



CCASS (CCMS) Terminal Installation Procedures

Date:

Jul 2023

TABLE OF CONTENTS

TABLE OF CONTENTS	2
1. OVERVIEW	3
1.1 BACKGROUND	3
2. System Requirements	4
2.1 PC CONFIGURATION REQUIREMENTS	4
HIGHLIGHTED BELOW ARE THE MINIMUM PC CONFIGURATIONS FOR CCASS (CCMS) TERMINALS.	4
2.2 COMPUTER VIRUS/WORM SECURITY MEASURES:	5
3. Communication Line Setup	7
3.1 CONNECT PC TERMINAL WITH ROUTER	7
4. Network Setup	9
4.1 WINDOWS IP ADDRESS CONFIGURATIONS	9
4.2 DNS SERVERS.....	13
4.3 DISASTER RECOVERY	13
4.4 SOURCE IP ADDRESS	13
4.5 DNS SETTINGS VERIFICATION	13
4.6 SPECIAL NETWORK SETTINGS FOR PC NOT COMPLIANT TO STANDARD CONFIGURATIONS.....	15
4.7 APPLICATION SERVICES TO BE ACCESSED	16
4.8 SPECIAL SETTINGS FOR DOMAIN NAME RESOLUTION	16
5. CCASS (CCMS) Terminal	17
5.1 INTERNET BROWSER SETTINGS	17
5.2 SETUP FOR MS EDGE BROWSER WITH INTERNET EXPLORER MODE.....	17
5.3 COMPATIBILITY VIEW SETTINGS (IN INTERNET EXPLORER 11).....	32
5.4 LOCAL INTRANET SETTINGS	33
5.5 DISABLE CERTIFICATE REVOCATION CHECK	34
5.6 DISABLE AUTOCOMPLETE FOR USER NAMES AND PASSWORDS.....	35
5.7 BROWSING HISTORY.....	36
5.8 TLS CONNECTION SETTINGS	38
5.9 VERIFY JAVA PLUGIN	39
5.10 UNINSTALL PREVIOUS JAVA PLUGIN	40
5.11 JAVA PLUGIN INSTALLATION	41
5.12 JAVA PLUGIN CONFIGURATIONS	43
5.13 ACROBAT READER INSTALLATION.....	45

1. OVERVIEW

1.1 Background

This document serves as a technical reference guide for HKSCC / HKCC / SEOCH Participants and HKSCC Designated Banks to install and configure their PC terminal for CCASS (CCMS) functions. This document applicable to both Participants and Designated Banks for the installation of CCASS (CCMS) Terminals.

2. System Requirements

2.1 PC Configuration Requirements

Highlighted below are the minimum PC configurations for CCASS (CCMS) Terminals.

Item	Description
CPU	1GHz
Memory	2GB
HD	20GB
OS	Win 10 Pro (64 bit) ¹
Browser	MS Edge ² version 94 or above
JRE	Oracle JRE 8u341 ³ (both x86 and x64)
Software	<ul style="list-style-type: none"> • Acrobat Reader 11 or above • Anti-virus
Bandwidth⁴	1M

¹ Windows 10 Pro version 20H1 or higher

² With Internet Explorer Mode enabled for CCASS/3 Terminal website

³ One needs proper license subscription to download Oracle JRE 8u341. 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 8u341 from (<https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html>).

⁴ 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 CCASS (CCMS) design to protect it from computer virus or worms attacks. Participants are reminded that their PCs should be dedicated solely to accessing CCASS (CCMS) services as uncontrolled access to the Internet will expose Participants' CCASS (CCMS) Terminals 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 with CCASS (CCMS) Terminal for uploading or downloading CCASS (CCMS) information.

In view of the above, CCASS (CCMS) Terminal users should pay attention and take proactive action to the security measures in their own CCASS (CCMS) Terminals in the following two areas:

Virus protection

Participants are recommended to install anti-virus software on their CCASS (CCMS) Terminals and regularly update the virus definitions from the vendor. For CCASS (CCMS) Terminals 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 at CCASS (CCMS) Terminal.

Microsoft OS patch

Participants are also advised to regularly review the latest Microsoft security patches and install them on their C3Ts 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 CCASS (CCMS) Terminals 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 CCASS (CCMS) Terminal.

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 CCASS (CCMS) Terminal. The patches may be in different formats, please follow Microsoft's instruction to install the patches.

PROHIBITED ACTIONS ON CCASS (CCMS) HOST SYSTEM:

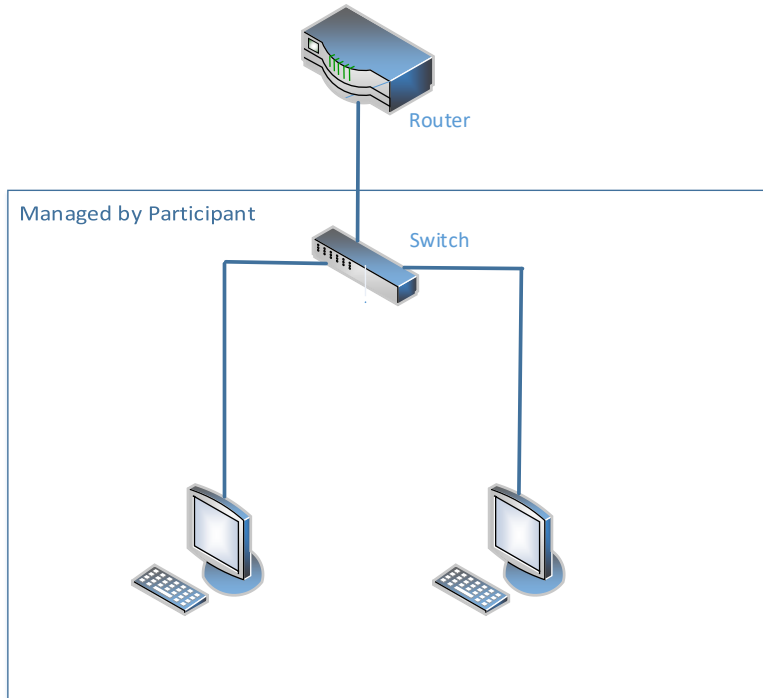
Participants must not perform any unauthorized access or security scanning (no matter at network, system or application level) on the CCASS (CCMS) system and any related network device not owned by them. Any such attempt will be regarded as illegal access or malicious intrusion to CCASS (CCMS) host system.

3. Communication Line Setup

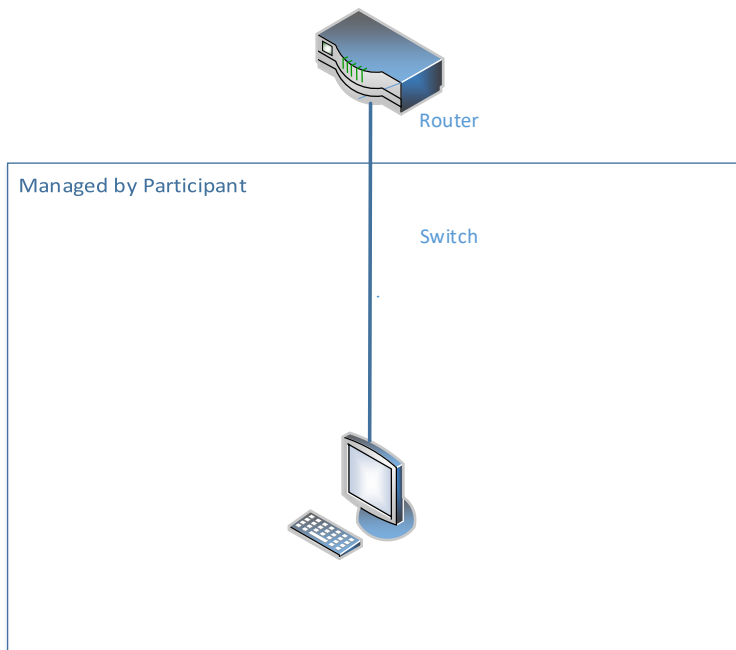
3.1 Connect PC Terminal with Router

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.

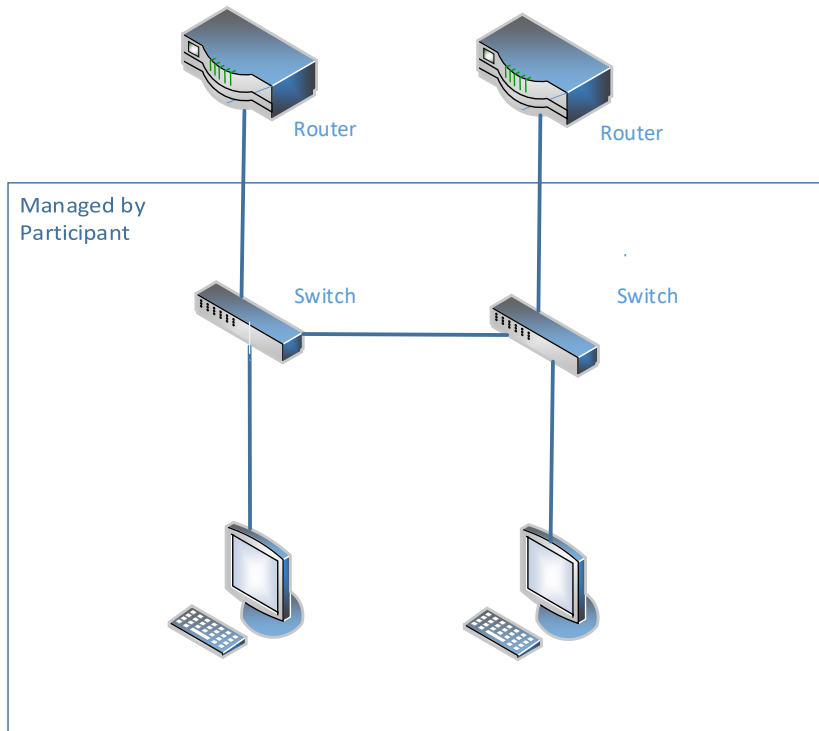
Option 1: Single Link Connection



Option 2: Single Link Connection with Direct Connection to Router



Option 3: Dual Link Connection



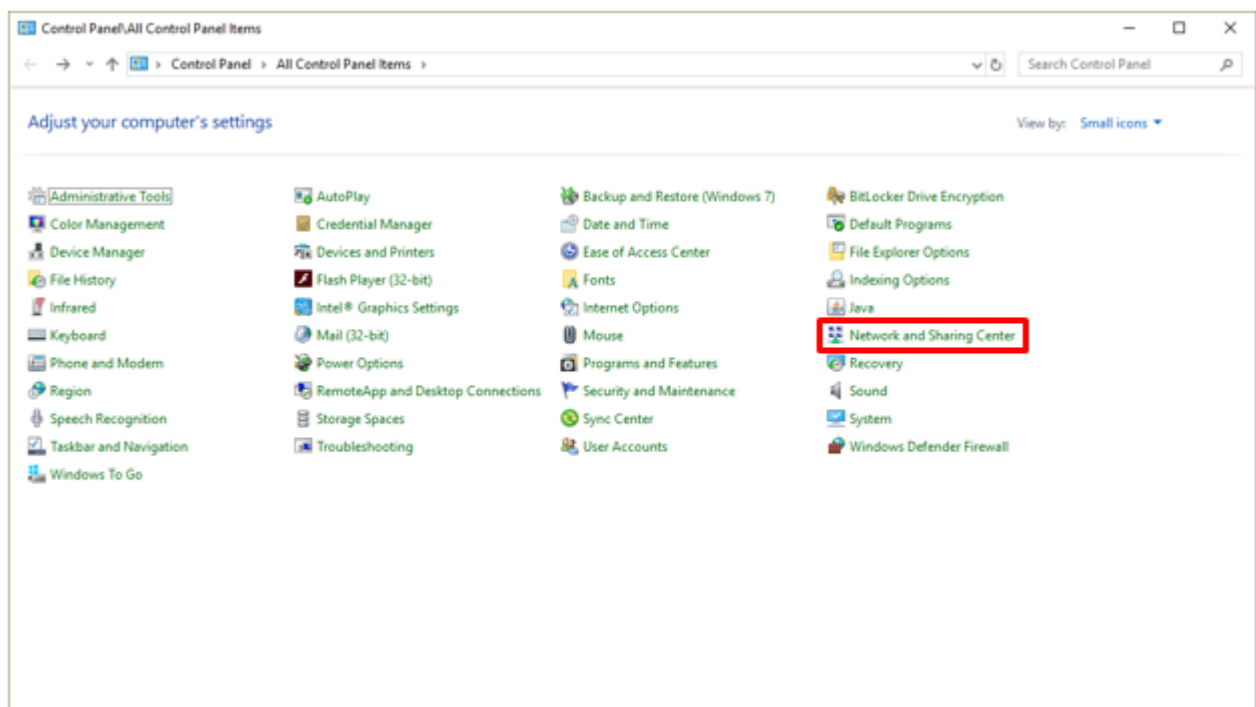
To maintain robustness, Participants should establish contingency plan and build in resilience to cope with emergencies and disruptions in their clearing and settlement operations. The contingency plan should include suitable backup arrangements to prevent single points of failure from disrupting their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

