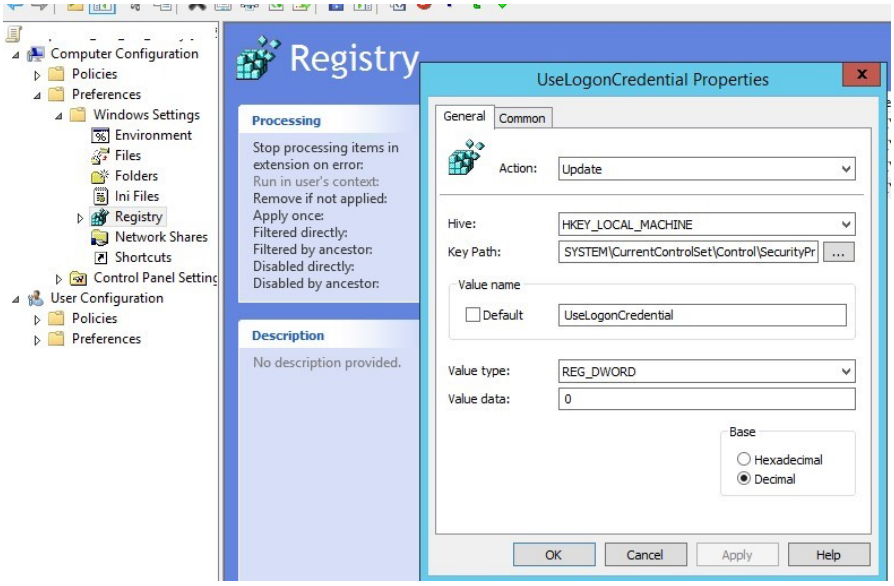
MimiKatz\Credential Stealing prevention Techniques

Disabling Wdigest

WDigest protocol appeared in Windows XP and was used to perform HTTP Digest Authentication that used user passwords in clear text. The feature to totally prohibit storing passwords in clear text in LSASS appeared in Windows 8.1 and Server 2012 R2. To prohibit storing WDigest in the memory, in these OSs there is the DWORD parameter with the name **UseLogonCredential** and the value 0 in the following branch of the registry: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest.**

If you want to completely disable WDigest authentication method, set the value of **Negotiate** parameter to **0** in the same registry branch **(HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\WDigest).**

To enable this feature in Windows 7, 8 and Windows Server 2008 R2 / 2012, install KB2871997 update and then set these keys in the registry. In the domain environment, it is easier to distribute the registry keys using GPO.



Tip. If you want to disable storing WDigest in the memory, first of all test if users and applications are correctly authenticated on your IIS servers.

