

คู่มือการใช้งาน

KTNBS

บริษัท เค ที เอ็น บิสซิเนส โซลูชั่นส์ จำกัด

(คนทำเน็ตส์)

Self-Sign Certificate



การทำ Self-Sign Certificate HTTPS

KTN Business Solutions Company Limited (www.ktnbs.com)

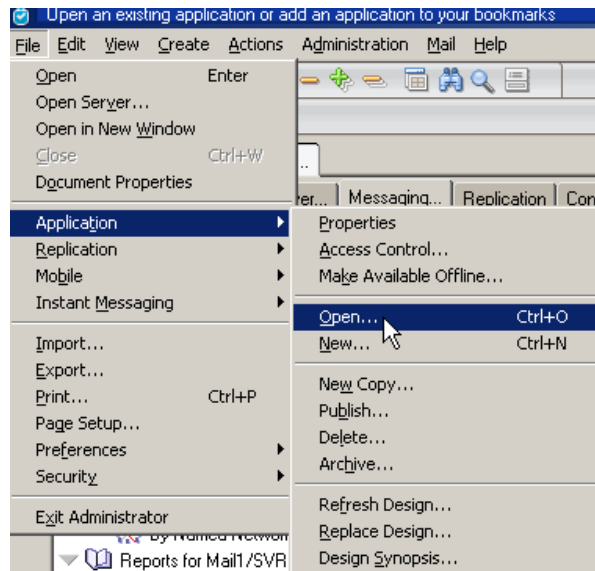
110/39 Soi Ladprao 18, Chompon, Chatuchak, Bangkok 10900, Thailand

For more information, please call 086-355-4735 or 02-938-5739 or email: sales@ktnbs.com

Self-Sign certificate HTTPS

1. สร้าง Application ขึ้นมาใหม่

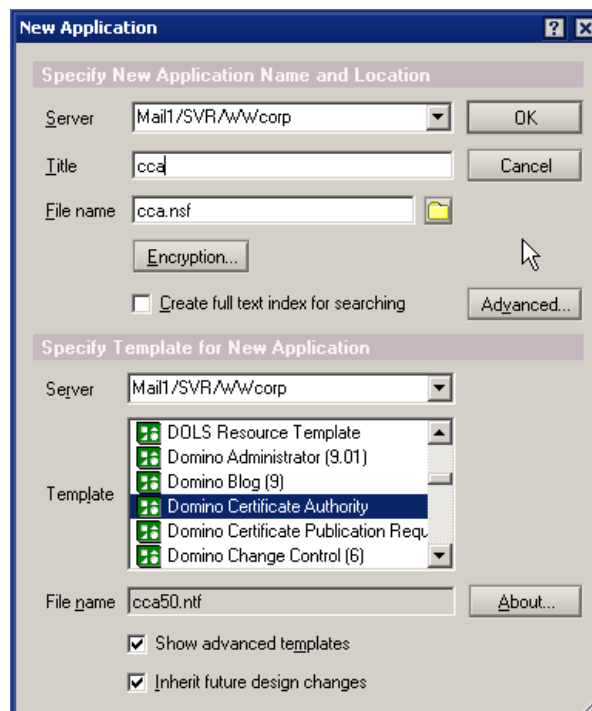
1.1 File > Application > Open หรือ Ctrl+O



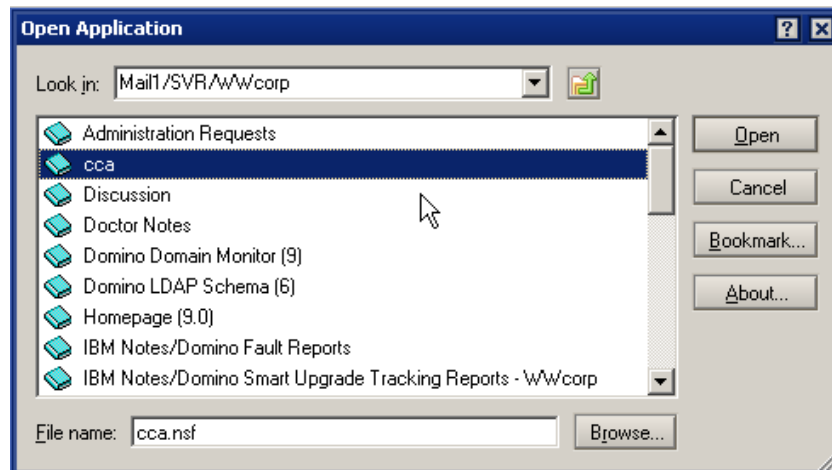
1.2. เลือก Server ที่ต้องการสร้าง จากนั้น คลิก Show advanced templates

