Network access: Do not allow storage of passwords and credentials for network authentication

By Archiveddocs

Archived: 2026-04-05 16:09:48 UTC

Applies To: Windows Server 2003, Windows Vista, Windows XP, Windows Server 2008, Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8

This security policy reference topic for the IT professional describes the best practices, location, values, policy management and security considerations for this policy setting.

Reference

This security setting determines whether Credential Manager saves passwords and credentials for later use when it gains domain authentication.

Possible values

- Enabled

  Credential Manager does not store passwords and credentials on the computer.

- Disabled

  Credential Manager will store passwords and credentials on this computer for later use for domain authentication.

- Not defined

Best practices

It is a recommended practice to disable the ability of the Windows operating system to cache credentials on any computer where credentials are not needed. Evaluate your servers and workstations to determine the requirements. Cached credentials are designed primarily to be used on laptops that require domain credentials when disconnected from the domain.

Location

*GPO_name***\Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**

Default values

The following table lists the actual and effective default values for this policy. Default values are also listed on the policy's property page.

Server type or Group Policy Object (GPO)	Default value
Default domain policy	Disabled
Default domain controller policy	Disabled
Stand-alone server default settings	Disabled
Domain controller effective default settings	Not defined
Member server effective default settings	Not defined
Effective GPO default settings on client computers	Not defined

Operating system version differences

This policy is present in Windows Server 2003 and Windows XP, and it is named **Network access: Do not allow storage of credentials or .NET Passports for network authentication**. The policy name was modified for Windows Server 2008 and Windows Vista. However, this policy can be applied to all Windows server operating systems through Group Policy.

Policy management

This section describes features and tools that are available to help you manage this policy.

Restart requirement

A restart of the computer is required before this policy will be effective when changes to this policy are saved locally or distributed through Group Policy.

Group Policy

Although the name of this policy was changed in Windows Server 2008 and Windows Vista, it can be applied to Windows Server 2003 and Windows XP.

Security considerations

This section describes how an attacker might exploit a feature or its configuration, how to implement the countermeasure, and the possible negative consequences of countermeasure implementation.

Vulnerability

Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly runs malicious software that reads the passwords and forwards them to another, unauthorized user.

Note

The chances of success for this exploit and others that involve malicious software are reduced significantly for organizations that effectively implement and manage an enterprise antivirus solution combined with sensible software restriction policies. For more information, see Software Restriction Policies.

Regardless of what encryption algorithm is used to encrypt the password verifier, a password verifier can be overwritten so that an attacker can authenticate as the user to whom the verifier belongs. Therefore, the administrator's password may be overwritten. This procedure requires physical access to the computer. Utilities exist that can help overwrite the cached verifier. By using one of these utilities, an attacker can authenticate by using the overwritten value.

Overwriting the administrator's password does not help the attacker access data that is encrypted by using that password. Also, overwriting the password does not help the attacker access any Encrypting File System (EFS) data that belongs to other users on that computer. Overwriting the password does not help an attacker replace the verifier, because the base keying material is incorrect. Therefore, data that is encrypted by using Encrypting File System or by using the Data Protection API (DPAPI) will not decrypt.

Countermeasure

Enable the **Network access: Do not allow storage of passwords and credentials for network authentication** setting.

To limit the number of changed domain credentials that are stored on the computer, set the **cachedlogonscount** registry entry. By default, the operating system caches the verifier for each unique user's ten most recent valid logons. This value can be set to any value between 0 and 50. By default, all versions of the Windows operating system remember 10 cached logons, except Windows Server 2008 R2 and Windows Server 2008, which are set at 25.

When you try to log on to a domain from a Windows-based client computer, and a domain controller is unavailable, you do not receive an error message. Therefore, you may not notice that you logged on with cached domain credentials. You can set a notification of logon that uses cached domain credentials with the ReportDC registry entry.

Potential impact

Users are forced to type passwords whenever they log on to their Windows Live ID or other network resources that are not accessible to their domain account. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory–based domain account.

Additional resources

For information about how the Windows operating system stores and manages credentials, see Cached and Stored Credentials Technical Overview.
