

HTTPS 憑證安裝 IIS

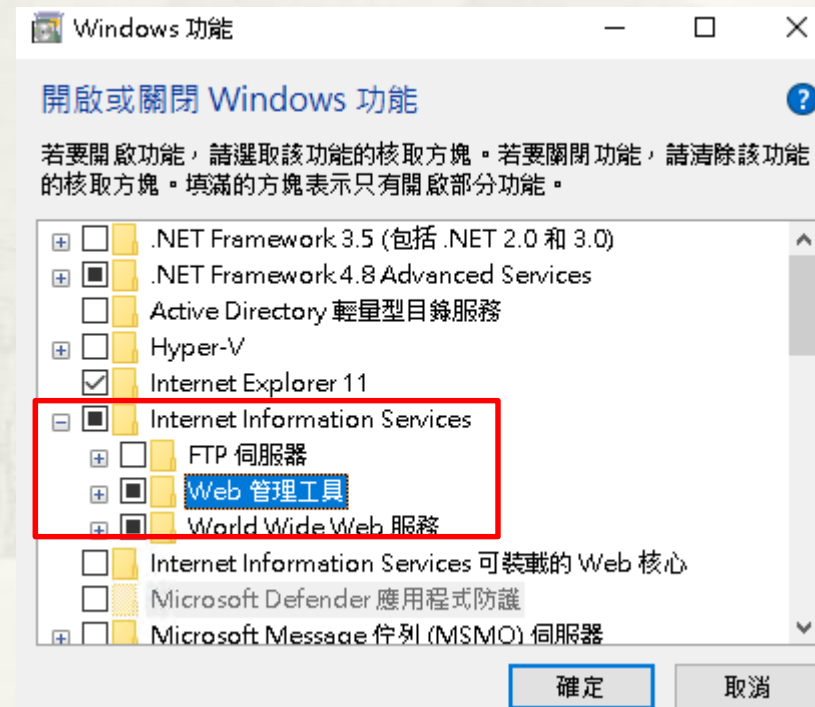
臺灣大學計資中心
網路組
游子興

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)



要求憑證

分辨名稱屬性

指定憑證的必要資訊。省份及縣市/位置必須指定成正式名稱，而且不能包含縮寫。

一般名稱(M):	devisyou.buda.idv.tw
組織(O):	NTU
組織單位(U):	CC
縣市/位置(L):	Taipei
省份(S):	Taiwan
國家/地區(R):	TW

Create CSR File

要求憑證



密碼編譯服務提供者內容

選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。不過，位元長度較大可能會降低效能。

密碼編譯服務提供者(S):

Microsoft RSA SChannel Cryptographic Provider

位元長度(B):

2048

要求憑證



檔案名稱

指定憑證要求的檔案名稱。這項資訊可傳送給憑證授權單位做為簽署之用。

指定憑證要求的檔案名稱(R):

C:\Users\user\Documents\server.txt

* CSR File



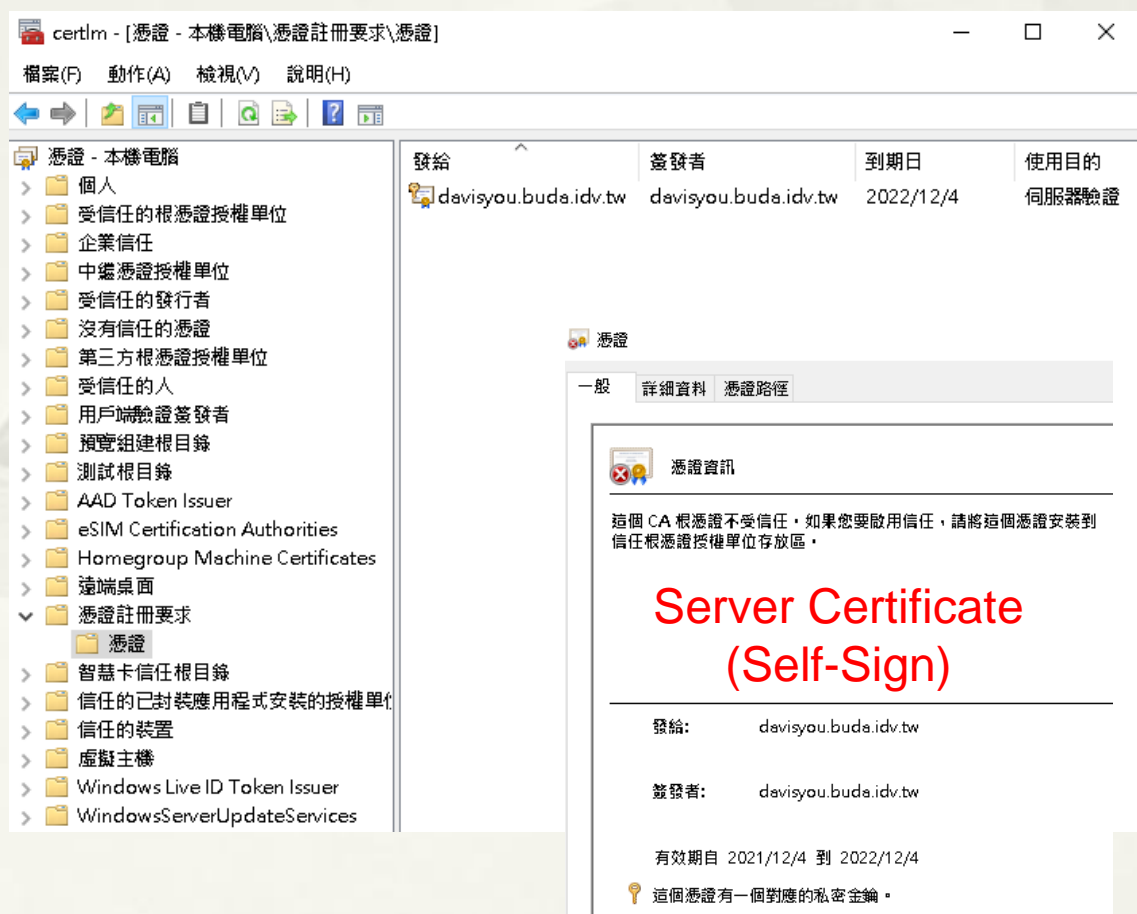
server.txt - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明

