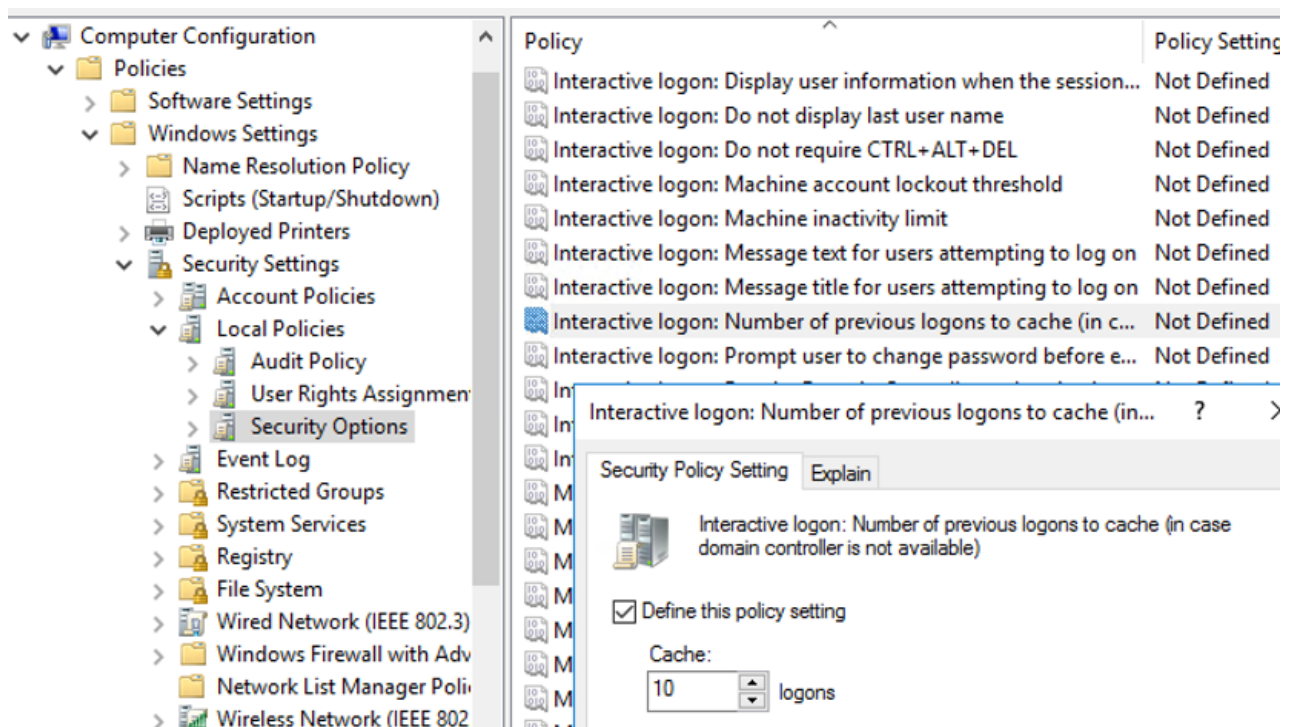


Cached Domain Logon Credentials on Windows

 woshub.com/cached-domain-logon-credentials-windows

June 1, 2021



Windows saves (caches) domain user credentials locally so users can log in without domain access if needed. This feature enables users to log on to their computers even when AD domain controllers are unavailable or powered off, or when the network cable is unplugged. This article examines the functionality and usage details of Cached Credentials in Windows domain environments.

Understanding Cached Domain Credentials in Windows

A user can sign in to an offline Windows computer with cached credentials if they have logged in successfully on that device at least once before. A hash of the username and password is saved to the registry when the user logs on to a domain computer. If the Active Directory domain is unavailable, Windows compares the entered username and password hash against the local cached credentials stored in the registry. The user is allowed to log on to the computer locally if the hash is found, even if there is no connection to a domain controller.

Using cached credentials allows mobile users to log in to their laptops and access their data even when disconnected from the corporate network.

