Published date: 30.03.2010  
Last Update: 23.02.2011  
Author: Adrian F. Dimcev, contact@carbonwind.net   
 With support for server side fingerprinting from SSL Labs <https://www.ssllabs.com/>

**ANNEX A1  
Common browsers/libraries/servers and the associated cipher suites implemented   
(work in progress)**

Provided “as is”, without any warranty.  
Work in progress, content incomplete and not reviewed yet.

Contents

[1. GnuTLS 3](#_Toc286234023)

[1.1. GnuTLS 2.8.6 Cipher Suites 4](#_Toc286234024)

[1.2. mod\_gnutls 0.5.5(GnuTLS 2.8.6 + Apache 2.2.15) Cipher Suites 12](#_Toc286234025)

[2. Mac OS X 19](#_Toc286234026)

[2.1. Safari 5.0.x on Mac OS X 10.5.8 Cipher Suites 20](#_Toc286234027)

[2.2. Safari 5.0.x on Mac OS X 10.6.6 Cipher Suites 21](#_Toc286234028)

[3. NSS(Network Security Services) 22](#_Toc286234029)

[3.1. NSS 3.12.5 Cipher Suites 22](#_Toc286234030)

[3.2. Firefox 3.6.x Cipher Suites 24](#_Toc286234031)

[3.3. Google Chrome 5 Beta on Linux Cipher Suites 27](#_Toc286234032)

[3.4. Google Chrome 9.0.x Cipher Suites 29](#_Toc286234033)

[3.5. mod\_nss 1.0.8 Cipher Suites 31](#_Toc286234034)

[3.6 Firefox 3.6.x on Fedora 14 35](#_Toc286234035)

[4. OpenSSL 39](#_Toc286234036)

[4.1. OpenSSL 0.9.8m Cipher Suites 42](#_Toc286234037)

[4.2. OpenSSL 1.0.0 Cipher Suites 47](#_Toc286234038)

[4.3. mod\_ssl (Apache 2.2.15 + OpenSSL 0.9.8m) Cipher Suites 54](#_Toc286234039)

[4.4. mod\_ssl (Apache 2.3.5 Alpha + OpenSSL 1.0.0) Cipher Suites 61](#_Toc286234040)

[5. Opera 69](#_Toc286234041)

[5.1 Opera 11.0x 70](#_Toc286234042)

[6. Schannel 72](#_Toc286234043)

[6.1. Schannel(NT 5.1.2600) Cipher Suites 73](#_Toc286234044)

[6.1.1. IE6 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites 74](#_Toc286234045)

[6.1.2. IE7 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites 75](#_Toc286234046)

[6.1.3. IE8 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites 76](#_Toc286234047)

[6.1.4. IIS 6.0 (Windows Server 2003 R2 SP2) 77](#_Toc286234048)

[6.1.5. Safari 5.0.x (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites 78](#_Toc286234049)

[6.2. Schannel(NT 6.0.6002) Cipher Suites 79](#_Toc286234050)

[6.2.1. IE7 (Windows Vista SP2) Cipher Suites 82](#_Toc286234051)

[6.2.2. IE8 (Windows Vista SP2) Cipher Suites 83](#_Toc286234052)

[6.2.3. IIS 7.0 (Windows Server 2008 SP2) Cipher Suites 84](#_Toc286234053)

[6.2.4. Safari 5.0.x (Windows Vista SP2) Cipher Suites 85](#_Toc286234054)

[6.3. Schannel (NT 6.1.7600) Cipher Suites 86](#_Toc286234055)

[6.3.1. IE8 (Windows 7) Cipher Suites 92](#_Toc286234056)

[6.3.2. IIS 7.5 (Windows Server 2008 R2) Cipher Suites 94](#_Toc286234057)

[6.3.3. Safari 5.0.x (Windows 7) Cipher Suites 96](#_Toc286234058)

[7. SSL Labs 97](#_Toc286234059)

[8. Wireshark 98](#_Toc286234060)

## 1. GnuTLS

According to its web site, GnuTLS is a project that aims to develop a library which provides a secure layer, over a reliable transport layer.

It supports SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.  
It does not support SSL 2.0.  
The 2.10 version supports TLS 1.2 and some cipher suites added in the TLS 1.2 RFC.

It does not support ECC.

mod\_gnutls uses the GnuTLS library to provide SSL 3.0, TLS 1.0 and TLS 1.1 (+ TLS 1.2 according to its web site, note tested) encryption for Apache HTTPD.

### 1.1. GnuTLS 2.8.6 Cipher Suites

GnuTLS 2.8.6 was analyzed, source build(Ubuntu Server 9.1 x64 was used).

It supports SSL 3.0, TLS 1.0 and TLS 1.1.  
It does not support SSL 2.0.

It does not support ECC.

Supports X.509(RSA, DSA) and OpenPGP certificates, SRP authentication(plain SRP, SRP-RSA and SRP-DSS) and PSK authentication(plain PSK and DHE-PSK).

SRP authentication cipher suites work over TLS 1.0 and TLS 1.1.

PSK authentication cipher suites work over TLS 1.0 and TLS 1.1.

To use OpenPGP certificates for a TLS session, the client adds to its Client Hello message the needed certificate type extension in order to inform the server it supports this - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0.

**!** TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5(0x0003) is usable over TLS 1.1(fixed in the branch version).

You can list for example the supported cipher suites, etc., for your GnuTLS build with:  
**gnutls-cli -l**

**Table 1.1.1** lists the cipher suites supported by GnuTLS 2.8.6, as well as the GnuTLS cipher suite name(the way is listed with the **gnutls-cli -l** the command). If the **GnuTLS Cipher Suite Name** column is yellow, then the cipher suite is listed under the **NORMAL** category.

You can use with the **gnutls-cli** or **gnutls-serv** commands the **--priority** directive.

**--priority** directive is a complex one used to specify the cipher suites and the SSL/TLS versions allowed(and more, like compression, etc.). There are some common keywords you can use to enable certain cipher suites, listed in **Table 1.1.2**. Note that the sorting imposed by some keywords is somehow relative on the server side, what cipher suite will be used also relates to the way the client lists the supported cipher suites.  
To the common keywords you can add or remove various values, listed in **Table 1.1.3**, which can add or disable some cipher suites or SSL/TLS protocol versions.

Example 1: Remove 3DES based cipher suites from the **NORMAL** category:  
**--priority: NORMAL:-3DES-CBC**

Example 2: Add Anonymous DH based cipher suites to the **NORMAL** category:  
**--priority: NORMAL:+ANON-DH**

Example 3: Remove SSL 3.0 from the **SECURE** category:  
**--priority: SECURE:-VERS-SSL3.0**

Example 4: Enable only a specific cipher suite TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, under TLS 1.0 and TLS 1.1 with no compression(assuming you use a RSA certificate):  
**--priority: NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL**

Example 5: Add compression(Deflate, zlib) to the **NORMAL** category:  
**--priority: NORMAL:+COMP-DEFLATE**

Example 6: Enable only the cipher suites listed in the below table(not necessarily in the order listed below) assuming you use a RSA certificate:  
**--priority: NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+AES-256-CBC:+DHE-RSA:+RSA:+SHA1:+COMP-NULL**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0|TLS 1.1 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | TLS 1.0|TLS 1.1 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0|TLS 1.1 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | TLS 1.0|TLS 1.1 |

There is another way to use certain cipher suites or SSL/TLS versions with the help of the **--ciphers** and **--protocols** directives instead of the **--priority** ones, but is no longer recommended to do so, thus we will not discuss this.

**Table 1.1.4** lists the cipher suites supported by GnuTLS along with the common keywords categories under the respective cipher suite can be found. For OpenPGP there aren’t specific cipher suites(for example TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA works with an OpenPGP certificate, as long as the client adds to its Client Hello message the needed certificate type extension - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0 -), to add this extension to the **gnutls-cli** Client Hello add the **CTYPE-OPENPGP** to the **--priority** directive on the client. Note that compression needs to be manually added to a category as is not enabled by default.

**Table 1.1.5** lists the cipher suites supported by GnuTLS as well as a specific combination of values to enable just the respective cipher suite(for all the supported SSL/TLS versions, plus the supported compression methods). The Deflate compression is red shaded as in order to use it zlib is needed, similar is true for the LZO compression, lzo is needed in order to use it. For OpenPGP there aren’t specific cipher suites(for example TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA works with an OpenPGP certificate, as long as the client adds to its Client Hello message the needed certificate type extension - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0 -), just make sure that the OpenPGP server certificate and private key are specified on the server(sometimes the **CTYPE-OPENPGP** might be needed to add on the server to the **--priority** directive).

**Table 1.1.1 GnuTLS 2.8.6 Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **GnuTLS Cipher Suite Name** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_NULL\_MD5 |
| 2 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_EXPORT\_ARCFOUR\_40\_MD5 |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_ARCFOUR\_MD5 |
| 4 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_ARCFOUR\_SHA1 |
| 5 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_3DES\_EDE\_CBC\_SHA1 |
| 6 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_3DES\_EDE\_CBC\_SHA1 |
| 7 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_RSA\_3DES\_EDE\_CBC\_SHA1 |
| 8 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_ARCFOUR\_MD5 |
| 9 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_3DES\_EDE\_CBC\_SHA1 |
| 10 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_AES\_128\_CBC\_SHA1 |
| 11 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_AES\_128\_CBC\_SHA1 |
| 12 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_RSA\_AES\_128\_CBC\_SHA1 |
| 13 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_AES\_128\_CBC\_SHA1 |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_AES\_256\_CBC\_SHA1 |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_AES\_256\_CBC\_SHA1 |
| 16 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_RSA\_AES\_256\_CBC\_SHA1 |
| 17 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_AES\_256\_CBC\_SHA1 |
| 18 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_CAMELLIA\_128\_CBC\_SHA1 |
| 19 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_CAMELLIA\_128\_CBC\_SHA1 |
| 20 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_RSA\_CAMELLIA\_128\_CBC\_SHA1 |
| 21 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_CAMELLIA\_128\_CBC\_SHA1 |
| 22 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_ARCFOUR\_SHA1 |
| 23 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_RSA\_CAMELLIA\_256\_CBC\_SHA1 |
| 24 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_DSS\_CAMELLIA\_256\_CBC\_SHA1 |
| 25 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_DHE\_RSA\_CAMELLIA\_256\_CBC\_SHA1 |
| 26 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0|TLS 1.1 | TLS\_ANON\_DH\_CAMELLIA\_256\_CBC\_SHA1 |
| 27 | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | TLS 1.0|TLS 1.1 | TLS\_PSK\_SHA\_ARCFOUR\_SHA1 |
| 28 | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | TLS 1.0|TLS 1.1 | TLS\_PSK\_SHA\_3DES\_EDE\_CBC\_SHA1 |
| 29 | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | TLS 1.0|TLS 1.1 | TLS\_PSK\_SHA\_AES\_128\_CBC\_SHA1 |
| 30 | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | TLS 1.0|TLS 1.1 | TLS\_PSK\_SHA\_AES\_256\_CBC\_SHA1 |
| 31 | TLS\_DHE\_PSK\_WITH\_RC4\_128\_SHA | 0x008E | TLS 1.0|TLS 1.1 | TLS\_DHE\_PSK\_SHA\_ARCFOUR\_SHA1 |
| 32 | TLS\_DHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008F | TLS 1.0|TLS 1.1 | TLS\_DHE\_PSK\_SHA\_3DES\_EDE\_CBC\_SHA1 |
| 33 | TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x0090 | TLS 1.0|TLS 1.1 | TLS\_DHE\_PSK\_SHA\_AES\_128\_CBC\_SHA1 |
| 34 | TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x0091 | TLS 1.0|TLS 1.1 | TLS\_DHE\_PSK\_SHA\_AES\_256\_CBC\_SHA1 |
| 35 | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_3DES\_EDE\_CBC\_SHA1 |
| 36 | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_RSA\_3DES\_EDE\_CBC\_SHA1 |
| 37 | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_DSS\_3DES\_EDE\_CBC\_SHA1 |
| 38 | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_AES\_128\_CBC\_SHA1 |
| 39 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_RSA\_AES\_128\_CBC\_SHA1 |
| 40 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_DSS\_AES\_128\_CBC\_SHA1 |
| 41 | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_AES\_256\_CBC\_SHA1 |
| 42 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_RSA\_AES\_256\_CBC\_SHA1 |
| 43 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | TLS 1.0|TLS 1.1 | TLS\_SRP\_SHA\_DSS\_AES\_256\_CBC\_SHA1 |

**Table 1.1.2 common GnuTLS 2.8.6 priority common keywords**

|  |  |  |
| --- | --- | --- |
| **No.** | **Keyword** | **Quick Info** |
| 1 | EXPORT | All the supported cipher suites including the export one, excepting the anonymous DH and NULL encryption ones |
| 2 | NORMAL | All the supported cipher suites excepting the export, NULL encryption and the anonymous DH ones |
| 3 | PERFORMANCE | All the supported cipher suites excepting the export, NULL encryption and the anonymous DH ones sorted in terms of performance |
| 4 | SECURE | All the supported cipher suites excepting the export, NULL encryption and the anonymous DH ones sorted in terms of strength |
| 5 | SECURE128 | All the supported cipher suites excepting the export, NULL encryption and the anonymous DH ones up to 128-bit key length |
| 6 | SECURE256 | All the supported cipher suites excepting the export, NULL encryption and the anonymous DH ones sorted in terms of strength |
| 7 | NONE | Nothing is enabled(this also disables protocols and compression methods) |

**Table 1.1.3 GnuTLS 2.8.6 priority values that can be added or removed to the common keywords**

| **No.** | **Keyword** | **Quick Info** |
| --- | --- | --- |
| 1 | 3DES-CBC | 3DES cipher |
| 2 | AES-128-CBC | AES 128-bit cipher |
| 3 | AES-256-CBC | AES 256-bit cipher |
| 4 | ARCFOUR-40 | RC4 export 40-bit cipher |
| 5 | ARCFOUR-128 | RC4 128-bit |
| 6 | CAMELLIA-128-CBC | Camellia 128-bit cipher |
| 7 | CAMELLIA-256-CBC | Camellia 256-bit cipher |
| 8 | ANON-DH | Anonymous DH |
| 9 | DHE-DSS | DSS authenticated DHE key exchange |
| 10 | DHE-RSA | RSA authenticated DHE key exchange |
| 11 | RSA | RSA authentication and key exchange |
| 12 | RSA-EXPORT | RSA-EXPORT authentication and key exchange |
| 13 | SRP | SRP authentication |
| 14 | SRP-DSS | SRP-DSS authentication |
| 15 | SRP-RSA | SRP-RSA authentication |
| 16 | MD5 | MD5 MAC |
| 17 | SHA1 | SHA1 MAC |
| 18 | COMP-DEFLATE | Deflate compression |
| 19 | COMP-NULL | NULL compression |
| 20 | COMP-LZO | LZO compression(experimental) |
| 21 | VERS-SSL3.0 | SSL 3.0 |
| 22 | VERS-TLS1.0 | TLS 1.0 |
| 23 | VERS-TLS1.1 | TLS 1.1 |
| 24 | %COMPAT | Disable MAC padding to assure compatibility with some broken clients |
| 25 | %SSL3\_RECORD\_VERSION | use SSL3.0 record version in Client Hello |
| 26 | CTYPE-OPENPGP | Certificate type OpenPGP(can be used to add the OpenPGP certificate type extension to a Client Hello) |
| 27 | CTYPE-X.509 | Certificate type X.509 |

**Table 1.1.4 GnuTLS 2.8.6 cipher suites(and the priority categories under the respective cipher suite can be found)**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **GnuTLS priority** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0|TLS 1.1 | ? |
| 2 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 4 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 5 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 6 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 7 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 8 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 9 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 10 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 11 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 12 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 13 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 16 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 17 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE256:+ANON-DH |
| 18 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 19 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 20 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 21 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 22 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 23 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 24 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 25 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 26 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE256:+ANON-DH |
| 27 | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 28 | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 29 | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 30 | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 31 | TLS\_DHE\_PSK\_WITH\_RC4\_128\_SHA | 0x008E | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 32 | TLS\_DHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008F | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 33 | TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x0090 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 34 | TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x0091 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 35 | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 36 | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 37 | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 38 | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 39 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 40 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 41 | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 42 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 43 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |

**Table 1.1.5 GnuTLS 2.8.6 cipher suites(and a combination of values to enable the respective cipher suite under priority)**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **GnuTLS priority** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0|TLS 1.1 | ? |
| 2 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-40:+RSA-EXPORT:+MD5:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+MD5:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 4 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 5 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 6 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 7 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 8 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+ANON-DH:+MD5:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 9 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 10 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 11 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 12 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 13 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 16 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 17 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 18 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 19 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 20 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 21 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 22 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 23 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 24 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 25 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 26 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 27 | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+ARCFOUR-128:+PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 28 | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 29 | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 30 | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 31 | TLS\_DHE\_PSK\_WITH\_RC4\_128\_SHA | 0x008E | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+ARCFOUR-128:+DHE-PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 32 | TLS\_DHE\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008F | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+DHE-PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 33 | TLS\_DHE\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x0090 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+DHE-PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 34 | TLS\_DHE\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x0091 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+DHE-PSK:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 35 | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 36 | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 37 | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 38 | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 39 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 40 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 41 | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 42 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |
| 43 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE:+COMP-LZO |

### 1.2. mod\_gnutls 0.5.5(GnuTLS 2.8.6 + Apache 2.2.15) Cipher Suites

According to its web site mod\_gnutls uses the GnuTLS library to provide SSL 3.0, TLS 1.0 and TLS 1.1 encryption for Apache HTTPD.

mod\_gnutls 0.5.5 was analyzed with GnuTLS 2.8.6 and Apache 2.2.15, all source builds(Ubuntu Server 9.1 x64 was used).

