

瀏覽器更新後發生問題調整設定說明

如果瀏覽器更新到最新的版本後就可能發生問題，這可能就要檢查你主機上的協定是否有不安全的設定，需要做關閉才能正常瀏覽。

只要更新到最新版本就會出現問題，如下圖

Chrome 的版本 84.0.4147.89 最新版本



你的連線可能有安全漏洞

這個網站的安全性設定過舊，因此你傳送給這個網站的的資訊 (例如密碼、訊息或信用卡資訊) 可能會外洩。

NET::ERR_SSL_OBSOLETE_VERSION

隱藏詳細資料

返回安全性瀏覽

用來載入這個網站的連線使用傳輸層安全標準 (TLS) 1.0 或 1.1，現已不適用，並將在日後遭到停用。一旦停用，使用者將無法載入這個網站。伺服器應啟用傳輸層安全標準 (TLS) 1.2 以上版本。

繼續前往 _____ (不安全)

Firefox 的版本 78.0.2 最新版本



安全連線失敗

連線到 _____ 時發生錯誤。對方使用不支援的安全通訊協定版本。

錯誤碼: SSL_ERROR_UNSUPPORTED_VERSION

- 因為無法驗證已接收資料的真實性，無法顯示您嘗試檢視的頁面。
- 請向網站擁有者回報此問題。

更多資訊...

此網站可能不支援 Firefox 最低支援的 TLS 1.2 版通訊協定。開啟 TLS 1.0 或 TLS 1.1 可能可以進行連線。

將於未來的版本中永久結束支援 TLS 1.0 及 TLS 1.1。

開啟 TLS 1.0 與 1.1



用 sslabs 來查看你主機上的協定設定

<https://www.ssllabs.com/ssltest/analyze.html?d=>

1. 目前 Protocols 設定要將 tls 1.0 以下的版本關閉
2. 只要出現 INSECURE 協定都要關閉

The screenshot shows the 'Protocols' section with the following settings:

Protocol	Status
TLS 1.3	No
TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3 INSECURE	Yes
SSL 2	No

The 'Cipher Suites' section shows the following settings:

Cipher Suite	Strength
# TLS 1.0 (server has no preference)	-
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	WEAK 112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	WEAK 112
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	WEAK 128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	WEAK 128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	WEAK 128
TLS_RSA_WITH_RC4_128_SHA (0x5)	INSECURE 128
TLS_RSA_WITH_IDEA_CBC_SHA (0x7)	WEAK 128

調整主機上的協定說明

範例說明(1) IIS

工具載點

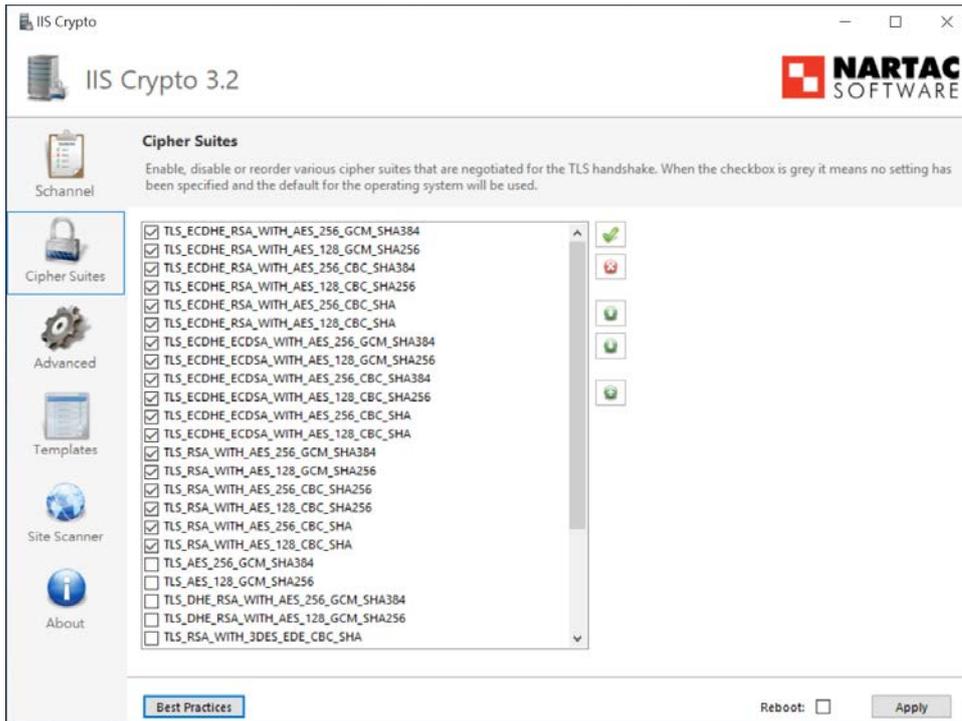
<https://www.nartac.com/Products/IISCrypto/>

