HTTPS 憑證安裝
IIS

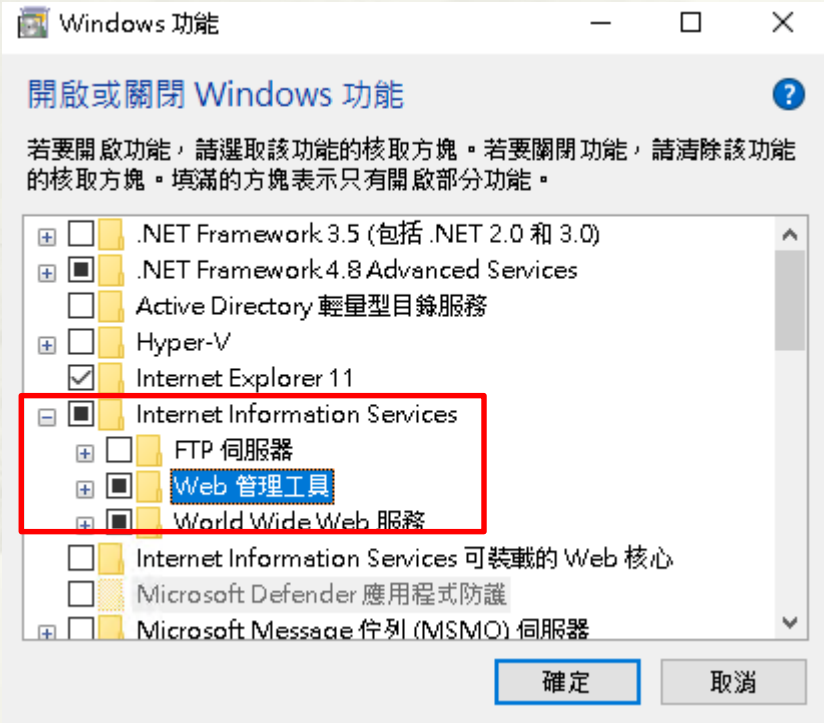
臺灣大學計資中心
網路組
游子興

大綱

* Install IIS
* Install Server Certificate
  * Manual
    * Create CSR File and Import Server Certificate
    * Import .pfx (Certificate/Private Key)
  * Automatic
    * win-acme Without IIS
    * win-acme With IIS

Install IIS @ Windows10

* 開始 > 設定 > 應用程式 > 程式和功能: 開啟或關閉 Windows 功能
* Internet Information Service
  * Web 管理工具
  * World Wide Web 服務

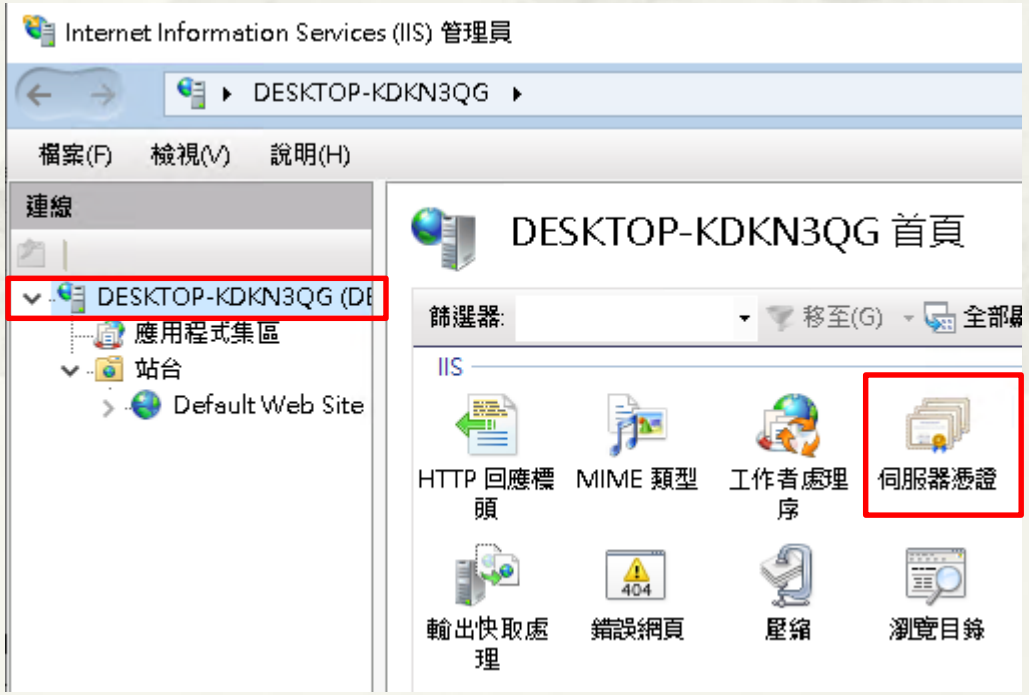


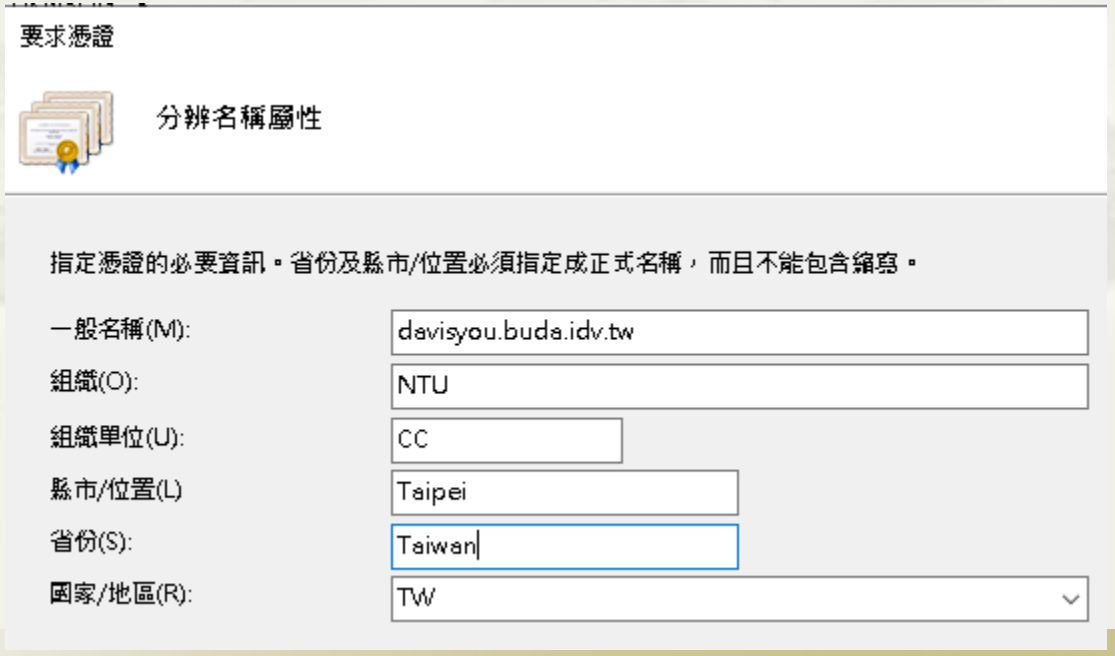
Manual Install
Create CSR File
Import Server Certificate

Certificate Signing Request

Create CSR File

* 開始 > Windows 系統管理工具 > Internet Information Services(IIS)





Create CSR File

* CSR File

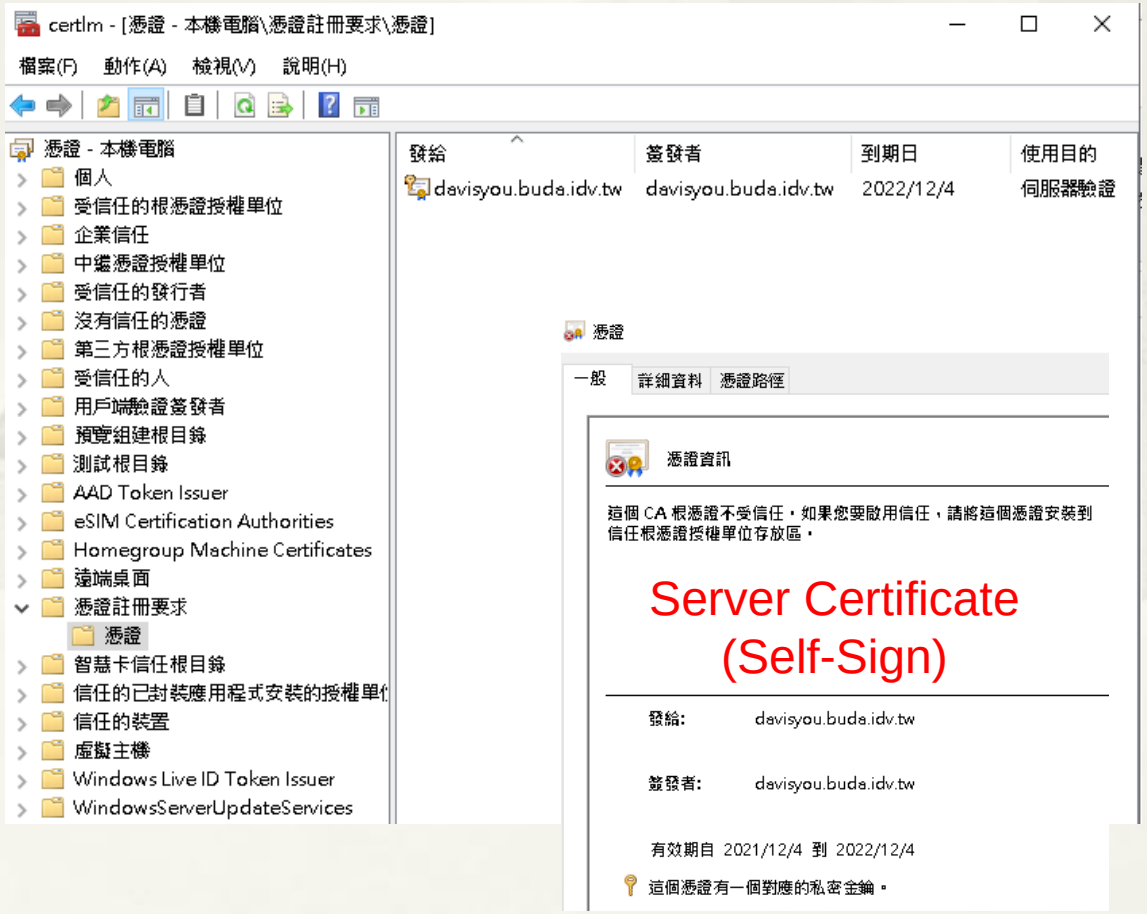
server.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

