Cached and Stored Credentials Technical Overview

learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)

- Article
- 08/31/2016

In this article

Applies To: Windows Vista, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8

This topic for the IT professional describes how credentials are formed in Windows and how the operating system manages them.

Introduction

When a user or service wants to access a computing resource, they must provide information that proves their identity. Their identity is typically in the form of their account's user name. This might be the user name that is the Security Accounts Manager (SAM) account name or the User Principal Name (UPN). But to prove their identity, they must provide secret information, which is called the *authenticator*. An authenticator can take various forms depending on the authentication protocol and method. The combination of an identity and an authenticator is called an *authentication credential*.

The process of creating, submitting, and verifying credentials is described simply as authentication, which is implemented through various authentication protocols, such as the Kerberos protocol. Authentication establishes the identity of the user, but not necessarily the user's permission to access or change a specific computing resource. That process is known as *authorization*.

Credentials are typically created or converted to a form that is required by the authentication protocols that are available on a computer. Credentials can be stored in the Local Security Authority Subsystem Service (LSASS) process memory for use by the account during a session. Credentials must also be stored on a hard disk drive in authoritative databases, such as the SAM database and in the database that is used by Active Directory Domain Services (AD DS).

For more information about storage, see Credentials storage in this topic.

Credential authenticators

The authenticator types used in the Windows operating system are as follows:

Plaintext credentials

When a user signs in to a computer running Windows and provides a user name and credentials (such as a password or PIN), the information is provided to the computer in plaintext. This plaintext password is used to authenticate the user’s identity by converting it into the form that is required by the authentication protocol. Some versions of Windows also retain an encrypted copy of this password that can be unencrypted to plaintext for use with authentication methods such as Digest authentication.

Note

Windows operating systems never store any plaintext credentials in memory or on the hard disk drive. Only reversibly encrypted credentials are stored there. When later access to the plaintext forms of the credentials is required, Windows stores the passwords in encrypted form that can only be decrypted by the operating system to provide access in authorized circumstances.

These protections, however, cannot prevent a malicious user with system-level access from illicitly extracting them in the same manner that the operating system would for legitimate use.

NT hash

The NT hash of the password is calculated by using an unsalted MD4 hash algorithm. MD4 is a cryptographic one-way function that produces a mathematical representation of a password. This hashing function is designed to always produce the same result from the same password input, and to minimize collisions where two different passwords can produce the same result. This hash is always the same length and cannot be directly decrypted to reveal the plaintext password. Because the NT hash only changes when the password changes, an NT hash is valid for authentication until a user’s password is changed.

Note

To protect against brute-force attacks on the NT hashes or online systems, users who authenticate with passwords should set strong passwords or passphrases that include characters from multiple sets and are as long as the user can easily remember. For password complexity guidelines, see the **Strong passwords** section in the Passwords Technical Overview.

LM hash

LAN Manager (LM) hashes are derived from the user password. Legacy support for LM hashes and the LAN Manager authentication protocol remains in the NTLM protocol suite. Default configurations in Windows and Microsoft security guidance have discouraged its use.

LM hashes inherently are more vulnerable to attacks because:

- LM hashes require a password to be less than 15 characters long and they contain only ASCII characters.
- LM hashes do not differentiate between uppercase and lowercase letters.

Windows logon cached password verifiers

These verifiers are not credentials because they cannot be presented to another computer for authentication, and they can only be used to locally verify a credential. They are stored in the registry on the local computer and provide credentials validation when a domain-joined computer cannot connect to AD DS during a user's logon. These "cached logons" or more specifically, cached domain account information, can be managed using the security policy setting Interactive logon: Number of previous logons to cache (in case domain controller is not available).

Credentials storage

The following sections describe where credentials are stored in Windows operating systems. Windows credentials are composed of a combination of an account name and the authenticator. These are stored and retrieved from the following locations depending on the status of the user's session, which might be active or inactive, and local or networked.

Security Accounts Manager database

The SAM database is stored as a file on the local hard disk drive, and it is the authoritative credential store for local accounts on each Windows computer. This database contains all the credentials that are local to that specific computer, including the built-in local Administrator account and any other local accounts for that computer.