4. Network Setup

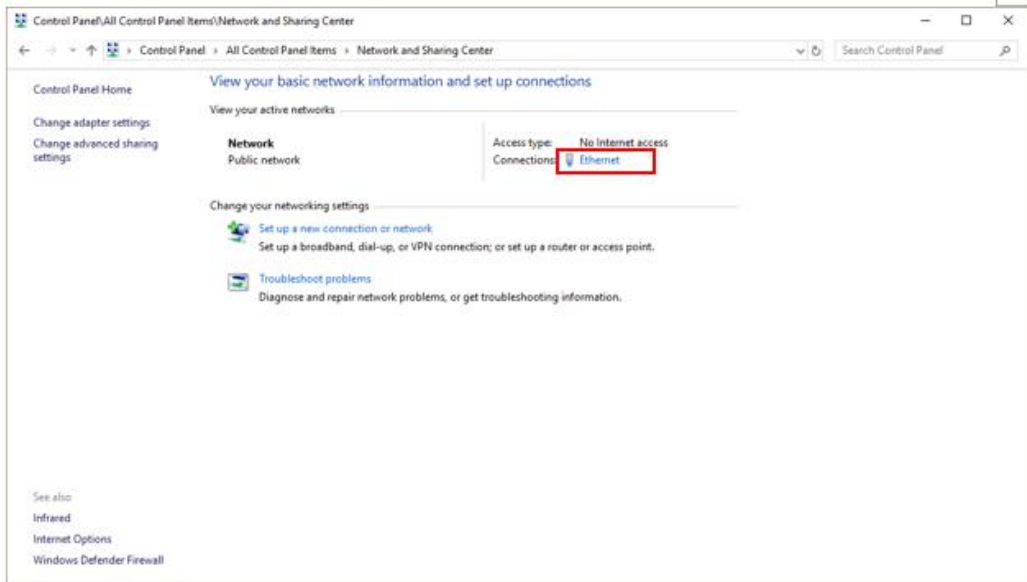
Please follow procedures below for the PC terminal.

4.1 Windows IP address Configurations

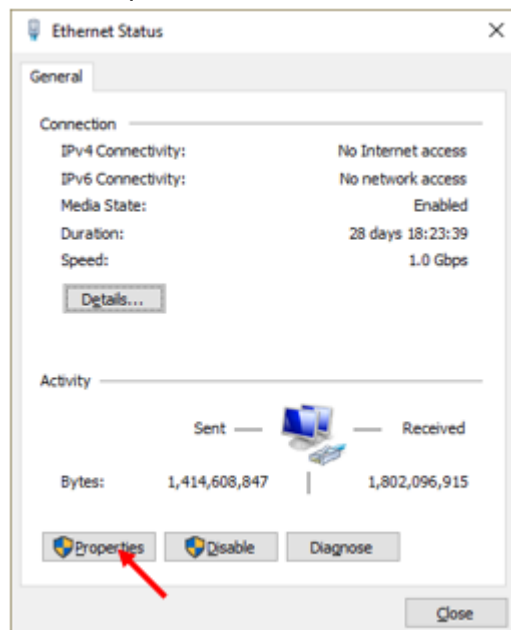
1. To configure TCP/IP for the WAN Router & Ethernet Card Connection, you need an “administrator” account. Please ensure you have the appropriate access right.
2. Click “Search” and input “Control Panel”
3. Select “Control Panel”
4. Click on "Network and Sharing Centre"



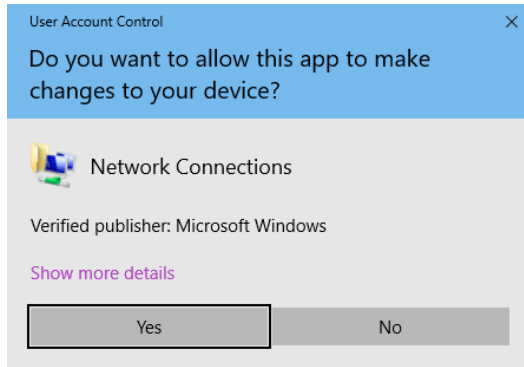
5. Click “Local Area Connection” or ”Ethernet” under “View your active networks”.



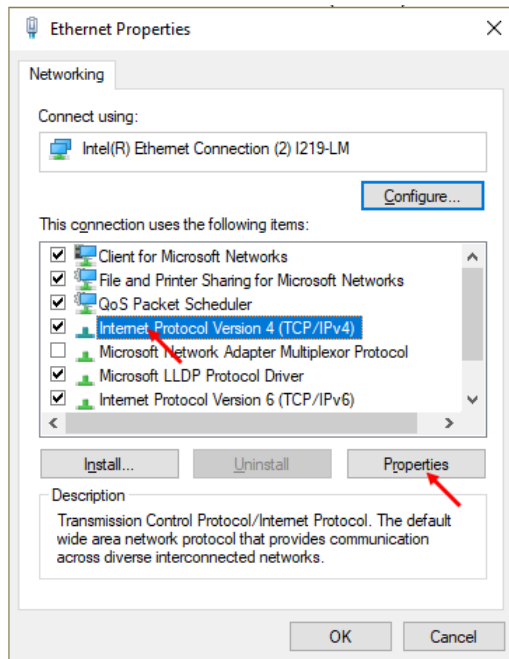
6. Click “Properties”.



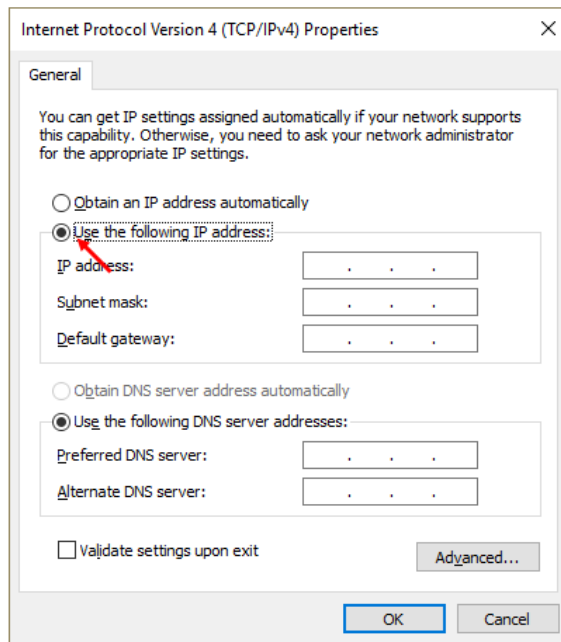
7. Click "Yes" in for alert message.



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 (CCMS) Terminal: 10.1xx.x.11 - 10.1xx.x.100

Participant Gateway (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 (CCMS) Terminal: 10.1xx.x.139 - 10.1xx.x.228

Participant Gateway (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 (CCMS) Primary site)

Alternate DNS Server: 10.243.65.1 (CCASS (CCMS) Secondary site)

4.3 Disaster Recovery

During disaster recovery (DR) failover, participants' PC 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 required on the PC. Therefore, it is important for the PC to be configured with **both** Primary and Alternate DNS server IP addresses above.

If for any reason other DNS server is used, it should be ensured that DNS forwarding is enabled to resolve the domain names of "ccass.com" and "hkexposttrade.com.hk" from HKEX DNS servers.

4.4 Source IP Address

Each SDNet circuit is assigned with a pre-defined range of IP addresses. The participant / designated bank should ensure that terminals should appear with the same IP address as original in each connection. If there is any Network Address Translation (NAT) performed, the participant / designated bank should be responsible for translating back it 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 a one-to-one mapping. That is, IP address of each terminal should be translated to a unique value within the original IP address range.

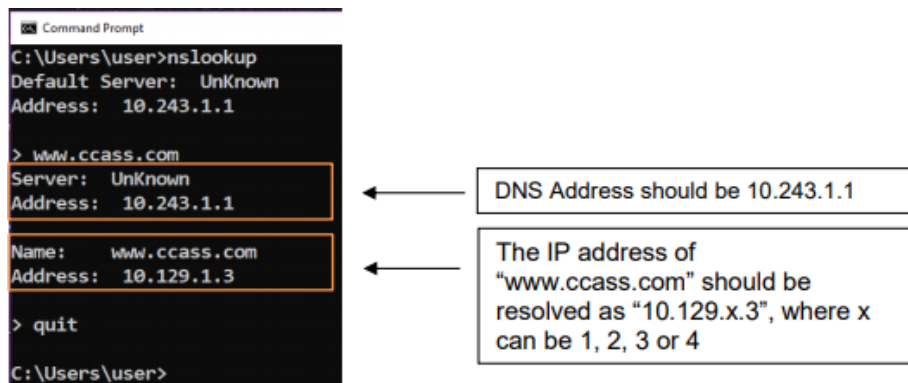
4.5 DNS Settings Verification

Please follow steps below to verify your DNS settings after completion of DNS setup (section 4.2).

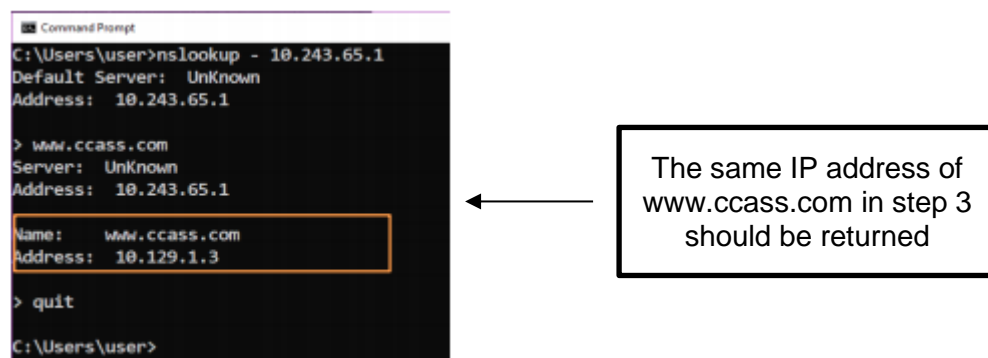
1. Go to Start and type cmd in the search field to open the command prompt



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



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



7. Type quit to exit and close the command prompt window
8. CCASS (CCMS) is in service, logon CCASS (CCMS) Terminal normally to verify the connectivity
9. Please repeat the above verifications for all your CCASS (CCMS) Terminals

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 (CCMS) service. Please follow sections below for additional configurations.

4.7 Application Services to be Accessed

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

CCASS (CCMS):

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 ⁵ www.ccass.com	TCP: 441, 442, 443	CCASS Web ⁶ (PR & DR)
HTTPS	10.243.2.15 sso.hkexposttrade.com.hk	TCP:443	CCASS 2FA Logon (PR) ⁷
HTTPS	10.243.66.15 sso.hkexposttrade.com.hk	TCP:443	CCASS 2FA Logon (DR)

4.8 Special Settings for Domain Name Resolution

Important Notes : If your DNS setting⁸ 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 are different from its Primary ones. In addition, HTTPS services must be accessed by domain name and thus all host entries in tables above should 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

⁵ 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 (CCMS) web IP for your SDNet line.

⁶ The web IP address for CCASS (CCMS) is the same in both its Primary and Secondary sites if via the same SDNet line

⁷ Participants will be redirected to CCASS 2FA Logon for authentication and then switch back to CCASS Online functions or Security Management functions automatically.

⁸ 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.

b. CCASS 2FA Logon

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.

1.

5. CCASS (CCMS) Terminal

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

- **MS Edge Browser with IE Mode**: Configurations must be made or otherwise some CCASS (CCMS) functions may not work properly. For details, please refer to **Section 5.1** to **Section 5.8** below
- **Java Plugin**: if you do not have Java Plugin installed, please go to **Section 5.11** 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 5.13** for the installation procedures.

5.1 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.

