

CCASS (& CCMS) Terminal Installation Procedures

Version: 5.0

Date: Jan 2017

Procedures:

The purpose of this section is to describe the installation procedures for the CCASS (& CCMS) Terminal ("C3T"). The installation processes are organized into six high-level steps:

A. Hardware Setup

- To setup the required hardware for C3T

B. Communication Line Setup

- To setup the required communication line for C3T

C. Windows IP Address and Configuration Setup

- To setup the Windows setting, including IP address and display for C3T

D. CCASS & CCMS Access Setup

- To initialise the access to CCASS & CCMS, including accepting server certificate, installing java plug-in and Acrobat Reader

E. Initialise smartcard and first time logon to CCASS & CCMS

- To initialise smartcard and logon to CCASS & CCMS

A. Hardware Setup

1. Ensure C3T PC with Following System Configuration

Items	Descriptions																
Minimum Hardware Configuration	For all supported Windows platforms <ul style="list-style-type: none">– Personal Computer with 1GHz or faster x86 (32-bit) or x64 (64-bit) processor– Memory: 1GB (32-bit) or 2GB (64-bit)– Local Hard Disk: 16 GB (32-bit) or 20GB (64-bit) of free space– LAN interface: Fast Ethernet card or Gigabit Ethernet card X 1– Communication port: 1 USB port for smartcard reader or 1 COM and 1 PS/2 port for COM port reader																
Software Configuration	<ul style="list-style-type: none">– Operating System:<ul style="list-style-type: none">▪ MS Windows 7 Professional 32-bit or 64-bit¹ (Chinese or English) version with Service Pack 1 (Win7 Pro SP1)▪ MS Windows 8.1 Pro 64-bit¹ (Chinese or English) version (Win8.1 Pro)▪ MS Windows 10 Pro 64-bit¹ (Chinese or English) version (Win10 Pro)– Browser:<ul style="list-style-type: none">▪ Internet Explorer 11 (IE 11)– Java Runtime Environment:<ul style="list-style-type: none">▪ JRE 8u111 (32-bit)– Adobe Acrobat Reader (for viewing circulars, available in CCASS (& CCMS) Commissioning Website):<ul style="list-style-type: none">▪ Adobe Acrobat Reader 11 or above <p>Notes:</p> <p>1. Only 32-bit JRE are supported for C3T on any supported 64-bit Windows platform</p> <p>Since the above software are released at different times by vendors, the combinations of Operating System, Browser and Java Runtime Environment supported are illustrated in the below table:</p> <table><tr><th></th><th>Win7 Pro SP1</th><th>Win8.1 Pro</th><th>Win10 Pro</th></tr><tr><th></th><th>JRE 8u111</th><th>JRE 8u111</th><th>JRE 8u111</th></tr><tr><td>IE 11</td><td>✓</td><td>✓</td><td>✓</td></tr></table> <p>Legend:</p> <table><tr><td>✓</td><td>Supported</td></tr><tr><td>✗</td><td>Not supported</td></tr></table>		Win7 Pro SP1	Win8.1 Pro	Win10 Pro		JRE 8u111	JRE 8u111	JRE 8u111	IE 11	✓	✓	✓	✓	Supported	✗	Not supported
	Win7 Pro SP1	Win8.1 Pro	Win10 Pro														
	JRE 8u111	JRE 8u111	JRE 8u111														
IE 11	✓	✓	✓														
✓	Supported																
✗	Not supported																
Security Device	<ul style="list-style-type: none">– Smartcard Reader:<ul style="list-style-type: none">▪ GemPCUSB-SL(IDBridge CT40)(USB), GemPCUSB-SW (USB) and GemPC410 (com port)																

CCASS (& CCMS) Terminal Installation Procedure

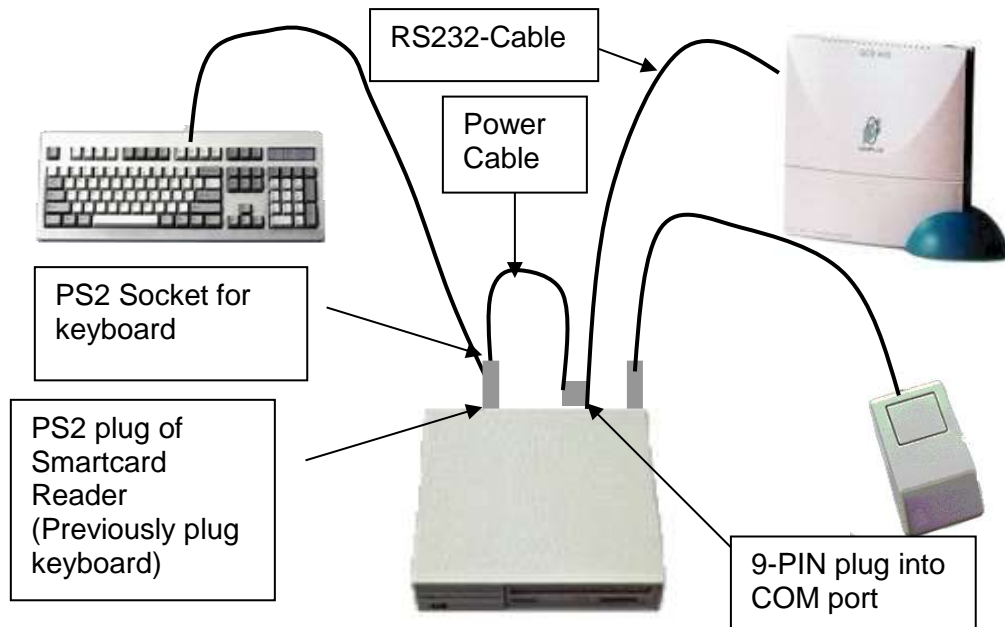
Items	Descriptions
	<ul style="list-style-type: none"> ▪ These readers can be used on all supported Windows version
Network Device	<ul style="list-style-type: none"> – Hub/Switch and Cable: <ul style="list-style-type: none"> ▪ Only required for dual SDNet/2 links or multi-C3T sharing one single SDNet/2 link ▪ One Fast Ethernet (100Mbps) Hub or Ethernet Switch with 10/100 or 100/1000 auto sense and it must support standard UTP connections (100BaseT or 1000BaseT) ▪ One Category 5 (for 100BaseT) or Category 5E/6/6A standard UTP (unshielded twisted-pair) cable for each C3T (to connect the C3T to the Hub or Switch)
C3T LAN Port or Network Device setting for CCASS & CCMS connection via SDNet/2	<ul style="list-style-type: none"> – Fast Ethernet (100Mbps): <ul style="list-style-type: none"> ▪ Speed – Auto ▪ Duplex – Auto – Gigabit Ethernet (1000Mbps) <ul style="list-style-type: none"> ▪ Speed – Auto ▪ Duplex – Auto <p>Note: <i>Participants / designated banks should contact their SDNet/2 Accredited Vendor if they require network port setting different from the above.</i></p>

2 Install Smartcard Reader

2.1 Serial Port Smartcard Reader

This procedure applies to smartcard reader of model GemPC410 and no specific driver is required to be installed. Nevertheless, please ensure your PC has a COM port and PS/2 port for connection.

The following diagram depicts the PC and Smartcard Reader setup:





- 2.1.1 Shut down the computer before installing Smartcard Reader for safety purpose
- 2.1.2 Connect the RS232-cable (9-PIN) of the Smartcard Reader to the C3T PC's COM port
- 2.1.3 Connect the power cable to the jack end of the socket on the Smartcard Reader
- 2.1.4 Connect the power cable to the keyboard port (PS2 port) of the C3T PC
- 2.1.5 Connect the keyboard's PS2 plug to the piggy-backed connector of the power cable
- 2.1.6 Switch on the computer again

2.2 USB Smartcard Reader

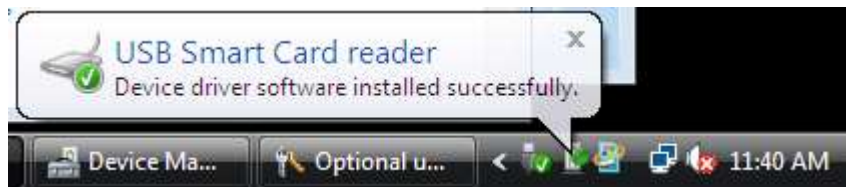
This procedure applies to all supported USB smartcard readers and **NO DRIVER** is required to be installed.

- 2.2.1 Check which USB readers you are using: GemPCUSB-SL (ID Bridge CT40) or GemPCUSB-SW. The model number is also printed at the back of the reader.

	
GemPCUSB-SL (IDBridge CT40)	GemPCUSB-SW

- 2.2.2 Connect the USB smartcard reader to the USB port on the computer

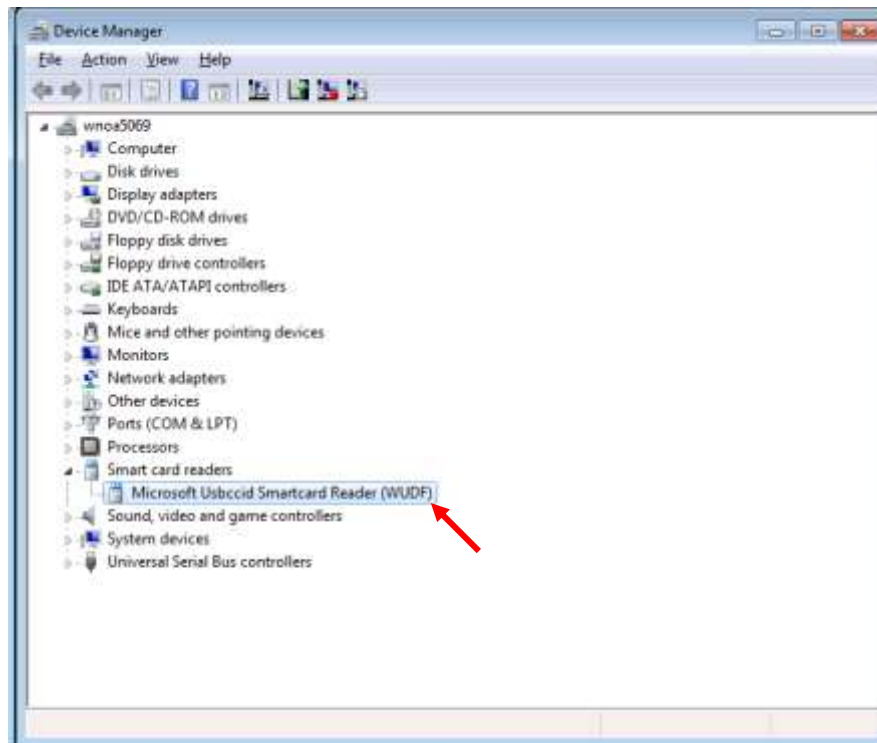
- 2.2.3 Smartcard reader driver software is automatically installed to the computer



- 2.2.4 Open the Control Panel → Hardware and Sound.

- 2.2.5 Then select “Device Manager” and open the “smart card reader”, under which a smart card reader will show up. This means that a smart card reader has been properly setup.

