CCASS/ VaR Online/ RAP Technical Guide for HKSCC Participants

Version:	3.0
Date:	Mar 2022

Modification History

Version	Date	Modified By	Synopsis
1.0	May 2021	HKSCC	First issue
2.0	Jun 2021	HKSCC	Updated the following • section 4.6 IP addresses of VaR Online • section 5.10 new section on TLS Connection Settings
3.0	Mar 2022	HKSCC	• Updated for replacing IE 11 by MS Edge as the supported browser of C3T(Section 5.3 to Section 5.10) • Added support of smartcard reader model IDBridge CT30 • Added support of Google Chrome version for VaR Online

TABLE OF CONTENTS

1 OVERVIEW

1.1 Background

This document serves as a CCASS technical guide for HKSCC Participants to install and configure their PC terminals to access CCASS via SDNet. Section 2 provides a summary of system requirement, while sections 3 & 4 documented the communication line & network setup requirement.

HKSCC Participants should refer Section 5 for the hardware, software requirements and configuration for installing CCASS Terminals. *HKSCC Participants, being Clearing Participants*, should also access to Report Access Platform (RAP) for risk related reports and VaR Online for margin & stress test simulation purposes. Respective requirements are documented in Sections 6 & 7.

2 System Requirements

2.1 PC Configuration Requirements

Highlighted below are the minimum PC configurations for CCASS Terminals, RAP & VaR Online.

Item	CCASS	RAP	VaR Online
CPU	1GHz	1GHz	2.4GHz
Memory	2GB	2GB	8GB
HD	20GB	20GB	22GB
OS	Win 10 Pro (64 bit) Win 8.1 Pro (64 bit) [1]	Win 10 Pro (64 bit)	Win 10 Pro (64 bit)
Browser	IE 11[2] and MS Edge[3] version 94 or above	N/A	Google Chrome[4]
JRE	Oracle JRE 8u311[5] (both x86 and x64)	N/A	N/A
Software	• CCASS Smartcard Client • Acrobat Reader 11 or above • Anti-virus	• SFTP Client • Anti-virus	• Anti-virus
Security Device	Smartcard Reader[6]	N/A	N/A
Bandwidth[7]	1M	1M	1M

[1] *Microsoft will end support for Microsoft Windows 8.1 on 10 January 2023, Therefore, all CCASS (CCMS) terminals with Windows 8.1 Pro have to be upgraded to Windows 10 Pro before December 2022.*

[2] *Microsoft will end support for Internet Explorer 11 on 15 June 2022. Therefore, all CCASS(CCMS) terminals have to be upgraded to MS Edge browser before 1 June 2022*.

[3] *With Internet Explorer Mode enabled for CCASS/3 Terminal website*

[4] *Please install Google Chrome version 100.0.4896.88 to prepare for the Official Launch of VaR Platform and its version will be in general aligned with the Google Chrome used in HKATS.*

[5] *One needs proper license subscription to download Oracle JRE 8u311. Please refer to details on (https://www.oracle.com/java/java-se-subscription.html) about Oracle Java SE Desktop subscription. And then download Oracle JRE 8u311 from (https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html).*

[6] *CCASS currently support Thales GemPCUSB-SL(IDBridge CT40)(USB), IDBridge CT30 and GemPCUSB-SW (USB)*

[7] *Minimum requirement, CP should assess and evaluate its own bandwidth requirement based on their business needs.*

2.2 Computer Virus/Worm Security Measures:

Computer virus or worms are one of the concerns in security measure of computer system. Various security measures have been employed in the design of HKEX Systems, such as CCASS, RAP and VaR Online to protect it from computer virus or worms attacks. Participants are reminded that their PCs should be dedicated solely to accessing the CCASS, RAP or VaR Online services as uncontrolled access to the Internet will expose Participants' PC to various security attacks from the Internet. Besides, there are other potential sources of computer virus or worms e.g. use of external storage device for uploading or downloading information.

In view of the above, users should pay attention and take proactive action to the security measures in their own PCs or equipment for CCASS, RAP or VaR Online services in the following two areas:

Virus protection

Participants are recommended to install anti-virus software on their dedicated PCs for accessing CCASS, RAP and VaR Online, if applicable and regularly update the virus definitions from the vendor. For dedicated PCs not connected to the Internet, in some case, the vendor may make available the definition files daily in the Internet for download. Participants may download the updated virus definition file with a PC with Internet access, save the file in a disk or flash disk and install the update to their dedicated PCs.

Microsoft OS patch

Participants are also advised to regularly review the latest Microsoft security patches and install them on their dedicated PCs accordingly. Participants may subscribe to Microsoft technical security notifications to keep up to date about security vulnerability and patches available: (https://www.microsoft.com/en-us/msrc/technical-security-notifications)

For dedicated PCs not connected to the Internet, Microsoft security patches can be downloaded from Microsoft Download Center (or Microsoft Update Catalogue) separately with a PC with Internet access. Participants may then save the file in a disk or flash disk and install the patch at the dedicated PCs.

Sample Procedures:

1. Go to Microsoft Download Center: https://www.microsoft.com/download or Microsoft Update Catalogue: https://catalog.update.microsoft.com
2. Search a particular security patch with the Security Bulletins Number (e.g. MS08-078) or Knowledge Base (KB) Articles number. (e.g. KB960714) that appears in the security notification.
3. Follow the instructions to download and save the file to disk or flash disk.
4. Use the disk or flash disk to install the patch on the dedicated PCs. The patches may be in different formats, please follow Microsoft's instruction to install the patches.

PROHIBITED ACTIONS ON HKEX SYSTEM:

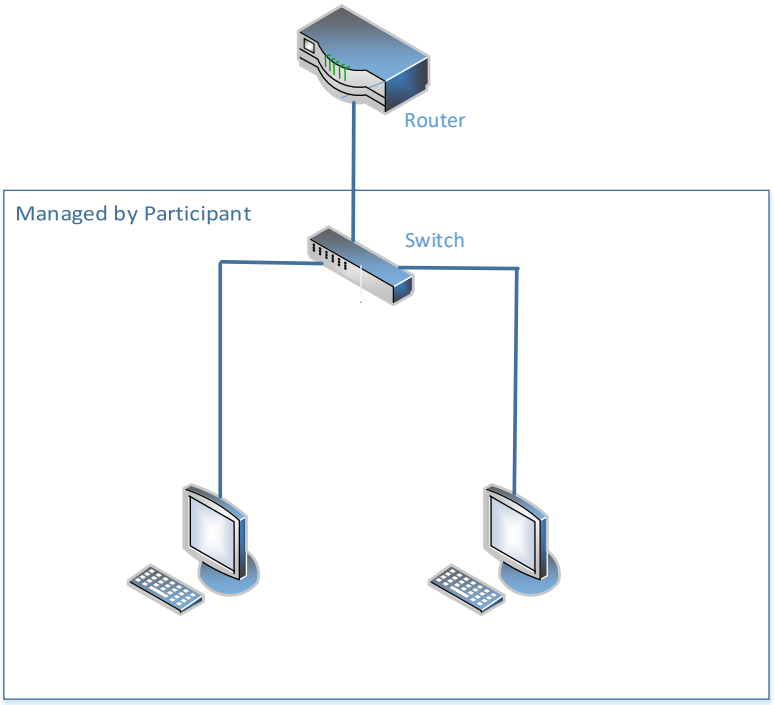
Participants must not perform any unauthorized access or security scanning (no matter at network, system or application level) on HKEX systems and any related network device not owned by them. Any such attempt will be regarded as illegal access or malicious intrusion.

3 Communication Line Setup

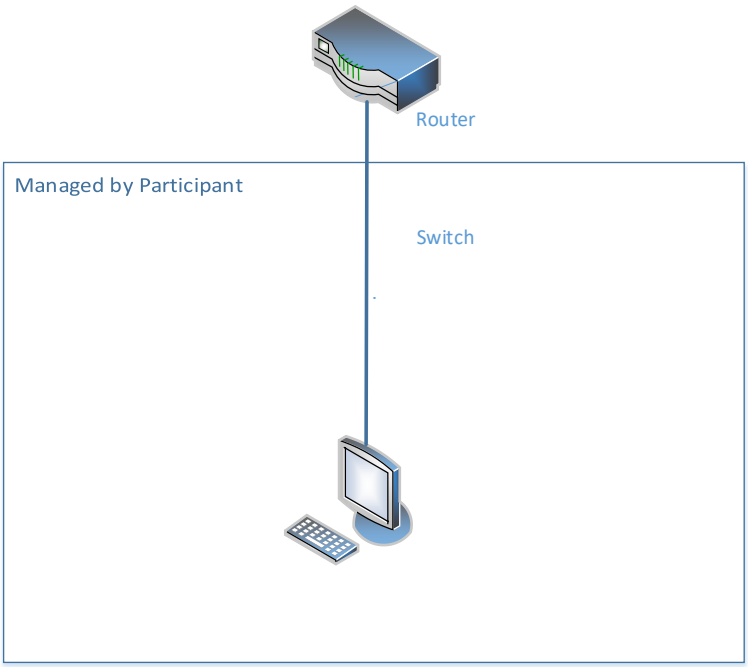
3.1 Connect PC Terminal with Router

Ensure the SDNet line and router are installed and configured properly by the vendor and connect the PC to switch/router with a LAN cable. There are 3 possible options to establish the connection.

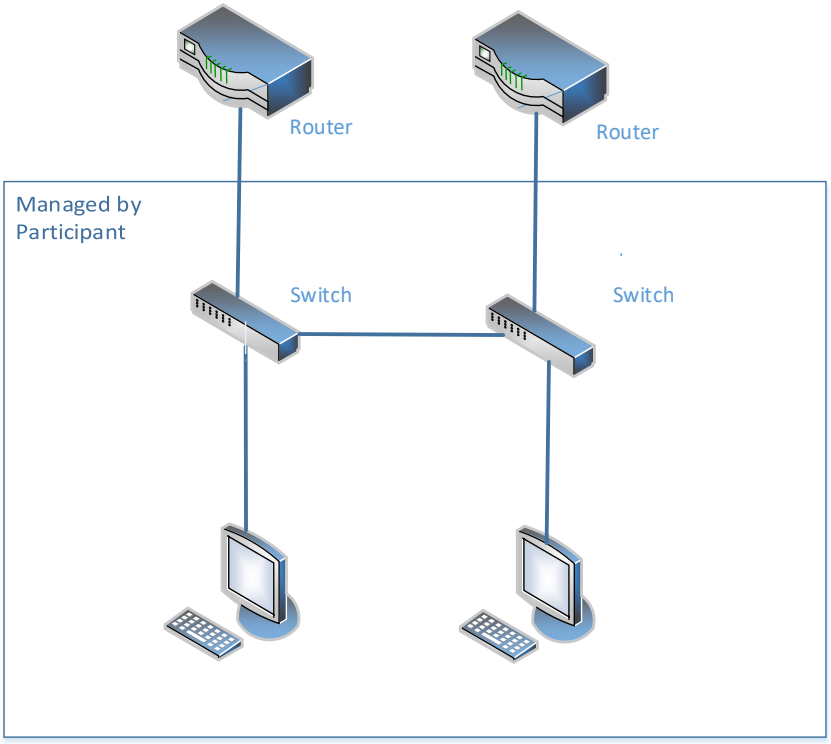
Option 1: Single Link Connection



Option 2: Single Link Connection with Direct Connection to Router



Option 3: Dual Link Connection



To maintain robustness, Participants should establish contingency plan and build in resilience to cope with emergencies and disruptions in their clearing and settlement operations. The contingency plan should include suitable backup arrangements to prevent single points of failure from disrupting their operations such as dual link connections (Option 3), backup site for remote operations/communications facilities.

4 Network Setup

The network configurations is common for CCASS, RAP and VaR Online; please follow procedures below for the PC setup.

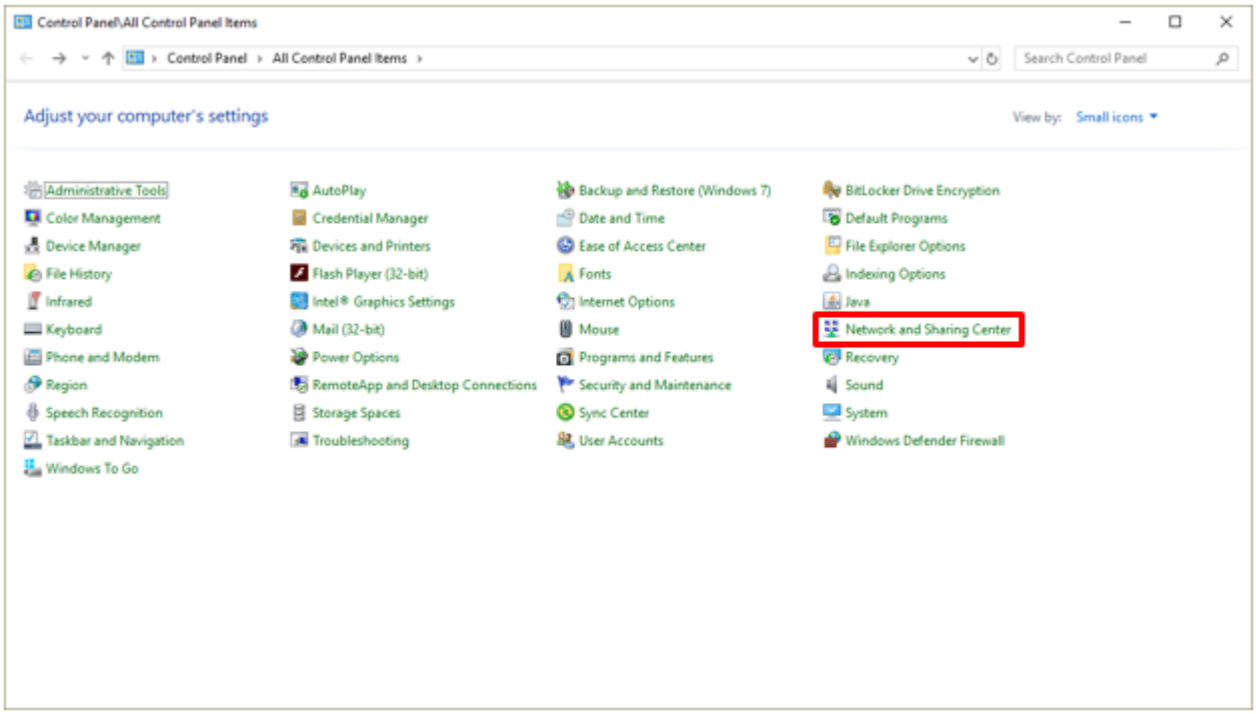
4.1 Windows IP address Configurations

1. To configure TCP/IP for the WAN Router & Ethernet Card Connection, you need an “administrator” account. Please ensure you have the appropriate access right.