5.2 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>



HONG KONG EXCHANGES AND CLEARING LIMITED

WELCOME TO

CCASS/3 Terminal Commissioning

Download Area



PRESS [HERE](#) TO DOWNLOAD CCASS/3 TERMINAL SITE LIST

PRESS [HERE](#) TO DOWNLOAD CCASS/3 TERMINAL INSTALLATION PROCEDURES

PRESS [HERE](#) TO DOWNLOAD ROOT CA CERTIFICATE

PRESS [HERE](#) TO DOWNLOAD PROCEDURE TO INSTALL ROOT CA CERTIFICATE

CLICK [HERE](#) TO DOWNLOAD ADOBE® ADOBE® READER®

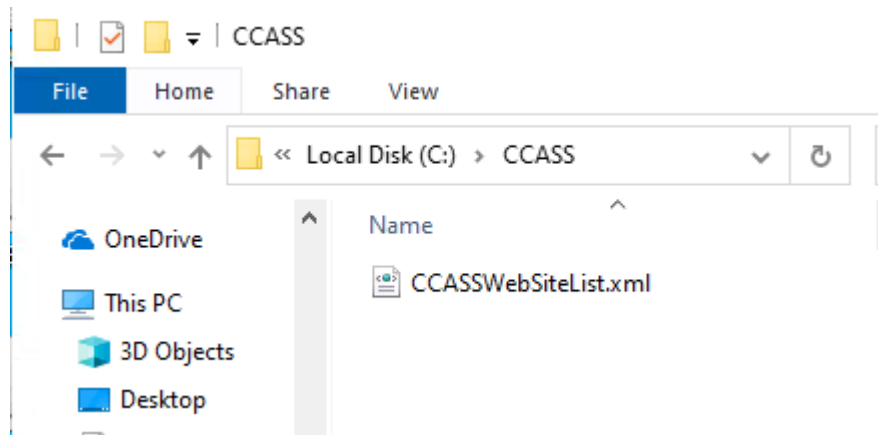
BY DOWNLOADING THIS SOFTWARE ONTO YOUR PC FROM THIS COMMISSIONING WEB PAGE, YOU AGREE TO USE THIS SOFTWARE FOR THE PURPOSE OF VIEWING PDF FILES WITHIN THIS CCASS/3 NETWORK ONLY. YOU ARE NOT ALLOWED TO REPRODUCE, MODIFY OR REDISTRIBUTE THE SOFTWARE OR USE IT FOR ANY OTHER PURPOSE, YOU FURTHER AGREE TO INDEMNIFY HKEX AND ITS SUBSIDIARIES AGAINST ANY CLAIMS, DAMAGES, EXPENSES AND COSTS THAT MAY ARISE AS A RESULT OF ANY UNAUTHORIZED USE BY YOU OF THE SOFTWARE.

IF YOU NEED TO CHECK THE SOFTWARE COMPATIBILITIES IN YOUR COMPUTER, PLEASE CLICK [HERE](#).

- 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”

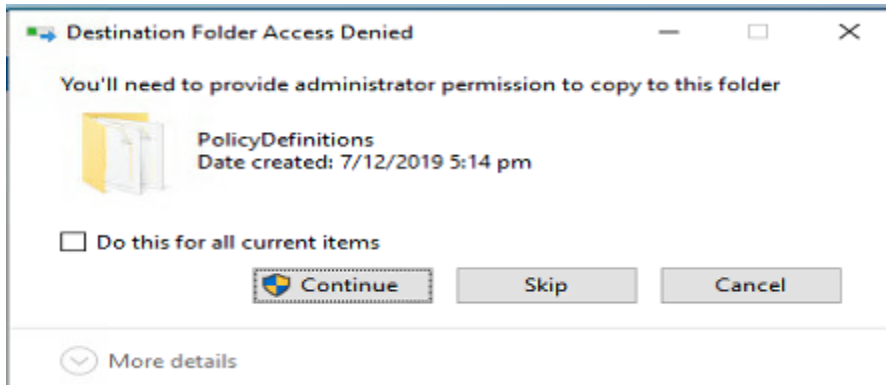
Download the latest build and version of Edge for business



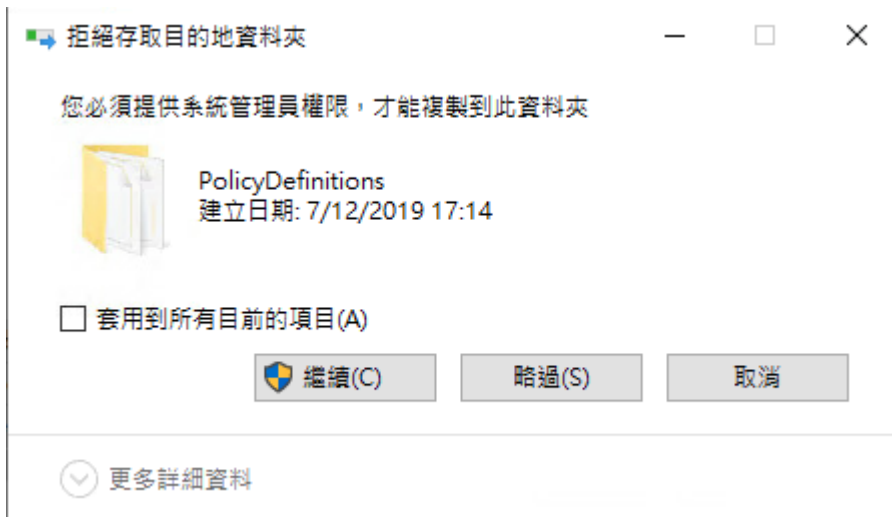
5. Install MS Edge by running MicrosoftEdgeEnterpriseX64.msi installer
6. Unzip MS Edge policy files to a temporary folder (e.g. C:\TEMP\)
7. Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\ to C:\Windows\PolicyDefinitions\

 msedge.admx	11/11/2021 11:24 pm	ADMX File
 msedgeupdate.admx	11/11/2021 11:24 pm	ADMX File
 msedgewebview2.admx	11/11/2021 11:24 pm	ADMX File

Click Continue for this security prompt to confirm copying:



For Chinese Windows OS:



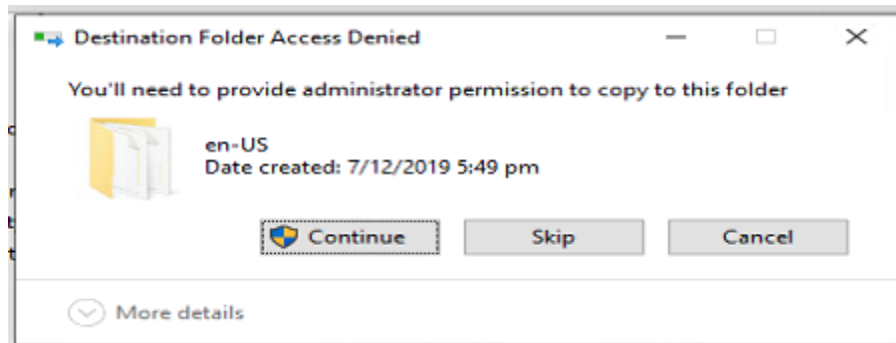
- Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\en-US\ to C:\Windows\PolicyDefinitions\en-US (for English Windows OS), or

Name	Date modified	Type
msedge.adml	11/11/2021 11:24 pm	ADML File
msedgeupdate.adml	11/11/2021 11:24 pm	ADML File
msedgewebview2.adml	11/11/2021 11:24 pm	ADML File

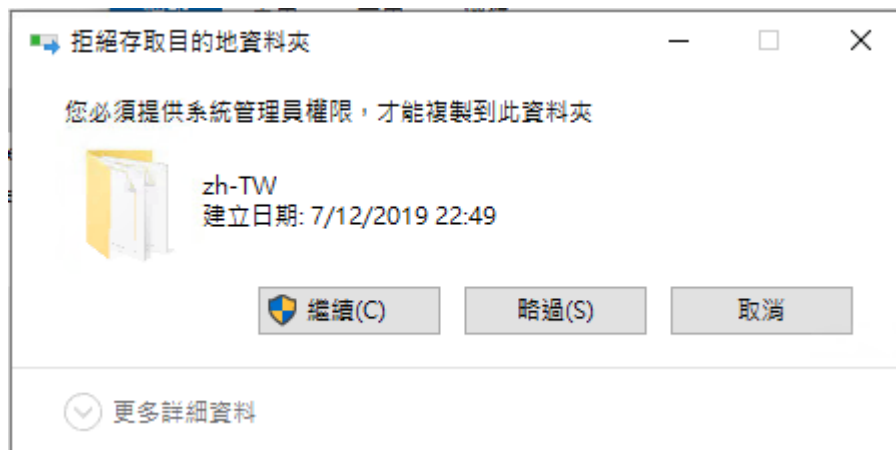
Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\zh-TW\ to C:\Windows\PolicyDefinitions\ zh-TW (for Traditional Chinese Windows OS)

Name	Date modified	Type
msedge.adml	11/11/2021 11:24 pm	ADML File
msedgeupdate.adml	11/11/2021 11:24 pm	ADML File
msedgewebview2.adml	11/11/2021 11:24 pm	ADML File

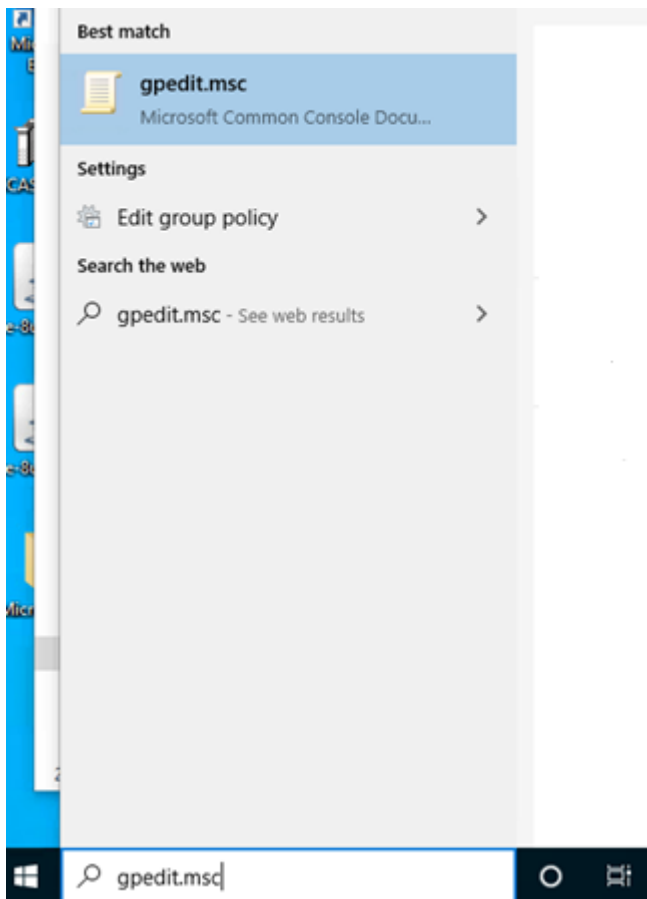
Click Continue for this security prompt to confirm copying:



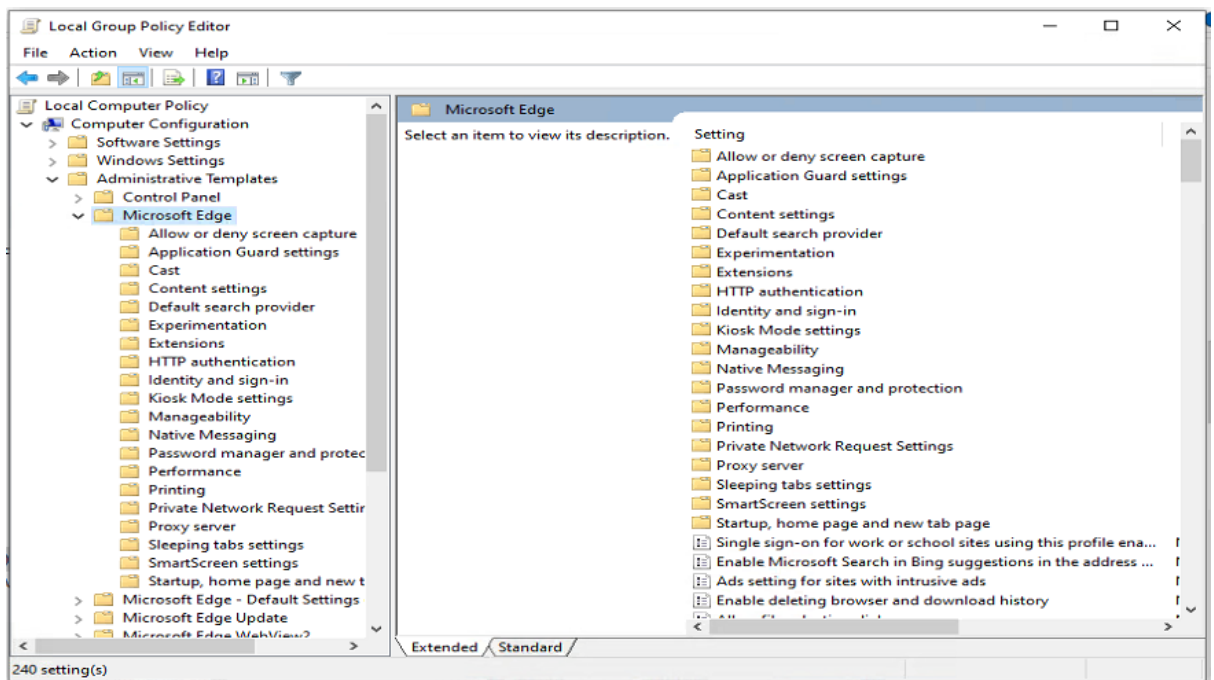
For Chinese Windows OS:



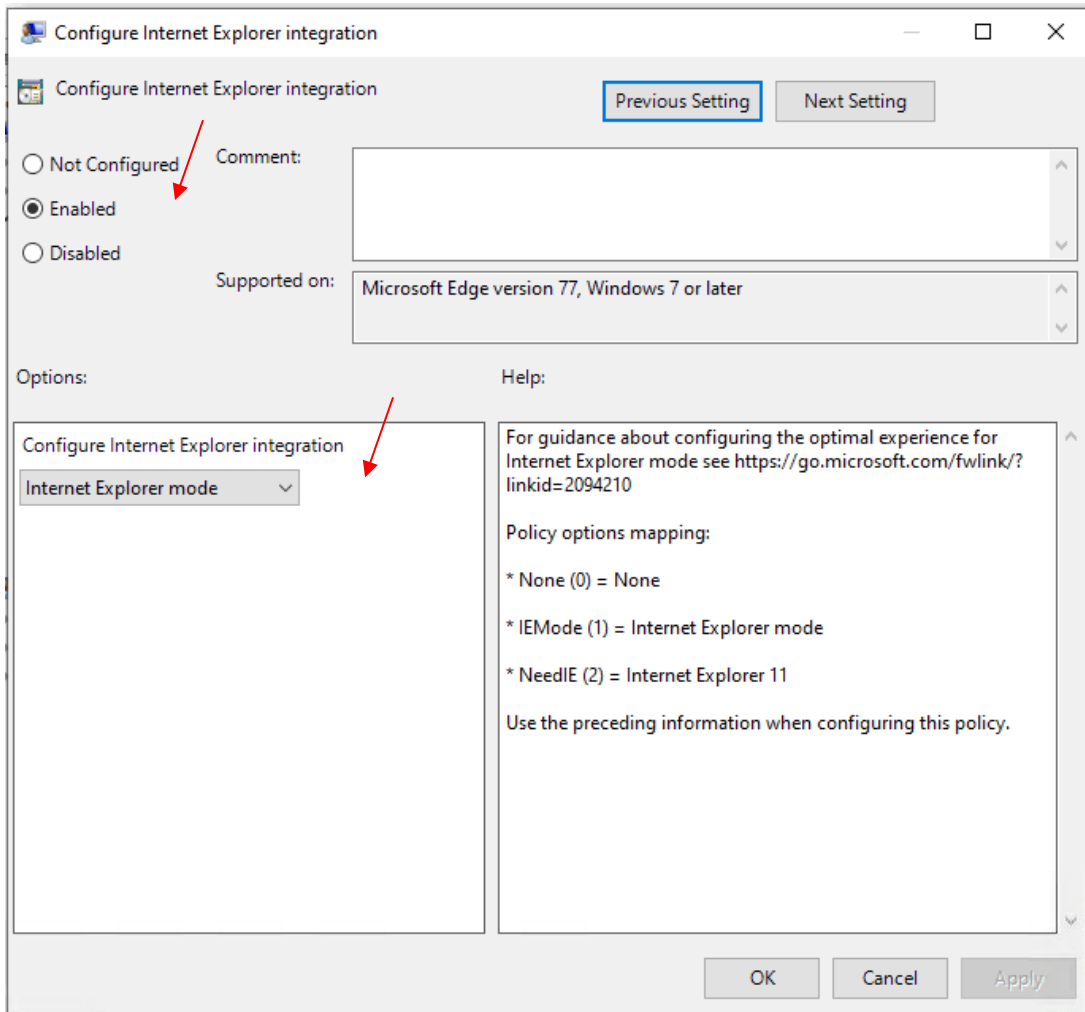
9. Open “Edit Group Policy” by typing “gpedit.msc” in the Search field box



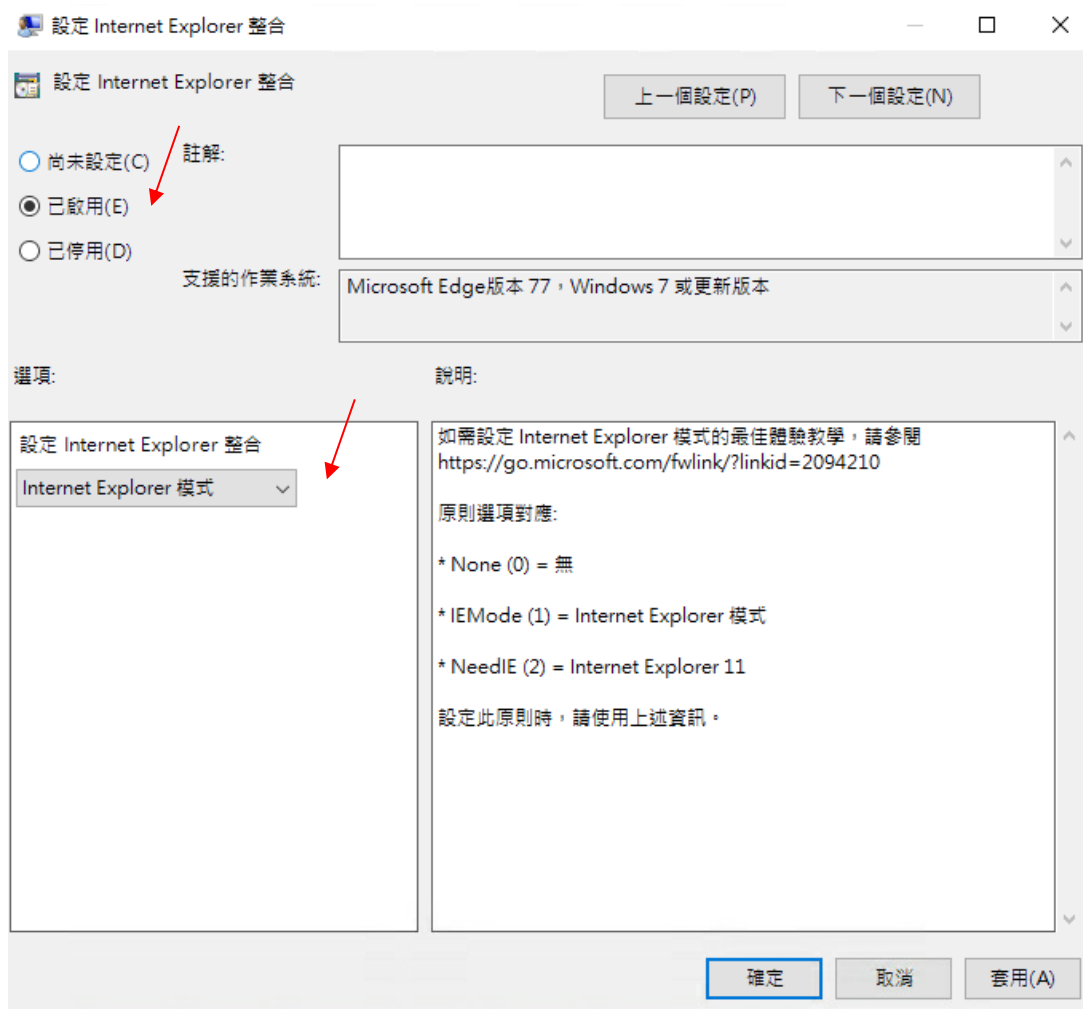
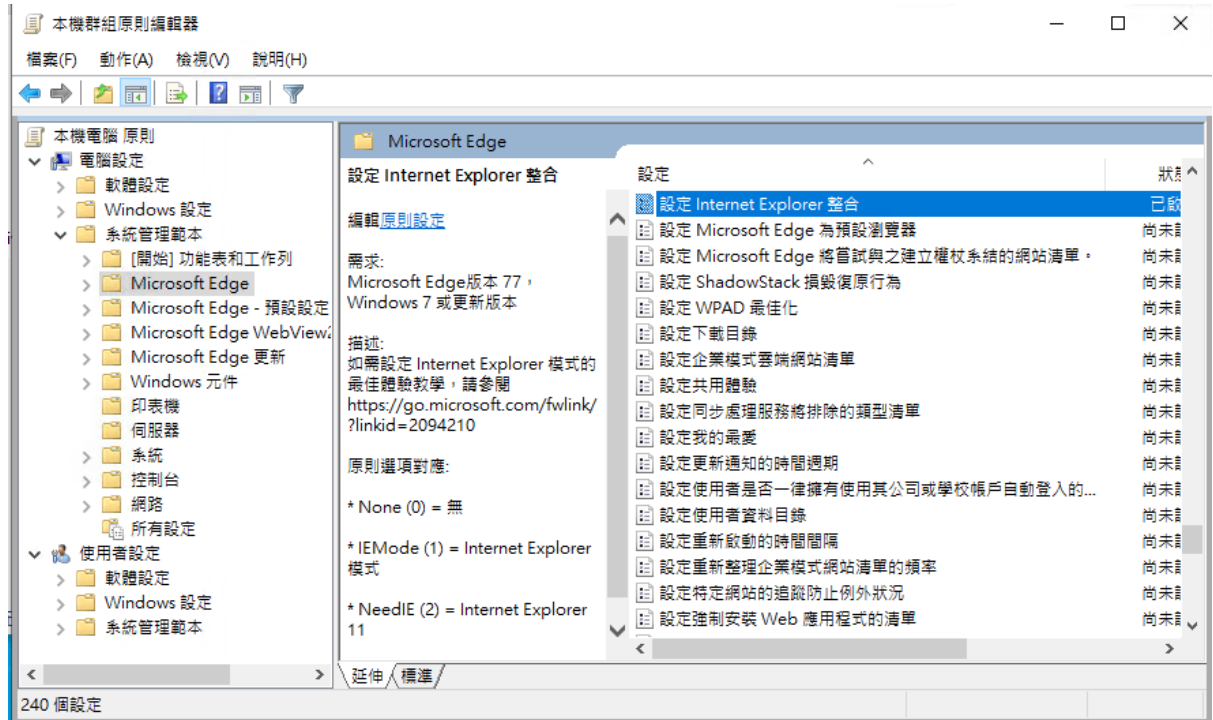
10. Browse to “Computer Configuration” > “Administrative Templates” > “Microsoft Edge”



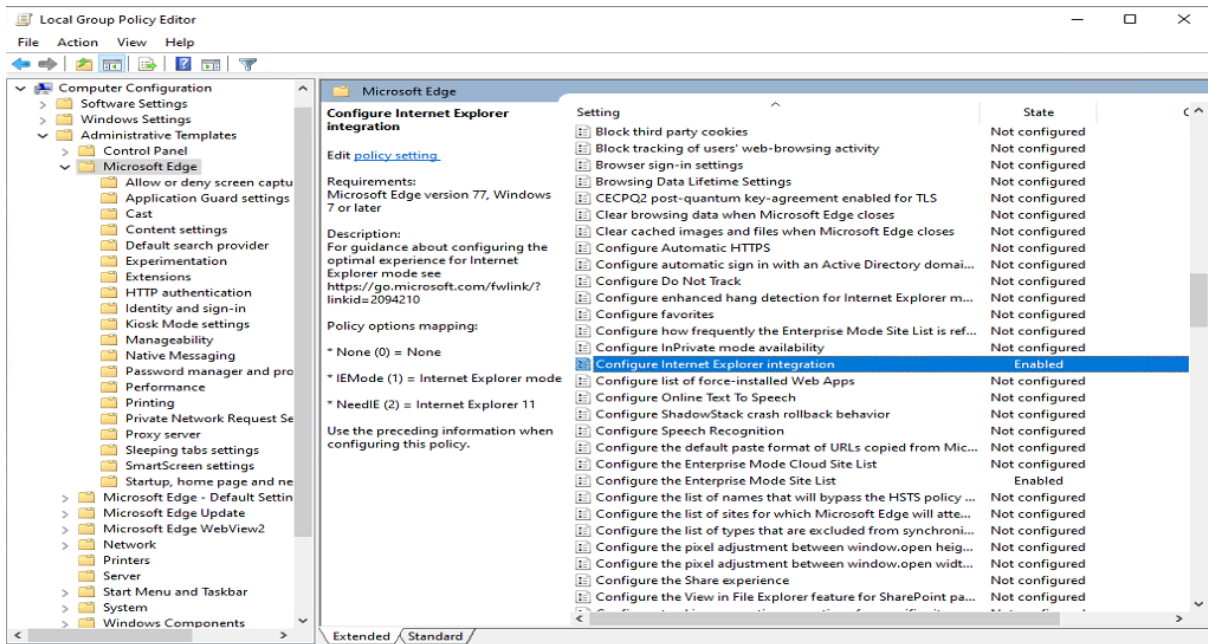
- 11. Change Setting “Configure Internet Explorer Integration”
- 12. Select “**Enable**” and, in Options section, select “**Internet Explorer mode**” in the drop down box

