Activate SSL on PAC Controllers
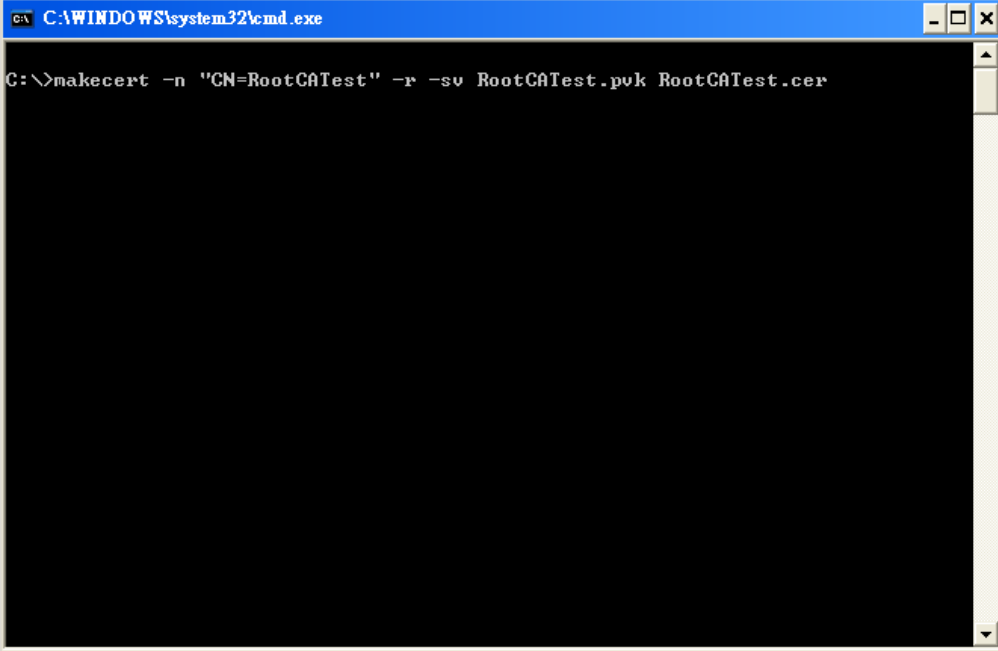
1. Obtain "makecert.exe"
2. Produce certificate files

    2.1 Open the CMD windows on PC and enter command as below:

    makecert -n "CN=RootCATest" -r -sv RootCATest.pvk RootCATest.cer

    CN = Certificate Name

    Please refer to link below about command reference:

    http://msdn.microsoft.com/zh-tw/library/bfsktky3%28v=vs.80%29.aspx

    2.2 After command executed, the dialog showed as blow.   Please enter a password to create private key.
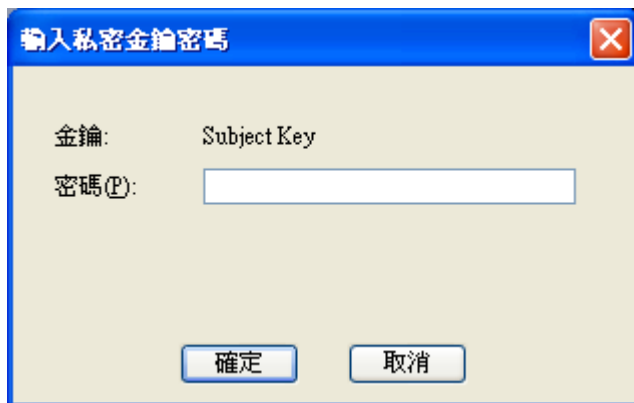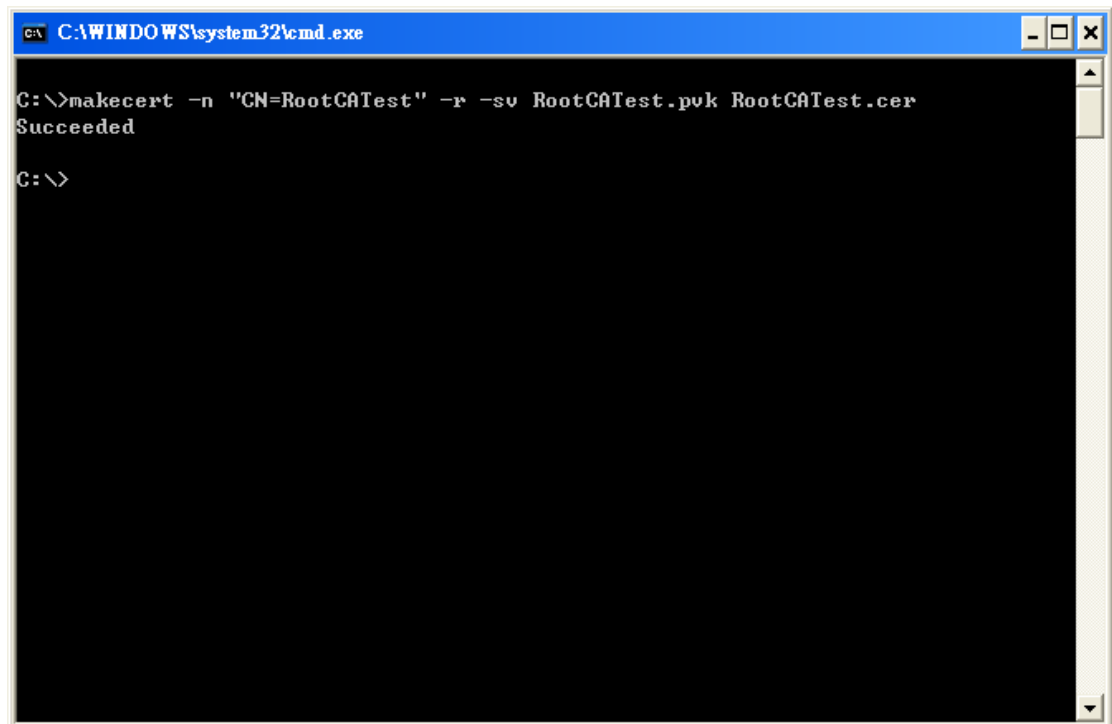
2.3 After step 2.2, dialog showed as below.   Please enter the password as private key.

2.4 Certificate files were successfully produced if Succeeded message showed on CMD windows.

3. Upload the certificate (.cer file) and the private key (.pvk file) from your development workstation to WinPAC, ViewPAC or XPAC.
4. Edit the registry.   The editing tool can be found in \System_Disk\TOOLS\registryeditor\REGEDIT.exe.   If the XPAC controller, skip step 4.
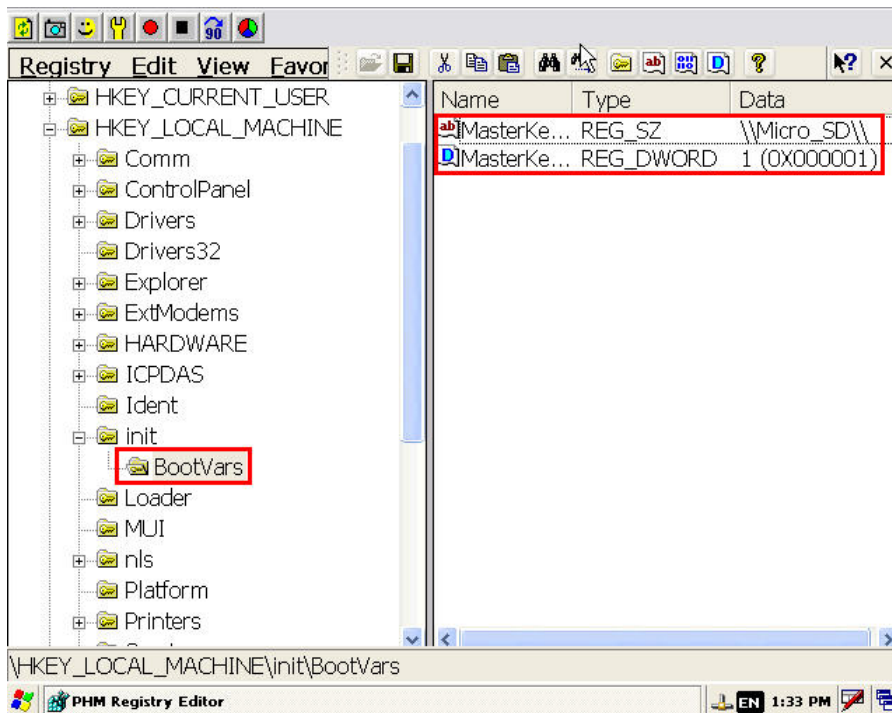
4.1 Create a new key named "**BootVars**" in **HKEY_LOCAL_MACHINE\init**