It does not support SSL 2.0, as SSL 2.0 is not supported by GnuTLS.

It can use a RSA or DSA certificate(X.509).  
Additionally OpenPGP certificates and SRP authentication(plain SRP, SRP-RSA, SRP-DSS) are supported.

SRP authentication cipher suites work over TLS 1.0 and TLS 1.1.

To use OpenPGP certificates for a TLS session, the client adds to its Client Hello message the needed certificate type extension in order to inform the server it supports this - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0 -.

GnuTLS can use in the same time a RSA and a DSA certificates. mod\_gnutls does not support this.

It can use in the same time a RSA/DSA and an OpenPGP certificate while also supporting SRP authentication.

For the DHE exchanges, by default a 2048-bit modulus is used. You can overwrite this with the **GnuTLSDHFile** directive which specifies the path to a PKCS #3 encoded DH parameters file.

**GnuTLSCertificateFile** directive specifies the path to the server certificate(RSA/DSA PEM encoded certificate).  
**GnuTLSKeyFile** directive specifies the path to the server private key(RSA/DSA private key).

**GnuTLSPGPCertificateFile** directive specifies the path to the OpenPGP server certificate(base 64 encoded).  
**GnuTLSPGPKeyFile** directive specifies the path to the OpenPGP server private key.

**GnuTLSSRPPasswdFile** directive specifies the path to a SRP password file which holds the username, a password verifier and the dependency to the SRP parameters.  
**GnuTLSSRPPasswdConfFile** directive specifies the path to a SRP password.conf file which holds the SRP parameters and is associated with the password file.

As said, a virtual host can use all these in the same time(if the **GnuTLSPriorities** directive permits too). Example:  
**GnuTLSPGPCertificateFile /usr/local/apache2/conf/openpgp-server.txt  
GnuTLSPGPKeyFile /usr/local/apache2/conf/openpgp-server-key.key  
GnuTLSCertificateFile /usr/local/apache2/conf/rsa\_server.pem  
GnuTLSKeyFile /usr/local/apache2/conf/rsa\_server.key  
GnuTLSSRPPasswdFile /usr/local/apache2/conf/srp-passwd.txt  
GnuTLSSRPPasswdConfFile /usr/local/apache2/conf/srp-tpasswd.conf**

**GnuTLSRSAFile** directive specifies the path to a PKCS #1 encoded RSA parameters which are used when the RSA-EXPORT key exchange method is enabled.

**GnuTLSPriorities** directive is a complex one used to specify the cipher suites and the SSL/TLS versions allowed(and more). There are some common keywords(similar with the ones from GnuTLS) you can use to enable certain cipher suites, listed in **Table 1.2.1**. Note that the sorting imposed on the server by some keywords is somehow relative, what cipher suite will be used also relates to the way the client lists the supported cipher suites.

To the common keywords you can add or remove various values(similar with the ones from GnuTLS), listed in **Table 1.2.2**, which will add or disable some cipher suites or SSL/TLS protocol versions.

Example 1: remove 3DES based cipher suites from the **NORMAL** category:  
**GnuTLSPriorities: NORMAL:!3DES-CBC**

Example 2: Add Anonymous DH based cipher suites to the **NORMAL** category:  
**GnuTLSPriorities: NORMAL:+ANON-DH**

Example 3: Remove SSL 3.0 from the **SECURE** category:  
**GnuTLSPriorities: SECURE:!VERS-SSL3.0**

Example 4: Enable only a specific cipher suite TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, under TLS 1.0 and TLS 1.1 with no compression(assuming you use a RSA certificate):  
**GnuTLSPriorities: NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL**

Example 5: Add compression(Deflate, zlib) to the **NORMAL** category:  
**GnuTLSPriorities:NORMAL:+COMP-DEFLATE**

Example 6: Enable only the cipher suites listed in the below table(not necessarily in the order listed below) assuming you use a RSA certificate:  
**GnuTLSPriorities: NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+AES-256-CBC:+DHE-RSA:+RSA:+SHA1:+COMP-NULL**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0|TLS 1.1 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | TLS 1.0|TLS 1.1 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0|TLS 1.1 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | TLS 1.0|TLS 1.1 |

**Table 1.2.3** lists the cipher suites supported by mod\_gnutls along with the common keywords categories under the respective cipher suite can be found. Note that since mod\_gnutls does not come with its own default configuration sample, a specific cipher suite is not necessarily disabled. As an exception, we can consider the TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 cipher suite(red shaded), for which we need a separate directive in order to use it(**GnuTLSRSAFile**). For OpenPGP there aren’t specific cipher suites(for example TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA works with an OpenPGP certificate, as long as the client adds to its Client Hello message the needed certificate type extension - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0 -).

**Table 1.2.4** lists the cipher suites supported by mod\_gnutls as well as a specific combination of values to enable just the respective cipher suite(for all the supported SSL/TLS versions, plus the supported compression methods). The Deflate compression is red shaded as in order to use it zlib is needed. For OpenPGP there aren’t specific cipher suites(for example TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA works with an OpenPGP certificate, as long as the client adds to its Client Hello message the needed certificate type extension - usually this extension is used with TLS 1.0 and TLS 1.1 but not with SSL 3.0 -), just make sure that the OpenPGP server certificate and private key are specified on the server(sometimes a **CTYPE-OPENPGP** might be needed to add on the server to the **GnuTLSPriorities** directive).

**Table 1.2.1 common mod\_gnutls 0.5.5 GnuTLSPriorities keywords**

|  |  |  |
| --- | --- | --- |
| **No.** | **Keyword** | **Quick Info** |
| 1 | EXPORT | All the supported cipher suites including the export one, excepting the anonymous DH ones |
| 2 | NORMAL | All the supported cipher suites excepting the export and the anonymous DH ones |
| 3 | PERFORMANCE | All the supported cipher suites excepting the export and the anonymous DH ones sorted in terms of performance |
| 4 | SECURE | All the supported cipher suites excepting the export and the anonymous DH ones sorted in terms of strength |
| 5 | SECURE128 | All the supported cipher suites excepting the export and the anonymous DH ones up to 128-bit key length |
| 6 | SECURE256 | All the supported cipher suites excepting the export and the anonymous DH ones sorted in terms of strength |
| 7 | NONE | Nothing is enabled(this also disables protocols and compression methods) |

**Table 1.2.2 mod\_gnutls 0.5.5 GnuTLSPriorities values that can be added or removed to the common keywords**

| **No.** | **Keyword** | **Quick Info** |
| --- | --- | --- |
| 1 | 3DES-CBC | 3DES cipher |
| 2 | AES-128-CBC | AES 128-bit cipher |
| 3 | AES-256-CBC | AES 256-bit cipher |
| 4 | ARCFOUR-40 | RC4 export 40-bit cipher |
| 5 | ARCFOUR-128 | RC4 128-bit |
| 6 | CAMELLIA-128-CBC | Camellia 128-bit cipher |
| 7 | CAMELLIA-256-CBC | Camellia 256-bit cipher |
| 8 | ANON-DH | Anonymous DH |
| 9 | DHE-DSS | DSS authenticated DHE key exchange |
| 10 | DHE-RSA | RSA authenticated DHE key exchange |
| 11 | RSA | RSA authentication and key exchange |
| 12 | RSA-EXPORT | RSA-EXPORT authentication and key exchange |
| 13 | SRP | SRP authentication |
| 14 | SRP-DSS | SRP-DSS authentication |
| 15 | SRP-RSA | SRP-RSA authentication |
| 16 | MD5 | MD5 MAC |
| 17 | SHA1 | SHA1 MAC |
| 18 | COMP-DEFLATE | Deflate compression |
| 19 | COMP-NULL | NULL compression |
| 20 | VERS-SSL3.0 | SSL 3.0 |
| 21 | VERS-TLS1.0 | TLS 1.0 |
| 22 | VERS-TLS1.1 | TLS 1.1 |
| 23 | %COMPAT | Disable MAC padding to assure compatibility with some broken clients |
| 25 | CTYPE-OPENPGP | Certificate type OpenPGP(sometimes you may need to add this to the GnuTLSPriorities directive) |
| 26 | CTYPE-X.509 | Certificate type X.509 |

**Table 1.2.3 mod\_gnutls 0.5.5 (GnuTLS 2.8.6 + Apache 2.2.15) cipher suites(and the categories under the respective cipher suite can be found)**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **mod\_gnutls GnuTLSPriorities** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 4 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 5 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 6 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 7 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 8 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 10 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 11 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 12 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 13 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 14 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 15 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 16 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE256:+ANON-DH |
| 17 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 18 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 19 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 20 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE128:+ANON-DH |
| 21 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 22 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 23 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 24 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 25 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0|TLS 1.1 | EXPORT:+ANON-DH|NORMAL:+ANON-DH|PERFORMANCE:+ANON-DH|SECURE:+ANON-DH|SECURE256:+ANON-DH |
| 26 | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 27 | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 28 | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 29 | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 30 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 31 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE128 |
| 32 | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 33 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |
| 34 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | TLS 1.0|TLS 1.1 | EXPORT|NORMAL|PERFORMANCE|SECURE|SECURE256 |

**Table 1.2.4 mod\_gnutls 0.5.5 (GnuTLS 2.8.6 + Apache 2.2.15) cipher suites(and a combination of values to enable the respective cipher suite)**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **mod\_gnutls GnuTLSPriorities** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-40:+RSA-EXPORT:+MD5:+COMP-NULL:+COMP-DEFLATE |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+MD5:+COMP-NULL:+COMP-DEFLATE |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 4 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 5 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 6 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 7 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+ANON-DH:+MD5:+COMP-NULL:+COMP-DEFLATE |
| 8 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+3DES-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 10 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 11 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 12 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 13 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 14 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 15 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 16 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+AES-256-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 17 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 18 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 19 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 20 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-128-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 21 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+ARCFOUR-128:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 22 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 23 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+DHE-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 24 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+DHE-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 25 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+VERS-SSL3.0:+CAMELLIA-256-CBC:+ANON-DH:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 26 | TLS\_SRP\_SHA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01A | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 27 | TLS\_SRP\_SHA\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01B | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 28 | TLS\_SRP\_SHA\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC01C | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+3DES-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 29 | TLS\_SRP\_SHA\_WITH\_AES\_128\_CBC\_SHA | 0xC01D | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 30 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC01E | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 31 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0xC01F | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-128-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 32 | TLS\_SRP\_SHA\_WITH\_AES\_256\_CBC\_SHA | 0xC020 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 33 | TLS\_SRP\_SHA\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC021 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP-RSA:+SHA1:+COMP-NULL:+COMP-DEFLATE |
| 34 | TLS\_SRP\_SHA\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0xC022 | TLS 1.0|TLS 1.1 | NONE:+VERS-TLS1.1:+VERS-TLS1.0:+AES-256-CBC:+SRP-DSS:+SHA1:+COMP-NULL:+COMP-DEFLATE |

## 2. Mac OS X

Test

### 2.1. Safari 5.0.x on Mac OS X 10.5.8 Cipher Suites

Safari 5.0.3 tested, cipher suites listed within **Table 2.1**.

SSL 2.0 appears to not be supported.

SSL 3.0 and TLS 1.0 are supported and enabled by default.

**Table 2.1**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 |
| 6 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 8 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 |
| 12 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 |
| 13 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 |
| 14 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 |
| 16 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 17 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 18 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 |
| 19 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |

### **2.2. Safari 5.0.x on Mac OS X 10.6.6** Cipher Suites

Safari 5.0.3 tested, cipher suites listed within **Table 2.2**.

SSL 2.0 appears to not be supported.

SSL 3.0 and TLS 1.0 are supported and enabled by default.

Compared with Mac OS X 10.5.8, Mac OS X 10.6.6 supports some ECC based cipher suites.

**Table 2.2**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 |
| 6 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 8 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 |
| 12 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 |
| 13 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 |
| 14 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 |
| 16 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 17 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 18 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 |
| 19 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |
| 20 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 |
| 21 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 |
| 22 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 |
| 23 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 |
| 24 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 |
| 25 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 |
| 26 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 |
| 28 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 |
| 29 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 |
| 30 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 |
| 31 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 |
| 32 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 |
| 33 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 |
| 34 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 |
| 35 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 |

3. NSS(Network Security Services)  
NSS 3.12.4 and NSS 3.12.5 were currently analyzed.

NSS is used by browsers(Firefox, Google Chrome), web servers(Apache with mod\_nss), etc.

Usually NSS is built with support for ECC(Elliptic Curve Cryptography). However some Linux distros, like Fedora(version 12 as writing), come with support for ECC disabled by default. As a result applications that use NSS, for example the Firefox version that ships with Fedora, will not be able to use ECC cipher suites.

NSS supports the three “popular” elliptic curves(which should assure interoperability):  
 - secp256r1(aka NIST P-256)  
 - secp384r1(aka NIST P-384)  
 - secp521r1(aka NIST P-521)

NSS currently supports: SSL 2.0, SSL 3.0, TLS 1.0.

The current cipher suites implemented by NSS are listed within the **security/source/security/nss/lib/ssl/sslenum.c** file(if you have downloaded the source code). Or online at:  
<http://mxr.mozilla.org/security/source/security/nss/lib/ssl/sslenum.c>

DHE cipher suites are not supported on the server side.

As of NSS 3.11, Fortezza based cipher suites have been deprecated.

DH 2236-bit modulus is the NSS upper limitation.  
RSA 8192-bit modulus is the NSS upper limitation.

### 3.1. NSS 3.12.5 Cipher Suites

**Table 3.1** lists the cipher suites currently supported by NSS 3.12.5. For more details about each cipher suite refer to the main tables.  
Since the FORTEZZA based cipher suites were deprecated, they are not listed below.

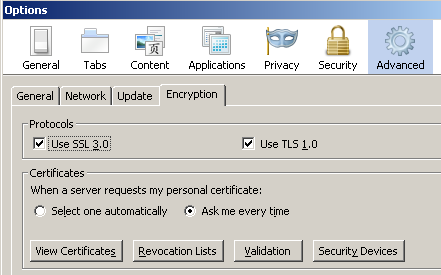
**Table 3.1 NSS 3.12.5 Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 |
| 7 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 |
| 8 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 12 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 |
| 13 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 |
| 14 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 15 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 |
| 16 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 |
| 17 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 |
| 18 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 |
| 19 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 20 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 |
| 21 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 22 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 23 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 |
| 24 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |
| 25 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 |
| 26 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 |
| 27 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 |
| 28 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 |
| 29 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 |
| 30 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 |
| 31 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 |
| 32 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 |
| 33 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 |
| 34 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 |
| 35 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 |
| 36 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 |
| 37 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 |
| 38 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 |
| 39 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 |
| 40 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 |
| 41 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 |
| 42 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 |
| 43 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 |
| 44 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 |
| 45 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 |
| 46 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 |
| 47 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 |
| 48 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 |
| 49 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 |
| 50 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 |
| 51 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 |
| 52 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 |
| 53 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 |
| 54 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 |
| 55 | SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA | 0xFEFE | SSL 3.0|TLS 1.0 |
| 56 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 |

### 3.2. Firefox 3.6.x Cipher Suites

Firefox 2.x, 3.x, 3.5.x and 3.6(latest 3.6.13) were analyzed. As mentioned above, due to some ECC restrictions on some Linux distros, the Firefox version shipped on those Linux distros might not support ECC cipher suites.

You can adjust the SSL/TLS settings from **Options**(on Windows) or **Preferences**(on Linux or Mac), **Advanced** tab, **Encryption** tab, from where you can enable or disable the SSL/TLS version used.