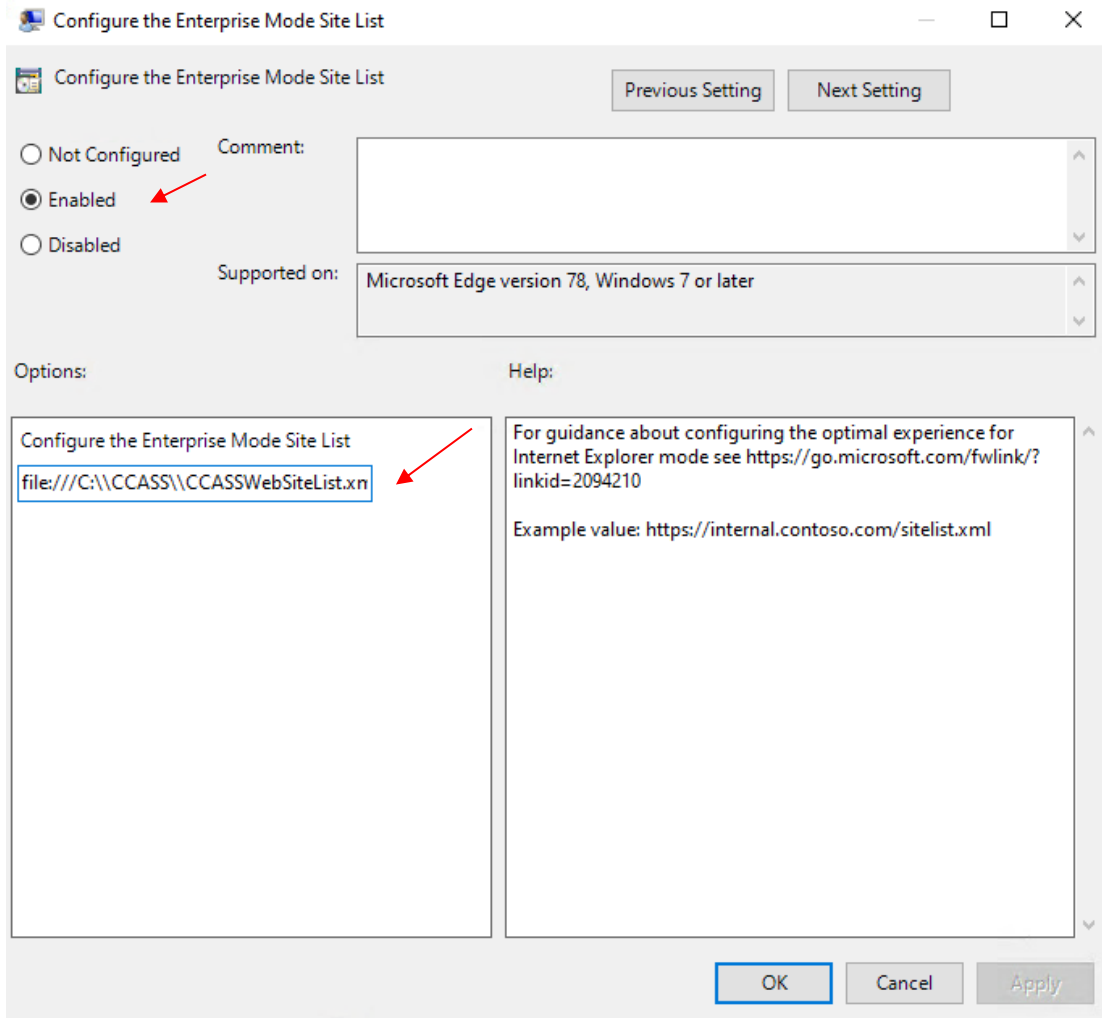


For Chinese Windows OS:

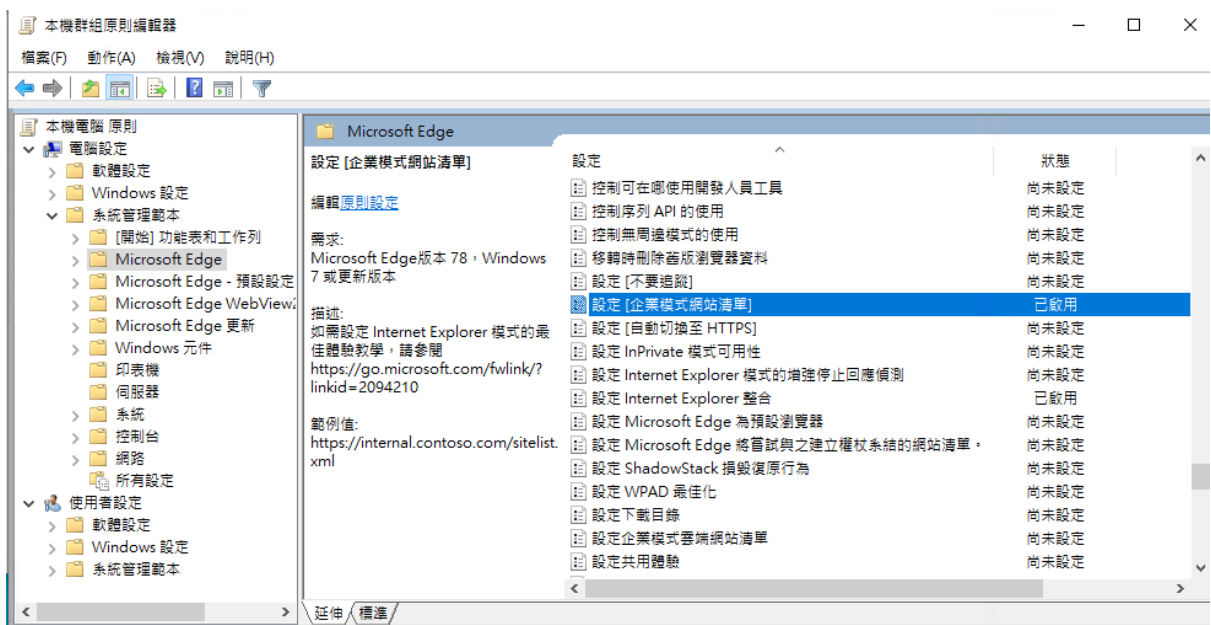


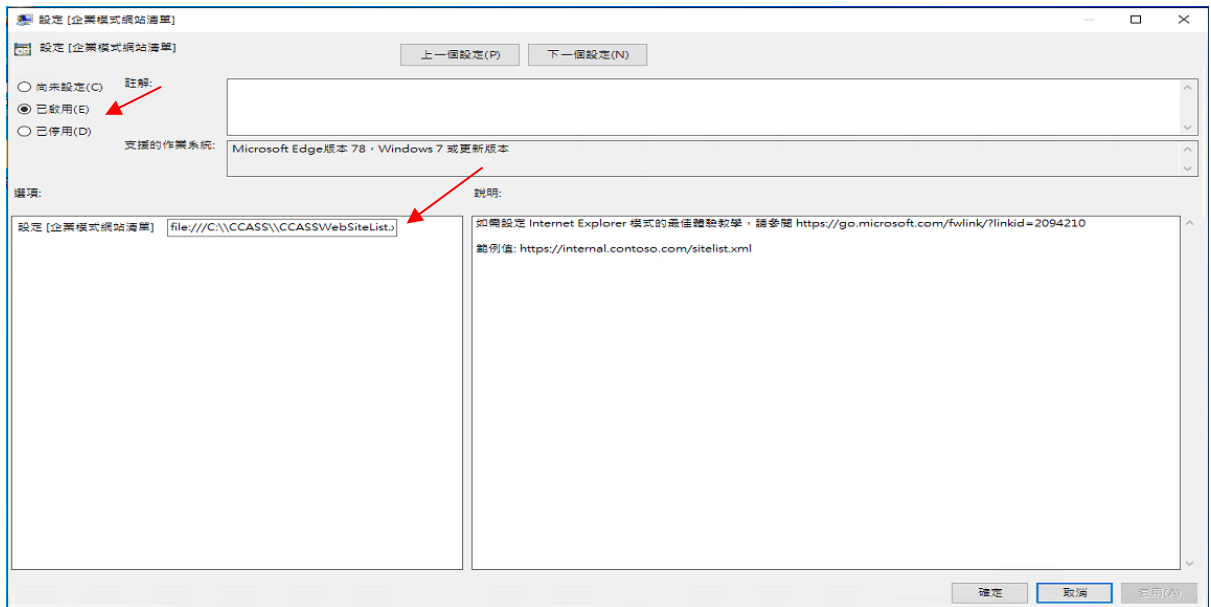
13. Click OK to save
14. Change Setting “Configure the Enterprise Mode Site List”
15. Select “**Enable**” and, in Options section, input Enterprise Mode Site List as “file:///C:\\CCASS\\CCASSWebSiteList.xml”





For Chinese Windows OS:

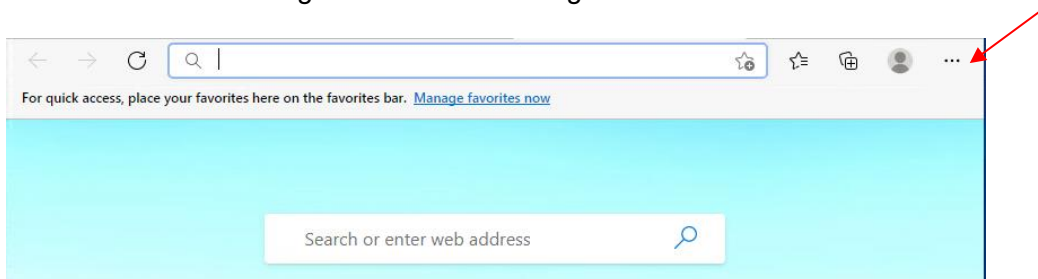




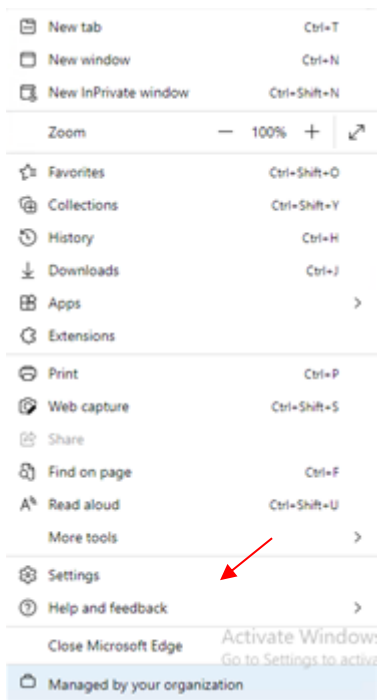
16. Click OK to save

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



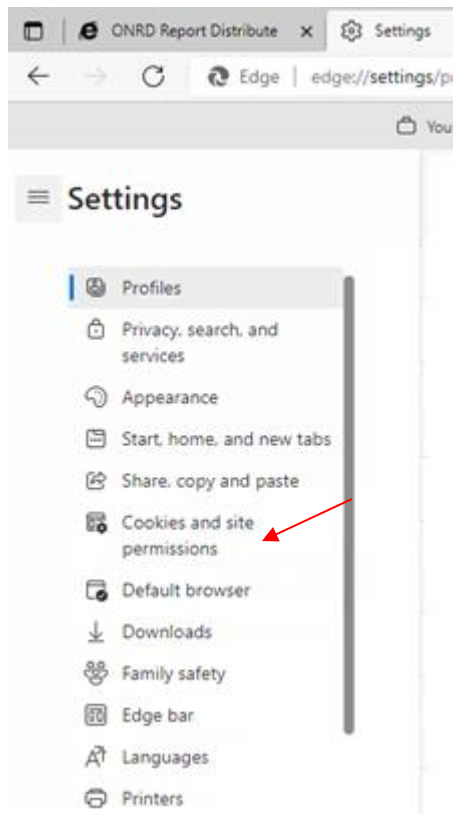
b. Go to Settings



For Chinese Windows OS:



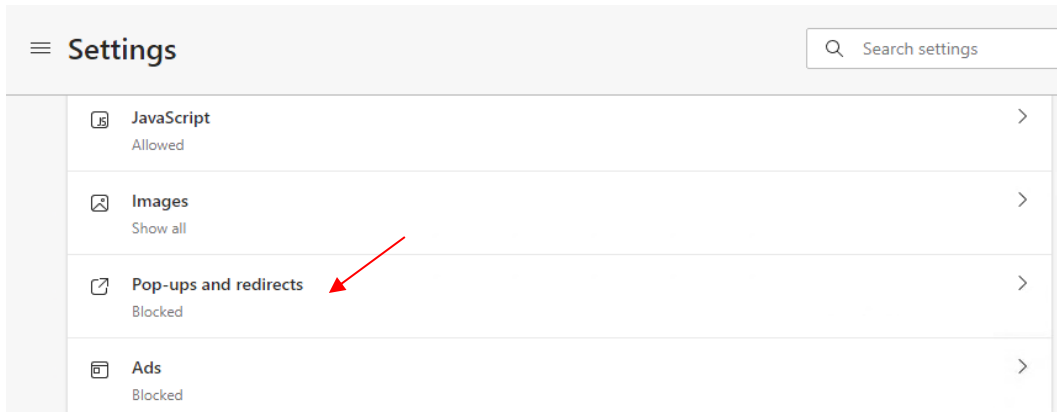
c. Click “Cookies and site permissions”



For Chinese Windows OS:



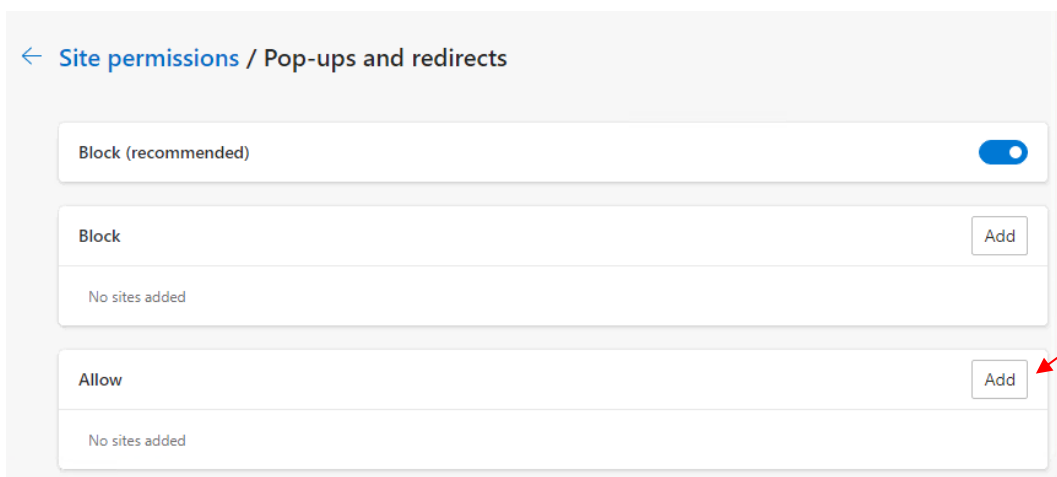
d. Go to “Pop-ups and redirects”



For Chinese Windows OS:



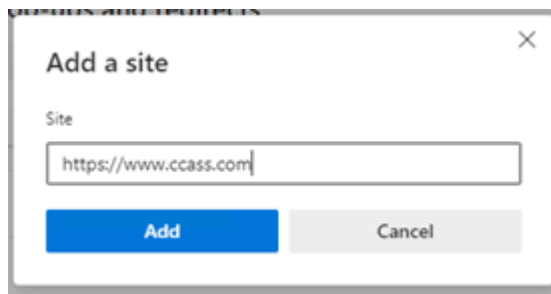
e. Go to “Allow” section and click “Add” button



For Chinese Windows OS:



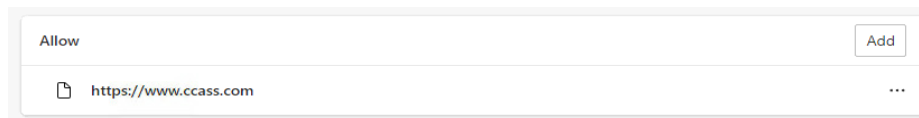
f. Input <https://www.ccass.com> and click “Add”



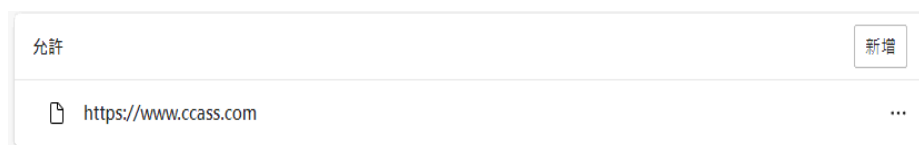
For Chinese Windows OS:



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



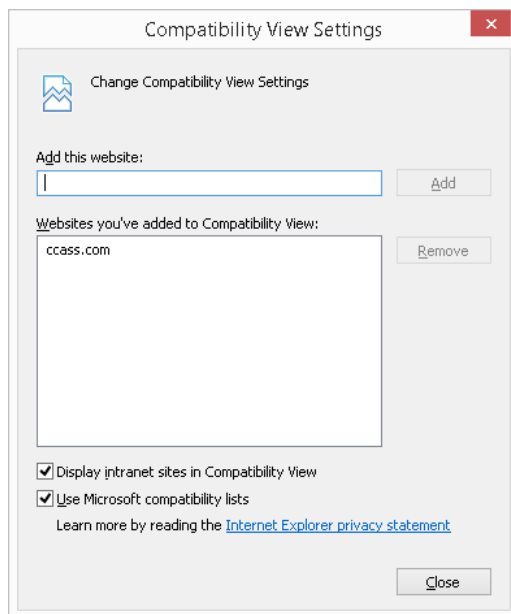
For Chinese Windows OS:



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

5.3 Compatibility View Settings (in Internet Explorer 11)

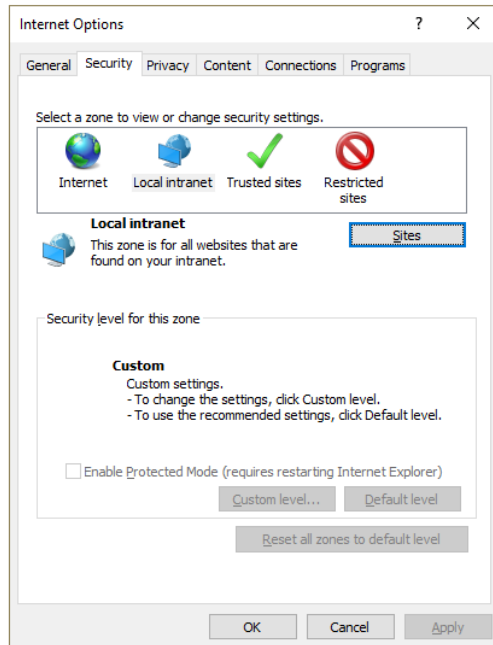
1. Open IE window, and then select “Tools” → “Compatibility View settings”.
2. Type www.ccass.com
3. Click “Add”, then “ccass.com” should be shown at the box “Websites you’ve added to Compatibility View:”



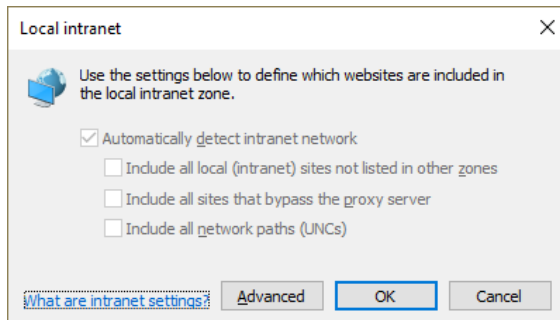
4. Click “Close” to close the window to complete the setting

5.4 Local Intranet Settings

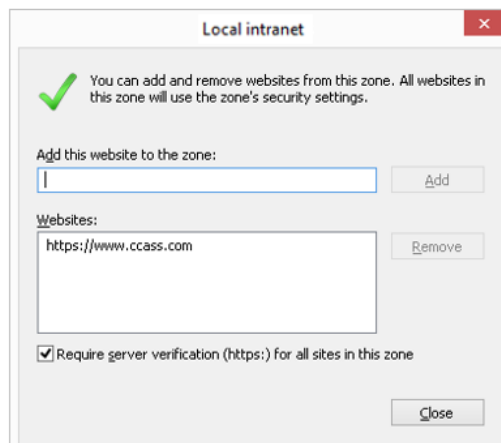
1. Go to “Control Panel” → “Internet options” and then click on “Security” tab.
2. Then click on “Local intranet” and click on “Sites”



3. Click “Advanced”.



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

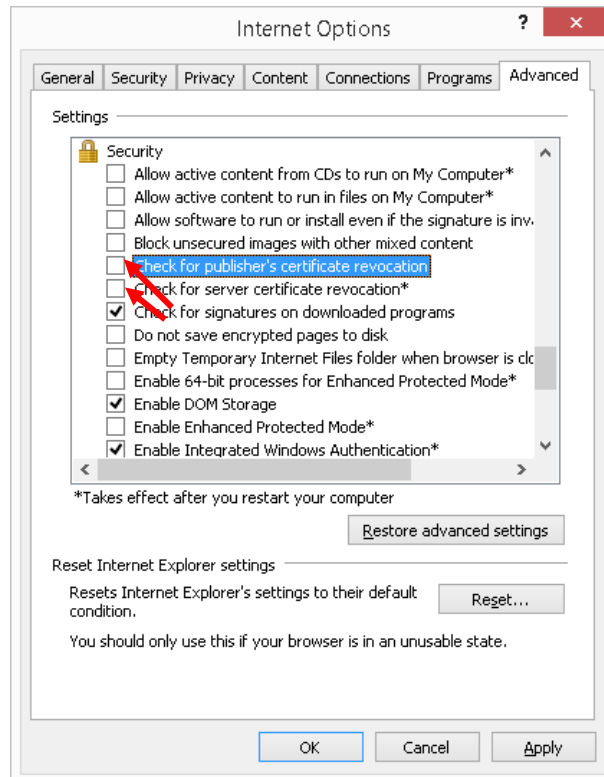


5. Click “Close” and then OK to close the window to complete the setting

5.5 Disable Certificate Revocation Check

It apply to standalone CCASS (CCMS) Terminal with no Internet connection.

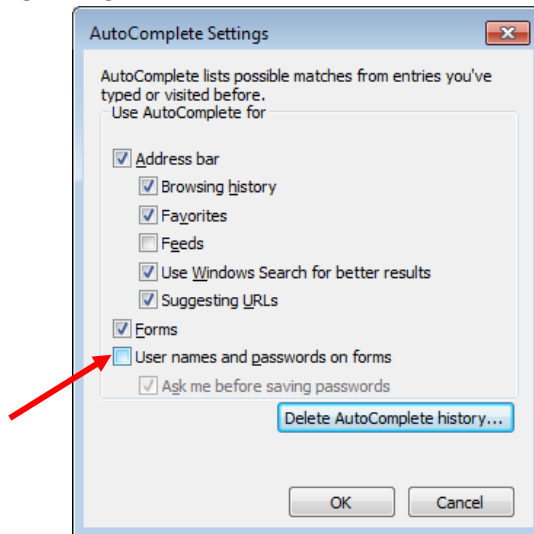
1. Go to “Control Panel” → “Internet options” and then click on “Advanced” tab.
2. Go to Security section and **uncheck** the following options
 - i. Check for publisher’s certificate revocation
 - ii. Check for server certificate revocation



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

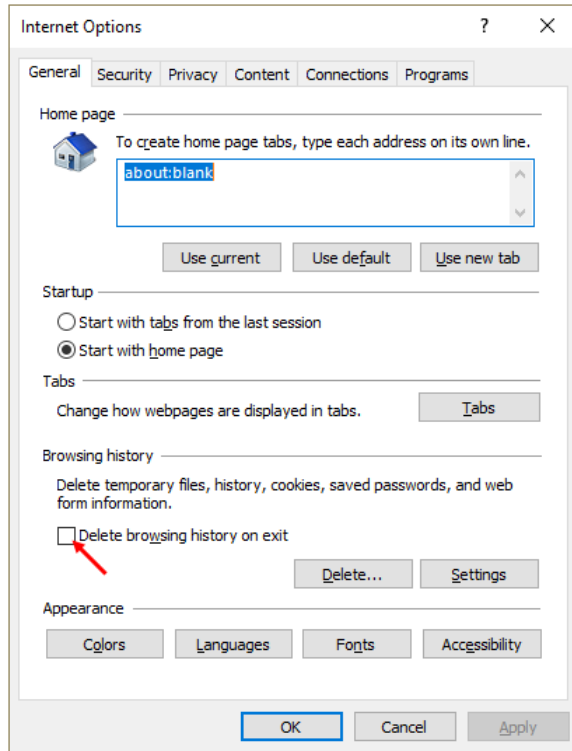
5.6 Disable AutoComplete for User Names and Passwords

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

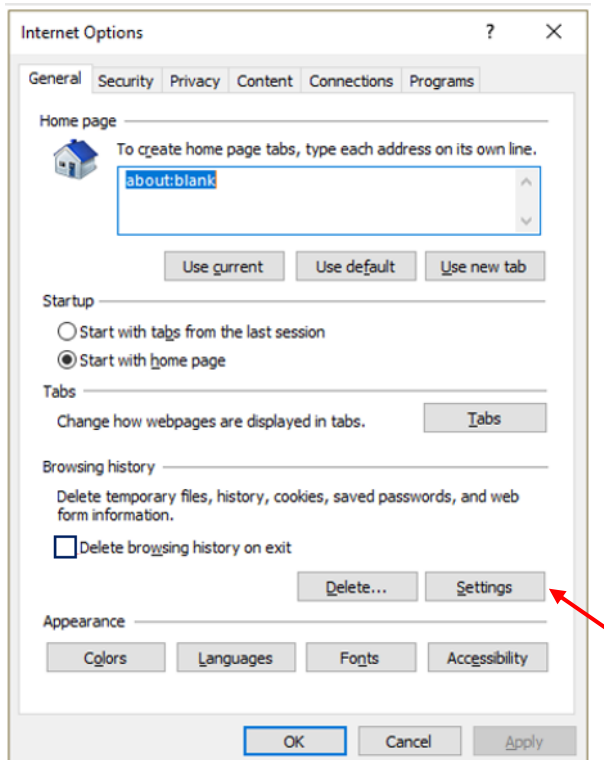


5.7 Browsing History

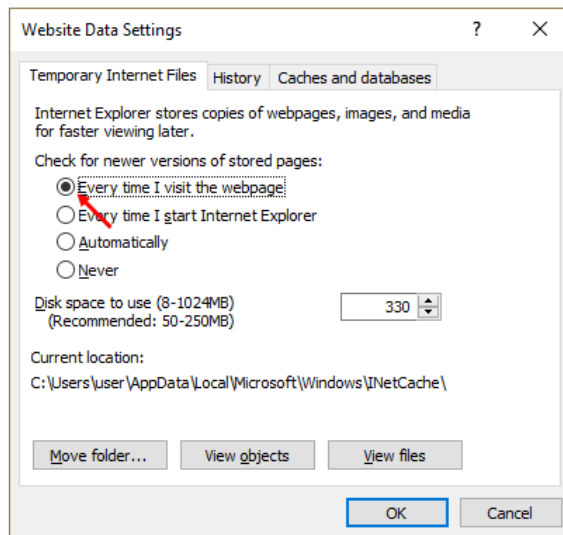
1. Go to “Control Panel” → “Internet options” and then go to “Browsing History”.
2. Ensure that the option “Delete browsing history on exit” is **not checked**



