

# SSL憑證安裝與申請

---

臺灣大學計資中心

網路組

游子興

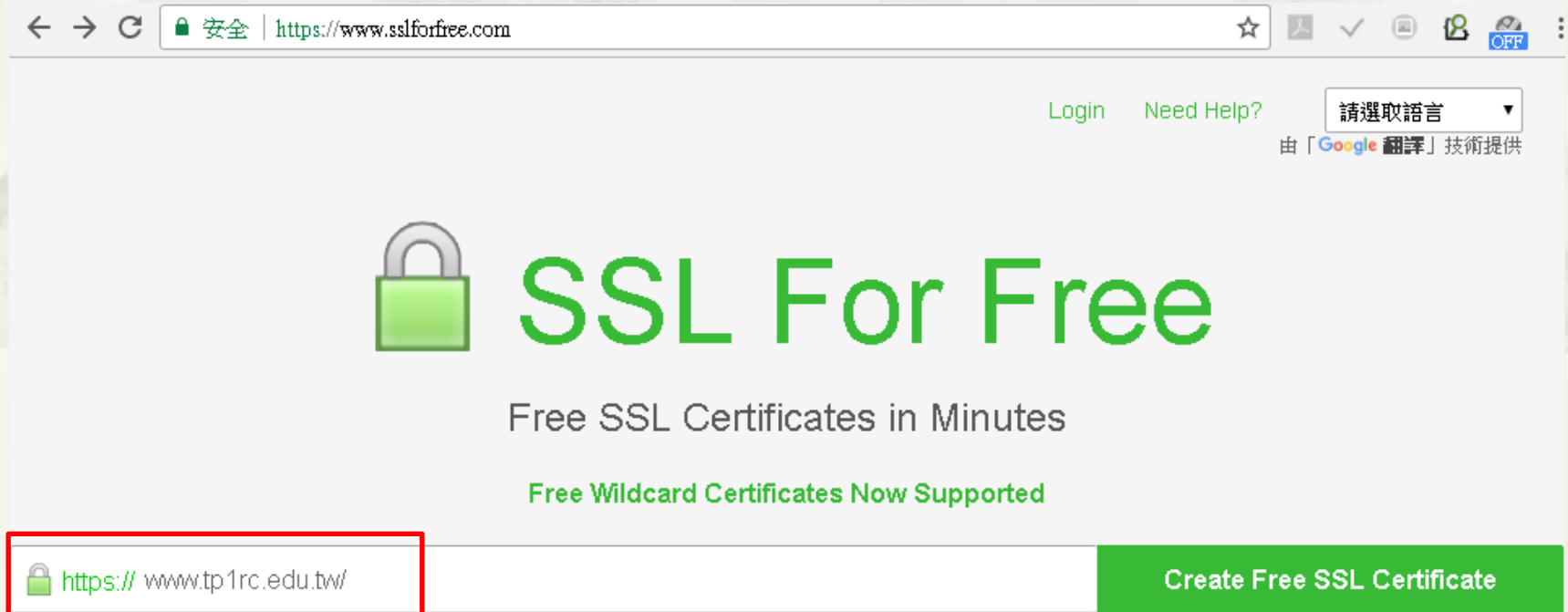


---

申請免費憑證  
**90 DAYS**

# 免費憑證申請(90 days)

- \* <https://www.sslforfree.com/>
- \* Let's Encrypt
  - \* a free, automated, and open Certificate Authority.



The screenshot shows a web browser window with the address bar displaying "安全 | https://www.sslforfree.com". The page content includes a green padlock icon, the text "SSL For Free" in large green font, and the subtitle "Free SSL Certificates in Minutes". Below this, it states "Free Wildcard Certificates Now Supported". In the top right corner, there are links for "Login" and "Need Help?", a language selection dropdown menu set to "請選取語言", and a note "由「Google 翻譯」技術提供". At the bottom, there is a red-bordered input field containing "https:// www.tp1rc.edu.tw/" and a green button labeled "Create Free SSL Certificate".

# 輸入 Domain Name

- \* <https://www.sslforfree.com/create?domains=www.tp1rc.edu.tw>

The screenshot shows a web browser window with the address bar containing the URL <https://www.sslforfree.com/create?domains=www.tp1rc.edu.tw>. The page title is "Free SSL Certificate Validation for 'www.tp1rc.edu.tw'". Below the title, there are links for "(Add / Edit Domains | Regenerate Account)". A paragraph of text explains the verification process, mentioning the "Lets Encrypt service agreement" and the need to whitelist IP 66.133.109.36. At the bottom, there are three green buttons for verification methods: "Automatic FTP Verification", "Manual Verification" (highlighted with a red border), and "Manual Verification (DNS)".