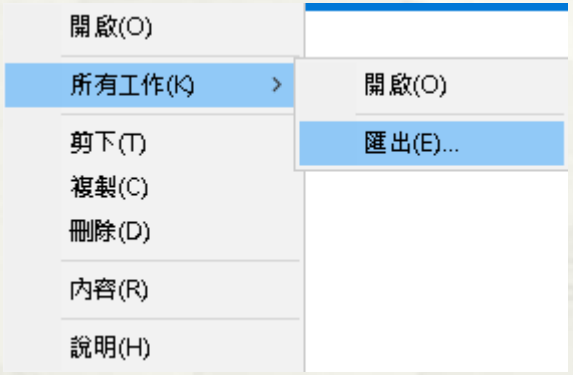
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEXDCCA0QCAQAwaTELMAkGA1UEBhMCVFcxDzANBgNVBAgMBlRhaXdhbjEPMA0G
A1UEBwwGVGFpcGVpMQwwCgYDVQQKDANOVFUxCzAJBgNVBAsMAkNDMR0wGwYDVQQD
DBRkYXZpc3lvdS5idWRhLmlkdi50dzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALwB5CPWKCw+mE6MxGL93ZDXJesQO0JNHOShQAaH2XzPPJmoBargPign
KfVvfioh/cOvGh6aldY3W7JgtSt5jhV+wFwnrtDLmcYfAESaWULy/HUneyanfOVy
z+u+Zirp2d2PAsxI8TNneWEEYyDSRiaIdNRhDAOgTk2XkeYYaAICbek3QAIHBZ6k
tXSGbIUSCFAz91UmLEjwabgzvKuY4VnbH+RfgCcd6onp7vmcnUw13Rc4BUa4IHRs
L1i7BfoPgdSoEnMOOw5PBLgLAfq+M6GVEOsbY7qXj9Qh2yBDbUCxKpHEMKLcMhmT
kgXD3Eb5sl4wtGCk6YGYGk49DEHPF6kCAwEAAaCCAawwHAYKKwYBBAGCNw0CAzEO
FgwxMC4wLjE5MDQzLjIwRgYJKwYBBAGCNxUUMTkwNwIBBQwPREVTS1RPUC1LREtO
M1FHDBRERVNLVE9QLUtES04zUUdcdXNlcgwLSW5ldE1nci5leGUwcgYKKwYBBAGC
NwOCAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgA
YQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYA
aQBkAGUAcgMBADCBzwYJKoZIhvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DAT
BgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMC
AgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMAsGCWCGSAFlAwQBLTAL
BglghkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0G
A1UdDgQWBBTlCwD8kPrwcmU71EfDO/KGx7WPizANBgkqhkiG9w0BAQUFAAOCAQEA
NcabvM4wq4zGE/DzXOH8tfWJDpGNoUXVOXVBhN3R3zL0mExw+flsXQHhZx5n3aDg
GHZxnrbMX+HlpiquVLFbJVa61fUJ9wwSzR2OCiAoT59b6EsZRwWe5QDNEAIj4bte
372D7NspzDX2Ceh0heVkxqijHvn+mBM/oLcJAiidDZ1FYCccZIuA2JCmlMts/rCU
ovitrJsPKN54PDiJXC+shqJy5Y3mwgC66I0OA0BVUw+VtkCq91VTPaLVZif6+AaW
0ShS955dFVAs0ELEIzefyZcu3ZI0+VbgpvlQk73sA8JwUdqF7IMWUw9KWnRPc5Cy
5w17IsdH63cEH89/P6HQTg==
-----END NEW CERTIFICATE REQUEST-----
```

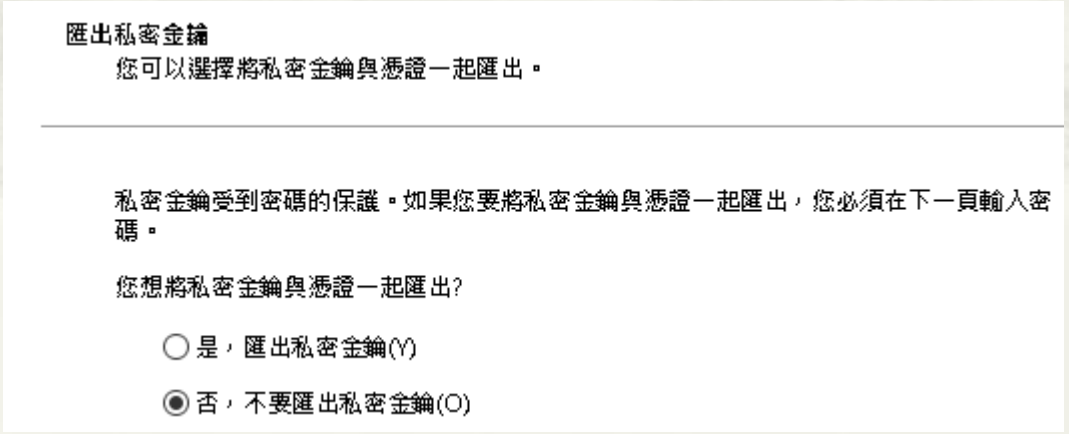
匯出 Server Certificate/Private Key

* certlm.msc (本機電腦)



* 匯出 Server Certificate





匯出 Server Certificate (Self-Sign)

匯出檔案格式

憑證可以用多種檔案格式匯出。

請選取您想要使用的格式:

- ○ DER 編碼二位元 X.509 (.CER)(D)
- ◉ Base-64 編碼 X.509 (.CER)(S)
- ○ 密碼編譯訊息語法標準 - PKCS #7 憑證 (.P7B)(C)
  - ☐ 如果可能的話，包含憑證路徑中的所有憑證(I)
- ○ 個人資訊交換 - PKCS #12 (.PFX)(P)
  - ☐ 如果可能的話，包含憑證路徑中的所有憑證(U)
  - ☐ 如果匯出成功即刪除私密金鑰(K)
  - ☐ 匯出所有延伸內容(A)
  - ☐ 啟用憑證隱私權(E)
- ○ Microsoft 序列憑證存放區 (.SST)(T)

要匯出的檔案

請指定您要匯出的檔案名稱

檔案名稱(F):

C:\Users\user\Documents\cert.cer　[瀏覽(R)...]

cert.cer - 記事本

檔案(F)　編輯(E)　格式(O)　檢視(V)　說明