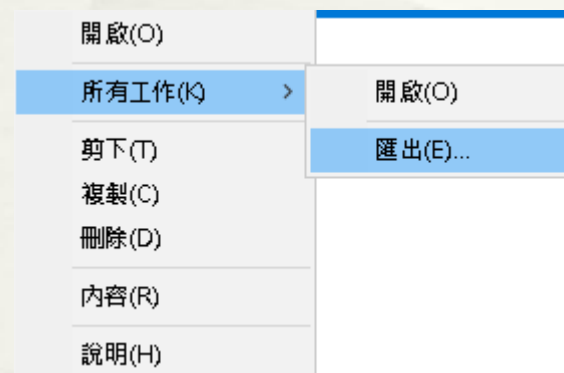
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEYDCCAQQCAQAwTELMAkGA1UEBhMCVFcxZANBgNVBAGMBIRhaXdhbjEPMAOG
A1UEBwwGVGFpcGVpMQwwCgYDVQQKDANOVFUxCzAJBgNVBAsMAkNDMROwGwYDVQQD
DBRkYXZpc3lvdS5idWRhLmlkdj50dzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALwB5CPWKCw+mE6MxGL93ZDXJesQ00JNHOSHQAaH2XzPPJmoBargPign
KfVvfi0h/c0vGh6a1dY3W7JgtSt5jhV+wFwnrtDLmcYfAESaWULy/HUneyanfoVy
z+u+Zirp2d2PAsxI8TNneWEEYyDSRIAIdNRhDAOGTk2XkeYYaAICbek3QA1HBZ6k
tXSGbIUSCFAz91UmLEjwabgzvKuY4VnbH+RfgCcd6onp7vmcnUw13Rc4BUa4IHRs
L1i7BfoPgDSoEnMOOw5PBLgLaFq+M6GVE0sbY7qXj9Qh2yBDbUCxKpHEMKLcmhmT
kgXD3Eb5s14wtGCk6YGYGk49DEHPF6kCAwEAAaCCAAwwHAYKKwYBBAGCNwOCAzEO
FgwMCA4wLjE5MDQzLjIwRgYJKwYBBAGCNxUUMTKwNwIBBQwPREVTS1RPUC1LREtO
M1FHDBRERVNLE9QLUtES04zUUdcdXNlcgwLSW51dElnci5leGUwcgYKKwYBBAGC
NwOCAjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAaAAgAFIAUwBBACAAUwBDAGgA
YQBuAG4AZQBsACAAQwByAHkACABOAG8AZwByAGEAcABOAGkAYwAgAFAAcBvAHYA
aQBkAGUAcmBADCzWYJKoZIhvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DAT
BgNVHSUEDDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMC
AgIAgDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMA5GCWCGSAF1AwQBLTAL
Bg1ghkgBZQMEAAQIwCwYJYIZIAWUDBAEFMaGBSsOAwIHMAoGCCqGSIb3DQMHBMBOG
A1UdDgQWBBT1CwD8kPrwcmU71EfDO/KGx7WPizANBgkqhkiG9w0BAQUFAAOCAQEA
NcabvM4wq4zGE/DzXOH8tfWJDpGNouXVOXVBhN3R3zL0mExw+flsXQHhZx5n3adg
GHZxnrbMX+HlpiquVLFbJVa61fUJ9wwSzR2OCiAoT59b6EsZRWWe5QDNEAIj4bte
372D7NspzDX2Ceh0heVxqiJHvn+mBM/oLcJAiidZ1FYCccZIUa2JCm1Mts/rCU
ovitrJsPKN54PDijXC+shqJy5Y3mwgC66IOAOBVUw+VtkCq91VTPaLVZif6+AAW
OShS955dFVAsOELEIzefyZcu3ZI0+VbgpvlQk73sA8JwUdqF7IMWUw9KWnRPc5Cy
5w17IsdH63cEH89/P6HQTg==
-----END NEW CERTIFICATE REQUEST-----
```

匯出 Server Certificate/Private Key

* certlm.msc (本機電腦)



* 匯出 Server Certificate



匯出私密金鑰

您可以選擇將私密金鑰與憑證一起匯出。

私密金鑰受到密碼的保護。如果您要將私密金鑰與憑證一起匯出，您必須在下一頁輸入密碼。

您想將私密金鑰與憑證一起匯出？

- ☐ 是，匯出私密金鑰(Y)
- ☒ 否，不要匯出私密金鑰(O)

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-----
MIIEHjCCAwagAwIBAgIQbdYyVlsh15VHGehc9dKD8TANBgkqhkiG9w0BAQUFADBP
MQswCQYDVQQGEwJUVzEPMAOGA1UECAwGVGFpd2FuMQ8wDQYDVQQHDAZUYWlwZWkx
DDAKBgNVBAoMA05UVTETMAkGA1UECwwCQ0MxHTAbBgNVBAMMFGRhmlzeW91LmJl
ZGEuaWR2LnR3MB4XDTE1MTIwNDA2NTgzMFoXDTE1MTIwNDA3MTgzMFowTELMAkG
A1UEBhMCVFcxZDZANBgNVBAgMB1RhaXdhbjEPMAOGA1UEBwwGVGFpcGVpMQwwCgYD
VQQKZANOVFVxZzAJBgNVBAsMAkNDMDR0wGwYDVQQDDBRkYXZpc3lvdS51dWRhLm1k
di50dzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALwB5CPWKCw+mE6M
xGL93ZDXJesQ00JNHOSHQAaH2XzPPJmoBargPignKfVvfioh/cOvGh6aldY3W7Jg
tSt5jhV+wFwnrtDLmcYfAESaWULy/HUneyanf0Vyz+u+Zirp2d2Pasx18TnneWEE
YyDSRialdNRhDA0gTk2XkeYYaA1Cbek3QA1HBZ6ktXSGb1USCFAz91UmLEjwabgz
vKuY4VnbH+RfgCcd6onp7vmcnUw13Rc4BUa41HRsL1i7BfoPgDSoEnMO0w5PBLgL
Afq+M6GVE0sbY7qXj9Qh2yBDbUCxKpHEMKLcMhmTkgXD3Eb5s14wtGCk6YGYGk49
DEHPF6kCAwEAAaOBwTCBvjAOBgNVHQ8BAf8EBAMCBPAwEwYDVR01BAwwCgYIKwYB
3QUHAwEwEAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAgICAIAwDgYIKoZIhvcN
AwQCAgCAMAsGCWCGSAF1AwQBKjALBg1ghkgBZQMEAS0wCwYJY1Z1AWUDBAECMAAG
CWCWCGSAF1AwQBBTAHBgUrdgMCBzAKBggqhkiG9w0DBzAdBgNVHQ4EFgQU5QsA/JD6
3HJ109RHwzvvyhse1j4swDQYJKoZIhvcNAQEFBQADggEBAQFBNHhZSkbQYwREVd1xBJ
VKPuycvAufnymSGNRqFRYQbhrGcb+kYJ5vwRd9J8ZzyROGZr0jrbesRHFZ1oiV1z
6rHv4uRUMssM4ZahY14D7+sPwwt0bUpBBqd/RxD814vFPx1Sfi+pYsjgCfwQa9Ba
7orIS7xGLG9kzPss54EgAq3HbLcib1lVtgEWMqBueQz1qkHdC9HuRrP/61KWY3oH
gGCnbl4EXCV5XZT6PTYWwGJM5D+YZckJ8qNZoNBVTgFfSYixrGPQkV1DCR+ry+Xu
bzb8v0Qo6EImsMe3cyGbSCEV02+pUyz+Ao4p9ZNtd7Tn4cla/dH/EmpL842fyQn
zy0=
-----END CERTIFICATE-----
```

