# Removing SSL Ciphers Suites using Group Policy

Microsoft recently applied a patch which alters the order of the cipher suites used when a DB user logs in to MS SQL.

<https://support.microsoft.com/en-us/kb/2929781>

This removes the DHE cipher suite, resulting in SecureSphere reporting “Hashed Users” even when we have the public / private keys.

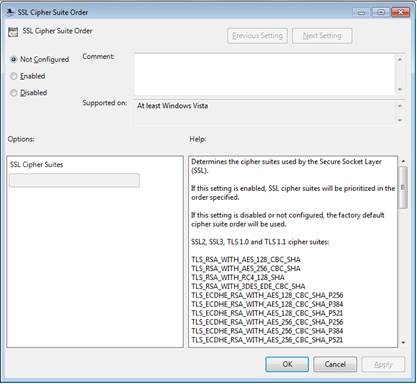
The solution to this involves the following steps (note the server requires a reboot to apply)….

**Solution / Workaround**

*The Solution is based on the removal of the DH ciphers from the windows server machine. it's done by reorder of the ciphers that can be used while removing unsupported ciphers from that list:*

1. Run gpedit.msc .

* In gpedit, Computer Configuration --> Administrative Templates --> Network --> SSL Configuration Settings
* On the right side menu click on the SSL Cipher Suite Order and edit.
* It will open an "SSL cipher suite order" window.



* + Under options SSL Cipher Suites, Select "Enabled". It will open an "SSL cipher suite order" window.  Add the cipher you want to use per the instruction in the help window on the right pane:
    - The following ciphers are supported by SecureSphere:

|  |
| --- |
| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA  TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA  TLS\_RSA\_WITH\_RC4\_128\_SHA  TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA  TLS\_RSA\_WITH\_RC4\_128\_MD5  TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256  TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 |

* + - Per the instructions the user can add this as an example:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA,TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA,TLS\_RSA\_WITH\_RC4\_128\_SHA,TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA,TLS\_RSA\_WITH\_RC4\_128\_MD5,TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256,TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256

* + Click on Apply and OK buttons.
  + **REBOOT** the server