SSL FOR FREE Login Need Help? 請選取語言  
由 Google 翻

## Free SSL Certificate Validation for "www.tp1rc.edu.tw"

([Add / Edit Domains](#) | [Regenerate Account](#))

Verify that you own the domain through your web server or if your domain is not yet on a web server then verify it through the DNS. This prevents other people from getting an *SSL certificate* for your domain. By continuing you agree to the [Lets Encrypt service agreement](#). You may need to whitelist 66.133.109.36 if your website is behind a firewall. **If you receive a 504 Gateway timeout and cannot connect anymore then open another incognito/private browser or a different browser to connect again.** If you have your own CSR use manual verification and input it after generating domain verification files. If you use IIS on Windows you may have to do [additional steps](#).

**Automatic FTP Verification**

Enter FTP information to automatically verify the domain

**Manual Verification**

Upload verification files manually to your domain to verify ownership.

**Manual Verification (DNS)**

Use this if you cannot verify through a web server or cannot use port 80. You will be adding a TXT record to your DNS server.

# Manually Verification

## Manually Verify Domain (HTTP Server)

If you do not have your FTP information then follow the following steps to verify domain ownership manually. The server will need to be on port 80 if HTTP (or port 80 open and forwarding to 443 if HTTPS). If your web server is not listening on port 80 then you will need to temporarily listen on port 80 or forward port 80 to the port for the web server.

1. Get domain verification files by clicking the button below
2. Upload domain verification files to domain ([Need help?](#))
3. Download your **free ssl certificate**

[Retry Manual Verification](#)

## Upload Verification Files

1. Download the following verification files by clicking on each link below

1. [Download File #1](#)

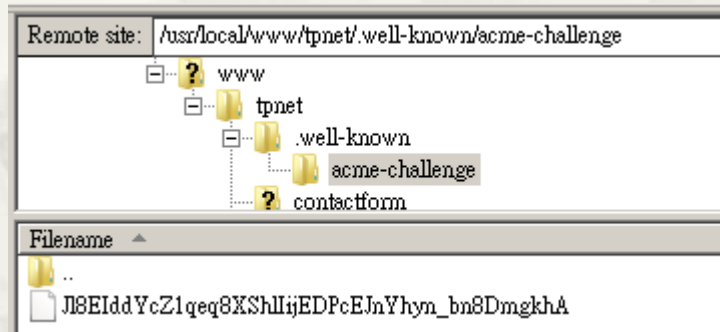
2. Create a folder in your domain named ".well-known" if it does not already exist. If you use Windows you may have to add a dot at the end of the folder name in order to create a folder with a dot at the beginning.
3. Create another folder in your domain under ".well-known" named "acme-challenge" if it does not already exist
4. Upload the downloaded files to the "acme-challenge" folder

5. Verify successful upload by visiting the following links in your browser

1. [http://www.tp1rc.edu.tw/.well-known/acme-challenge/Jl8ElddYcZ1qeq8XShllijEDPcEJnYhyn\\_bn8DmgkhA](http://www.tp1rc.edu.tw/.well-known/acme-challenge/Jl8ElddYcZ1qeq8XShllijEDPcEJnYhyn_bn8DmgkhA)

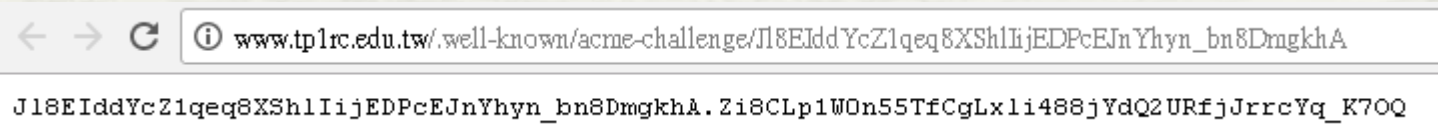
# 驗證 verification file

- \* Download verification file and Upload to web server



- \* Verify

- \* [http://www.tp1rc.edu.tw/.well-known/acme-challenge/J18E1ddYcZ1qeq8XShIijEDPcEJnYhyn\\_bn8DmgkhA](http://www.tp1rc.edu.tw/.well-known/acme-challenge/J18E1ddYcZ1qeq8XShIijEDPcEJnYhyn_bn8DmgkhA)



The background of the slide is a light beige color with a large, semi-circular fan shape in the center. The fan is filled with a traditional Chinese landscape painting, showing mountains, trees, and a small building. The painting is rendered in a soft, monochromatic style. A thin horizontal line is drawn across the middle of the fan, just above the main text.