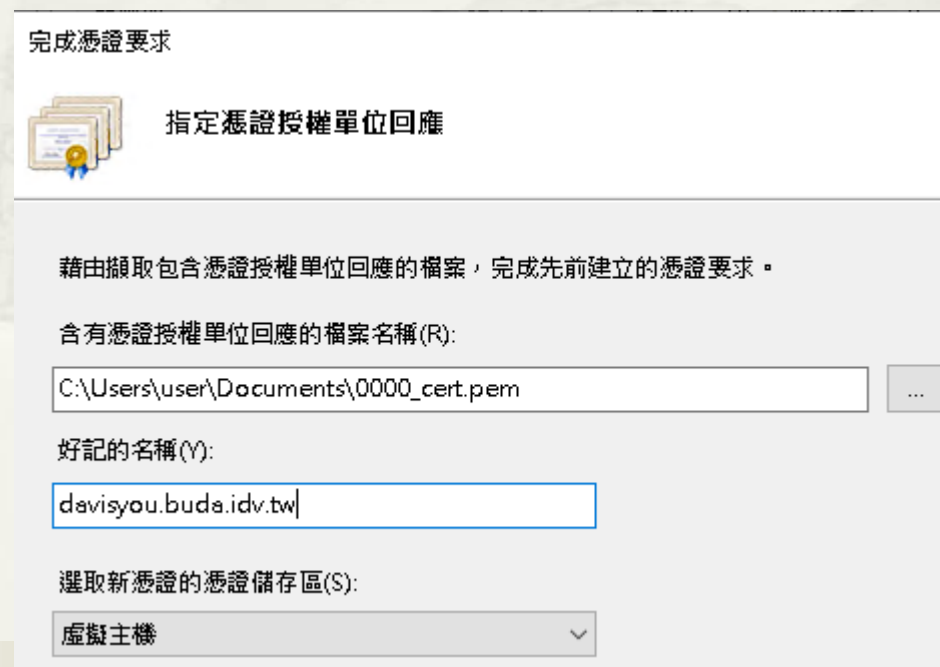
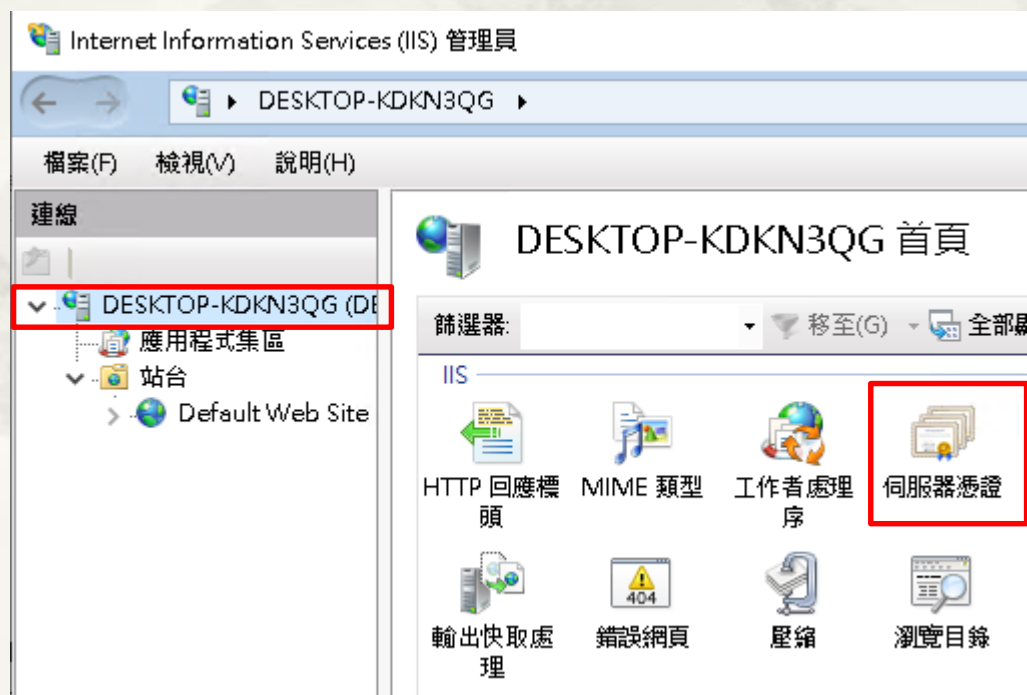

建立憑證要求

Background Steps

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

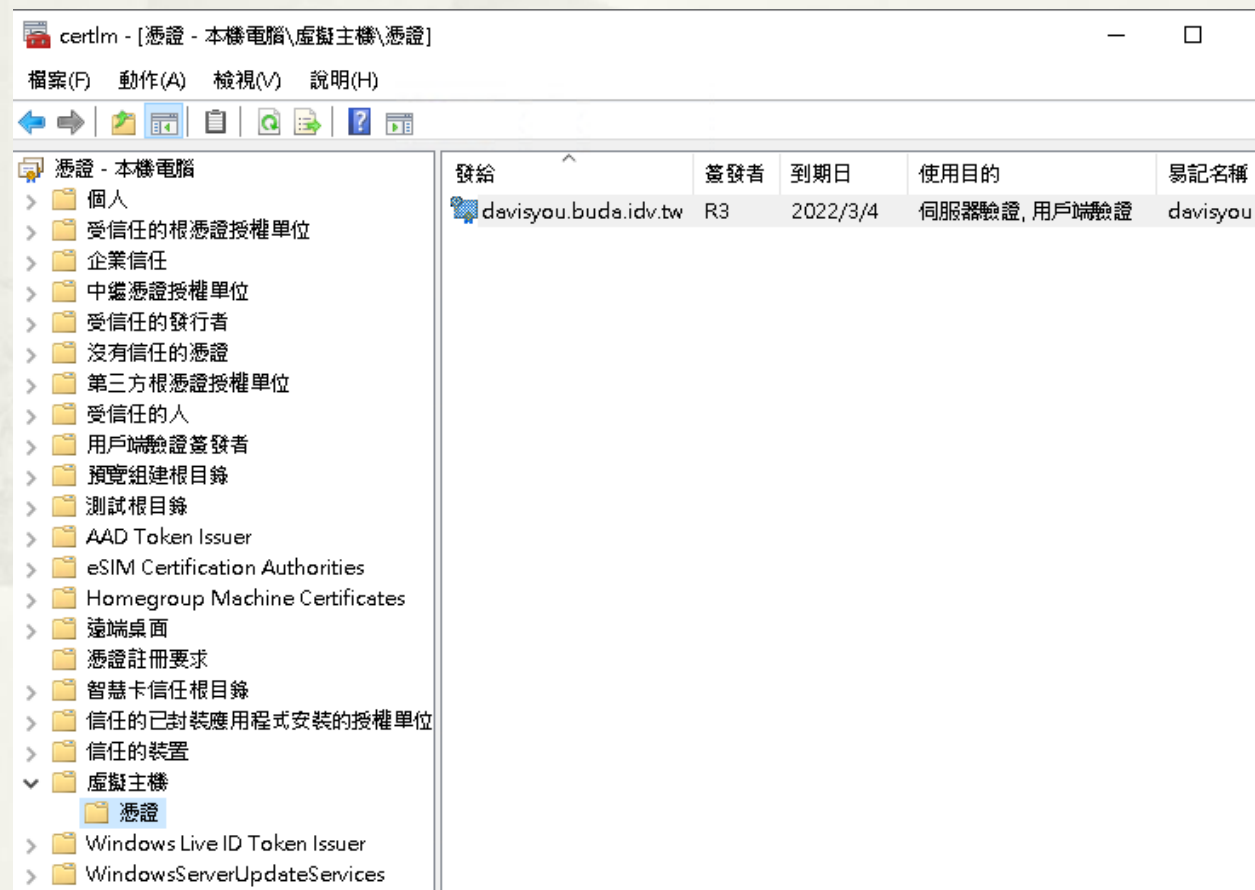
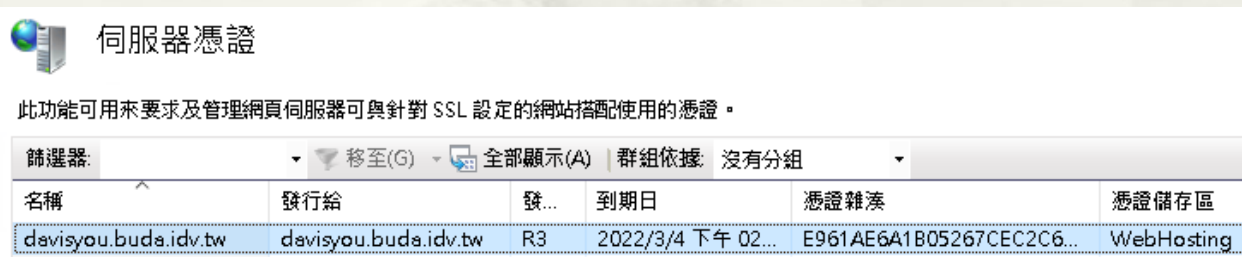
Import Server Certificate