3. Then click on Settings

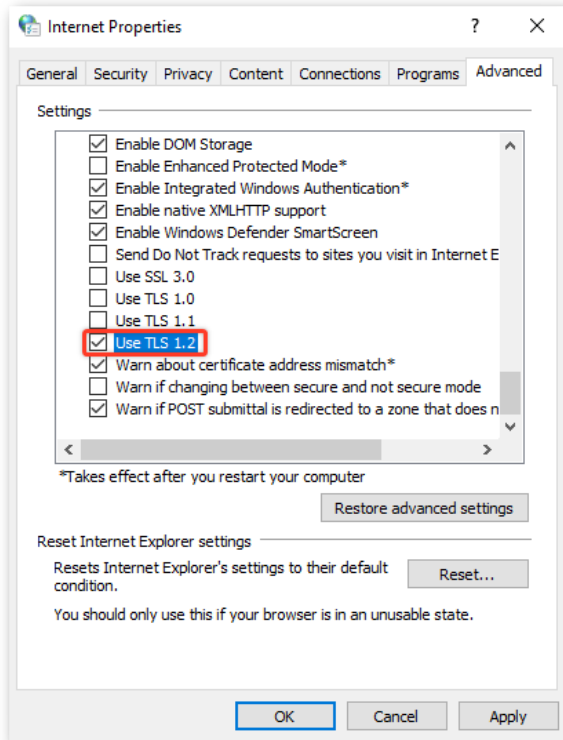


4. Ensure the option “Every time I visit the webpage” is **checked**



5.8 TLS Connection Settings

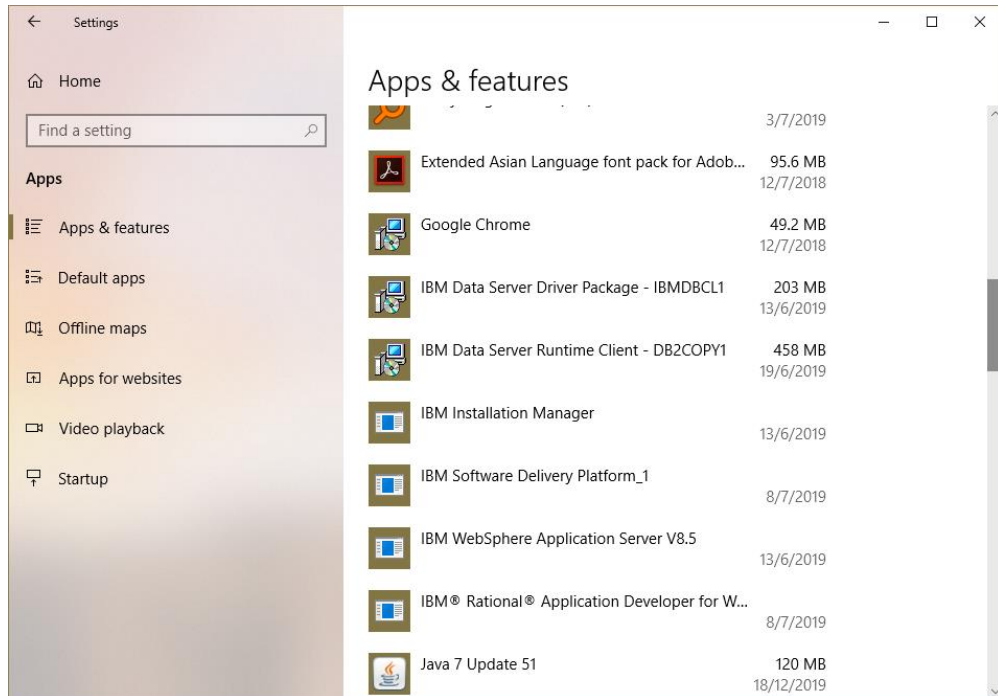
Only TLS 1.2 should be enabled while all other protocols should be disabled. Go to “Control Panel” → “Internet Options” → “Advanced” tab, and then scroll down to “Security” section. Check only TLS 1.2 and uncheck other SSL or TLS protocols.



5.9 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



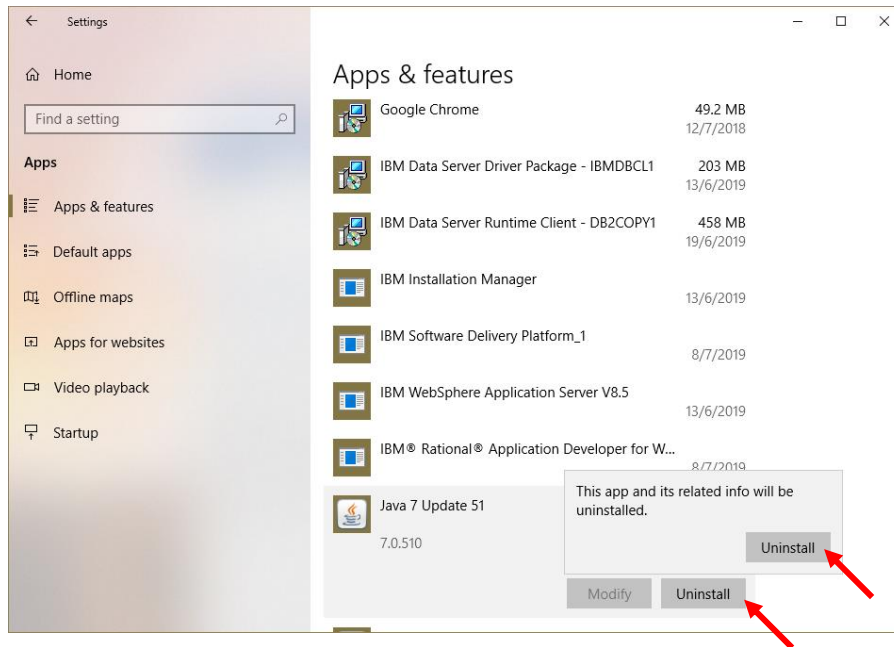
2. Find “Java X Update XX” in the list

- If non-supported JRE is found, please go to Section 5.10 for uninstallation
- If no JRE is found, please go to Section 5.11 for Java plugin installation

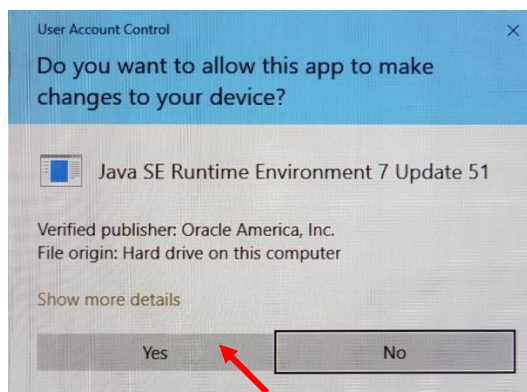
5.10 Uninstall Previous Java Plugin

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

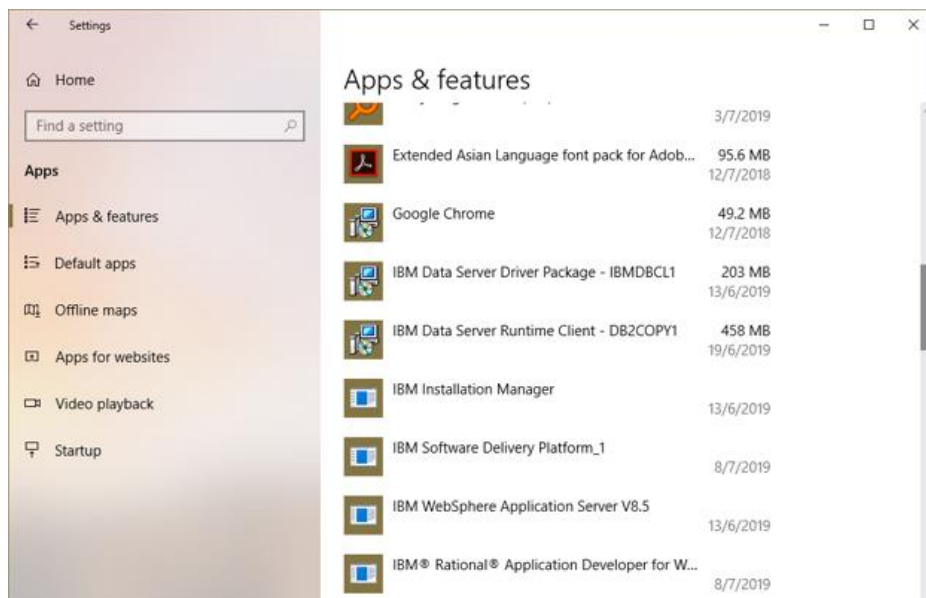
1. Go to “Uninstall a program” in Control Panel.
2. Ensure all Internet browser windows are closed.
3. Highlight the JRE item, and then click on the “Uninstall” button at the top. Click on “Uninstall” button for the alert “This app and its related info will be uninstalled” alert shows.



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



5. Check again that all JRE items should be removed



6. Restart the computer

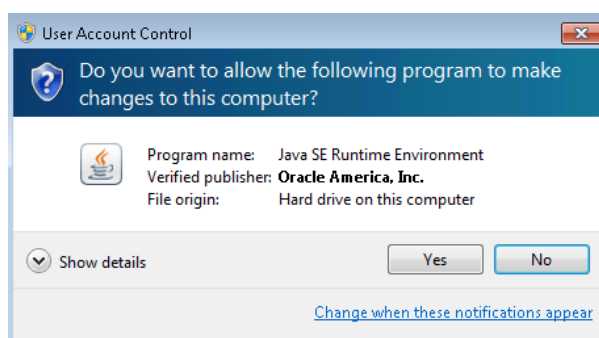
5.11 Java Plugin Installation

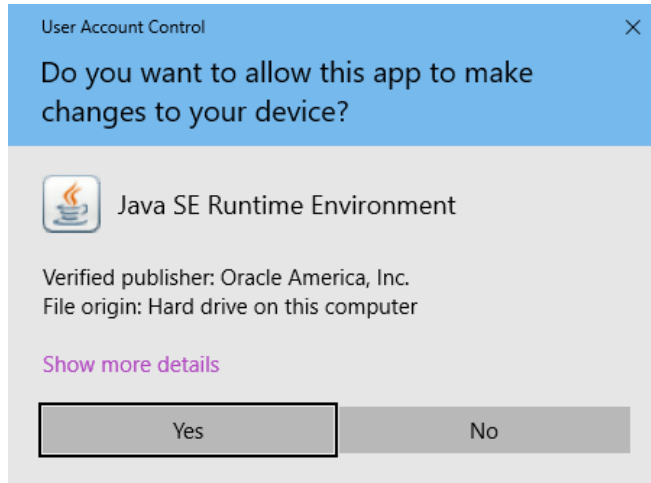
1. Ensure you have proper license subscription of Oracle Java, otherwise please refer to (<https://www.oracle.com/java/java-se-subscription.html>) about Oracle Java SE Desktop subscription.
2. Download the following two installers of Windows x86 and x64 version of Oracle Java SE Runtime Environment 8u341 from (<https://www.java.com/en/download/> or <https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html>).