For more granular settings, type **about:config** in the address bar and hit enter. You will access like so the advanced settings

**Table 3.2.1** lists the configuration settings names(advanced settings) that can be used to enable/disable a specific SSL/TLS version currently supported by Firefox 3.6.13. The color red means that the protocol version is disabled by default, and the color green means that the protocol version is enabled by default.

**Table 3.2.1 Firefox 3.6 Protocol Settings**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Firefox Setting Name** | **Enables/Disables** | **Default Value** |
| 1 | security.enable\_ssl2 | SSL 2.0 | false |
| 2 | security.enable\_ssl3 | SSL 3.0 | true |
| 3 | security.enable\_tls | TLS 1.0 | true |

**Table 3.2.2** lists the cipher suites currently supported by Firefox 3.6.13. For more details about each cipher suite or other versions of Firefox, refer to the main tables. The color red means that the cipher suite is disabled by default, and the color green means that the cipher suite is enabled by default. SSL 3.0 is gray shaded for ECC cipher suites as if you just enable SSL 3.0 in Firefox, Firefox does not add these cipher suites to its SSL 3.0 Client Hello. However, for example, in the default Firefox configuration(TLS 1.0 and SSL 3.0 enabled), if the server replies with SSL 3.0 and an ECC cipher suite, Firefox will accept this.

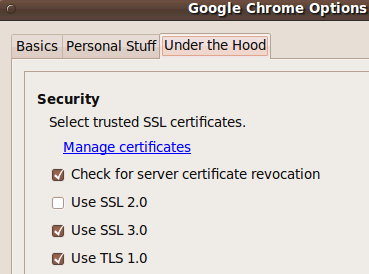
**Table 3.2.2 Firefox 3.6.13 Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Firefox Setting Name** | **Default Value** |
| --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | security.ssl2.rc4\_128 | false |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | security.ssl2.rc4\_40 | false |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | security.ssl2.rc2\_128 | false |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | security.ssl2.rc2\_40 | false |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | security.ssl2.des\_64 | false |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | security.ssl2.des\_ede3\_192 | false |
| 7 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_null\_md5 | false |
| 8 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_null\_sha | false |
| 9 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_40\_md5 | false |
| 10 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_128\_md5 | true |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_128\_sha | true |
| 12 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc2\_40\_md5 | false |
| 13 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_des\_sha | false |
| 14 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_des\_ede3\_sha | true |
| 15 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_des\_sha | false |
| 16 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_des\_ede3\_sha | true |
| 17 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_des\_sha | false |
| 18 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_des\_ede3\_sha | true |
| 19 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_aes\_128\_sha | true |
| 20 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_aes\_128\_sha | true |
| 21 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_aes\_128\_sha | true |
| 22 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_aes\_256\_sha | true |
| 23 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_aes\_256\_sha | true |
| 24 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_aes\_256\_sha | true |
| 25 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_camellia\_128\_sha | true |
| 26 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_camellia\_128\_sha | true |
| 27 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_camellia\_128\_sha | true |
| 28 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_1024\_des\_cbc\_sha | false |
| 29 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_1024\_rc4\_56\_sha | false |
| 30 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_camellia\_256\_sha | true |
| 31 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_camellia\_256\_sha | true |
| 32 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_camellia\_256\_sha | true |
| 33 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_seed\_sha | true |
| 34 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_ecdsa\_null\_sha | false |
| 35 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_ecdsa\_rc4\_128\_sha | true |
| 36 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_ecdsa\_des\_ede3\_sha | true |
| 37 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_ecdsa\_aes\_128\_sha | true |
| 38 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_ecdsa\_aes\_256\_sha | true |
| 39 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_ecdsa\_null\_sha | false |
| 40 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_ecdsa\_rc4\_128\_sha | true |
| 41 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_ecdsa\_des\_ede3\_sha | true |
| 42 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_ecdsa\_aes\_128\_sha | true |
| 43 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_ecdsa\_aes\_256\_sha | true |
| 44 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_rsa\_null\_sha | false |
| 45 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_rsa\_rc4\_128\_sha | true |
| 46 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_rsa\_des\_ede3\_sha | true |
| 47 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_rsa\_aes\_128\_sha | true |
| 48 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | security.ssl3.ecdh\_rsa\_aes\_256\_sha | true |
| 49 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_rsa\_null\_sha | false |
| 50 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_rsa\_rc4\_128\_sha | true |
| 51 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_rsa\_des\_ede3\_sha | true |
| 52 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_rsa\_aes\_128\_sha | true |
| 53 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | security.ssl3.ecdhe\_rsa\_aes\_256\_sha | true |
| 54 | SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA | 0xFEFE | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_fips\_des\_sha | false |
| 55 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_fips\_des\_ede3\_sha | true |

### 3.3. Google Chrome 5 Beta on Linux Cipher Suites

Google Chrome 5 Beta on Ubuntu 9.1 and Debian 5.0.3 x64 were analyzed.

The SSL/TLS settings can be adjusted from **Options**, **Under the Hood** tab, **Security** area, for example to enable or disable a specific SSL/TLS version.



**Table 3.3** lists the cipher suites currently supported by Google Chrome 5 Beta on Linux. For more details about each cipher suite, refer to the main tables. The color red means that the cipher suite is disabled by default, and the color green means that the cipher suite is enabled by default. SSL 3.0 is gray shaded for ECC cipher suites as if you just enable SSL 3.0 in Chrome, Chrome does not add these cipher suites to its SSL 3.0 Client Hello. However, for example, in the default Chrome configuration(TLS 1.0 and SSL 3.0 enabled), if the server replies with SSL 3.0 and an ECC cipher suite, Chrome will accept this.

**Table 3.3 Google Chrome 5 Beta on Linux Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 4 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 5 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | enabled |
| 15 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | enabled |
| 16 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | enabled |
| 17 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | enabled |
| 18 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | enabled |
| 21 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | enabled |
| 22 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | enabled |
| 23 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | enabled |
| 24 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | enabled |
| 25 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | enabled |
| 26 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | enabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | enabled |
| 28 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | enabled |
| 29 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | enabled |
| 30 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | enabled |
| 31 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | enabled |
| 32 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | enabled |
| 33 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | enabled |
| 34 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | enabled |
| 35 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | enabled |
| 36 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | enabled |
| 37 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | enabled |
| 38 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | enabled |
| 39 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 | enabled |

3.4. Google Chrome 9.0.x Cipher Suites  
Google Chrome 9.0.597.94 was tested; running on Windows XP/Vista/7, Ubuntu 10.04(not the version from Ubuntu repository), and Mac OS X 10.5.8/10.6.6.

**Table 3.4** lists the cipher suites currently supported by Google Chrome 9. For more details about each cipher suite, refer to the main tables. The color red means that the cipher suite is disabled by default, and the color green means that the cipher suite is enabled by default. SSL 3.0 is gray shaded for ECC cipher suites as if you just enable SSL 3.0 in Chrome, Chrome does not add these cipher suites to its SSL 3.0 Client Hello. However, for example, in the default Chrome configuration(TLS 1.0 and SSL 3.0 enabled), if the server replies with SSL 3.0 and an ECC cipher suite, Chrome will accept this.

**Table 3.4 Google Chrome 9.0.x Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 4 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 5 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | enabled |
| 15 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | enabled |
| 16 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | enabled |
| 17 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | enabled |
| 18 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | enabled |
| 21 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | enabled |
| 22 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | enabled |
| 23 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | enabled |
| 24 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | enabled |
| 25 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | enabled |
| 26 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | enabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | enabled |
| 28 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | enabled |
| 29 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | enabled |
| 30 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | enabled |
| 31 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | enabled |
| 32 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | enabled |
| 33 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | enabled |
| 34 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | enabled |
| 35 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | enabled |
| 36 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | enabled |
| 37 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | enabled |
| 38 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | enabled |
| 39 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 | enabled |

### 3.5. mod\_nss 1.0.8 Cipher Suites

mod\_nss (according to its web site) is an SSL provider derived from the mod\_ssl module for the Apache web server that uses the NSS libraries.

mod\_nss 1.0.8 was fingerprinted running on Fedora 12, Apache 2.2.14(the version shipped on Fedora) with NSS 3.12.5 + NSPR 4.8.2. Because Fedora comes without support for ECC, NSS with support for ECC was manually built and the resulted libraries were used.

mod\_nss 1.0.8 comes with support for SSL 2.0 disabled by default.

mod\_nss 1.0.8 comes with support for ECC disabled by default.

If compiled with support for ECC, mod\_nss 1.0.8 can use in the same time a RSA and an ECC certificate, decisions on which cipher suite to be used being made based on the Client Hello message, if the client lists support for ECC cipher suites that the server supports too, ECC cipher suites will be used.

NSS always chooses the "best/strongest" cipher. You can't specify preferred order.

mod\_nss does not support by default Caemellia or Seed cipher suites. You can adjust this if you modify the **nss\_engine\_init.c** file.

mod\_nss does not have support for DHE cipher suites due to the NSS mentioned above server side limitation.

SSL/TLS related configuration can be done within the **nss.conf** file(usually found at **/etc/httpd/conf.d/**).

**NSSNickname** directive specifies the RSA server certificate to be used

**NSSECCNickname** directive specifies the ECC server certificate to be used.

**NSSProtocol** directive specifies the SSL/TLS protocol to be used. Supported values are: **SSLv2**, **SSLv3**, **TLSv1**, **ALL**.

Example:   
**NSSProtocol SSLv3,TLSv1**.  
**NSSCipherSuite** directive specifies the cipher suites to be used. Use **+** to allow a cipher suite, and **–** to disallow a cipher suite. Within the original **nss.conf** file for the ECC configuration example, there is a small typo for the **-echde\_rsa\_null** cipher suite, it should be **-ecdhe\_rsa\_null**.

Example, without ECC:   
**NSSProtocol SSLv3,TLSv1  
NSSCipherSuite +rsa\_rc4\_128\_md5,+rsa\_rc4\_128\_sha,+rsa\_3des\_sha,-rsa\_des\_sha,-rsa\_rc4\_40\_md5,-rsa\_rc2\_40\_md5,-rsa\_null\_md5,-rsa\_null\_sha,-fips\_3des\_sha,-fips\_des\_sha,-fortezza,-fortezza\_rc4\_128\_sha,-fortezza\_null,-rsa\_des\_56\_sha,-rsa\_rc4\_56\_sha,+rsa\_aes\_128\_sha,+rsa\_aes\_256\_sha**

The example enables:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| 1 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 4 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |

Example, with ECC:   
**NSSProtocol SSLv3,TLSv1  
NSSCipherSuite +rsa\_rc4\_128\_md5,+rsa\_rc4\_128\_sha,+rsa\_3des\_sha,-rsa\_des\_sha,-rsa\_rc4\_40\_md5,-rsa\_rc2\_40\_md5,-rsa\_null\_md5,-rsa\_null\_sha,-fips\_3des\_sha,-fips\_des\_sha,-fortezza,-fortezza\_rc4\_128\_sha,-fortezza\_null,-rsa\_des\_56\_sha,-rsa\_rc4\_56\_sha,+rsa\_aes\_128\_sha,+rsa\_aes\_256\_sha,-ecdh\_ecdsa\_null\_sha,-ecdh\_ecdsa\_rc4\_128\_sha,-ecdh\_ecdsa\_3des\_sha,-ecdh\_ecdsa\_aes\_128\_sha,-ecdh\_ecdsa\_aes\_256\_sha,-ecdhe\_ecdsa\_null\_sha,-ecdhe\_ecdsa\_rc4\_128\_sha,+ecdhe\_ecdsa\_3des\_sha,+ecdhe\_ecdsa\_aes\_128\_sha,+ecdhe\_ecdsa\_aes\_256\_sha,-ecdh\_rsa\_null\_sha,-ecdh\_rsa\_128\_sha,-ecdh\_rsa\_3des\_sha,-ecdh\_rsa\_aes\_128\_sha,-ecdh\_rsa\_aes\_256\_sha,-ecdhe\_rsa\_null,-ecdhe\_rsa\_rc4\_128\_sha,+ecdhe\_rsa\_3des\_sha,+ecdhe\_rsa\_aes\_128\_sha,+ecdhe\_rsa\_aes\_256\_sha**

The example enables(assuming both a RSA and and ECC certificate are used simultaneously):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| 1 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 4 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 6 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 |
| 8 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 |
| 9 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 |

**Table 3.5** lists the cipher suites currently supported by mod\_nss 1.0.8(Apache 2.2.14) with NSS 3.12.5 and NSPR 4.8.2(source builds). Therefore, the status enabled/disabled of the cipher suites is only valid for this particular configuration. For more details about each cipher suite, refer to the main tables. The color red means that the cipher suite is disabled by default, the color green means that the cipher suite is enabled by default, the color orange means that the cipher suite was deprecated within the NSS library.

**Table 3.5 mod\_nss 1.0.8(Apache 2.2.14) with NSS 3.12.5 and NSPR 4.8.2 Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **mod\_nss Setting Name** | **Status** |
| --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | rc4 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | rc4export | disabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | rc2 | disabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | rc2export | disabled |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | des | disabled |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | desede3 | disabled |
| 7 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | rsa\_null\_md5 | disabled |
| 8 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | rsa\_null\_sha | disabled |
| 9 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | rsa\_rc4\_40\_md5 | disabled |
| 10 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | rsa\_rc4\_128\_md5 | enabled |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | rsa\_rc4\_128\_sha | enabled |
| 12 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | rsa\_rc2\_40\_md5 | disabled |
| 13 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | rsa\_des\_sha | disabled |
| 14 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | rsa\_3des\_sha | enabled |
| 15 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | rsa\_aes\_128\_sha | enabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | rsa\_aes\_256\_sha | enabled |
| 17 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | rsa\_des\_56\_sha | disabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | rsa\_rc4\_56\_sha | disabled |
| 19 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 | ecdh\_ecdsa\_null\_sha | disabled |
| 20 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | ecdh\_ecdsa\_rc4\_128\_sha | disabled |
| 22 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | ecdh\_ecdsa\_3des\_sha | disabled |
| 23 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | ecdh\_ecdsa\_aes\_128\_sha | disabled |
| 24 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | ecdh\_ecdsa\_aes\_256\_sha | disabled |
| 25 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 | ecdhe\_ecdsa\_null\_sha | disabled |
| 26 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | ecdhe\_ecdsa\_rc4\_128\_sha | disabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | ecdhe\_ecdsa\_3des\_sha | disabled |
| 28 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | ecdhe\_ecdsa\_aes\_128\_sha | disabled |
| 29 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | ecdhe\_ecdsa\_aes\_256\_sha | disabled |
| 30 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 | ecdh\_rsa\_null\_sha | disabled |
| 31 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | ecdh\_rsa\_128\_sha | disabled |
| 32 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | ecdh\_rsa\_3des\_sha | disabled |
| 33 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | ecdh\_rsa\_aes\_128\_sha | disabled |
| 34 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | ecdh\_rsa\_aes\_256\_sha | disabled |
| 35 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 | echde\_rsa\_null | disabled |
| 36 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | ecdhe\_rsa\_rc4\_128\_sha | disabled |
| 37 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | ecdhe\_rsa\_3des\_sha | disabled |
| 38 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | ecdhe\_rsa\_aes\_128\_sha | disabled |
| 39 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | ecdhe\_rsa\_aes\_256\_sha | disabled |
| 40 | SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA | 0xFEFE | SSL 3.0|TLS 1.0 | fips\_des\_sha | disabled |
| 41 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 | fips\_3des\_sha | enabled |
| 44 | SSL\_FORTEZZA\_KEA\_WITH\_NULL\_SHA | 0X001C | - | fortezza\_null | deprecated |
| 42 | SSL\_FORTEZZA\_KEA\_WITH\_FORTEZZA\_CBC\_SHA | 0x001D | - | fortezza | deprecated |
| 43 | SSL\_FORTEZZA\_KEA\_WITH\_RC4\_128\_SHA | 0x001E | - | fortezza\_rc4\_128\_sha | deprecated |

### 3.6 Firefox 3.6.x on Fedora 14

**Table 3.6** lists the cipher suites currently supported by Firefox 3.6.13(the Firefox version shipped with Fedora) on Fedora 14. For more details about each cipher suite or other versions of Firefox, refer to the main tables. The color red means that the cipher suite is disabled by default, and the color green means that the cipher suite is enabled by default.  
ECC cipher suites are not available for the Firefox version shipped with Fedora.

