

# IIS: S?a l?i encrypted using a modern cipher suite trên Chrome

admin Sun, Apr 14, 2019 [Chứng Chỉ Số SSL Certificates](#) 0 2252

Trong m?t s? tr??ng h?p cài SSL trên máy ch? IIS 7 & 8, b?n có th? g?p l?i sau khi truy c?p trên Chrome

Your connection to [domain.com](#) is encrypted using a modern cipher suite./ K?t n?i c?a b?n t?i [tenmien.com](#) ???c mã hóa b?ng b? s? 0 hi?n ??i.

---

B?n vui lòng làm theo h??ng d?n sau ?? kh?c ph?c:

**Update – 2.2.2016** – *The ciphers originally listed in this post no longer work to fix the obsolete cryptography warning as Google has upped the requirement from DHE with AES\_128\_GCM to ECDHE with AES\_128\_GCM or CHACHA20\_POLY1305. The only ciphers we have on Windows that are close to this requirement are all ECDHE-ECDSA which will require an ECC (Elliptic Curve Cryptography) certificate to be used vs ECDHE-RSA which requires a certificate signed with the standard RSA key algorithm.*

To get an ECC certificate, the CSR for the certificate has to be generated with ECDSA as the key algorithm (rather than RSA 2048 or 4096). If you do have one of these certificates you can then use the steps in this post to bump the following cipher suites to the top to satisfy the obsolete cryptography warning:

TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P256

I have an updated post about acquiring an ECC certificate and steps needed to implement the ECDHE\_ECDSA ciphers here:

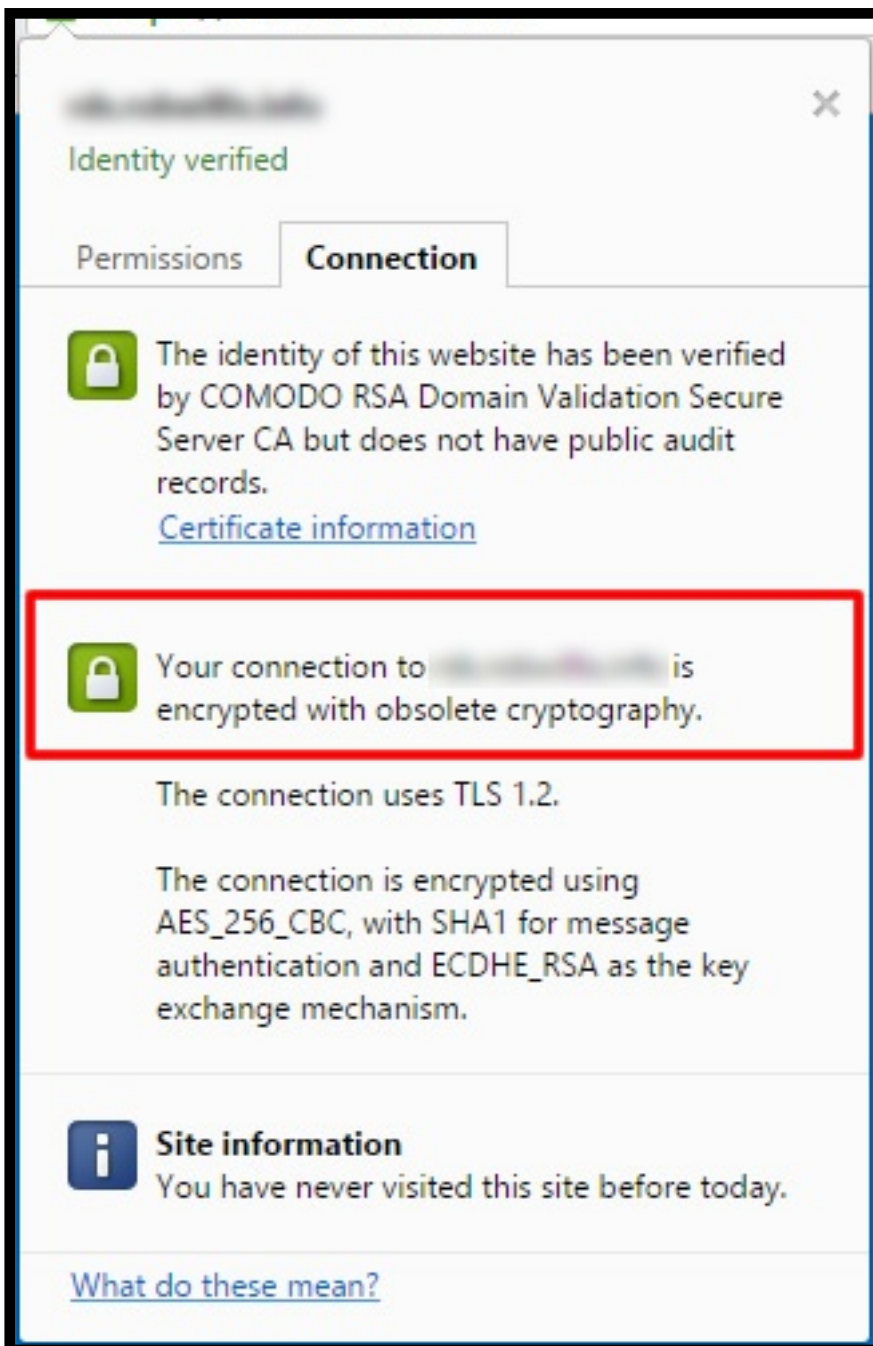
**[IIS 8 with ECC certificates – increasing your SSL Security on Windows Server 2012](#)**

