คู่มือการติดตั้ง Certificate SSL

1. ตัวอย่างการติดตั้ง SSL certificate บนระบบปฏิบัติการ Centos (nginx)

1.1.ติดตั้ง โมดูล mod_ssl

พิมพ์คำสั่ง # yum install mod_ssl

1.2.Upload ไฟล์ certificate ขึ้นเว็บ server ประกอบด้วยไฟล์

- certificate2024.pem copy them to path /etc/pki/tls/certs/
- PrivateKey2024.key copy them to path /etc/pki/tls/private/
- IntermediateCA2024.crt copy them to path /etc/pki/tls/certs/

3.ทำการติดตั้ง SSL โดยเข้าไปแก้ไขไฟล์ ssl.conf ใน apache ที่ path /etc/httpd/conf.d/ssl.conf

(แก้ไข document root และ servername ให้ถูกต้อง)

```
<VirtualHost *:443>
DocumentRoot "/var/www/html"
ServerName its.sut.ac.th:443

ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

SSLEngine on
SSLProtocol +TLSv1.2
SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
SSLCertificateFile /etc/pki/tls/certs/certificate2024.pem
SSLCertificateKeyFile /etc/pki/tls/private/PrivateKey2024.key
SSLCertificateChainFile /etc/pki/tls/certs/IntermediateCA2024.crt

<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
```

ระบุ **version** การเข้ารหัส (**TLS V.1.2** ขึ้นไป) ไม่ควรระบุ **ALL** หรือ **SSLV2 SSLV3 TLS1 TSL1.1** (ยกเลิกการใช้งานเนื่องจากไม่ปลอดภัย)

```
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>

BrowserMatch "MSIE [2-5]" \
        nokeepalive ssl-unclean-shutdown \
        downgrade-1.0 force-response-1.0

CustomLog logs/ssl_request_log \
         "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

</VirtualHost>
```

1.4 ใช้คำสั่ง restart Apache

พิมพ์คำสั่ง # service httpd restart

2. ตัวอย่างการติดตั้ง SSL certificate บนระบบปฏิบัติการ Ubuntu (Apache)

2.1 Upload ไฟล์ certificate ขึ้นเว็บ server ประกอบด้วยไฟล์

- certificate2024.pem copy them to path /etc/ssl/certs/
- PrivateKey2024.key copy them to path /etc/ssl/private/
- IntermediateCA2024.crt copy them to path /etc/apache2/ssl.crt/

2.2 แก้ไขไฟล์ Apache VirtualHost ที่ path /etc/apache2/sites-available/default-ssl.conf

```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
            ServerAdmin webmaster@localhost
            ServerName idm.sut.ac.th:443
            DocumentRoot /var/www/html
            ErrorLog ${APACHE_LOG_DIR}/error.log
            CustomLog ${APACHE_LOG_DIR}/access.log combined

            #   SSL Engine Switch:
            #   Enable/Disable SSL for this virtual host.
            SSLEngine on
            SSLProtocol +TLSv1.2
            SSLCertificateFile      /etc/ssl/certs/certificate2024.pem
            SSLCertificateKeyFile /etc/ssl/private/PrivateKey2024.key
            SSLCertificateChainFile /etc/apache2/ssl.crt/IntermediateCA2024.crt

            <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
            </FilesMatch>
            <Directory /usr/lib/cgi-bin>
                        SSLOptions +StdEnvVars
            </Directory>

            BrowserMatch "MSIE [2-6]" \
```

```
                    nokeepalive ssl-unclean-shutdown \
                    downgrade-1.0 force-response-1.0
            # MSIE 7 and newer should be able to use keepalive
            BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown


    </VirtualHost>
</IfModule>
```

2.3 ใช้คำสั่ง restart Apache

พิมพ์คำสั่ง # sudo service apache2 restart

3. ตัวอย่างการติดตั้ง SSL certificate บนระบบปฏิบัติการ Centos (Nginx)

3.1 Upload ไฟล์ certificate ขึ้นเว็บ server ประกอบด้วยไฟล์

- certificate2024.pem copy them to path /etc/ssl
- PrivateKey2024.key copy them to path /etc/ssl
- IntermediateCA2024.crt copy them to path /etc/ssl

3.2 แก้ไขไฟล์ virtual.conf ที่ path /etc/nginx/conf.d/virtual.conf

```
server {
    listen       443;
        ssl    on;
        ssl_certificate    /etc/ssl/certificate2024.pem;
        ssl_certificate_key    /etc/ssl/PrivateKey2024.key;
        ssl_protocols TLSv1.2;
        server_name  web.sut.ac.th;
        access_log /var/log/nginx/nginx.web.log;
        error_log /var/log/nginx/nginx.web.error.log;

location / {
        root   /var/www/html;
```

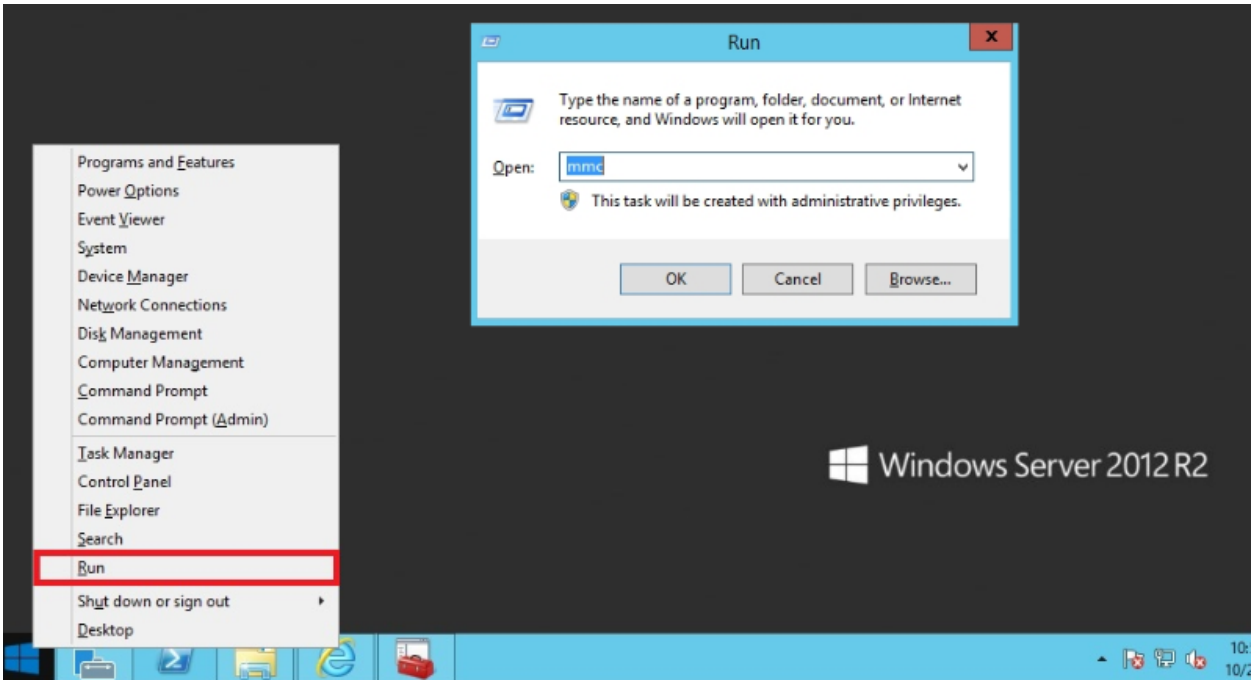
```
        index index.php index.html index.htm;
        try_files $uri $uri/ /index.php?$args;
        }

location ~ \.php$ {
        root   /var/www/html;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass unix:/var/run/php-fpm/php-fpm.sock;
        fastcgi_index index.php;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        fastcgi_param SCRIPT_NAME $fastcgi_script_name;
        }
}
```