CCASS (& CCMS) Terminal Installation Procedure

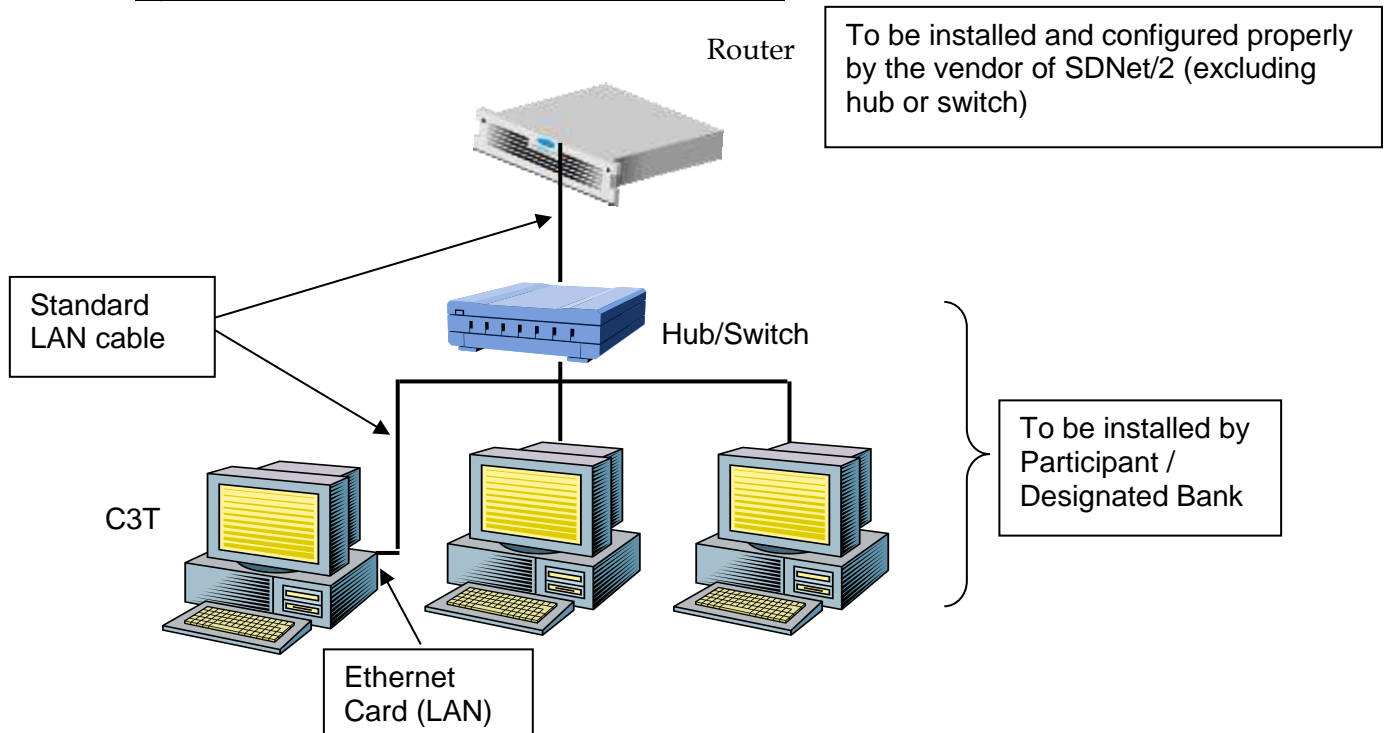


B. Communication Line Setup

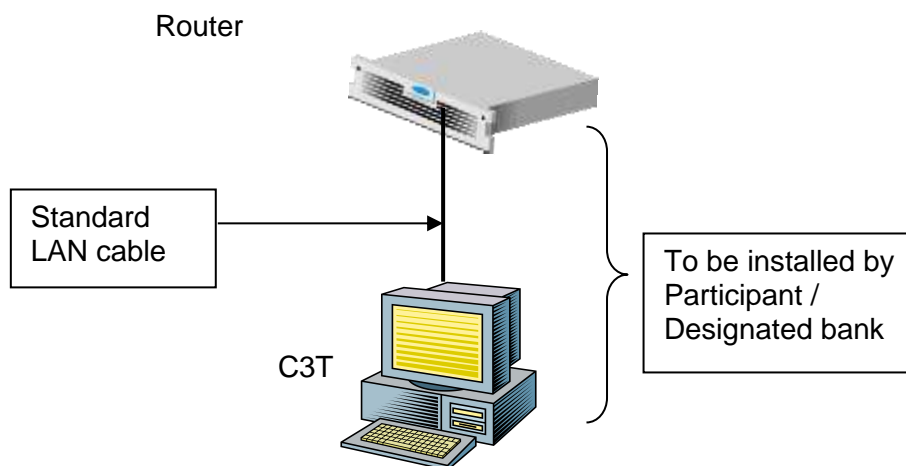
3.1 Connect C3T PC with Router

- 3.1.1 Ensure the Metro Ethernet communication line and router are installed and configured properly by the vendor of SDNet/2.
- 3.1.2 Connect the C3T PC to WAN router with a LAN cable. Two possible options to establish the connection:

Option 1 : Connection to Router via Hub or Switch



Option 2 : Direct Connection to Router



3.2 Network Configuration for C3T using Firewall (Optional)

The C3T uses open protocols to access the CCASS (& CCMS) host systems, i.e. TCP/IP, HTTPS, DNS. As a result, it is optional for participants / designated banks to make use of a Firewall to protect C3T which may reside inside their internal networks.

This section provides the necessary information for participants / designated banks to setup the firewall between C3T and the WAN routers. The following configurations must be strictly followed to allow access to CCASS (& CCMS) functions.

3.2.1 Destination IP addresses

The following table lists all IP addresses of the CCASS (& CCMS) servers that a C3T will connect to:

Server	IP addresses			
	Group 1	Group 2	Group 3	Group 4
Web Server	10.129.1.3	10.129.2.3	10.129.3.3	10.129.4.3
DNS Server	10.129.1.1	10.129.2.1	10.129.3.1	10.129.4.1

Please note that the CCASS (& CCMS) server IP addresses vary for participants / designated banks assigned to different network groups. Please double check your DNS Settings to verify which Group you belong to.

3.2.2 Services

The following services should be granted in the firewall. All services are opened in the CCASS (& CCMS) servers. There is no requirement for CCASS (& CCMS) servers to initiate a connection to the C3T.

Services	Port No.	Protocol	Direction	Description
DNS	53	UDP	From C3T to DNS server	Domain Name Service
HTTPS	443	TCP	From C3T to Web server	Online Traffic
	442	TCP	From C3T to Web server	File Download/Upload Traffic
	441	TCP	From C3T to Web Server	Logon Traffic

3.2.3 Source IP address

Each participant / designated bank circuit is assigned with a pre-defined range of IP addresses. The participant / designated bank should ensure that each C3T should appear with the same IP address as original in each connection. If there is any Network Address Translation (NAT) performed, the participants' / designated banks' firewall should be responsible for translating back it to the original IP address range (assigned by network vendor) or else the C3T login will fail the authentication. In addition, the NAT should be a one-to-one mapping of the C3T. That is, IP address of each C3T should be translated to a unique value within the original IP address range.

C. Windows IP Address and Configuration Setup

4. Configure Windows IP Address

4.1 Please refer to steps below.

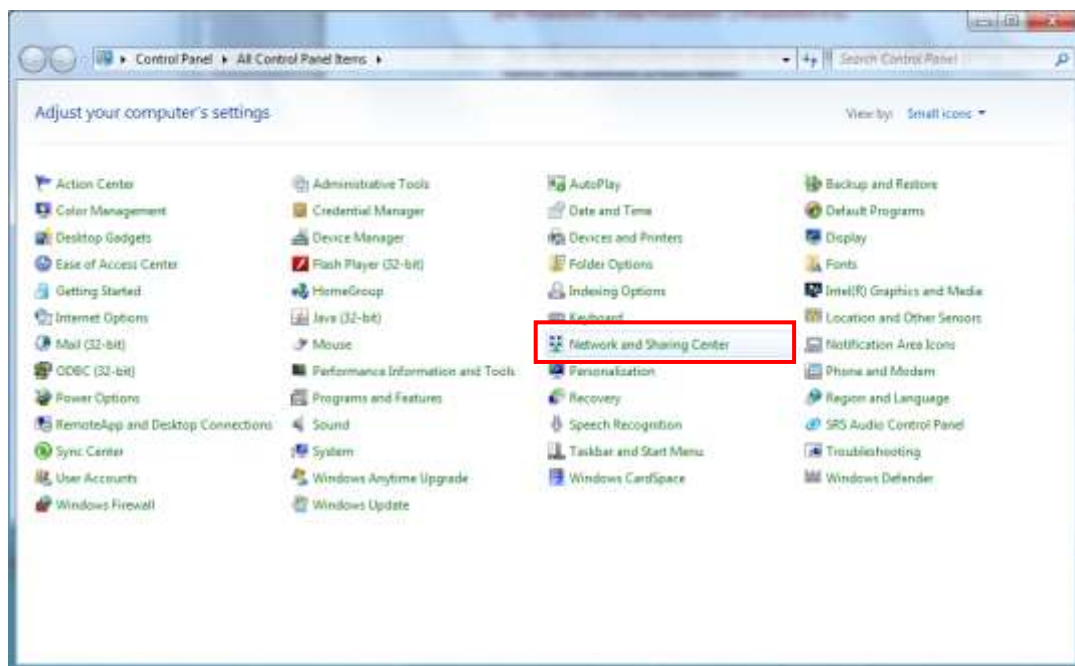
4.2 Configure TCP/IP for the WAN Router & Ethernet Card Connection
(on all supported Windows platform)

4.2.1 The following procedures require an account in “administrator” group. Please check before you perform actions below.

4.2.2 (Windows 7) Click “Start” button, select “Control Panel”.

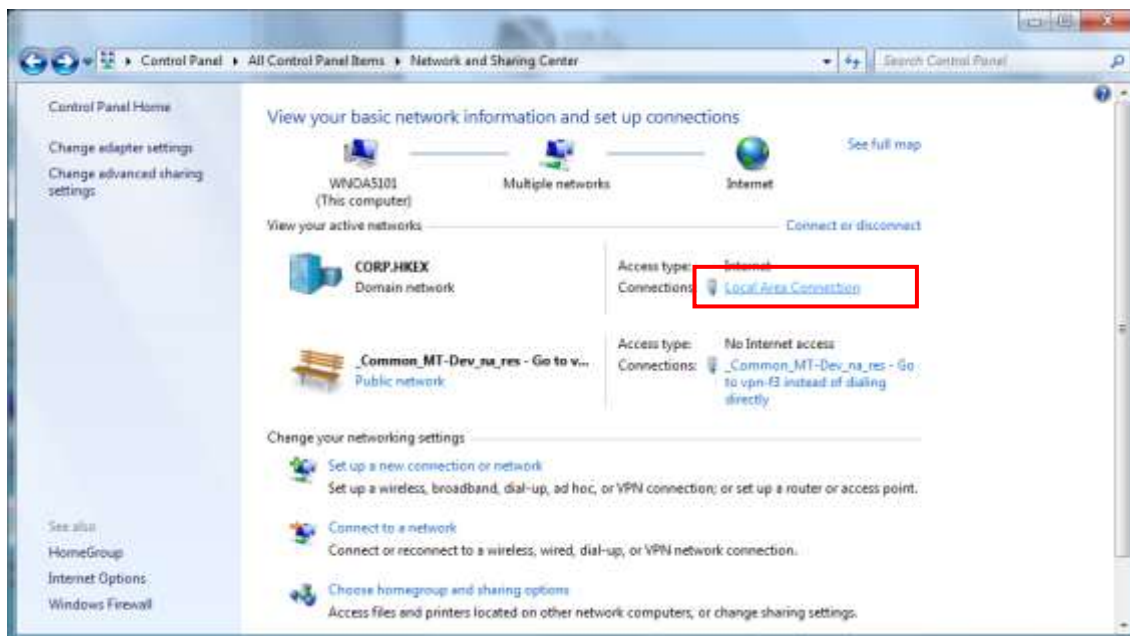
4.2.3 (Windows 8.1 or 10) Right-click “Start” button , select “Control Panel”,

4.2.4 Then click on "Network and Sharing Centre"

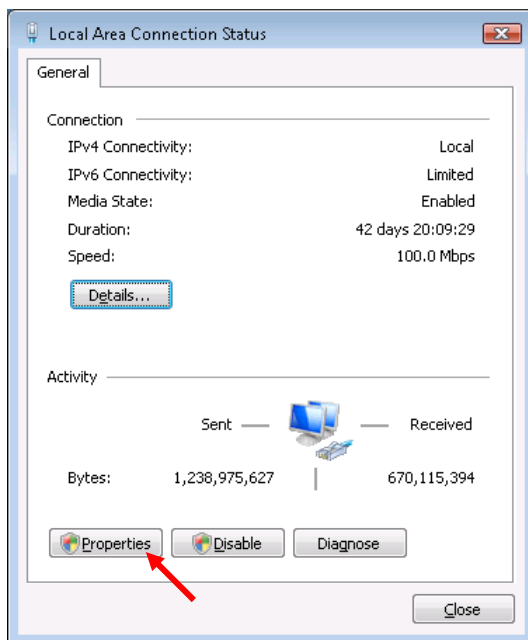


4.2.3 Click “Local Area Connection” under “View your active networks”.

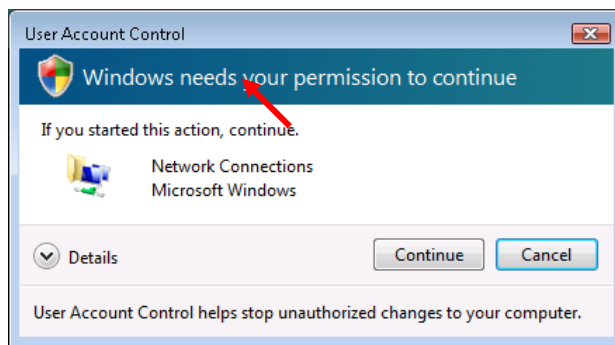
CCASS (& CCMS) Terminal Installation Procedure



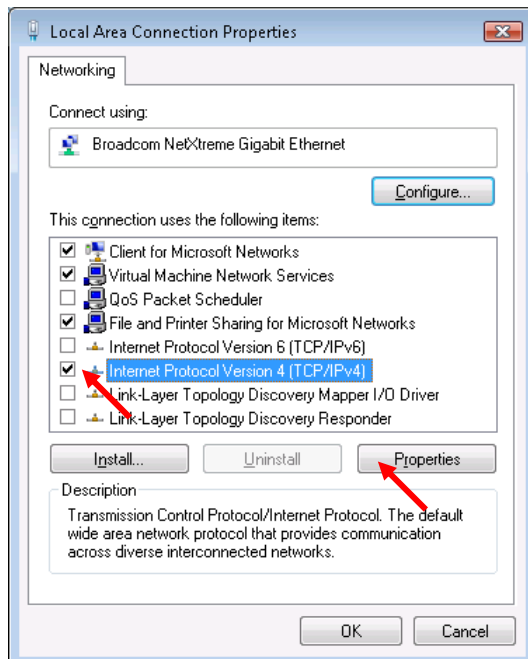
4.2.4 Click "Properties".