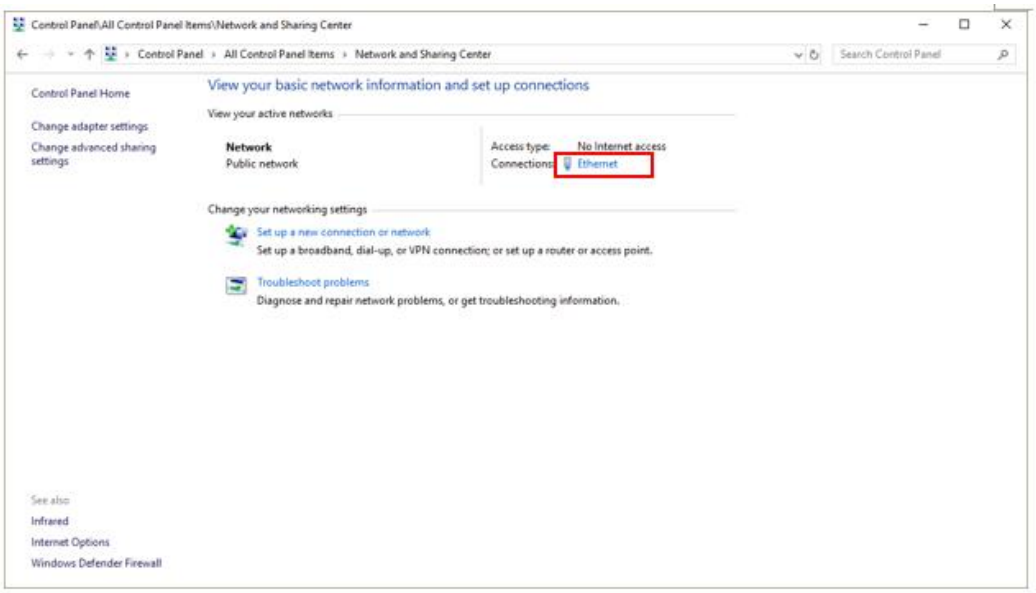
2. Click “Search” and input “Control Panel”

3. Select “Control Panel”

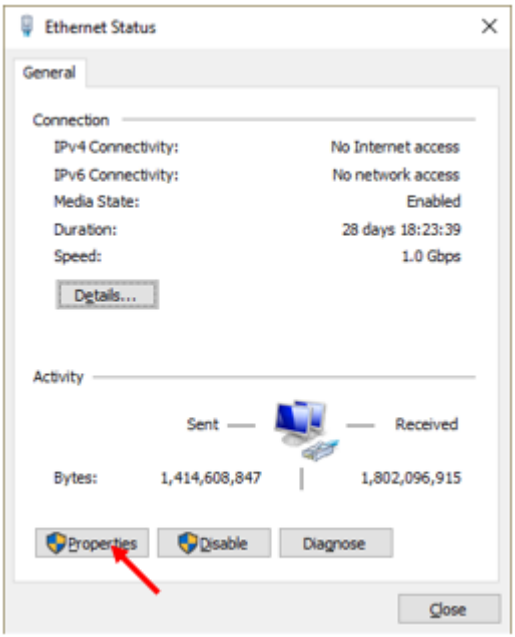
4. Click on "Network and Sharing Centre"



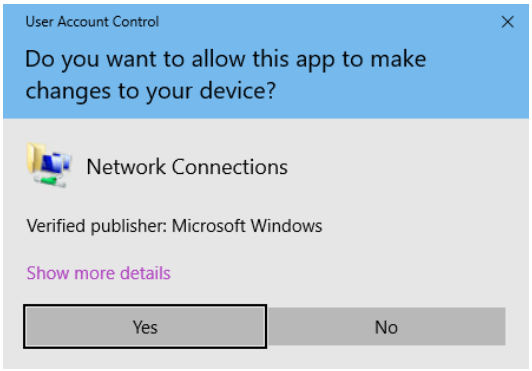
5. Click “Local Area Connection” or ”Ethernet” under “View your active networks”



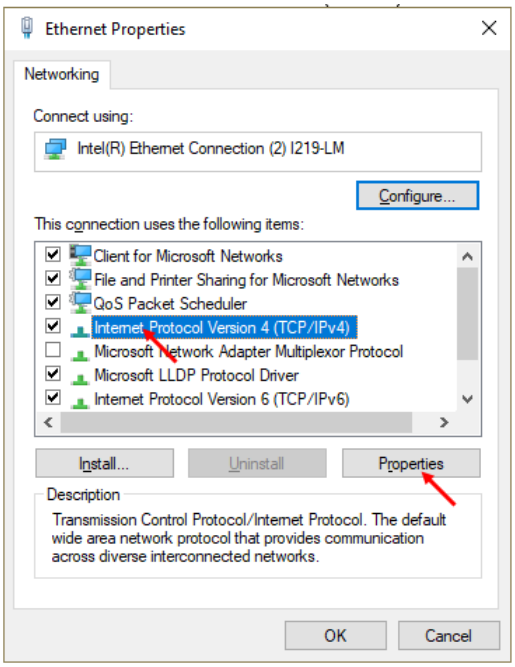
6. Click “Properties”



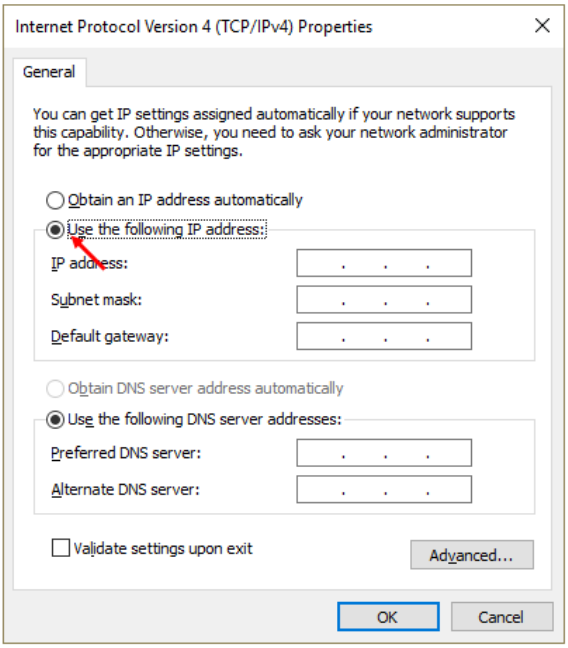
7. Click “Yes” in for alert message.



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



9. Select “Use the following IP address” radio button.



10. 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)

CCASS, RAP, VaR Online:	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)

CCASS, RAP, VaR Online:	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

11. Click “Gateway” tab, enter the Gateway IP Address given by vendor in the “Default Gateway"

12. Enter the DNS Server IP Addresses as stated in Section 4.2 for the "Preferred DNS Server" and “Alternate DNS Server”

13. Click “OK” button twice to save the changes

14. Restart the computer

4.2 DNS Servers

The Preferred Domain Name System (DNS) Server and Alternate DNS Server **MUST** be configured as below on PC.

Preferred DNS Server: 10.243.1.1 (CCASS Primary site)
Alternate DNS Server: 10.243.65.1 (CCASS Secondary site)

The URL or domain name for CCASS services are listed as below for reference.

1. CCASS – https://www.ccass.com
2. VaR Online – https://rmcd.hkexposttrade.com.hk[8]
3. VaR DA Platform – https://idm.hkexposttrade.com.hk/user-management/
4. RAP - rapcc.hkexposttrade.com.hk (SFTP on port 10022)

4.3 Disaster Recovery

During Disaster Recovery (DR) failover, Participants delegated PCs would rely on the Preferred and Alternate DNS server to resolve the URL to the corresponding IP address of DR site such that no change is required on the PC. Therefore, it is important for the PC to be configured with **both** Primary and Alternate DNS server IP addresses above.

In addition, it should be noted that DR failover could happen to any system individually or together. For instance, it may happen that only RAP need to be failed over to DR while CCASS and VaR Online remain intact with connection to primary site or vice versa. Nevertheless, it should be transparent to delegated PCs as HKEX DNS will resolve to DR site IP address(es) for that particular system automatically after failover to DR connection. When that particular system resumed in PR site afterward, HKEX DNS will also automatically switch back to resolve the PR site IP address(es). All in all, it would be totally transparent to the PC if recommended DNS settings above is followed.

[8] *Please note VaR Online connectivity verification will only be available after the completion of VaR DA application,*

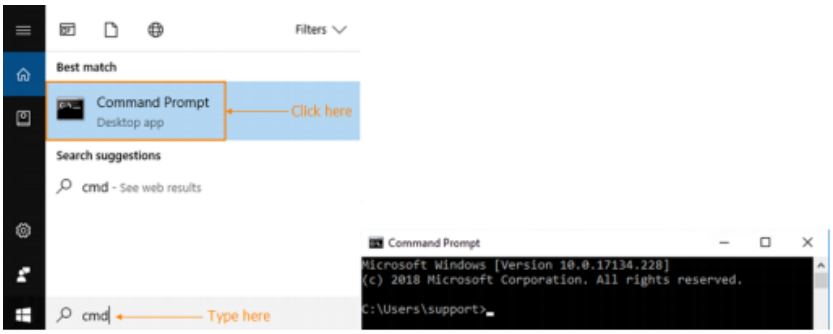
4.4 Source IP Address

Each SDNet circuit is assigned with a pre-defined range of IP addresses. Participants should ensure that their own delegated PCs should appear with the same IP address as original in each connection. If there is any Network Address Translation (NAT) performed, Participants should responsible and ensure the translated network addresses, if any, be translated back to the original IP address range (assigned by network vendor) or else login will fail due to IP address checking. In addition, NAT should be performed in a one-to-one mapping. That is, IP address of each delegated PC should be translated to a unique value within the original IP address range.

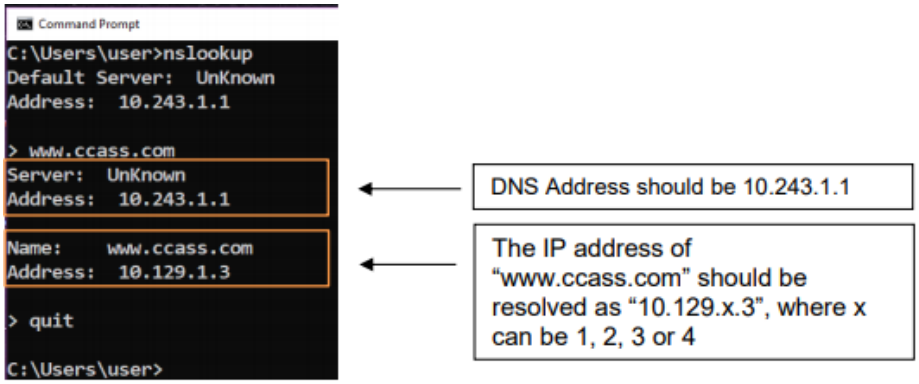
4.5 DNS Settings Verification

Please follow steps below to verify your DNS settings after completion of DNS setup (section 4.1).

1. Go to Start and type cmd in the search field to open the command prompt

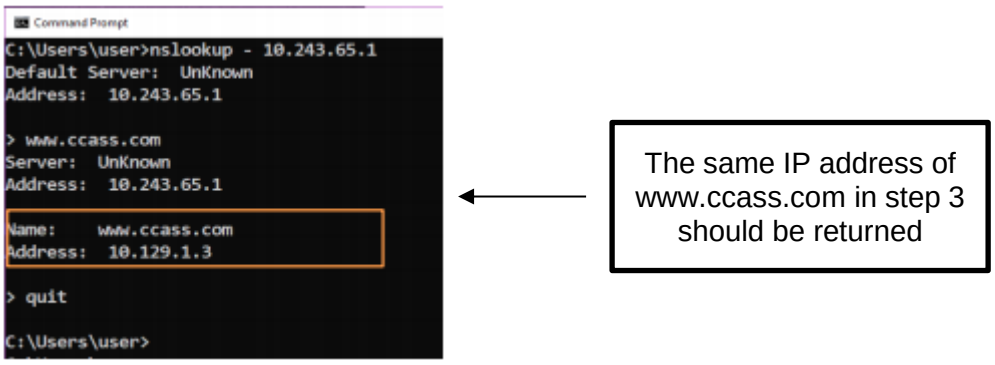


2. Type nslookup
3. Type www.ccass.com and the query result from the Primary DNS should be displayed as follows



4. Repeat with other application URL in 4.2 above

5. Type quit to exit
6. Type nslookup – 10.243.65.1
7. Type www.ccass.com and the query result from the Alternate DNS should be displayed as follows



8. Repeat with other application URL in 4.2 above
9. Type quit to exit and close the command prompt window
10. Please repeat the above verifications for all delegated PCs with CCASS, VaR Online and RAP connection

4.6 Special Network Settings for PC not compliant to Standard Configurations

If the PC does not connect to CCASS DNS servers for name resolving or there is any additional access control like firewall in between the PC and CCASS services. Please follow sections below for additional configurations.

4.7 CCASS Services to be accessed

Participants should ensure that the following services are accessible from PC to HKEX systems.

CCASS:

Services	IP Address/URL	Port No.	Description
DNS	10.243.1.1 10.243.65.1	UDP: 53	Domain Name Service
HTTPS	10.129.X.3[9] www.ccass.com	TCP: 441, 442, 443	CCASS Web[10] (PR & DR)

[9] *X could be 1, 2, 3 or 4 depending on the network segment of SDNet assigned by SDNet carrier. Please refer to DNS settings verification below to check the CCASS web IP for your SDNet line.*

[10] *The web IP address for CCASS is the same in both its Primary (PR) and Secondary/Disaster (DR) sites if via the same SDNet lines*

VaR Online:

Services	IP Address/URL	Port No.	Description
DNS	10.243.1.1 10.243.65.1	UDP:53	Domain Name Service
HTTPS	10.243.2.32 rmcd.hkexposttrade.com.hk	TCP:443	VaR Online (PR)
HTTPS	10.243.66.32 rmcd.hkexposttrade.com.hk	TCP:443	VaR Online (DR)
HTTPS	10.243.2.15 sso.hkexposttrade.com.hk	TCP:443	VaR Logon (PR)[11]
HTTPS	10.243.66.15 sso.hkexposttrade.com.hk	TCP:443	VaR Logon (DR)
HTTPS	10.243.2.14 idm.hkexposttrade.com.hk	TCP:443	VaR DA Platform (PR)
HTTPS	10.243.66.14 idm.hkexposttrade.com.hk	TCP:443	VaR DA Platform (DR)

RAP:

Services	IP Address/URL	Port No.	Description
DNS	10.243.1.1 10.243.65.1	UDP:53	Domain Name Service
SFTP	10.243.2.51 rapcc.hkexposttrade.com.hk	TCP:10022	RAP (PR)
SFTP	10.243.66.51 rapcc.hkexposttrade.com.hk	TCP:10022	RAP (DR)

4.8 Special Settings for Domain Name Resolution

Important Notes : If your DNS setting[12] does not follow the recommended standard configurations:

1. If for any reason other DNS setting is being used, Participants should be ensured that **DNS forwarding** is enabled to resolve the domain names of "ccass.com" and "hkexposttrade.com.hk" from HKEX DNS servers stated above. Otherwise, it would run into the risk that the delegated PCs will be unable to connect during DR failover, which might impact Participants' operations.

2. If host table is used instead, please note that the DR site IP addresses for VaR Online and RAP is different from its Primary ones. In addition, HTTPS services must be accessed by domain name and thus all host entries in tables above should

[11] *Participants will be redirected to VaR Logon for authentication and then switch back to VaR Online automatically.*

[12] *For CCASS connection, the IP address would be the same for both PR and DR and so there is no change upon DR failover. But for VaR and RAP connection, the IP for PR and DR is different and so it would be an issue if the delegated PCs unable to detect IP changes upon system failover.*

be included. As a result, manual changes would be required upon DR failover and also when fail back to PR site. It should also be noted that the DR failover could happen individually or together for any of the system below.

a. CCASS
b. VaR Online
c. VaR Logon and DA Platform
d. RAP

The manual changes is be prone to error and is not recommended. Participant would take their own risk in failure to connect to DR sites if they choose not to use HKEX DNS servers.

In general, using other DNS server or host table is not recommended. Participants should consider the risk and must perform thorough testing to ensure their own delegated PCs be able to connect and work properly during normal and failover scenarios.

5 CCASS Terminal

To use CCASS functions, the following hardware and software **must be** installed or configured on the PC terminal.

- **Smartcard Reader**: it is required for login with smartcard and please go to **Section 5.1** for setup
- **CCASS Smartcard Client**: CCASS Smartcard Client must be installed for smartcard operations. Please follow **Section 5.2** for the installation procedures.
- **MS Edge Browser with IE Mode**: Configurations must be made or otherwise some CCASS functions may not work properly. For details, please refer to **Section 5.3** to **Section 5.10** below
- **Java Plugin**: if you do not have Java Plugin installed, please go to **Section 5.13** 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 refer to Section 2.
- **Acrobat Reader**: Acrobat Reader is required to open files. If you do not have any Acrobat Reader installed. Please follow **Section 5.15** for the installation procedures.

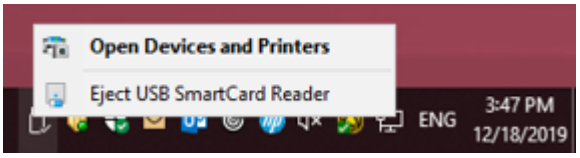
After the terminal is set up, please perform verification by following steps in **Section 5.16** on smartcard initialisation and commissioning logon.