# 產生憑證檔案-方法1

# 產生憑證檔案 (私鑰由 **sslforfree** 提供)

Download SSL Certificate

I Have My Own CSR

\* 輸入 email 憑證到期提醒

## Certificate Successfully Generated

You can download the files by clicking download below or copy and paste the following into the appropriate inputs to install. **SSL Certificates expire after 90 days** so be sure to re-generate your SSL Certificate before then otherwise your website might stop working. If you use IIS and need a PFX file then follow the instructions in the following link to convert the certificate and private key file into a .PFX file - <http://stackoverflow.com/a/17284371> (Install openssl and run `openssl pkcs12 -export -out "certificate_combined.pfx" -inkey "private.key" -in "certificate.crt" -certfile ca_bundle.crt` in a command prompt with path set to location of downloaded certificate files or use <https://www.digicert.com/util/>). All verification folders, files, or TXT records can also be deleted if you want as they are used only one time for verification purposes.

## Get Notified of Expiration

Create an account or login to get notified before your certificate expires and to manage all your certificates in one place.

Email:

Password:

([Forgot](#)  
[Password?](#))

Login

Create Account



# 下載憑證檔案

## \* 包含公、私鑰

### Certificate Files

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIGDTCCBPWgAwIBAgISA/7BMTYzf0YnPoAlK++3r6JEMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTA1VTMRyWFAYDVQQKEw1MZXQncyBFbmNyeXBOMSMwIQYDVQQD
ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSBYMTZAEFw0xODA0MzAwMTEOMThaFw0x
ODA3MjkWMTU0MThhbnBxGTAxBGNVBAMTEHd3dy50cDFyYy5lZHUudHcwggEiMAOG
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCftl8qe0Dc/YA/ACgclsL7e0wuya+R
OAUQK/bEluHHEZcBLZTNuiIG/B/eC83xFyIaLg50iryZ5pePwGdiKU3S/ixpvcXM
4e3AlvEvp1c8KLIAnmBHwJvYyJyUd5fg/UcUB+0xW1ZsUqAGDw56S802yEHvD
ZgJCKeivq/o2jHfK+ImlRb0vrkMHRoMQsLY2LoulzQ9NGGdnldHH/qY9t3Xo8DM0
02PgT0eQ8ku06Xlf8PEz1bf/0X/nXH0YW0CgPQRQvMUEUOTPNqJXUvSEgB3CtDZy
```

Private Key:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCCKYwggSiAgEAAoIBAQCftl8qe0Dc/YA/
ACgclsL7e0wuya+ROAUQK/bEluHHEZcBLZTNuiIG/B/eC83xFyIaLg50iryZ5peP
wGdiKU3S/ixpvcXM4e3AlvEvp1c8KLIAnmBHwJvYyJyUd5fg/UcUB+0xW1ZsUq
qAGDw56S802yEHvDZgJCKeivq/o2jHfK+ImlRb0vrkMHRoMQsLY2LoulzQ9NGGdn
ldHH/qY9t3Xo8DM002PgT0eQ8ku06Xlf8PEz1bf/0X/nXH0YW0CgPQRQvMUEUOTPN
qJXUvSEgB3CtDZy/m6RXfuSaQqBx7NfL98cRsdnPjiWI93ekJdF2ZsCRjwjr8B4
/0ZzE5nFAGMBAEACggEABt+d6+GfEo00c8GpeEhD3ve+zmqurCTJjv8dYS5QTDTw
4U0Zb1su4LCUFgXTCKeyt4a454obANKcPjsNF/voFgcLWUeqDh3BEjYn7R01E3k6
4+zs/tn9UTzYd3uaoF9tBfsTx/r5/OHIZYQSGJk+UluCFzq/YlLuEPhf142okpVa
```