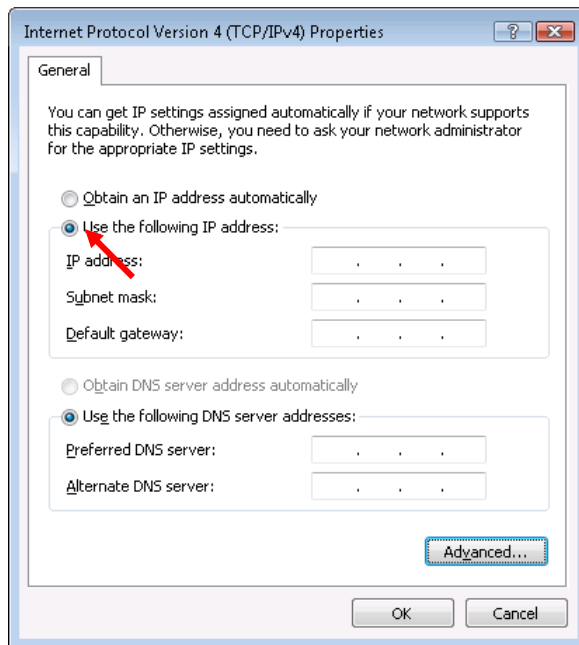
4.2.5 Click “Continue” for alert message.



4.2.6 Check “Internet Protocol Version 4 (TCP/IP)” and click “Properties”.



4.2.7 Select “Use the following IP address” radio button. For participant / designated bank with more than one C3T, please repeat steps 4.8 to 4.13 with different IP Addresses given by vendor for each C3T



4.2.8 Enter the "IP Address" and the "Subnet Mask" with the IP Address and Subnet Mask given by vendor according to the "IP Address Allocation Guidelines" below:-

a. 10.1xx.x.11 ~ 10.1xx.x.120 (for Gateway ending with .1)

C3T: 10.1xx.x.11 - 10.1xx.x.100

PG: 10.1xx.x.101 - 10.1xx.x.120

Reserved: 10.1xx.x.0 - 10.1xx.x.10
10.1xx.x.121 - 10.1xx.x.127

b. 10.1xx.x.139 ~ 10.1xx.x.248 (for Gateway ending with .129)

C3T: 10.1xx.x.139 - 10.1xx.x.228

PG: 10.1xx.x.229 - 10.1xx.x.248

Reserved: 10.1xx.x.128 - 10.1xx.x.138
10.1xx.x.249 - 10.1xx.x.255

4.2.9 Click "Gateway" tab, enter the Gateway IP Address given by vendor in the "Default Gateway"

4.2.10 Enter the DNS Server IP Address given by vendor in the "Preferred DNS Server"

4.2.11 Click "Add" button and then click "OK" button twice to save the changes

4.2.12 Restart the computer

D. CCASS (& CCMS) Software Setup

5. Software installation

5.1 To use CCASS (& CCMS) functions, the following software **must be** installed or configured on the C3T.

- **Internet Explorer**: Configurations must be made or otherwise some C3 functions may not work properly. For details, please refer to **section 6** below
- **Java Plugin**: if you do not have Java Plugin installed, please go to **section 7** for Java Plugin installation. If you have other Java Plugin version on the PC, please make sure all of them will be removed first. For supported JRE versions on Windows, please refers to section A.
- **Acrobat Reader**: Acrobat Reader is required to open the circular files. If you do not have any Acrobat Reader installed. Please follow **section 8** for the installation procedures.

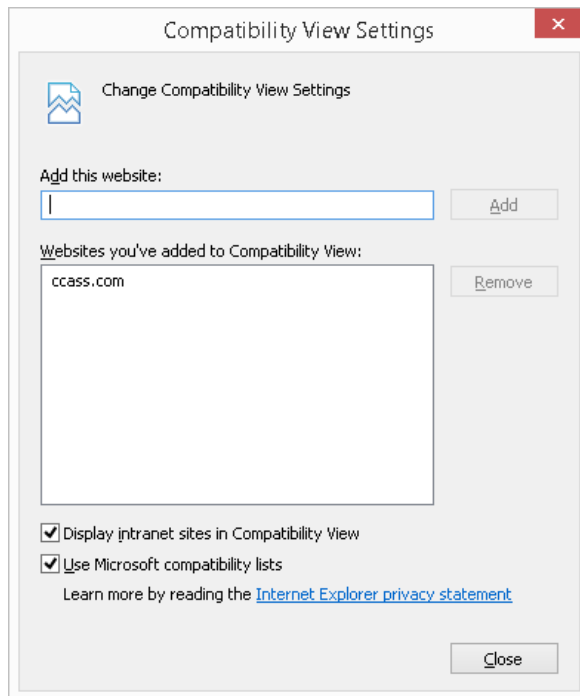
6. Internet Explorer Configurations

Please note that some PC may have disabled user access to settings below and you will need to ask your PC administrator for help. Please also remember to close all your IE windows and start new ones to make the changes effective.

6.1 Compatibility view settings

6.1.1 Open IE windows, and then select “Tools” → “Compatibility View settings”.

6.1.2 Type “www.ccass.com” and then click “Add.” “ccass.com” should be shown at the box “Websites you’ve added to Compatibility View.”



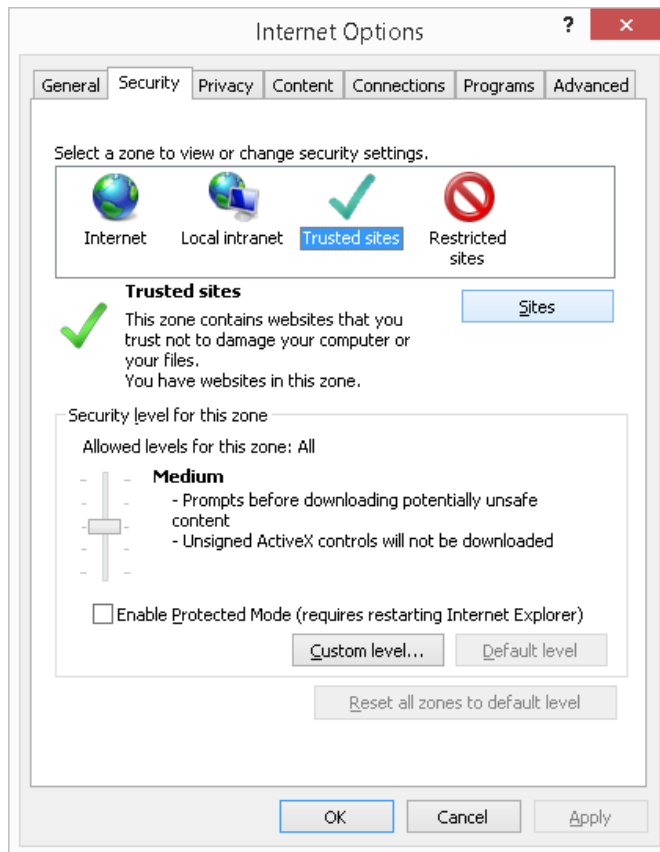
6.1.3 Click Close to close the window

6.2 Trusted site setting

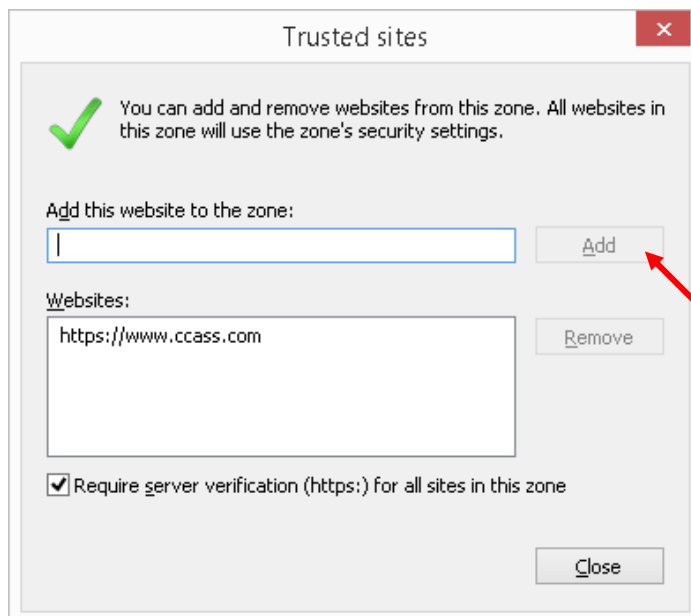
6.2.1 Open IE window, then select “Tools” → “Internet options” and then click on “Security”.

6.2.2 Then click on “Trusted Site” and click on “Sites”

CCASS (& CCMS) Terminal Installation Procedure



6.2.3 Type "https://www.ccass.com" and then click add "Add"

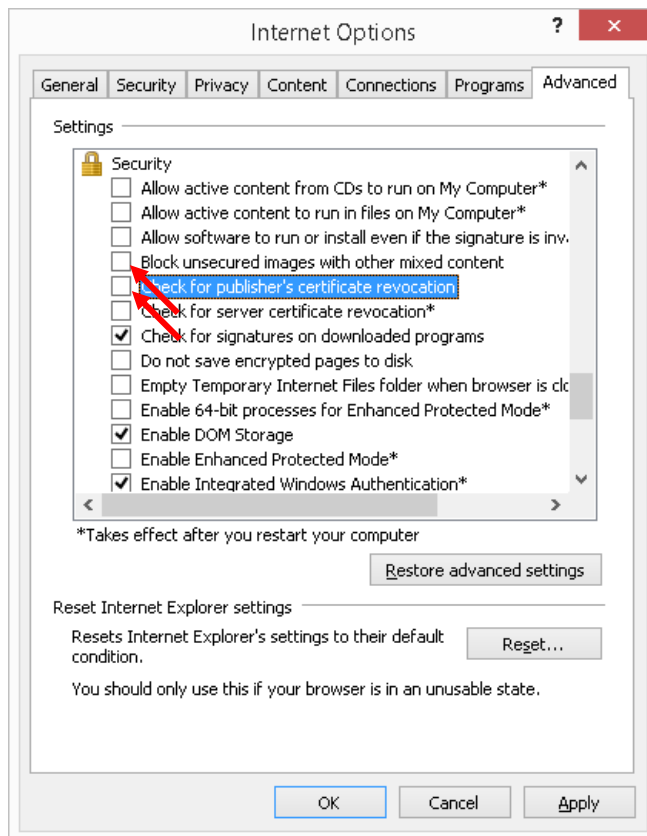


6.2.4 Click Close and then OK to close the windows

6.3 Disable certificate revocation check (for standalone C3T which does not have Internet connection)

CCASS (& CCMS) Terminal Installation Procedure

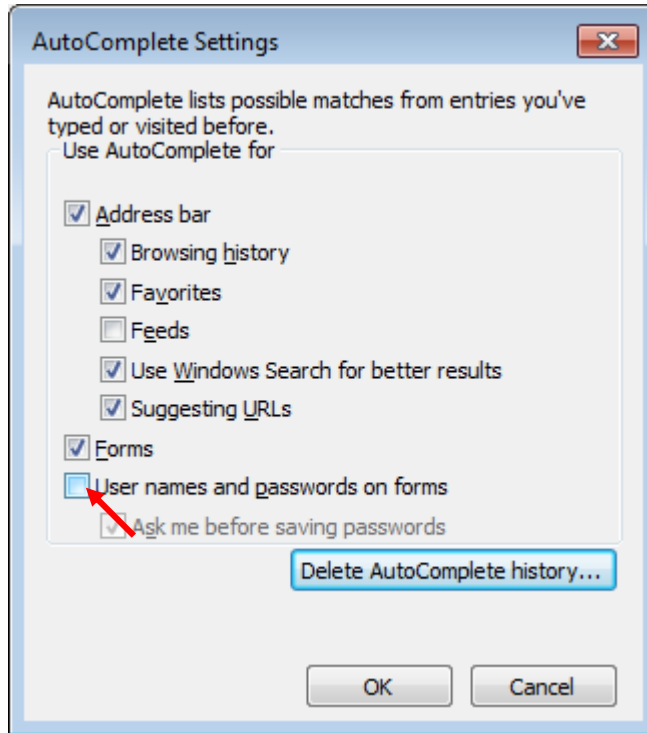
- 6.3.1 Open IE windows, then select “Tools” → “Internet options” and then click on “Security”.
- 6.3.2 Go to Security section and **uncheck** the following options
 - i. Check for publisher’s certificate revocation
 - ii. Check for server certificate revocation