The screenshot shows the IIS Crypto 3.2 software interface. The 'Schannel' tab is selected, showing the following settings:

- Server Protocols:**
 - Multi-Protocol Unified Hello
 - PCT 1.0
 - SSL 2.0
 - SSL 3.0
 - TLS 1.0
 - TLS 1.1
 - TLS 1.2
- Client Protocols:**
 - Multi-Protocol Unified Hello
 - PCT 1.0
 - SSL 2.0
 - SSL 3.0
 - TLS 1.0
 - TLS 1.1
 - TLS 1.2
- Ciphers:**
 - NULL
 - DES 56/56
 - RC2 40/128
 - RC2 56/128
 - RC2 128/128
 - RC4 40/128
 - RC4 56/128
 - RC4 64/128
 - RC4 128/128
 - Triple DES 168
 - AES 128/128
 - AES 256/256
- Hashes:**
 - MD5
 - SHA
 - SHA 256
 - SHA 384
 - SHA 512
- Key Exchanges:**
 - Diffie-Hellman
 - PKCS
 - ECDH

At the bottom, there is a 'Best Practices' button and a 'Reboot: Apply' button.

點選左小角的 Best Practices (最佳模式設定)



點選 Cipher Suites 將剛剛在 sslabs 偵測出的不安全的協定移除
 “確認設定完成後點選 Apply 在將主機重新啓動後才會生效”

之後在用 sslabs 覆查看還有沒有不安全的協定 (**INSECURE**)

範例說明(2) 其它常用主機

<https://ssl-config.mozilla.org/>

moz://a SSL Configuration Generator

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Go
- HAProxy
- Jetty
- lighttpd
- MySQL
- nginx
- Oracle HTTP
- Postfix
- PostgreSQL
- ProFTPD
- Redis
- Tomcat
- Traefik

Mozilla Configuration

- Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version

OpenSSL Version

Miscellaneous

HTTP Strict Transport Security
This also redirects to HTTPS, if possible

OCSP Stapling

apache 2.4.41, intermediate config, OpenSSL 1.1.1d

Supports Firefox 27, Android 4.4.2, Chrome 31, Edge, IE 11 on Windows 7, Java 8u31, OpenSSL 1.0.1, Opera 20, and Safari 9

```
# generated 2020-07-21, Mozilla Guideline v5.4, Apache 2.4.41, OpenSSL 1.1.1d, intermediate configuration
# https://ssl-config.mozilla.org/#server=apache&version=2.4.41&config=intermediate&openssl=1.1.1d&guideline=5.4

# this configuration requires mod_ssl, mod_socache_shmcb, mod_rewrite, and mod_headers
<VirtualHost *:80>
    RewriteEngine On
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>

<VirtualHost *:443>
    SSLEngine on

    # curl https://ssl-config.mozilla.org/ffdhe2048.txt >> /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateFile /path/to/signed_cert_and_intermediate_certs_and_dhparams
    SSLCertificateKeyFile /path/to/private_key

    # enable HTTP/2, if available
    Protocols h2 http/1.1

    # HTTP Strict Transport Security (mod_headers is required) (63072000 seconds)
    Header always set Strict-Transport-Security "max-age=63072000"
</VirtualHost>

# intermediate configuration
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384
SSLHonorCipherOrder off
SSLSessionTickets off

SSLUseStapling On
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
```

Copy

“點選你主機的版本，之後下方紅框裡的協定，設定在你主機上後重啓主機”

之後在用 **ssllabs** 覆查看還有沒有不安全的協定 (**INSECURE**)