```
-----BEGIN CERTIFICATE-----
MIIEHjCCAwagAwIBAgIQbdYyVlsHl5VHGeHc9dKD8TANBgkqhkiG9w0BAQUFADBp
MQswCQYDVQQGEwJUVzEPMA0GA1UECAwGVGFpd2FuMQ8wDQYDVQQHDAZUYWlwZWkx
DDAKBgNVBAoMA05UVTELMAkGA1UECwwCQ0MxHTAbBgNVBAMMFGRhdmlzeW91LmJ1
ZGEuaWR2LnR3MB4XDTIxMTIwNDA2NTgzMFoXDTIyMTIwNDA3MTgzMFowaTELMAkG
A1UEBhMCVFcxDzANBgNVBAgMBlRhaXdhbjEPMA0GA1UEBwwGVGFpcGVpMQwwCgYD
VQQKDANOVFUxCzAJBgNVBAsMAkNDMR0wGwYDVQQDDBRkYXZpc3lvdS5idWRhLmlk
di50dzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALwB5CPWKCw+mE6M
xGL93ZDXJesQO0JNHOShQAaH2XzPPJmoBargPignKfVvfioh/cOvGh6aldY3W7Jg
tSt5jhV+wFwnrtDLmcYfAESaWULy/HUneyanfOVyz+u+Zirp2d2PAsxI8TNneWEE
YyDSRiaIdNRhDAOgTk2XkeYYaAICbek3QAIHBZ6ktXSGbIUSCFAz91UmLEjwabgz
wKuY4VnbH+RfgCcd6onp7vmcnUwl3Rc4BUa4lHRsLli7BfoPgdSoEnMOOw5PBLgL
Afq+M6GVEOsbY7qXj9Qh2yBDbUCxKpHEMKLcMhmTkgXD3Eb5sl4wtGCk6YGYGk49