- 6.3.3 Click Apply and OK to close the window

6.4 **Disable AutoComplete for User names and Passwords**

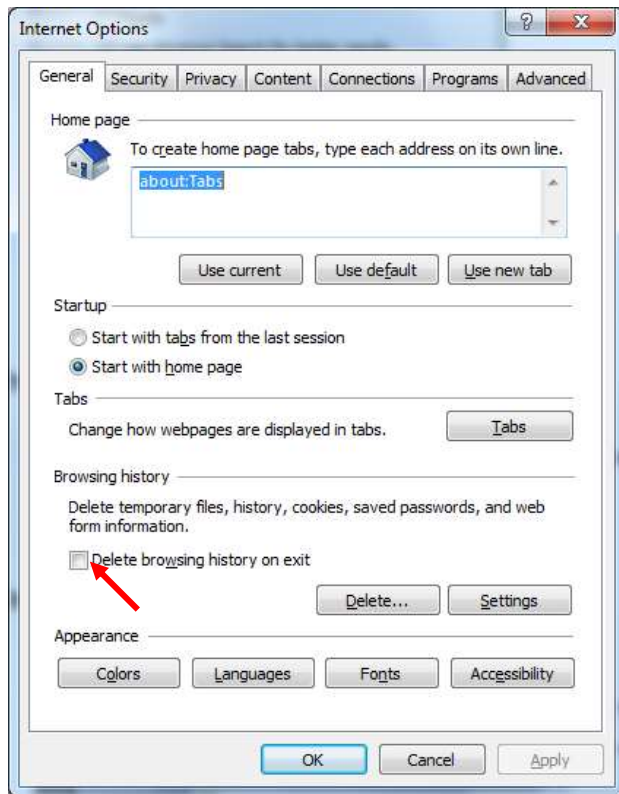
- 6.4.1 Open the IE (Internet Explorer). At the menu bar, select “Tools” and then “Internet Options”. The “Internet Options” window will be popped up. In the window, select “Content” and then “Settings”
- 6.4.2 Unselect the option “User names and passwords on forms”. Click OK to save



6.5 Browsing History

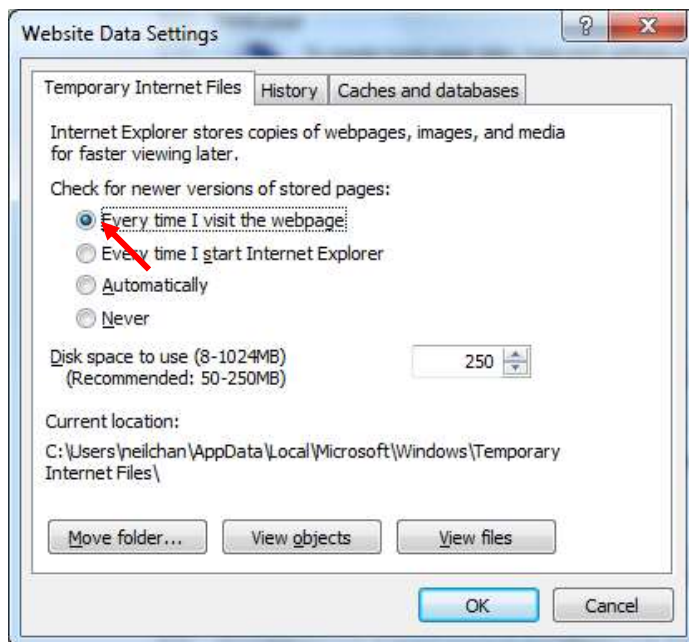
- 6.5.1 Open IE windows, then select “Tools” → “Internet options” and then click on “Browsing History”.
- 6.5.2 Ensure that the option “Delete browsing history on exit” is **not checked**

CCASS (& CCMS) Terminal Installation Procedure



6.5.3 Then click on Settings.

6.5.4 Ensure the option “Every time I visit the webpage” is **checked**



6.6 Enable Pop-up Window

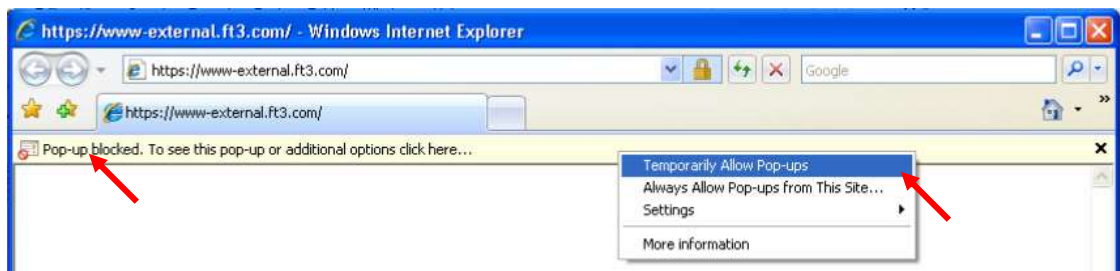
6.6.1 Go to CCASS (& CCMS) URL <https://www.ccass.com>

CCASS (& CCMS) Terminal Installation Procedure

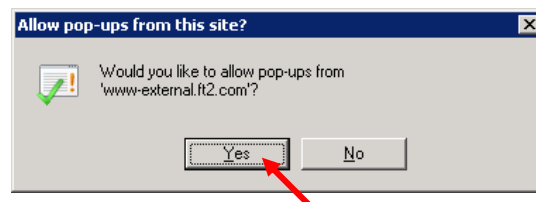
6.6.2 Warning is shown for popping up new window. Click “Close” to dismiss the warning.



6.6.3 Point to “Pop-up blocked” information bar, then right click on it and then click on “Always Allow Pop-ups from This Site...”



6.6.4 Click “Yes” to allow pop-ups from this site



6.6.5 Continue to go to logon page of CCASS (& CCMS)

6.7 Root CA Certificate Update (optional)

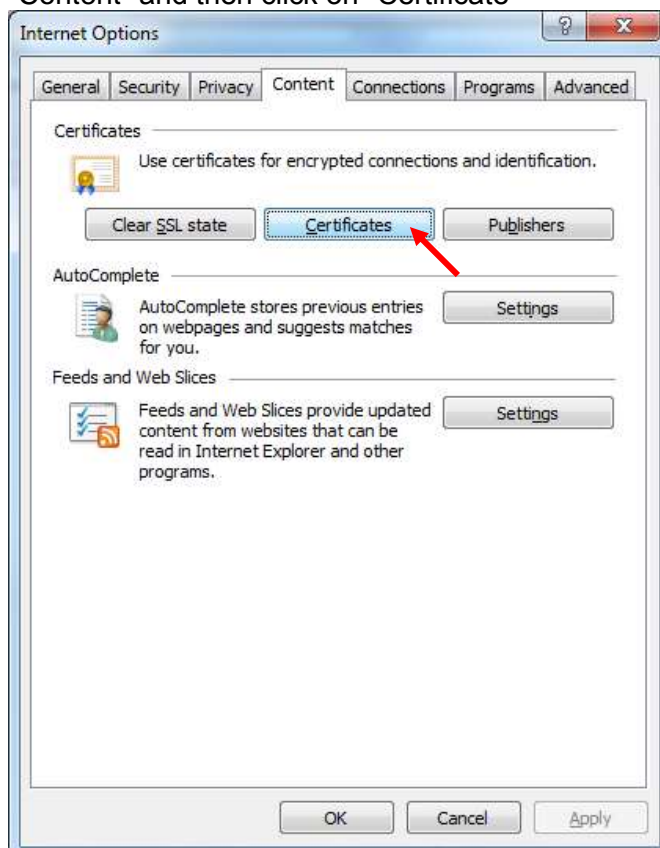
If participants do not have the new root CA certificate installed in their CCASS/3 Terminals, warning window will appear when they attempt to logon CCASS/3.



Therefore, if this warning window **does not appear**, that means the root CA certificate is properly installed already and please **skip** this section (6.7). Otherwise, please follow steps below to verify and install the root CA certificate.

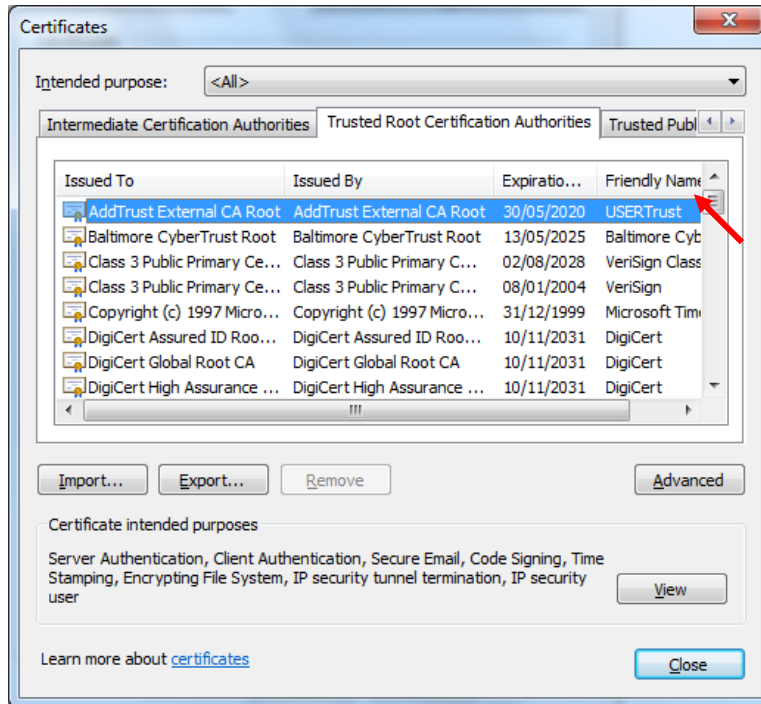
6.7.1 Verify Root CA certificate

6.7.1.1 Click Apply and Open IE windows, then select “Tools” → “Internet options” → “Content” and then click on “Certificate”

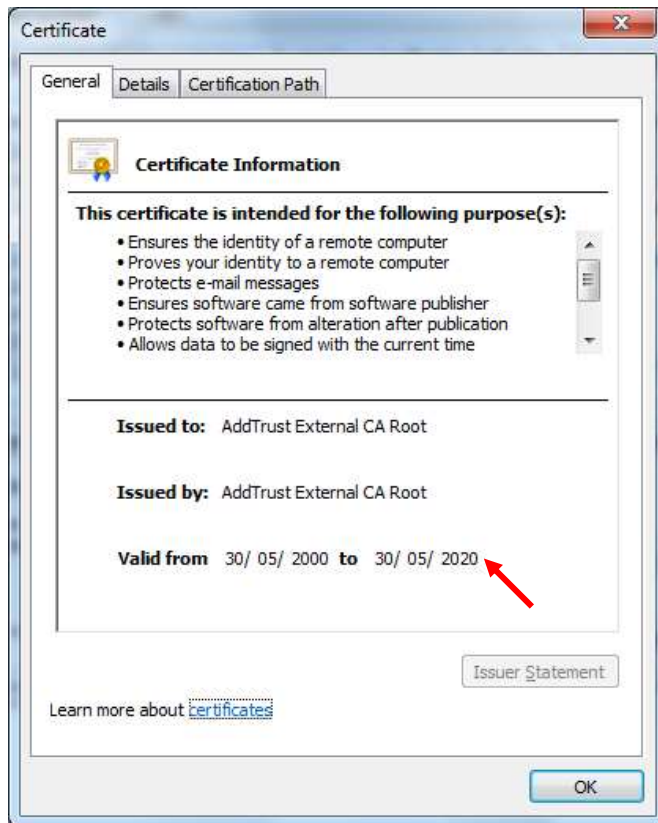


CCASS (& CCMS) Terminal Installation Procedure

6.7.1.2 The “Certificates” window will be prompted. Select “Trusted Root Certificate Authorities”. From the list, click “issued by” to sort the entries and select the one which is issued by “AddTrust External CA Root”. Then click “View”



6.7.1.3 After you click “View”, the “Certificate” window will be prompted. Check the validation period to see if the certificate is valid to 30/05/2000 to 30/05/2020



6.7.2 Install Root CA certificate

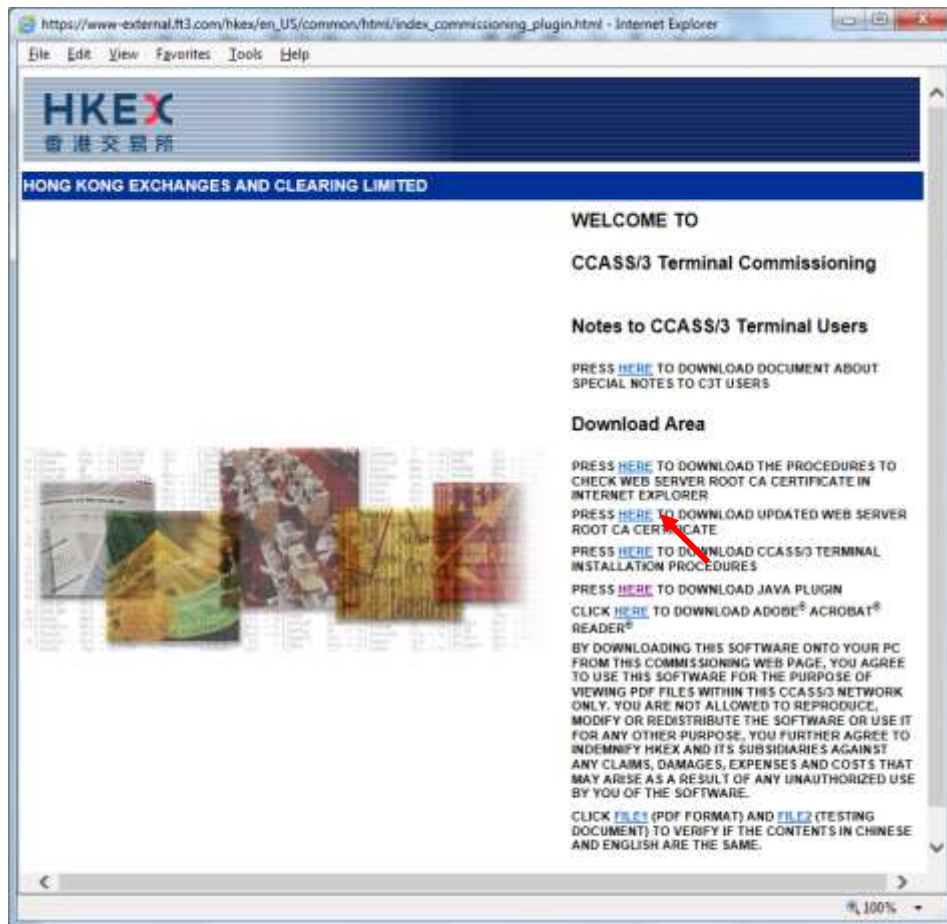
6.7.2.1 If you do not have any certificate issued by “AddTrust External CA Root”, please follow steps below to install it.