**Table 3.6 Firefox 3.6.13 Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Firefox Setting Name** | **Default Value** |
| --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | security.ssl2.rc4\_128 | false |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | security.ssl2.rc4\_40 | false |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | security.ssl2.rc2\_128 | false |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | security.ssl2.rc2\_40 | false |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | security.ssl2.des\_64 | false |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | security.ssl2.des\_ede3\_192 | false |
| 7 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_null\_md5 | false |
| 8 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_null\_sha | false |
| 9 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_40\_md5 | false |
| 10 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_128\_md5 | true |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc4\_128\_sha | true |
| 12 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_rc2\_40\_md5 | false |
| 13 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_des\_sha | false |
| 14 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_des\_ede3\_sha | true |
| 15 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_des\_sha | false |
| 16 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_des\_ede3\_sha | true |
| 17 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_des\_sha | false |
| 18 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_des\_ede3\_sha | true |
| 19 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_aes\_128\_sha | true |
| 20 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_aes\_128\_sha | true |
| 21 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_aes\_128\_sha | true |
| 22 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_aes\_256\_sha | true |
| 23 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_aes\_256\_sha | true |
| 24 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_aes\_256\_sha | true |
| 25 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_camellia\_128\_sha | true |
| 26 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_camellia\_128\_sha | true |
| 27 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_camellia\_128\_sha | true |
| 28 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_1024\_des\_cbc\_sha | false |
| 29 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_1024\_rc4\_56\_sha | false |
| 30 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_camellia\_256\_sha | true |
| 31 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_dss\_camellia\_256\_sha | true |
| 32 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | security.ssl3.dhe\_rsa\_camellia\_256\_sha | true |
| 33 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_seed\_sha | true |
| 34 | SSL\_RSA\_FIPS\_WITH\_DES\_CBC\_SHA | 0xFEFE | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_fips\_des\_sha | false |
| 35 | SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA | 0xFEFF | SSL 3.0|TLS 1.0 | security.ssl3.rsa\_fips\_des\_ede3\_sha | true |

## 4. OpenSSL

OpenSSL (according to its web site) is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. OpenSSL is based on SSLeay from Eric A. Young and Tim J. Hudson.

OpenSSL 0.9.8m and 1.0.0 were analyzed. This was mainly done on Ubuntu 9.1 Desktop, Ubuntu 9.1 Server x64, Debian 5.0.3 x64, Fedora 12, and FreeBSD 8.0.

OpenSSL currently supports(stable versions): SSL 2.0, SSL 3.0, TLS 1.0.

OpenSSL is by default compiled with support for ECC. The ECC cipher suites are not listed by default in 0.9.8m, you have to call them manually.

OpenSSL supports the three “popular” elliptic curves(which should assure interoperability):  
 - secp256r1(aka NIST P-256)  
 - secp384r1(aka NIST P-384)  
 - secp521r1(aka NIST P-521)

Some Linux distros, like Fedora 12, which have support for ECC disabled by default, will come with an OpenSSL version built without support for ECC.

The KRB5 cipher suites are disabled by default. If you build OpenSSL you have to manually enable support for them if you want to use them.

The IDEA cipher suites might be disabled or unusable on some distros due to patent issues.

The **EXPORT56** cipher suites are not present by default(in OpenSSL 0.9.8c and later the 56-bit export ciphers are disabled by default), you have to edit the **ssl/tls1.h** file and set the **TLS1\_ALLOW\_EXPERIMENTAL\_CIPHERSUITES** setting from 0 to 1 before building OpenSSL. It’s not recommended to do so.

The experimental cipher suites that can be enabled are the ones listed in table **Table 4.1**.

**Table 4.1 Experimental Cipher Suites**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| 1 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0065 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 |

There are additional patches that may enable support for other cipher suites, for the moment we do not focus on them.

mod\_ssl is a package that provides strong cryptography for the Apache 1.3 webserver via the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols by the help of OpenSSL.

mod\_ssl became part of the Apache HTTP Server with the release of the Apache 2 web server.

An alternative to mod\_ssl is Apache-SSL, a secure Webserver, based on Apache and SSLeay/OpenSSL.

We will focus on Apache 2.2.x and 2.3.x.

### 4.1. OpenSSL 0.9.8m Cipher Suites

In OpenSSL 0.9.8m, SEED and Camellia cipher suites are disabled by default. If you build OpenSSL you have to manually enable support for them.

The ECC cipher suites are not listed by default in OpenSSL 0.9.8m, you have to call them manually.

In OpenSSL 0.9.8m the ECDH-RSA based cipher suites do not work.

**Table 4.1.1** lists the general cipher strings supported by OpenSSL 0.9.8m.

**Table 4.1.2** lists the cipher suites supported by OpenSSL 0.9.8m. For more details about each cipher suite, refer to the main tables. The color red means that the cipher suite is disabled by default, the color green means that the cipher suite is enabled by default, the color orange means that the cipher suite was found not working. If the **OpenSSL Cipher String** column is yellow, then the cipher suite is listed in the **DEFAULT** cipher suites string(assuming the cipher suite is enabled).

eNULL = NULL  
kRSA = RSA  
aDSS = DSS

You can list the supported cipher suites with the **openssl ciphers** command.  
To get more details about the supported cipher suites you can use the **openssl ciphers -v** the command.  
Additionally use any of the values from **Table 4.1.1** with the **openssl ciphers** command.

**Table 4.1.1 OpenSSL 0.9.8m(source build) Cipher Strings**

| **No.** | **OpenSSL String Name** | **Meaning** |
| --- | --- | --- |
| 1 | -ssl2 | only SSL 2.0 cipher suites |
| 2 | -ssl3 | only SSL 3.0 cipher suites(not including eNULL and aNULL) |
| 3 | -tls1 | only TLS 1.0 cipher suites(not including eNULL and aNULL) |
| 4 | SSLv2 | only SSL 2.0 cipher suites |
| 5 | SSLv3 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 6 | TLSv1 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 7 | AES | cipher suites using AES |
| 8 | CAMELLIA | cipher suites using Camellia |
| 9 | DES | cipher suites using DES |
| 10 | 3DES | cipher suites using 3DES |
| 11 | IDEA | cipher suites using IDEA |
| 12 | RC2 | cipher suites using RC2 |
| 13 | RC4 | cipher suites using RC4 |
| 14 | SEED | cipher suites using SEED |
| 15 | MD5 | cipher suites using MD5 |
| 16 | SHA1 | cipher suites using SHA1 |
| 17 | SHA | cipher suites using SHA1 |
| 18 | ALL | all cipher suites except the eNULL ciphers |
| 19 | COMPLEMENTOFALL | the cipher suites not enabled by ALL, currently being eNULL |
| 20 | COMPLEMENTOFDEFAULT | the cipher suites not included in DEFAULT, currently being ADH and anonymous ECDH(aNULL) |
| 21 | DEFAULT | the default cipher suites list(determined at compile time, default this is: ALL:!aNULL:!eNULL) |
| 22 | HIGH | high encryption cipher suites(key lengths larger than 128-bits, + some cipher suites with 128-bit keys) |
| 23 | MEDIUM | medium encryption cipher suites, some of the ones using 128-bit encryption |
| 24 | LOW | low encryption cipher suites, the ones using 64-bit or 56-bit encryption algorithms(excluding export cipher suites) |
| 25 | EXP | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 26 | EXPORT | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 27 | EXPORT40 | 40-bit export encryption algorithms cipher suites |
| 28 | EXPORT56 | 56-bit export encryption algorithms cipher suites |
| 29 | eNULL | cipher suites offering no encryption |
| 30 | NULL | cipher suites offering no encryption |
| 31 | aNULL | cipher suites offering no authentication. The anonymous DH and anonymous ECDH algorithms. |
| 32 | DSS | cipher suites using DSS authentication |
| 33 | aDSS | cipher suites using DSS authentication |
| 34 | RSA | cipher suites using RSA key exchange |
| 35 | aRSA | cipher suites using RSA authentication |
| 36 | kRSA | cipher suites using RSA key exchange |
| 37 | DH | cipher suites using DH, including anonymous DH |
| 38 | ADH | anonymous DH cipher suites |
| 39 | EDH \* | cipher suites using DH, excluding anonymous DH |
| 40 | kEDH | cipher suites using ephemeral DH key agreement |
| 41 | aGOST \*\* | cipher suites using GOST R 34.10 (either 2001 or 94) for authentication |
| 42 | aGOST01 \*\* | cipher suites using GOST R 34.10-2001 authentication. |
| 43 | aGOST94 \*\* | cipher suites using GOST R 34.10-94 authentication |
| 44 | kGOST \*\* | cipher suites using VKO 34.10 key exchange |
| 45 | GOST94 \*\* | cipher suites using HMAC based on GOST R 34.11-94 |
| 46 | GOST89MAC \*\* | cipher suites using GOST 28147-89 MAC instead of HMAC |
| 47 | @STRENGTH | can be used at any point to sort the current cipher list in order of encryption algorithm key length |

\* There are some issues with this string. May be usable or not depending on how OpenSSL is compiled.  
\*\* Needs an external engine supporting GOST algorithms.

**Table 4.1.2 OpenSSL 0.9.8m(source build) Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **OpenSSL Cipher Suite String** | **OpenSSL Cipher String** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | RC4-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | EXP-RC4-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | RC2-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|MEDIUM|DEFAULT | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | EXP-RC2-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 5 | SSL\_CK\_IDEA\_128\_CBC\_WITH\_MD5 | 0x050080 | SSL 2.0 | IDEA-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|IDEA|MD5|MEDIUM|DEFAULT | enabled |
| 6 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | DES-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|DES|MD5|LOW|DEFAULT | enabled |
| 7 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | DES-CBC3-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|3DES|MD5|HIGH|DEFAULT | enabled |
| 8 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | NULL-MD5 | SSLv3|TLSv1|RSA|aRSA|kRSA|eNULL|NULL|MD5|COMPLEMENTOFALL | enabled |
| 9 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | NULL-SHA | SSLv3|TLSv1|RSA|aRSA|kRSA|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | EXP-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 12 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 13 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | EXP-RC2-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 14 | TLS\_RSA\_WITH\_IDEA\_CBC\_SHA | 0x0007 | SSL 3.0|TLS 1.0 | IDEA-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|IDEA|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 15 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 | EXP-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 16 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 17 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 18 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 | EXP-EDH-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 19 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|kEDH|DH|EDH\*|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 21 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 | EXP-EDH-RSA-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 22 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 23 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 24 | TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0017 | SSL 3.0|TLS 1.0 | EXP-ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|EXP|EXPORT40|COMPLEMENTOFDEFAULT | enabled |
| 25 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0 | ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|MEDIUM|COMPLEMENTOFDEFAULT | enabled |
| 26 | TLS\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0019 | SSL 3.0|TLS 1.0 | EXP-ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|EXP|EXPORT40|COMPLEMENTOFDEFAULT | enabled |
| 27 | TLS\_DH\_anon\_WITH\_DES\_CBC\_SHA | 0x001A | SSL 3.0|TLS 1.0 | ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|LOW|COMPLEMENTOFDEFAULT | enabled |
| 28 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0 | ADH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 29 | TLS\_KRB5\_WITH\_DES\_CBC\_SHA | 0x001E | SSL 3.0|TLS 1.0 | KRB5-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|SHA1|SHA|LOW|DEFAULT | disabled |
| 30 | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001F | SSL 3.0|TLS 1.0 | KRB5-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|3DES|SHA1|SHA|HIGH|DEFAULT | disabled |
| 31 | TLS\_KRB5\_WITH\_RC4\_128\_SHA | 0x0020 | SSL 3.0|TLS 1.0 | KRB5-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 32 | TLS\_KRB5\_WITH\_IDEA\_CBC\_SHA | 0x0021 | SSL 3.0|TLS 1.0 | KRB5-IDEA-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|IDEA|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 33 | TLS\_KRB5\_WITH\_DES\_CBC\_MD5 | 0x0022 | SSL 3.0|TLS 1.0 | KRB5-DES-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|MD5|LOW|DEFAULT | disabled |
| 34 | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_MD5 | 0x0023 | SSL 3.0|TLS 1.0 | KRB5-DES-CBC3-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|3DES|MD5|HIGH|DEFAULT | disabled |
| 35 | TLS\_KRB5\_WITH\_RC4\_128\_MD5 | 0x0024 | SSL 3.0|TLS 1.0 | KRB5-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|MD5|MEDIUM|DEFAULT | disabled |
| 36 | TLS\_KRB5\_WITH\_IDEA\_CBC\_MD5 | 0x0025 | SSL 3.0|TLS 1.0 | KRB5-IDEA-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|IDEA|MD5|MEDIUM|DEFAULT | disabled |
| 37 | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_SHA | 0x0026 | SSL 3.0|TLS 1.0 | EXP-KRB5-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 38 | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_SHA | 0x0027 | SSL 3.0|TLS 1.0 | EXP-KRB5-RC2-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC2|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 39 | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_SHA | 0x0028 | SSL 3.0|TLS 1.0 | EXP-KRB5-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 40 | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_MD5 | 0x0029 | SSL 3.0|TLS 1.0 | EXP-KRB5-DES-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 41 | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x002A | SSL 3.0|TLS 1.0 | EXP-KRB5-RC2-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC2|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 42 | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x002B | SSL 3.0|TLS 1.0 | EXP-KRB5-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 43 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 44 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | DHE-DSS-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 45 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | DHE-RSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 46 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0 | ADH-AES128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 47 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 48 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | DHE-DSS-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 49 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | DHE-RSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 50 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0 | ADH-AES256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 51 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|SHA1|SHA |HIGH|DEFAULT | disabled |
| 52 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 53 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 54 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 55 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | EXP1024-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 56 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 57 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | EXP1024-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 58 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0065 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 59 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | DHE-DSS-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|kEDH|DH|EDH\*|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 60 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 61 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 62 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 63 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 64 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|SEED|SHA1|SHA|MEDIUM | disabled |
| 65 | TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0099 | SSL 3.0|TLS 1.0 | DHE-DSS-SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|SEED|SHA1|SHA|MEDIUM | disabled |
| 66 | TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA | 0x009A | SSL 3.0|TLS 1.0 | DHE-RSA-SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|SEED|SHA1|SHA|MEDIUM | disabled |
| 67 | TLS\_DH\_anon\_WITH\_SEED\_CBC\_SHA | 0x009B | SSL 3.0|TLS 1.0 | ADH-SEED-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|SEED|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | disabled |
| 68 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-NULL-SHA | - | enabled |
| 69 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-RC4-SHA | - | enabled |
| 70 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-DES-CBC3-SHA | - | enabled |
| 71 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES128-SHA | - | enabled |
| 72 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES256-SHA | - | enabled |
| 73 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-NULL-SHA | - | enabled |
| 74 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-RC4-SHA | - | enabled |
| 75 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-DES-CBC3-SHA | - | enabled |
| 76 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES128-SHA | - | enabled |
| 77 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES256-SHA | - | enabled |
| 78 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 | ECDH-RSA-NULL-SHA | aRSA | unusable |
| 79 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | ECDH-RSA-RC4-SHA | aRSA | unusable |
| 80 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | ECDH-RSA-DES-CBC3-SHA | aRSA | unusable |
| 81 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | ECDH-RSA-AES128-SHA | aRSA | unusable |
| 82 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | ECDH-RSA-AES256-SHA | aRSA | unusable |
| 83 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 | ECDHE-RSA-NULL-SHA | aRSA | enabled |
| 84 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | ECDHE-RSA-RC4-SHA | aRSA | enabled |
| 85 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | ECDHE-RSA-DES-CBC3-SHA | aRSA | enabled |
| 86 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES128-SHA | aRSA | enabled |
| 87 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES256-SHA | aRSA | enabled |
| 88 | TLS\_ECDH\_anon\_WITH\_NULL\_SHA | 0xC015 | SSL 3.0|TLS 1.0 | AECDH-NULL-SHA | aNULL|COMPLEMENTOFDEFAULT | enabled |
| 89 | TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA | 0xC016 | SSL 3.0|TLS 1.0 | AECDH-RC4-SHA | aNULL|COMPLEMENTOFDEFAULT | enabled |
| 90 | TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC017 | SSL 3.0|TLS 1.0 | AECDH-DES-CBC3-SHA | aNULL|COMPLEMENTOFDEFAULT | enabled |
| 91 | TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0xC018 | SSL 3.0|TLS 1.0 | AECDH-AES128-SHA | aNULL|COMPLEMENTOFDEFAULT | enabled |
| 92 | TLS\_ECDH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0xC019 | SSL 3.0|TLS 1.0 | AECDH-AES256-SHA | aNULL|COMPLEMENTOFDEFAULT | enabled |

\* There are some issues with this string. May be usable or not depending on how OpenSSL is compiled.

### 4.2. OpenSSL 1.0.0 Cipher Suites

The SEED and Camellia cipher suites are now enabled by default.

The ECC cipher suites are now listed by default.

The ECDH-RSA based cipher suites do work now.

The SSL 2.0 cipher suites are no longer part of the **DEFAULT** cipher string.

Initial support for RFC 4279 PSK TLS cipher suites. The currently supported ones are listed in **Table 4.2.1**.