Title พิมพ์คำว่า cca

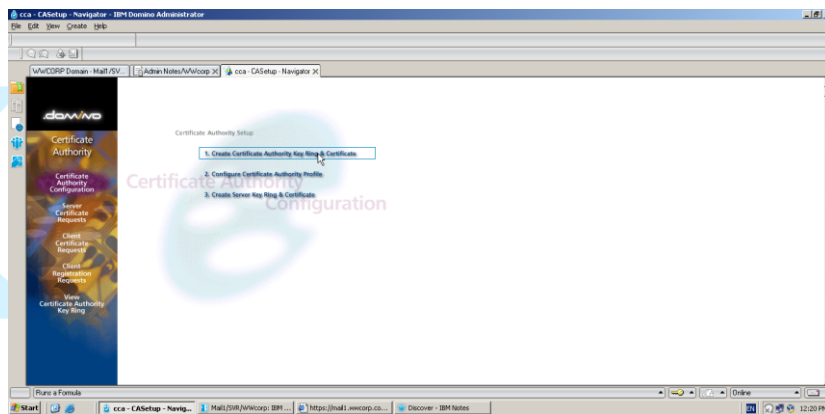
Template เลือก Domino Certificate Authority



2. เปิด Application ที่สร้างไว้ขึ้นมา เลือก cca แล้ว open



3. เลือก 1. Create Certificate Authority key Ring & Certificate



3.1. ไล่ - Password KeyRing

- กำหนด Key Site
- สร้าง Distinguished Name
- คลิก Create Certificate Authority Key Ring

Create Certificate Authority Key Ring

This form lets you create the Certificate Authority key ring.

Key Ring Information	Quick Help
Key Ring File Name: CAKey.kyr	Specify the file name and password for the key ring.
Key Ring Password: [Redacted]	
Password Verify: [Redacted]	
Key Size	
Key Size: 1024	
Distinguished Name	
Common Name: KTNBS	The Distinguished Name provides your unique identity as a Certificate Authority. This is the information that will display as the "Issuer" in certificates that you sign.
Organization: KTNbusinesssolution	
Organizational Unit: MIS (optional)	
City or Locality: Bangkok Yai (optional)	
State or Province: Bangkok (no abbreviations)	
Country: TH (two character country code)	

Create Certificate Authority Key Ring

3.2. คลิก OK

Key ring created with self signed trusted root certificate

Your Certificate Authority key ring has been created.

Key ring file name: c:\IBM\Notes\Data\CAKey.kyr

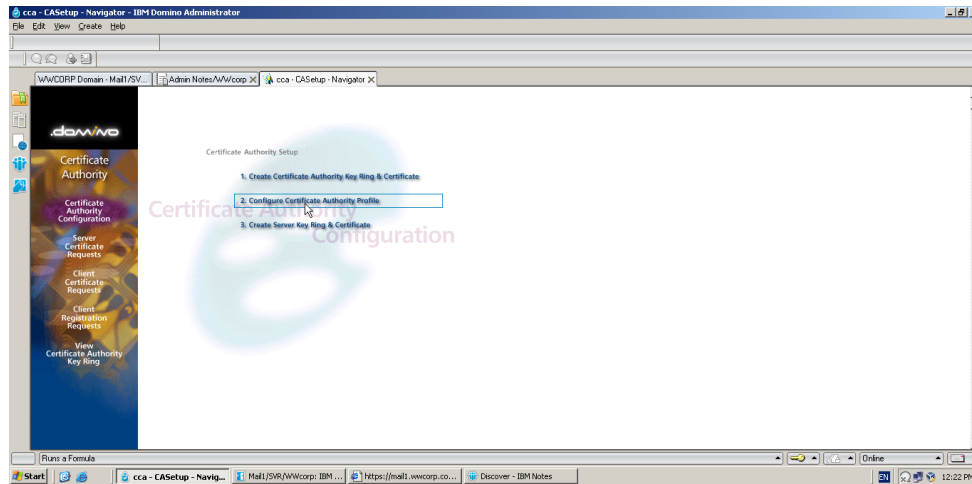
Distinguished Name:

Common name: KTNBS
Organization: KTNbusinesssolution
Organizational unit: MIS
City: Bangkok Yai
State: Bangkok
Country: TH

This certificate is valid from: Today to 05/18/2024

OK

4. เลือก 2. Configura Certificate Authority Profile



4.1. กำหนด - part ของ CA Key file

- Certificate Server DNS Name
- Use SSL for certificate transaction?
- Certificate Server Port Number
- Mail confirmation of signed certificate to requestor?
- Submit signed certificates to AdminP for addition to the Directory?
- Default validity period (Expire Date)

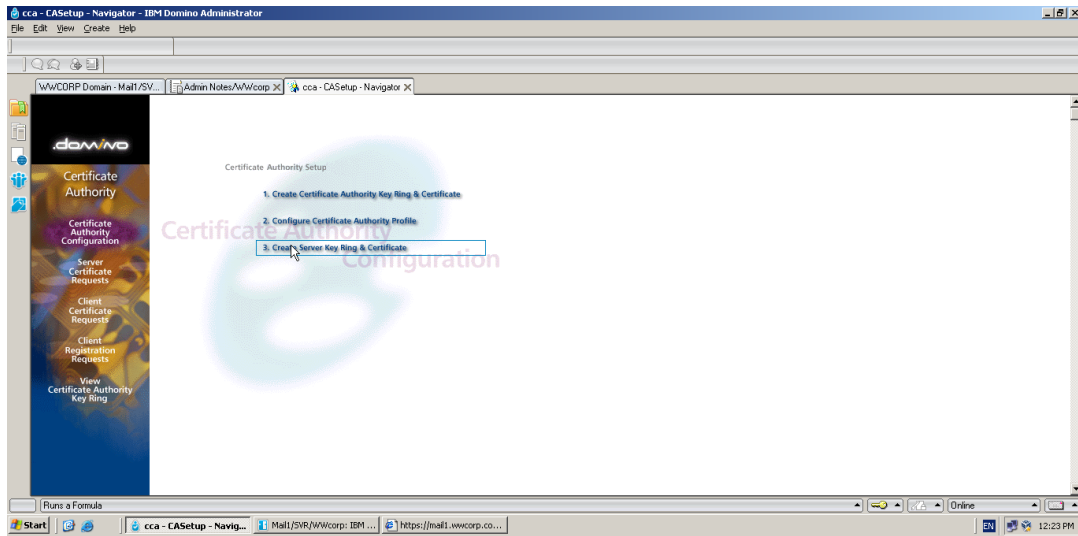
Certificate Authority Profile

Use this form to configure settings needed by the Certificate Authority application.

CA Settings	Quick Help
CA Key File <input type="text" value="c:\IBM\Notes\Data\CAKey.kyr"/>	- The name of the CA key ring file is stored here automatically when you create it. If you move the CA key ring file, you must update the path here so the application can find it. - The DNS for the server is needed for the automatic generation of the e-mail that is sent to users for certificate pickup. If this is selected, the automatically generated e-mail will contain a reference to the SSL port for secure certificate pick-up - The port number is also needed for the automatic generation of the e-mail that is sent to users for certificate pickup. This is the TCP/IP port on which the Certificate Server will be running.
Certificate Server DNS Name <input type="text" value="localhost mail1.wwwcorp.com"/>	
Use SSL for certificate transactions? <input checked="" type="checkbox"/> Yes	
Certificate Server Port Number <input type="text" value="80"/>	
Mail confirmation of signed certificate to requestor? <input checked="" type="checkbox"/> Yes	Selecting this default option is for an e-mail confirmation of a signed certificate request Selecting this default option is for the signed certificate request to be submitted to the Administration Process for storage of the certificate in the Domino Directory This is the default number of years that the signed certificate is valid
Submit signed certificates to AdminP for addition to the Directory? <input checked="" type="checkbox"/> Yes	
Default validity period <input type="text" value="5"/>	