5.1 Install Smartcard Reader

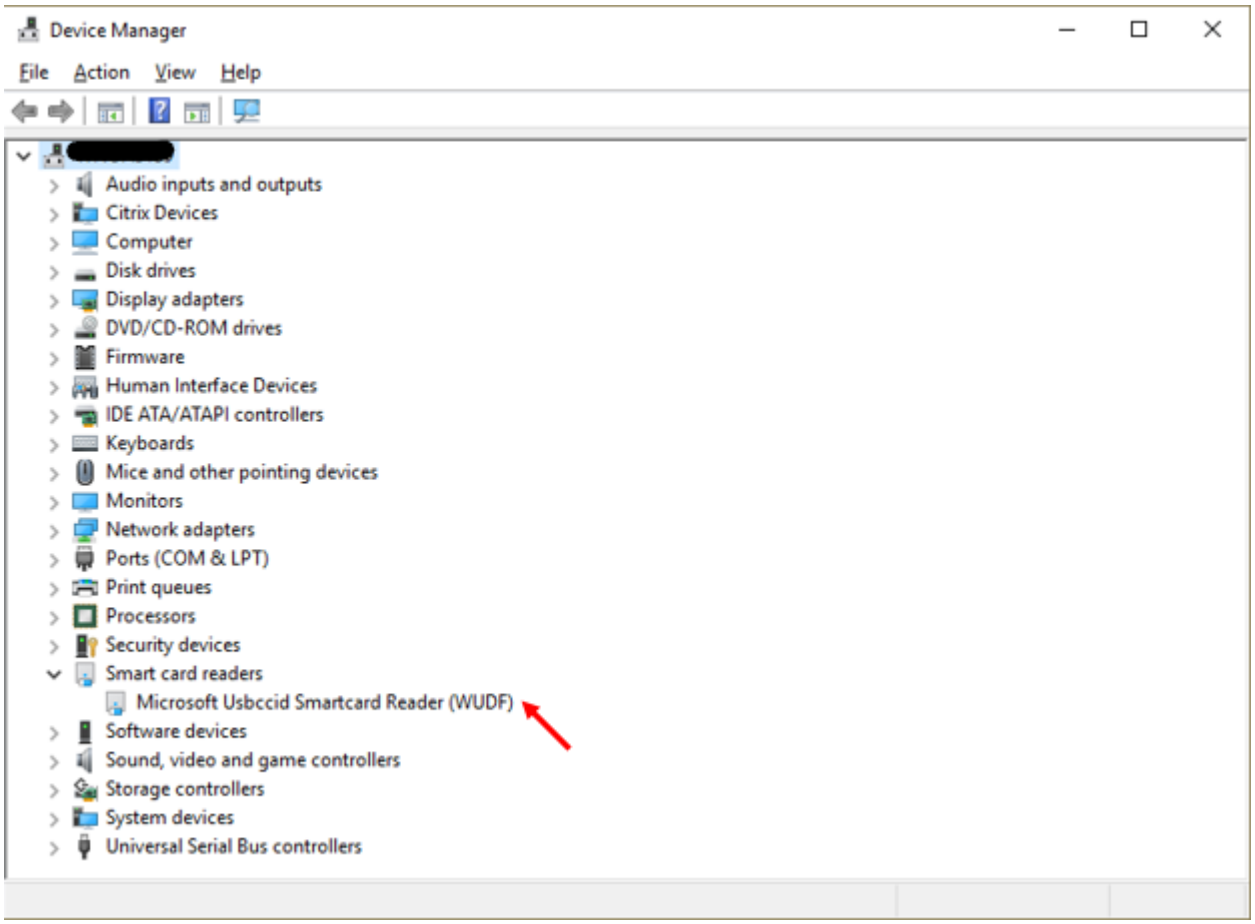
1. Check which USB readers you are using: GemPCUSB-SL (ID Bridge CT40) or GemPCUSB-SW or ID Bridge CT30. The model number is also printed at the back of the reader.

		
GemPCUSB-SL (IDBridge CT40)	GemPCUSB-SW	IDBridge CT30

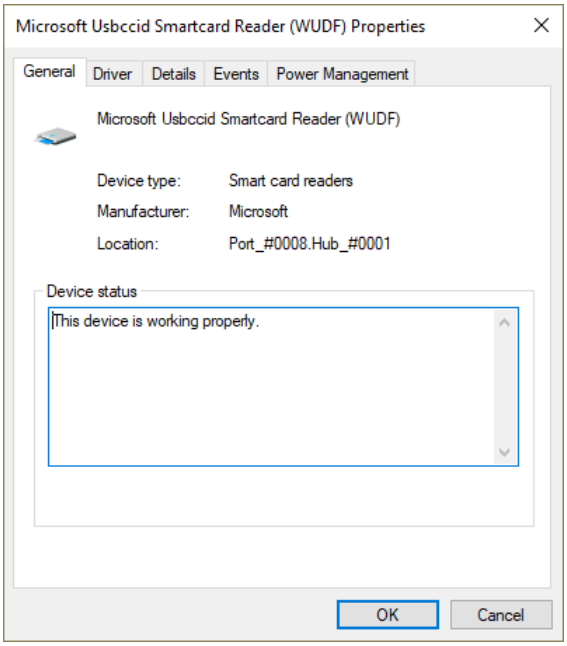
2. Connect the USB smartcard reader to the USB port on the computer and the smartcard reader driver software is automatically installed to the computer



3. Open the Control Panel → Hardware and Sound. 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.



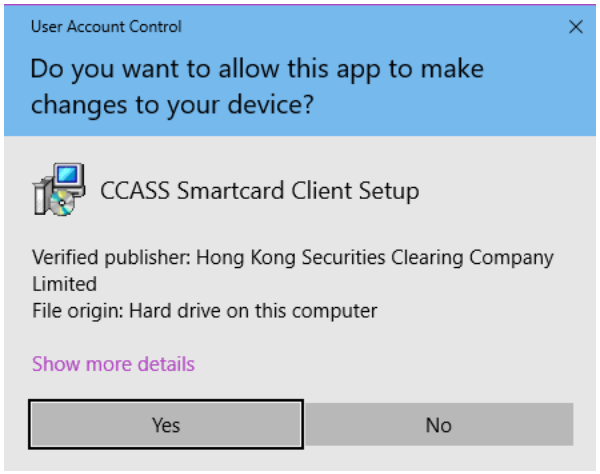
4. Double click on Microsoft Usbccid Smartcard Reader (WUDF). Ensure Device status is “This device is working properly”.



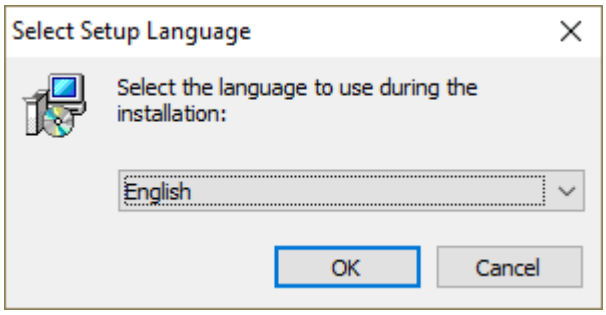
5.2 Install Smartcard Client

1. Launch Internet browser, enter https://www.ccass.com/commissioning/download in address box. Then click the associated link to download the CCASS Smartcard Client installer.

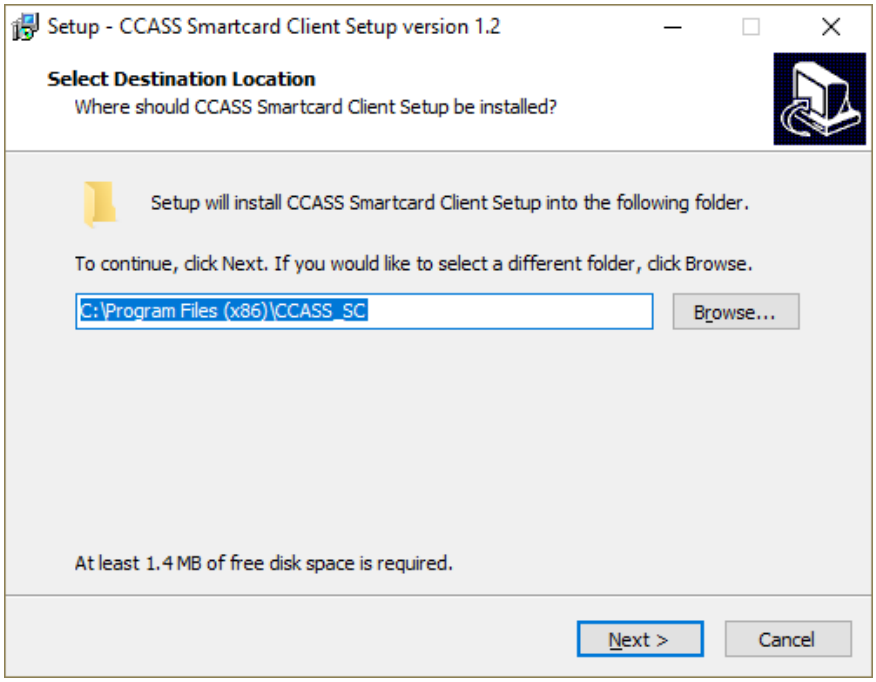
2. Click “Run” button to continue and start to install “CCASSClientSetup.exe”.
3. Verify publisher name as “Hong Kong Securities Clearing Company Limited”, and click Yes.



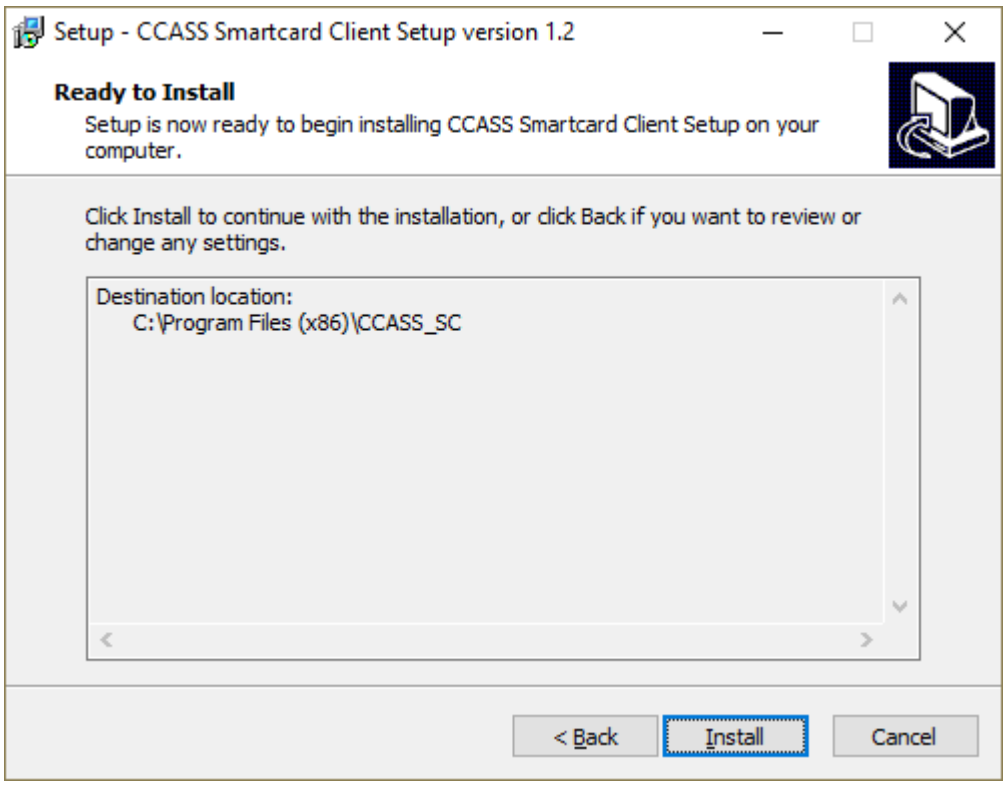
4. Select “English” and click “OK”.



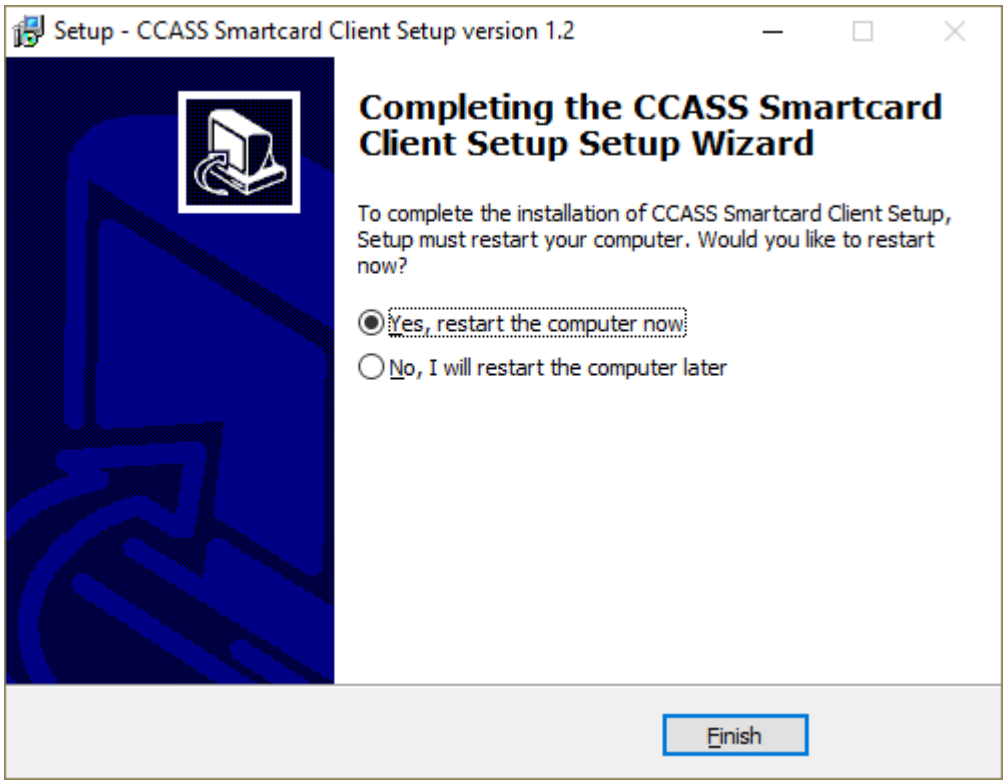
5. Input the desired installation location, and click “Next”.



6. Review installation location, and click “Install”.



7. Installation completes. Select “Yes, restart the computer now” and then click “Finish” to end installation. The PC should be reboot automatically.



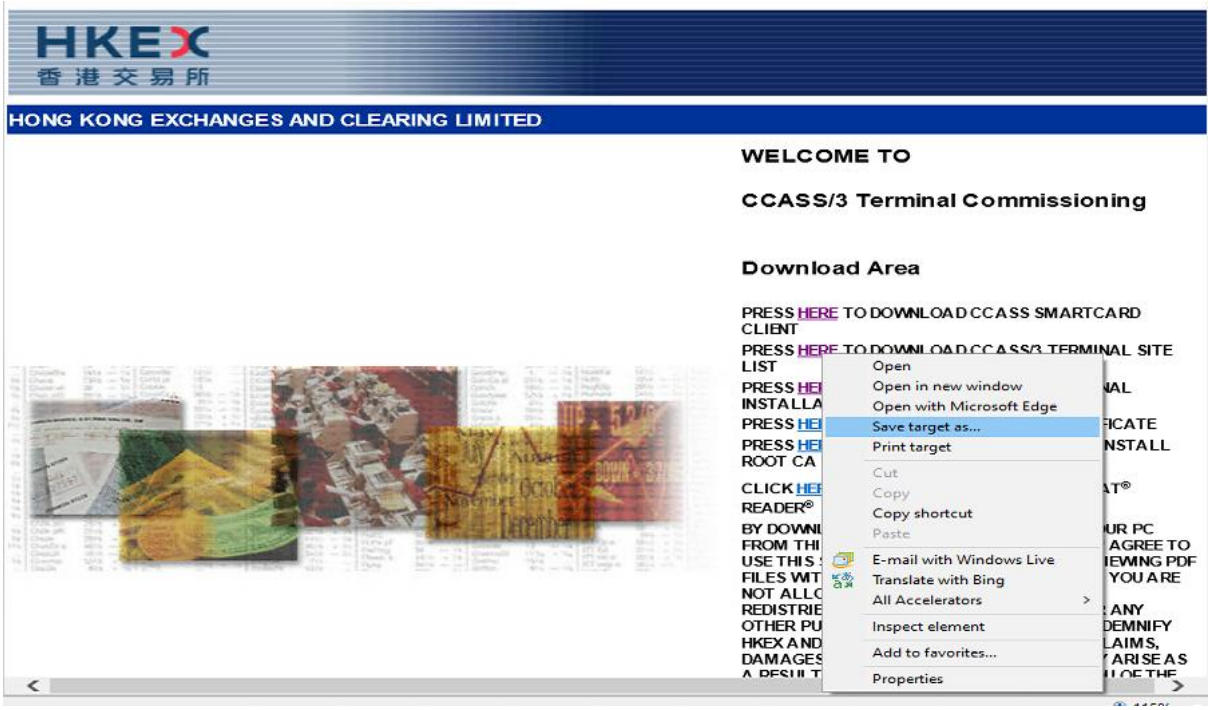
5.3 Internet browser Settings

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 MS Edge browser windows and start new ones to make the changes effective.