*If you have a regular certificate signed with RSA like most are, I would go with*

the settings mentioned in this post:

## Hardening SSL & TLS connections on Windows Server 2008 R2 & 2012 R2

This post is going to be a quick and simple tip that should work on IIS 7 and IIS 8 to fix the “**Your connection to [somedomain.com](#) is encrypted with obsolete cryptography.**” warning that recently popped up in Google Chrome seen below:



Before we can fix it, we need to make sure that the following patch is installed from MS14-066:

[KB2992611](#)

Which adds support for the following cipher suites:

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

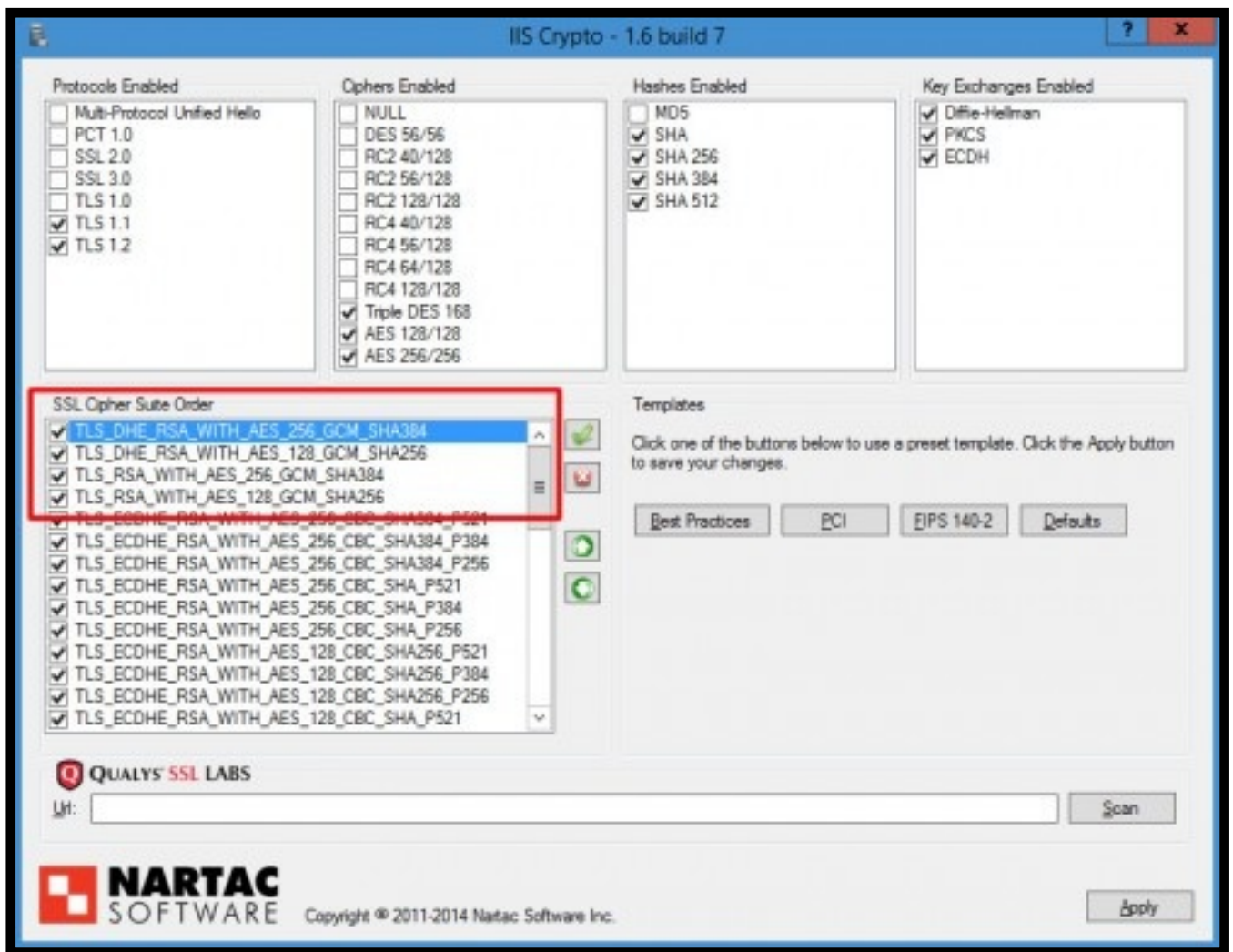
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

