Unable to access network shares when using built-in windows VPN client (RAS) and ESA

Mitchell | ESET Nederland - 2018-07-27 - Reacties (0) - ESA Troubleshooting

Problem:

The default behaviour of the built-in windows VPN client is to store the credentials used for authenticating to the VPN server to the windows credentials manager.

Because these credentials are the domain credentials, these credentials are also used to authenticate to network shares and such, because the password contains the OTP generated by the ESA app or hardtoken these cannot be used for authenticating to network shares. Continuous attempts result in the account being locked out.

Solutions:

Solution 1:

edit the VPN settings to not use the VPN credentials when authenticating to network servers. This setting is not exposed through Windows' UI, so you need to locate the .pbk file associated with your VPN connection (which might be in `%userprofile%\AppData\Roaming\Microsoft\Network\Connections\PBK` or `C:\ProgramData\Microsoft\Network\Connections\Pbk`).

1. Right click on the VPN's .pbk file and open it with Notepad. (Remember to untick 'Always use this program for this file type')
2. Roughly 5 lines down will be an entry 'UseRasCredentials=1'
3. Change this to 'UseRasCredentials=0'
4. Save the file.

Solution 2:

There is a security policy setting that does specifically what we are looking for: Network access: Do not allow storage of passwords and credentials for network authentication. By enabling this setting, VPN credentials are not stored and therefore are not used to attempt to authenticate to network resources like shared files and Exchange. This setting can be enabled in domain GPO to be applied to all domain computers.