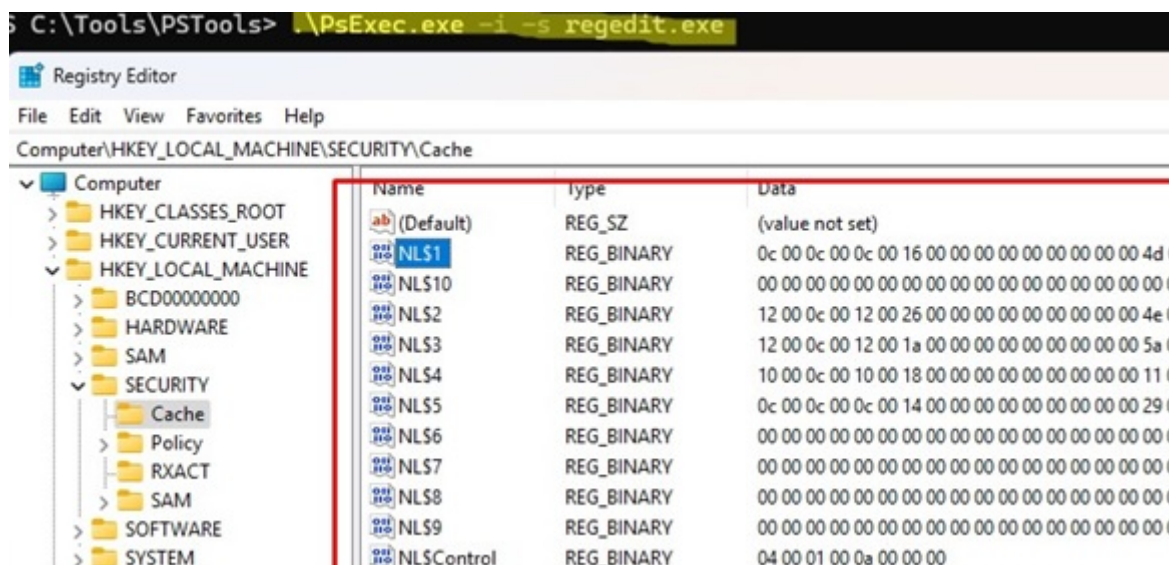
Cached credentials are stored in the registry under the reg key

HKEY_LOCAL_MACHINE\Security\Cache

(file %systemroot%\System32\config\SECURITY). Each saved hash is stored in the **NL\$x** parameter (where x is a cached data index).

By default, even the local administrator cannot access this registry key. However, it is possible to view its contents using Regedit.exe if you run it with NT AUTHORITY\SYSTEM privileges using the Psexec tool.

`Psexec.exe -i -s regedit.exe`



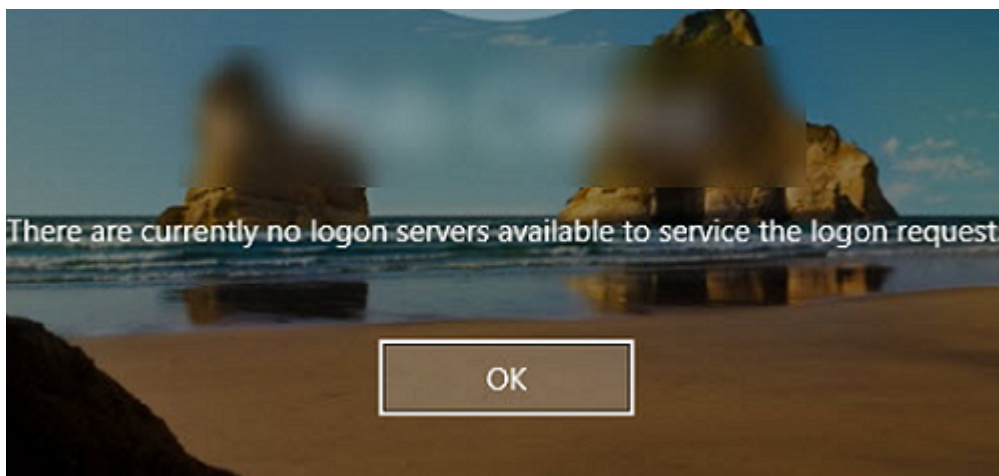
The credential hash does not contain the domain username and password in plain text. Instead, a salt is generated based on the username, which is used to decrypt the password hash (the MS-Cache v2 hash/mscash2 format is used). The result is saved to the registry. Passwords and their hashes in clear text cannot be extracted from the registry. Therefore, if an attacker obtains such a cryptographic hash, he will have to use brute force to crack the passwords.

The registry might contain multiple hashes of domain accounts that have previously logged into this computer. By default, the hashes of the last ten (10) users are saved.

Unlike domain passwords, the credentials stored in the registry never expire. They can only be overwritten by a new hash when a user logs in with a new password or when the credential cache limit is exceeded.

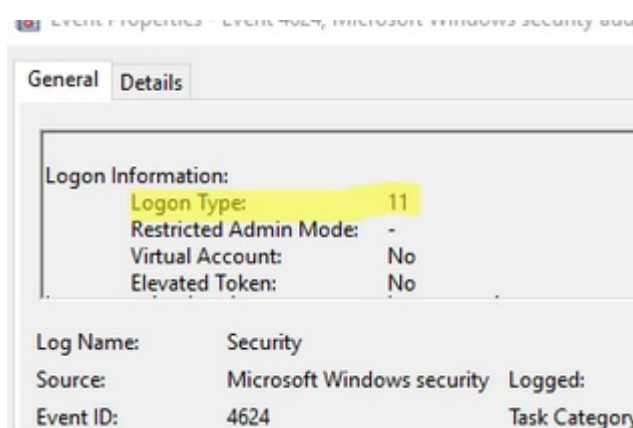
If there are no cached credentials in the local cache, the following message will appear when you try to log on to an offline computer:

There are currently no logon servers available to service the logon request.