4.2 Add a String Value: **MasterKeyFileDir = "\\Micro_SD\\"** (The path is the path where master key and private key located)

4.3 Add a DWORD Value: **MasterKeysInRegistry = 1**

4.4 Save Register.

4.5 Save and reboot WinPAC or ViewPAC.

5. Import Certificate to Windows CE. Please refer to link below for more information.

http://msdn.microsoft.com/en-us/library/ms900349.aspx

5.1 On the WinPAC, ViewPAC or XPAC-CE6, select the **Start-> Settings-> Control Panel -> Certificates menu**.
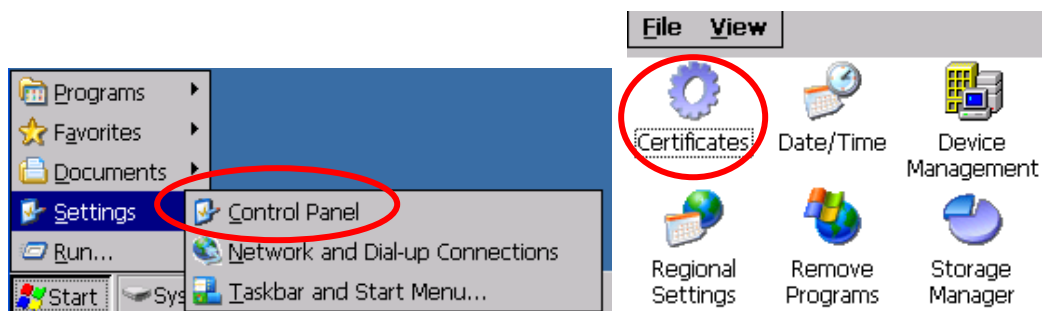
5.2 On the **Certificates** dialog box, select **My Certificate**s from the drop down list on the **Stores** tab and click **Import…** button to import the certificate file (*.cer).
