2

You may experience authentication issues when you access a network-attached storage device after you upgrade to Windows Server 2008, to Windows Vista, to Windows Server 2003, or to Windows XP

SYMPTOMS

When you access a network-attached storage device after you upgrade to Windows Server 2008, to Windows Vista, to Windows Server 2003, or to Windows XP, you may experience authentication issues. Typically, you receive an error message that states that access is denied or that the operating system cannot log on the user. This issue occurs even though you provide the correct user name and the correct password.

CAUSE

By default, Windows-based client computers are configured to use only NTLM version 2 (NTLMv2) authentication when the client computers use challenge/response authentication to authenticate to servers. This default behavior may cause problems when Windows authenticates to third-party products that cannot handle NTLMv2 authentication.

WORKAROUND

To work around this issue, follow these steps:

1. Click **Start**, click **Run**, type **regedit** in the **Open** box, and then click **OK**.
2. Locate and then click the following subkey: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA**
3. In the details pane, double-click **LMCompatibilityLevel**.
4. In the **Value data** box, type the value that is appropriate for your scenario, and then click **OK**.

   Note For more information about the values that you can type, see the table that follows these steps.
5. Exit Registry Editor.

The following table describes the values that you can type in step 4.

Value	Description	Notes
0	Send LAN Manager (LM) responses and NTLM responses.	Client computers send LM responses and NTLM responses. Client computers never use NTLMv2 session security. Domain controllers accept LM authentication, NTLM authentication, and NTLMv2 authentication.
1	Send LM authentication and NTLM authentication and use NTLMv2 session security if negotiated.	Client computers use LM authentication and NTLM authentication. Client computers use NTLMv2 session security if the server supports NTLMv2 session security. Domain controllers accept LM authentication, NTLM authentication, and NTLMv2 authentication.
2	Send only NTLM responses.	Client computers use only NTLM authentication. Client computers use NTLMv2 session security if the server supports NTLMv2 session security. Domain controllers accept LM authentication, NTLM authentication, and NTLMv2 authentication.
3	Send only NTLMv2 responses.	Client computers use only NTLMv2 authentication. Client computers use NTLMv2 session security if the server supports NTLMv2 session security. Domain controllers accept LM authentication, NTLM authentication, and NTLMv2 authentication.
4	Send only NTLM responses and refuse LM authentication.	Client computers use only NTLM authentication. Client computers use NTLMv2 session security if the server supports NTLMv2 session security. Domain controllers refuse LM authentication. Domain controllers accept NTLM authentication and NTLMv2 authentication.
5	Send only NTLMv2 responses and refuse LM authentication and NTLM authentication.	Client computers use only NTLMv2 authentication. Client computers use NTLMv2 session security if the server supports NTLMv2 session security. Domain controllers refuse LM authentication and NTLM authentication. Domain controllers accept only NTLMv2 authentication.

RESOLUTION

To resolve this issue, contact the third-party vendor to obtain an updated version of the network-attached storage device that supports NTLMv2.

MORE INFORMATION

Windows supports the following levels of challenge/response authentication for network logons:

- LM
- NTLM version 1 (NTLMv1)
- NTLMv1 with NTLMv2 session security
- NTLMv2

The LM variant protocol allows for interoperability with earlier versions of Windows, such as Microsoft Windows 95 and Microsoft Windows 98. However, the passwords that are used in LM authentication are case-insensitive and are divided into seven-character chunks. These restrictions make it easier for someone to recover your password.

NTLMv1 authentication contains improvements that allow for passwords that are case-sensitive and that are not divided.

NTLMv2 authentication expands the key space to 128-bits. Additionally, NTLMv2 authentication uses different keys for client to server communication and for server to client communication. This behavior improves the signing and sealing of messages. NTLMv2 is the recommended level of challenge/response authentication.

APPLIES TO

- Windows Server 2008 Datacenter without Hyper-V
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 for Itanium-Based Systems
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Vista Enterprise
- Windows Vista Enterprise 64-bit Edition
- Windows Vista Business
- Windows Vista Business 64-bit Edition
- Windows Vista Ultimate
- Windows Vista Ultimate 64-bit Edition
- Windows Vista Home Premium
- Windows Vista Home Premium 64-bit Edition
- Windows Vista Home Basic
- Windows Vista Home Basic 64-bit Edition
- Microsoft Windows Server 2003, Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003, Datacenter Edition for Itanium-Based Systems
- Microsoft Windows Server 2003, Datacenter x64 Edition
- Microsoft Windows Server 2003, Enterprise x64 Edition
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition for Itanium-based Systems
- Microsoft Windows Server 2003, Standard x64 Edition
- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional

Keywords: kbregistry kbexpertiseinter kbtshoot kbprb KB954387

Get Help Now

Contact a support professional by E-mail, Online, or Phone

Microsoft Support

Microsoft

©2010 Microsoft