3.3 ใช้คำสั่ง restart nginx&php

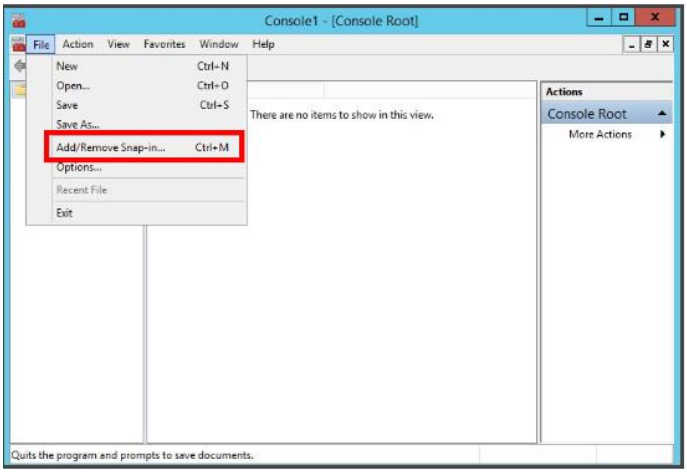
พิมพ์คำสั่ง # service nginx restart && service php-fpm restart

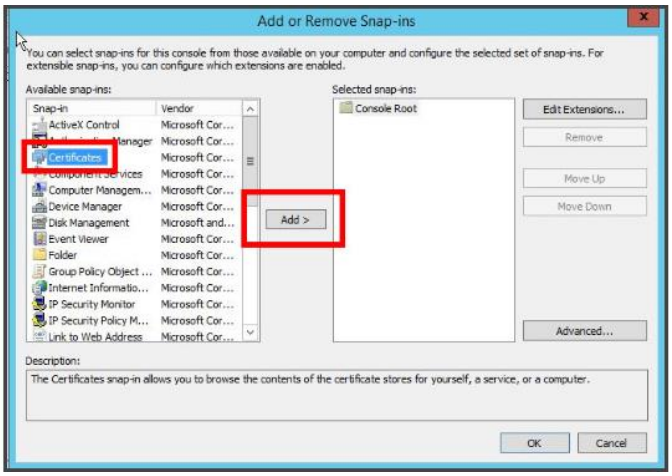
4. ตัวอย่างการติดตั้ง SSL Certificate สำหรับ windows server (อ้างอิง Windows Server 2012)

4.1. เข้าสู่ Microsoft Management Console (MMC) โดยไปที่ run >> mmc

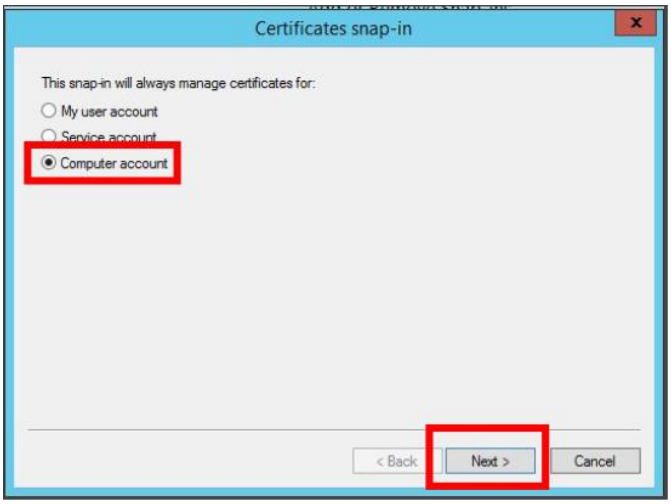


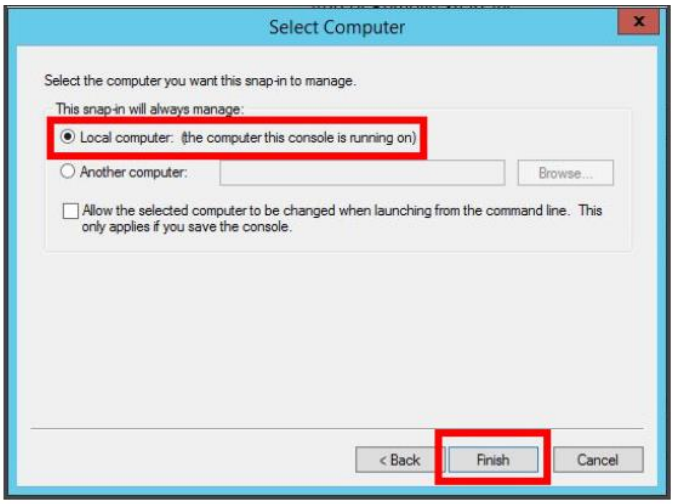
4.2 เลือกที่เมนู File >> Add/Remove Snap-in >> เลือก Certificates และกด Add