DEHPF6kCAwEAAaOBwTCBvjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR0lBAwwCgYIKwYB
BQUHAwEweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcN
AwQCAgCAMAsGCWCGSAFlAwQBKjALBglghkgBZQMEAS0wCwYJYIZIAWUDBAECMAsG
CWCGSAFlAwQBBTAHBgUrDgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQU5QsA/JD6
8HJl09RHwzvyhse1j4swDQYJKoZIhvcNAQEFBQADggEBADFNHZSkbQYwREVd1xBJ
VKPuycvAufnymSGNRqFRYQbhrgCb+kYJ5vwRd9J8ZzyROGZrOjrbesRHFZ1oiVIz
5rHv4uRUMssM4ZahYl4D7+sPwwt0bUpBBqd/RxD8i4vFPx1Sfi+pYsjgCfwQa9Ba
7orIS7xGLG9kzPss54EgAq3HbLciblVtgEWMqBueQzlqkHdC9HuRrP/61KWy3oH
gGCnbl4EXCV5XZT6PTYWwGJM5D+YZckJ8qNZoNBYTgFfSYixrGPQkVlDCR+ry+xu
bzb8v0Qo6EImSme3cyGbSCEV02+pPUyz+Ao4p9ZNtd7Tn4c1a/dH/EmpL842fyQn
zy0=
-----END CERTIFICATE-----
```

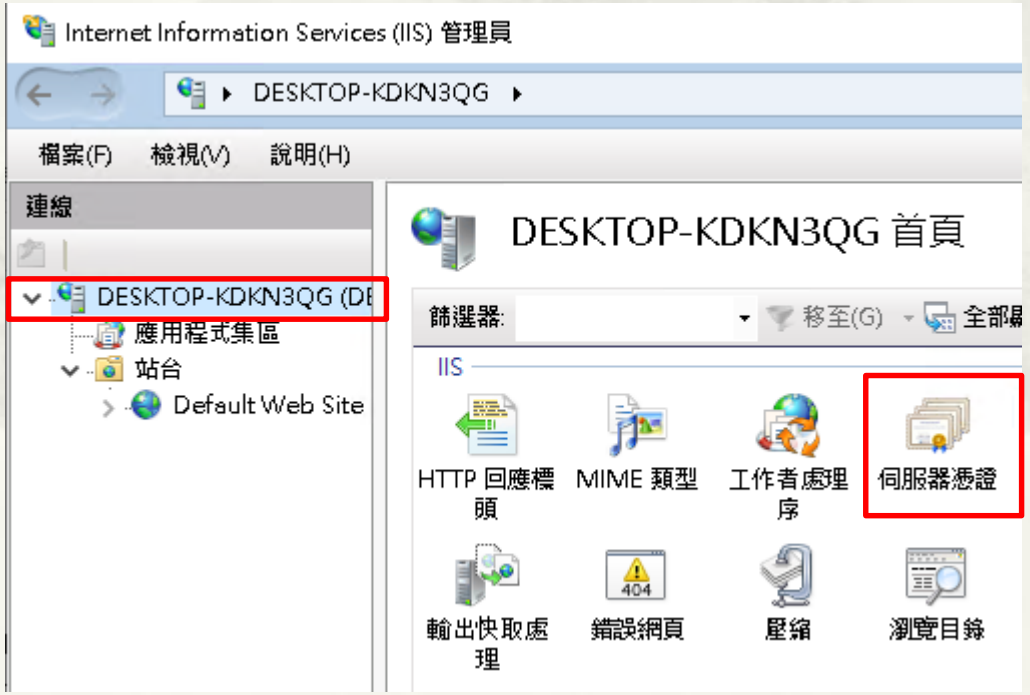
建立憑證要求

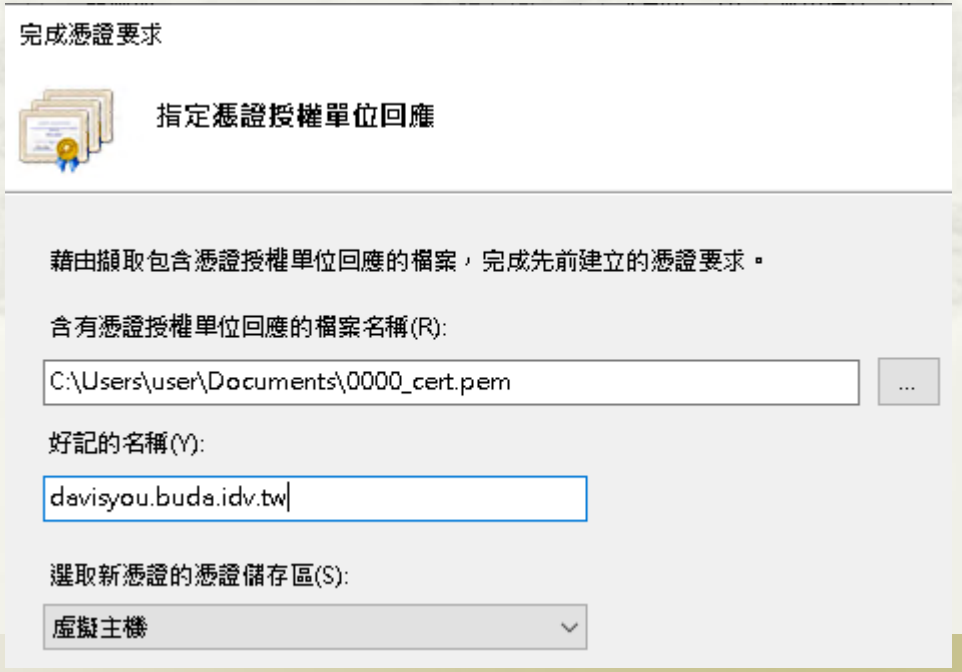
Background Steps

* Private Key