CA Bundle (Contains Root And Intermediate Certificates):

```
AQH/BAgwBgEB/wIBADA0BgNVHQ8BAF8EBAMCAAYwfwYIKwYBBQUHAQEczBxMDIG
CCsGAQUFBzABhiZodHRwOi8vaXNyZy50cnVzdG1kLm9jczAuaWRlbnRydXN0LmNv
bTA7BggrBgEFBQcAcAoYvaHR0cDovL2FwcHMuaWRlbnRydXN0LmNvbS9yb290cy9k
c3Ryb290Y2F4My5wN2MwHwYDVR0jBBgwFoAUXKexpHsScfcb4UuQdf/EFWCfIRAw
VAYDVR0gBE0wS2AlBgZngQwBAGewPwYlKwYBBAGC3xMBAQEwMDAuBggrBgEFBQcC
ARYiaHR0cDovL2Mwcy5yb290LXpxLmXldHMIbnNyeXB0Lm9yZzA8BgNVHR8ENTAz
MDGgl6AthitodHRwOi8vY3JsLmLkZW50cnVzdC5jb20vRFRmUUK9PVENBWDNDUkwa
Y3JsMBOGAlUdDgQWBBSoSmpjBH3duubR0bemRWXv86jsoTANBgkqhkiG9w0BAQsF
AAOCAQEAA3TPXEfnjWjdGBX7CVW+d1a5cEilaUcne8IkCJLxWWh9KEik3JHRRHGJo
uM2VcGfl96S8TihRzZvoroeD6ti6WqEBmtzW3Wodatg+Vy0eph4EYpr/lwXKtx8/
```

Download All SSL Certificate Files



# 產生憑證檔案-方法2

# 自行產生私鑰

- \* 產生 RSA 2048bit, 3-DES 加密，PEM 格式 Server Private Key
  - \* ~# openssl genrsa -des3 -out private.key 2048
    - \* Enter PEM pass phrase: -- 需記此密碼，每次啟動 httpd 均會用到
    - \* Verify password -- Enter PEM pass phrase:

# 使用私鑰產生憑證申請檔

- \* ~\$ openssl req -new -key private.key -out server.csr
  - \* Enter PEM pass phrase: -- 輸入 Private Key 密碼
- \* 輸入基本資料
  - \* Country Name (2 letter code) [GB]:TW
  - \* State or Province Name (full name) [Berkshire]:Taiwan
  - \* Locality Name (eg, city) [Newbury]:Taipei
  - \* Organization Name (eg, company) [My Company Ltd]:National Taiwan University
  - \* Organizational Unit Name (eg, section) []:CCNET
  - \* Common Name (eg, your name or your server's hostname) []:www.tp1rc.edu.tw
  - \* Email Address []:davisyou@ntu.edu.tw
  - \*
    - \* Please enter the following 'extra' attributes
    - \* to be sent with your certificate request
    - \* A challenge password []: 直接 Enter
    - \* An optional company name []: 直接 Enter

# 產生憑證檔案 (使用憑證申請檔)

```
[root@tplrc ~]# cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwgaAx CzAJBgNVBAYTA1RXMQ8wDQYDVQQIDAZUYW13YW4xDzAN
BgNVBACMB1RhaXBlaTEjMCEGA1UECgwaTmF0aW9uYWwgVGFpd2FuIFVuaXZlcnNp
dHkxCzAJBgNVBAsMAmNjMRkwFwYDVQQDDBB3d3cudHAcMmUzWWR1LnR3MSIwIAYJ
KoZlIhvcNAQkBFhNkYXZpc3lvdUBudHUuZWRR1LnR3MIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAm3/i/UY1f08eM1IPjc/vVjywkAwOiX2i/NXbhH5+/wn8
0QeAn6m9DPOJi40aFB9C0GM7J8tV1crX3WWWQueDqYPNofeXGL4TMSbgaiewHA/41
NOul2ziFiI/WIHFBTyLmamCbcYk8aWdSxx2XJJBRSMEjYPSKGFyvkVWr3SLcEF
3SXOYHYTsdvypIionbt8DPwxiYd6Elggezjz6xuTrLcjiE0XL+V7hw/IjoMcJ7rU
UmXPYJBVtsA+J1GxjUEiNYZ2qCeEiNvWQP9304eQs5bklO++Dm0Q9kBftR787wQW
3ftlqzJD3AJwKo6XNas9azmKgci5DofhSPGmtXiaKwIDAQABoAAwDQYJKoZIhvcN
AQEFBQADggEBABDcNoBiE3CMFZxremYmysrc9x0qy9QWbN5Nxx6xghPY1MmhufFNS
TR7gd0uNpL5zjqPCQ1lz1+EXRVkHFuKM7JZQLHh0bG+Y1536jzbG4wS3MgUEBpDy
Ly8P804wur0YpdI9RX54YOZmxKDiKPIeSAINbwgZNXnTDhh3LFCk829UqbVAF2Kc
APKbDnH+selUe5Rph1k8UexqGjEdWas8vfS2xG2pHsBNLmP7jfy9POI5F1gyjmUE
45E4VQxgwVwjxf+1EbQ1QBi+5P8fw3DP24XjoEAwTaDRCKcYuhzycRsbZCuiTAz
jOAAx/Vgh7ZJ5LhjHqAjT8IBv56rLPzMcYM=
-----END CERTIFICATE REQUEST-----
```