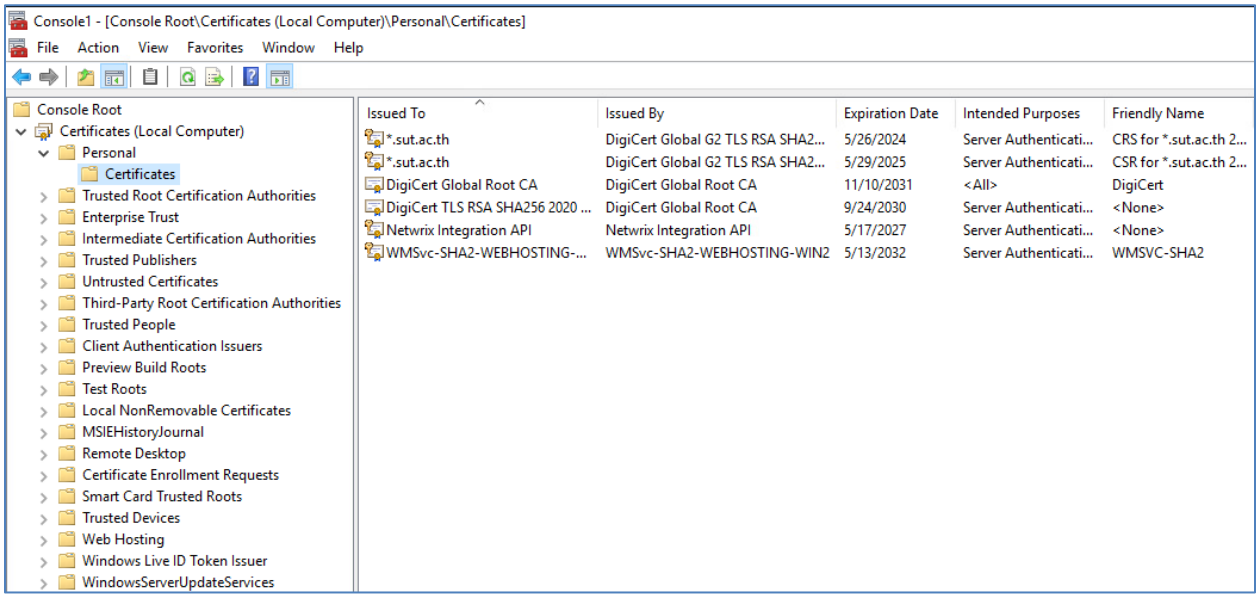


4.3 เลือก Computer Account >> Next >> Local Computer >> Finish



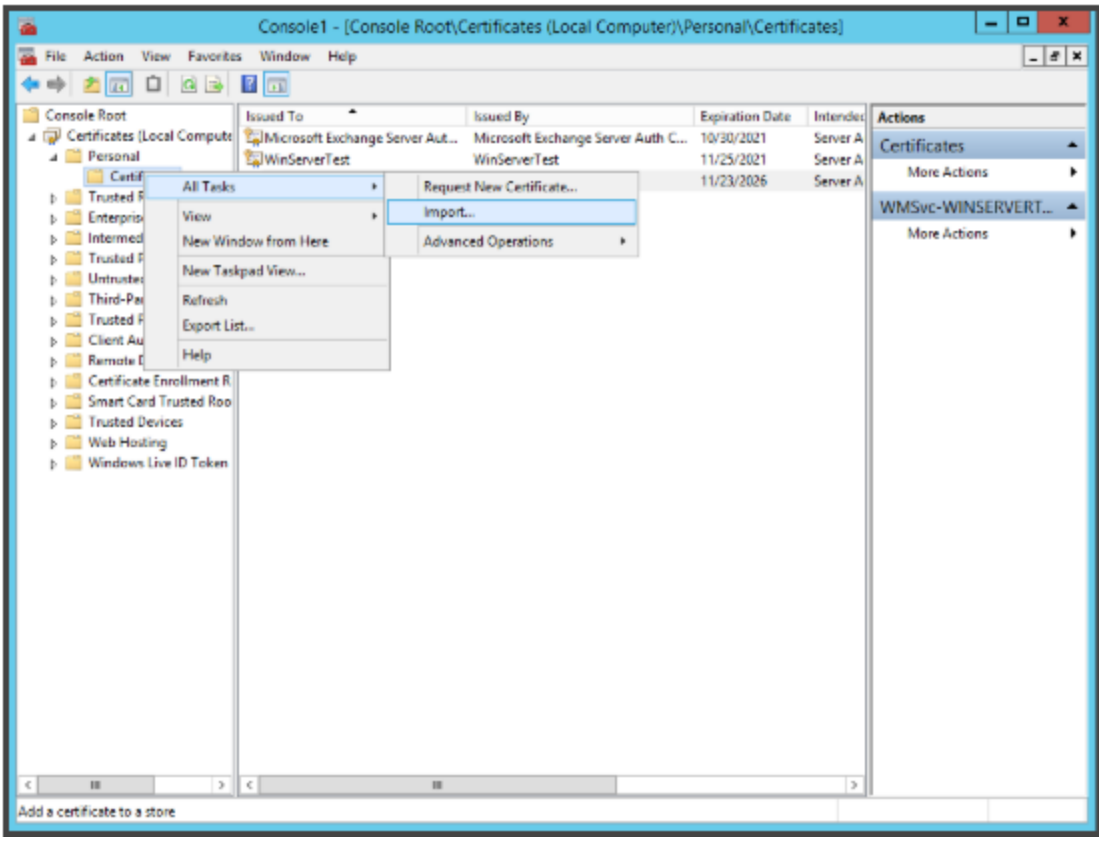


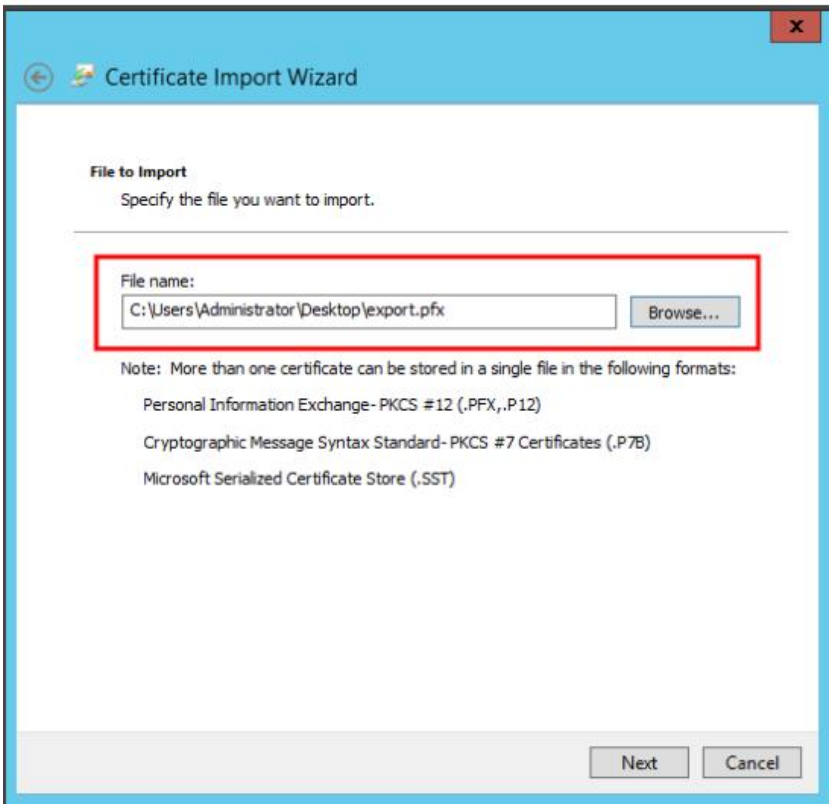
4.4. จากนั้น ไปที่หน้าหลักของ Microsoft Management Console (MMC) แล้วไปที่ Certificates (Local Computer) >> Personal >> Certificates ดังรูป