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

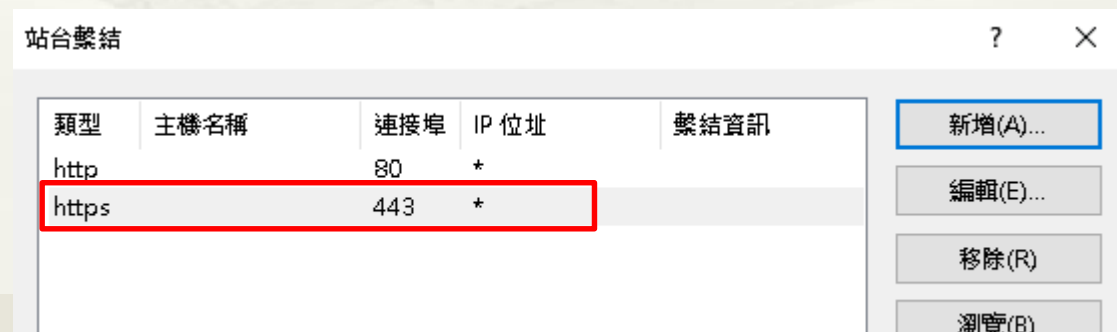
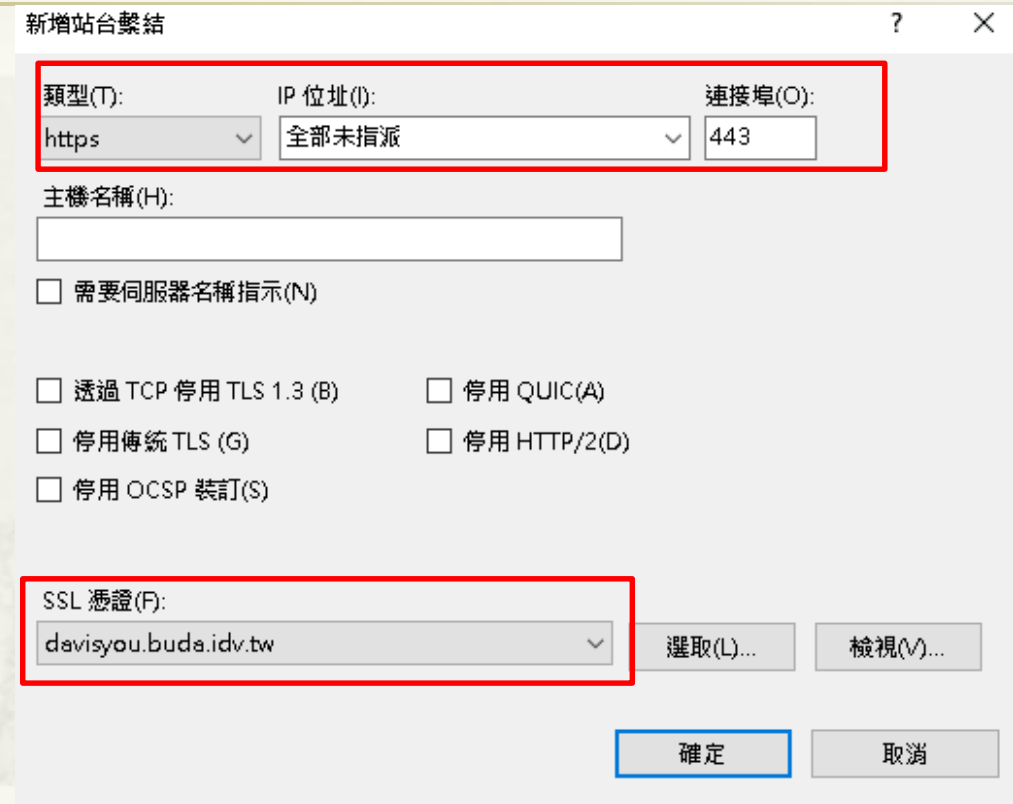
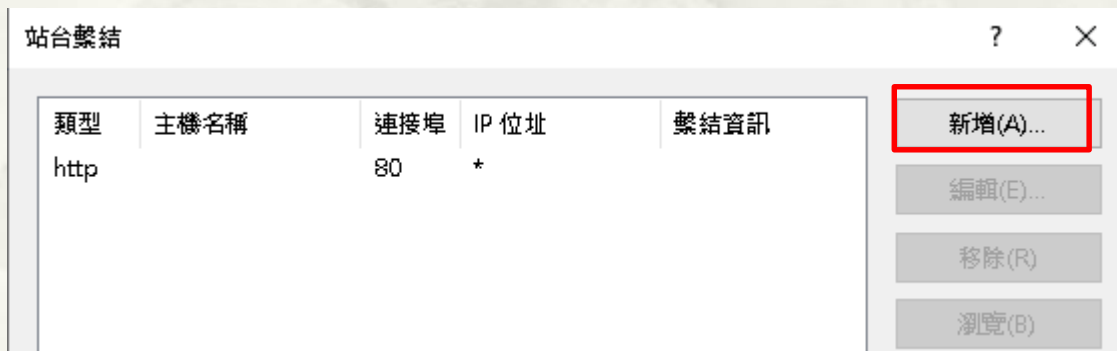


Import Server Certificate

* certlm.msc (本機電腦)