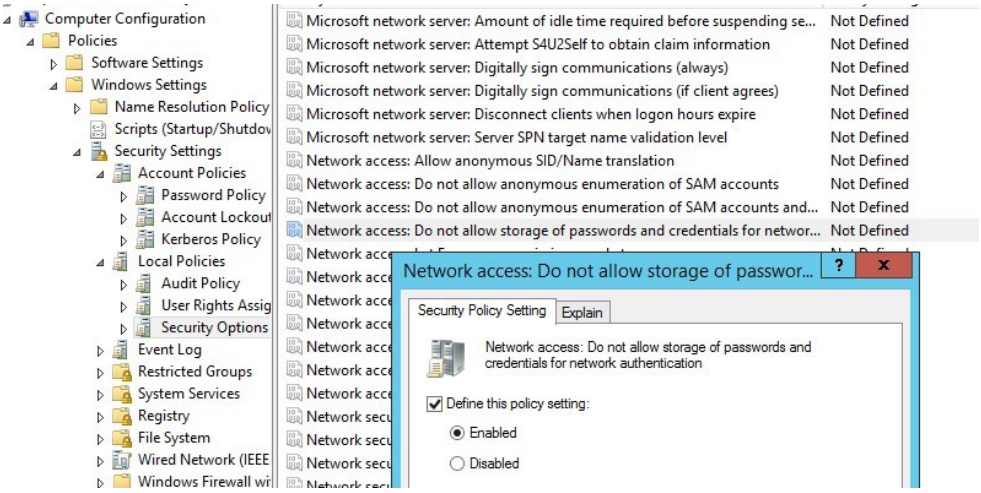
Protected Users Security Group

When using the functional level of Windows Server 2012 R2 domain, you can use a special security group Protected Users to protect privileged users. In particular, these accounts are protected against compromise due to the fact that the members of the group can authenticate only using Kerberos (no NTLM, WDigest or CredSSP, etc.). Follow the link above to get more information. It is better to add the accounts of domain and servers administrators, to this group. This feature is available on the servers and will be available in Windows Server 2012 R2 (for Windows Server 2008 R2 you will have to install the above mentioned **KB2871997** update).

How Prevent the use of saved passwords

You can prevent domain users from storing their passwords in Credential Manager to access the network resources.

To do it, enable **Network access: Do not allow storage of passwords and credentials for network authentication** policy in the Computer Configuration -> Windows Settings ->Security Settings ->Local Policies ->Security Options section.

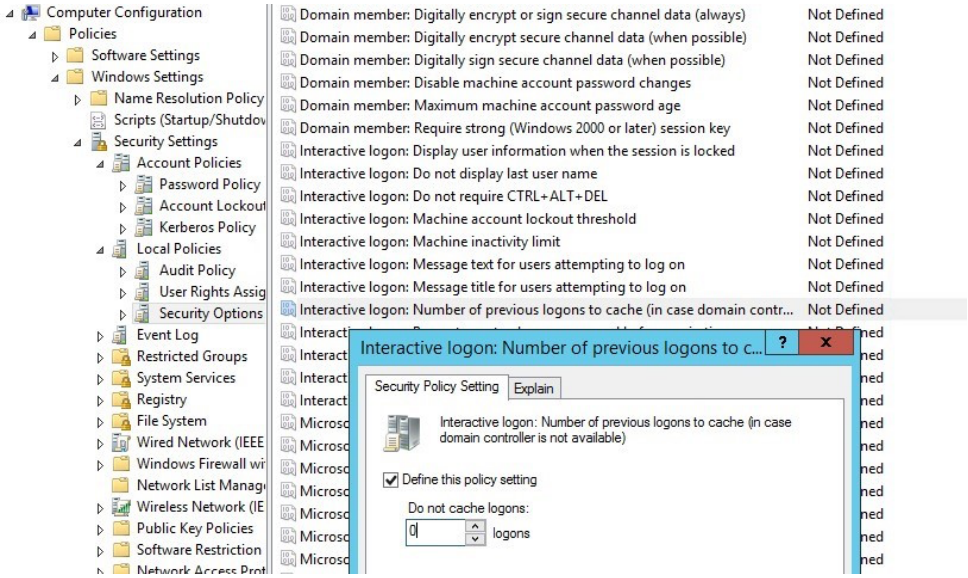


Note. Please, note that the storage of passwords will also be forbidden for the Task Scheduler jobs.

How to Disable Credential Caching

One of mimikatz features is getting hashes of user passwords from **HKEY_LOCAL_MACHINE\SECURITY\Cache** key of the registry, where the password hashes of last 10 (by default) logged on domain users are saved. Usually these hashes can be used to authenticate users in the system if the domain controller is not available.

It is recommended to prohibit storing the cached credentials by enabling **Interactive Logon: Number of previous logons to cache (in case domain controller is not available)** policy in **Computer Configuration -> Windows Settings -> Local Policy -> Security Options** by changing the value of its parameter to **0**.



Also, to accelerate LSASS memory clear from the credentials of logged off users, create a DWORD parameter with the name **TokenLeakDetectDelaySecs** and the value of **30** in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. It means that the memory will be cleared in 30 seconds after the user has logged off. In Windows 7, 8/ Server 2008R2, 2012, you will have to install the above-mentioned KB2871997 update to make this key work.