* Certificate Signing Request
* Server Certificate (Self-Sign)

Import Server Certificate

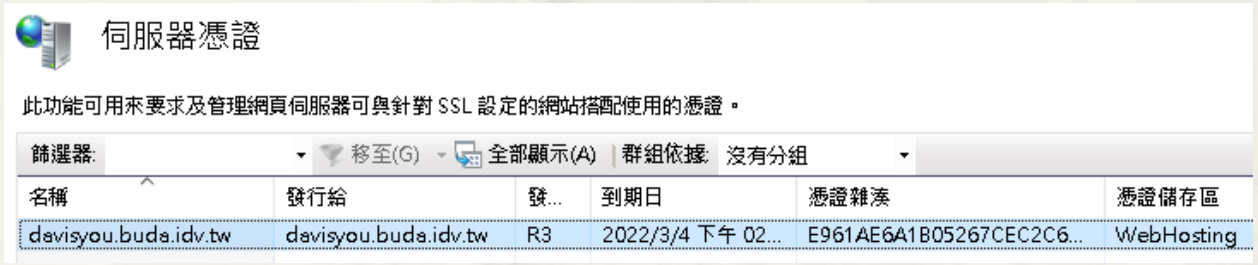
* 開始 > Windows 系統管理工具 > Internet Information Services(IIS)

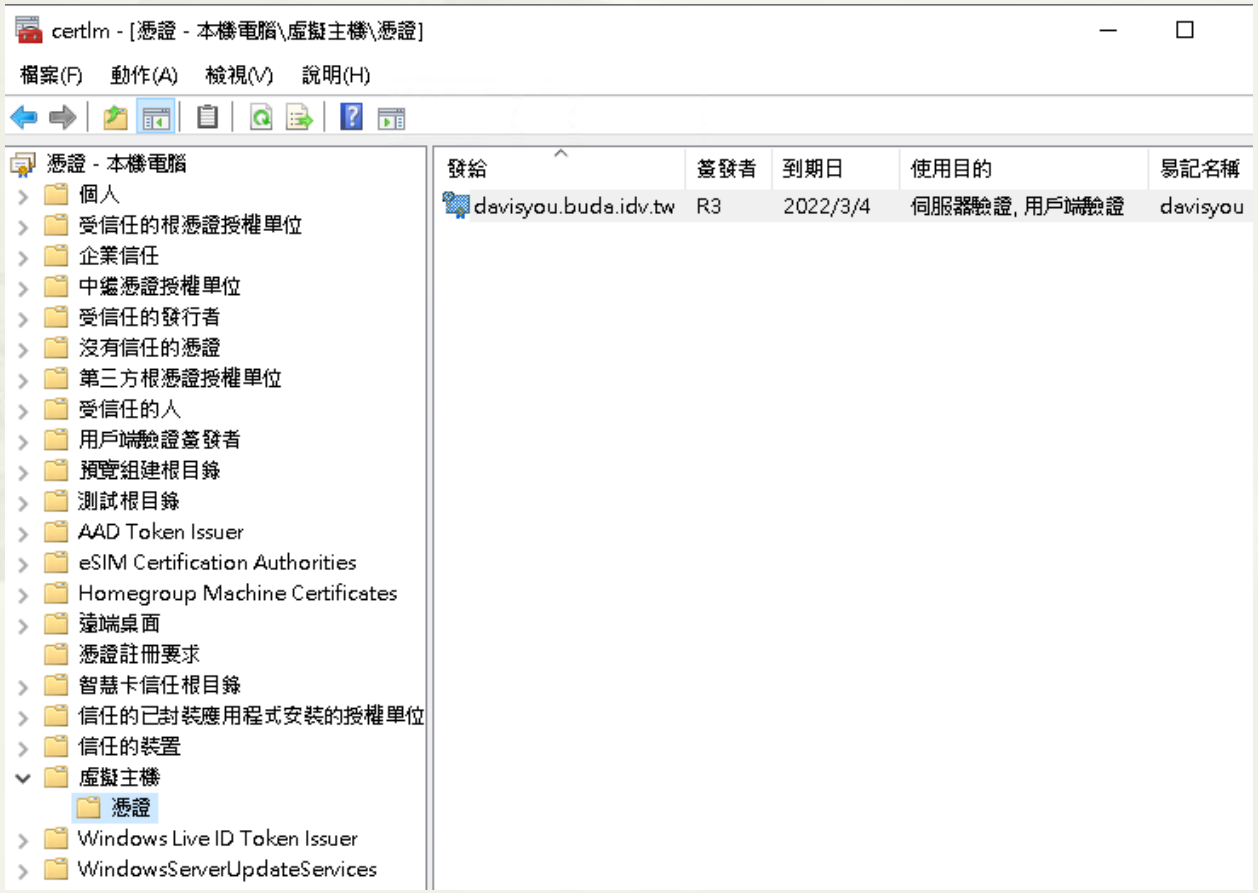




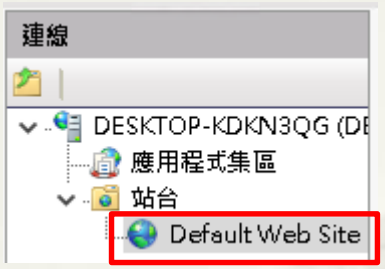
Import Server Certificate

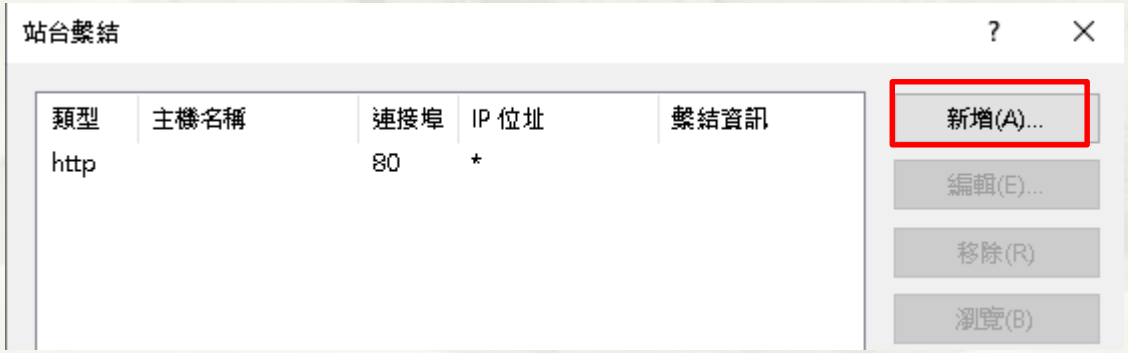
* certlm.msc (本機電腦)

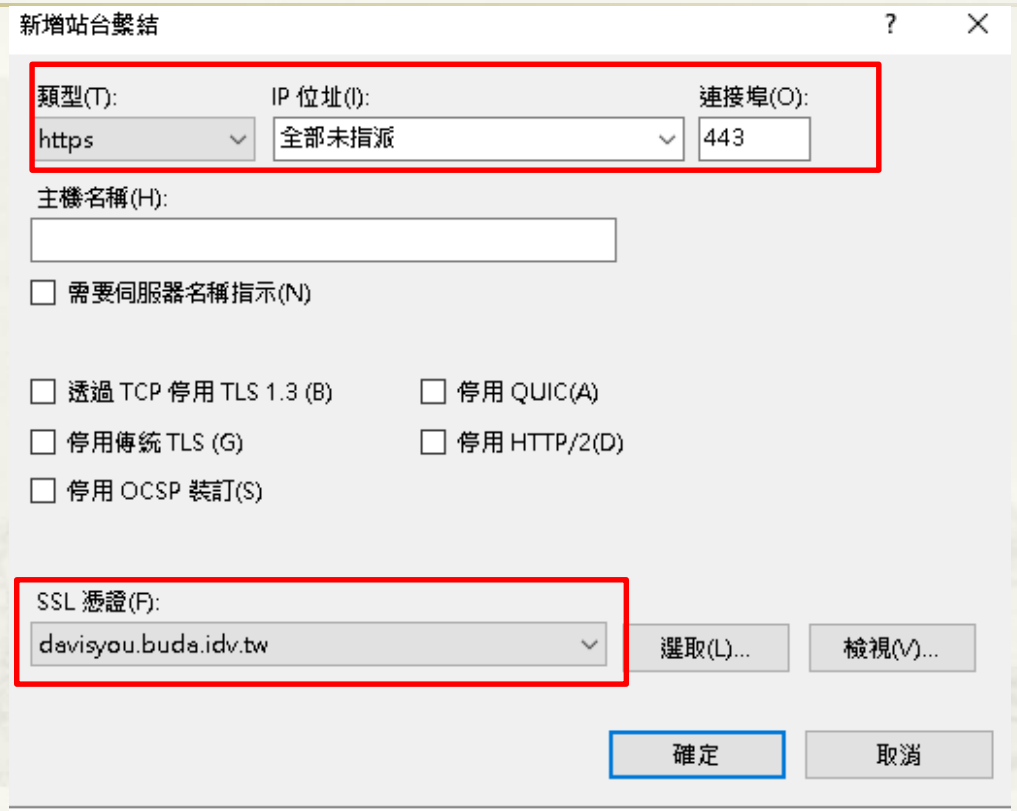


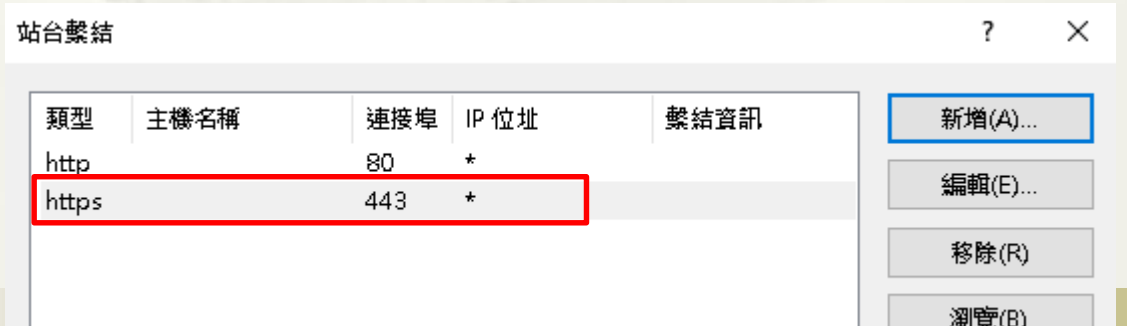


HTTPS Config



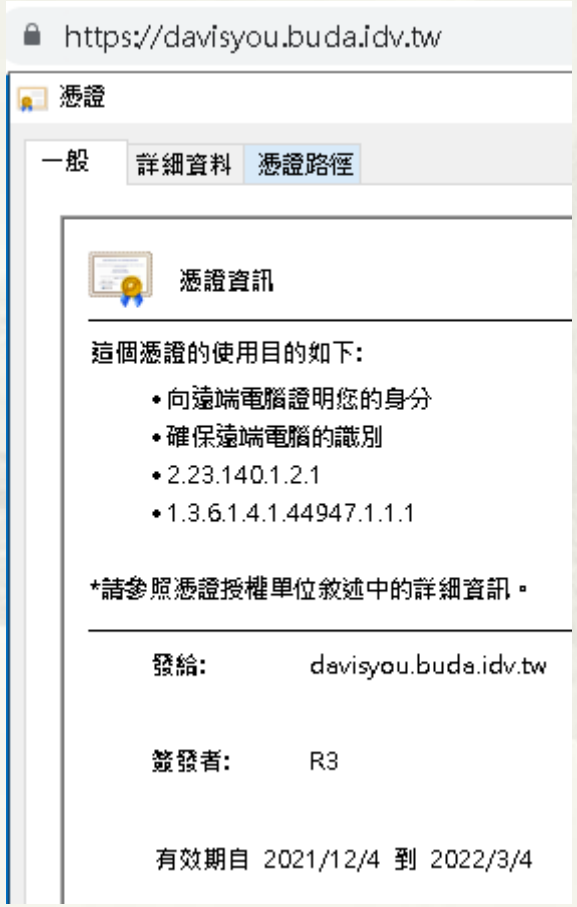




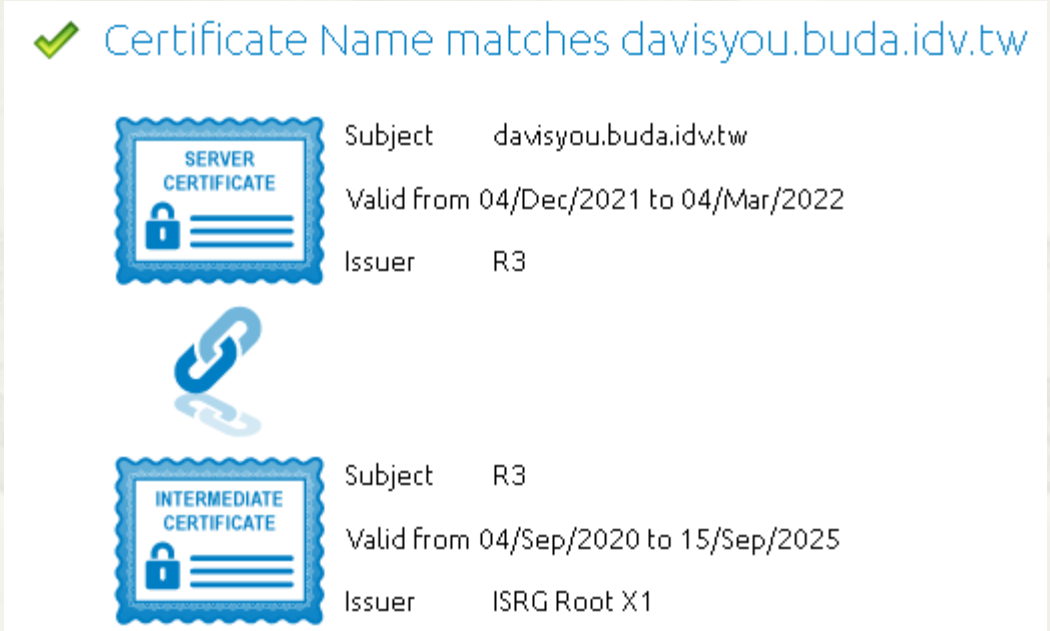


Check

* https://davisyou.buda.idv.tw



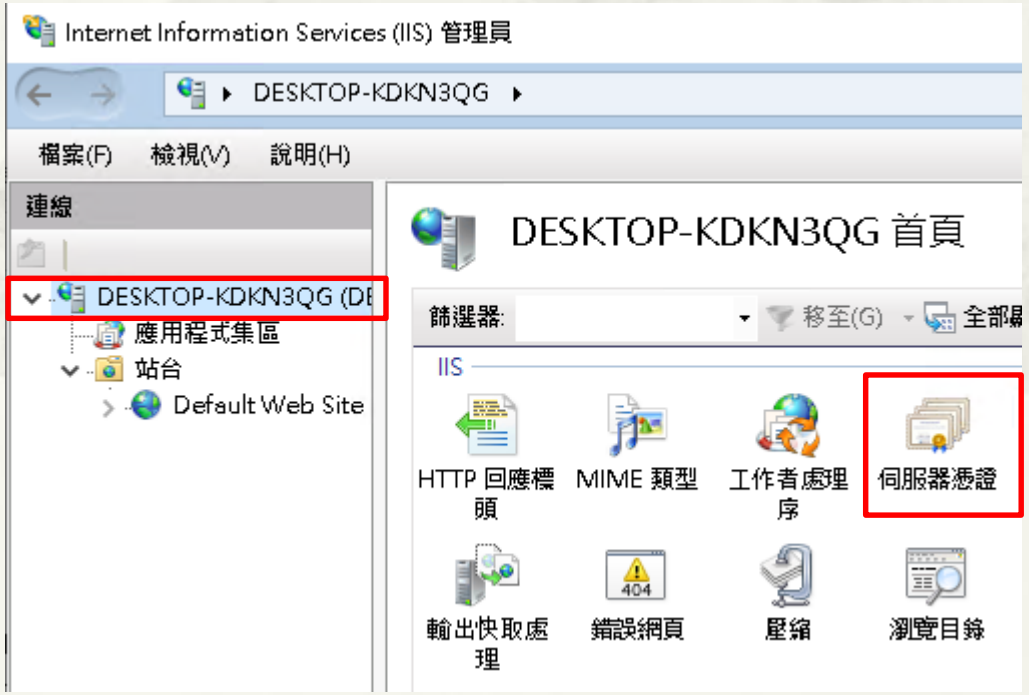
* Certificate Chain
* https://www.digicert.com/help/

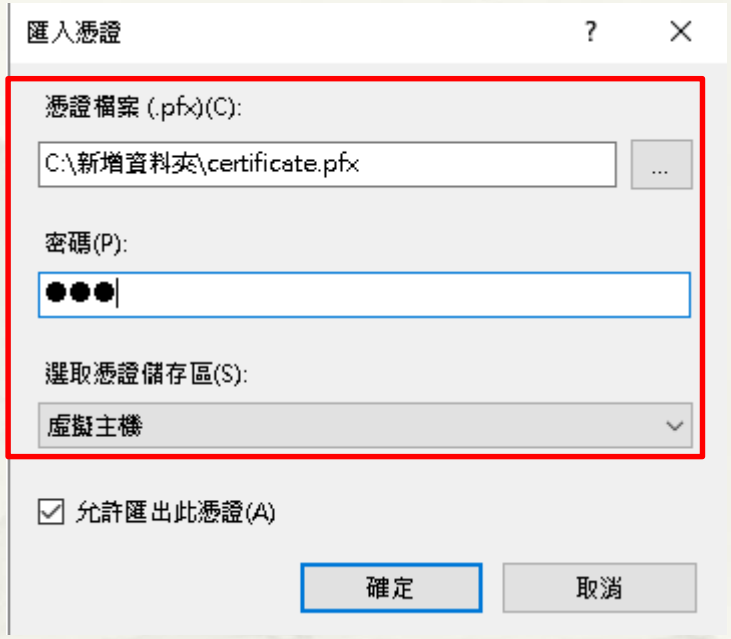


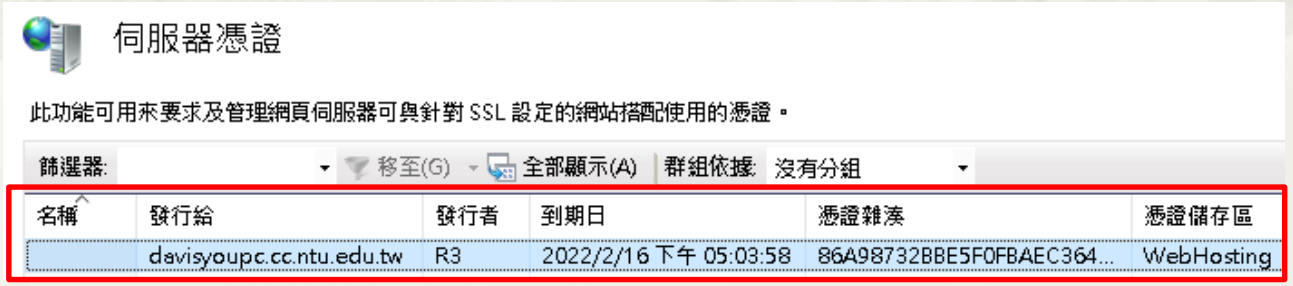
Manual
Import .pfx
(Certificate/Private Key)

Install Certificate