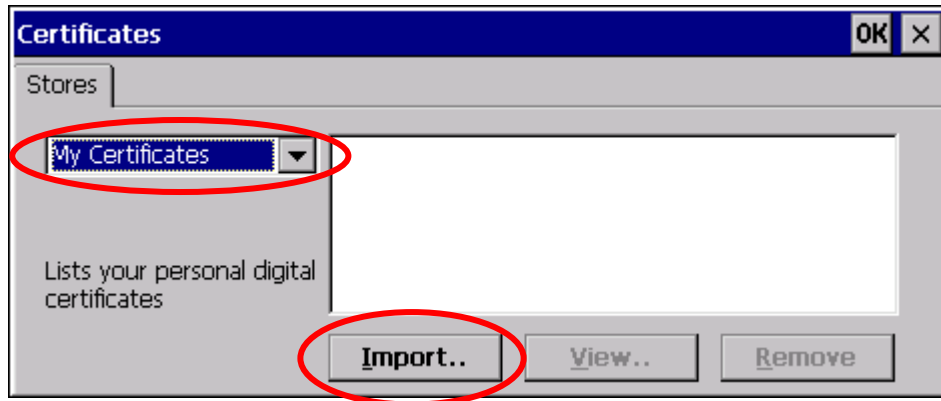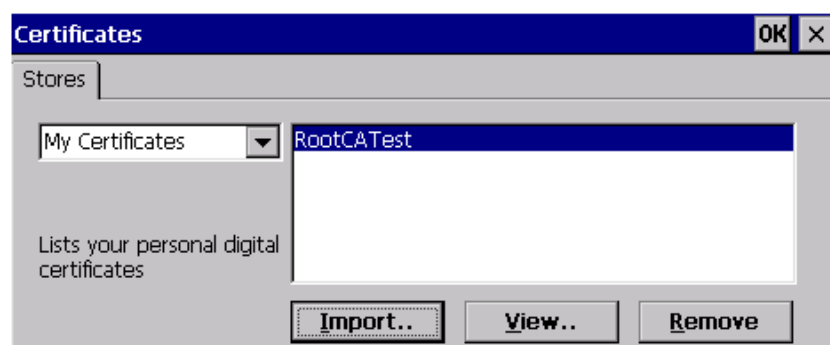
5.3 On the **Import Certificate or Key** dialog, select the **From a File** open and then click **OK**.
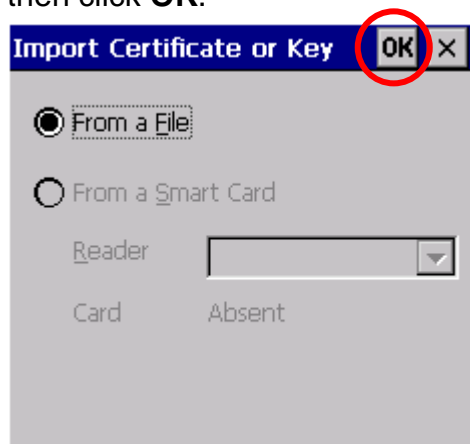
5.4 On the **Select a Certificate File** dialog box, select the .cer file and click **OK**.
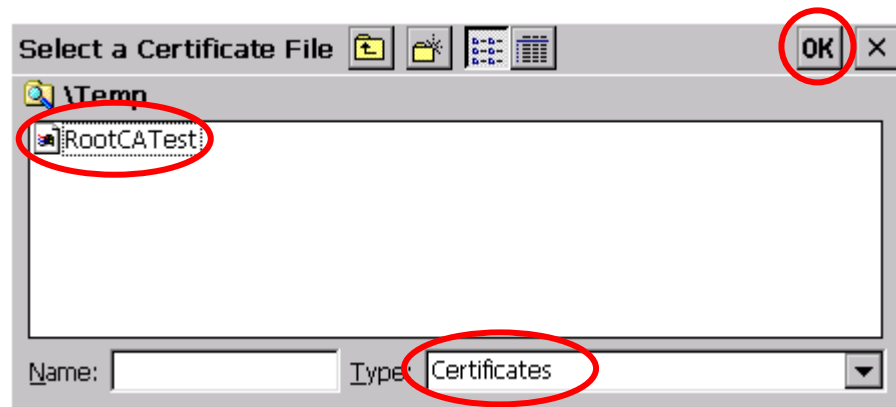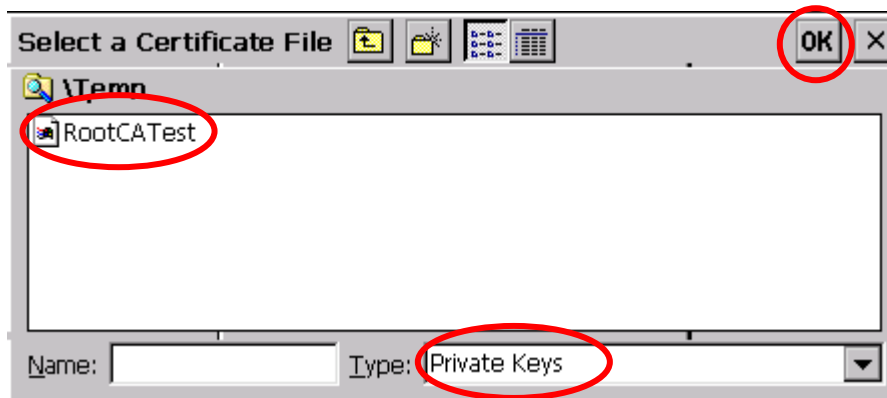

5.5 The certificate name is displayed in the list of personal digital certificates.
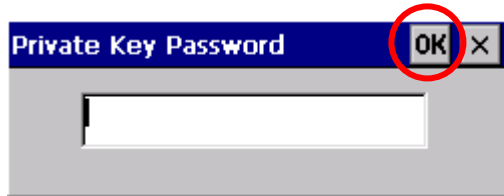
5.6   Repeat step 5.2 and 5.3.