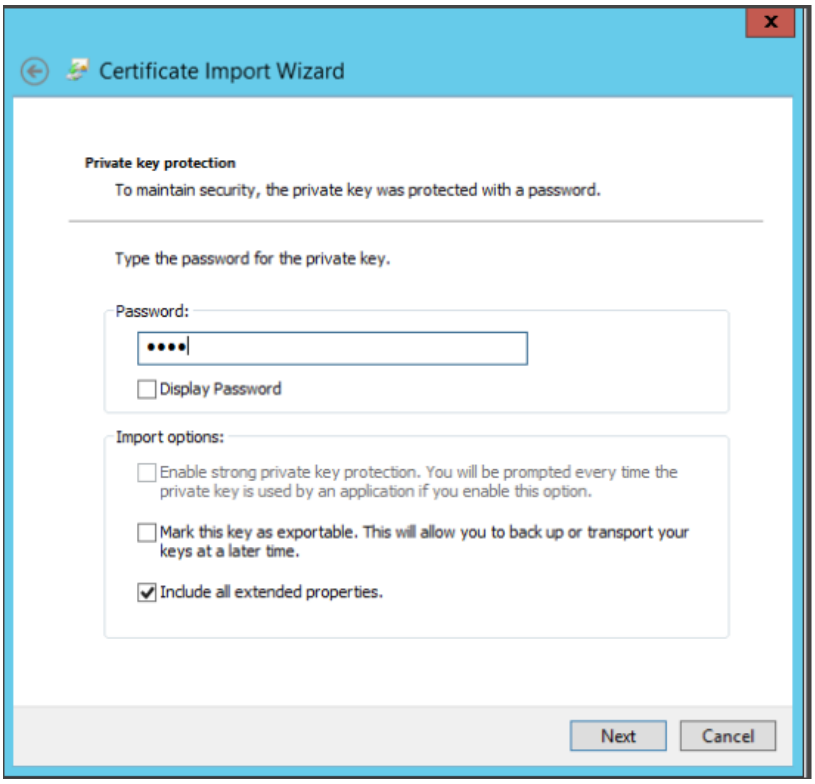
4.5 คลิกขวาที่โฟลเดอร์ Certificates ที่อยู่ภายใต้ Personal เลือก All task >> Import