Save & Close

5. เลือก 3. Create Server Key Ring & Certificate



KTNBS

- 5.1. กำหนด
- Keyfile.kyr
 - Password Key Ring
 - Key Site
 - CA Certificate label
 - Server Distinguished Name

คลิกที่ Create Server Key Ring

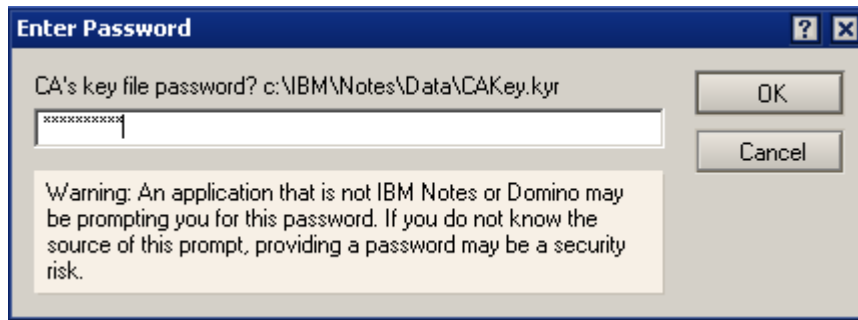
Create CA Server Key Ring

Use this form to create the server key ring for the CA server. When you submit the form, Domino will carry out all the internal steps of creating the server key ring, creating the server certificate request, signing it with the CA certificate, then installing the CA certificate and the signed server certificate into the server key ring.

Note: Once the server key ring has been created, you should use the Server Certificate Admin application to view and manage the server key ring contents.

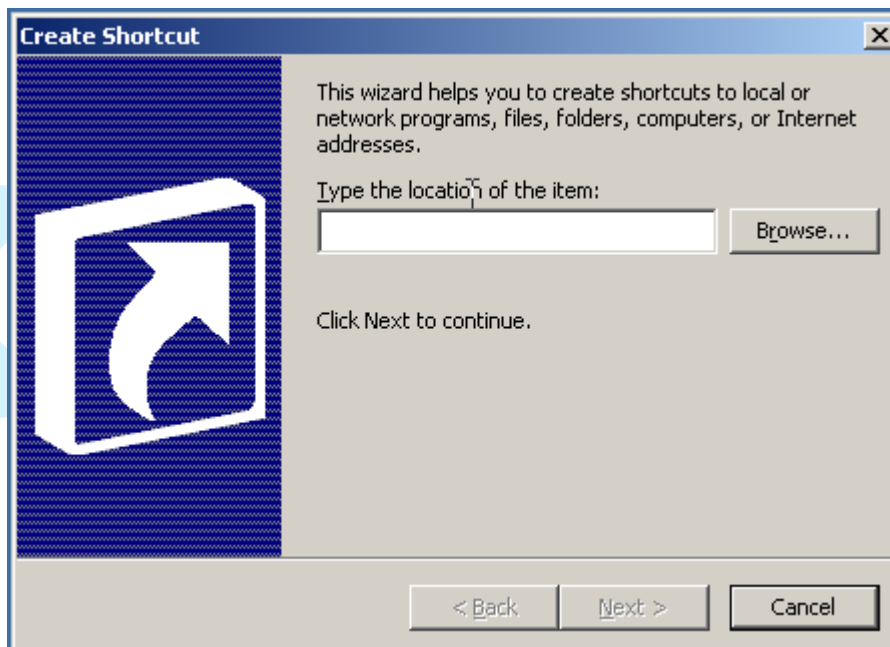
Server Key Ring Information	
Key Ring File Name: <input type="text" value="keyfile.kyr"/>	Specify the name and password for the server key ring file you are creating.
Key Ring Password: <input type="password" value="*****"/>	
Password Verify: <input type="password" value="*****"/>	
Key Size	
Key Size: <input type="text" value="1024"/>	Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength. Note: With International Editions of the Domino server, the 1024 bit key size can only be used if you qualify for and have
CA Certificate Label: <input type="text" value="CAKeypair"/>	Note: With International Editions of the Domino server, the 1024 bit key size can only be used if you qualify for and have purchased a Verisign Global Server ID This label identifies the CA Trusted Root certificate that is automatically installed in the server key ring you are creating.
Server Distinguished Name	
Common Name: <input type="text" value="localhost"/> <small>mail1.wwwcorp.com e.g., www.myserver.com</small>	The Distinguished Name is the information that uniquely identifies your site. Note: The Common Name should be the URL of your CA Web site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.
Organization: <input type="text" value="KTNbusinesssolution"/>	
Organizational Unit: <input type="text" value="MIS (optional)"/>	
City or Locality: <input type="text" value="Bangkok Yai (optional)"/>	
State or Province: <input type="text" value="Bangkok (no abbreviations)"/>	
Country: <input type="text" value="TH (two character country code)"/>	