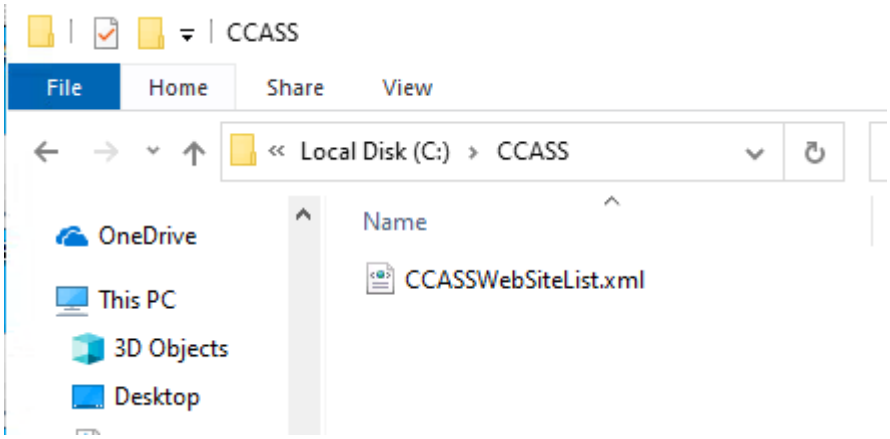
5.4 Setup for MS Edge browser with Internet Explorer Mode

1. Download CCASS/3 Terminal Site List file from Commissioning Website
   https://www.ccass.com/commissioning/download

2. Right click “HERE” on “PRESS HERE TO DOWNLOAD CCASS/3 TERMINAL SITE LIST, and select “Save target as…”



3. Save the file to C:\CCASS\CCASSWebSiteList.xml



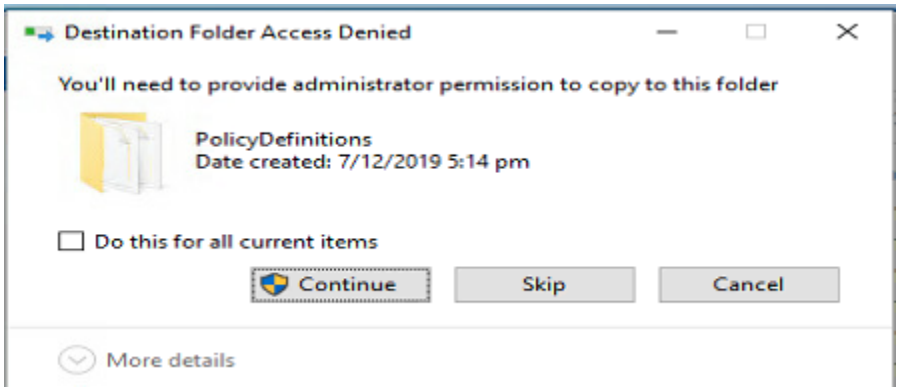
4. Download MS Edge browser and policy files

   a. Go to https://www.microsoft.com/en-us/edge/business/download
   b. Click the link to download MS Edge browser for “Windows 64-bit”

c. Click the link to download for “Windows 64-bit Policy”

5. Install MS Edge by running MicrosoftEdgeEnterpriseX64.msi installer
6. Unzip MS Edge policy files to a temporary folder (e.g. C:\TEMP\)
7. Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\ to C:\Windows\PolicyDefinitions\

Click Continue for this security prompt to confirm copying:

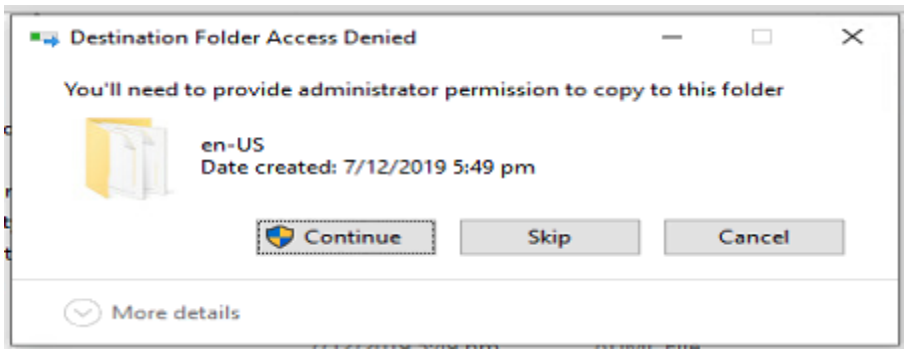


For Chinese Windows OS:

8. Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\en-US\ to C:\Windows\PolicyDefinitions\en-US (for English Windows OS), or

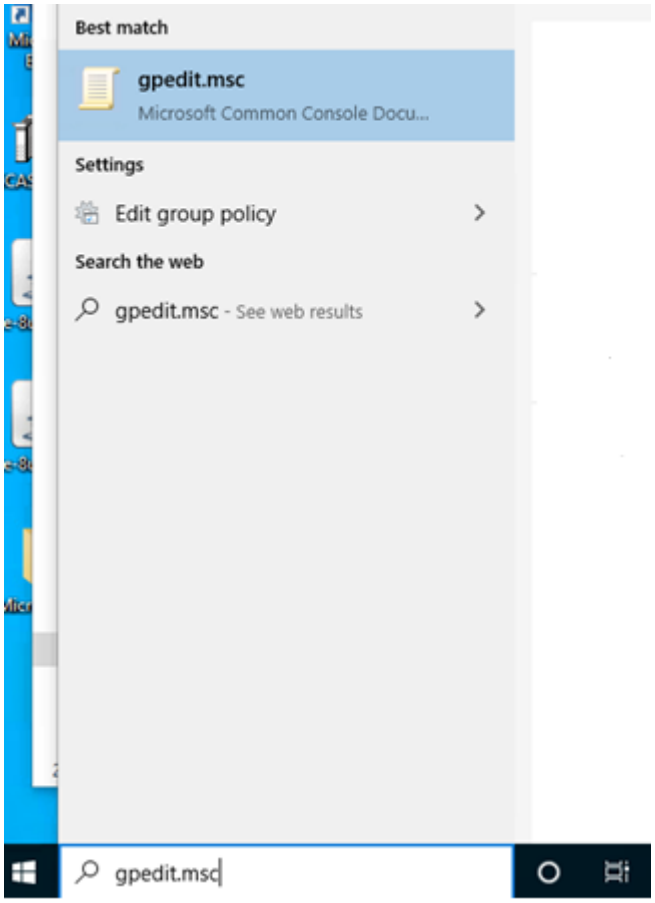
Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\zh-TW\ to C:\Windows\PolicyDefinitions\zh-TW (for Traditional Chinese Windows OS)

Click Continue for this security prompt to confirm copying:

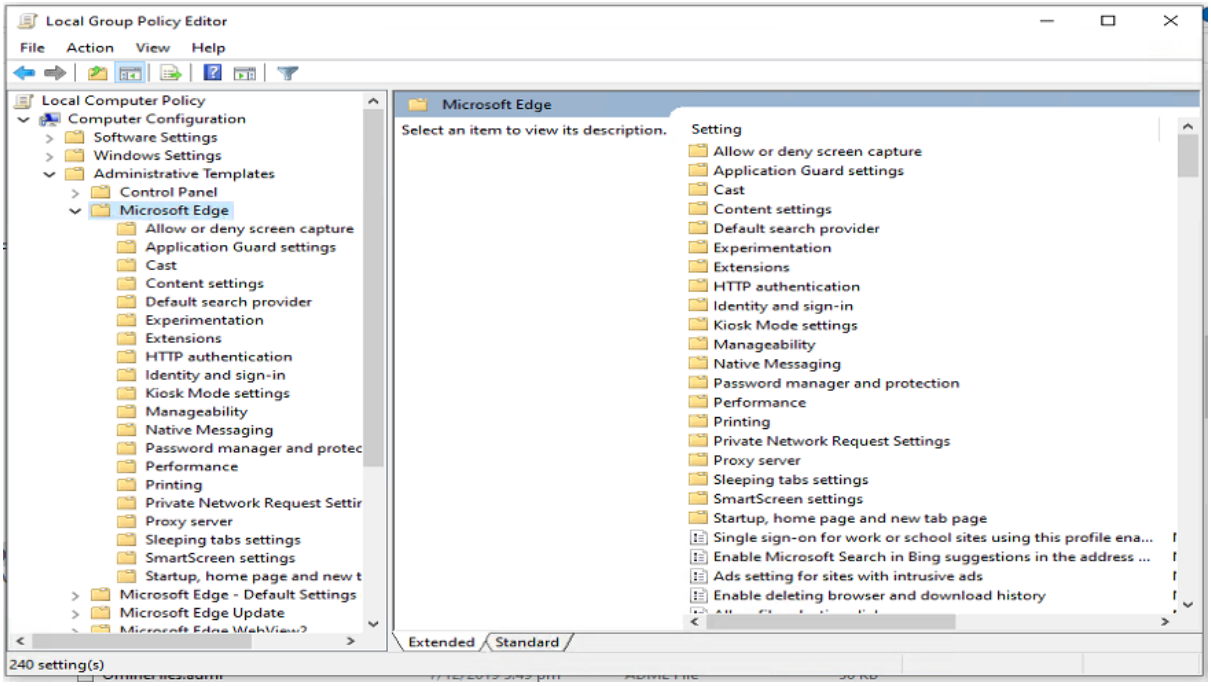


For Chinese Windows OS:

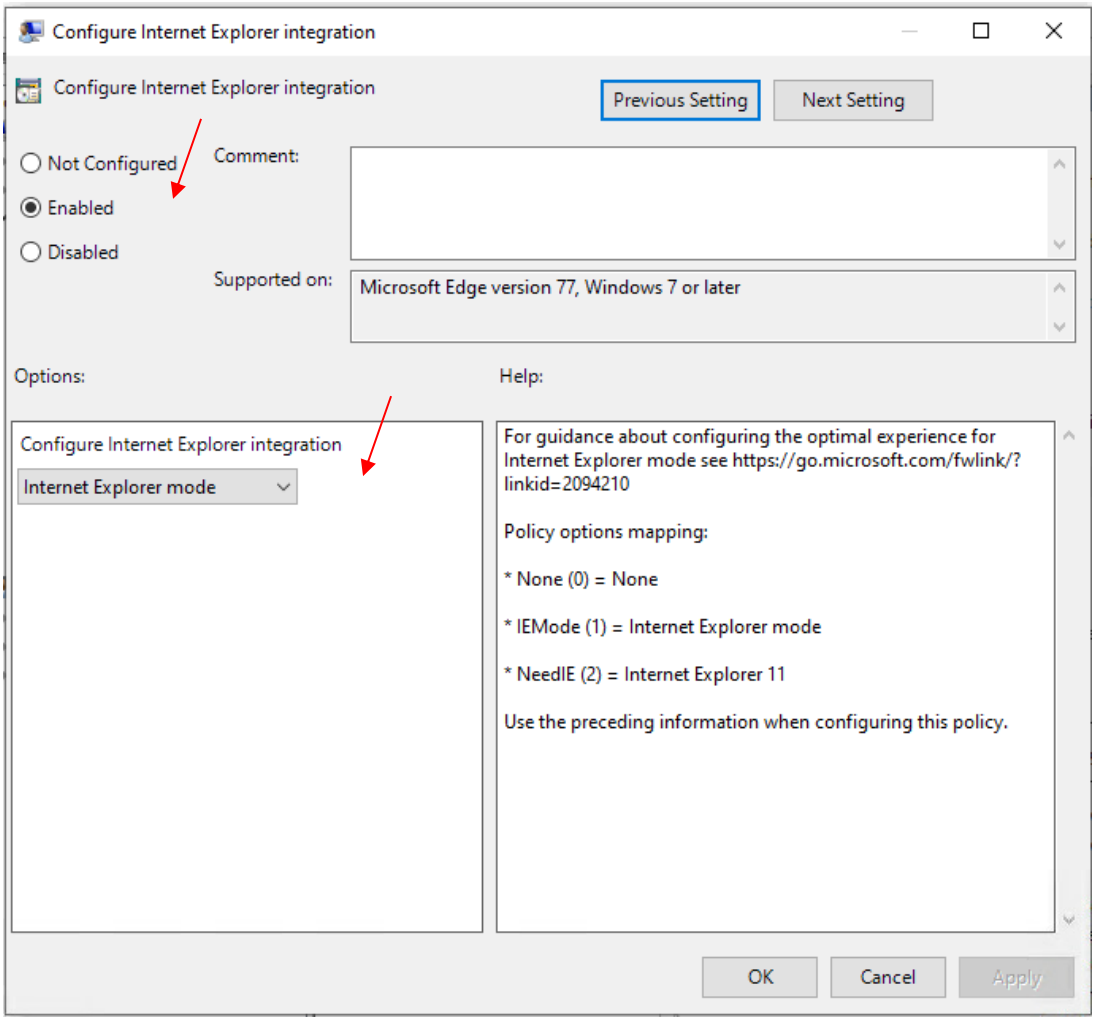
9. Open “Edit Group Policy” by typing “gpedit.msc” in the Search field box



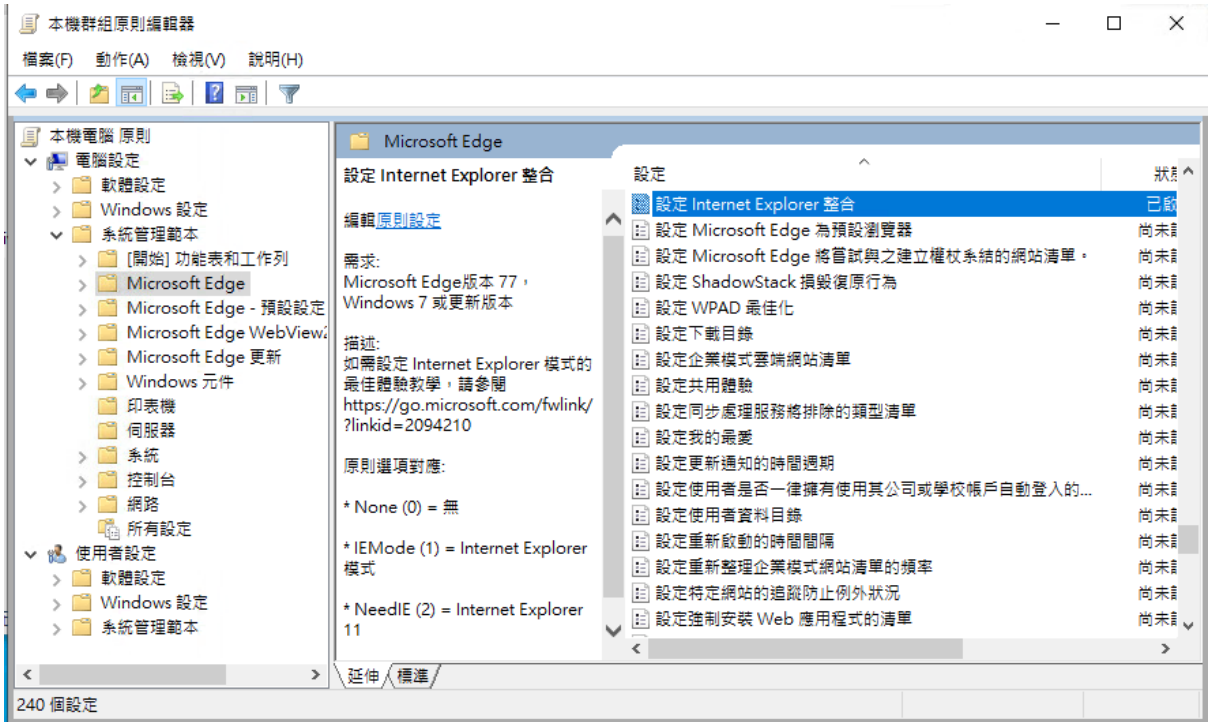
10. Browse to “Computer Configuration” > “Administrative Templates” > “Microsoft Edge”

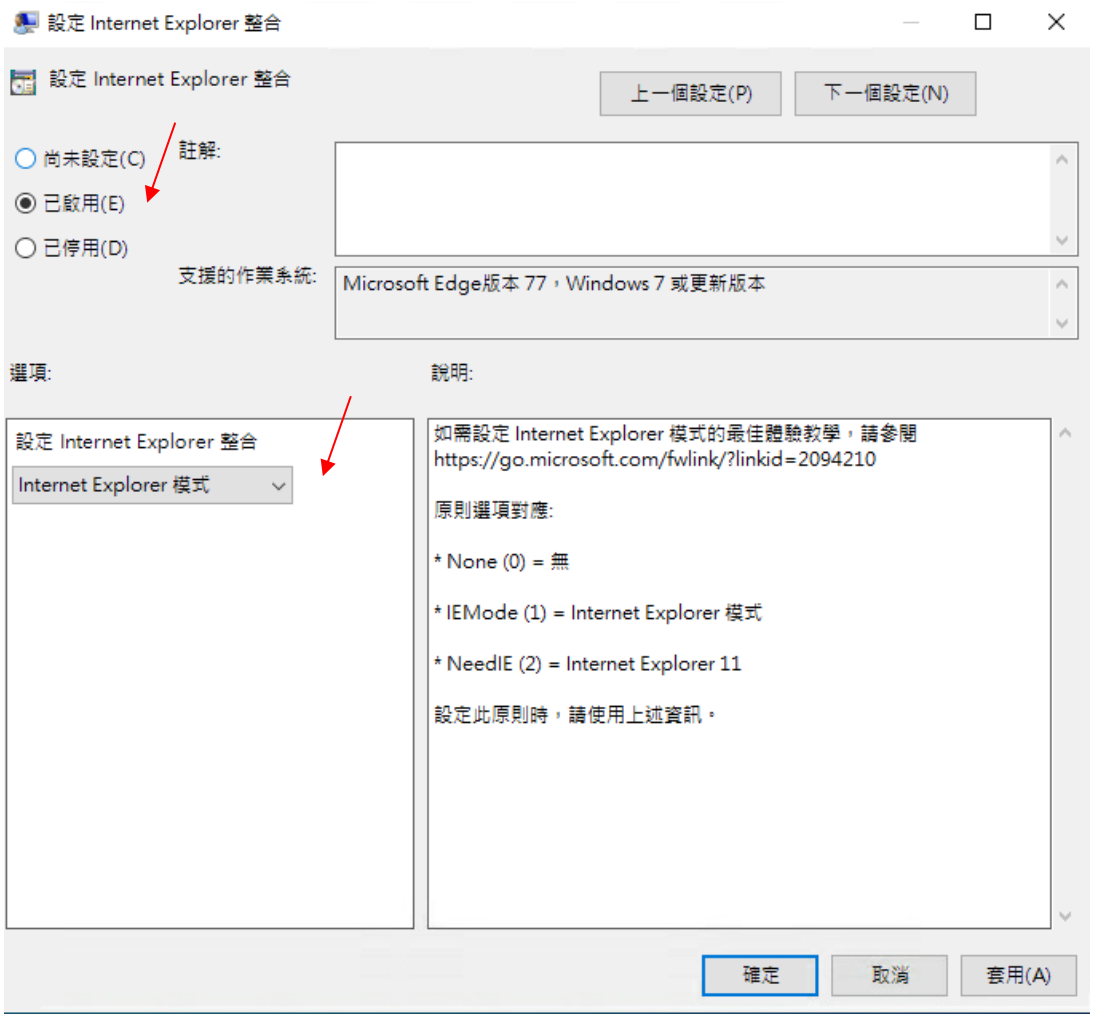


11. Change Setting “Configure Internet Explorer Integration”
12. Select “**Enable**” and, in Options section, select “**Internet Explorer mode**” in the drop down box