6.7.2.2 Go to the commissioning web site with the following

URL: <https://www.ccass.com/commissioning/download>

Then click the link “PRESS HERE TO DOWNLOAD UPDATED WEB SERVER ROOT CA CERTIFICATE” to download the new root CA certificate

CCASS (& CCMS) Terminal Installation Procedure

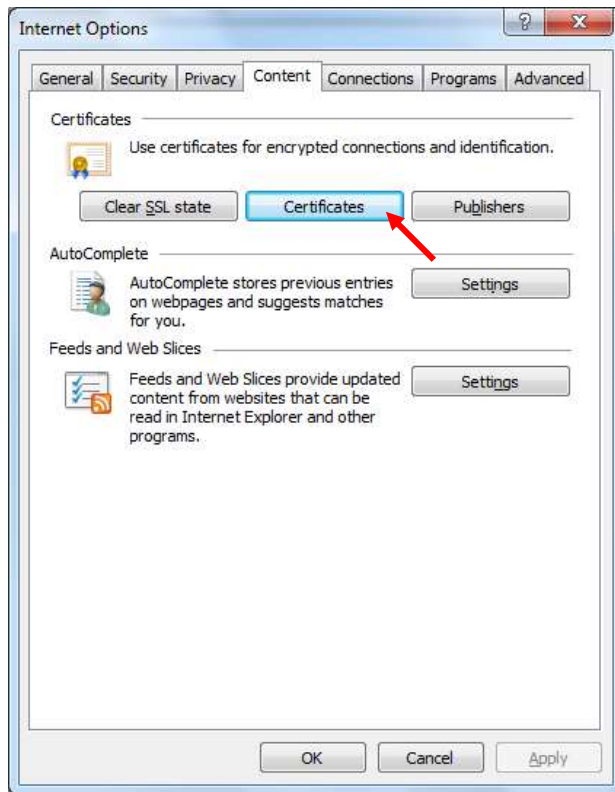


6.7.2.3 Right click on the link and select “Save target as”. Then save the file in a temporary folder e.g. “(C:\temp\)” (you do not need to change the filename)

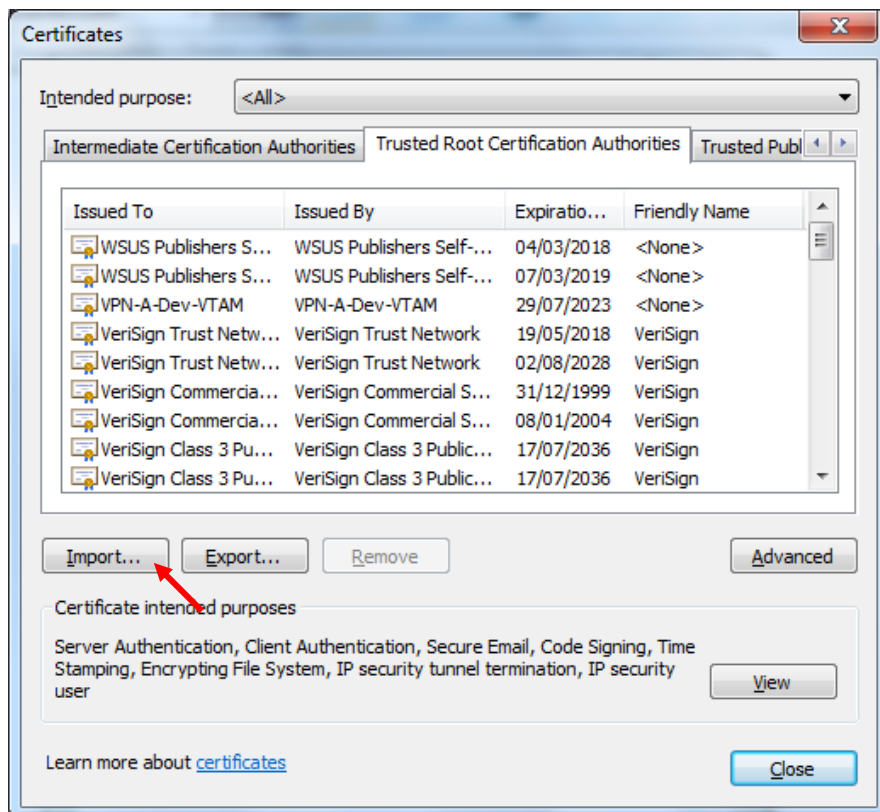


6.7.2.4 Open the IE (Internet Explorer). At the menu bar, select “Tools” (工具) and then “Internet Options” (網際網路選項). The “Internet Options” window will be popped up. In the window, select “Content” (內容) and then “Certificates” (憑證)

CCASS (& CCMS) Terminal Installation Procedure



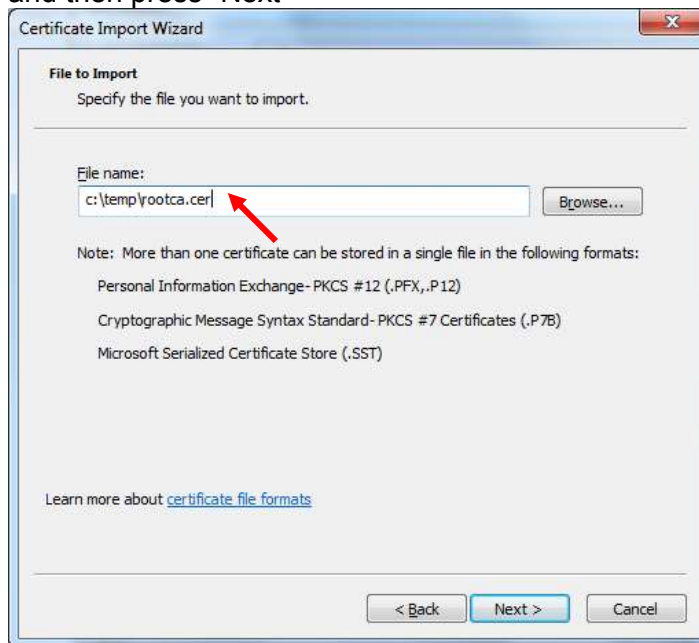
6.7.2.5 The “Certificate Manager” window will be prompted. Select “Trusted Root Certification Authorities” (信任的根憑證授權) and then “Import ...” (匯入)



6.7.2.6 Press “Next”



6.7.2.7 Type the path to the downloaded root CA file, e.g. “c:\temp\rootca.cer” in “File name” and then press “Next”

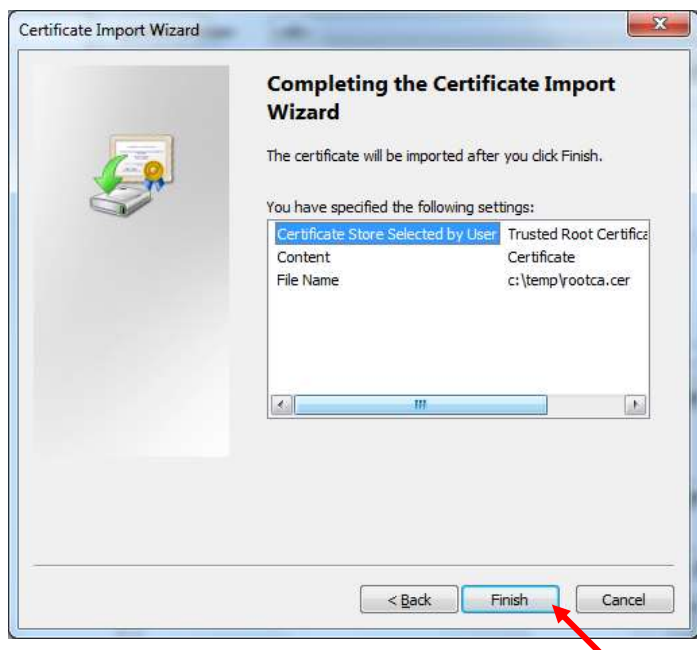


6.7.2.8 Make sure “Trusted Root Certification Authorities” (信任的根憑證授權) is selected and then press “Next”

CCASS (& CCMS) Terminal Installation Procedure



6.7.2.9 Press Finish



6.7.2.10 Click "Yes" to dismiss the warning

CCASS (& CCMS) Terminal Installation Procedure



6.7.2.11 Press "OK"



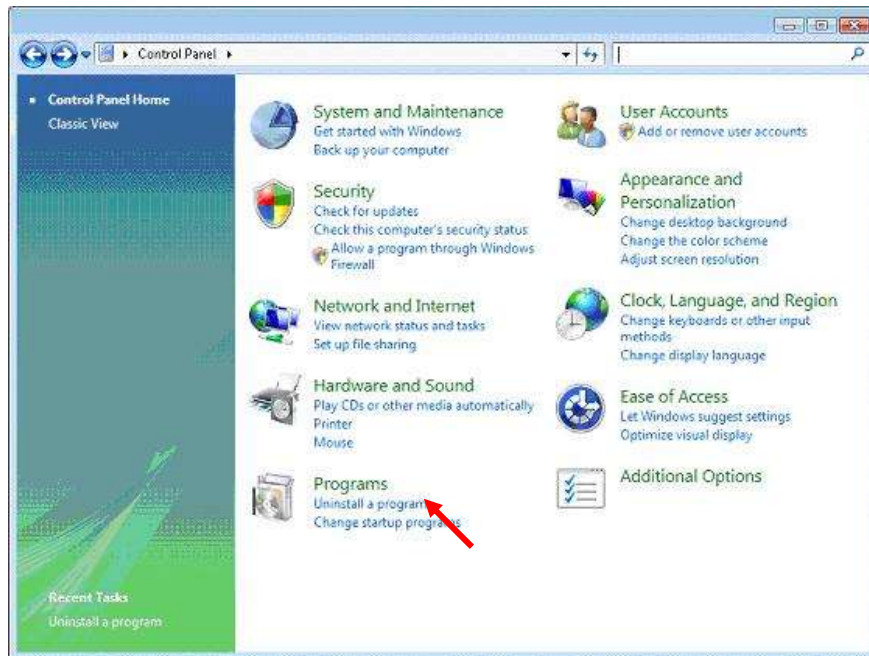
6.7.2.12 If the certificate warning window still appears on C3 logon page, please check with your PC administrator if there is any security policy to restrict you from certificate import.

7. Install Java Plugin (JRE)

7.1 Verify Java Plugin

As C3T function requires Java Plugin (JRE) and supported version may vary on different Windows, version has to be verified and please refer to section A for details on JRE version.

