## 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

📾 C:\WINDOWS\system32\cmd.exe	- 🗆 ×
C:∖>makecert -n "CN=RootCATest" -r -sv RootCATest.pvk RootCATest.cer	<b>^</b>
	-

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.

建立私密金繪密碼		×
金鑰:	Subject Key	
密碼(P):		
確認密碼(C):		
確定	無 取消	

2.3 After step 2.2, dialog showed as below. Please enter the password as private key.

输入私密金銷	自密碼	X
金鑰:	Subject Key	
密碼(P):		
	確定 取消	

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

C:\WINDOWS\system32\cmd.exe	- 🗆	×
C:∖>makecert -n "CN=RootCATest" -r -sv RootCATest.pvk RootCATest.cer Succeeded		
C: \>		
		-

- 3. Upload the certificate (.cer file) and the private key (.pvk file) from your development workstation to WinPAC, ViewPAC or XPAC.
- Edit the registry. The editing tool can be found in \System\_Disk\TOOLS\registryeditor\REGEDIT.exe. If the XPAC controller, skip step 4.

😰 🗃 🙂 💾 💌 🔐 🚳				
Registry Edit View Eavor	አ 🖻 🛍 🚧	🎪 😖 🍓 関	8	<b>№?</b> ×
🗄 🙆 HKEY_CURRENT_USER 🛛 🔼	Name	Туре	Data	
🖻 َ HKEY_LOCAL_MACHINE	औMasterKe	REG_SZ	\\Micro_	_SD\\
🐵 🙆 Comm	🔍 MasterKe	REG_DWORD	1 (OXOO	0001)
🗉 应 ControlPanel				
😥 应 Drivers				
🖾 Drivers 32				
🗉 🙆 Explorer				
😥 应 ExtModems				
🐵 应 HARDWARE				
😥 应 ICPDAS				
- 🖾 Ident				
🖻 📴 init 📃				
- BootVars				
🖾 Loader				
MUI				
🕀 应 nls				
🖻 Platform				
🐵 🙆 Printers	121			
				2
M PHM Registry Editor			.EN 1:33 P	м 🗭 🔜

- 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 Certificates** from the drop down list on the **Stores** tab and click **Import...** button to import the certificate file (\*.cer).

Certificates	ОК 🗙
Stores	
My Certificates	
Lists your personal digital certificates	
<u>I</u> mport ⊻iew	Remove

5.3 On the **Import Certificate or Key** dialog, select the **From a File** open and then click **OK**.

import Certif	ficate or Key	ОК	×
From a El	e	$\smile$	
O From a Sr	mart Card		
<u>R</u> eader			~
Card	Absent		

5.4 On the **Select a Certificate File** dialog box, select the .cer file and click **OK**.

Select a Certificate File 🗈 💣	Ш (ок) ×
(Temp	$\mathbf{i}$
RootCATest	
Name: Type Certi	ficates

5.5 The certificate name is displayed in the list of personal digital certificates.

Certificates		ок 🗙
Stores		
My Certificates	RootCATest	
Lists your personal digital certificates		
	Import <u>V</u> iew <u>R</u> emov	re

- 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**.

Select a Certificate File 主 📸 📰	<u>ок</u> ×
() \Temp	$\mathbf{\overline{\mathbf{V}}}$
RootCATest	
Name: Type: Private Keys	•

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.

	Graphics Tools Graphics Help	InduSoft Web Studio - Screen1
Target System Information Options Communication View	er Preferences Service G Securit System	Thin Access Woble E-Mail/FTP
Periect Employer 0 ×	and a strength of the strength	
Project Explorer 4 ×	Project Settings Information Options Viewer Communication Web Preferences Advanced Secondary Data Server IP Address: Backup URL:	Advanced In Commander Advo Screen Scaling Enable File Compression Virtual Keyboard: Default: Keyped Scale: 100% v Scale: 100% v Sc
	ISSymbol URL: http://www.indusoft.com/ISSSymbol/v70.1.1/ Web Tunneling Gateway P Enabled TCP Port: 80 SSL Port: 443 Timeout for switching stations: 0 OK	Address: Cancel

- 1.1 In InduSoft, click on the Project tab  $\rightarrow$  Thin Client  $\rightarrow$  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/Docume nts/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.



$\gamma \gamma$	Sove and Reheat the WinDAC ViewDAC or VDAC CEE	
z.১	Save and Repool the WINPAC, VIEWPAC OF APAC-CEO	

**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\_manu al\_v1.0.7.pdf

🕹 EN 2:47 PM 🏴 🔁

3. Browsing the pages using SSL

🛃 IndWebSvc Register

3.1 On IE browser, input https://IP\_Address/Screen\_Name.html (Ex: https://192.168.0.104/main.html)

🥖 表型错误	瀏覽已封鎖 - Windows Internet Explorer		
00-	[2] https://192.168.0.114/main.html	💌	<b>P</b> -
🚖 我的最愛	🏉 憑證錯誤: 瀏覽已封鎖	🍈 🔹 🗟 🔹 🖶 🔹 網頁 🕑 🗸 安全性 🕲 🗸	I具() • <b>() •</b> <sup>≫</sup>
8	此網站的安全性憑證有問題。		
	此網站出示的安全性湛證是為其他網站的位址所發行的。		5
	安全性應證問題可能表示其他人可能正在嘗試欺騙您,或是攔截您傳送到該伺服器的任何資料。 我們建議您關閉此網頁,而且不要繼續瀏覽此網站。		
_	⌀ 按這裡關閉此網頁。		
	😵 繼續瀏覽此網站 (不建議)。		
	● 其他資訊		
			×

**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.