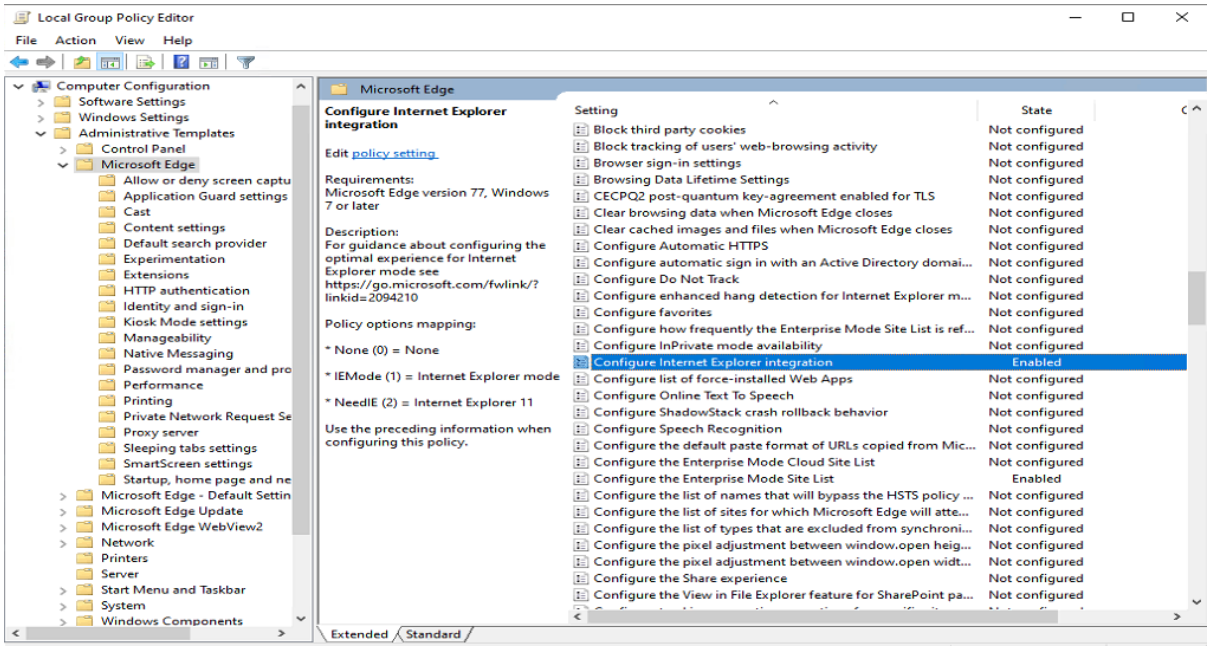

Configure Internet Explorer integration
Configure Internet Explorer integration
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Microsoft Edge version 77, Windows 7 or later
Options:
Help:
Configure Internet Explorer integration
Internet Explorer mode
For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210
Policy options mapping:
* None (0) = None
* IEMode (1) = Internet Explorer mode
* NeedIE (2) = Internet Explorer 11
Use the preceding information when configuring this policy.
OK
Cancel
Apply

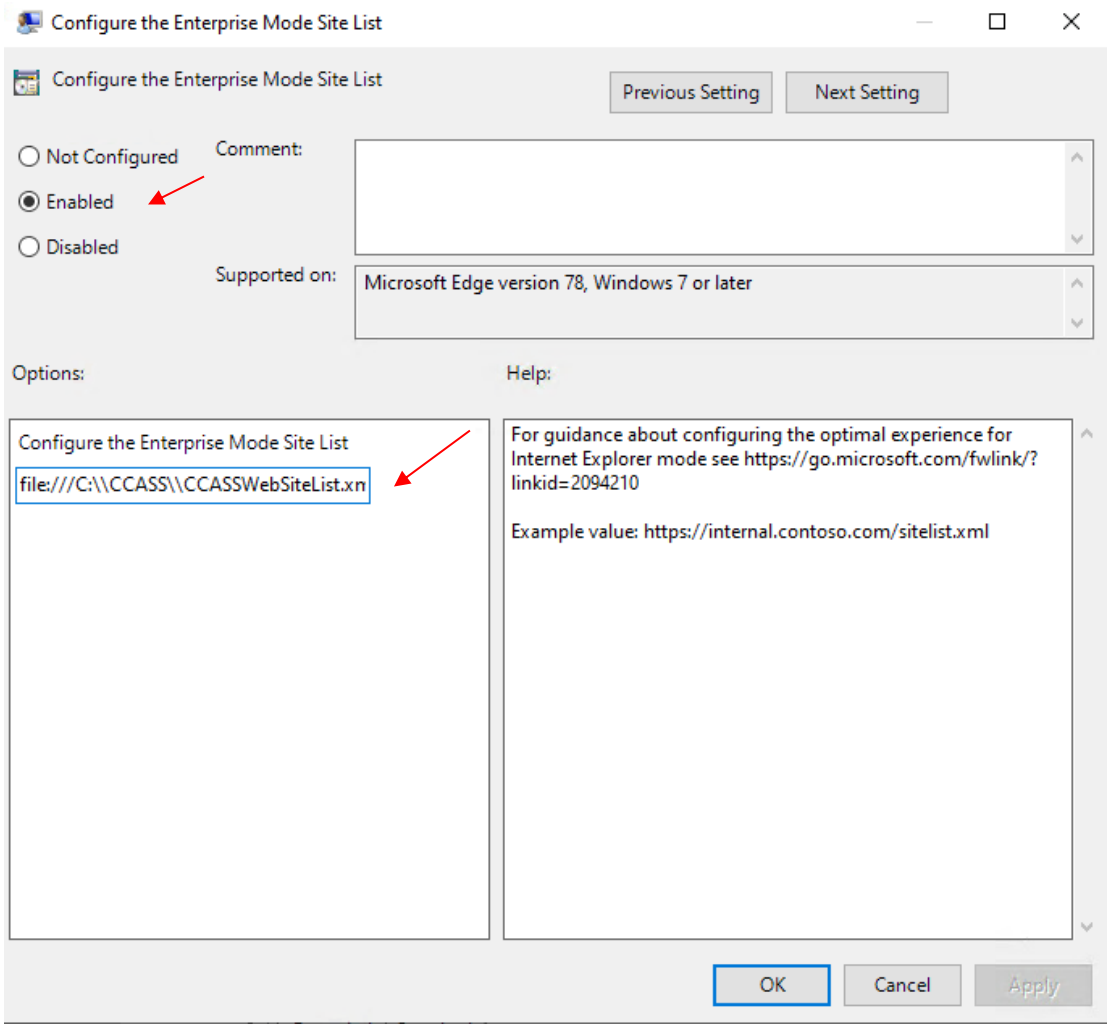
For Chinese Windows OS:



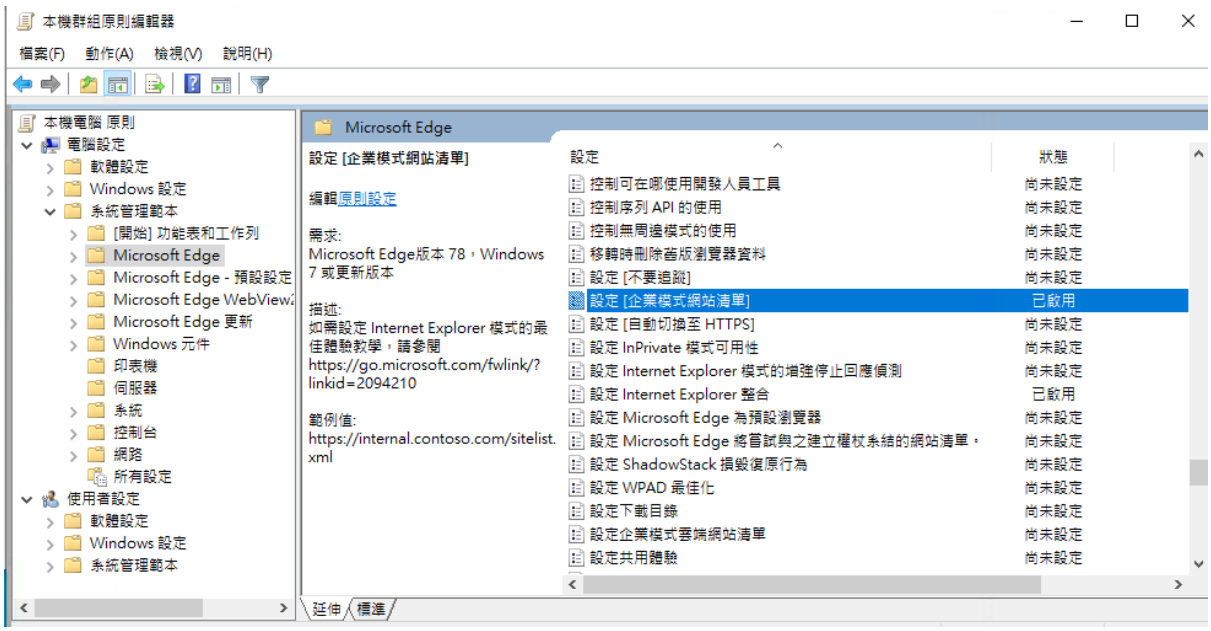


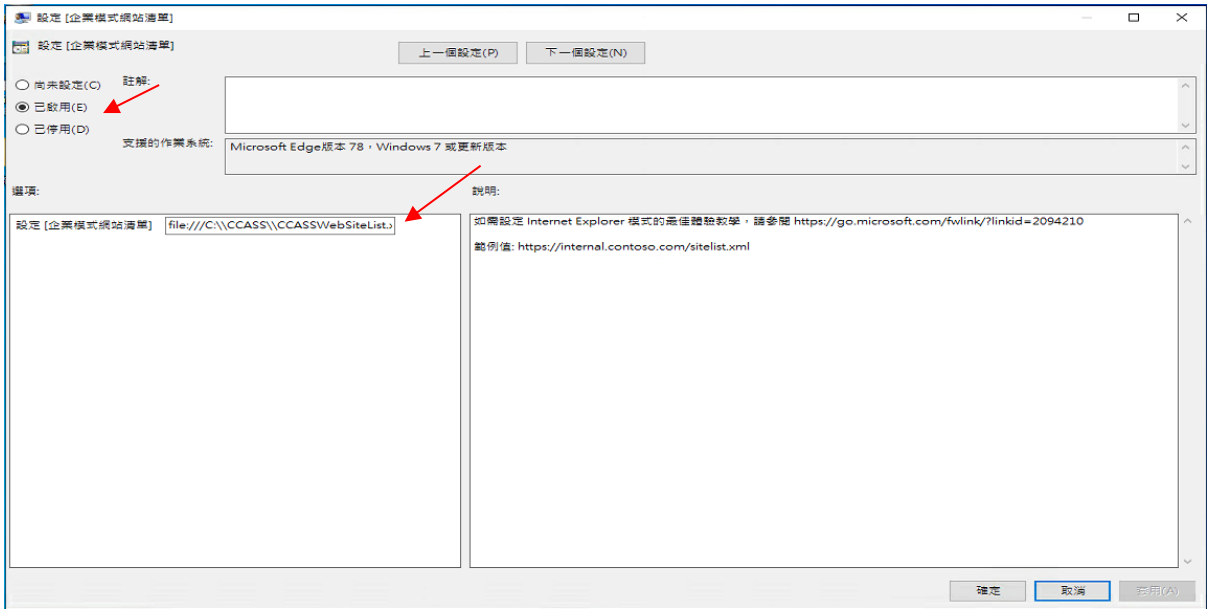
13. Click OK to save
14. Change Setting “Configure the Enterprise Mode Site List”
15. Select “**Enable**” and, in Options section, input Enterprise Mode Site List as “file:///C:\\CCASS\\CCASSWebSiteList.xml”





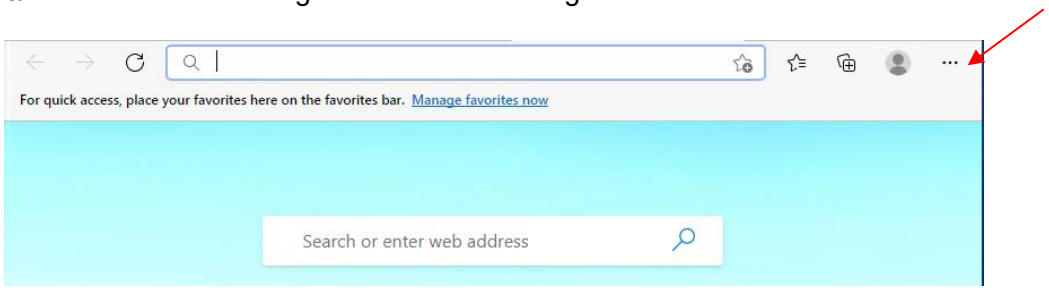
For Chinese Windows OS:



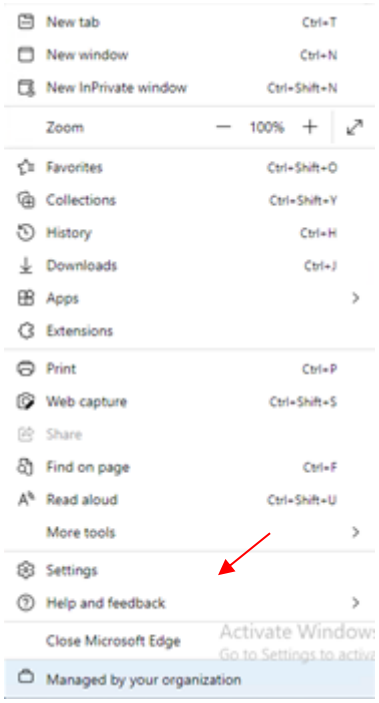


16. Click OK to save
17. Enable Pop-Up https://www.ccass.com:443 and https://www.ccass.com:442 in MS Edge browser

    a. Select "…" on the right hand corner of Edge browser

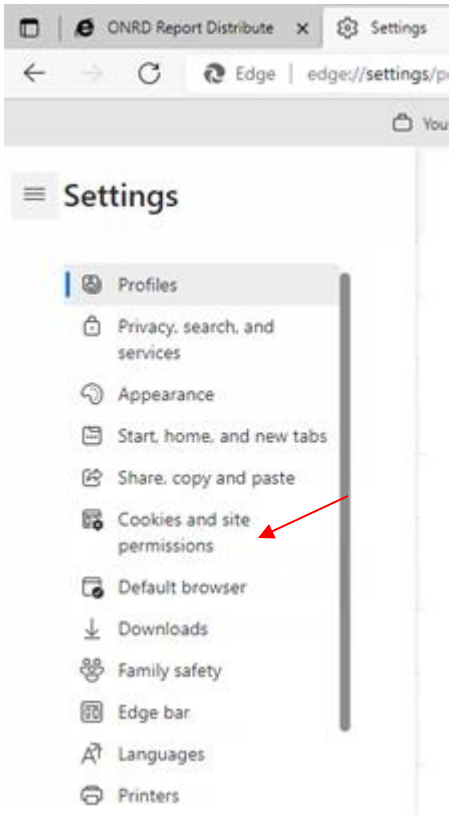


b. Go to Settings



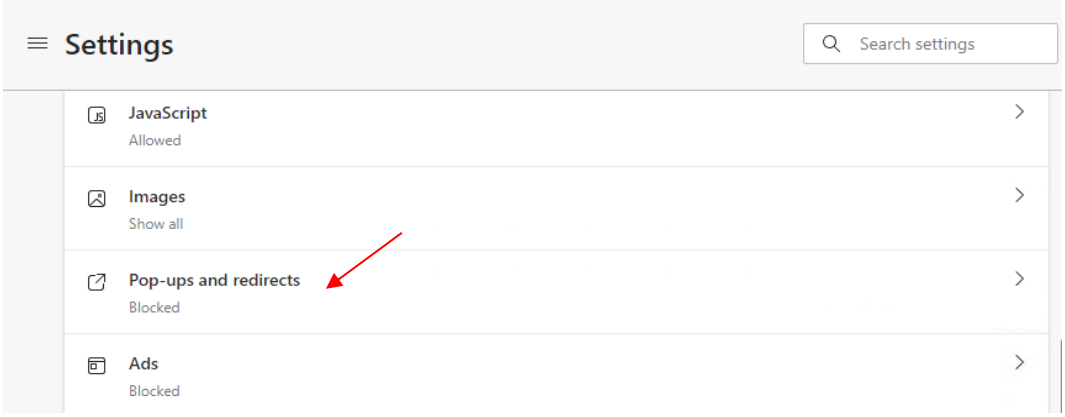
For Chinese Windows OS:

c. Click “Cookies and site permissions”