7.1.1 Click “Start” button, select “Control Panel”



7.1.2 Click the link “Uninstall a program” under “Programs”

Intel® Trusted Connect Service Client	Intel Corporation	30/11/2012	10.6 MB	1.23.605.1
Intel® USB 3.0 extensible Host Controller Driver	Intel Corporation	01/12/2012	18.4 MB	1.0.3.214
Japanese Fonts Support For Adobe Reader X	Adobe Systems Incorporated	02/01/2013	61.6 MB	10.0.0
Java 8 Update 77	Oracle Corporation	19/04/2016	89.1 MB	8.0.770.3

7.1.3 Find “Java X Update XX” in the list

- If non-supported JRE is found, please go to 7.2 for uninstallation
- If no JRE are found, the please go to 7.3 for Java plugin installation

7.2 Uninstall previous version of Java Plugin

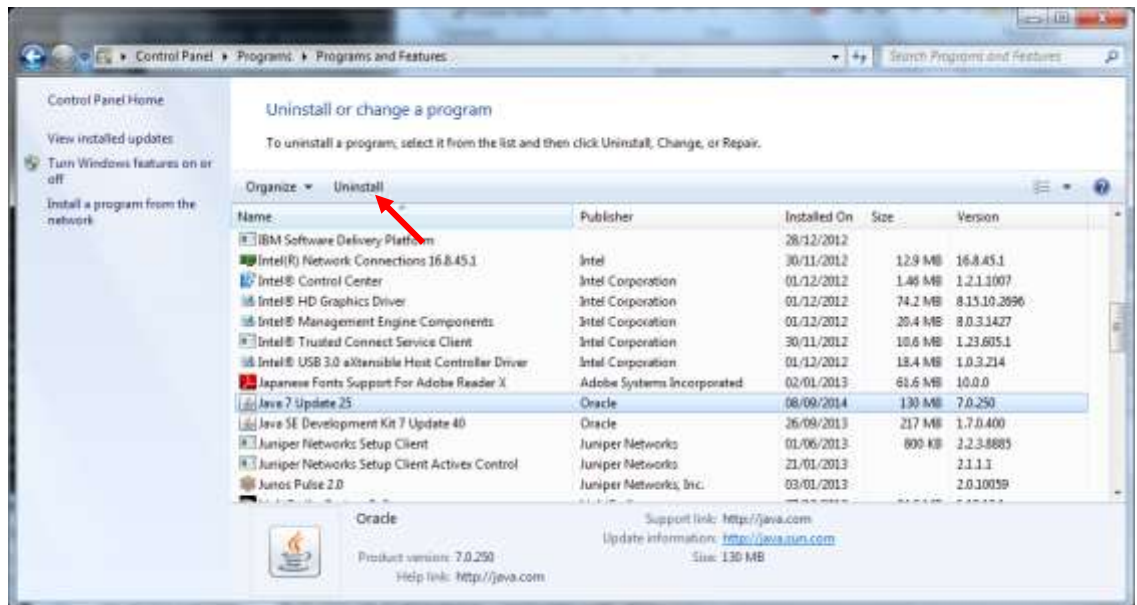
Please make sure any previous version of JRE is removed before the new one is installed.

7.2.1 Follow procedures in 7.1 to go to “Uninstall a program”.

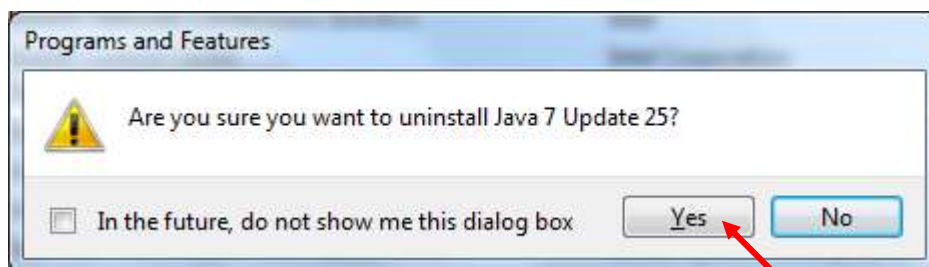
7.2.2 Ensure all Internet Explorers windows are closed.

7.2.3 Highlight the JRE item, and then click on the “Uninstall” button at the top.

CCASS (& CCMS) Terminal Installation Procedure

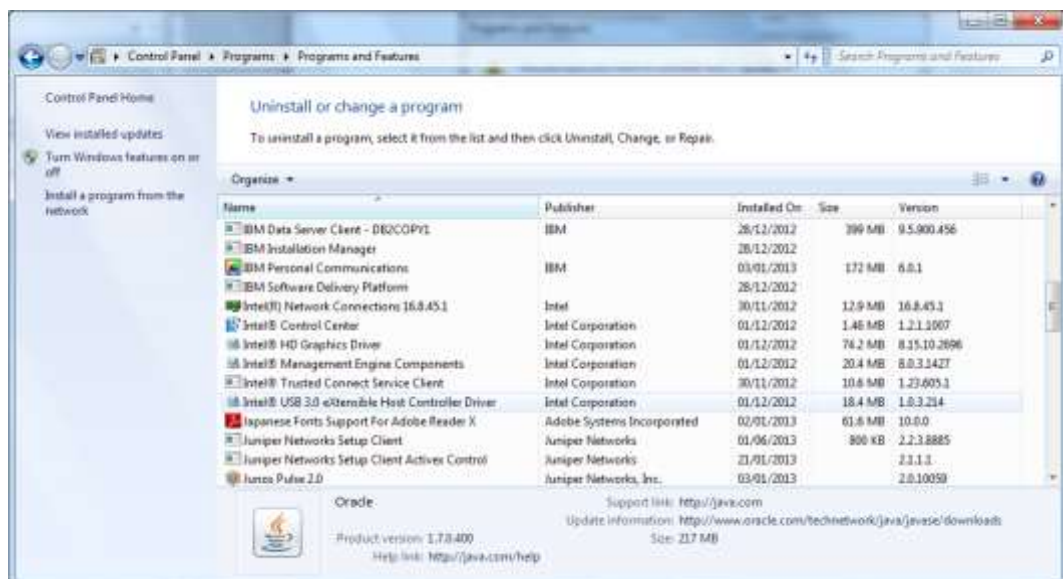


7.2.4 Click “Yes” button to continue



7.2.5 Click “Yes” when the “User Control Windows” appear

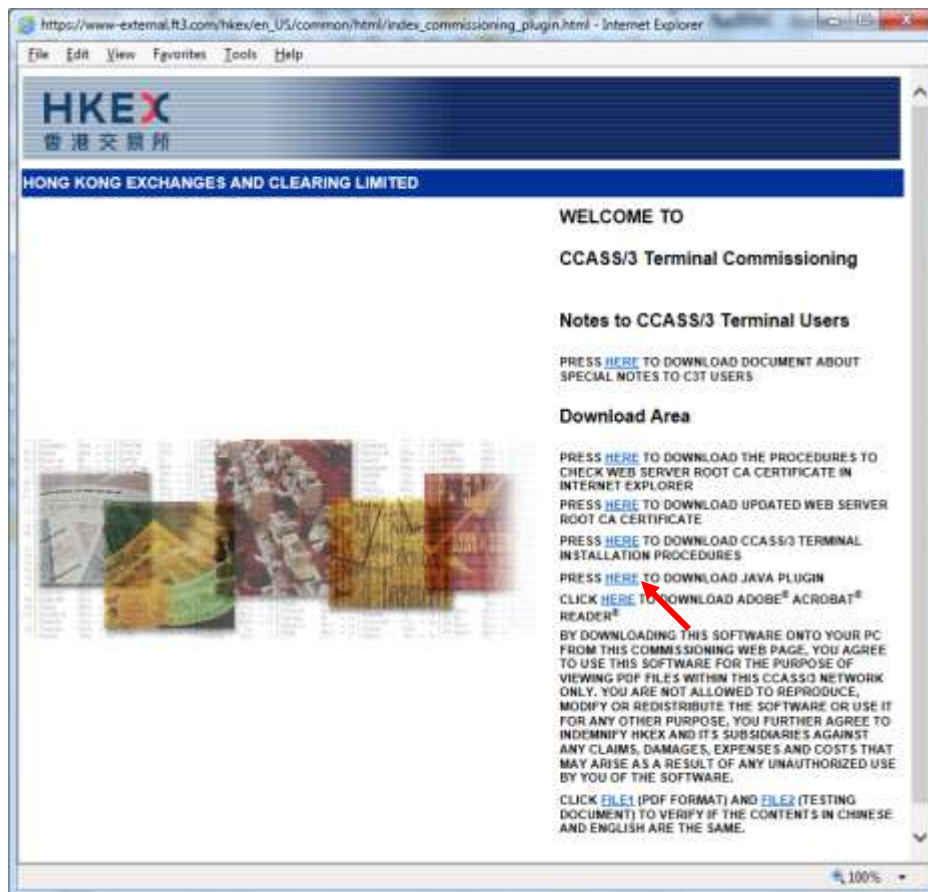
7.2.6 Check that all JRE items should be removed



7.2.7 Restart the computer

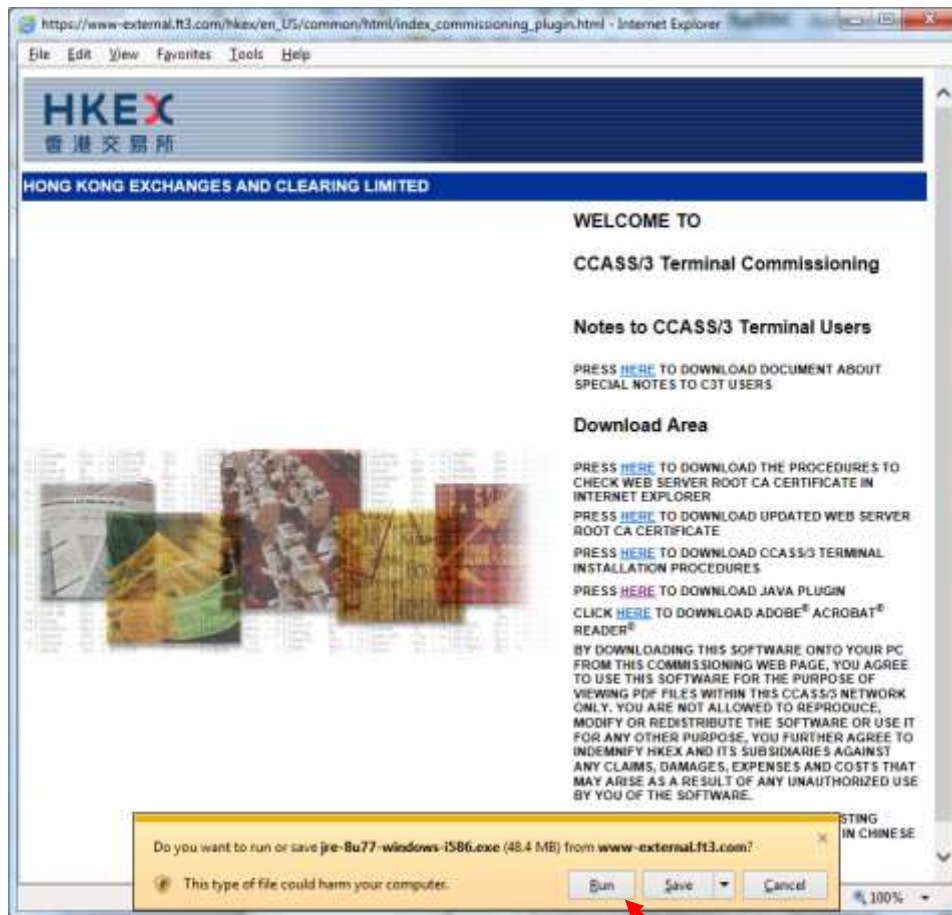
7.3 Install java Plugin

- 7.3.1 Launch Internet Explorer, enter <https://www.ccass.com/commissioning/download> in address box. Then click on “PRESS HERE TO DOWNLOAD JAVA PLUGIN IF NEEDED”.