**Table 4.2.1 OpenSSL 1.0.0 PSK TLS Cipher Suites**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Cipher Suite | Hex Value | SSL/TLS Version |
| 1 | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | SSL 3.0|TLS 1.0 |
| 2 | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | SSL 3.0|TLS 1.0 |
| 3 | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | SSL 3.0|TLS 1.0 |
| 4 | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | SSL 3.0|TLS 1.0 |

GOST engine, supporting several GOST algorithms and public key formats. The currently supported cipher suites are listed in **Table 4.2.2**.

The GOST cipher suites do not work under SSL 3.0.

**Table 4.2.2 OpenSSL 1.0.0 GOST Cipher Suites**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| 1 | TLS\_GOSTR341094\_WITH\_28147\_CNT\_IMIT | 0x0080 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_GOSTR341001\_WITH\_28147\_CNT\_IMIT | 0x0081 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_GOSTR341094\_WITH\_NULL\_GOSTR3411 | 0x0082 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_GOSTR341001\_WITH\_NULL\_GOSTR3411 | 0x0083 | SSL 3.0|TLS 1.0 |

**Table 4.2.3** lists the general cipher strings supported by OpenSSL 1.0.0. If a green shade is present near a string(**No.** column), then this string is new in OpenSSL 1.0.0.

**Table 4.2.4** lists the cipher suites supported by OpenSSL 1.0.0. For more details about each cipher suite, refer to the main tables. The color red means that the cipher suite is disabled by default, the color green means that the cipher suite is enabled by default. If the **OpenSSL Cipher String** column is yellow, then the cipher suite is listed in the **DEFAULT** cipher suites string(assuming the respective cipher suite is enabled).

kRSA = RSA  
SHA1 = SHA  
EXP = EXPORT  
eNULL = NULL  
AECDH =! aECDH

You can list the supported cipher suites with the **openssl ciphers** command.  
To get more details about the supported cipher suites you can use the **openssl ciphers -v** the command.  
Additionally use any of the values from **Table 4.2.3** with the **openssl ciphers** command.

**Table 4.2.3 OpenSSL 1.0.0(source build) Cipher Strings**

| **No.** | **Open String Name** | **Meaning** |
| --- | --- | --- |
| 1 | -ssl2 | only SSL 2.0 cipher suites |
| 2 | -ssl3 | only SSL 3.0 cipher suites(not including eNULL and aNULL) |
| 3 | -tls1 | only TLS 1.0 cipher suites(not including eNULL and aNULL) |
| 4 | SSLv2 | only SSL 2.0 cipher suites |
| 5 | SSLv3 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 6 | TLSv1 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 7 | AES | cipher suites using AES |
| 8 | AES128 | cipher suites using AES 128-bit |
| 9 | AES256 | cipher suites using AES 256-bit |
| 10 | CAMELLIA | cipher suites using Camellia |
| 11 | CAMELLIA128 | cipher suites using Camellia 128-bit |
| 12 | CAMELLIA256 | cipher suites using Camellia 256-bit |
| 13 | DES | cipher suites using DES |
| 14 | 3DES | cipher suites using 3DES |
| 15 | IDEA | cipher suites using IDEA |
| 16 | RC2 | cipher suites using RC2 |
| 17 | RC4 | cipher suites using RC4 |
| 18 | SEED | cipher suites using SEED |
| 19 | MD5 | cipher suites using MD5 |
| 20 | SHA1 | cipher suites using SHA1 |
| 21 | SHA | cipher suites using SHA1 |
| 22 | ALL | all cipher suites except the eNULL ciphers |
| 23 | COMPLEMENTOFALL | the cipher suites not enabled by ALL, currently being eNULL |
| 24 | COMPLEMENTOFDEFAULT | the cipher suites not included in DEFAULT, currently being ADH and AECDH(aNULL). |
| 25 | DEFAULT | the default cipher suites list(determined at compile time, default this is: ALL:!aNULL:!eNULL) |
| 26 | HIGH | high encryption cipher suites(key lengths larger than 128-bits, + some cipher suites with 128-bit keys) |
| 27 | MEDIUM | medium encryption cipher suites, some of the ones using 128-bit encryption |
| 28 | LOW | low encryption cipher suites, the ones using 64-bit or 56-bit encryption algorithms(excluding export cipher suites) |
| 29 | EXP | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 30 | EXPORT | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 31 | EXPORT40 | 40-bit export encryption algorithms cipher suites |
| 32 | EXPORT56 | 56-bit export encryption algorithms cipher suites |
| 33 | eNULL | cipher suites offering no encryption |
| 34 | NULL | cipher suites offering no encryption |
| 35 | aNULL | cipher suites offering no authentication. The anonymous DH and anonymous ECDH algorithms(ADH and AECDH). |
| 36 | DSS | cipher suites using DSS authentication |
| 37 | aDSS | cipher suites using DSS authentication |
| 38 | RSA | cipher suites using RSA key exchange |
| 39 | aRSA | cipher suites using RSA authentication |
| 40 | kRSA | cipher suites using RSA key exchange |
| 41 | DH | cipher suites using DH, including anonymous DH |
| 42 | ADH | anonymous DH cipher suites |
| 43 | EDH | cipher suites using DH, excluding anonymous DH |
| 44 | kEDH | cipher suites using ephemeral DH key agreement |
| 45 | ECDH | ECDH cert or ephemeral ECDH |
| 46 | aECDH | ECDH cert |
| 47 | AECDH | anonymous ECDH |
| 48 | EECDH | non-anonymous ephemeral ECDH |
| 49 | kECDH | ECDH cert (signed with either RSA or ECDSA) |
| 50 | kECDHe | ECDH cert, signed with ECDSA |
| 51 | kECDHr | ECDH cert, signed with RSA |
| 52 | kEECDH | ephemeral ECDH |
| 53 | ECDSA | ECDSA cert |
| 54 | aECDSA | ECDSA cert |
| 55 | PSK | PSK authentication |
| 56 | aGOST | cipher suites using GOST R 34.10 (either 2001 or 94) for authentication |
| 57 | aGOST01 | cipher suites using GOST R 34.10-2001 authentication. |
| 58 | aGOST94 | cipher suites using GOST R 34.10-94 authentication |
| 59 | kGOST | cipher suites using VKO 34.10 key exchange |
| 60 | GOST94 | cipher suites using HMAC based on GOST R 34.11-94 |
| 62 | GOST89MAC | cipher suites using GOST 28147-89 MAC instead of HMAC |
| 63 | @STRENGTH | can be used at any point to sort the current cipher list in order of encryption algorithm key length |

**Table 4.2.4 OpenSSL 1.0.0(source build) Cipher Suites**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **OpenSSL Cipher Suite String** | **OpenSSL Cipher String** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | RC4-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | EXP-RC4-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40 | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | RC2-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|MEDIUM | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | EXP-RC2-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40 | enabled |
| 5 | SSL\_CK\_IDEA\_128\_CBC\_WITH\_MD5 | 0x050080 | SSL 2.0 | IDEA-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|IDEA|MD5|MEDIUM | enabled |
| 6 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | DES-CBC-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|DES|MD5|LOW | enabled |
| 7 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | DES-CBC3-MD5 | -ssl2|SSLv2|ALL|RSA|aRSA|kRSA|3DES|MD5|HIGH | enabled |
| 8 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | NULL-MD5 | SSLv3|TLSv1|RSA|aRSA|kRSA|MD5|eNULL|NULL|COMPLEMENTOFALL | enabled |
| 9 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | NULL-SHA | SSLv3|TLSv1|RSA|aRSA|kRSA|SHA1|eNULL|NULL|COMPLEMENTOFALL | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | EXP-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 12 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 13 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | EXP-RC2-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 14 | TLS\_RSA\_WITH\_IDEA\_CBC\_SHA | 0x0007 | SSL 3.0|TLS 1.0 | IDEA-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|IDEA|SHA1|SHA|MEDIUMDEFAULT | enabled |
| 15 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 | EXP-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT40 |DEFAULT | enabled |
| 16 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 17 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 18 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 | EXP-EDH-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 19 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 21 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 | EXP-EDH-RSA-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 22 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 23 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 24 | TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0017 | SSL 3.0|TLS 1.0 | EXP-ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|EXP|EXPORT40|COMPLEMENTOFDEFAULT | enabled |
| 25 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0 | ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|MEDIUM|COMPLEMENTOFDEFAULT | enabled |
| 26 | TLS\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0019 | SSL 3.0|TLS 1.0 | EXP-ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|EXP|EXPORT40|COMPLEMENTOFDEFAULT | enabled |
| 27 | TLS\_DH\_anon\_WITH\_DES\_CBC\_SHA | 0x001A | SSL 3.0|TLS 1.0 | ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|LOW|COMPLEMENTOFDEFAULT | enabled |
| 28 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0 | ADH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 29 | TLS\_KRB5\_WITH\_DES\_CBC\_SHA | 0x001E | SSL 3.0|TLS 1.0 | KRB5-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|SHA1|SHA|LOW|DEFAULT | disabled |
| 30 | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001F | SSL 3.0|TLS 1.0 | KRB5-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|3DES|SHA1|SHA|HIGH|DEFAULT | disabled |
| 31 | TLS\_KRB5\_WITH\_RC4\_128\_SHA | 0x0020 | SSL 3.0|TLS 1.0 | KRB5-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 32 | TLS\_KRB5\_WITH\_IDEA\_CBC\_SHA | 0x0021 | SSL 3.0|TLS 1.0 | KRB5-IDEA-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|IDEA|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 33 | TLS\_KRB5\_WITH\_DES\_CBC\_MD5 | 0x0022 | SSL 3.0|TLS 1.0 | KRB5-DES-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|MD5|LOW|DEFAULT | disabled |
| 34 | TLS\_KRB5\_WITH\_3DES\_EDE\_CBC\_MD5 | 0x0023 | SSL 3.0|TLS 1.0 | KRB5-DES-CBC3-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|3DES|MD5|HIGH|DEFAULT | disabled |
| 35 | TLS\_KRB5\_WITH\_RC4\_128\_MD5 | 0x0024 | SSL 3.0|TLS 1.0 | KRB5-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|MD5|MEDIUM|DEFAULT | disabled |
| 36 | TLS\_KRB5\_WITH\_IDEA\_CBC\_MD5 | 0x0025 | SSL 3.0|TLS 1.0 | KRB5-IDEA-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|IDEA|MD5|MEDIUM|DEFAULT | disabled |
| 37 | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_SHA | 0x0026 | SSL 3.0|TLS 1.0 | EXP-KRB5-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 38 | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_SHA | 0x0027 | SSL 3.0|TLS 1.0 | EXP-KRB5-RC2-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC2|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 39 | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_SHA | 0x0028 | SSL 3.0|TLS 1.0 | EXP-KRB5-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|SHA1|SHA|EXP|EXPORT40|DEFAULT | disabled |
| 40 | TLS\_KRB5\_EXPORT\_WITH\_DES\_CBC\_40\_MD5 | 0x0029 | SSL 3.0|TLS 1.0 | EXP-KRB5-DES-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|DES|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 41 | TLS\_KRB5\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x002A | SSL 3.0|TLS 1.0 | EXP-KRB5-RC2-CBC-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC2|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 42 | TLS\_KRB5\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x002B | SSL 3.0|TLS 1.0 | EXP-KRB5-RC4-MD5 | -ssl3|-tls1|SSLv3|TLSv1|ALL|KRB5|RC4|MD5|EXP|EXPORT40|DEFAULT | disabled |
| 43 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|AES128 |SHA1|SHA|HIGH|DEFAULT | enabled |
| 44 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | DHE-DSS-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 45 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | DHE-RSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|AES|AES128|SHA1|HIGH|DEFAULT | enabled |
| 46 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0 | ADH-AES128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|AES128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 47 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 48 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | DHE-DSS-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 49 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | DHE-RSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 50 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0 | ADH-AES256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|AES256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 51 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 52 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 53 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 54 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 55 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | EXP1024-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 56 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-DES-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|kEDH|DH|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 57 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | EXP1024-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 58 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0065 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 59 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | DHE-DSS-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 60 | TLS\_GOSTR341094\_WITH\_28147\_CNT\_IMIT | 0x0080 | SSL 3.0|TLS 1.0 | GOST94-GOST89-GOST89 | -ssl3|-tls1|SSLv3|TLSv1|ALL|aGOST|aGOST94|kGOST|GOST89MAC|HIGH | disabled |
| 61 | TLS\_GOSTR341001\_WITH\_28147\_CNT\_IMIT | 0x0081 | SSL 3.0|TLS 1.0 | GOST2001-GOST89-GOST89 | -ssl3|-tls1|SSLv3|TLSv1|ALL|aGOST|aGOST01|kGOST|GOST89MAC|HIGH | disabled |
| 62 | TLS\_GOSTR341094\_WITH\_NULL\_GOSTR3411 | 0x0082 | SSL 3.0|TLS 1.0 | GOST94-NULL-GOST94 | SSLv3|TLSv1|aGOST|aGOST94|kGOST|eNULL|NULL|GOST94|COMPLEMENTOFALL | disabled |
| 63 | TLS\_GOSTR341001\_WITH\_NULL\_GOSTR3411 | 0x0083 | SSL 3.0|TLS 1.0 | GOST2001-NULL-GOST94 | SSLv3|TLSv1|aGOST|aGOST01|kGOST|eNULL|NULL|GOST94|COMPLEMENTOFALL | disabled |
| 64 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 65 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 66 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 67 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 68 | TLS\_PSK\_WITH\_RC4\_128\_SHA | 0x008A | SSL 3.0|TLS 1.0 | PSK-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|PSK|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 69 | TLS\_PSK\_WITH\_3DES\_EDE\_CBC\_SHA | 0x008B | SSL 3.0|TLS 1.0 | PSK-3DES-EDE-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|PSK|3DES|SHA1|SHA1|SHA|HIGH|DEFAULT | enabled |
| 70 | TLS\_PSK\_WITH\_AES\_128\_CBC\_SHA | 0x008C | SSL 3.0|TLS 1.0 | PSK-AES128-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|PSK|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 71 | TLS\_PSK\_WITH\_AES\_256\_CBC\_SHA | 0x008D | SSL 3.0|TLS 1.0 | PSK-AES256-CBC-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|PSK|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 72 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 73 | TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0099 | SSL 3.0|TLS 1.0 | DHE-DSS-SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 74 | TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA | 0x009A | SSL 3.0|TLS 1.0 | DHE-RSA-SEED-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 75 | TLS\_DH\_anon\_WITH\_SEED\_CBC\_SHA | 0x009B | SSL 3.0|TLS 1.0 | ADH-SEED-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|SEED|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | enabled |
| 76 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-NULL-SHA | SSLv3|TLSv1|aECDH|ECDH|kECDH|kECDHe|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 77 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 78 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 79 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 80 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 81 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-NULL-SHA | SSLv3|TLSv1|aECDSA|ECDSA|ECDH|EECDH|kEECDH|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 82 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 83 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 84 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 85 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 86 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 | ECDH-RSA-NULL-SHA | SSLv3|TLSv1|aECDH|ECDH|kECDH|kECDHr|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 87 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | ECDH-RSA-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|KECDHr|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 88 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | ECDH-RSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 89 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | ECDH-RSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 90 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | ECDH-RSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 91 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 | ECDHE-RSA-NULL-SHA | SSLv3|TLSv1|aRSA|ECDH|EECDH|kEECDH|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 92 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | ECDHE-RSA-RC4-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 93 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | ECDHE-RSA-DES-CBC3-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 94 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES128-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 95 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES256-SHA | -ssl3|-tls1|SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 96 | TLS\_ECDH\_anon\_WITH\_NULL\_SHA | 0xC015 | SSL 3.0|TLS 1.0 | AECDH-NULL-SHA | SSLv3|TLSv1|AECDH|ECDH|kEECDH|aNULL|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | enabled |
| 97 | TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA | 0xC016 | SSL 3.0|TLS 1.0 | AECDH-RC4-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|RC4|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | enabled |
| 98 | TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC017 | SSL 3.0|TLS 1.0 | AECDH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 99 | TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0xC018 | SSL 3.0|TLS 1.0 | AECDH-AES128-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|AES|AES128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 100 | TLS\_ECDH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0xC019 | SSL 3.0|TLS 1.0 | AECDH-AES256-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|AES|AES256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |

### 4.3. mod\_ssl (Apache 2.2.15 + OpenSSL 0.9.8m) Cipher Suites

mod\_ssl became part of the Apache HTTP Server with the release of the Apache 2 web server.

Can use in the same time a RSA and a DSA certificate.

For the DHE exchanges, by default a 1024-bit modulus is used.

**SSLCertificateFile** directive points to the PEM encoded server certificate.

**SSLCertificateKeyFile** directive can be used to point at the key file if the key is not combined with the certificate.