When a user logs on to a computer using cached credentials, an event with **Event ID 4624** (An account was successfully logged on) and **Logon Type 11** (CachedInteractive) will appear in the Security log. These events can be used to [view local logon attempts on a Windows computer](#). The following logon types are also possible:

- **Logon Type 12:** CachedRemoteInteractive – remote connection using cached credentials
- **Logon Type 13:** CachedUnlocked – the [computer screen is unlocked after a period of inactivity](#) using a cached password.



Configure Credentials Caching with Group Policy

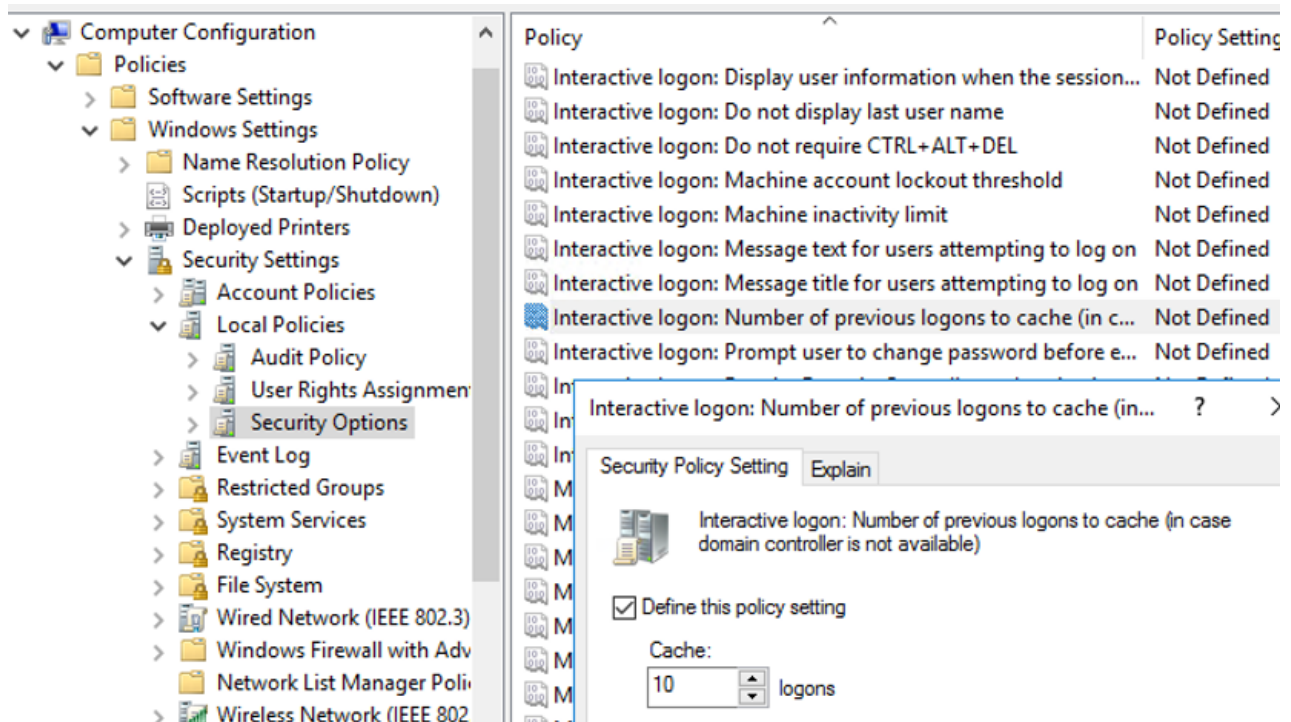
Using Group Policy, you can set the number of unique users whose credentials may be saved in the local cache on domain computers.

You can change the maximum number of cached credentials that can be saved using the GPO **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** option (Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options). You can set any value from 0 to 50.

The default value is 10, meaning the registry stores the credential data of the last ten users who logged in.

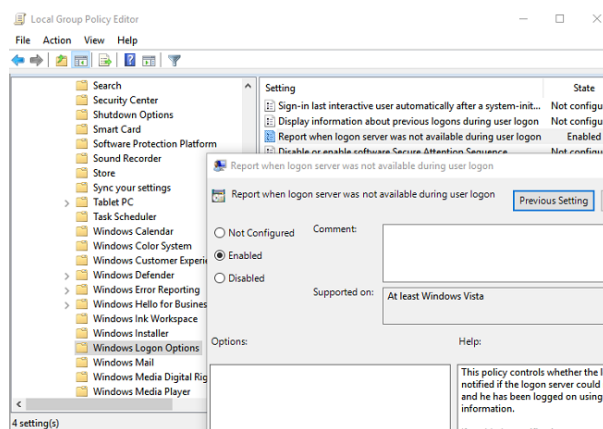
Setting this to **0** will prevent Windows from caching user credentials. In this case, if the domain is unavailable and a user tries to log on, they will see the error:

There are currently no logon servers available to service the logon request.