- 7.3.2 Click “Run” button to continue and start to install Java Runtime

CCASS (& CCMS) Terminal Installation Procedure



7.3.3 Click "Yes" when the "User Control Windows" appear

7.3.4 Ensure all Internet Explorers windows are closed.

7.3.5 Click "Install>" button to continue

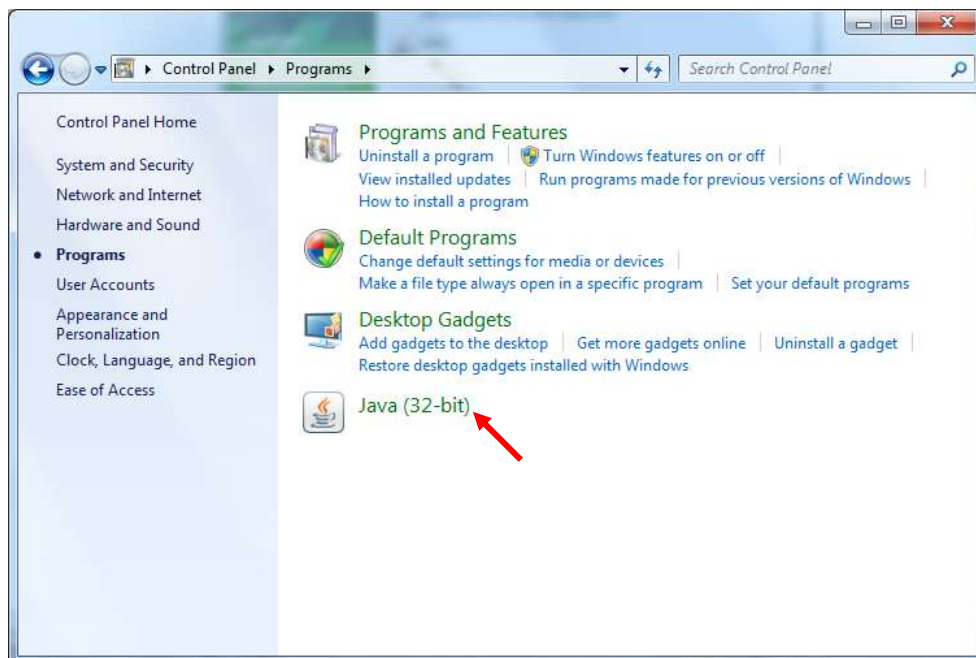


7.3.6 Wait for installation to complete and click “Close”

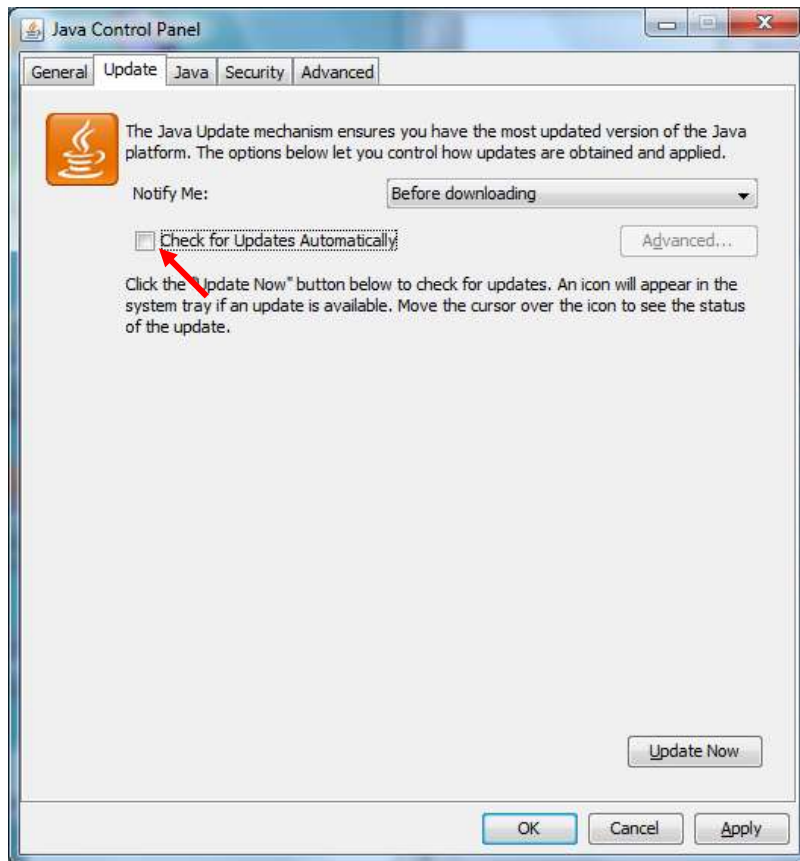


7.4 Java Plugin Configurations

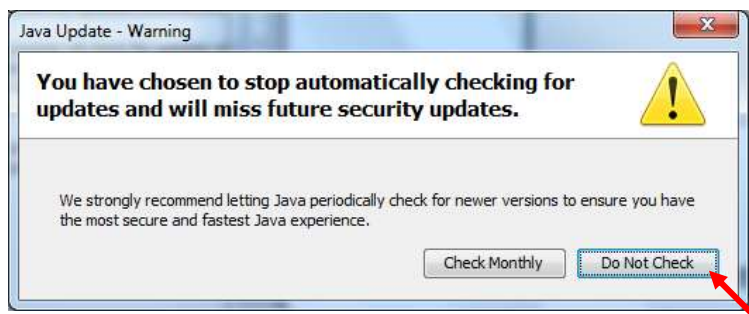
7.4.1 Auto update should be disabled. To do so, click “Start” to launch start menu then “Control Panel” and then click “Program” and then click “Java”



7.4.2 Select “Update” tab and uncheck “Check for Updates Automatically”.



7.4.3 Click “Never Check” button in the warning dialog.

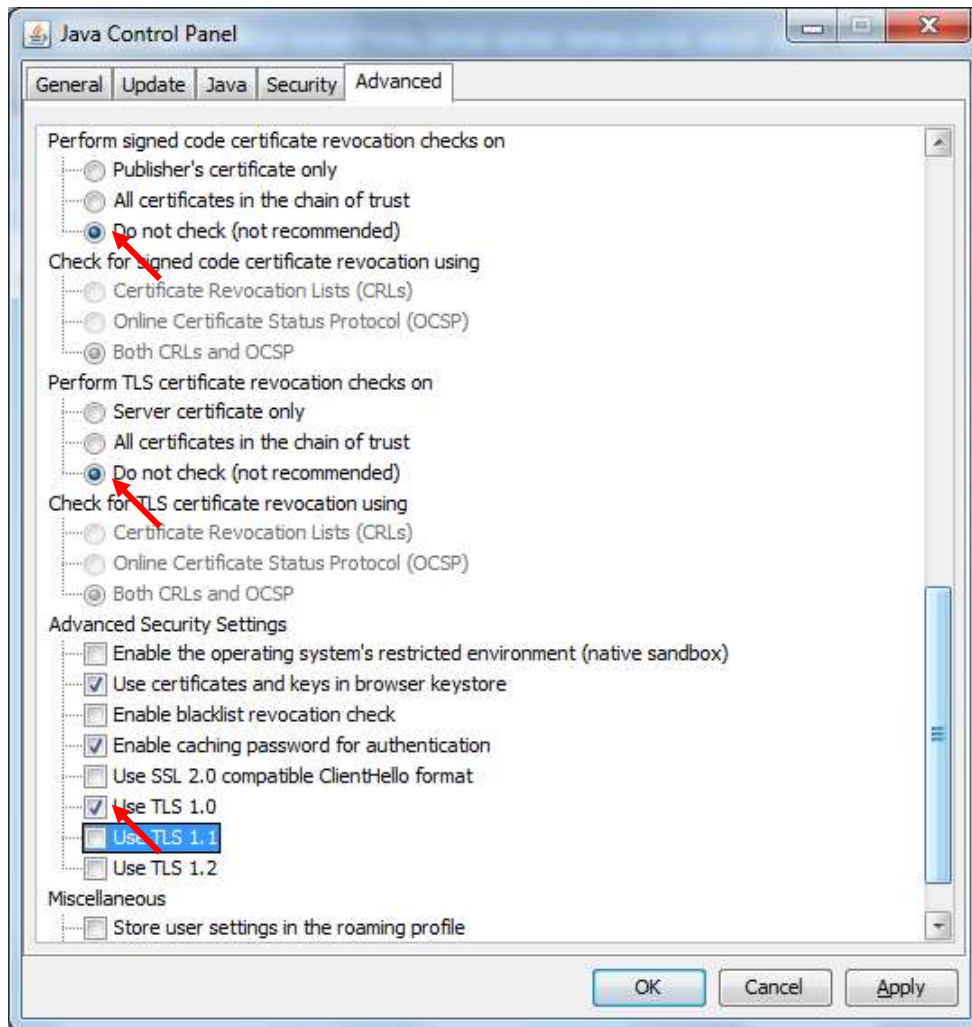


7.4.4 Click “Advanced” Tab and then scroll to the bottom.

7.4.5 Select the following settings in Advanced settings

- a) Perform signed code certificate revocation checks on
Do not check
- b) Perform TLS certificate revocation checks on
Do not check
- c) Advanced Security Settings
Use TLS 1.0

CCASS (& CCMS) Terminal Installation Procedure



7.4.6 Click Apply and then OK to exit the window.

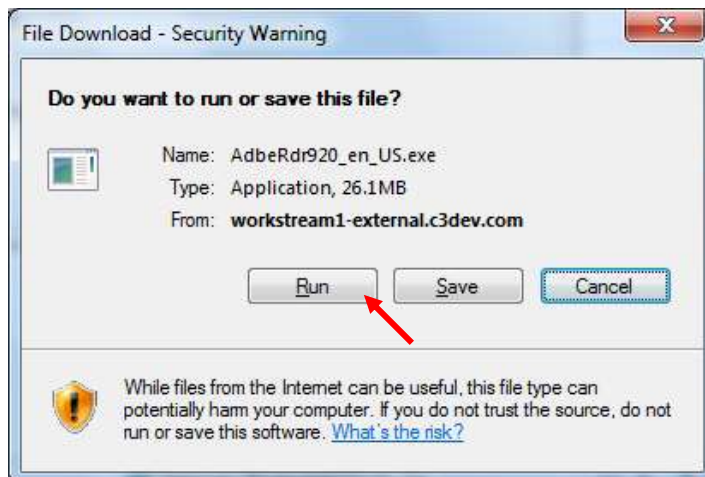
8. Install Adobe Acrobat Reader

8.1 Install Reader

- 8.1.1 Launch Internet Explorer, enter <https://www.cass.com/commissioning/download> in address box. Click the associated link to download Adobe Acrobat Reader.

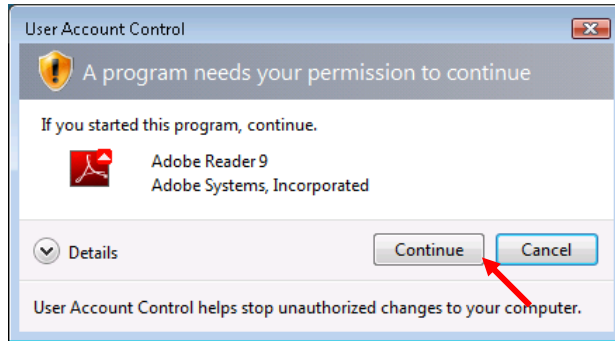


- 8.1.2 Click **“Run”** or **“Open”** button and wait for installation starting after the file to be downloaded to the PC

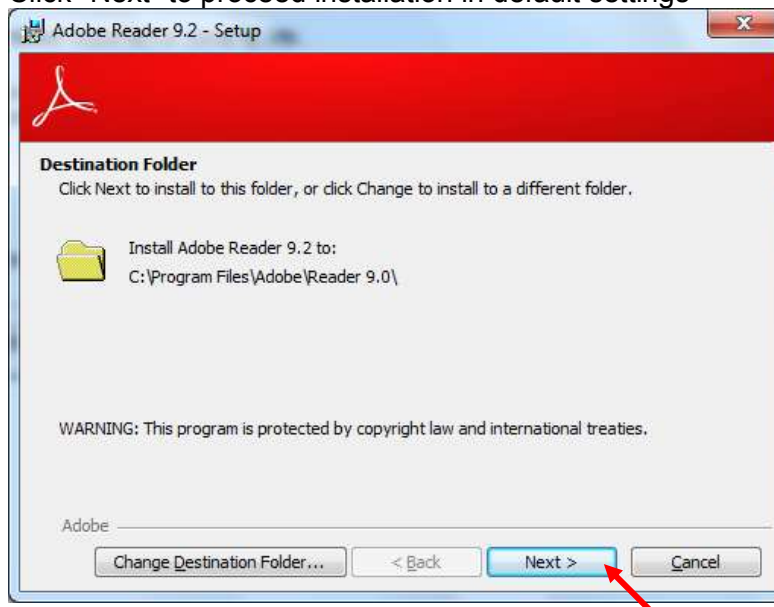


CCASS (& CCMS) Terminal Installation Procedure

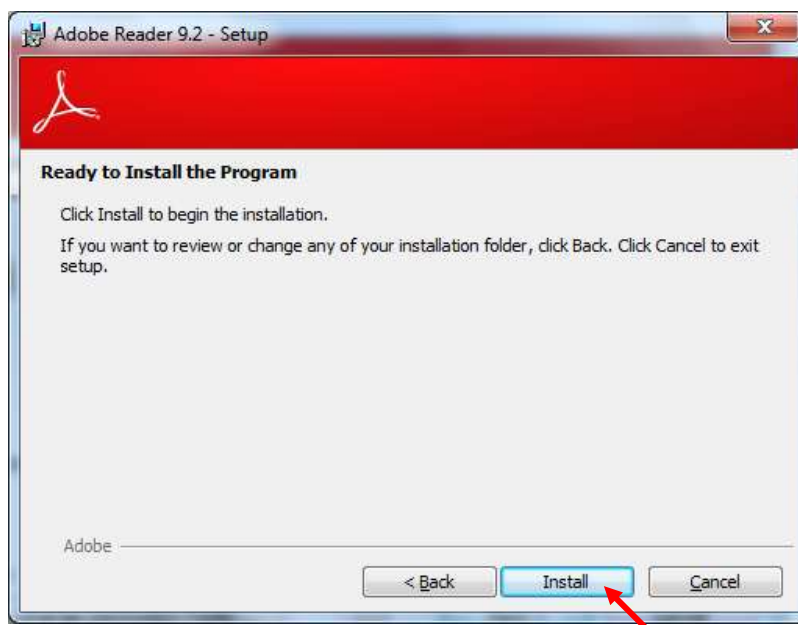
8.1.3 Click “Continue” button to continue and start to install Acrobat Reader