Download SSL Certificate

I Have My Own CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwgaAx CzAJBgNVBAYTA1RXMQ8wDQYDVQQIDAZUYW13YW4xDzAN
BgNVBACMB1RhaXBlaTEjMCEGA1UECgwaTmF0aW9uYWwgVGFpd2FuIFVuaXZlcnNp
WwgVGFpd2FuIFVuaXZlcnNp
dHkxCzAJBgNVBAsMAmNjMRkwFwYDVQQDDBB3d3cudHAcMmUzWWR1LnR3MSIwIAYJ
KoZlIhvcNAQkBFhNkYXZpc3lvdUBudHUuZWRR1LnR3MIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAm3/i/UY1f08eM1IPjc/vVjywkAwOiX2i/NXbhH5+/wn8
0QeAn6m9DPOJi40aFB9C0GM7J8tV1crX3WWWQueDqYPNofeXGL4TMSbgaiewHA/41
NOul2ziFiI/WIHFBTyLmamCbcYk8aWdSxx2XJJBRSMEjYPSKGFyvkVWr3SLcEF
3SXOYHYTsdvypIionbt8DPwxiYd6Elggezjz6xuTrLcjiE0XL+V7hw/IjoMcJ7rU
UmXPYJBVtsA+J1GxjUEiNYZ2qCeEiNvWQP9304eQs5bklO++Dm0Q9kBftR787wQW
3ftlqzJD3AJwKo6XNas9azmKgci5DofhSPGmtXiaKwIDAQABoAAwDQYJKoZIhvcN
AQEFBQADggEBABDcNoBiE3CMFZxremYmysrc9x0qy9QWbN5Nxx6xghPY1MmhufFNS
TR7gd0uNpL5zjqPCQ1lz1+EXRVkHFuKM7JZQLHh0bG+Y1536jzbG4wS3MgUEBpDy
Ly8P804wur0YpdI9RX54YOZmxKDiKPIeSAINbwgZNXnTDhh3LFCk829UqbVAF2Kc
APKbDnH+selUe5Rph1k8UexqGjEdWas8vfS2xG2pHsBNLmP7jfy9POI5F1gyjmUE
45E4VQxgwVwjxf+1EbQ1QBi+5P8fw3DP24XjoEAwTaDRCKcYuhzycRsbZCuiTAz
jOAAx/Vgh7ZJ5LhjHqAjT8IBv56rLPzMcYM=
-----END CERTIFICATE REQUEST-----
```

# 下載憑證檔案

## \* 私鑰自行保管

### Certificate Files

Certificate:

```
-----BEGIN CERTIFICATE-----
MIIGCzCCBP0gAwIBAgISAwUQYU6yFP0+UAeh/TqzrdViMAOGCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTA1VTMRWwFAYDQQKEw1MZXQncyBFbmNyeXBOMSMwIQYDVQQD
ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSBYMzAeFw0xODAwMzAwMTI0NTBaFw0x
ODA3MjkwMTI0NTBaMBsxGTAXBgNVBAMTEHd3dy50cDFyYy51ZHUudHcwggEiMAOG
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCbf+L9Rjv87x4yUg+Nz+9WPLCQDA6J
faL81duEfn7/CfzRB4Cfqb0M84mLjRoUH0LQYzsnYlXVytfdZC540pg82h95cYv
hMxJuBqJ7AcD/jU066Xb0IWIj9YgcUFPiUzqYJtxiTxpZ1LFfZcckFFIz8QSNg9I
oZ/K+RVavdItwQXJc5gdh0x2/KkiKidu3wM/DGJh3oTWCP70PPrG50sty0ITRcv
5XuHD8i0gxnutRSZc9gkFW2wD4nUbGNQSIlhnaoJ4SI29ZA/3fTh5CzluSU7740
-----END CERTIFICATE-----
```

Private Key:

You provided your own CSR which means the private key was probably generated when you got the CSR. We do not have access to the private key in this case to show it.

CA Bundle (Contains Root And Intermediate Certificates):