**Note as the KB mentions there were quite a few issues reported with this patch, so be sure to test before you put it in production and have a roll back plan in place.**

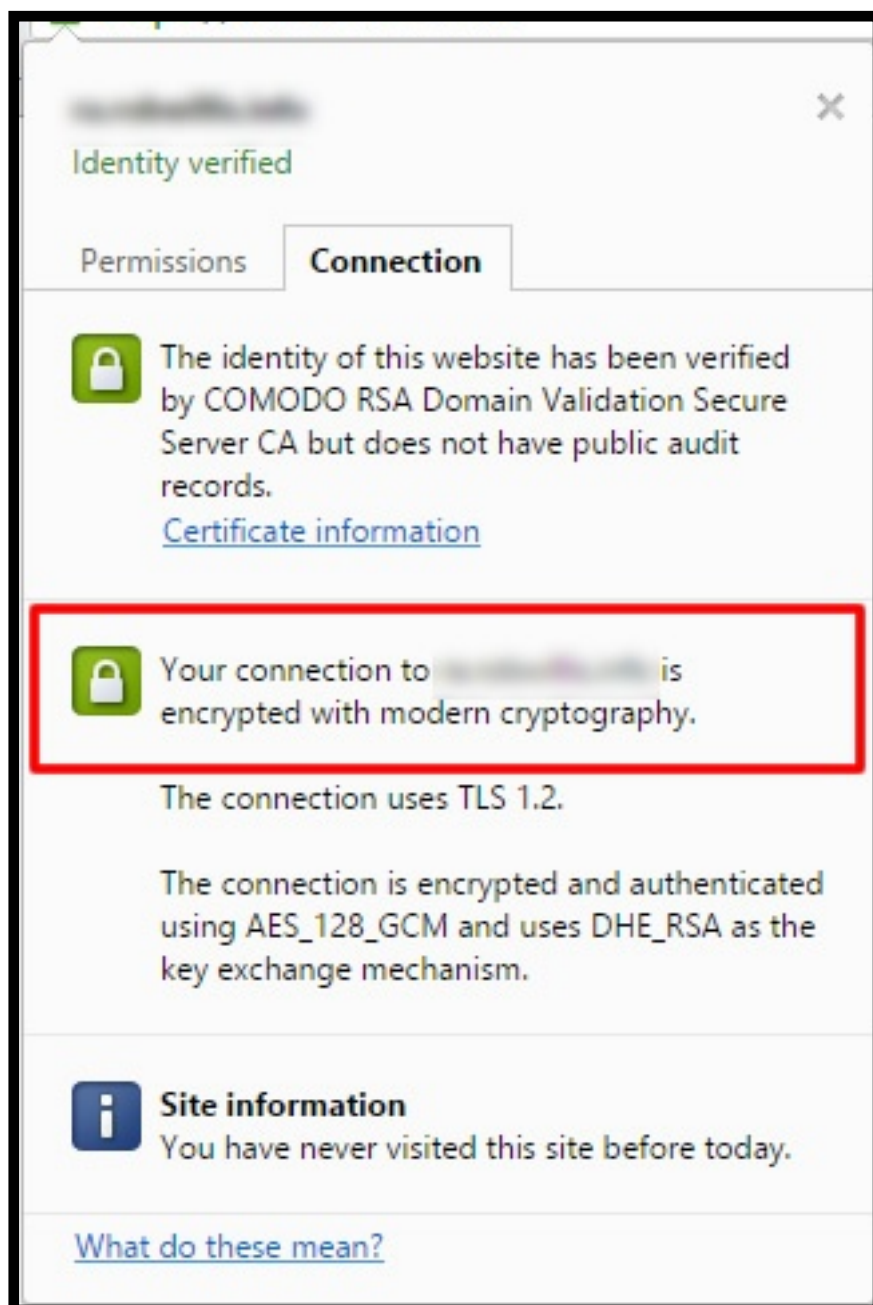
Once the patch is installed, we will need to download [IIS Crypto from Nartac Software](#) and then follow these steps:

1. Open IIS Crypto and apply the “**Best Practices**” template
2. On the bottom left in the Cipher Suite Order box find and move the following cipher suites to the top of the list and make sure they are now checked (screen shot below):  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
3. Uncheck TLS 1.0 under Protocols Enabled (optional but recommended on 2008R2/12/12R2)
4. Reboot the server and test in a new browser window, preferably an incognito/private one, otherwise you may need to clear your browser cache to see the changes.

IIS Crypto settings:



And Chrome now shows that we are using Modern Cryptography:



Hope this helps!

Ngu?n: <http://robwillis.info/2015/05/fix-obsolete-cryptography-warning-in-chrome-on-iis-8/>

Online URL: <https://huongdan.maxserver.com/article-61.html>