Example, both a RSA and a DSA certificate are used in the same time:

**SSLCertificateFile "/usr/local/apache2/conf/rsa\_server.pem"  
SSLCertificateKeyFile "/usr/local/apache2/conf/rsa\_server.key"**

**SSLCertificateFile "/usr/local/apache2/conf/dsa\_server.pem"  
SSLCertificateKeyFile "/usr/local/apache2/conf/dsa\_server.key"**

**SSLCipherSuite** directive is a complex one, being used to specify the cipher suites. The values usable with this directive are similar with the cipher strings from OpenSSL.  
The SSLv3 and TLS 1.0 values(aliases) are equivalent(SSLv3 = TLSv1), either of these enables both SSL 3.0 and TLS 1.0. And SSLv3 or TLSv1 enable all the SSL 3.0 or TLSv1 cipher suites, including the eNULL and aNULL ones.  
You cannot really dictate the preferred cipher suite with (just) the **SSLCipherSuite** directive. For example say you do(in order to list in a desired order some cipher suites):  
**openssl ciphers AES:RC4:+AES -v**  
Which basically first lists the AES and RC4 cipher suites, and then moves the AES ciphers to the end of the list. If you put on Apache:  
**SSLCipherSuite AES:RC4:+AES**  
and the client lists first AES cipher suites, an AES based cipher suite will be used.  
To use the server’s preferred cipher suite order enable the **SSLHonorCipherOrder** directive:  
**SSLHonorCipherOrder on**

**Table 4.3.1** lists the general mod\_ssl aliases that can be used with the **SSLCipherSuite** directive.

**SSLProtocol** directive can be used to control the SSL protocol flavors. Acceptable values are: **all**, **SSLv2**, **SSLv3**, **TLSv1**.  
Normally you don’t really need to use this, unless you want to disable just SSL 3.0 or just TLS 1.0.

Example 1:  
**SSLCipherSuite AES+kEDH+aRSA**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |

Example 2:  
**SSLCipherSuite DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:AES256-SHA:AES128-SHA**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |

Example 3:  
**SSLCipherSuite HIGH:!ADH:!SSLv2**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default), assuming you use in the same time a RSA and a DSA certificate:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 6 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 8 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |

Example 4:  
**SSLProtocol all -SSLv3  
SSLCipherSuite aRSA+AES**

**Note**: Normally there aren’t any AES cipher suites under SSL 2.0, so there aren’t such cipher suites under the **aRSA+AES** cipher suites list(so we don’t have to add a **!SSLv2** under the **SSLCipherSuite** directive too).  
Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), only TLS 1.0 is allowed):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | TLS 1.0 |

**Table 4.3.2** lists the cipher suites supported by mod\_ssl, Apache 2.2.15 + OpenSSL 0.9.8m were analyzed, both built from source. Therefore, the status enabled/disabled of the cipher suites is only relevant for this particular configuration. Note that a RSA and a DSA certificate were used in the same time.  
The default configuration on Apache 2.2.15 is(according to the **httpd-ssl.conf** file):  
**SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL**  
Which in case of a default source built of OpenSSL 0.9.m is somehow misleading. Note that the **eNULL** cipher suites are not enabled by this configuration.

**Table 4.3.1 mod\_ssl(Apache 2.2.15 + OpenSSL 0.9.8m, both source builds) SSLCipherSuite General Aliases**

| **No.** | **mod\_ssl category Alias** | **Meaning** |
| --- | --- | --- |
| 1 | SSLv2 | only SSL 2.0 cipher suites |
| 2 | SSLv3 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 3 | TLSv1 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 4 | AES | cipher suites using AES |
| 5 | CAMELLIA | cipher suites using Camellia |
| 6 | DES | cipher suites using DES |
| 7 | 3DES | cipher suites using 3DES |
| 8 | IDEA | cipher suites using IDEA |
| 9 | RC2 | cipher suites using RC2 |
| 10 | RC4 | cipher suites using RC4 |
| 11 | SEED | cipher suites using SEED |
| 12 | MD5 | cipher suites using MD5 |
| 13 | SHA1 | cipher suites using SHA1 |
| 14 | SHA | cipher suites using SHA1 |
| 15 | ALL | all cipher suites except the eNULL ciphers |
| 16 | COMPLEMENTOFALL | the cipher suites not enabled by ALL, currently being eNULL |
| 17 | COMPLEMENTOFDEFAULT | the cipher suites not included in DEFAULT, currently being ADH(or aNULL) |
| 18 | DEFAULT | the default cipher suites list(determined at OpenSSL compile time, default this is: ALL:!aNULL:!eNULL) |
| 19 | HIGH | high encryption cipher suites(key lengths larger than 128-bits, + some cipher suites with 128-bit keys) |
| 20 | MEDIUM | medium encryption cipher suites, some of the ones using 128-bit encryption |
| 21 | LOW | low encryption cipher suites, the ones using 64-bit or 56-bit encryption algorithms(excluding export cipher suites) |
| 22 | EXP | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 23 | EXPORT | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 24 | EXPORT40 | 40-bit export encryption algorithms cipher suites |
| 25 | EXPORT56 | 56-bit export encryption algorithms cipher suites |
| 26 | eNULL | cipher suites offering no encryption |
| 27 | NULL | cipher suites offering no encryption |
| 28 | aNULL | cipher suites offering no authentication. The anonymous DH algorithms(ADH). |
| 29 | DSS | cipher suites using DSS authentication |
| 30 | aDSS | cipher suites using DSS authentication |
| 31 | RSA | cipher suites using RSA key exchange |
| 32 | aRSA | cipher suites using RSA authentication |
| 33 | kRSA | cipher suites using RSA key exchange |
| 34 | DH | cipher suites using DH, including anonymous DH |
| 35 | ADH | anonymous DH cipher suites |
| 36 | EDH \* | cipher suites using DH, excluding anonymous DH |
| 37 | kEDH | cipher suites using ephemeral DH key agreement |

\* There are some issues with this string. May be usable or not depending on how OpenSSL 0.9.8m is compiled.

**Table 4.3.2 mod\_ssl Apache 2.2.15(source build) + OpenSSL 0.9.8m(source build) Cipher Suites and Aliases usable with the SSLCipherSuite Directive**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **mod\_ssl Cipher Suite Aliases** | **mod\_ssl category Aliases** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | RC4-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | EXP-RC4-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | RC2-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|MEDIUM|DEFAULT | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | EXP-RC2-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 5 | SSL\_CK\_IDEA\_128\_CBC\_WITH\_MD5 | 0x050080 | SSL 2.0 | IDEA-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|IDEA|MD5|MEDIUM|DEFAULT | enabled |
| 6 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | DES-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|DES|MD5|LOW|DEFAULT | enabled |
| 7 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | DES-CBC3-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|3DES|MD5|HIGH|DEFAULT | enabled |
| 8 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | NULL-MD5 | SSLv3|TLSv1|RSA|aRSA|kRSA|eNULL|NULL|MD5|COMPLEMENTOFALL | disabled |
| 9 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | NULL-SHA | SSLv3|TLSv1|RSA|aRSA|kRSA|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | EXP-RC4-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | RC4-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 12 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | RC4-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 13 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | EXP-RC2-CBC-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 14 | TLS\_RSA\_WITH\_IDEA\_CBC\_SHA | 0x0007 | SSL 3.0|TLS 1.0 | IDEA-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|IDEA|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 15 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 | EXP-DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 16 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 17 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | DES-CBC3-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 18 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 | EXP-EDH-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 19 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|kEDH|DH|EDH\*|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 21 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 | EXP-EDH-RSA-DES-CBC-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 22 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 23 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 24 | TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0017 | SSL 3.0|TLS 1.0 | EXP-ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|EXP|EXPORT40|COMPLEMENTOFDEFAULT | disabled |
| 25 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0 | ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|MEDIUM|COMPLEMENTOFDEFAULT | disabled |
| 26 | TLS\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0019 | SSL 3.0|TLS 1.0 | EXP-ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|EXP|EXPORT40|COMPLEMENTOFDEFAULT | disabled |
| 27 | TLS\_DH\_anon\_WITH\_DES\_CBC\_SHA | 0x001A | SSL 3.0|TLS 1.0 | ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|LOW|COMPLEMENTOFDEFAULT | disabled |
| 28 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0 | ADH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 29 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | AES128-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 30 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | DHE-DSS-AES128-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 31 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | DHE-RSA-AES128-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 32 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0 | ADH-AES128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 33 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | AES256-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 34 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | DHE-DSS-AES256-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 35 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | DHE-RSA-AES256-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|AES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 36 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0 | ADH-AES256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 37 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | CAMELLIA128-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|SHA1|SHA |HIGH|DEFAULT | disabled |
| 38 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 39 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 40 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 41 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | EXP1024-DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 42 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 43 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | EXP1024-RC4-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 44 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0065 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-RC4-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 45 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | DHE-DSS-RC4-SHA | SSLv3|TLSv1|ALL|DSS|kEDH|DH|EDH\*|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 46 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | CAMELLIA256-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 47 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 48 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|CAMELLIA|SHA1|SHA|HIGH|DEFAULT | disabled |
| 49 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 50 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | SEED-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|SEED|SHA1|SHA|MEDIUM | disabled |
| 51 | TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0099 | SSL 3.0|TLS 1.0 | DHE-DSS-SEED-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH\*|SEED|SHA1|SHA|MEDIUM | disabled |
| 52 | TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA | 0x009A | SSL 3.0|TLS 1.0 | DHE-RSA-SEED-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH\*|SEED|SHA1|SHA|MEDIUM | disabled |
| 53 | TLS\_DH\_anon\_WITH\_SEED\_CBC\_SHA | 0x009B | SSL 3.0|TLS 1.0 | ADH-SEED-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|SEED|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | disabled |

\* There are some issues with this string. May be usable or not depending on how OpenSSL 0.9.m is compiled.

### 4.4. mod\_ssl (Apache 2.3.5 Alpha + OpenSSL 1.0.0) Cipher Suites

mod\_ssl became part of the Apache HTTP Server with the release of the Apache 2 web server.

ECC is supported with mod\_ssl(Apache 2.3.5 Alpha) if built against an OpenSSL version supporting ECC(we tested with OpenSSL 1.0.0).

mod\_ssl(Apache 2.3.5 Alpha) can use in the same time a RSA, a DSA certificate and an ECC certificate(this was an ECDSA signed certificate or a RSA signed one containing an ECC key).

Apache 2.3.5 Alpha mod\_ssl(OpenSSL 1.0.0) supports the three “popular” elliptic curves(which should assure interoperability):  
 - secp256r1(aka NIST P-256)  
 - secp384r1(aka NIST P-384)  
 - secp521r1(aka NIST P-521)

For the DHE exchanges, by default a 1024-bit modulus is used.

**SSLCertificateFile** directive points to the PEM encoded server certificate.

**SSLCertificateKeyFile** directive can be used to point at the key file if the key is not combined with the certificate.

Example, both a RSA , a DSA and an ECC certificate are used in the same time:

**SSLCertificateFile "/usr/local/apache2/conf/rsa\_server.pem"  
SSLCertificateKeyFile "/usr/local/apache2/conf/rsa\_server.key"**

**SSLCertificateFile "/usr/local/apache2/conf/dsa\_server.pem"  
SSLCertificateKeyFile "/usr/local/apache2/conf/dsa\_server.key"**

**SSLCertificateFile "/usr/local/apache2/conf/ecc\_server.pem"  
SSLCertificateKeyFile "/usr/local/apache2/conf/ecc\_server.key"**

**SSLCipherSuite** directive is a complex one, being used to specify the cipher suites. The values usable with this directive are similar with the cipher strings from OpenSSL.  
The SSLv3 and TLS 1.0 values(aliases) are equivalent(SSLv3 = TLSv1), either of these enables both SSL 3.0 and TLS 1.0. And SSLv3 or TLSv1 enable all the SSL 3.0 or TLSv1 cipher suites, including the eNULL and aNULL ones.  
You cannot really dictate the preferred cipher suite with (just) the **SSLCipherSuite** directive. For example say you do(in order to list in a desired order some cipher suites):  
**openssl ciphers AES:RC4:+AES –v**  
Which basically first lists the AES and RC4 cipher suites, and then moves the AES ciphers to the end of the list. If you put:  
**SSLCipherSuite AES:RC4:+AES**  
and the client lists first AES cipher suites, an AES based cipher suite will be used.  
This behavior may prevent you, when using an ECDSA and a RSA certificate in the same time(to support clients that only can use RSA based cipher suites), from selecting on the server side an ECDSA based cipher suites when the client support such cipher suites, if the client lists first the RSA based ones. For example Firefox 3.6 lists first an ECDSA based cipher suite, while IE8 on Windows 7 a RSA based one with a kRSA exchange.  
To use the server’s preferred cipher suite order enable the **SSLHonorCipherOrder** directive:  
**SSLHonorCipherOrder on**

**Table 4.4.1** lists the general mod\_ssl aliases that can be used with the **SSLCipherSuite** directive. If a green shade is present near a string(**No.** column), then this string is new in Apache 2.3.5 Alpha compared to Apache 2.2.25.

**SSLProtocol** directive can be used to control the SSL protocol flavors. Acceptable values are: **all**, **SSLv2**, **SSLv3**, **TLSv1**.  
Normally you don’t really need to use this, unless you want to disable just SSL 3.0 or just TLS 1.0.

Example 1:  
**SSLCipherSuite AES+kEDH+aRSA**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |

Example 2:  
**SSLCipherSuite ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:AES256-SHA:AES128-SHA**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default), assuming you use a RSA certificate(signed with RSA and containing a RSA key):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 |
| 6 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 |

Example 3:  
**SSLCipherSuite HIGH:!ADH:!AECDH:!SSLv2**

Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), TLS 1.0 is used by default), assuming you use in the same time a RSA(signed with RSA and containing a RSA key) and an ECDSA certificate(signed with ECDSA and containing an ECC key):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 |
| 5 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 |
| 6 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 |
| 7 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 |
| 12 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 |
| 13 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 |
| 14 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 |
| 15 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 |
| 16 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 |
| 17 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 |
| 18 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 |
| 19 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 |

Example 4:  
**SSLProtocol all -SSLv3  
SSLCipherSuite aRSA+AES**

**Note**: Normally there aren’t any AES cipher suites under SSL 2.0, so there aren’t such cipher suites under the **aRSA+AES** cipher suites list(so we don’t have to add a **!SSLv2** under the **SSLCipherSuite** directive too).  
Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), only TLS 1.0 is allowed) assuming you use a RSA certificate(signed with RSA and containing a RSA key):

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | TLS 1.0 |

Example 5:  
**SSLProtocol all -SSLv3  
SSLCipherSuite aECDSA+AES:aRSA+AES**

**Note**: Normally there aren’t any AES cipher suites under SSL 2.0, so there aren’t such cipher suites under the **aECDSA+AES:aRSA+AES** cipher suites list(so we don’t have to add a !SSLv2 under the **SSLCipherSuite** directive too).  
Enables(not necessarily in the preferred order(it relates to the way the cipher suites were listed by the client), only TLS 1.0 is allowed), assuming you use a RSA(signed with RSA and containing a RSA key) and an ECDSA certificate(signed with ECDSA and containing an ECC key) in the same time:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Protocol Version** |
| 1 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 |
| 2 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | TLS 1.0 |
| 3 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 |
| 4 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | TLS 1.0 |
| 5 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 |
| 6 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 |
| 7 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 |
| 8 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 |

**Table 4.4.2** lists the cipher suites supported by mod\_ssl, Apache 2.3.5 Alpha + OpenSSL 1.0.0 were analyzed, both built from source. Therefore, the status enabled/disabled of the cipher suites is only relevant for this particular configuration. Note that a RSA, a DSA and an ECC certificate(the ECC one was an ECDSA signed certificate or a RSA signed one containing an ECC key) were used in the same time.  
The default configuration on Apache 2.3.5 Alpha is(according to the **httpd-ssl.conf** file):  
**SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL**  
Which in case of a default source built of OpenSSL 1.0.0 is somehow misleading. Note that the **eNULL** cipher suites are not enabled by this configuration. And that some AECDH cipher suites are enabled by default. To disable them add to the **SSLCipherSuite** directive the **!AECDH** cipher string.