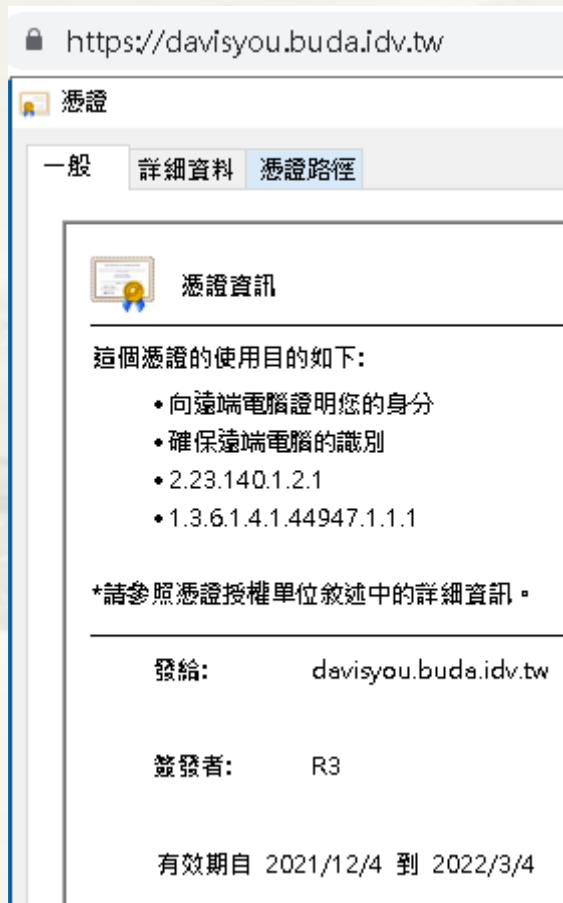


HTTPS Config



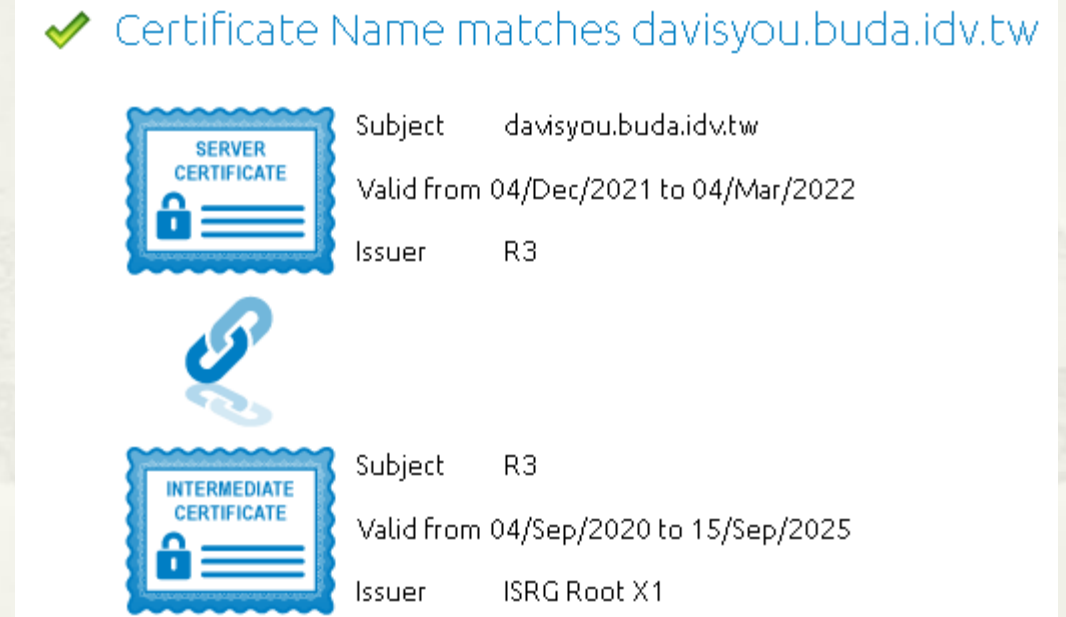
Check

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



* Certificate Chain

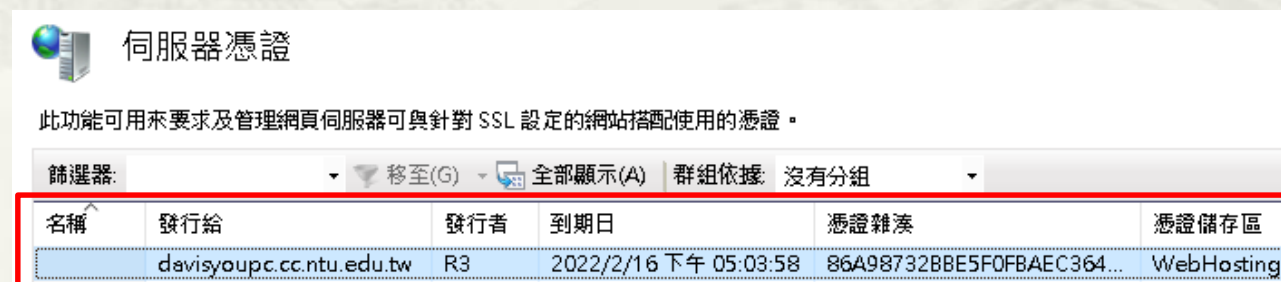
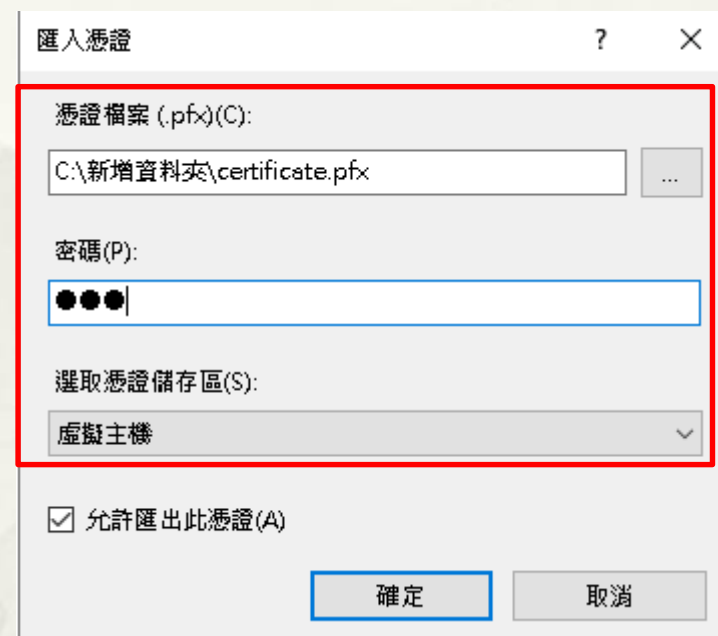
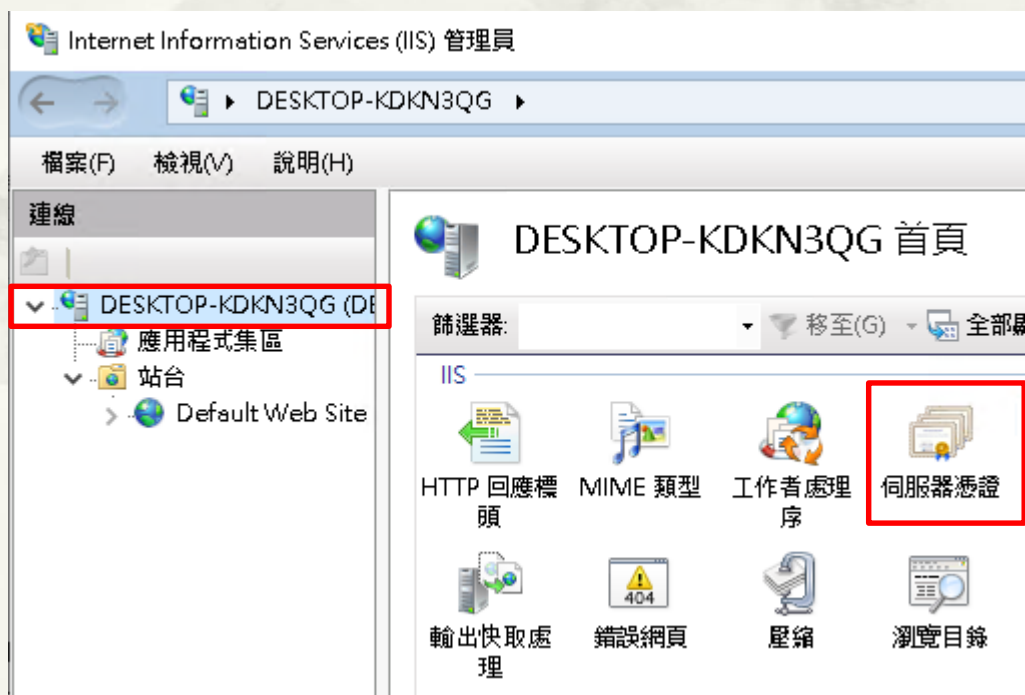
* <https://www.digicert.com/help/>