5.7   On the **Select a Certificate File** dialog box, choose **Private Keys** in the Type list, select the .pvk file, and then click **OK**.
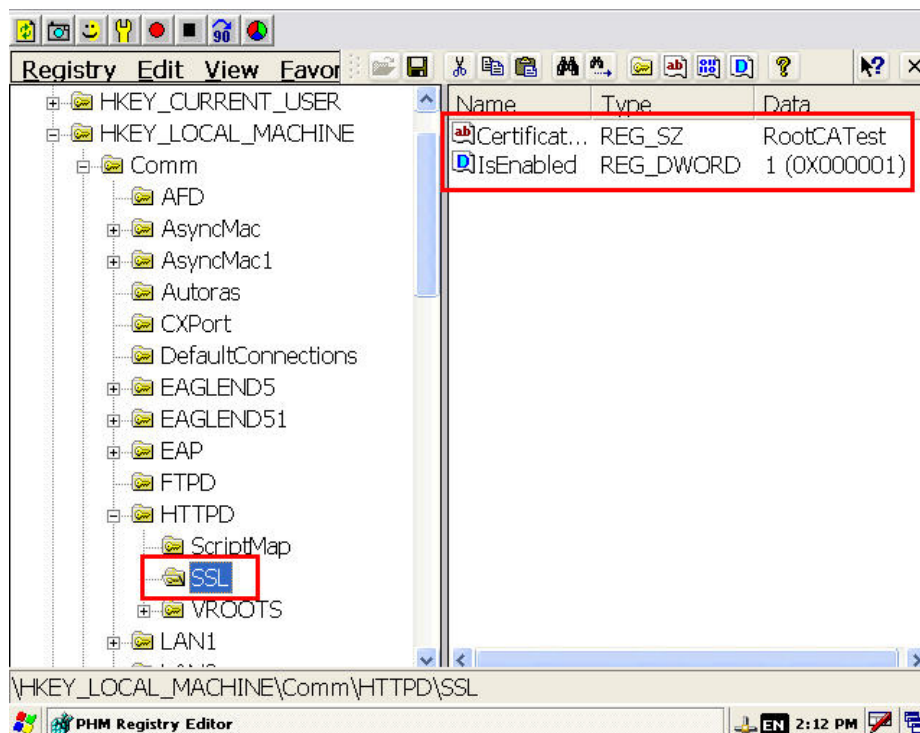

5.8   Enter the password for the private key in the **Private Key Password** dialog box and click **OK**. The

5.9   Click OK to close the **Certificates** dialog.

6.   Edit the registry to activate the SSL and configure the Certificate name.   For more information, please refer to link blow.