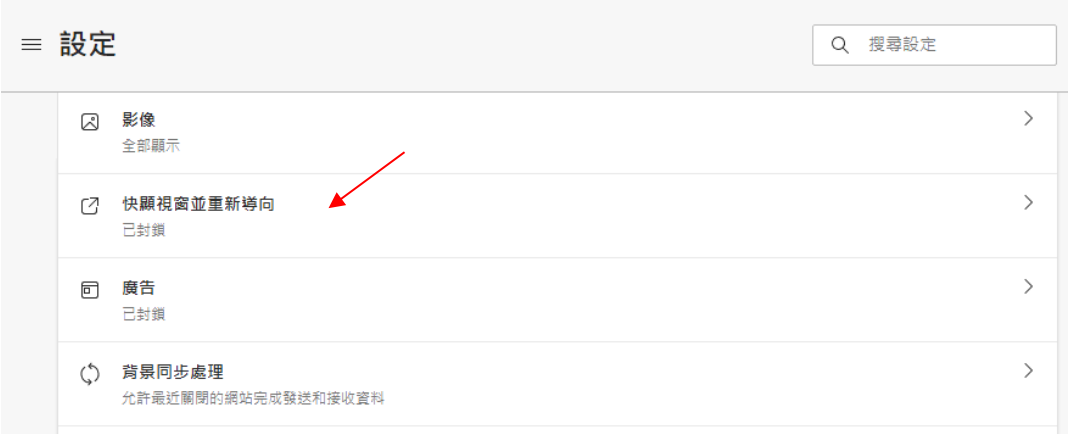


For Chinese Windows OS:

d. Go to “Pop-ups and redirects”



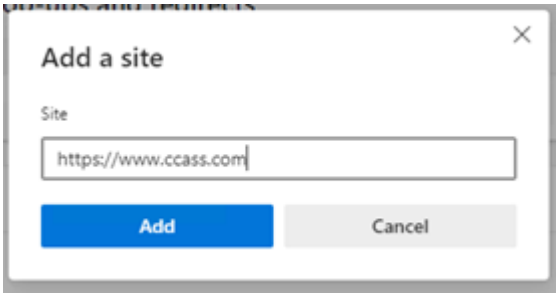
For Chinese Windows OS:



e. Go to “Allow” section and click “Add” button

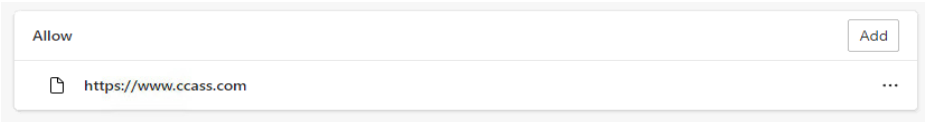
For Chinese Windows OS:

f. Input https://www.ccass.com and click “Add”

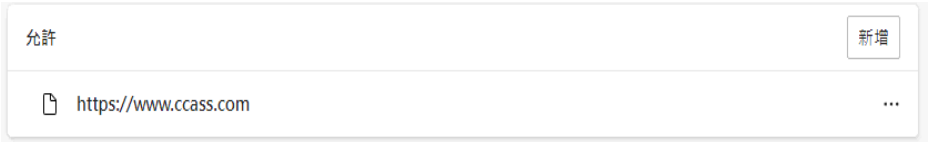


For Chinese Windows OS:

g. Confirm to see the website https://www.ccass.com is added



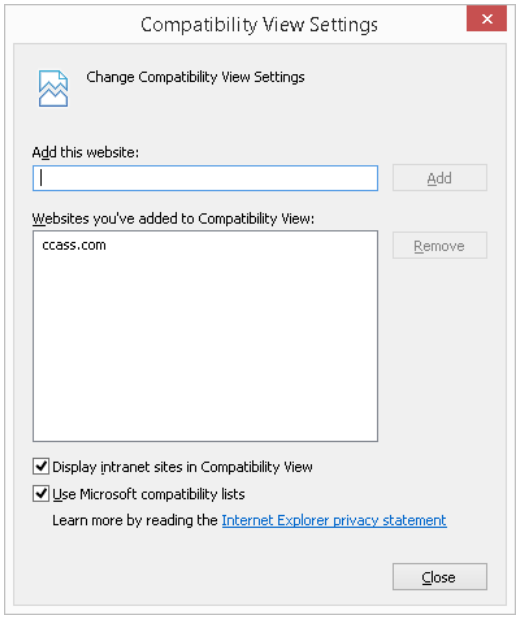
For Chinese Windows OS:



h. For new PC, it is still required to enable Compatibility View in IE11 if it has not yet been enabled for ccass.com

5.5 Compatibility View Settings (in Internet Explorer 11)

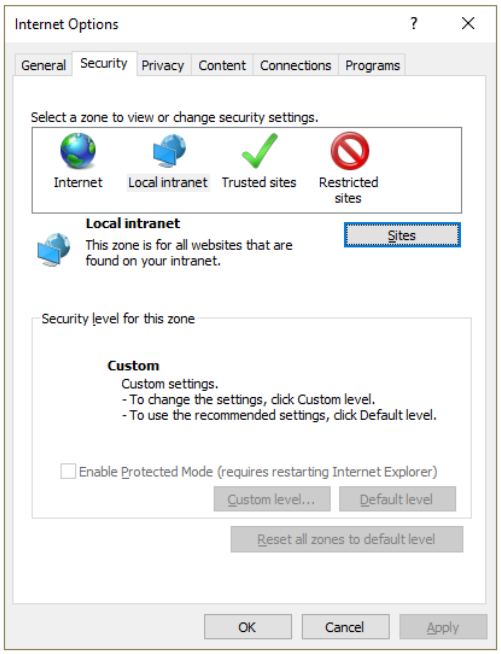
1. Open IE window, and then select “Tools” → “Compatibility View settings”.
2. Type www.ccass.com
3. Click “Add”, then “ccass.com” should be shown at the box “Websites you ‘ve added to Compatibility View:”



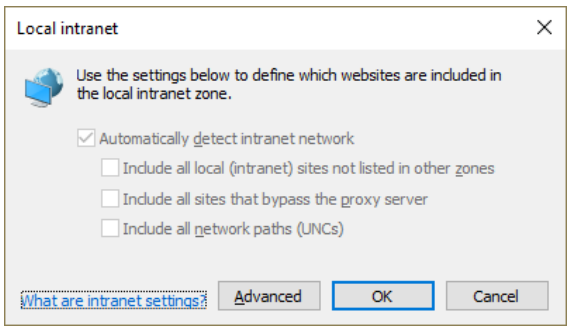
4. Click “Close” to close the window to complete the setting

5.6 Local Intranet Settings

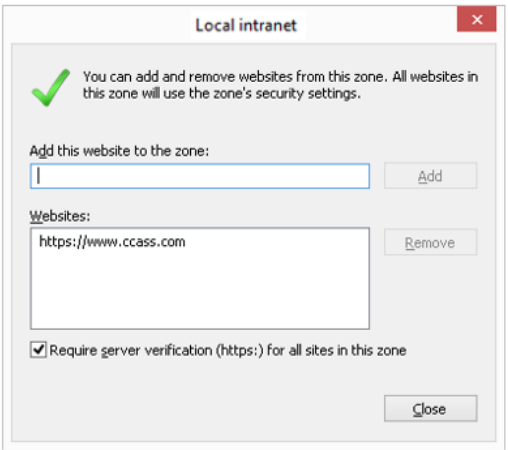
1. Go to “Control Panel” → “Internet options” and then click on “Security” tab.
2. Then click on “Local intranet” and click on “Sites”



3. Click “Advanced”.



4. Type “https://www.ccass.com” and then click add “Add”

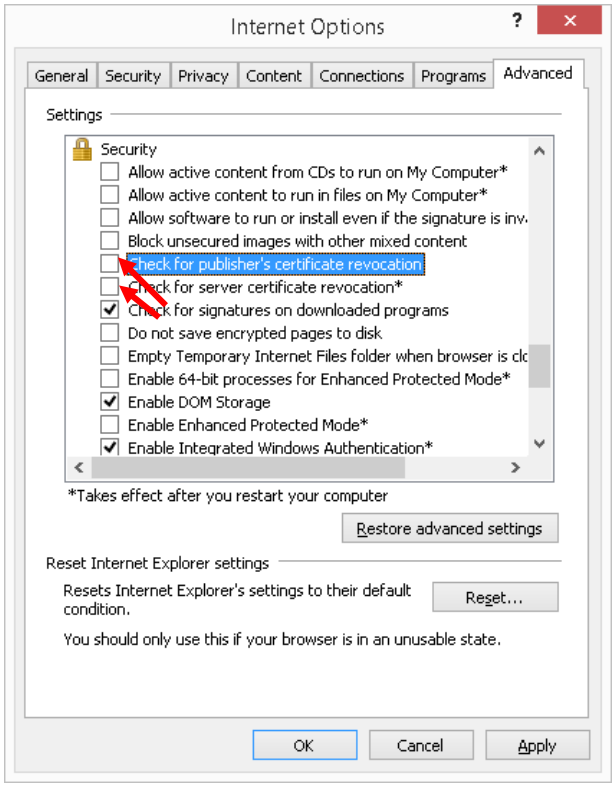


5. Click “Close” and then OK to close the window to complete the setting

5.7 Disable Certificate Revocation Check

It apply to standalone CCASS Terminal with no Internet connection.

1. Go to “Control Panel” → “Internet options” and then click on “Advanced” tab.
2. Go to Security section and **uncheck** the following options
   i. Check for publisher’s certificate revocation
   ii. Check for server certificate revocation



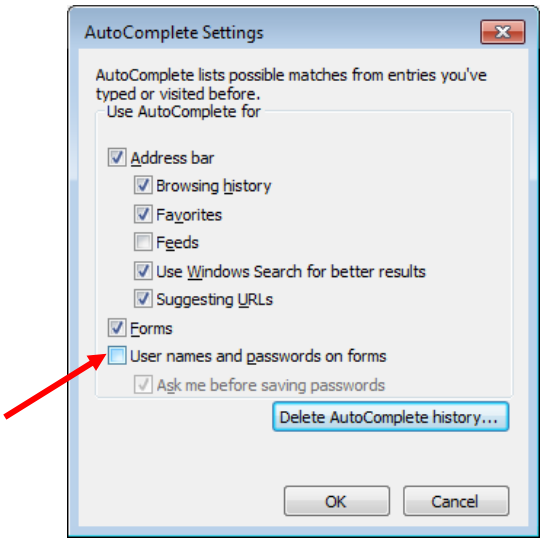
3. Click “Apply” and OK to close the window to complete the setting

5.8 Disable AutoComplete for User Names and Passwords

1. Go to “Control Panel” → “Internet options” and then click on “Content” tab. Click “Settings” button

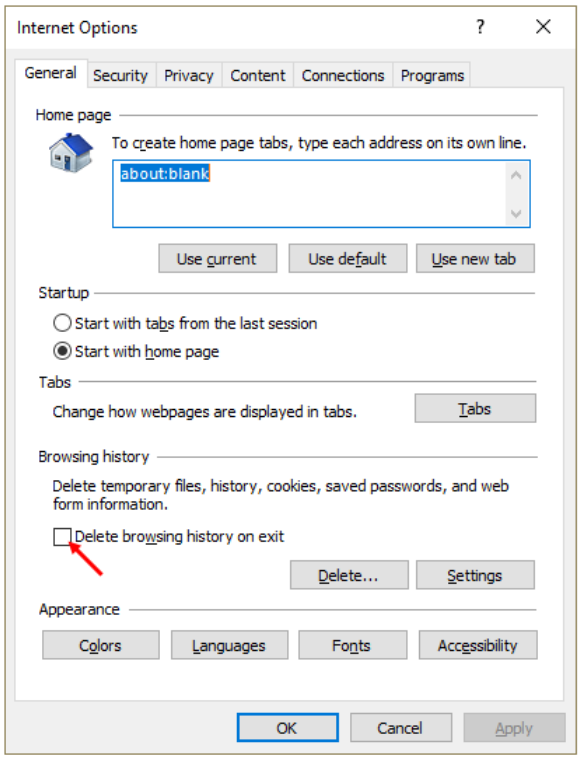
2. Uncheck the option “User names and passwords on forms”

3. Click “OK” to save

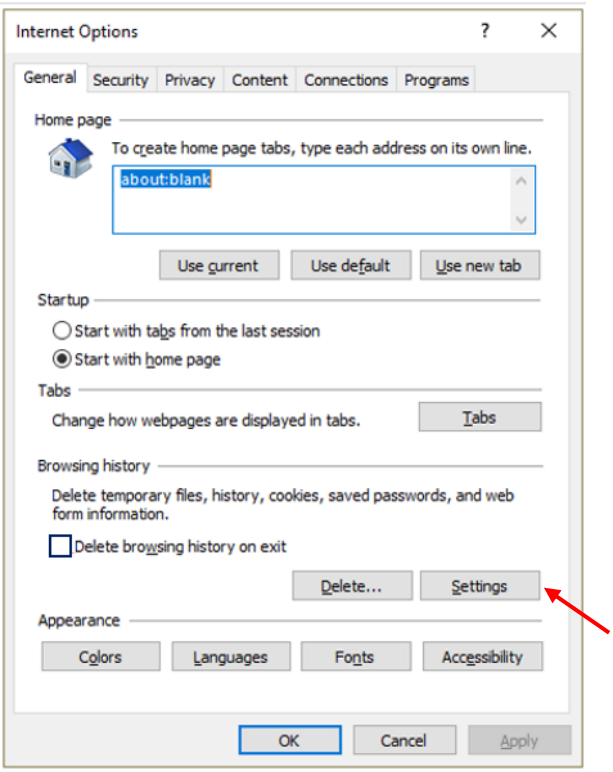


5.9 Browsing History

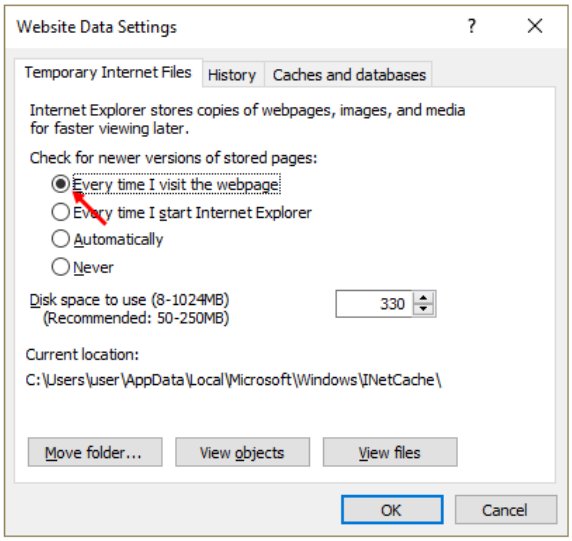
1. Go to “Control Panel” → “Internet options” and then go to “Browsing History”.
2. Ensure that the option “Delete browsing history on exit” is **not checked**