จากนั้น เลือกไฟล์ .pfx จาก ที่เตรียมไว้ แล้วกด Next

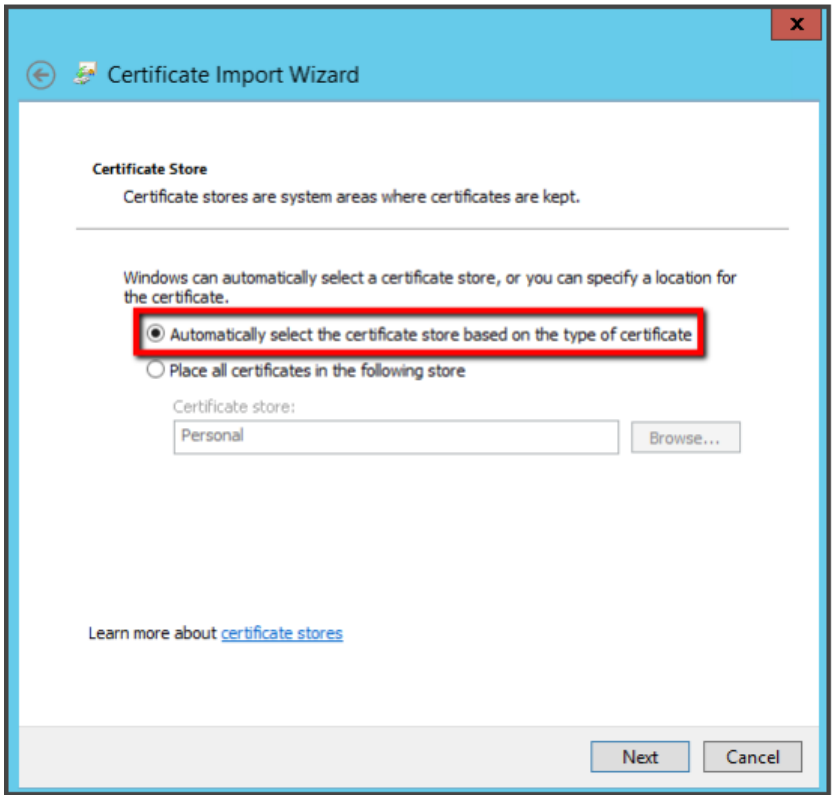




4.6 ทำการใส่รหัสผ่านที่ได้รับจากศูนย์คอมพิวเตอร์

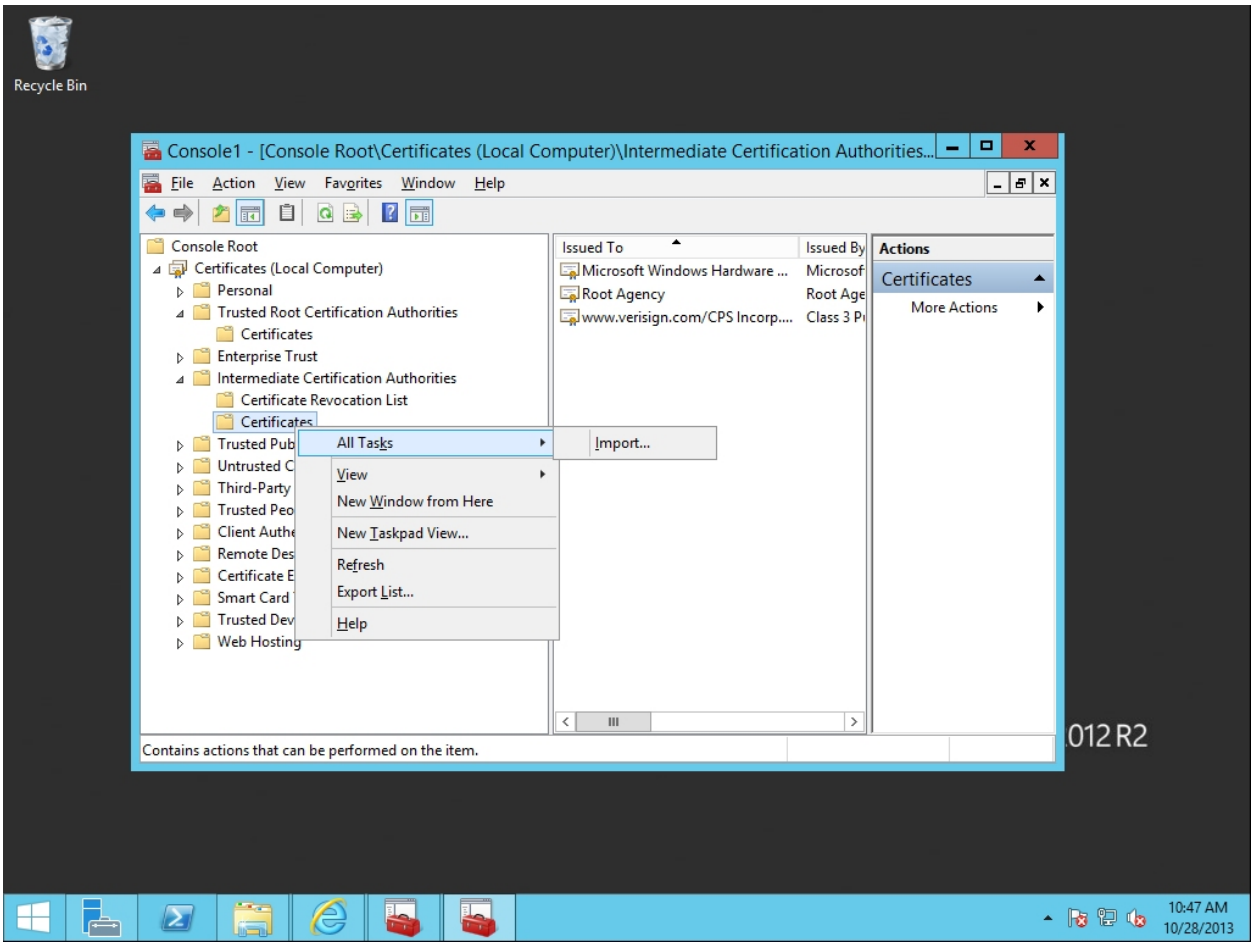


4.7. เลือก “Automatically select the certificate store based on the type of certificate” จากนั้นกด Next เมื่อถึงหน้า Completing the Certificate Import Wizard กด Finish