```
-----BEGIN CERTIFICATE-----
MIIEkjCCA3qgAwIBAgIQCGFBQgAAAV0Fc2oLheynCDANBgkqhkiG9w0BAQsFADA/
MSQwIgdYDQKEExtEaWpdGFsIFNpZ25hdHVyZS8UcnVzdCBDby4xFzAVBgNVBAMT
DkRRTVBCSb290IENBIHkgZmB4XDE2MDMxNzE2NDAOM1oXDTIxMDMxNzE2NDAOM1ow
SjELMAkGA1UEBhMCVVMxFTAJBgNVBAoTUDUxldCdzIEVuuY3J5cHQuIzAhBgNVBAMT
GkxldCdzIEVuuY3J5cHQuQXV0aG9yaXR5IFgzMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCqKCAQEAnMM8Fr1Lke3c103g7NoYzDq1zUmGSXhvb418XCSL7e4S0EF
q6meNQH7LEqxGiHC6PjdeTm86dicbp5gWaf15Gan/PQeGdxYgk01ZHP/uaZ6WA8
SMx+yyk13Ei3dRxta67nsHjcaHJyse6cF6s5K671B5TaYucv9bTyWaN8jKkKQDI20
Z8h/pzq4UmEUEz916YKHy9v6D1b2honzhT+Xhq+w3Brvaw2VFh3EK6B1spkENnWA
-----END CERTIFICATE-----
```

[Download All SSL Certificate Files](#)



---

# 憑證檔案安裝 APACHE

# Apache 尚未安裝 https

## \* netstat -lnp

```
[root@localhost ~]# netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State                   PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN                  1026/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN                  1234/master
tcp6       0      0 :::80                  :::*                    LISTEN                  1411/httpd
tcp6       0      0 :::22                  :::*                    LISTEN                  1026/sshd
tcp6       0      0 :::1:25                :::*                    LISTEN                  1234/master
udp        0      0 0.0.0.0:68             0.0.0.0:*               *                       841/dhclient
udp        0      0 0.0.0.0:37179          0.0.0.0:*               *                       841/dhclient
udp6       0      0 :::26369               :::*                    *                       841/dhclient
raw6       0      0 :::58                  :::*                    *                       720/NetworkManager
```



# Apache 安裝 https

- \* 安裝 Apache mod\_ssl
  - \* yum install mod\_ssl
  - \* systemctl restart httpd

```
[root@localhost conf.d]# netstat -lntp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1026/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1234/master
tcp6       0      0 :::80                   :::*                    LISTEN      1513/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      1026/sshd
tcp6       0      0 :::1:25                 :::*                    LISTEN      1234/master
tcp6       0      0 :::443                   :::*                    LISTEN      1513/httpd
udp        0      0 0.0.0.0:68              0.0.0.0:*               *          841/dhclient
udp        0      0 0.0.0.0:37179           0.0.0.0:*               *          841/dhclient
udp6       0      0 :::26369                :::*                    *          841/dhclient
raw6       0      0 :::58                   :::*                    *          720/NetworkManager
```

# Apache SSL 設定檔

---

- \* CentOS

- \* `/etc/httpd/conf.d/ssl.conf`

- \* Ubuntu:

- \* `/etc/apache2/sites-enabled/default-ssl.conf`

# Apache SSL 設定檔內容

```
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

# Certificate Authority (CA):
# Set the CA certificate verification path where to find CA
# certificates for client authentication or alternatively one
# huge file containing all of them (file must be PEM encoded)
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
```

# 重啟 Apache

---

- \* CentOS 6
  - \* `service httpd restart`
- \* CentOS 7
  - \* `systemctl restart httpd`
- \* Ubuntu
  - \* `service apache2 restart`

# 若私鑰有設定密碼

- \* 重啟 apache 需輸入私鑰密碼

```
[root@davisyoucc ~]# systemctl start httpd
Enter SSL pass phrase for davisyoucc.ntu.edu.tw:443 (RSA) : *****
```

- \* reboot 後 apache 未輸入密碼無法啟動

```
[root@davisyoucc ~]# systemctl status httpd
■ httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
  Active: activating (start) since Wed 2018-05-02 09:55:54 CST; 26s ago
    Docs: man:httpd(8)
          man:apachectl(8)
  Main PID: 911 (httpd)
    CGroup: /system.slice/httpd.service
            └─ 911 /usr/sbin/httpd -DFOREGROUND
               └─ 1181 /bin/systemd-ask-password Enter SSL pass phrase for davisyoucc.ntu.edu.tw:443 (...