This option can also be configured using the REG_SZ registry value **CachedLogonsCount** in the **HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon** registry key.

When logging in with saved credentials, the user does not see that the domain controller is unavailable. With GPO, you can display a notification about logging with cached credentials. To do it, enable the GPO option **Report when logon server was not available during user logon** policy under the Computer Configuration -> Policies -> Administrative templates -> Windows Components -> Windows Logon Options.



After a user logs on, the following notification will appear in the tray:

A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on might not be available.

This option can be enabled via the Registry:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows NT/Current Version/Winlogon

- ValueName: ReportControllerMissing
- Data Type: REG_SZ
- Value: 1

Security Risks of Cached Credentials on Windows Workstations

Local caching of user authentication data poses several security risks. An attacker who gains physical access to a computer or laptop with cached credentials can use brute-force to decrypt the password hash. Complicated passwords are more difficult to crack using brute force.

It depends on the length and complexity of the password. If a password is complex, brute-forcing it can take an extremely long time. So, caching credentials for accounts with local administrator (or domain administrator) permissions is not secure.

Disabling credential caching on office and administrator computers is one way to mitigate security risks. For mobile devices, it is advisable to reduce the number of cached accounts to one. In other words, if an administrator logs into a computer and their credentials are cached, the administrator's password hash will overwrite the cached credentials when the device owner logs in.

The name of the last logon [username can be hidden from the Windows login screen](#). You can create separate GPOs in your domain to control the use of cached credentials for different devices and user categories (for example, using GPO Security filters, [WMI filters](#), or deploying the *CachedLogonsCount* [registry parameter using GPP item-level targeting](#)).

- For mobile (laptop) users: *CachedLogonsCount* = 1
- For office desktops: *CachedLogonsCount* = 0

Such policies will reduce the chance of obtaining privileged user hashes from [domain-joined computers](#).

You can enable BitLocker system drive encryption to protect cached credentials on mobile devices.

You can add administrator (privileged) accounts to the **Protected Users** built-in domain group (available for domains with a Windows Server 2012 R2 functional level or higher). Saving cached credentials is not allowed for this security group's members are not permitted.

Users who access their computers with cached logins and then establish a VPN tunnel to the corporate network may experience [periodic lockouts of their domain accounts](#). This can happen if the password stored locally does not match the user's password in the

domain (for example, this could happen if the user has changed their password according to the [domain's password policy settings](#)). To prevent this, configure [Windows to run the VPN tunnel before the user logs in](#).

Clearing Cached Credentials on Windows

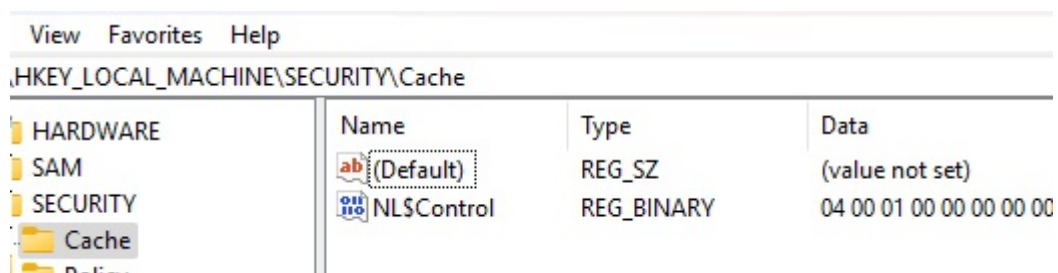
To clear cached credentials data, you must delete the **NL\$##** entries from the registry. But doing this manually is not convenient since it requires running the removal command on behalf of SYSTEM.

To clear all saved credentials, enable the Group Policy option Interactive logon: Number of previous logons to cache (in case domain controller is not available) and set the value to **0** (as described above).

Or run the following command in elevated CMD:

```
reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon" /v  
CachedLogonsCount /t REG_SZ /d 0 /f
```

After running the **gpupdate /force** command to [update the GPO settings](#), the cached credentials from the registry will be deleted.



Name	Type	Data
(Default)	REG_SZ	(value not set)
NL\$Control	REG_BINARY	04 00 01 00 00 00 00 00

Then you can either disable the policy or set it back to the default value of 10. After this, the credentials for all subsequent user logons to this computer will be automatically cached.