The SAM database stores information on each account, including the user name and the NT password hash. By default, the SAM database does not store LM hashes on current versions of Windows. No password is ever stored in a SAM database—only the password hashes. The NT password hash is an unsalted MD4 hash of the account's password. This means that if two accounts use an identical password, they will also have an identical NT password hash.

LSASS process memory

The Local Security Authority Subsystem Service (LSASS) stores credentials in memory on behalf of users with active Windows sessions. This allows users to seamlessly access network resources, such as file shares, Exchange Server mailboxes, and SharePoint sites, without re-entering their credentials for each remote service.

LSASS can store credentials in multiple forms, including:

- Reversibly encrypted plaintext
- Kerberos tickets (TGTs, service tickets)
- NT hash
- LM hash

If the user logs on to Windows by using a smart card, LSASS will not store a plaintext password, but it will store the corresponding NT hash value for the account and the plaintext PIN for the smart card. If the account attribute is enabled for a smart card that is required for interactive logon, a random NT hash value is automatically generated for the account instead of the original password hash. The password hash that is automatically generated when the attribute is set does not change.

If a user logs on to Windows with a password that is compatible with LM hashes, this authenticator will be present in memory.

The storage of plaintext credentials in memory cannot be disabled, even if the credential providers that require them are disabled.

The stored credentials are directly associated with the LSASS logon sessions that have been started since the last restart and have not been closed. For example, LSA sessions with stored LSA credentials are created when a user does any of the following:

- Logs on to a local session or RDP session on the computer
- Runs a task by using the **RunAs** option
- Runs an active Windows service on the computer
- Runs a scheduled task or batch job
- Runs a task on the local computer by using a remote administration tool

LSA secrets on the hard disk drive

A Local Security Authority (LSA) secret is a secret piece of data that is accessible only to SYSTEM account processes. Some of these secrets are credentials that must persist after reboot, and they are stored in encrypted form on the hard disk drive. Credentials stored as LSA secrets might include:

- Account password for the computer’s AD DS account
- Account passwords for Windows services that are configured on the computer
- Account passwords for configured scheduled tasks
- Account passwords for IIS application pools and websites

AD DS database (NTDS.DIT)

The Active Directory Domain Services (AD DS) database is the authoritative store of credentials for all user and computer accounts in an AD DS domain. The two types of domain controllers in AD DS that manage credentials differently are:

Writable Each writable domain controller in the domain contains a full copy of the domain’s AD DS database, including account credentials for all accounts in the domain.

Read-only Read-only domain controllers (RODCs) house a partial local replica with credentials for a select subset of the accounts in the domain. By default, RODCs do not have a copy of privileged domain accounts.

The database stores a number of attributes for each account, which includes user names types and the following:

- NT hash for the current password
- NT hashes for password history (if configured)

NT hash values are also retained in AD DS for previous passwords to enforce password history during password change operations. The number of password history NT hash values retained is equal to the number of passwords configured in the password history enforcement policy.

LM hashes may also be stored in the AD DS database depending on the domain controller operating system version, configuration settings, and password change frequency.

Credential Manager store

Users may choose to save passwords in Windows by using an application or through the Credential Manager Control Panel applet. These credentials are stored on the hard disk drive and protected by using the Data Protection Application Programming Interface (DPAPI). Any program running as that user will be able to access credentials in this store.

Credential Manager can obtain its information in two ways:

Explicit creation When users enter a user name and password for a target computer or domain, that information is stored and used when the users attempt to log on to an appropriate computer. If no stored information is available and users supply a user name and password, they can save the information. If the user decides to save the information, Credential Manager receives and stores it.

System population When the operating system attempts to connect to a new computer on the network, it supplies the current user name and password to the computer. If this is not sufficient to provide access, Credential Manager attempts to supply the necessary user name and password. All stored user names and passwords are examined, from most specific to least specific as appropriate to the resource, and the connection is attempted in the order of those user names and passwords. Because user names and passwords are read and applied in order, from most to least specific, no more than one user name and password can be stored for each individual target or domain.

Credential Manager uses the Credential Locker, formerly known as Windows Vault, for secure storage of user names and passwords.

Related resources

- Passwords Technical Overview
- Windows Logon and Authentication Technical Overview
- Credential Locker Overview