5.2. ระบุรหัสผ่าน Password > Ok

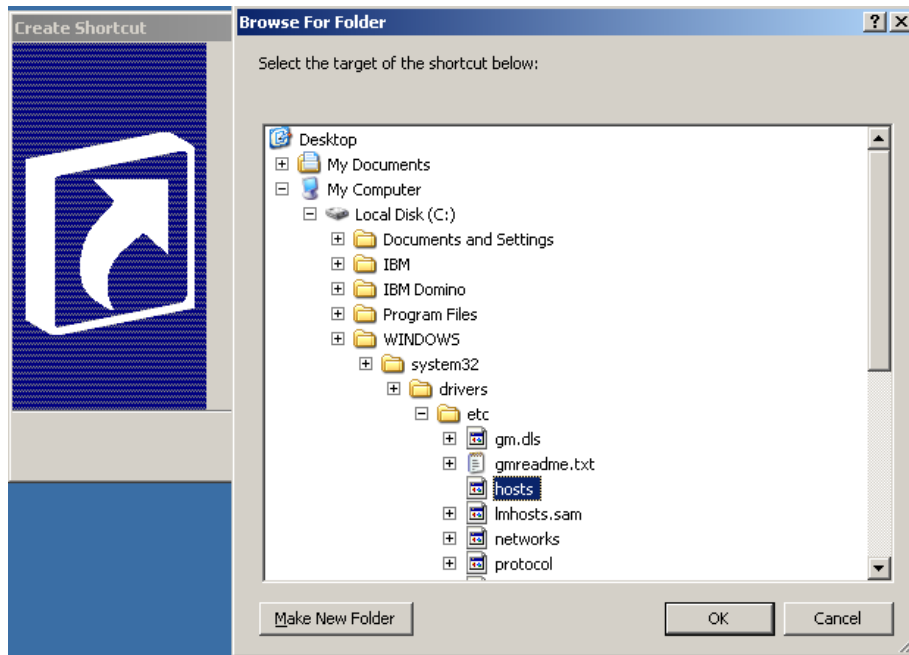


6. สร้าง Hosts Shortcut

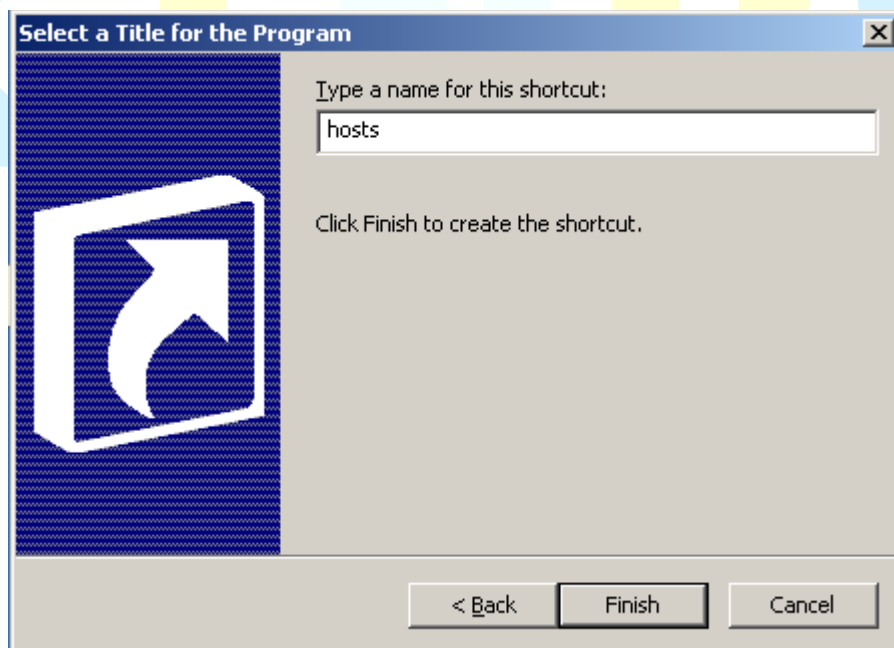
- คลิก Browse...