May 02 09:55:54 davisyoucc.ntu.edu.tw systemd[1]: Starting The Apache HTTP Server...
```

# 重啟自動私鑰密碼

## \* 私鑰密碼輸入方式

```
# Pass Phrase Dialog:  
# Configure the pass phrase gathering process.  
# The filtering dialog program ('builtin' is a internal  
# terminal dialog) has to provide the pass phrase on stdout.  
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog
```

### \* SSLPassPhraseDialog

- \* builtin -- CentOS 6

- \* exec:/usr/libexec/httpd-ssl-pass-dialog -- CentOS 7

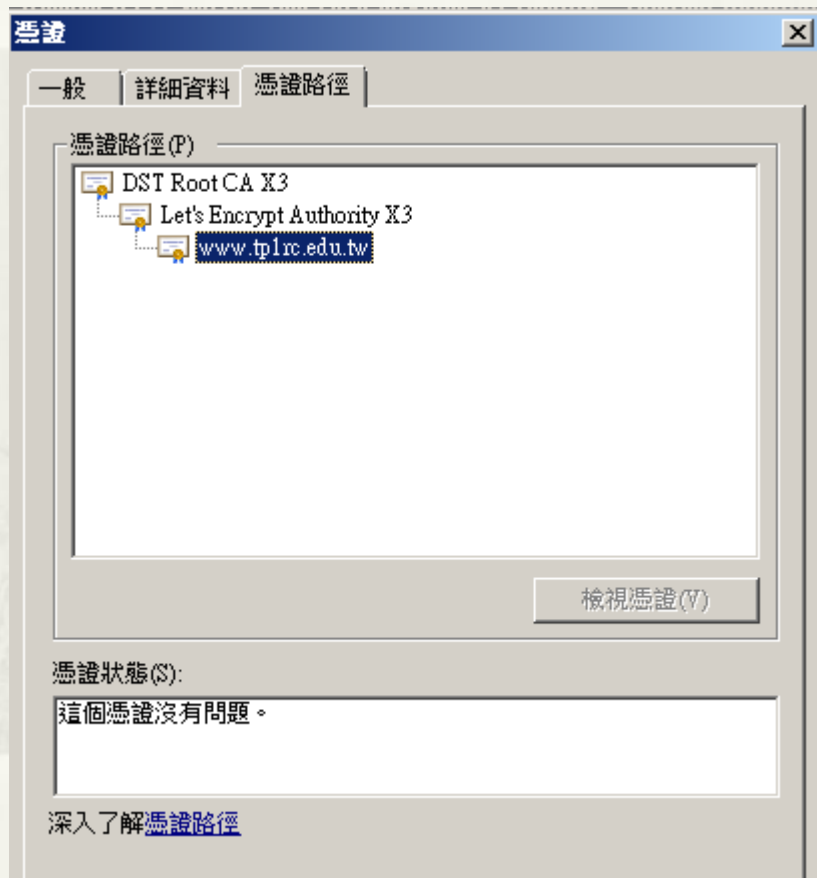
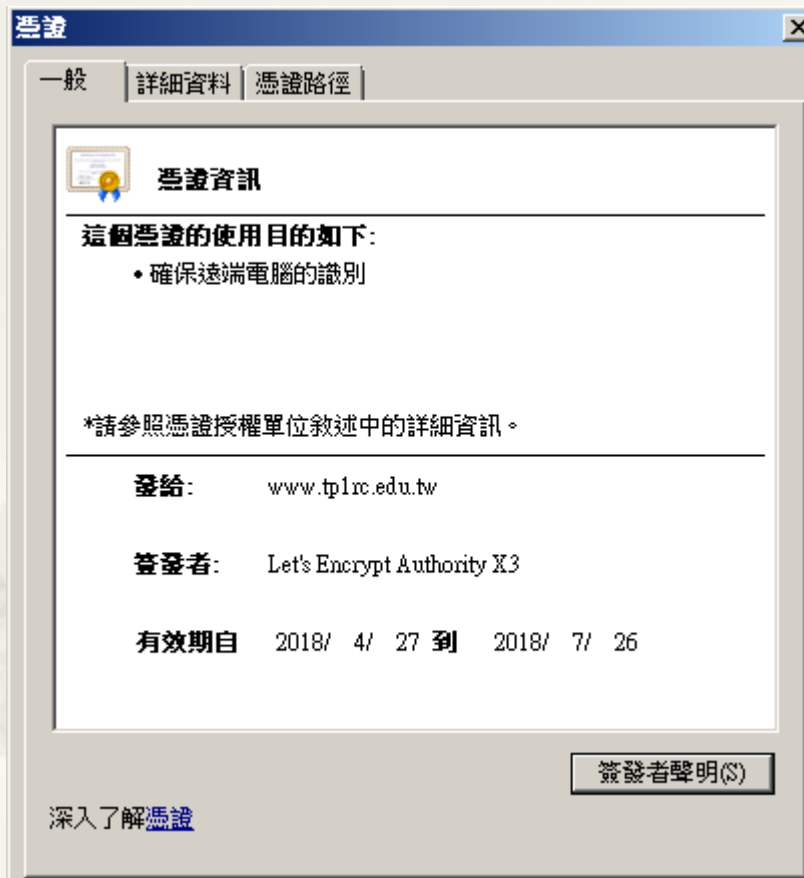
- \* exec:/root/apache\_pass.sh - 設定自動輸入密碼

### \* /root/apache\_pass.sh 內容