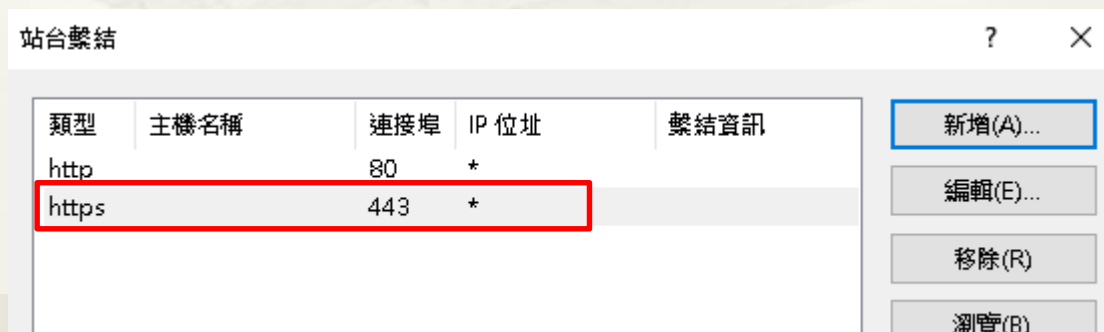
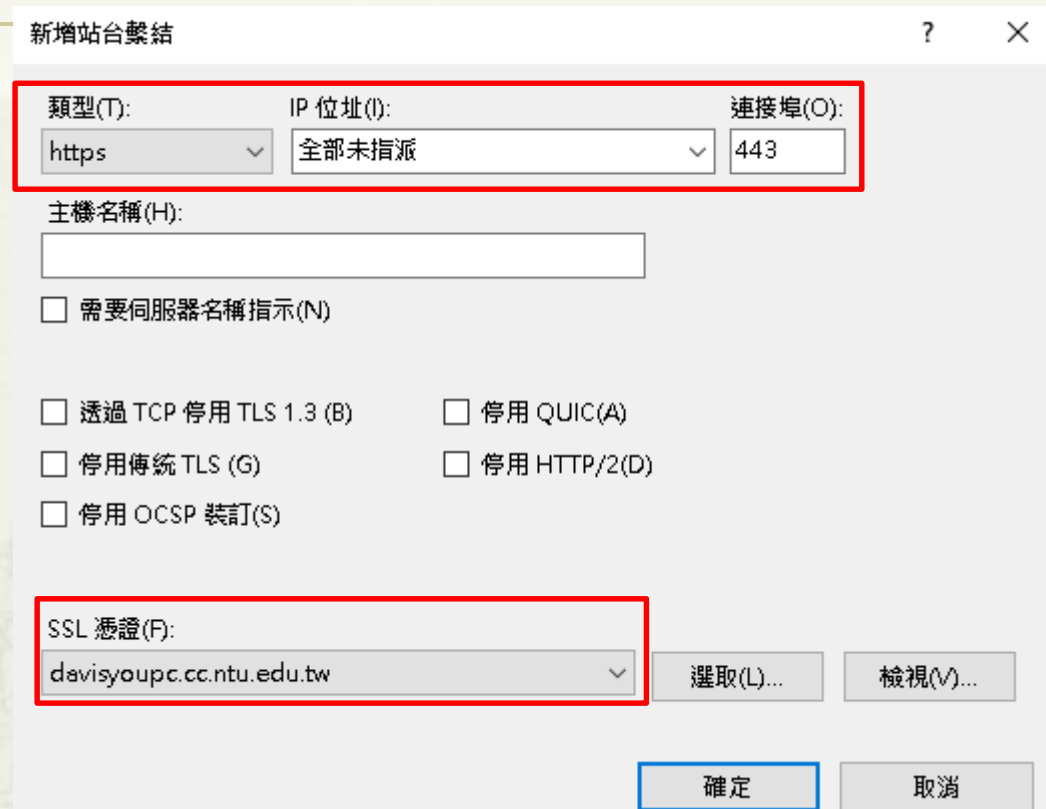
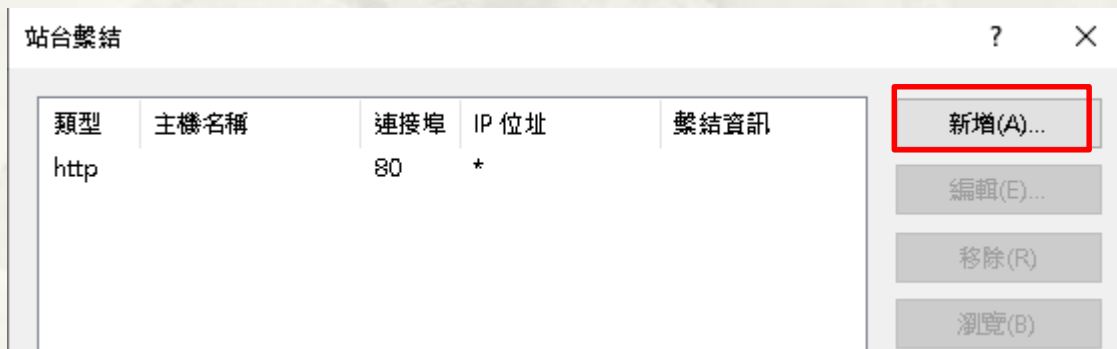
Manual Import .pfx (Certificate/Private Key)

Install Certificate

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



HTTPS Config



The background of the slide features a faint, stylized image of a traditional Chinese landscape painting, possibly a 'Shan Shui' (mountain-water) genre, rendered in a light, monochromatic tone. The painting is depicted as if it were a fan, with the landscape elements radiating from a central point at the bottom, creating a semi-circular shape. The scene includes misty mountains, a winding river or path, and small figures or structures, typical of classical Chinese ink wash art.

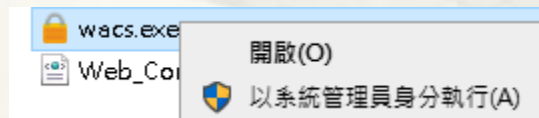
Install win-acme

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



The background of the slide features a large, light-colored fan shape. Inside the fan is a detailed, monochromatic illustration of a traditional East Asian landscape, showing mountains, trees, and a winding path. The fan is set against a plain, light background.

win-acme Without IIS

win-acme Without IIS

```
CA\ 系統管理員: 命令提示字元 - wacs
C:\Users\user\Desktop\acme>wacs

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
Source plugin IIS not available: No supported version of IIS detected.

Please specify how the list of domain names that will be included in the
certificate should be determined. If you choose for one of the "all bindings"
options, the list will automatically be updated for future renewals to
reflect the bindings at that time.

1: Read bindings from IIS
2: Manual input
3: CSR created by another program
C: Abort

How shall we determine the domain(s) to include in the certificate?: 2

Description:      A host name to get a certificate for. This may be a
                  comma-separated list.

Host: davisyoupc.cc.ntu.edu.tw
```