http://msdn.microsoft.com/en-us/library/ee499201%28v=winembedded.60%29.aspx

6.1 Create a new key named "**SSL**" in
HKEY_LOCAL_MACHINE\COMM\HTTPD

6.2 Add a String Value: **CertificateSubject = "RootCATest"** (name of the certificate).

6.3 Add a DWORD Value: **IsEnabled = 1**

6.4 Save Register.

6.5 Save and reboot WinPAC, ViewPAC or XPAC-CE6.

Enabling SSL for InduSoft Web Thin Client

1. Configure the SSL settings in InduSoft.
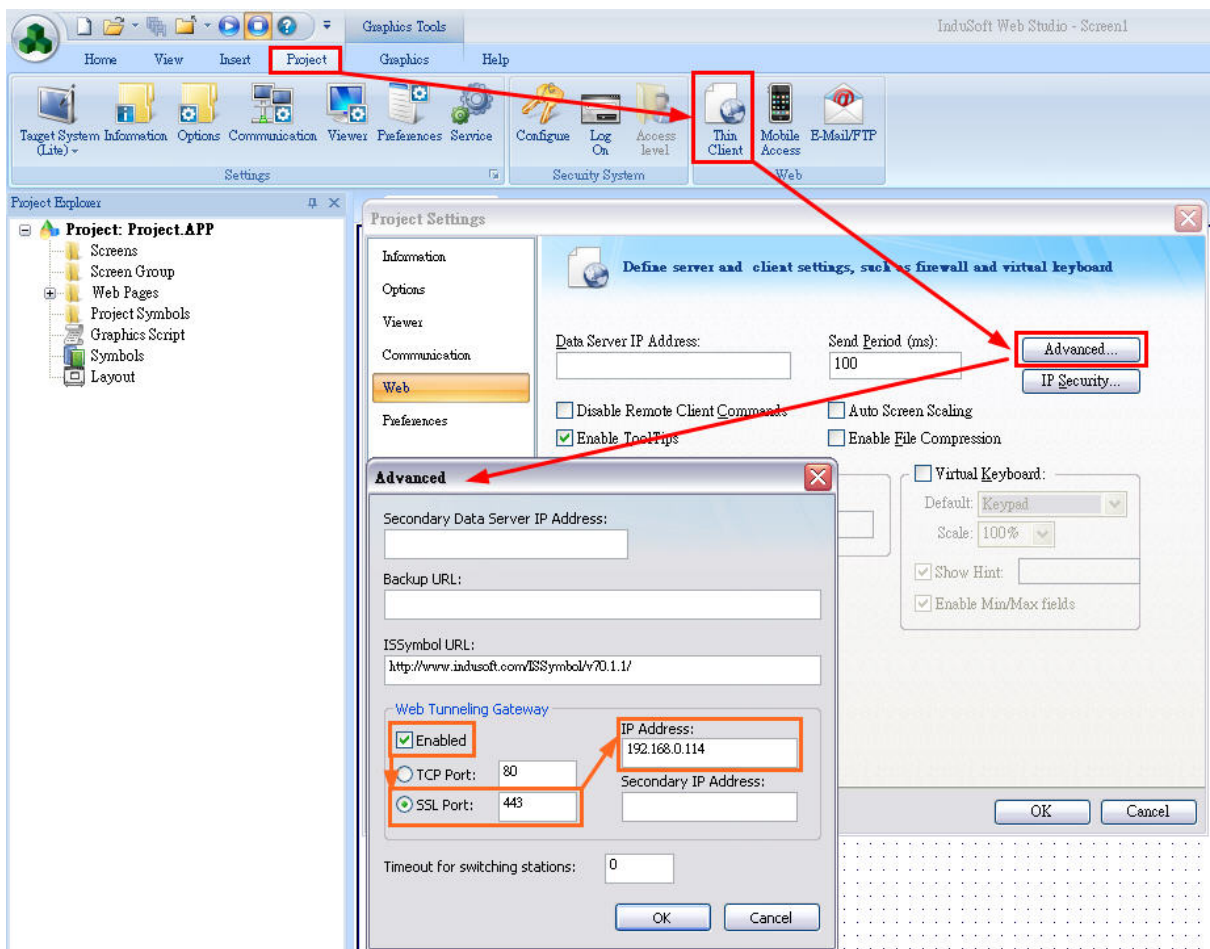
1.1 In InduSoft, click on the Project tab → Thin Client → Advanced button.

1.2 After Advanced dialog showed, check the Web Tunneling Gateway **Enabled** checkbox and choose **SSL Port**.   Change SSL Port number if necessary. The default SSL port is 443.

1.3 Modify the **IP Address** where the Web Tunneling Gateway is running (generally where InduSoft is running).

Note: For detail information about configuring Web Thin Client, please refer to user manual on section "Deploying as a Web Application". The manual can be downloaded from
http://www.icpdas.com/products/Software/InduSoft/IWS_Downloads/PC/Documents/TechRef.pdf