**Table 4.4.1 mod\_ssl(Apache 2.3.5 Alpha + OpenSSL 1.0.0, both source builds) SSLCipherSuite General Aliases**

| **No.** | **mod\_ssl Category Alias** | **Meaning** |
| --- | --- | --- |
| 1 | SSLv2 | only SSL 2.0 cipher suites |
| 2 | SSLv3 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 3 | TLSv1 | all the SSL 3.0 or TLS 1.0 cipher suites(including eNULL and aNULL) |
| 4 | AES | cipher suites using AES |
| 5 | AES128 | cipher suites using AES 128-bit |
| 6 | AES256 | cipher suites using AES 256-bit |
| 7 | CAMELLIA | cipher suites using Camellia |
| 8 | CAMELLIA128 | cipher suites using Camellia 128-bit |
| 9 | CAMELLIA256 | cipher suites using Camellia 256-bit |
| 10 | DES | cipher suites using DES |
| 11 | 3DES | cipher suites using 3DES |
| 12 | IDEA | cipher suites using IDEA |
| 13 | RC2 | cipher suites using RC2 |
| 14 | RC4 | cipher suites using RC4 |
| 15 | SEED | cipher suites using SEED |
| 16 | MD5 | cipher suites using MD5 |
| 17 | SHA1, SHA | cipher suites using SHA1 |
| 18 | SHA | cipher suites using SHA1 |
| 19 | ALL | all cipher suites except the eNULL ciphers |
| 20 | COMPLEMENTOFALL | the cipher suites not enabled by ALL, currently being eNULL |
| 21 | COMPLEMENTOFDEFAULT | the cipher suites not included in DEFAULT, currently being ADH and AECDH(aNULL). |
| 22 | DEFAULT | the default cipher suites list(determined at compile time, default this is: ALL:!aNULL:!eNULL) |
| 23 | HIGH | high encryption cipher suites(key lengths larger than 128-bits, + some cipher suites with 128-bit keys) |
| 24 | MEDIUM | medium encryption cipher suites, some of the ones using 128-bit encryption |
| 25 | LOW | low encryption cipher suites, the ones using 64-bit or 56-bit encryption algorithms(excluding export cipher suites) |
| 26 | EXP | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 27 | EXPORT | export encryption algorithms(including 40-bit and 56-bits algorithms) cipher suites |
| 28 | EXPORT40 | 40-bit export encryption algorithms cipher suites |
| 29 | EXPORT56 | 56-bit export encryption algorithms cipher suites |
| 30 | eNULL | cipher suites offering no encryption |
| 31 | NULL | cipher suites offering no encryption |
| 32 | aNULL | cipher suites offering no authentication. The anonymous DH and ECDH algorithms. |
| 33 | DSS | cipher suites using DSS authentication |
| 34 | aDSS | cipher suites using DSS authentication |
| 35 | RSA | cipher suites using RSA key exchange |
| 36 | aRSA | cipher suites using RSA authentication |
| 37 | kRSA | cipher suites using RSA key exchange |
| 38 | DH | cipher suites using DH, including anonymous DH |
| 39 | ADH | anonymous DH cipher suites |
| 40 | EDH | cipher suites using DH, excluding anonymous DH |
| 41 | kEDH | cipher suites using ephemeral DH key agreement |
| 42 | ECDH | ECDH cert or ephemeral ECDH |
| 43 | aECDH | ECDH cert |
| 44 | AECDH | anonymous ECDH |
| 45 | EECDH | non-anonymous ephemeral ECDH |
| 46 | kECDH | ECDH cert (signed with either RSA or ECDSA) |
| 47 | kECDHe | ECDH cert, signed with ECDSA |
| 48 | kECDHr | ECDH cert, signed with RSA |
| 49 | kEECDH | ephemeral ECDH |
| 50 | ECDSA | ECDSA cert |
| 51 | aECDSA | ECDSA cert |

**Table 4.4.2 mod\_ssl Apache 2.3.5 Alpha(source build) + OpenSSL 1.0.0(source build) Cipher Suites and Aliases usable with the SSLCipherSuite Directive**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **mod\_ssl Cipher Suite Alias** | **mod\_ssl category Alias** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | RC4-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | EXP-RC4-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40 | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | RC2-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|MEDIUM | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | EXP-RC2-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40 | enabled |
| 5 | SSL\_CK\_IDEA\_128\_CBC\_WITH\_MD5 | 0x050080 | SSL 2.0 | IDEA-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|IDEA|MD5|MEDIUM | enabled |
| 6 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | DES-CBC-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|DES|MD5|LOW | enabled |
| 7 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | DES-CBC3-MD5 | SSLv2|ALL|RSA|aRSA|kRSA|3DES|MD5|HIGH | enabled |
| 8 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | NULL-MD5 | SSLv3|TLSv1|RSA|aRSA|kRSA|MD5|eNULL|NULL|COMPLEMENTOFALL | disabled |
| 9 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | NULL-SHA | SSLv3|TLSv1|RSA|aRSA|kRSA|SHA1|eNULL|NULL|COMPLEMENTOFALL | disabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | EXP-RC4-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | RC4-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|MD5|MEDIUM|DEFAULT | enabled |
| 12 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | RC4-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 13 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | EXP-RC2-CBC-MD5 | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC2|MD5|EXP|EXPORT40|DEFAULT | enabled |
| 14 | TLS\_RSA\_WITH\_IDEA\_CBC\_SHA | 0x0007 | SSL 3.0|TLS 1.0 | IDEA-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|IDEA|SHA1|SHA|MEDIUMDEFAULT | enabled |
| 15 | TLS\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0008 | SSL 3.0|TLS 1.0 | EXP-DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT40 |DEFAULT | enabled |
| 16 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 17 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | DES-CBC3-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 18 | TLS\_DHE\_DSS\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0011 | SSL 3.0|TLS 1.0 | EXP-EDH-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 19 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 20 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | EDH-DSS-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 21 | TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0014 | SSL 3.0|TLS 1.0 | EXP-EDH-RSA-DES-CBC-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|DES|SHA1|SHA|EXP|EXPORT40|DEFAULT | enabled |
| 22 | TLS\_DHE\_RSA\_WITH\_DES\_CBC\_SHA | 0x0015 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|DES|SHA1|SHA|LOW|DEFAULT | enabled |
| 23 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0 | EDH-RSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 24 | TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0017 | SSL 3.0|TLS 1.0 | EXP-ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|EXP|EXPORT40|COMPLEMENTOFDEFAULT | disabled |
| 25 | TLS\_DH\_anon\_WITH\_RC4\_128\_MD5 | 0x0018 | SSL 3.0|TLS 1.0 | ADH-RC4-MD5 | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|RC4|MD5|MEDIUM|COMPLEMENTOFDEFAULT | disabled |
| 26 | TLS\_DH\_anon\_EXPORT\_WITH\_DES40\_CBC\_SHA | 0x0019 | SSL 3.0|TLS 1.0 | EXP-ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|EXP|EXPORT40|COMPLEMENTOFDEFAULT | disabled |
| 27 | TLS\_DH\_anon\_WITH\_DES\_CBC\_SHA | 0x001A | SSL 3.0|TLS 1.0 | ADH-DES-CBC-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|DES|SHA1|SHA|LOW|COMPLEMENTOFDEFAULT | disabled |
| 28 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0 | ADH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 29 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0 | AES128-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|AES128 |SHA1|SHA|HIGH|DEFAULT | enabled |
| 30 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0 | DHE-DSS-AES128-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 31 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0 | DHE-RSA-AES128-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|AES|AES128|SHA1|HIGH|DEFAULT | enabled |
| 32 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0x0034 | SSL 3.0|TLS 1.0 | ADH-AES128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|AES128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 33 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0 | AES256-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 34 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0 | DHE-DSS-AES256-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 35 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0 | DHE-RSA-AES256-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 36 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0x003A | SSL 3.0|TLS 1.0 | ADH-AES256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|AES|AES256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 37 | TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0041 | SSL 3.0|TLS 1.0 | CAMELLIA128-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 38 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0044 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 39 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0045 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 40 | TLS\_DH\_anon\_WITH\_CAMELLIA\_128\_CBC\_SHA | 0x0046 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA128-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|CAMELLIA128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 41 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | EXP1024-DES-CBC-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 42 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-DES-CBC-SHA | SSLv3|TLSv1|ALL|DSS|kEDH|DH|DES|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 43 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | EXP1024-RC4-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 44 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0065 | SSL 3.0|TLS 1.0 | EXP1024-DHE-DSS-RC4-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|RC4|SHA1|SHA|EXP|EXPORT56|DEFAULT | disabled |
| 45 | TLS\_DHE\_DSS\_WITH\_RC4\_128\_SHA | 0x0066 | SSL 3.0|TLS 1.0 | DHE-DSS-RC4-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | disabled |
| 46 | TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0084 | SSL 3.0|TLS 1.0 | CAMELLIA256-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 47 | TLS\_DHE\_DSS\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0087 | SSL 3.0|TLS 1.0 | DHE-DSS-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 48 | TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0088 | SSL 3.0|TLS 1.0 | DHE-RSA-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 49 | TLS\_DH\_anon\_WITH\_CAMELLIA\_256\_CBC\_SHA | 0x0089 | SSL 3.0|TLS 1.0 | ADH-CAMELLIA256-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|CAMELLIA|CAMELLIA256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | disabled |
| 50 | TLS\_RSA\_WITH\_SEED\_CBC\_SHA | 0x0096 | SSL 3.0|TLS 1.0 | SEED-SHA | SSLv3|TLSv1|ALL|RSA|aRSA|kRSA|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 51 | TLS\_DHE\_DSS\_WITH\_SEED\_CBC\_SHA | 0x0099 | SSL 3.0|TLS 1.0 | DHE-DSS-SEED-SHA | SSLv3|TLSv1|ALL|DSS|aDSS|kEDH|DH|EDH|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 52 | TLS\_DHE\_RSA\_WITH\_SEED\_CBC\_SHA | 0x009A | SSL 3.0|TLS 1.0 | DHE-RSA-SEED-SHA | SSLv3|TLSv1|ALL|aRSA|kEDH|DH|EDH|SEED|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 53 | TLS\_DH\_anon\_WITH\_SEED\_CBC\_SHA | 0x009B | SSL 3.0|TLS 1.0 | ADH-SEED-SHA | SSLv3|TLSv1|ALL|DH|kEDH|aDH|aNULL|SEED|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | disabled |
| 54 | TLS\_ECDH\_ECDSA\_WITH\_NULL\_SHA | 0xC001 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-NULL-SHA | SSLv3|TLSv1|aECDH|ECDH|kECDH|kECDHe|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 55 | TLS\_ECDH\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC002 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-RC4-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 56 | TLS\_ECDH\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC003 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 57 | TLS\_ECDH\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC004 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES128-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 58 | TLS\_ECDH\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC005 | SSL 3.0|TLS 1.0 | ECDH-ECDSA-AES256-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHe|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 59 | TLS\_ECDHE\_ECDSA\_WITH\_NULL\_SHA | 0xC006 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-NULL-SHA | SSLv3|TLSv1|aECDSA|ECDSA|ECDH|EECDH|kEECDH|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 60 | TLS\_ECDHE\_ECDSA\_WITH\_RC4\_128\_SHA | 0xC007 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-RC4-SHA | SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 61 | TLS\_ECDHE\_ECDSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC008 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 62 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES128-SHA | SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 63 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | SSL 3.0|TLS 1.0 | ECDHE-ECDSA-AES256-SHA | SSLv3|TLSv1|ALL|aECDSA|ECDSA|ECDH|EECDH|kEECDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 64 | TLS\_ECDH\_RSA\_WITH\_NULL\_SHA | 0xC00B | SSL 3.0|TLS 1.0 | ECDH-RSA-NULL-SHA | SSLv3|TLSv1|aECDH|ECDH|kECDH|kECDHr|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 65 | TLS\_ECDH\_RSA\_WITH\_RC4\_128\_SHA | 0xC00C | SSL 3.0|TLS 1.0 | ECDH-RSA-RC4-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|KECDHr|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 66 | TLS\_ECDH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC00D | SSL 3.0|TLS 1.0 | ECDH-RSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 67 | TLS\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC00E | SSL 3.0|TLS 1.0 | ECDH-RSA-AES128-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 68 | TLS\_ECDH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00F | SSL 3.0|TLS 1.0 | ECDH-RSA-AES256-SHA | SSLv3|TLSv1|ALL|aECDH|ECDH|kECDH|kECDHr|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 69 | TLS\_ECDHE\_RSA\_WITH\_NULL\_SHA | 0xC010 | SSL 3.0|TLS 1.0 | ECDHE-RSA-NULL-SHA | SSLv3|TLSv1|aRSA|ECDH|EECDH|kEECDH|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 70 | TLS\_ECDHE\_RSA\_WITH\_RC4\_128\_SHA | 0xC011 | SSL 3.0|TLS 1.0 | ECDHE-RSA-RC4-SHA | SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|RC4|SHA1|SHA|MEDIUM|DEFAULT | enabled |
| 71 | TLS\_ECDHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC012 | SSL 3.0|TLS 1.0 | ECDHE-RSA-DES-CBC3-SHA | SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|3DES|SHA1|SHA|HIGH|DEFAULT | enabled |
| 72 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES128-SHA | SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|AES|AES128|SHA1|SHA|HIGH|DEFAULT | enabled |
| 73 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | SSL 3.0|TLS 1.0 | ECDHE-RSA-AES256-SHA | SSLv3|TLSv1|ALL|aRSA|ECDH|EECDH|kEECDH|AES|AES256|SHA1|SHA|HIGH|DEFAULT | enabled |
| 74 | TLS\_ECDH\_anon\_WITH\_NULL\_SHA | 0xC015 | SSL 3.0|TLS 1.0 | AECDH-NULL-SHA | SSLv3|TLSv1|AECDH|ECDH|kEECDH|aNULL|eNULL|NULL|SHA1|SHA|COMPLEMENTOFALL | disabled |
| 75 | TLS\_ECDH\_anon\_WITH\_RC4\_128\_SHA | 0xC016 | SSL 3.0|TLS 1.0 | AECDH-RC4-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|RC4|SHA1|SHA|MEDIUM|COMPLEMENTOFDEFAULT | enabled |
| 76 | TLS\_ECDH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0xC017 | SSL 3.0|TLS 1.0 | AECDH-DES-CBC3-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|3DES|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 77 | TLS\_ECDH\_anon\_WITH\_AES\_128\_CBC\_SHA | 0xC018 | SSL 3.0|TLS 1.0 | AECDH-AES128-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|AES|AES128|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |
| 78 | TLS\_ECDH\_anon\_WITH\_AES\_256\_CBC\_SHA | 0xC019 | SSL 3.0|TLS 1.0 | AECDH-AES256-SHA | SSLv3|TLSv1|ALL|AECDH|ECDH|kEECDH|aNULL|AES|AES256|SHA1|SHA|HIGH|COMPLEMENTOFDEFAULT | enabled |

## 5. Opera

Test

5.1 Opera 11.0x  
Opera 11.01 was tested.

SSL 2.0 is not supported.  
SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 are supported and enabled by default.

Opera is a little bit tricky to fingerprint.

The RSA-SHA256 based cipher suites were successfully tested also under TLS 1.0 and TLS 1.1 against https://www.mikestoolbox.net/.  
Note that Opera adds SHA256-based cipher suites to a SSL 3.0 Client Hello, which is not “normal” behavior. Not sure what happens if the server actually replies with such a cipher suite under SSL 3.0.

Could not successfully establish a TLS session with the ADH-based cipher suites, either with GnuTLS(2.10 version) or with OpenSSL 1.0.0c.

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | disabled |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 4 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 5 | TLS\_DH\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000D | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 6 | TLS\_DH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0010 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 7 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 8 | TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0016 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 9 | TLS\_DH\_anon\_WITH\_3DES\_EDE\_CBC\_SHA | 0x001B | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 ? | disabled |
| 10 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 11 | TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0030 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 12 | TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0031 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 14 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x0033 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 15 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 16 | TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0036 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 17 | TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0037 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 18 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 19 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0039 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 20 | TLS\_RSA\_WITH\_NULL\_SHA256 | 0x003B | TLS 1.0|TLS 1.1|TLS 1.2 ? | disabled |
| 21 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003C | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 22 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x003D | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 23 | TLS\_DH\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x003E | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 24 | TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003F | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 25 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x0040 | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 26 | TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x0067 | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 27 | TLS\_DH\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x0068 | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 28 | TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x0069 | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 29 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x006A | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 30 | TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x006B | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 31 | TLS\_DH\_anon\_WITH\_AES\_128\_CBC\_SHA256 | 0x006C | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 ? | disabled |
| 32 | TLS\_DH\_anon\_WITH\_AES\_256\_CBC\_SHA256 | 0x006D | (SSL 3.0)|TLS 1.0|TLS 1.1|TLS 1.2 ? | disabled |

## 6. Schannel

Test

### **6.1. Schannel(NT 5.1.2600) Cipher Suites**

**Table 6.1** lists the cipher suites currently supported by Schannel(NT 5.1.2600). For more details about each cipher suite refer to the main tables.

Schannel(NT 5.1.2600) supports SSL 2.0, SSL 3.0 and TLS 1.0.