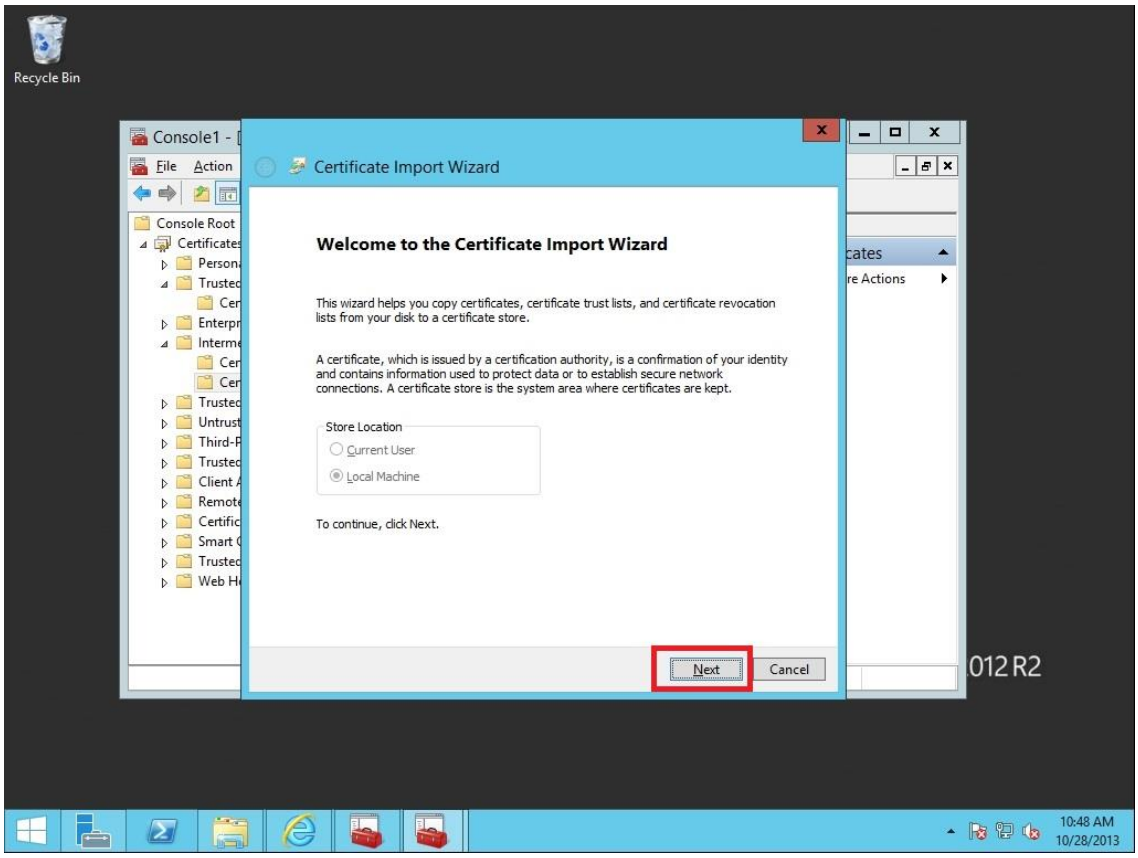


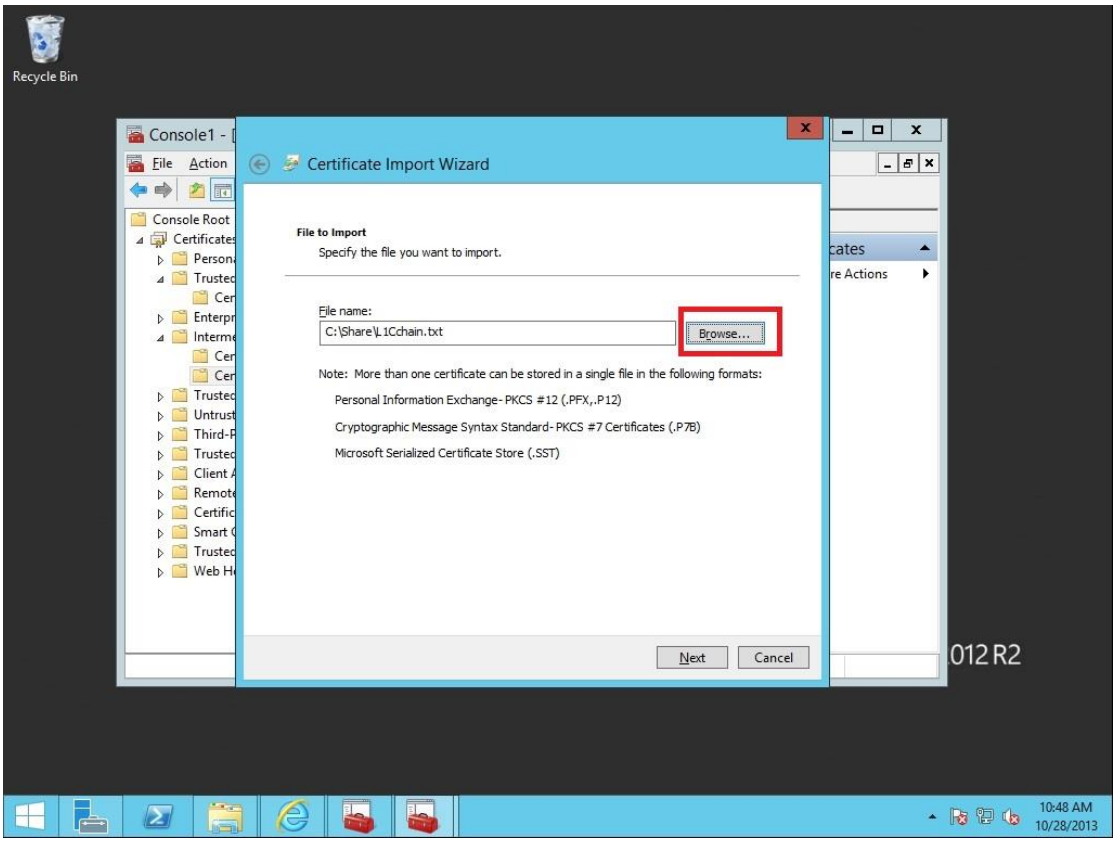
4.8. ขั้นตอนต่อมา ทำการติดตั้ง Intermediate CA โดยไปที่ MMC Console > Certificates (Local Computer) ที่เปิดไว้ก่อนหน้านี้

4.9. ที่หน้าหลัก ให้คลิกที่ Certificates (Local Computer) >> เลือก “Intermediate Certification Authorities >> Certificate” จากนั้นคลิกขวา All Tasks >> Import

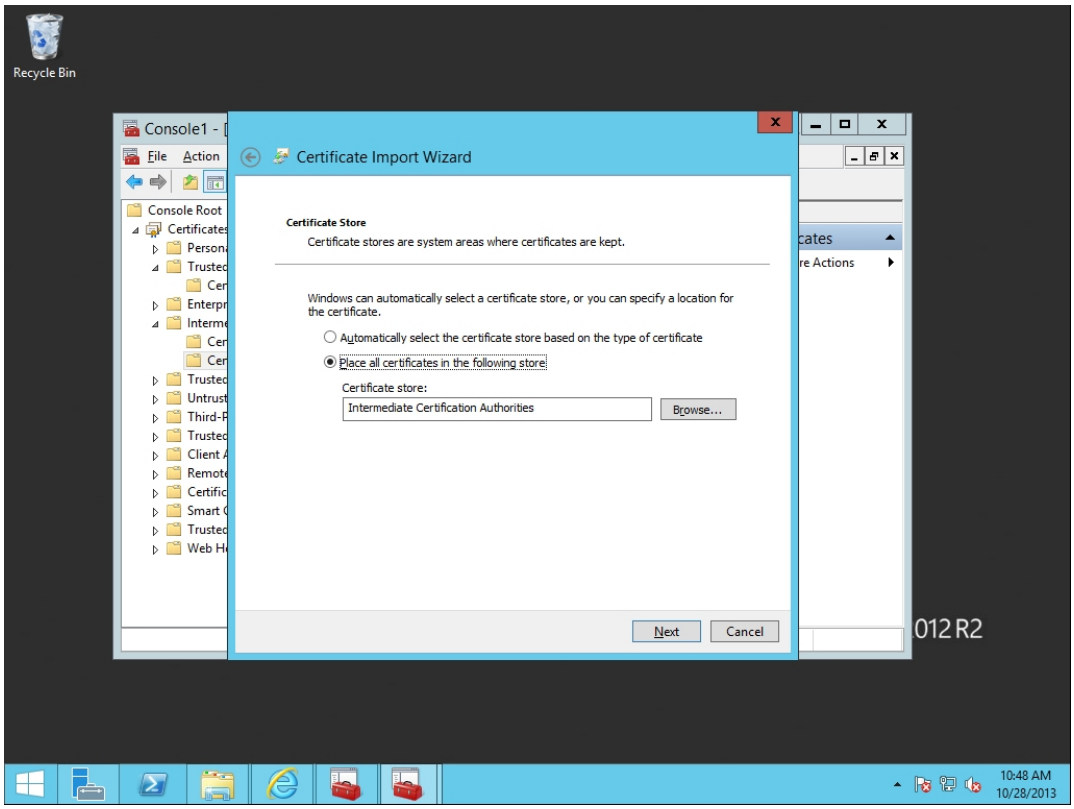


4.10. เมื่อเข้าสู่หน้าแรกในการ Import กด Next จากนั้นเลือกที่ตั้งไฟล์ Intermediate CA