2. Install the Web Tunneling Gateway service on WinPAC, ViewPAC, or XPAC-CE6
   2.1 Copy **IndWebSvc.dll** and **WebGtw.exe** to InduSoft Runtime folder (ex: \Micro_SD\InduSoft\)
   2.2 Execute the **WebGtw.exe** to install the service. If successfully installed, the message box showed as below.
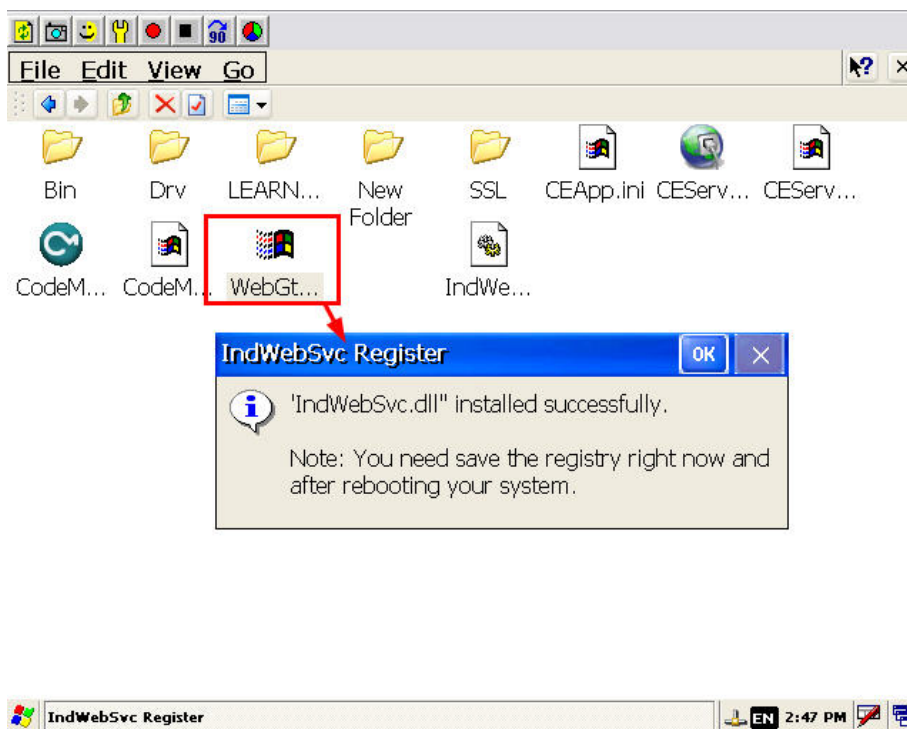
   2.3 Save and Reboot the WinPAC, ViewPAC or XPAC-CE6

Note: For detail information about configuring the web server, please refer to manual below on page 55.
http://ftp.icpdas.com/pub/cd/winpac/napdos/vp-2000_ce50/document/viewpac_2xw1_user_manual_v1.0.7.pdf

3. Browsing the pages using SSL
   3.1 On IE browser, input **https://IP_Address/Screen_Name.html** (Ex: https://192.168.0.104/main.html)
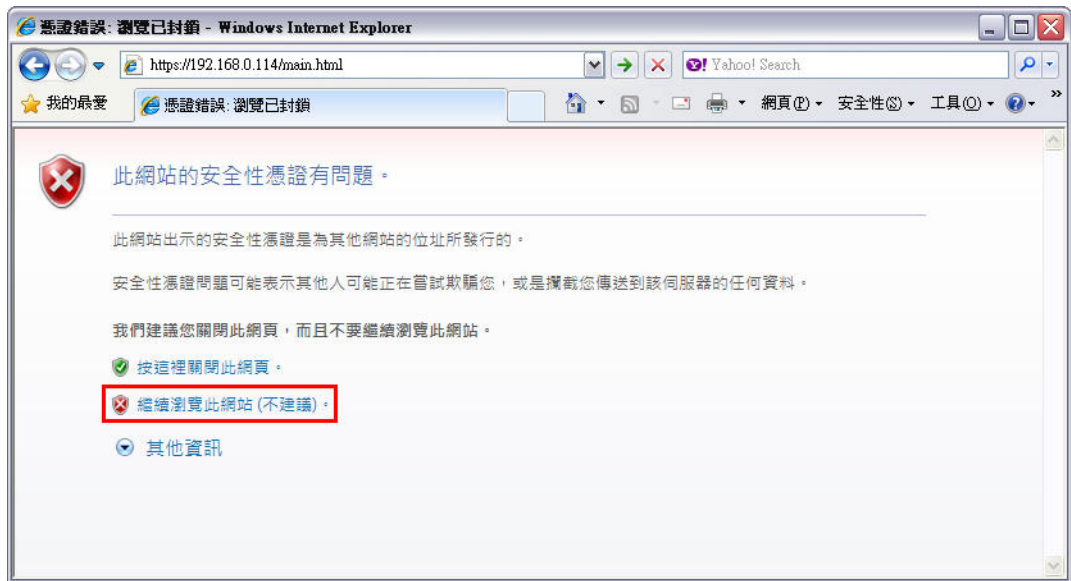
Note: The error may be showed as image above. This error occurs when the certificate has been issued by a certification authority that is not recognized by Internet Explorer.   Additional annual fee is needed to obtain an authorized certificate.   Users will need to apply one themselves in order to avoid the error.

3.2   Click "Continue to this website (not recommended)" to continue browsing web pages.