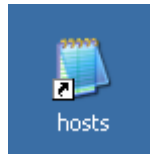
- เลือก hosts > OK



- ตั้งชื่อ hosts > Finish



7. ดับเบิลคลิก ไฟล์ hosts

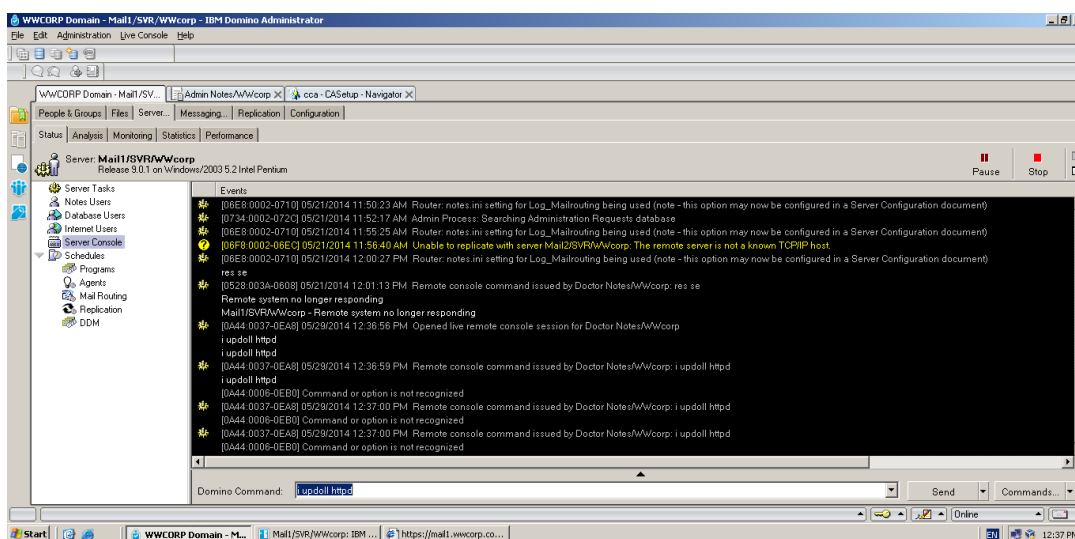


7.1. กำหนด IP > Server > url > บันทึก

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com                # x client host
127.0.0.1       localhost
10.10.10.1      mail1                    mail1.wwcorp.com
```

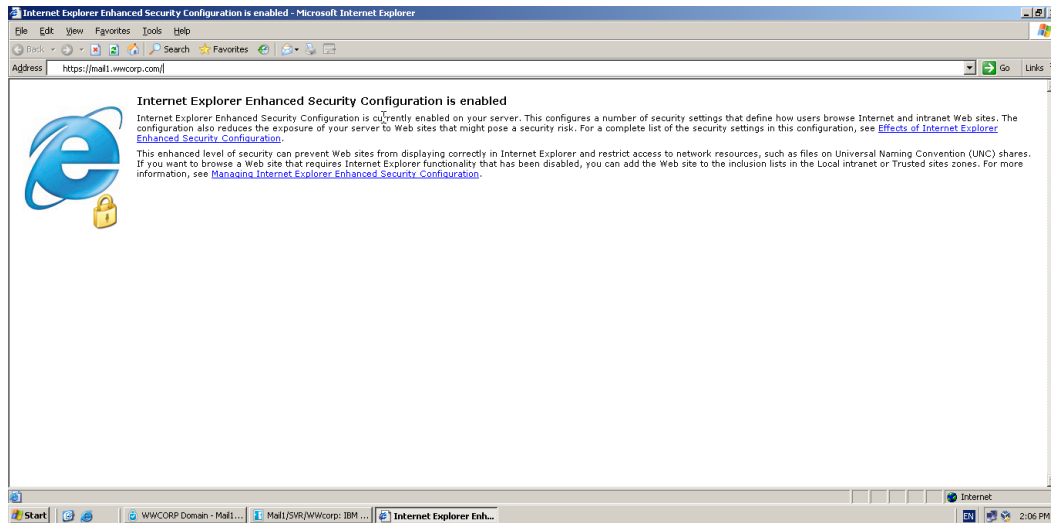
