

# SSL 证书- IIS

优化加密算法

(cipher)

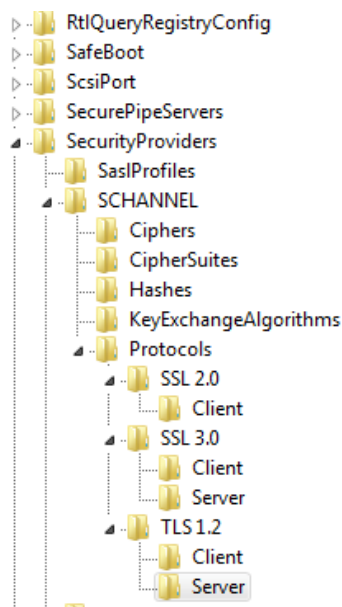


## 优化加密算法 (cipher)

**重要：**这个章节、方法或工作包含修改登录的步骤。然而，如果您不当修改登录，可能会发生严重的问题。因此，请务必小心执行这些步骤。为加强保护，修改登录之前，请务必将它备份起来。以后您就可以在发生问题时还原登录。如需有关如何备份和还原登录的详细资讯，检视「Microsoft 知识库」中的文件：

1. 按一下 **[开始]** ，再按一下 **[执行]** ，输入 regedt32 或 regedit ，然后按一下 **[确定]** 。
2. 在「登录编辑程式」中，找出下列登录机码：

HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders  
\SCHANNEL\Protocols



3. 在 **[编辑]** 功能表上，按一下 **[新增值]** 。
4. 在 **[资料类型]** 清单中，按一下 **[DWORD]** 。
5. 在 **[数值名称]** 方块中，输入 Enabled ，然后按一下 **[确定]** 。

**注意：**如果出现此值，请按两下这个值以编辑其目前的值。

6. 请在「二进位编辑器」中输入 **[00000000]** ，将新机码的值设定为等于「0」。

[HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders  
\SCHANNEL\Protocols\PCT 1.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 2.0\Server]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\SSL 3.0\Server]

"DisabledByDefault"=dword:00000000

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\TLS1.1\Client]

"Enabled"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\TLS1.1\Server]

"Enabled"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\TLS1.2\Client]

"Enabled"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\TLS1.2\Server]

"Enabled"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168]

"Enabled"=dword:00000000

参考 : <https://support.microsoft.com/en-us/kb/245030>