Schannell(NT 5.1.2600) is used by IIS 6.0(Windows Server 2003 R2 SP2 tested), IE6/IE7/IE8(Windows XP SP3 and x64 SP2 tested). Additionally the Safari browser makes use of the Schannel.  
Latest versions of Chrome(9.0.x as writing) moved away from Schannel and use NSS instead.

Windows Server 2003(R2 SP2 tested) and Windows XP x64(SP2 tested) support two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1**).

**Table 6.1**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** |
| --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 |
| 7 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 |
| 8 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 |
| 9 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 |
| 10 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 |
| 11 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 |
| 12 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 |
| 13 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 |
| 14 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 |
| 15 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 |
| 16 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 |
| 17 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 |
| 18 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 |
| 19 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 |
| 20 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 |
| 21 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 |

### **6.1.1. IE6 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites**

**Table 6.1.1** lists the cipher suites currently supported by IE6(NT 5.1.2600).

Note that TLS 1.0 is disabled by default within IE6(that’s why TLS 1.0 is marked with red within table **Table 6.1.1**).

Windows XP x64(SP2 tested) supports two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1.1**).

**Table 6.1.1**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | enabled |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | enabled |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 15 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 \* | disabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 \* | disabled |
| 17 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | enabled |
| 18 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | enabled |

\* Windows XP x64 SP2 cipher suites only

### **6.1.2. IE7 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites**

**Table 6.1.2** lists the cipher suites currently supported by IE7(NT 5.1.2600).

Note that SSL 2.0 is disabled by default within IE7.

Windows XP x64(SP2 tested) supports two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1.2**).

**Table 6.1.2**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | disabled |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 15 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 \* | disabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 \* | disabled |
| 17 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | enabled |
| 18 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | enabled |

\* Windows XP x64 SP2 cipher suites only

### **6.1.3. IE8 (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites**

**Table 6.1.3** lists the cipher suites currently supported by IE8(NT 5.1.2600).

Note that SSL 2.0 is disabled by default within IE8.

Windows XP x64(SP2 tested) supports two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1.2**).

**Table 6.1.3**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | disabled |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 15 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 \* | disabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 \* | disabled |
| 17 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | enabled |
| 18 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | enabled |

\* Windows XP x64 SP2 cipher suites only

### **6.1.4. IIS 6.0 (Windows Server 2003 R2 SP2)**

**Table 6.1.4** lists the cipher suites currently supported by IIS6.0(NT 5.1.2600).

Windows Server 2003(R2 SP2 tested) supports two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1.4**).

**Table 6.1.4**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | enabled |
| 3 | SSL\_CK\_RC2\_128\_CBC\_WITH\_MD5 | 0x030080 | SSL 2.0 | enabled |
| 4 | SSL\_CK\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5 | 0x040080 | SSL 2.0 | enabled |
| 5 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | enabled |
| 6 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | enabled |
| 11 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | enabled \*\* |
| 14 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled \*\* |
| 15 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 \* | disabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 \* | disabled |
| 17 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | enabled |
| 18 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | enabled |
| 19 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | enabled |

\* Windows XP x64 SP2 cipher suites only  
\*\* Attempt to use it resulted in a “Record Overflow” TLS alert.

6.1.5. Safari 5.0.x (Windows XP SP3 / Windows XP x64 SP2) Cipher Suites

**Table 6.1.5** lists the cipher suites currently supported by Safari 5.0.3(NT 5.1.2600).

Note that Safari 5.0.x does not seem to support SSL 2.0.

Windows XP x64(SP2 tested) supports two AES-based cipher suites with the help of a KB patch(these two are usable under TLS 1.0 and are marked with red within **Table 6.1.5**).

**Table 6.1.5**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | enabled |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 4 | TLS\_RSA\_EXPORT\_WITH\_RC2\_CBC\_40\_MD5 | 0x0006 | SSL 3.0|TLS 1.0 | enabled |
| 5 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 \* | disabled |
| 10 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 \* | disabled |
| 11 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | enabled |
| 12 | SSL\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | enabled |
| 13 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | enabled |

\* Windows XP x64 SP2 cipher suites only

### **6.2. Schannel(NT 6.0.6002) Cipher Suites**

**Table 6.2** lists the cipher suites currently supported by Schannel(NT 6.0.6002). For more details about each cipher suite refer to the main tables.

Schannel(NT 6.0.6002) supports SSL 2.0, SSL 3.0 and TLS 1.0.

Compared with Schannel(NT 5.1.2600), Schannel(NT 6.0.6002) adds native support for some AES based cipher suites, and some ECC based cipher suites.

Schannel(NT 6.0.6002) supports the three “popular” elliptic curves(which should assure interoperability):  
 - secp256r1(aka NIST P-256)  
 - secp384r1(aka NIST P-384)  
 - secp521r1(aka NIST P-521)

Schannel(NT 6.0.6002) is used by IIS 7.0(Windows Server 2008 SP2 tested), IE7/IE8(Windows Vista SP2 tested). Additionally the Safari browser makes use of the Schannel.  
Latest versions of Chrome(9.0.x as writing) moved away from Schannel and use NSS instead.

**Table 6.2**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 5 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 13 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 17 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 20 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 21 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 22 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 23 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 24 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

The following cipher suites(all supported cipher suites) are listed under:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protocol Provider\KM\00010002\Functions  
and  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protocol Provider\UM\00010002\Functions

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\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA  
TLS\_RSA\_WITH\_RC4\_128\_MD5  
SSL\_CK\_RC4\_128\_WITH\_MD5  
SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
TLS\_RSA\_WITH\_NULL\_MD5  
TLS\_RSA\_WITH\_NULL\_SHA  
TLS\_RSA\_WITH\_DES\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA  
TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA  
TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA  
TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA  
TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5  
SSL\_CK\_DES\_64\_CBC\_WITH\_MD5  
SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5

The following cipher suites(all enabled cipher suites) are listed under:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions

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\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA  
TLS\_RSA\_WITH\_RC4\_128\_MD5  
SSL\_CK\_RC4\_128\_WITH\_MD5  
SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
TLS\_RSA\_WITH\_NULL\_MD5  
TLS\_RSA\_WITH\_NULL\_SHA

### **6.2.1. IE7 (Windows Vista SP2) Cipher Suites**

**Table 6.2.1** lists the cipher suites currently supported by IE7(NT 6.0.6002).

Note that SSL 2.0 is disabled by default within IE7.

**Table 6.2.1**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 5 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 6 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 9 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 16 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 17 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 20 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 21 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 22 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

### **6.2.2. IE8 (Windows Vista SP2) Cipher Suites**

**Table 6.2.2** lists the cipher suites currently supported by IE8(NT 6.0.6002).

Note that SSL 2.0 is disabled by default within IE8.

**Table 6.2.2**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 5 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 6 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 9 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 16 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 17 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 20 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 21 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 22 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

### **6.2.3. IIS 7.0 (Windows Server 2008 SP2) Cipher Suites**

Test **Table 6.2.3** lists the cipher suites currently supported by IIS 7.0(NT 6.0.6002).

**Table 6.2.3**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 5 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 6 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 7 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 9 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 16 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 17 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 20 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 21 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 22 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

### **6.2.4. Safari 5.0.x (Windows Vista SP2) Cipher Suites**

**Table 6.2.4** lists the cipher suites currently supported by Safari 5.0.3(NT 6.0.6002).

Note that Safari 5.0.x does not seem to support SSL 2.0.

**Table 6.2.4**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 4 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 5 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 7 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 9 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 10 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 11 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 12 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 13 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 14 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 15 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 16 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 17 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 18 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

### **6.3. Schannel (NT 6.1.7600) Cipher Suites**

**Table 6.3** lists the cipher suites currently supported by Schannel(NT 6.1.7600); (protocol TLS 1.1 and TLS 1.2 may be disabled by default, they are at least for the server side). For more details about each cipher suite refer to the main tables.

Schannel(NT 6.1.7600) supports SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2.

Compared with Schannel(NT 6.0.6002), Schannel(NT 6.1.7600) adds support for TLS 1.1, TLS 1.2, and some SHA256 based cipher suites.

Schannel(NT 6.1.7600) supports the three “popular” elliptic curves(which should assure interoperability):  
 - secp256r1(aka NIST P-256)  
 - secp384r1(aka NIST P-384)  
 - secp521r1(aka NIST P-521); this one is disabled by default

Schannel(NT 6.1.7600) supports the signature algorithms(used within the TLS 1.2 signature\_algorithms extension):  
- RSA/SHA256  
- RSA/SHA384  
- RSA/SHA512; disabled by default  
- RSA/SHA1  
- ECDSA/SHA256  
- ECDSA/SHA384  
- ECDSA/SHA512; disabled by default  
- ECDSA/SHA1  
- DSA/SHA1

Schannel(NT 6.1.7600) is used by IIS 7.5(Windows Server 2008 R2 tested), IE8(Windows 7 tested). Additionally the Safari browser makes use of the Schannel.  
Latest versions of Chrome(9.0.x as writing) moved away from Schannel and use NSS instead.

**Table 6.3**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 5 | TLS\_RSA\_WITH\_NULL\_MD5 | 0x0001 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | disabled |
| 6 | TLS\_RSA\_WITH\_NULL\_SHA | 0x0002 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 7 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 8 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 9 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 10 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 12 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 13 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 16 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 17 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 20 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 21 | TLS\_RSA\_WITH\_NULL\_SHA256 | 0x003B | TLS 1.2 | enabled |
| 22 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003C | TLS 1.2 | enabled |
| 23 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x003D | TLS 1.2 | enabled |
| 24 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x0040 | TLS 1.2 | enabled |
| 25 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x006A | TLS 1.2 | enabled |
| 26 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 28 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 29 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 30 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC023 | TLS 1.2 | enabled |
| 31 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC024 | TLS 1.2 | enabled |
| 32 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC027 | TLS 1.2 | enabled |
| 33 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC028 | TLS 1.2 | disabled |
| 34 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02B | TLS 1.2 | enabled |
| 35 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC02C | TLS 1.2 | enabled |

The following cipher suites(all supported cipher suites) are listed under:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protocol Provider\KM\00010002\Functions  
and  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protocol Provider\UM\00010002\Functions

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\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P521  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA  
TLS\_RSA\_WITH\_RC4\_128\_MD5  
SSL\_CK\_RC4\_128\_WITH\_MD5  
SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
TLS\_RSA\_WITH\_NULL\_SHA  
TLS\_RSA\_WITH\_NULL\_MD5  
TLS\_RSA\_WITH\_DES\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA  
TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA  
TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA  
TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA  
TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5  
SSL\_CK\_DES\_64\_CBC\_WITH\_MD5  
SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P521  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P521  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384\_P521  
TLS\_RSA\_WITH\_NULL\_SHA256

The following cipher suites(all enabled cipher suites) are listed under:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002\Functions

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_RSA\_WITH\_RC4\_128\_SHA  
TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA\_P384  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P256  
TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA\_P384  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256  
TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA  
TLS\_RSA\_WITH\_RC4\_128\_MD5  
SSL\_CK\_RC4\_128\_WITH\_MD5  
SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
TLS\_RSA\_WITH\_NULL\_SHA256  
TLS\_RSA\_WITH\_NULL\_SHA

The following signatures algorithms(used within the TLS 1.2 signature\_algorithms extension, all enabled by default) are listed under:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010003\Functions

RSA/SHA256  
RSA/SHA384  
RSA/SHA1  
ECDSA/SHA256  
ECDSA/SHA384  
ECDSA/SHA1  
DSA/SHA1

### **6.3.1. IE8 (Windows 7) Cipher Suites**

**Table 6.3.1** lists the cipher suites currently supported by IE8(NT 6.1.7600).

Protocols TLS 1.1 and TLS 1.2 are disabled by default in IE8(but you can enable them from the UI).  
SSL 2.0 is also disabled by default within IE8.

**Table 6.3.1**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | disabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | disabled |
| 5 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 6 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 7 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 8 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 9 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 16 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003C | TLS 1.2 | disabled |
| 17 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x003D | TLS 1.2 | disabled |
| 18 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x0040 | TLS 1.2 | disabled |
| 19 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x006A | TLS 1.2 | disabled |
| 20 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 21 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 22 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 23 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 24 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 25 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 26 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC023 | TLS 1.2 | disabled |
| 28 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC024 | TLS 1.2 | disabled |
| 29 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC027 | TLS 1.2 | disabled |
| 30 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC028 | TLS 1.2 | disabled |
| 31 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02B | TLS 1.2 | disabled |
| 32 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC02C | TLS 1.2 | disabled |

### **6.3.2. IIS 7.5 (Windows Server 2008 R2) Cipher Suites**

Test **Table 6.3.2** lists the cipher suites currently supported by IIS 7.5(NT 6.1.7600).

Protocols TLS 1.1 and TLS 1.2 for server side are disabled by default for IIS 7.5(but you can enable them from the registry).

**Table 6.3.2**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | SSL\_CK\_RC4\_128\_WITH\_MD5 | 0x010080 | SSL 2.0 | enabled |
| 2 | SSL\_CK\_RC4\_128\_EXPORT40\_WITH\_MD5 | 0x020080 | SSL 2.0 | disabled |
| 3 | SSL\_CK\_DES\_64\_CBC\_WITH\_MD5 | 0x060040 | SSL 2.0 | disabled |
| 4 | SSL\_CK\_DES\_192\_EDE3\_CBC\_WITH\_MD5 | 0x0700C0 | SSL 2.0 | enabled |
| 5 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 6 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 7 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 8 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 9 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 10 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 11 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 12 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 13 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 14 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 15 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 16 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 17 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 18 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 19 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0x003C | TLS 1.2 | disabled |
| 20 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 | 0x003D | TLS 1.2 | disabled |
| 21 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256 | 0x0040 | TLS 1.2 | disabled |
| 22 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256 | 0x006A | TLS 1.2 | disabled |
| 23 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 24 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 25 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 26 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0|TLS 1.1|TLS 1.2 | enabled |
| 27 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC023 | TLS 1.2 | disabled |
| 28 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC024 | TLS 1.2 | disabled |
| 29 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 | 0xC027 | TLS 1.2 | disabled |
| 30 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | 0xC028 | TLS 1.2 | disabled |
| 31 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | 0xC02B | TLS 1.2 | disabled |
| 32 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | 0xC02C | TLS 1.2 | disabled |

### **6.3.3. Safari 5.0.x (Windows 7) Cipher Suites**

**Table 6.3.3** lists the cipher suites currently supported by Safari 5.0.3(NT 6.1.7600).

Protocols SSL 2.0, TLS 1.1 and TLS 1.2 are not supported by Safari 5.0.x.

**Table 6.3.3**

| **No.** | **Cipher Suite** | **Hex Value** | **SSL/TLS Version** | **Status** |
| --- | --- | --- | --- | --- |
| 1 | TLS\_RSA\_EXPORT\_WITH\_RC4\_40\_MD5 | 0x0003 | SSL 3.0|TLS 1.0 | disabled |
| 2 | TLS\_RSA\_WITH\_RC4\_128\_MD5 | 0x0004 | SSL 3.0|TLS 1.0 | enabled |
| 3 | TLS\_RSA\_WITH\_RC4\_128\_SHA | 0x0005 | SSL 3.0|TLS 1.0 | enabled |
| 4 | TLS\_RSA\_WITH\_DES\_CBC\_SHA | 0x0009 | SSL 3.0|TLS 1.0 | disabled |
| 5 | TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA | 0x000A | SSL 3.0|TLS 1.0 | enabled |
| 6 | TLS\_DHE\_DSS\_WITH\_DES\_CBC\_SHA | 0x0012 | SSL 3.0|TLS 1.0 | disabled |
| 7 | TLS\_DHE\_DSS\_WITH\_3DES\_EDE\_CBC\_SHA | 0x0013 | SSL 3.0|TLS 1.0 | enabled |
| 8 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0x002F | TLS 1.0 | enabled |
| 9 | TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA | 0x0032 | TLS 1.0 | enabled |
| 10 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0x0035 | TLS 1.0 | enabled |
| 11 | TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA | 0x0038 | TLS 1.0 | enabled |
| 12 | TLS\_RSA\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0062 | SSL 3.0|TLS 1.0 | disabled |
| 13 | TLS\_DHE\_DSS\_EXPORT1024\_WITH\_DES\_CBC\_SHA | 0x0063 | SSL 3.0|TLS 1.0 | disabled |
| 14 | TLS\_RSA\_EXPORT1024\_WITH\_RC4\_56\_SHA | 0x0064 | SSL 3.0|TLS 1.0 | disabled |
| 15 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA | 0xC009 | TLS 1.0 | enabled |
| 16 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA | 0xC00A | TLS 1.0 | enabled |
| 17 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | 0xC013 | TLS 1.0 | enabled |
| 18 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA | 0xC014 | TLS 1.0 | enabled |

## 7. SSL Labs

Test

## 8. Wireshark

Test