```
#!/bin/sh
```

```
echo "123456"
```

# 憑證內容



# SSL Server Test

\* <https://www.ssllabs.com/>

**Qualys. SSL Labs** Home Projects Qualys.com Contact


You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.tp1rc.edu.tw

## SSL Report: www.tp1rc.edu.tw (140.112.2.208)

Assessed on: Wed, 02 May 2018 03:16:51 UTC | [Hide](#) | [Clear cache](#) [Scan Another »](#)

### Summary

**Overall Rating**



| Category         | Score |
|------------------|-------|
| Certificate      | 100   |
| Protocol Support | 90    |
| Key Exchange     | 70    |
| Cipher Strength  | 90    |



# SSL Server Test disable SSLv3

## Configuration



### Protocols

|                       |     |
|-----------------------|-----|
| TLS 1.3               | No  |
| TLS 1.2               | Yes |
| TLS 1.1               | Yes |
| TLS 1.0               | Yes |
| SSL 3 <b>INSECURE</b> | Yes |
| SSL 2                 | No  |

For TLS 1.3 tests, we currently support draft version 18.

\* SSLProtocol all -SSLv2 -SSLv3

```
# SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by default:
SSLProtocol all -SSLv2 -SSLv3

# SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
```

# https in Wireshark


The image shows a Wireshark network traffic capture window. The top pane displays a list of network packets. Packet 402 is highlighted, showing a TLSv1.2 Client Hello message. The bottom pane shows the detailed view of this packet, with several fields highlighted in red boxes.

| No. | tcp.stream | Time     | TTL | Source        | Src Port | Destination   | Dest Port | Dst MAC         | Protocol | Length | Info                          |
|-----|------------|----------|-----|---------------|----------|---------------|-----------|-----------------|----------|--------|-------------------------------|
| 355 | 4          | 3.713245 | 128 | 172.16.0.2    | 64628    | 157.240.15.35 | 443       | Vmware_06:53:db | TCP      | 66     | 64628 → 443 [SYN] Seq=0 Win=0 |
| 400 | 4          | 3.844362 | 53  | 157.240.15.35 | 443      | 172.16.0.2    | 64628     | Dell_8b:ab:44   | TCP      | 66     | 443 → 64628 [SYN, ACK] Seq=1  |
| 401 | 4          | 3.844441 | 128 | 172.16.0.2    | 64628    | 157.240.15.35 | 443       | Vmware_06:53:db | TCP      | 54     | 64628 → 443 [ACK] Seq=1 Ack=1 |
| 402 | 4          | 3.844754 | 128 | 172.16.0.2    | 64628    | 157.240.15.35 | 443       | Vmware_06:53:db | TLSv1.2  | 571    | Client Hello                  |
| 442 | 4          | 3.973036 | 53  | 157.240.15.35 | 443      | 172.16.0.2    | 64628     | Dell_8b:ab:44   | TCP      | 60     | 443 → 64628 [ACK] Seq=1 Ack=1 |

Secure Sockets Layer

- TLsv1.2 Record Layer: Handshake Protocol: Client Hello
  - Content Type: Handshake (22)
  - Version: TLS 1.0 (0x0301)
  - Length: 512
  - Handshake Protocol: Client Hello
    - Handshake Type: Client Hello (1)
    - Length: 508
    - Version: TLS 1.2 (0x0303)
    - Random: a0c1af898e6698e0869e3efd22eef67083ec39bc655c3f1e...
    - Session ID Length: 32
    - Session ID: 7108b7f3195629e96dd69368c0cd2825a968b79067d1880a...
    - Cipher Suites Length: 28
    - Cipher Suites (14 suites)
      - Compression Methods Length: 1
      - Compression Methods (1 method)
      - Extensions Length: 407
      - Extension: Reserved (GREASE) (len=0)
      - Extension: renegotiation\_info (len=1)
      - Extension: server\_name (len=21)
        - Type: server\_name (0)
        - Length: 21
        - Server Name Indication extension
          - Server Name list length: 19
          - Server Name Type: host\_name (0)
          - Server Name length: 16
          - Server Name: www.facebook.com

---



簡報完畢  
謝謝