3. Then click on Settings

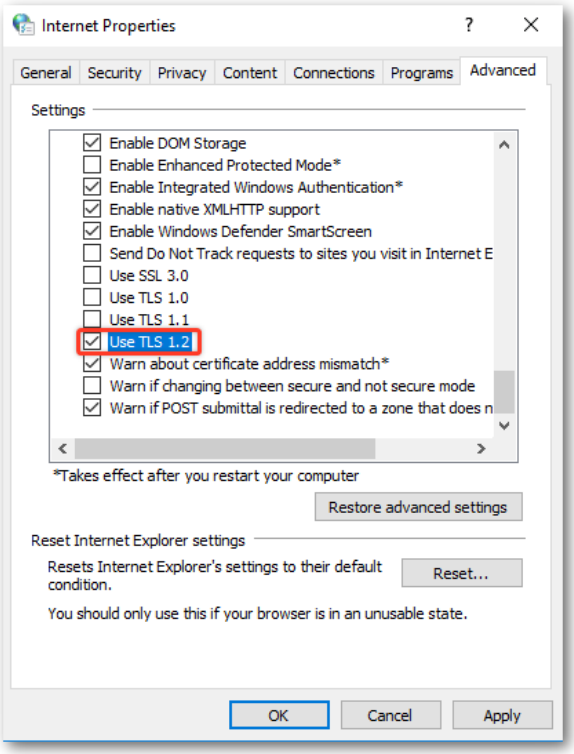


4. Ensure the option “Every time I visit the webpage” is **checked**



5.10 TLS Connection Settings

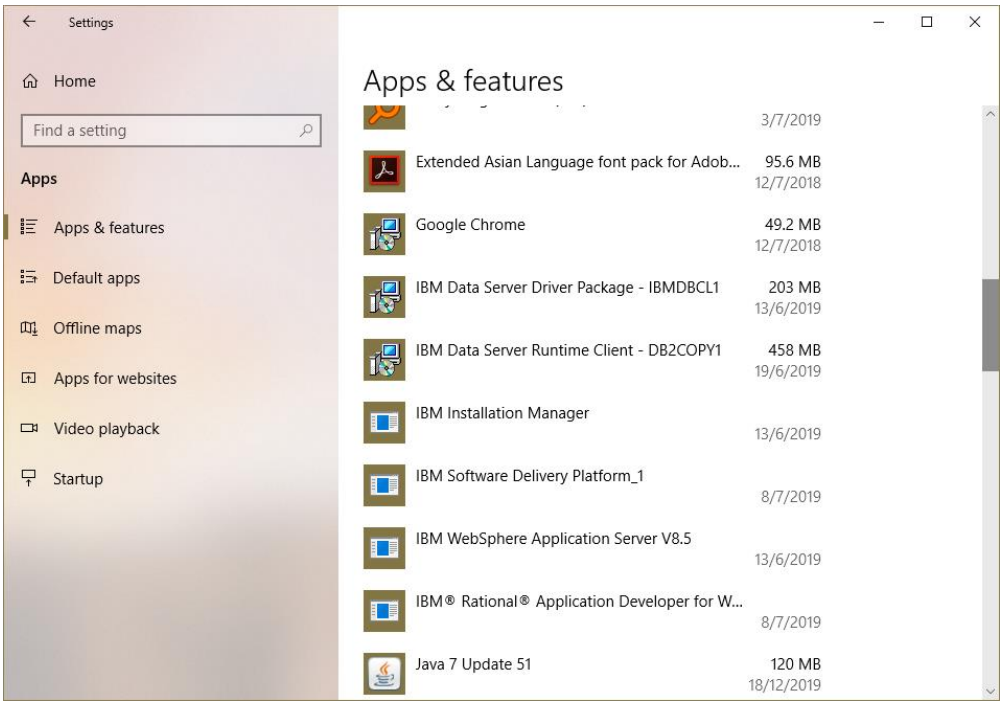
Only TLS 1.2 should be enabled while all other protocols should be disabled.
Go to “Control Panel” → “Internet Options” → “Advanced” tab, and then scroll down to “Security” section. Check only TLS 1.2 and uncheck other SSL or TLS protocols.



5.11 Verify Java Plugin

Please follow steps below to verify if there is any obsolete JRE installed that would require un-installation.

1. Click “Start” button, select “Windows Settings”. Go to Apps



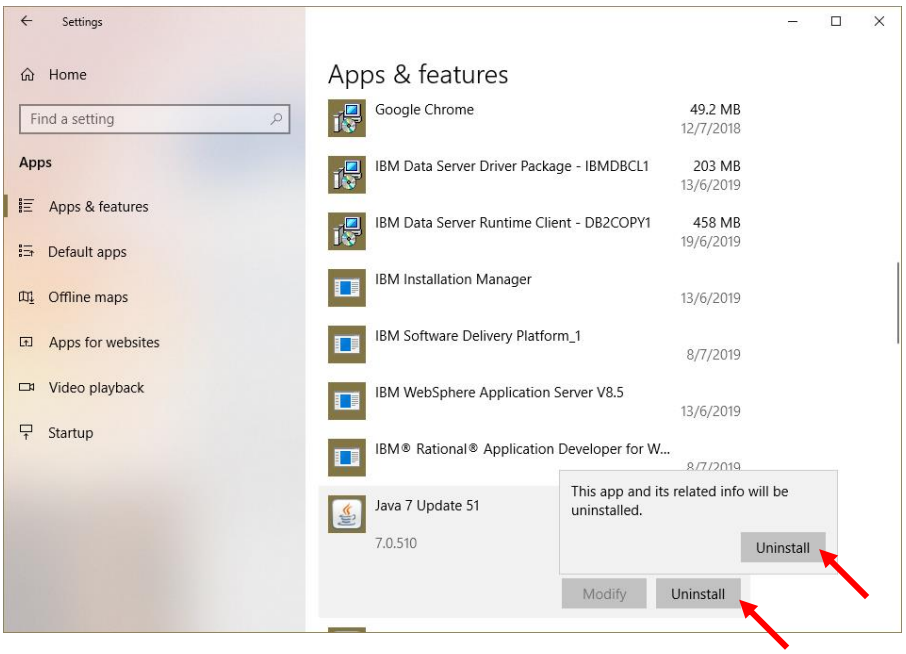
2. Find “Java X Update XX” in the list

- **If non-supported JRE is found, please go to Section 5.12 for uninstallation**
- **If no JRE is found, please go to Section 5.13 for Java plugin installation**

5.12 Uninstall Previous Java Plugin

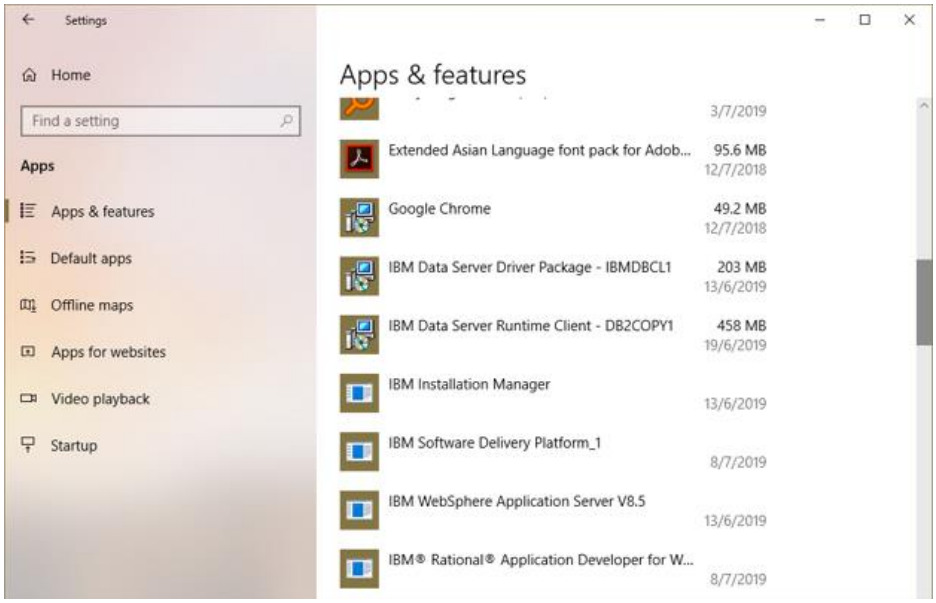
Please make sure any previous version of JRE is removed before the new one is installed.

1. Go to “Uninstall a program” in Control Panel.
2. Ensure all Internet browser windows are closed.
3. Highlight the JRE item, and then click on the “Uninstall” button at the top. Click on “Uninstall” button for the alert “This app and its related info will be uninstalled” alert shows.



4. Click “Yes” when the “User Account Control” appear

5. Check again that all JRE items should be removed



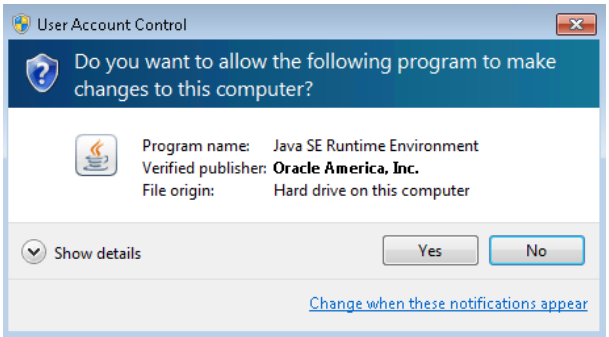
6. Restart the computer

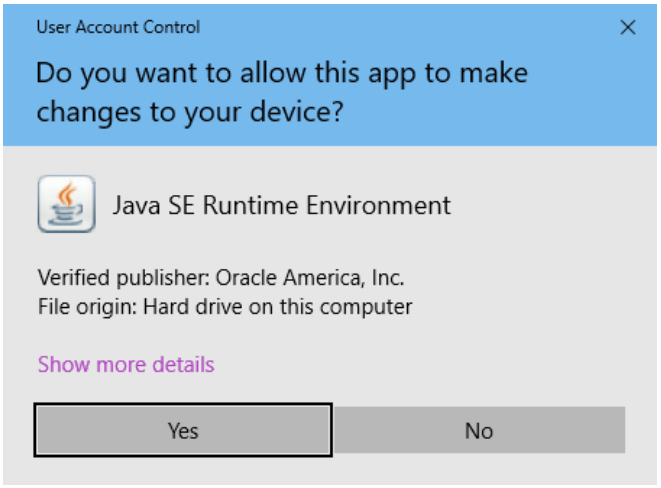
5.13 Java Plugin Installation

1. Ensure you have proper license subscription of Oracle Java, otherwise please refer to (https://www.oracle.com/java/java-se-subscription.html) about Oracle Java SE Desktop subscription.
2. Download the following two installers of Windows x86 and x64 version of Oracle Java SE Runtime Environment 8u311 from (https://www.java.com/en/download/ or https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html).

   jre-8u311-windows-i586.exe – for Windows x86

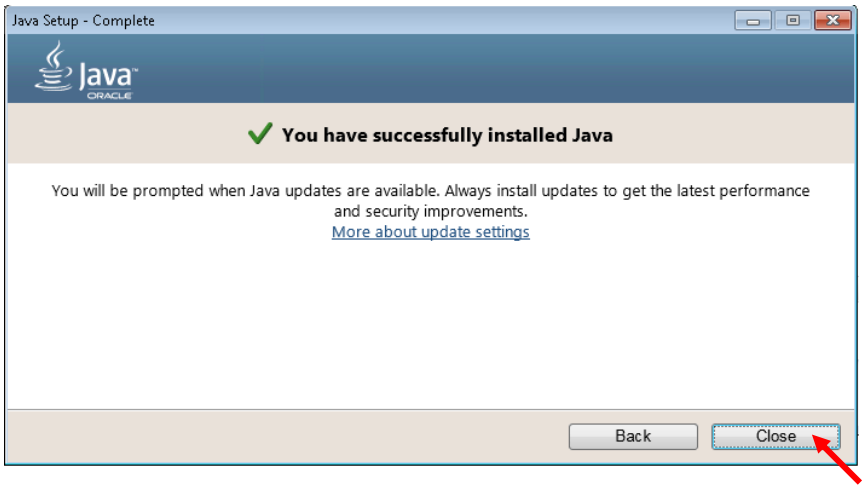
   jre-8u311-windows-x64.exe – for Windows x64
3. Double click to start installation of both installers.
4. Click “Yes” when the “User Account Control” Window appears





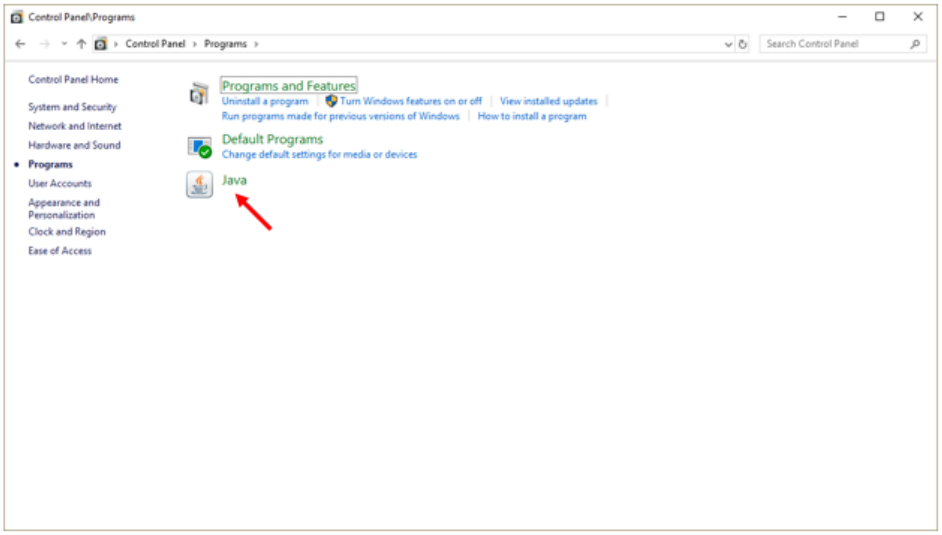
5. Ensure all Internet browser windows are closed.
6. Click “Install>”button to continue

7. Wait for installation to complete and click “Close”

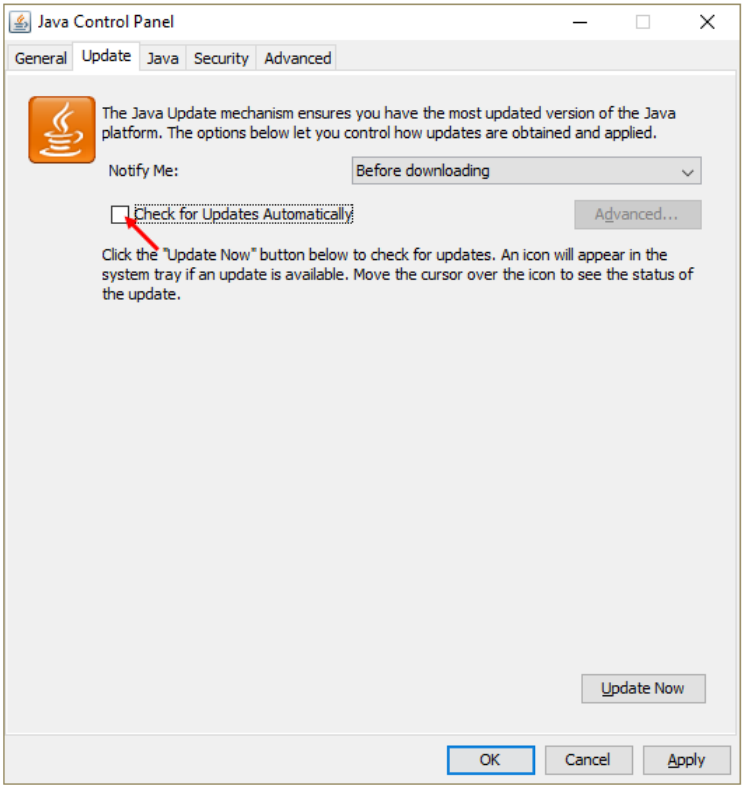


5.14 Java Plugin Configurations

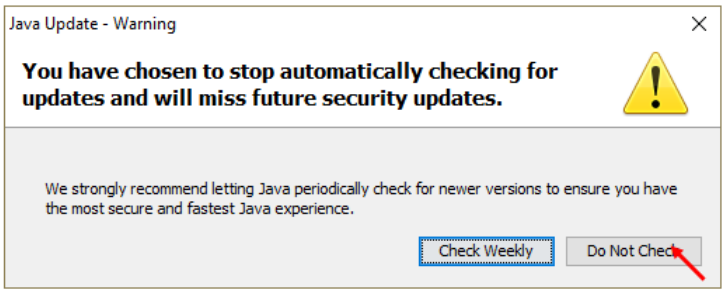
1. Auto update should be disabled. To do so, click “Start” to launch start menu then “Control Panel” and then click “Program” and then click “Java”



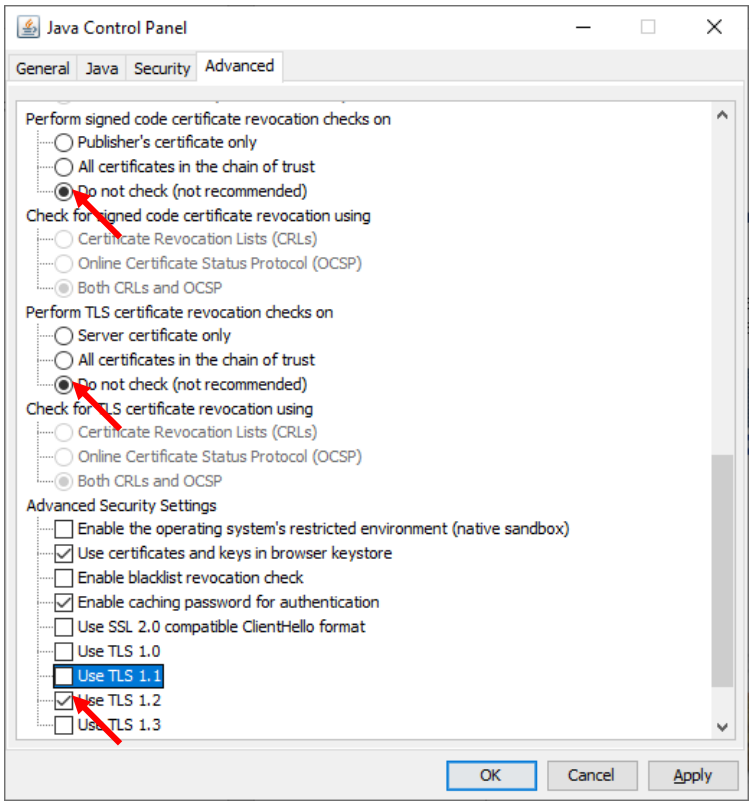
2. Select “Update” tab and uncheck “Check for Updates Automatically”.