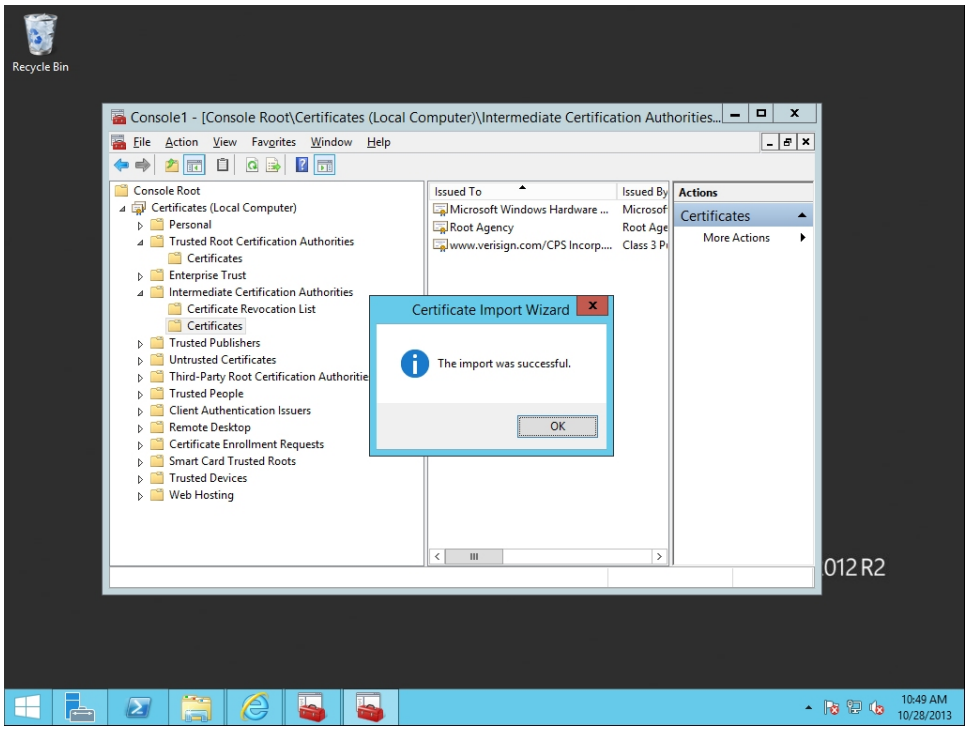

Recycle Bin
Console1 -
File Action
Console Root
Certificates
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel
012 R2
10:48 AM
10/28/2013


Recycle Bin
Console1 -
File Action
Console Root
Certificates
Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Share\L1Cchain.txt
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel
012 R2
10:48 AM
10/28/2013

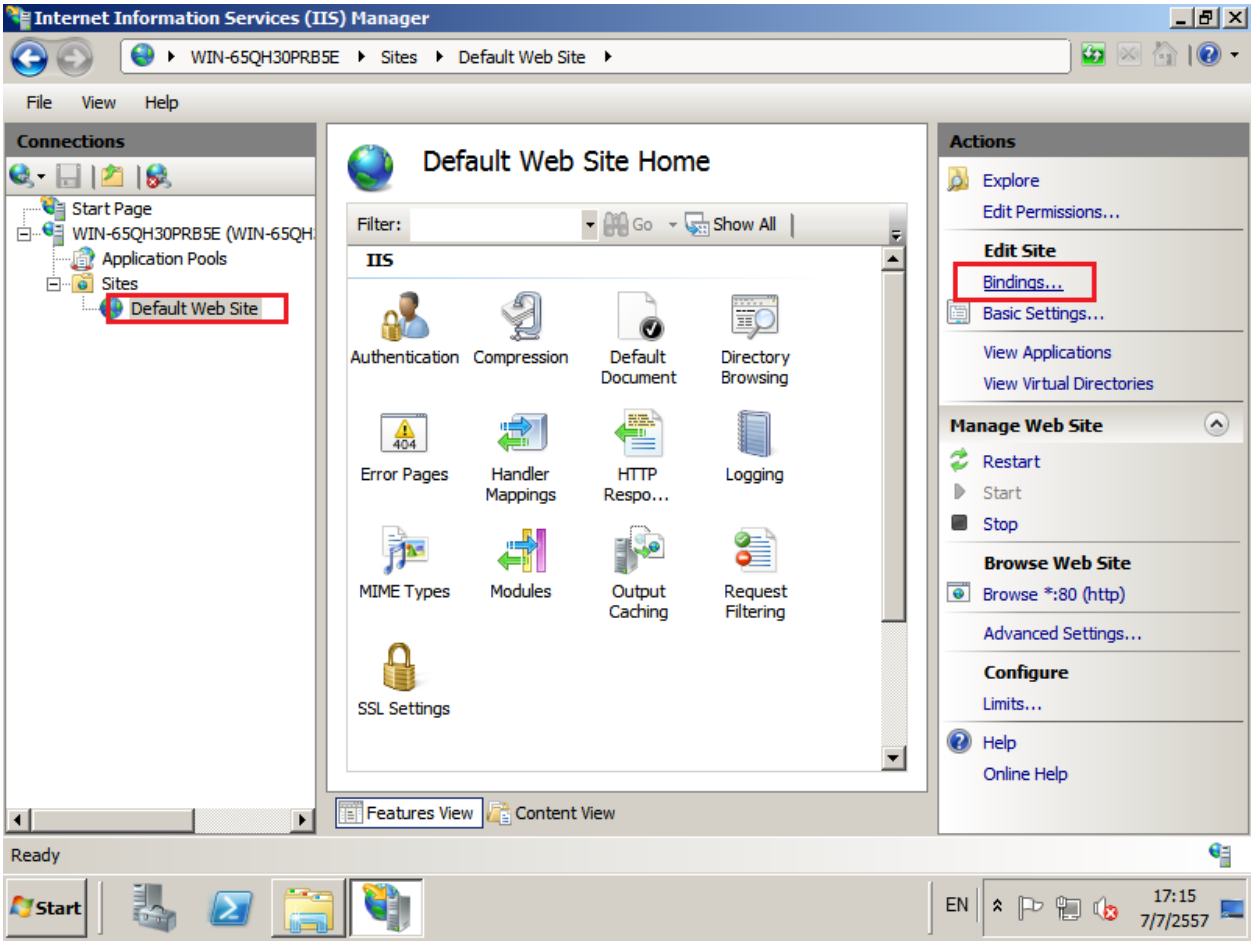
4.11. เลือก “Place all certificates in the following store” จากนั้นกด Next



4.12. เมื่อทำตามขั้นตอนทั้งหมดเสร็จสิ้นแล้ว หาก Import สำเร็จ จะขึ้นข้อความแจ้งเตือนว่า “The import was successful”