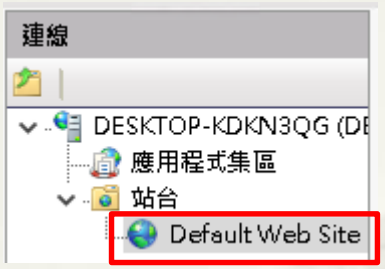
* 開始 > Windows 系統管理工具 > Internet Information Services(IIS)

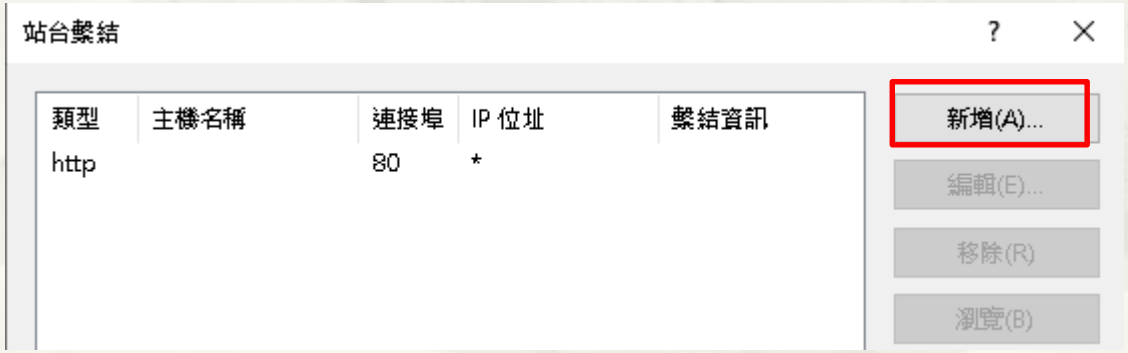


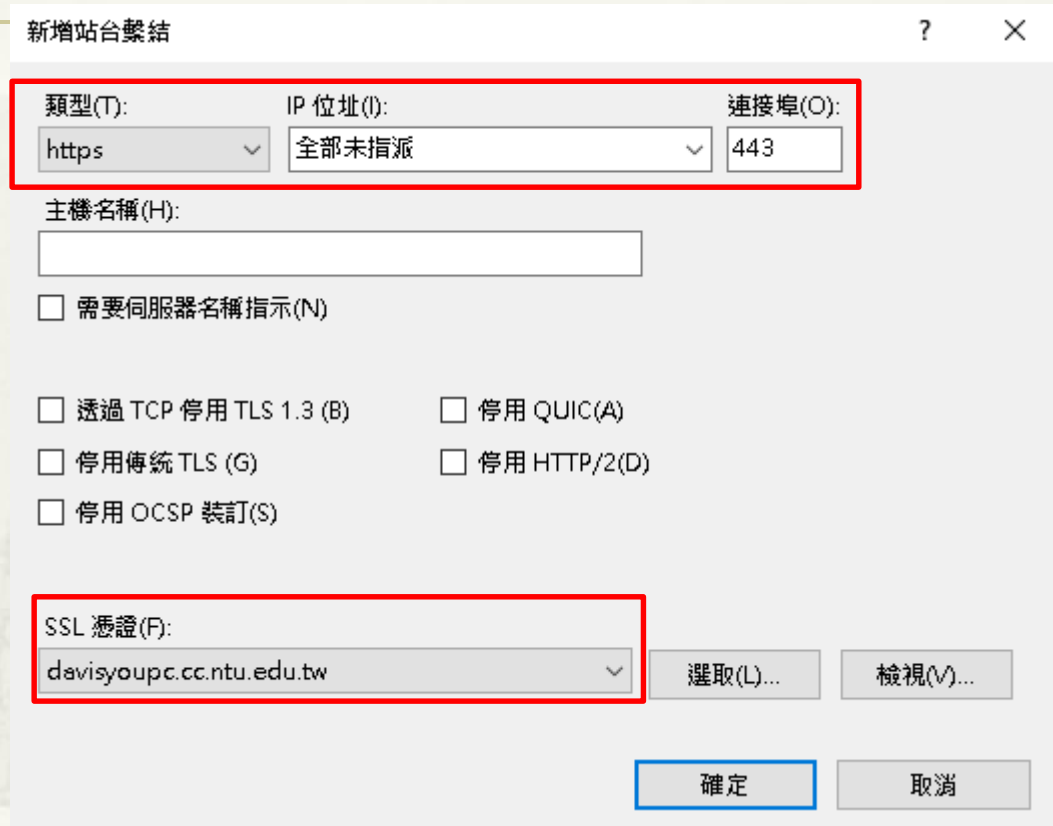


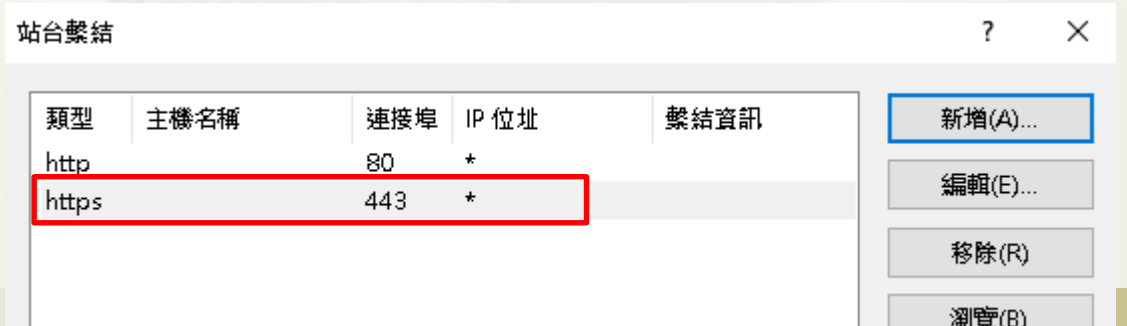


HTTPS Config





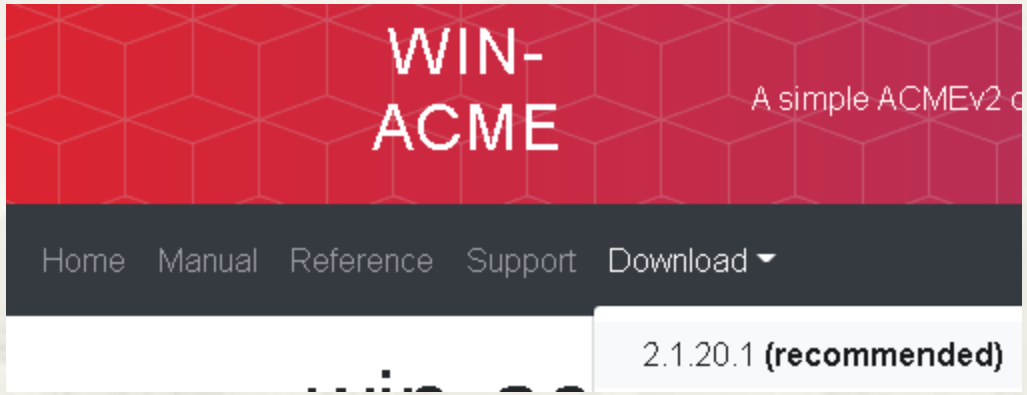




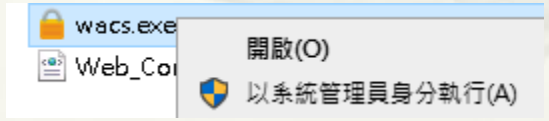
Install win-acme

win-acme Without IIS

* https://www.win-acme.com/

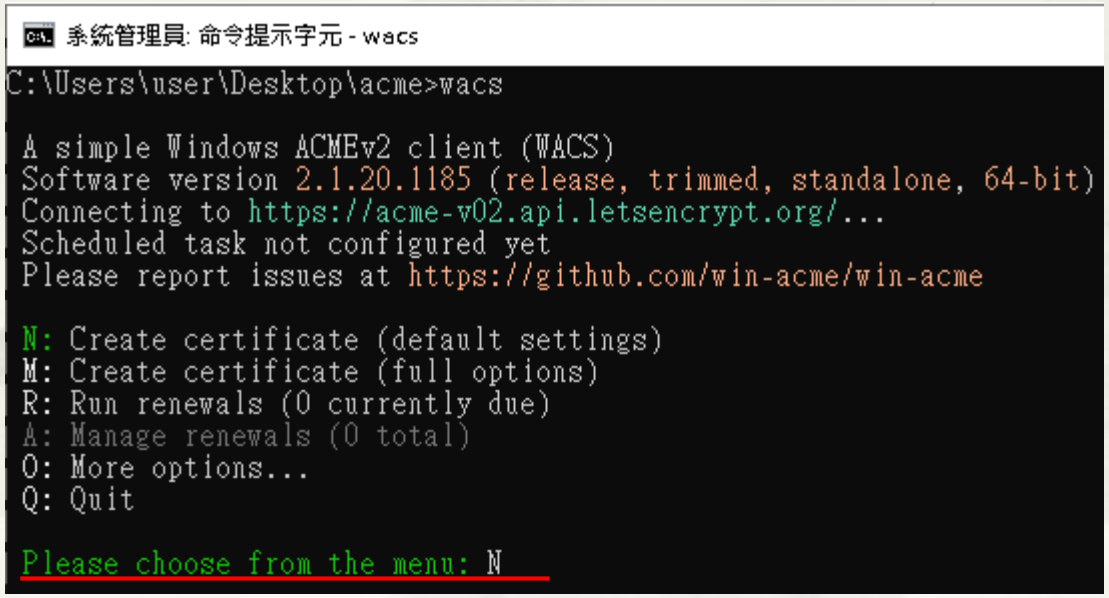


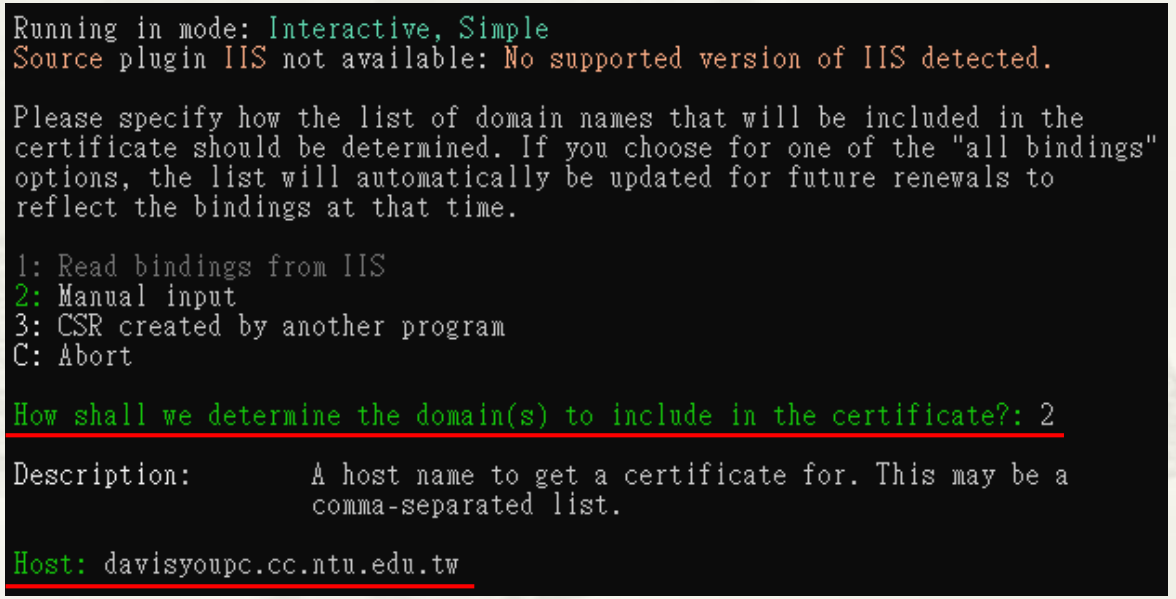
* Unzip win-acme.v2.1.20.1185.x64.trimmed.zip
* 系統管理者執行



win-acme
Without IIS

win-acme Without IIS





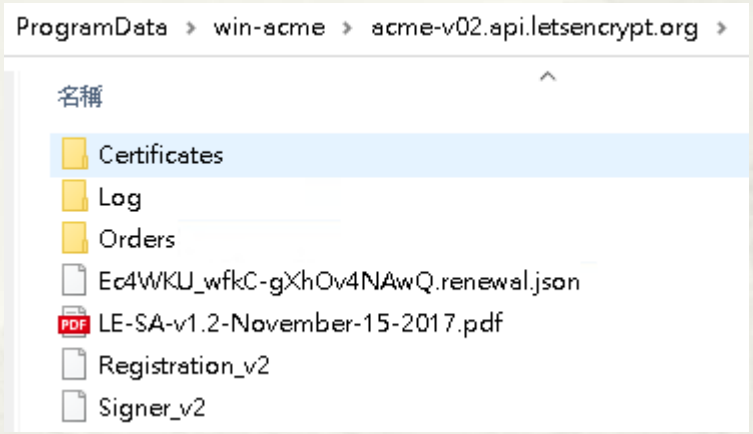
win-acme Without IIS

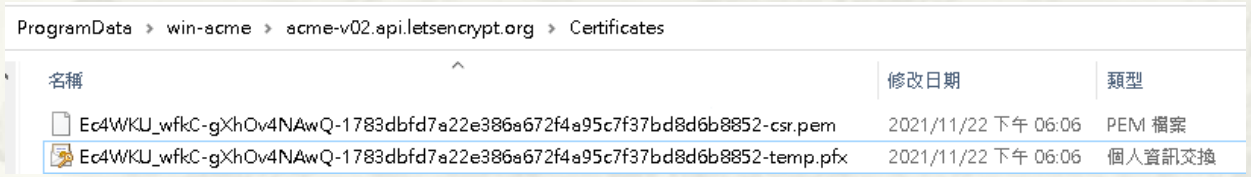
```
Source generated using plugin Manual: davisyoupc.cc.ntu.edu.tw
Installation plugin IIS not available: No supported version of IIS detected.