8. Run คำสั่ง command

- ไปที่ Server Console คลิกที่ tab Server > Status > >คลิกที่ Run (ปุ่มสีเขียว)
- พิมพ์คำสั่ง I updoll httpd ที่ command > Enter 2-3 ครั้ง

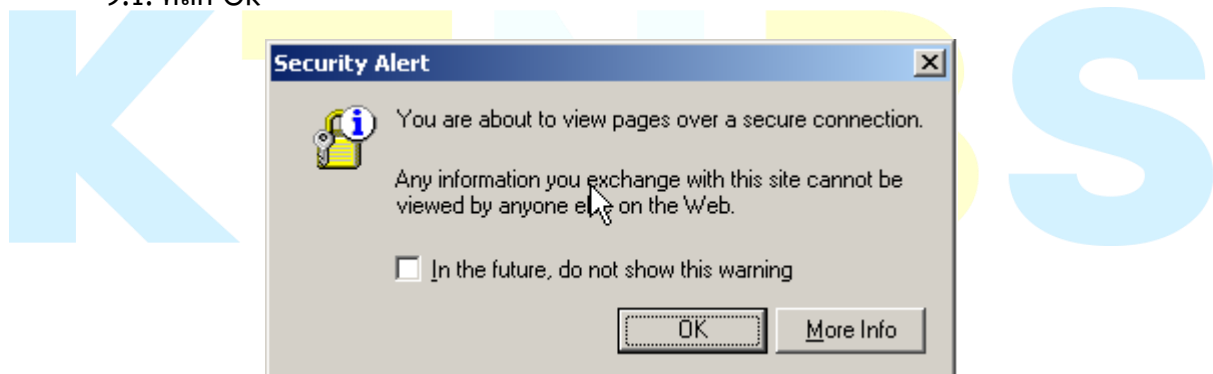


9. ทดสอบ

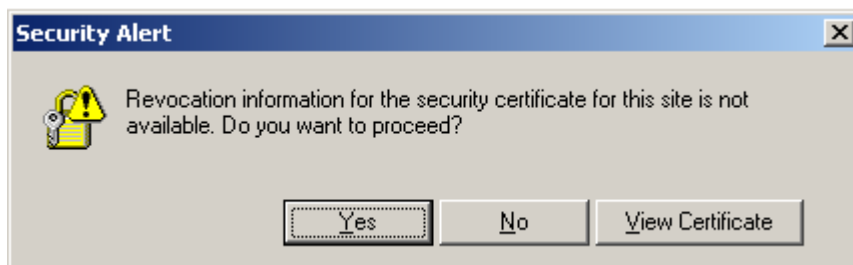
- เปิด Browser ขึ้นมา แล้วใส่ url : <https://mail1.wwcorp.com/> แล้ว Enter



9.1. คลิก Ok



9.2. คลิก Yes



9.3. คลิก Yes



KTNBS