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

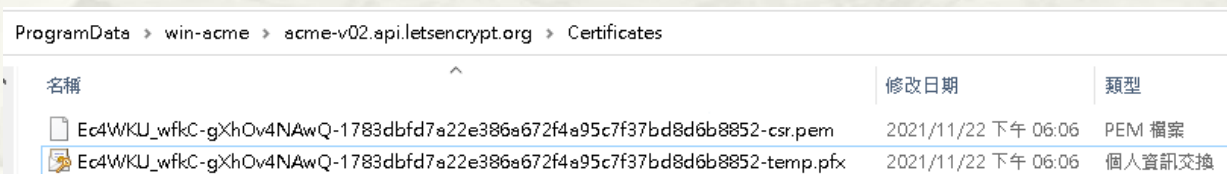
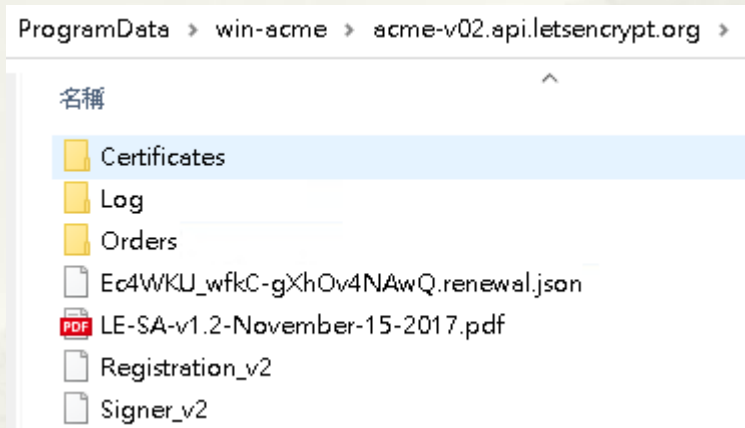
```
[davisyoupc.cc.ntu.edu.tw] Authorizing...
[davisyoupc.cc.ntu.edu.tw] Authorizing using http-01 validation (SelfHosting)
[davisyoupc.cc.ntu.edu.tw] Authorization result: valid
Downloading certificate [Manual] davisyoupc.cc.ntu.edu.tw
Store with CertificateStore...
Installing certificate in the certificate 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

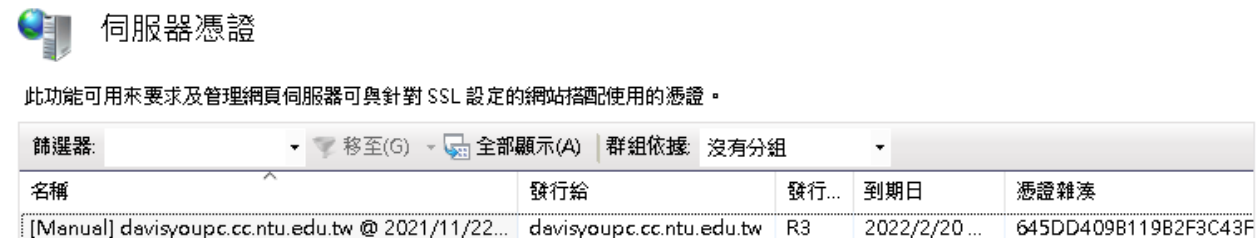


* certlm.msc (本機電腦)

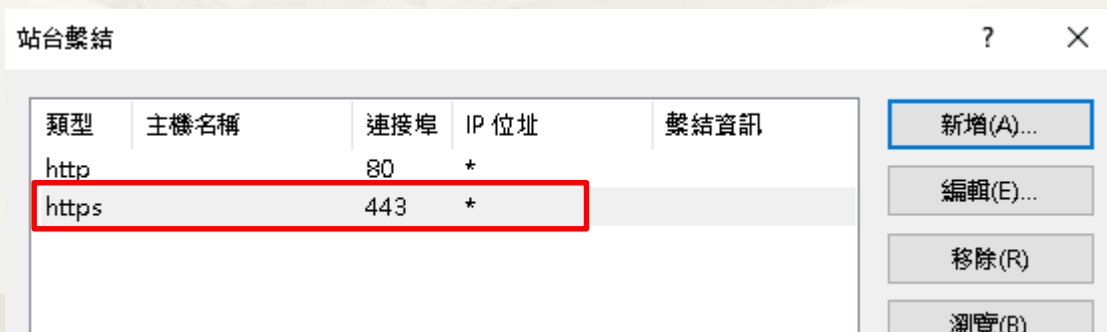
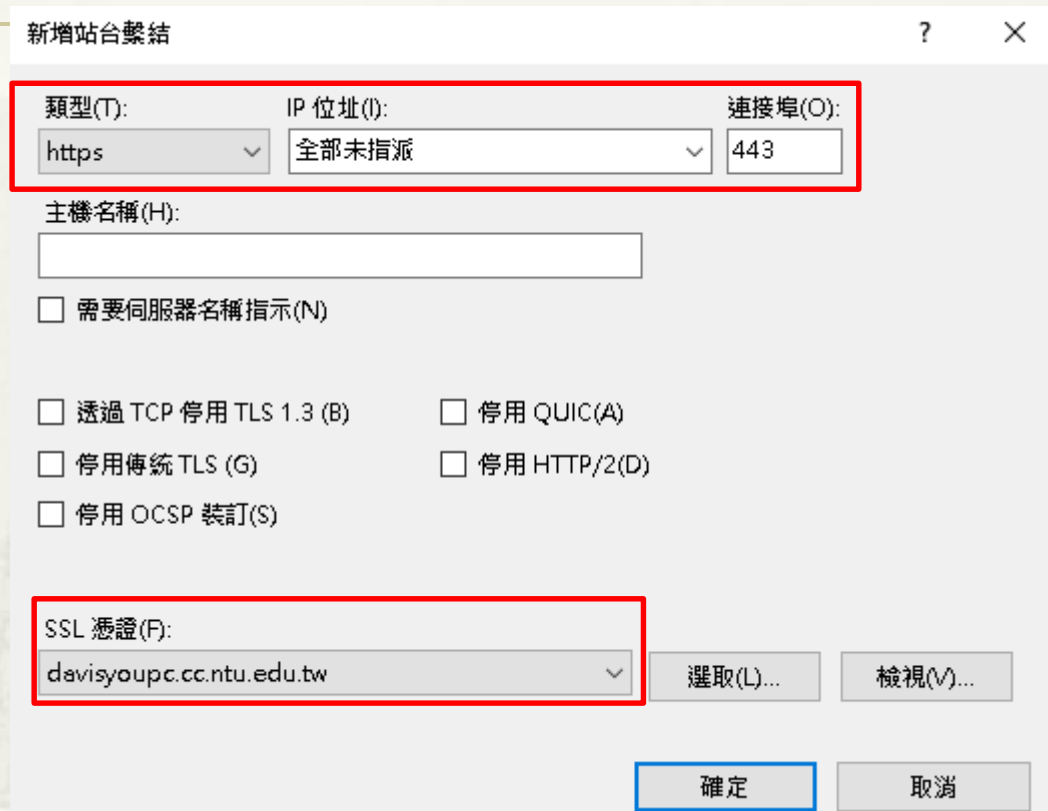
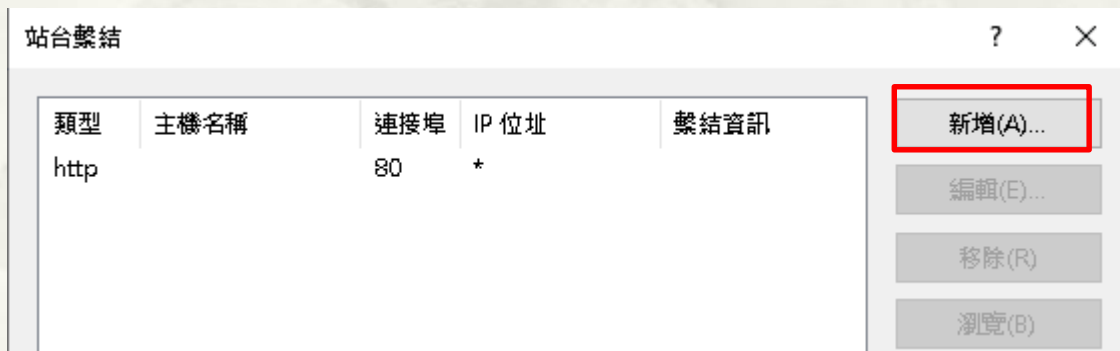
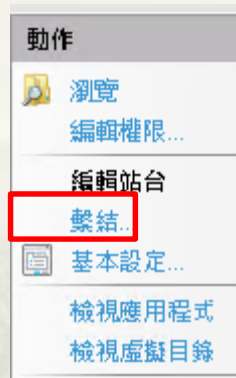
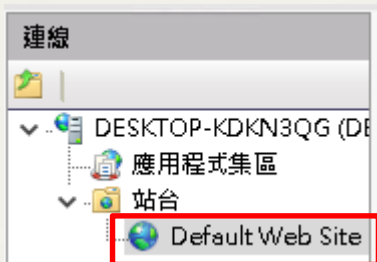


* 安裝 IIS

* 伺服器憑證已安裝

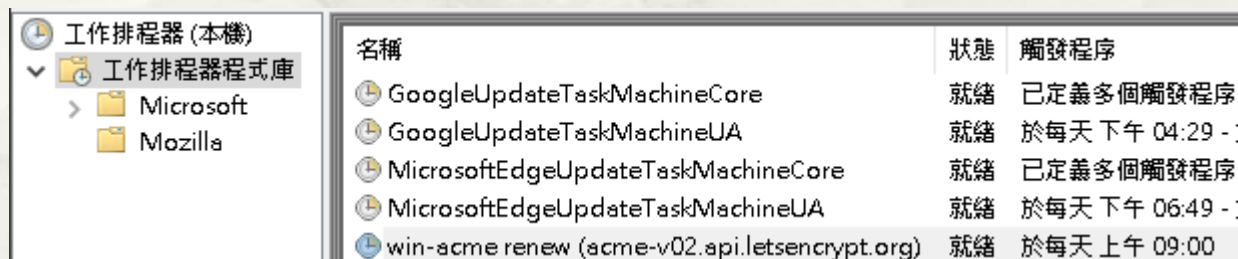


HTTPS Config



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




名稱	狀態	觸發程序
GoogleUpdateTaskMachineCore	就緒	已定義多個觸發程序
GoogleUpdateTaskMachineUA	就緒	於每天下午 04:29 - 05:00
MicrosoftEdgeUpdateTaskMachineCore	就緒	已定義多個觸發程序
MicrosoftEdgeUpdateTaskMachineUA	就緒	於每天下午 06:49 - 07:00
win-acme renew (acme-v02.api.letsencrypt.org)	就緒	於每天上午 09:00



win-acme Without IIS

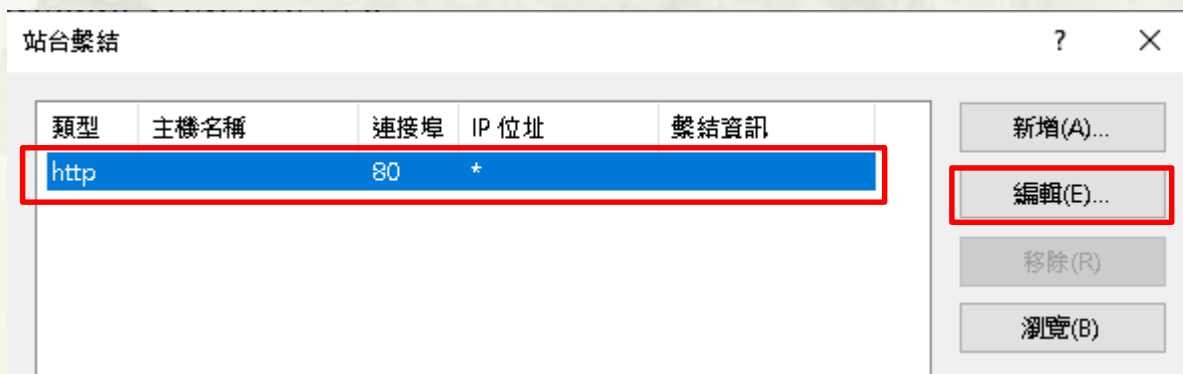
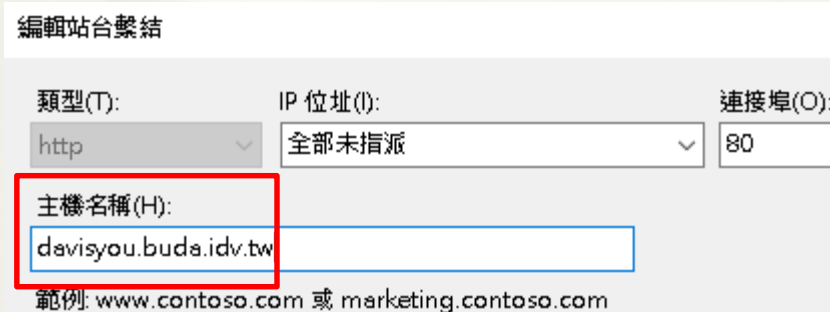
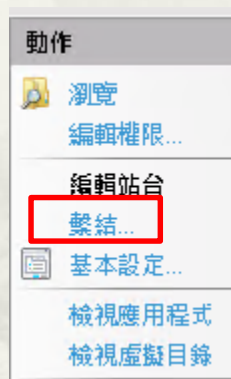
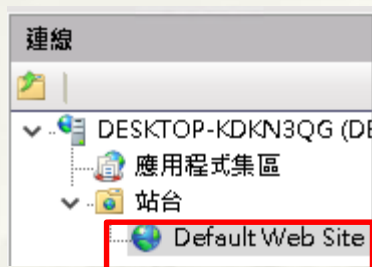
Background Steps

- * 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

