Filter by title

Windows Security
- Account lockouts
- Bitlocker
- Domain and forest trusts
- Internet Protocol security (IPSec)
- Kerberos authentication
- Legacy authentication (NTLM)
  - Audit event shows authentication package as NTLMv1
  - Audit use of NTLMv1 on a domain controller
  - Domain members fail authentication
  - Error when you connect to a Web site
  - How to disable automatic machine account password changes
  - **How to prevent Windows from storing an LM hash of the password**
  - Network access validation algorithms and examples
  - New setting modifies NTLM network authentication
  - NTLM user authentication
  - Performance tuning for NTLM authentication
  - Windows updates add new NTLM pass-through authentication protections for CVE-2022-21857
- Netlogon, secure channel, DC Locator
- Permissions, access control, and auditing
- Secure channel issues
- Security templates
- Windows LAPS
- Windows Servicing, Updates and Features on Demand
- Windows Server End of Support (EoS) FAQ
- Support Tools

Download PDF

How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases

Article • 12/26/2023 • 4 contributors

In this article

Summary
More information

This article provides three methods to prevent Windows from storing a LAN Manager (LM) hash of your password in Active Directory and local Security Accounts Manager (SAM) databases.

Original KB number: 299656

Summary

Windows doesn't store your user account password in clear-text. Instead, it generates and stores user account passwords by using two different password representations, known as hashes. When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generates both an LM hash and a Windows NT hash (NT hash) of the password. These hashes are stored in the local SAM database or Active Directory.

The LM hash is relatively weak compared to the NT hash, and it's prone to fast brute force attack. So you may want to prevent Windows from storing an LM hash of your password. This article describes how to make Windows only store the stronger NT hash of your password.

More information

Windows 2000 and Windows Server 2003 servers can authenticate users that connect from computers running earlier versions of Windows. However, versions of Windows earlier than Windows 2000 don't use Kerberos for authentication. For backward compatibility, Windows 2000 and Windows Server 2003 support:

- LM authentication
- Windows NT (NTLM) authentication
- NTLM version 2 (NTLMv2) authentication

NTLM, NTLMv2, and Kerberos all use the NT hash, also known as the Unicode hash. The LM authentication protocol uses the LM hash.

You should prevent the storage of the LM hash if you don't need it for backward compatibility. If your network contains Windows 95, Windows 98, or Macintosh clients, you may experience the following problems when you prevent the storage of LM hashes for your domain:

- Users without an LM hash can't connect to a Windows 95 or Windows 98 computer that's acting as a server. This issue doesn't occur if the Directory Services Client for Windows 95 and Windows 98 is installed on the server.
- Users on Windows 95 or Windows 98 computers can't authenticate to servers by using their domain account. This issue doesn't occur if the users have the Directory Services Client installed on their computers.
- Users on Windows 95 or Windows 98 computers can't authenticate by using a local account on a server that has disabled LM hashes. This issue doesn't occur if the users have the Directory Services Client installed on their computers.
- Users can't change their domain passwords from a Windows 95 or Windows 98 computer. Or, users may experience account lockout issues when they try to change passwords from these earlier clients.
- Users of Macintosh Outlook 2001 clients can't access their mailboxes on Microsoft Exchange servers. Users may see the following error in Outlook:

  > The logon credentials supplied were incorrect. Make sure your username and domain are correct, then type your password again.

To prevent Windows from storing an LM hash of your password, use any of the following methods.

Method 1: Implement the NoLMHash policy by using Group Policy

To disable the storage of LM hashes of a user's passwords in the local computer's SAM database in Windows XP or Windows Server 2003, use Local Group Policy. To disable the storage of LM hashes of a user's passwords in a Windows Server 2003 Active Directory environment, use Group Policy in Active Directory. Follow these steps:

1. In Group Policy, expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies**, and then select **Security Options**.
2. In the list of available policies, double-click **Network security: Do not store LAN Manager hash value on next password change**.
3. Select **Enabled** > **OK**.

Method 2: Implement the NoLMHash policy by editing the registry

In Windows 2000 Service Pack 2 (SP2) and later, use one of the following procedures to prevent Windows from storing an LM hash value on your next password change.

Windows 2000 SP2 and Later

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:

322756 How to back up and restore the registry in Windows

> The **NoLMHash** registry key and its functionality were not tested or documented and should be considered unsafe to use in production environments before Windows 2000 SP2.

To add this key by using Registry Editor, follow these steps:

1. Start Registry Editor (Regedt32.exe).
2. Locate and then select the following key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

3. On the **Edit** menu, click **Add Key**, type *`NoLMHash`*, and then press Enter.
4. Exit Registry Editor.
5. Restart the computer, and then change your password to make the setting active.

> **Note**
>
> - This registry key change must be made on all Windows 2000 domain controllers to disable the storage of LM hashes of users' passwords in a Windows 2000 Active Directory environment.
> - This registry key prevents new LM hashes from being created on Windows 2000 computers. But it doesn't clear the history of previous LM hashes that are stored. Existing LM hashes that are stored will be removed as you change passwords.

Windows XP and Windows Server 2003

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
>
> 322756 How to back up and restore the registry in Windows

To add this DWORD value by using Registry Editor, follow these steps:

1. Select **Start** > **Run**, type *regedit*, and then click **OK**.
2. Locate and then select the following key in the registry:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type *`NoLMHash`*, and then press ENTER.
5. On the **Edit** menu, select **Modify**.
6. Type *1*, and then select **OK**.
7. Restart your computer, and then change your password.

> **Note**

- This registry change must be made on all Windows Server 2003 domain controllers to disable the storage of LM hashes of users' passwords in a Windows 2003 Active Directory environment. If you're a domain administrator, you can use Active Directory Users and Computers Microsoft Management Console (MMC) to deploy this policy to all domain controllers or all computers on the domain as described in Method 1 (Implement the NoLMHash Policy by Using Group Policy).
- This DWORD value prevents new LM hashes from being created on Windows XP-based computers and Windows Server 2003-based computers. The history of all previous LM hashes is cleared when you complete these steps.

ⓘ Important

If you're creating a custom policy template that may be used on both Windows 2000 and Windows XP or Windows Server 2003, you can create both the key and the value. The value is in the same place as the key, and a value of 1 disables LM hash creation. The key is upgraded when a Windows 2000 system is upgraded to Windows Server 2003. However, it's okay if both settings are in the registry.

Method 3: Use a password that's at least 15 characters long

The simplest way is to use a password that's at least 15 characters long. In this case, Windows stores an LM hash value that can't be used to authenticate the user.

Feedback