4.13. เข้าสู่ IIS Manager ทำการเลือกเว็บไซต์ที่ต้องการติดตั้ง SSL ให้ถูกต้อง หลังจากนั้น ให้ทำการคลิ๊ก Binding ที่อยู่ทางด้านขวามือ จะพบหน้าต่าง Site Binding ขึ้นมา



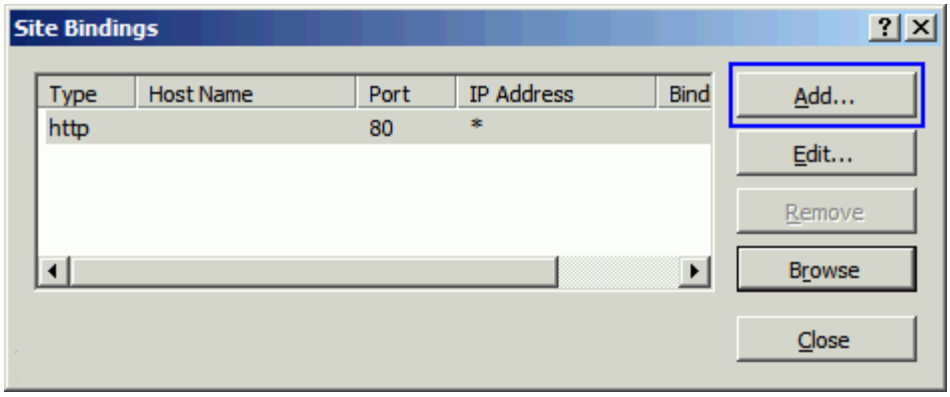
4.14. คลิกปุ่ม Add แล้วระบุข้อมูลต่างๆดังนี้

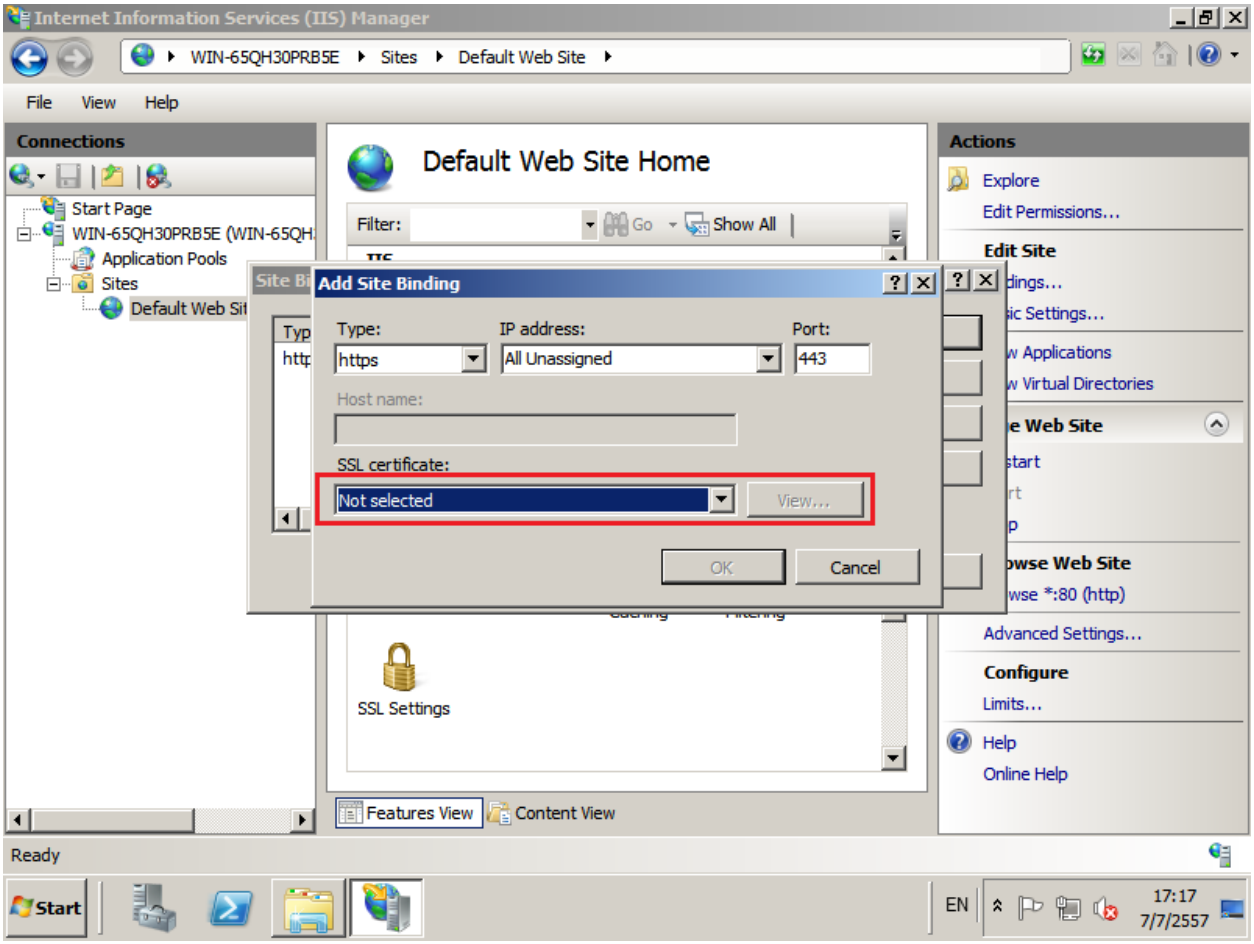
Type: ให้ทำการเลือก https

IP address: ทำการเลือก All Unassigned หรือเลือก IP เว็บไซต์ให้ถูกต้อง

Port: ให้กำหนดเป็น Port 443

SSL Certificate: ให้ทำการเลือกไฟล์ certificate ที่ได้ติดตั้งไว้





4.15. หลังจากติดตั้งเสร็จแล้ว ให้ทำการตรวจสอบการติดตั้ง SSL Certificate โดยผ่านทางเว็บไซต์ https://ssl.in.th/ssl-checker/

*หากเรียกใช้เว็บไซต์ แล้วยังไม่สามารถใช้งานได้ แนะนำให้ Restart Server เพื่อการเรียกใช้ไฟล์ใน Certificate store ได้อย่างครบถ้วนและถูกต้อง

ที่มา : https://netway.co.th/kb/ssl-certificate/how-to-install-ssl-certificate/how-to-import-ssl-certificate-on-windows-server-2008-and-more