With the certificate saved to the store(s) of your choice, you may choose one
or more steps to update your applications, e.g. to configure the new
thumbprint, or to update bindings.

1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 3

Terms of service:   C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf

Open in default application? (y/n*) - <Enter>

Do you agree with the terms? (y*/n) - <Enter>

Enter email(s) for notifications about problems and abuse (comma-separated): davisyou@ntu.edu.tw
```

```
[davisyoupc.cc.ntu.edu.tw] Authorizing...
[davisyoupc.cc.ntu.edu.tw] Authorizing using http-01 validation (SelfHosting)
[davisyoupc.cc.ntu.edu.tw] Authorization result: valid
Downloading certificate [Manual] davisyoupc.cc.ntu.edu.tw
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [Manual] davisyoupc.cc.ntu.edu.tw @ 2021/11/22 18:06:11 to store My
Installing with None...
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\Users\user\Desktop\acme
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 09:00:00
- Random delay 04:00:00
- Time limit 02:00:00
Adding renewal for [Manual] davisyoupc.cc.ntu.edu.tw
Next renewal scheduled at 2022/1/16 18:05:19
Certificate [Manual] davisyoupc.cc.ntu.edu.tw created

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit

Please choose from the menu: Q
```

win-acme Without IIS

* C:\ProgramData\win-acme

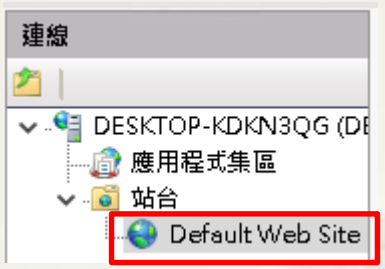


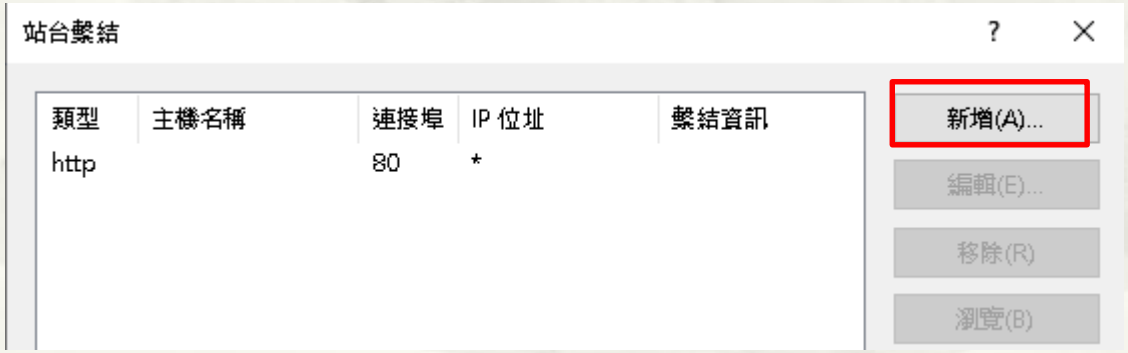


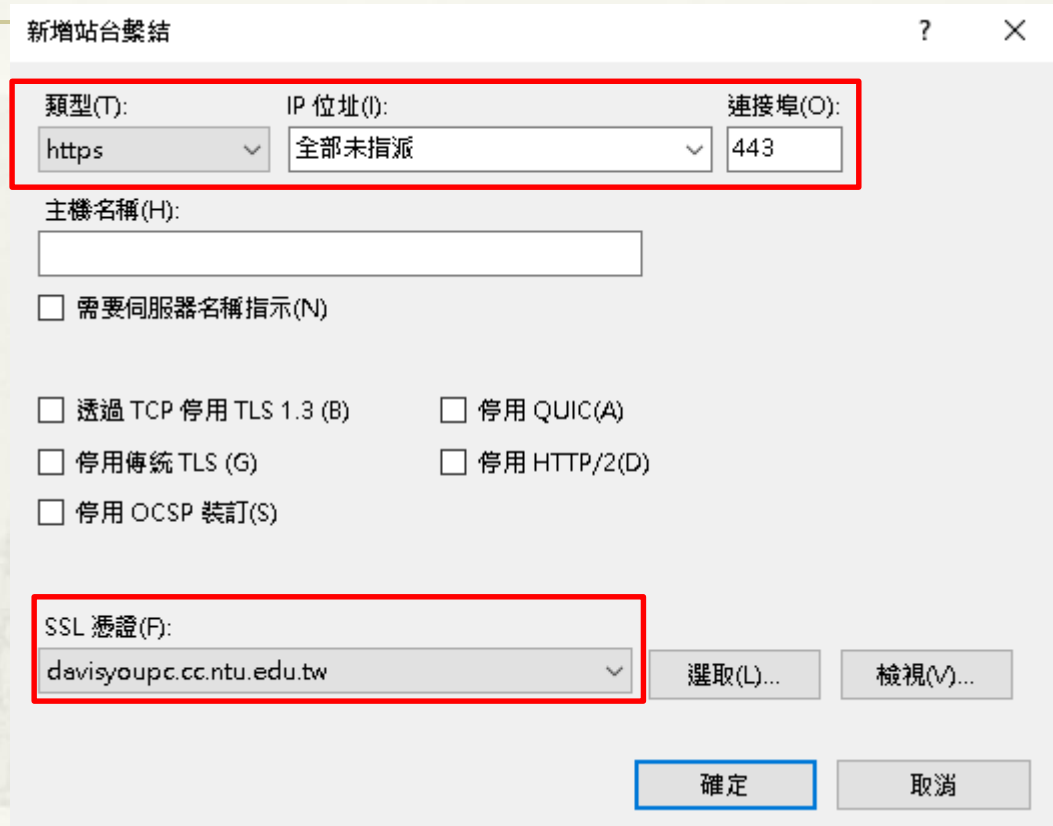
* certlm.msc (本機電腦)

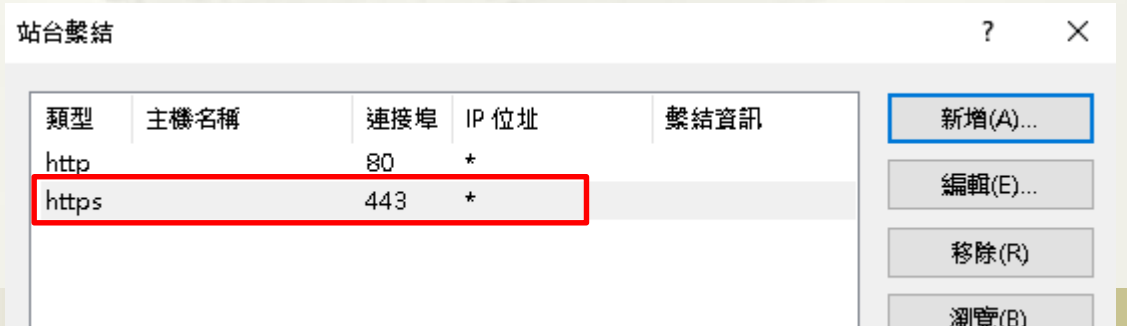
* 安裝 IIS
  * 伺服器憑證已安裝

HTTPS Config



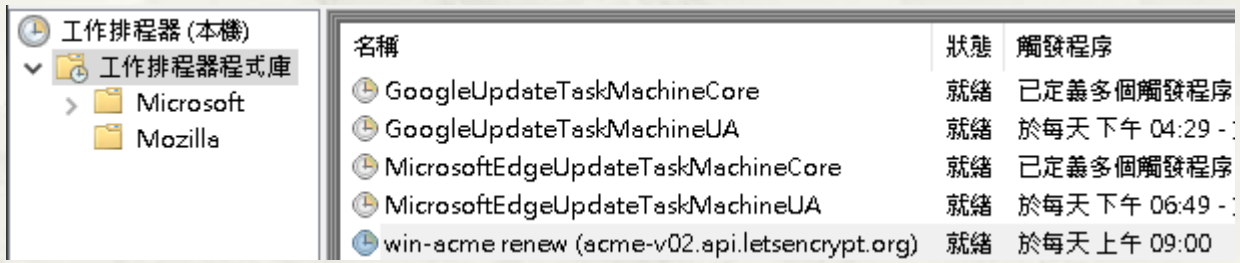


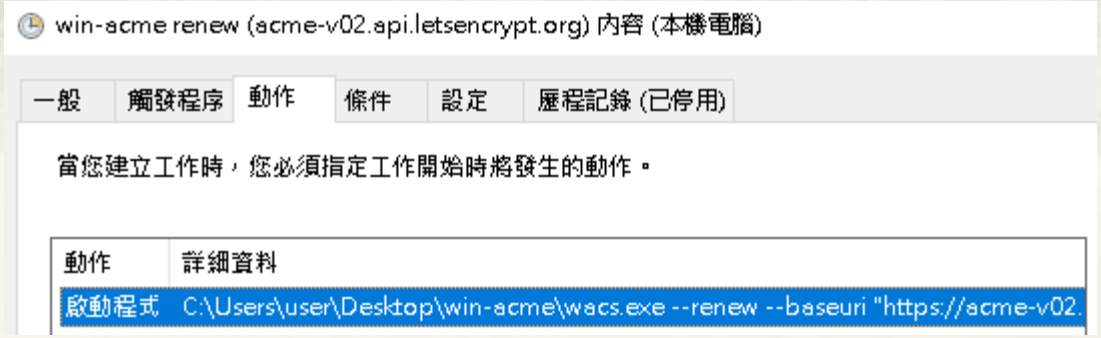




Auto Renew

- 在安裝完 win-acme 之後，win-acme 會自動在「工作排程器」建立一個排程，執行週期是每天
- 開始 > Windows 系統管理工具 > 工作排程器



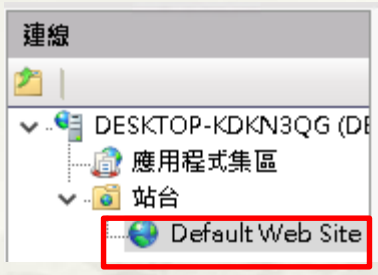


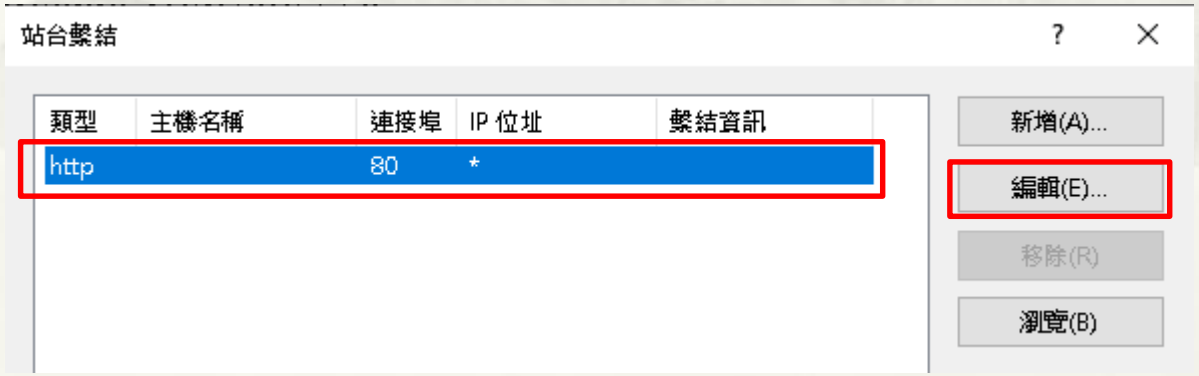
win-acme Without IIS Background Steps

* Create .pfx and Import to Windows Cert Store
  * Private Key
  * Server Certificate
* 工作排程器
  * Auto Renew Job

win-acme
With IIS

win-acme With IIS



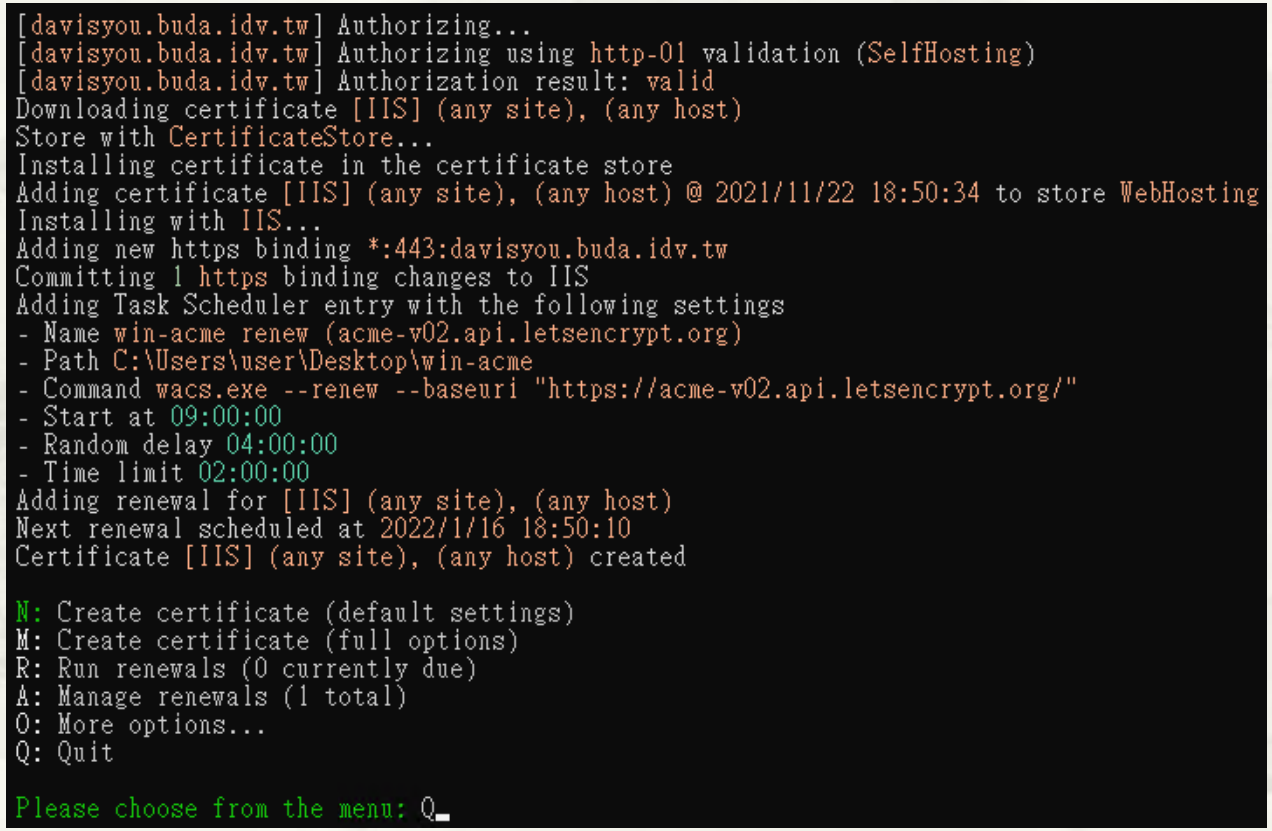


win-acme With IIS