8.1.4 Click “Next” to proceed installation in default settings

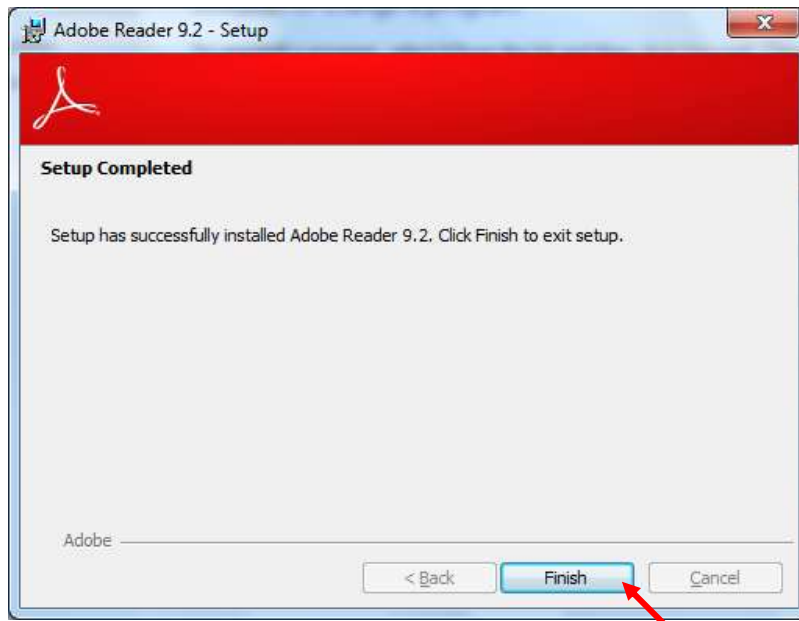


8.1.5 Click “Install” to start installation



8.1.6 Click “Finish” to complete installation.

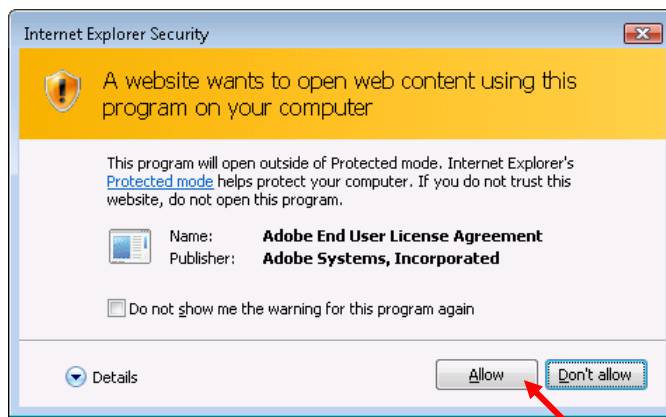
CCASS (& CCMS) Terminal Installation Procedure



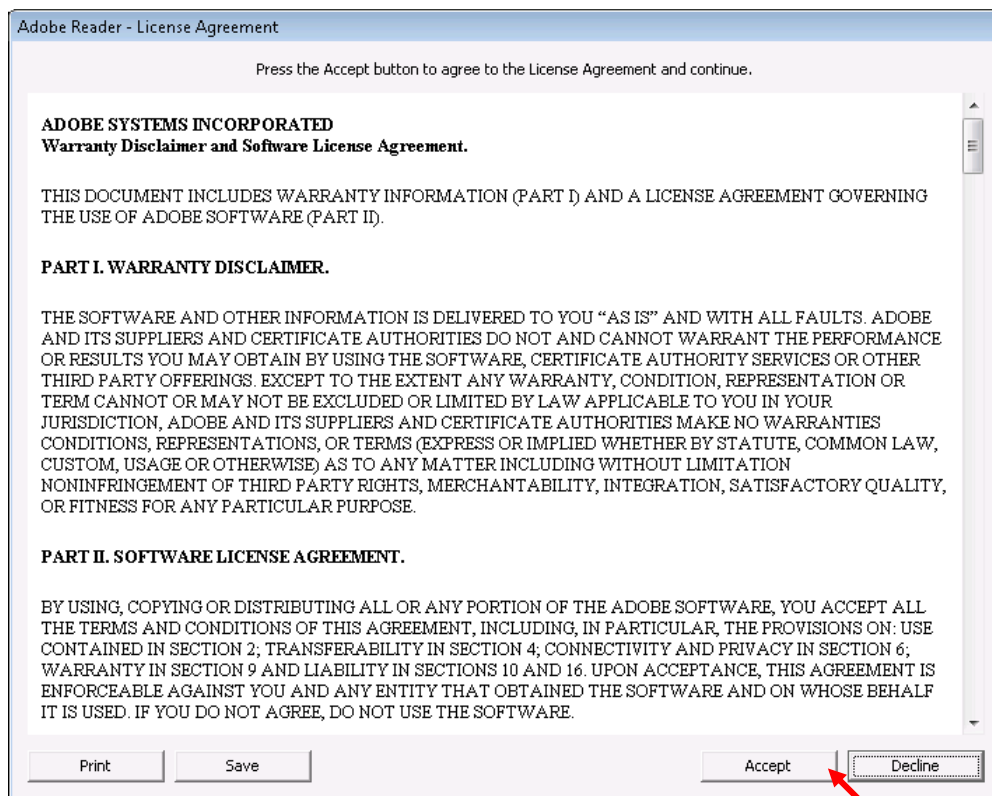
- 8.1.7 Click “**FILE1**” and “**FILE2**” to view testing files. The verification is successful if the contents in Chinese and English are the same.



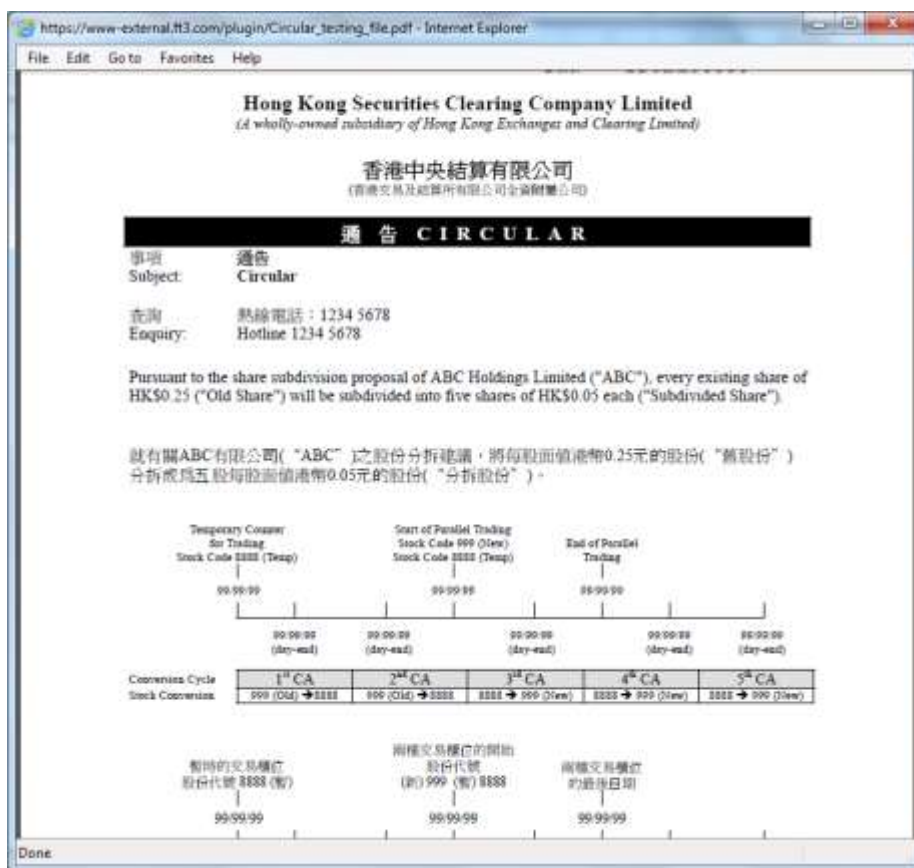
8.1.8 Click “FILE1” and then click “Allow” to open the file



8.1.9 For first use of Acrobat Reader, read Software License Agreement carefully and click “Accept” button if you accept it.



8.1.10 “FILE1” successfully opened by Acrobat Reader.



8.1.11 Click “FILE2”. Document successfully opened by IE.

CCASS (& CCMS) Terminal Installation Procedure

https://www-external.ft3.com/plugin/Circular_testing_file.gif - Internet Explorer

File Edit View Favorites Tools Help

Hong Kong Securities Clearing Company Limited
(A wholly-owned subsidiary of Hong Kong Exchanges and Clearing Limited)

香港中央結算有限公司
(香港交易及結算所有限公司全資附屬公司)

通告 C I R C U L A R

事項 通告
Subject: Circular

查詢 熱線電話：1234 5678
Enquiry: Hotline 1234 5678

Pursuant to the share subdivision proposal of ABC Holdings Limited ("ABC"), every existing share of HK\$0.25 ("Old Share") will be subdivided into five shares of HK\$0.05 each ("Subdivided Share").

就有關 ABC 有限公司 ("ABC") 之股份分拆建議，將每股面值港幣 0.25 元的股份 ("舊股份") 分拆成為五股每股面值港幣 0.05 元的股份 ("分拆股份")。

	Temporary Counter for Trading Stock Code 8888 (Temp)	Start of Parallel Trading Stock Code 999 (New) Stock Code 8888 (Temp)	End of Parallel Trading		
	99/99/99	99/99/99	99/99/99		
	99/99/99 (day-end)	99/99/99 (day-end)	99/99/99 (day-end)	99/99/99 (day-end)	99/99/99 (day-end)
Conversion Cycle	1 st CA	2 nd CA	3 rd CA	4 th CA	5 th CA
Stock Conversion	999 (Old) → 8888	999 (Old) → 8888	8888 → 999 (New)	8888 → 999 (New)	8888 → 999 (New)

兩種交易價位的開始

100%

B. Initialise Smartcard and First Time Logon to CCASS (& CCMS)

9. Initialise Smartcard

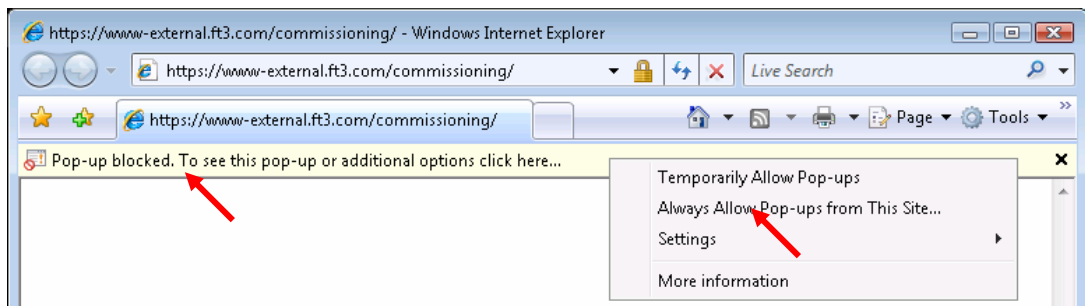
9.1 Initialise card

- 9.1.1 Launch Internet Explorer, insert Smartcard and type CCASS (& CCMS) Logon URL <https://www.ccass.com/commissioning>

Warning is shown for popping up new window. Click “Close” to dismiss the warning.



- 9.1.2 Point to “Pop-up blocked” information bar, then right click on it and then click on “Always Allow Pop-ups from This Site...”

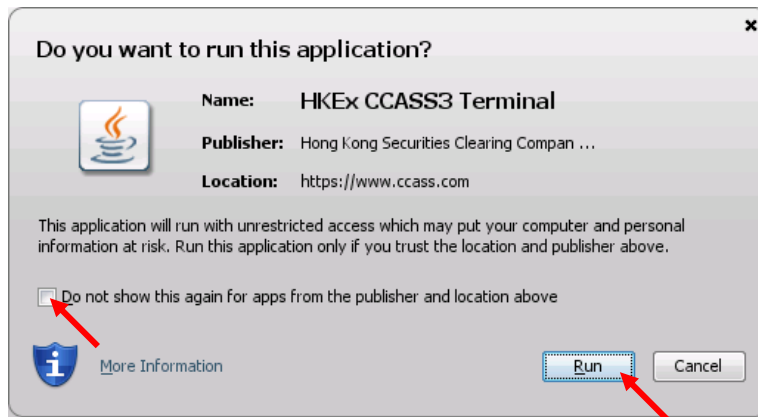


- 9.1.3 Click “Yes” to allow pop-ups from this site



CCASS (& CCMS) Terminal Installation Procedure

- 9.1.4 To perform CCASS (& CCMS) function, an applet will be downloaded and the following security warning will be prompted up:



- 9.1.5 Check "Do not show this again for apps from the publisher and location above" and then click "Run" button to always grant the session



- 9.1.6 Please wait until the next windows pop up.
Smartcard must be initialised for first time usage. Click "HERE" icon to proceed



9.1.7 Enter New Password and New Password (Re-enter) then click “Initialise” button



https://www-external.ft3.com:441/hkex/en_US/common/html/init_...

HKEX
香港交易所

Initialise Smartcard

Please insert your smartcard into the reader and enter a password (6 to 8-digit number) for your smartcard.

New Password :

New Password (Re-enter) :

9.1.8 Click “OK” button to finish initialisation and go back to logon windows



10. Logon to CCASS (& CCMS)

10.1 After initialising the smartcard, go back to the logon windows as follows



10.2 Enter your password and click “Commission” button in the page to perform C3T commissioning



10.3 C3T installation procedure finishes. Close all browsers.