3. Click “Do Not Check” button in the warning dialog.



4. Click “Advanced” Tab and then scroll to the bottom.
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 1.2

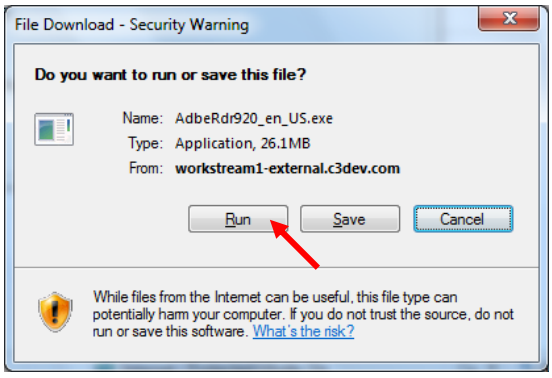


6. Click Apply and then OK to exit the window.

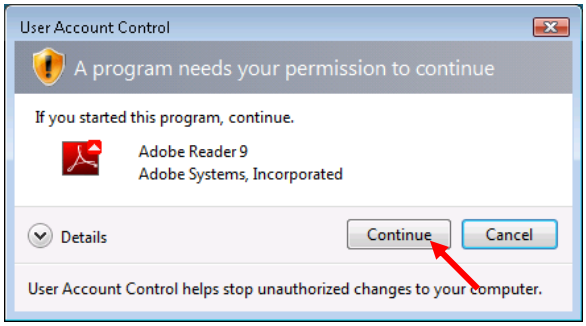
5.15 Acrobat Reader Installation

1. Launch Internet browser, enter https://www.ccass.com/commissioning/download in address box. Click the associated link to download Adobe Acrobat Reader.

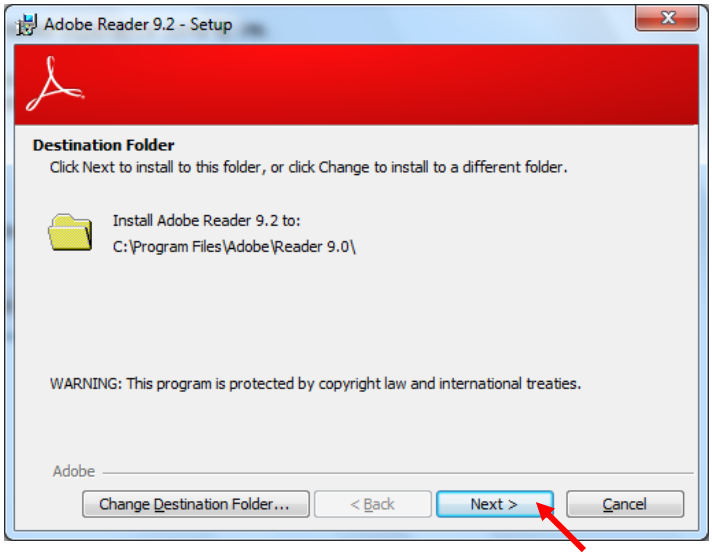
2. Click "**Run**" or "**Open**" button and wait for installation starting after the file to be downloaded to the PC



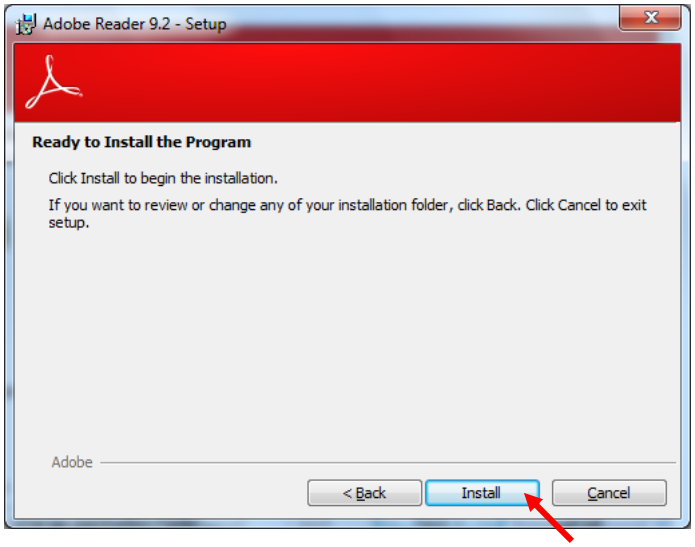
3. Click "Continue" button to continue and start to install Acrobat Reader



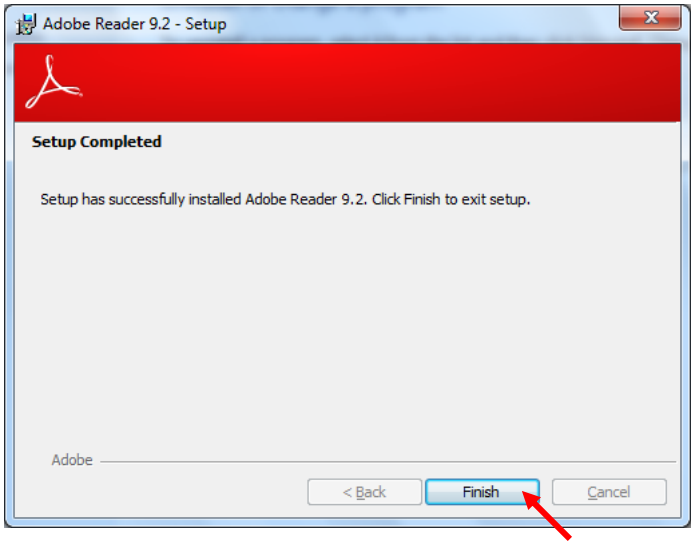
4. Click “Next” to proceed installation in default settings



5. Click “Install” to start installation



6. Click "**Finish**" to complete installation.

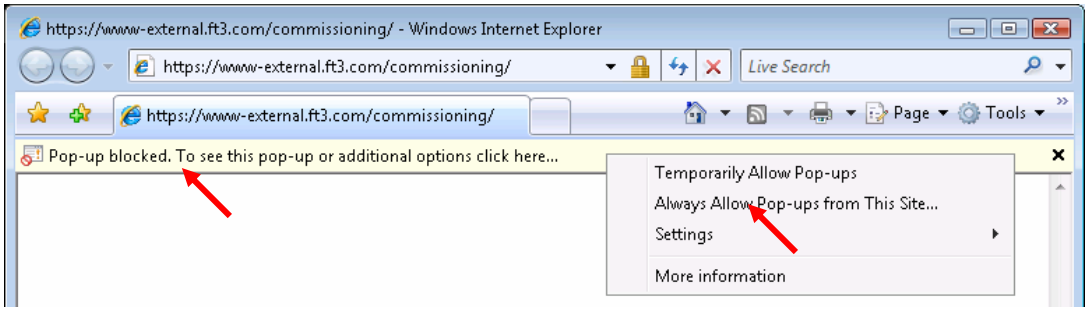


5.16 Smartcard Initialization and Commissioning Logon

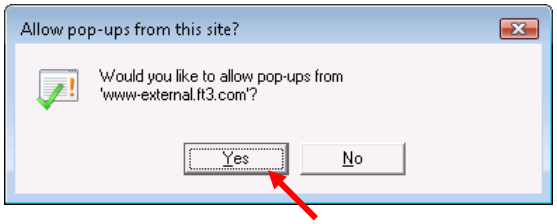
1. Launch Internet browser, insert Smartcard and type CCASS Logon URL https://www.ccass.com

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

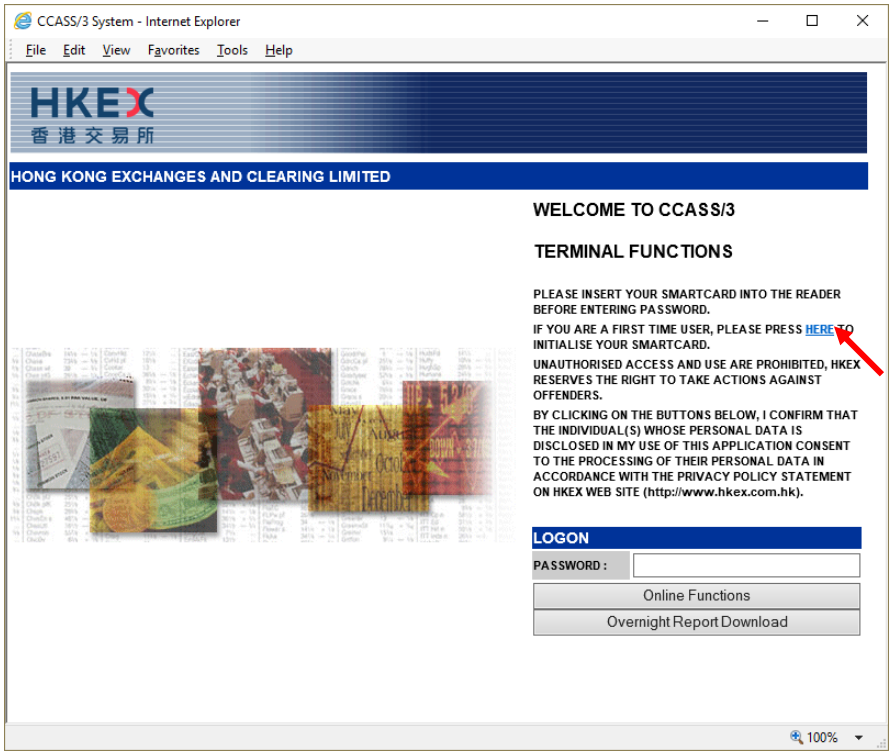
2. Point to “Pop-up blocked” information bar, then right click on it and then click on “Always Allow Pop-ups from This Site…”



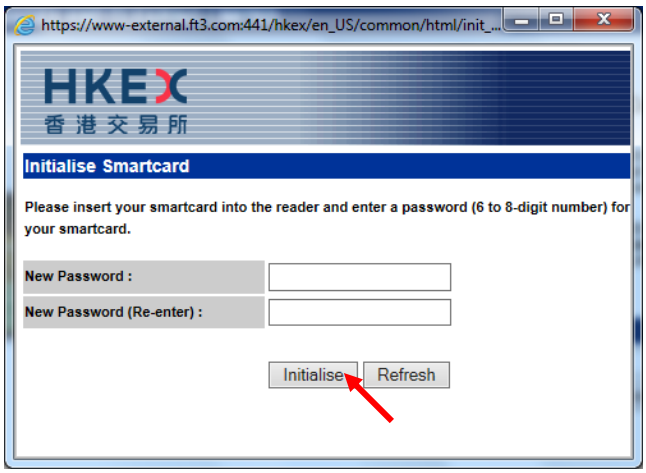
3. Click “Yes” to allow pop-ups from this site



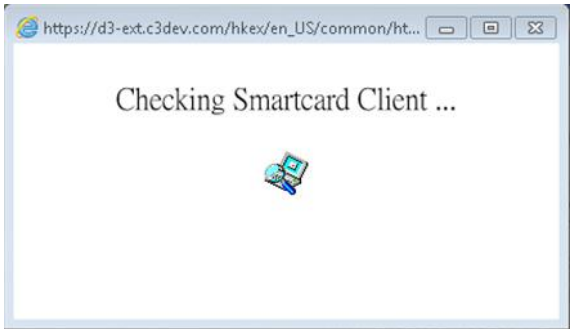
4. A new window will pop up. Smartcard must be initialised for first time usage. Click “HERE” icon to proceed



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



6. Another pop up window will show to connect to Smartcard Reader.



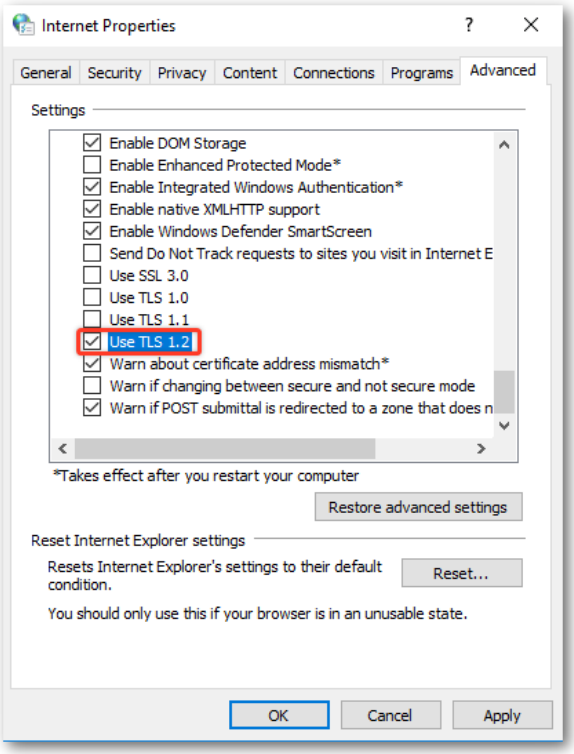
7. Click “OK” button to finish initialisation and go back to logon CCASS Terminal

6 VaR Online

HKSCC Clearing Participants who would like monitor and conduct risk management simulation can apply for VaR Online DA and setup their own user access to VaR Online.

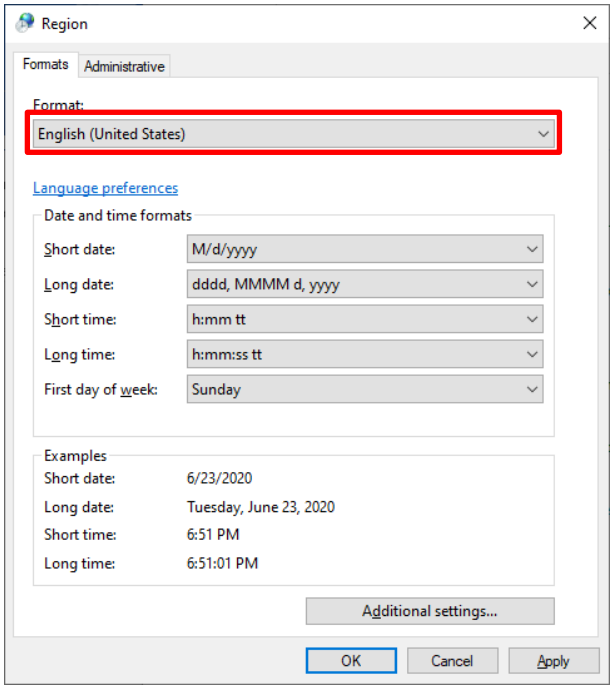
6.1 TLS Connection Settings

Only TLS 1.2 should be enabled while all other protocols should be disabled. Go to “Control Panel” → “Internet Options” → “Advanced” tab and then scroll down to “Security” section. Check only TLS 1.2 and uncheck other SSL or TLS protocols.



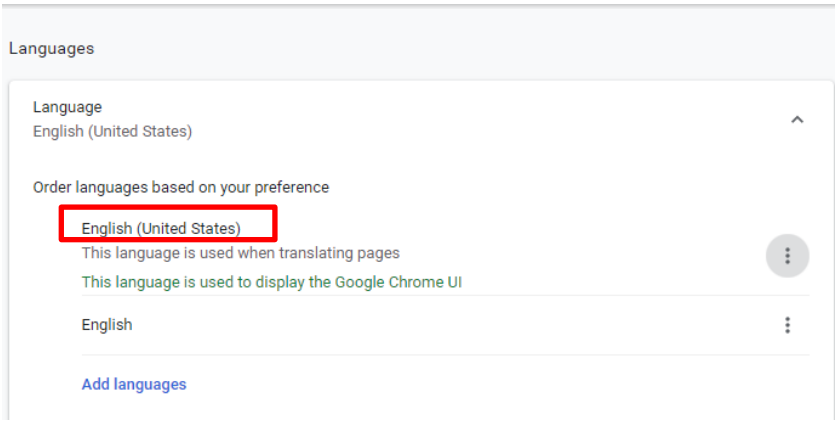
6.2 Language Settings in Windows

Please ensure the language of operating system is set to English (United Status). Go to “Control Panel” → “Region”



6.3 Language Settings in Chrome

Please ensure the language of Chrome is set to English. Go to “Settings” → “Advanced” → “Languages”



6.4 Language Settings for VaR Online

Please ensure the language of the delegated PC is to English (United States). Go to “Settings” → “Languages”

7 RAP Technical Setup

After the network setup is completed, HKSCC Clearing Participants should proceed to configure their RAP setup & connectivity according to the HKSCC Report Access Platform (RAP) Technical Guide (https://www.hkex.com.hk/Services/Next-Generation-Post-Trade-Programme/-/media/HKEX-Market/Services/Next-Generation-Post-Trade-Programme/NGRM/HKSCC%20Report%20Access%20Platform%20(RAP)%20Technical%20Guide.pdf)