```
A simple Windows ACMEv2 client (WACS)
Software version 2.1.20.1185 (release, trimmed, standalone, 64-bit)
Connecting to https://acme-v02.api.letsencrypt.org/...
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: N

Running in mode: Interactive, Simple

Please select which website(s) should be scanned for host names. You may
input one or more site identifiers (comma-separated) to filter by those
sites, or alternatively leave the input empty to scan *all* websites.

1: Default Web Site (1 binding)

Site identifier(s) or <Enter> to choose all: <Enter>
```

```
1: davisyou.buda.idv.tw (Site 1)

Listed above are the bindings found on the selected site(s). By default all
of them will be included, but you may either pick specific ones by typing the
host names or identifiers (comma-separated) or filter them using one of the
options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: A

1: davisyou.buda.idv.tw (Site 1)

Continue with this selection? (y*/n) - <Enter>

Source generated using plugin IIS: davisyou.buda.idv.tw

Terms of service:   C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf

Open in default application? (y/n*) - <Enter>

Do you agree with the terms? (y*/n) - <Enter>

Enter email(s) for notifications about problems and abuse (comma-separated): davisyou@ntu.edu.tw
```

win-acme With IIS

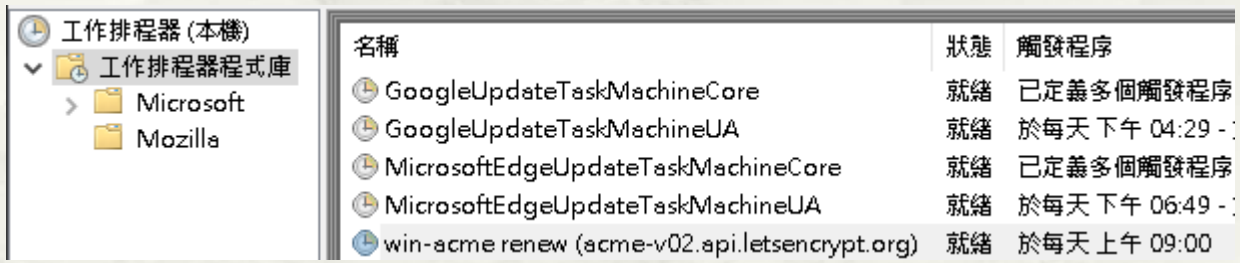


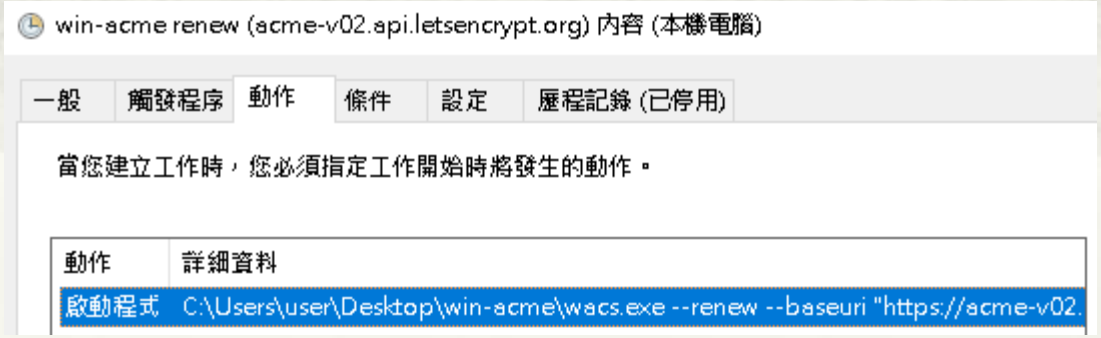
win-acme With IIS

* IIS

Auto Renew

- 在安裝完 win-acme 之後，win-acme 會自動在「工作排程器」建立一個排程，執行週期是每天
- 開始 > Windows 系統管理工具 >工作排程器





win-acme With IIS Background Steps

* Create .pfx and Import to Windows Cert Store
  * Private Key
  * Server Certificate
* IIS Config
* 工作排程器
  * Auto Renew Job

簡報完畢
謝謝