

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

admin Sun, Apr 14, 2019 [Chứng Chỉ Số SSL Certificates](#) 0 2303

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:

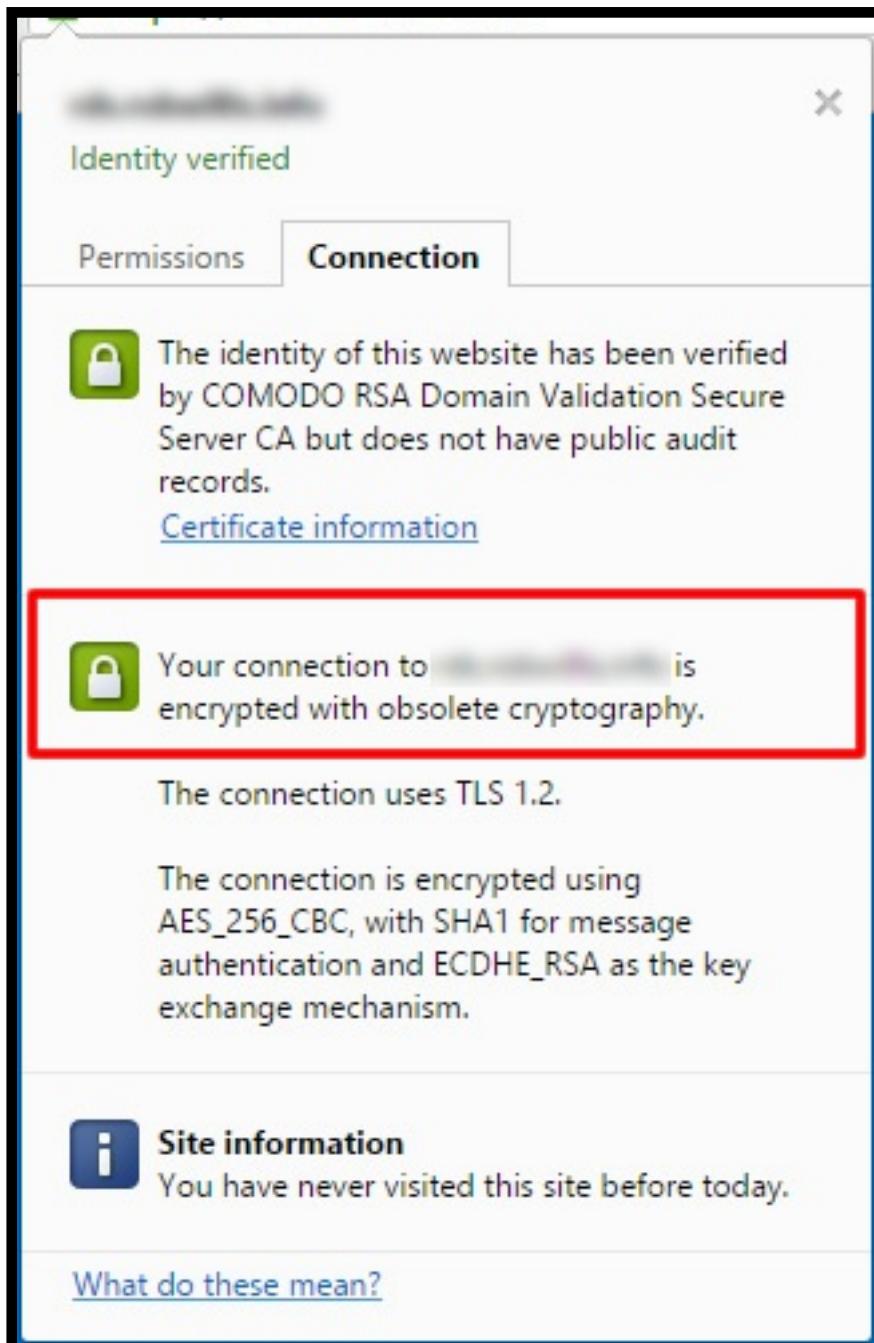
[IIS 8 with ECC certificates – increasing your SSL Security on Windows Server 2012](#)

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:

IIS Crypto - 1.6 build 7

Protocols Enabled	Options Enabled	Hashes Enabled	Key Exchanges Enabled
<input type="checkbox"/> Multi-Protocol Unified Hello	<input type="checkbox"/> NULL	<input type="checkbox"/> MD5	<input checked="" type="checkbox"/> Diffie-Hellman
<input type="checkbox"/> PCT 1.0	<input type="checkbox"/> DES 56/64	<input checked="" type="checkbox"/> SHA	<input checked="" type="checkbox"/> PKCS
<input type="checkbox"/> SSL 2.0	<input type="checkbox"/> RC2 40/128	<input checked="" type="checkbox"/> SHA 256	<input checked="" type="checkbox"/> ECDH
<input type="checkbox"/> SSL 3.0	<input type="checkbox"/> RC2 56/128	<input checked="" type="checkbox"/> SHA 384	
<input type="checkbox"/> TLS 1.0	<input type="checkbox"/> RC2 128/128	<input checked="" type="checkbox"/> SHA 512	
<input checked="" type="checkbox"/> TLS 1.1	<input type="checkbox"/> RC4 40/128		
<input checked="" type="checkbox"/> TLS 1.2	<input type="checkbox"/> RC4 56/128		
	<input type="checkbox"/> RC4 64/128		
	<input type="checkbox"/> RC4 128/128		
	<input checked="" type="checkbox"/> Triple DES 168		
	<input checked="" type="checkbox"/> AES 128/128		
	<input checked="" type="checkbox"/> AES 256/256		

SSL Cipher Suite Order

- 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
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521

Templates

Click one of the buttons below to use a preset template. Click the Apply button to save your changes.

Best Practices PCI FIPS 140-2 Defaults

QUALYS SSL LABS

URL: Scan

NARTAC SOFTWARE Copyright © 2011-2014 Nartac Software Inc.

And Chrome now shows that we are using Modern Cryptography:

Identity verified

Permissions Connection

 The identity of this website has been verified by COMODO RSA Domain Validation Secure Server CA but does not have public audit records.

[Certificate information](#)

 Your connection to [REDACTED] is encrypted with modern cryptography.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses DHE_RSA as the key exchange mechanism.

 Site information

You have never visited this site before today.

[What do these mean?](#)

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>