```
[davisyou.buda.idv.tw] Authorizing...
[davisyou.buda.idv.tw] Authorizing using http-01 validation (SelfHosting)
[davisyou.buda.idv.tw] Authorization result: valid
Downloading certificate [IIS] (any site), (any host)
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [IIS] (any site), (any host) @ 2021/11/22 18:50:34 to store WebHosting
Installing with IIS...
Adding new https binding *:443:davisyou.buda.idv.tw
Committing 1 https binding changes to IIS
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\Users\user\Desktop\win-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 [IIS] (any site), (any host)
Next renewal scheduled at 2022/1/16 18:50:10
Certificate [IIS] (any site), (any host) 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 With IIS

* IIS

 伺服器憑證

此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。

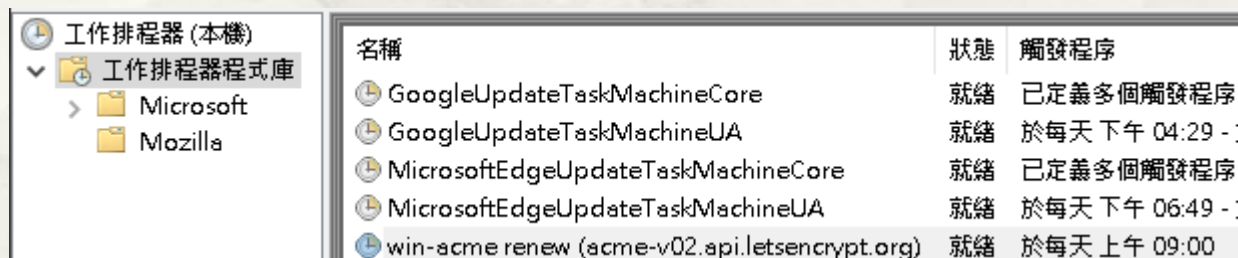
篩選器: 移至(G) 全部顯示(A) 群組依據: 沒有分組

名稱	發行給	發行者	到期日	憑證雜湊	憑證儲存區
[IIS] (any site), (any host) @ 2021/11/22 1...	davisyoudv.tw	R3	2022/2/20 下午 0...	20951638AB91DE57EB69B...	WebHosting

站台繫結				
類型	主機名稱	連接埠	IP 位址	繫結資訊
http	davisyoudv.tw	80	*	
https	davisyoudv.tw	443	*	

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




名稱	狀態	觸發程序
GoogleUpdateTaskMachineCore	就緒	已定義多個觸發程序
GoogleUpdateTaskMachineUA	就緒	於每天下午 04:29 - 05:00
MicrosoftEdgeUpdateTaskMachineCore	就緒	已定義多個觸發程序
MicrosoftEdgeUpdateTaskMachineUA	就緒	於每天下午 06:49 - 07:00
win-acme renew (acme-v02.api.letsencrypt.org)	就緒	於每天上午 09:00



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