jre-8u341-windows-i586.exe – for Windows x86

jre-8u341-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

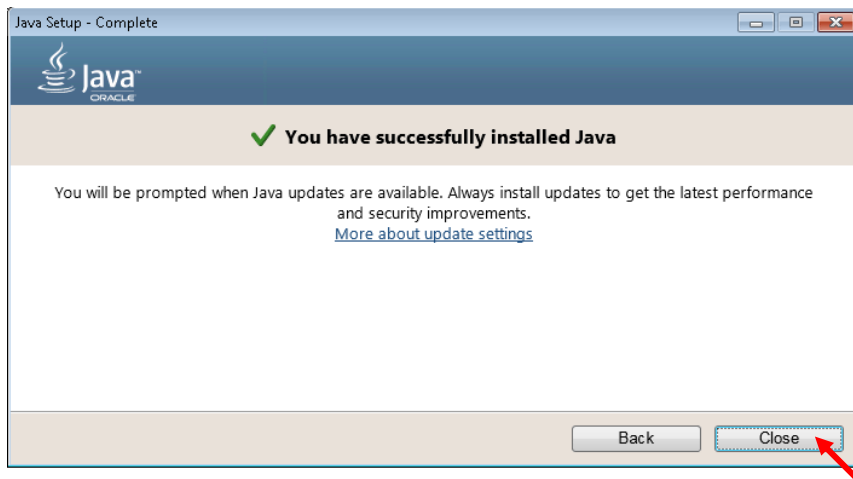




- 5. Ensure all Internet browser windows are closed.
- 6. Click "Install>"button to continue

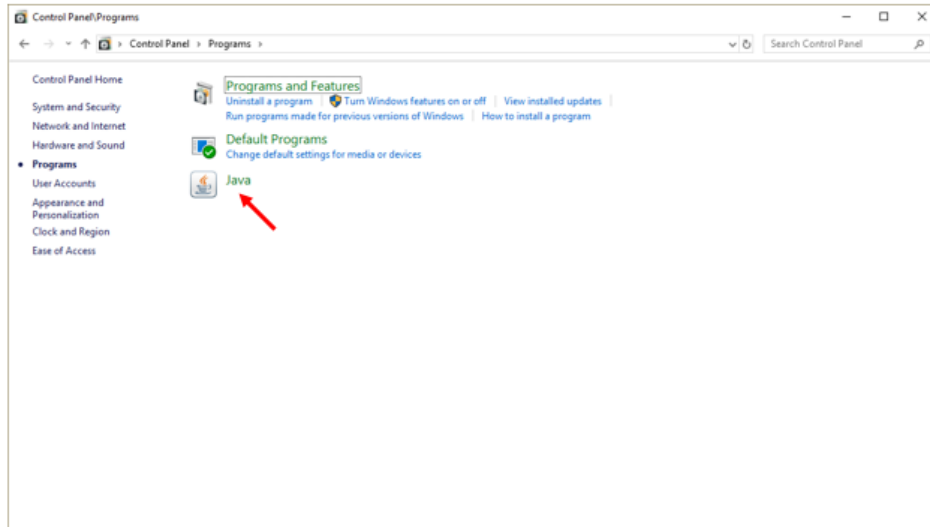


- 7. Wait for installation to complete and click "Close"

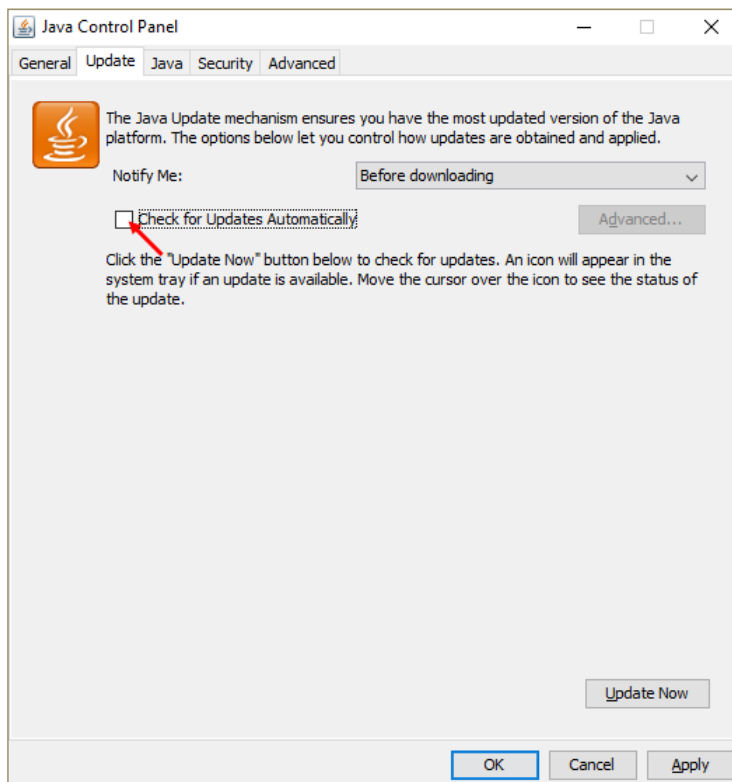


5.12 Java Plugin Configurations

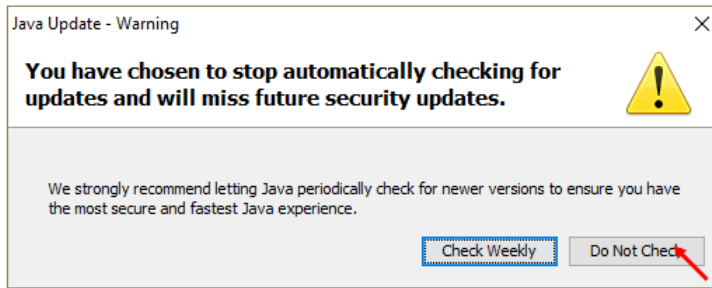
1. Auto update should be disabled. To do so, click “Start” to launch start menu then “Control Panel” and then click “Program” and then click “Java”



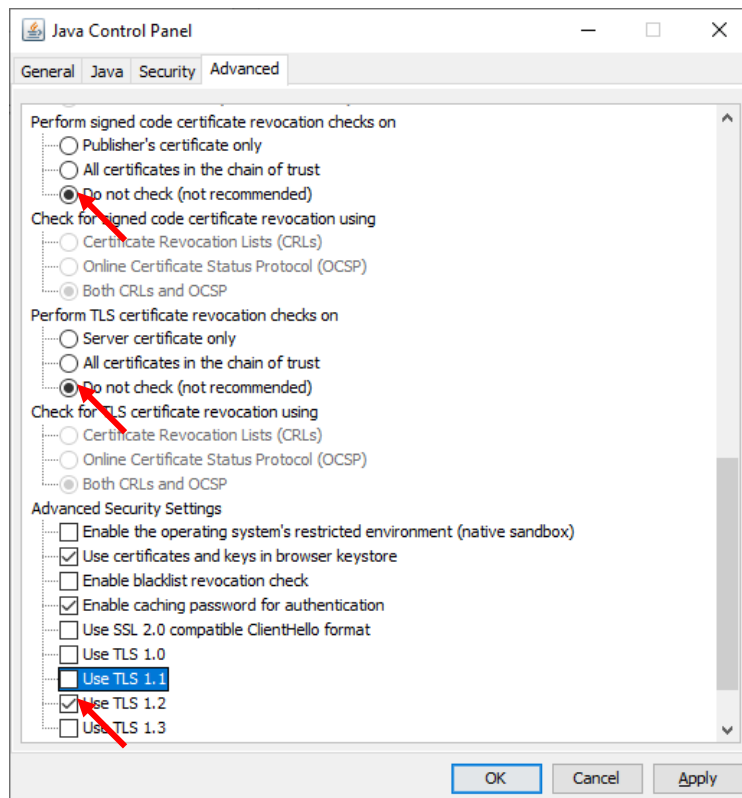
2. Select “Update” tab and uncheck “Check for Updates Automatically”.



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



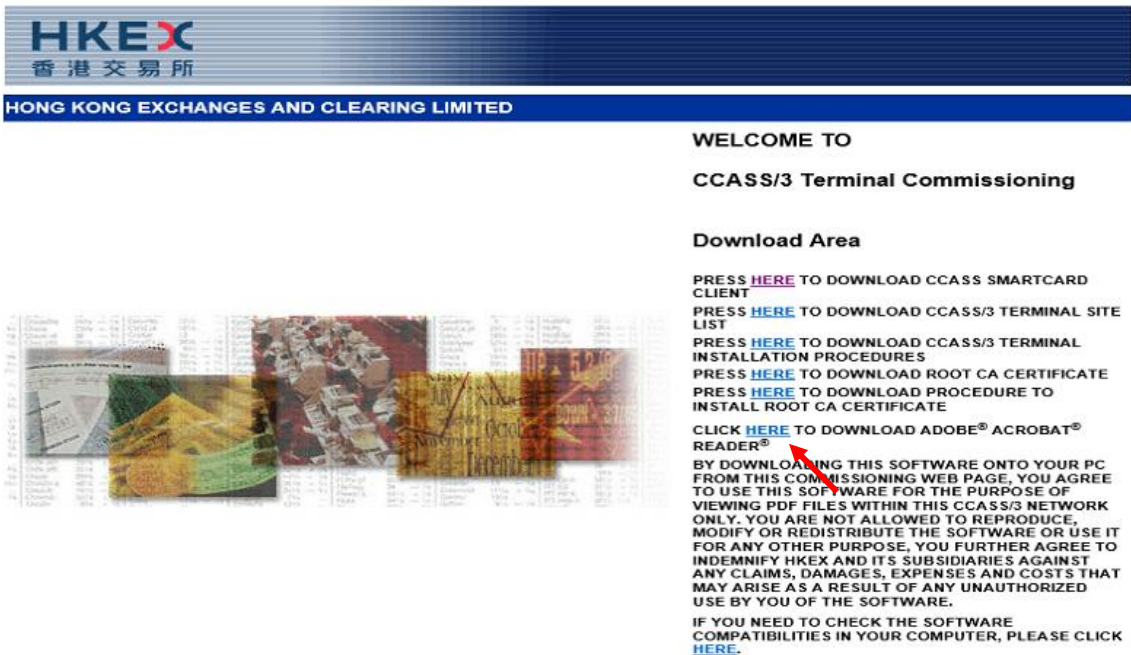
4. Click “Advanced” Tab and then scroll to the bottom.
5. Select the following settings in Advanced settings
 - a) Perform signed code certificate revocation checks on
Do not check
 - b) Perform TLS certificate revocation checks on
Do not check
 - c) Advanced Security Settings
Use TLS 1.2



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

5.13 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.



The screenshot shows the website header for HKEX (Hong Kong Exchanges and Clearing Limited). The main content area is titled "WELCOME TO CCASS/3 Terminal Commissioning". Under the "Download Area" section, there are several links labeled "HERE" for downloading various components. A red arrow points to the link for "ADOBE® ACROBAT® READER®". Below the links is a legal disclaimer and a link to check software compatibilities.

WELCOME TO
CCASS/3 Terminal Commissioning

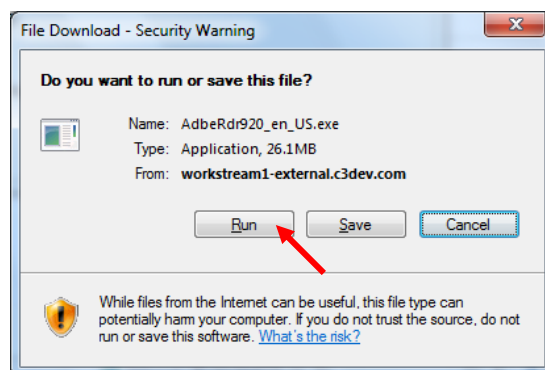
Download Area

PRESS [HERE](#) TO DOWNLOAD CCASS SMARTCARD CLIENT
 PRESS [HERE](#) TO DOWNLOAD CCASS/3 TERMINAL SITE LIST
 PRESS [HERE](#) TO DOWNLOAD CCASS/3 TERMINAL INSTALLATION PROCEDURES
 PRESS [HERE](#) TO DOWNLOAD ROOT CA CERTIFICATE
 PRESS [HERE](#) TO DOWNLOAD PROCEDURE TO INSTALL ROOT CA CERTIFICATE
 CLICK [HERE](#) TO DOWNLOAD ADOBE® ACROBAT® READER®

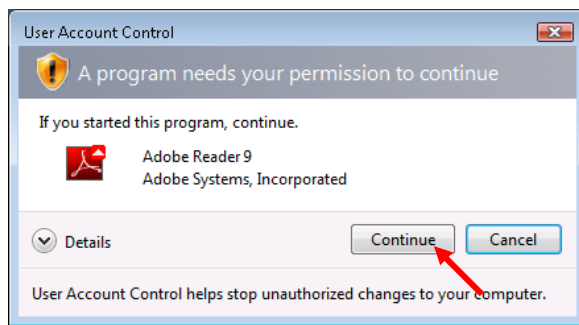
BY DOWNLOADING THIS SOFTWARE ONTO YOUR PC FROM THIS COMMISSIONING WEB PAGE, YOU AGREE TO USE THIS SOFTWARE FOR THE PURPOSE OF VIEWING PDF FILES WITHIN THIS CCASS/3 NETWORK ONLY. YOU ARE NOT ALLOWED TO REPRODUCE, MODIFY OR REDISTRIBUTE THE SOFTWARE OR USE IT FOR ANY OTHER PURPOSE. YOU FURTHER AGREE TO INDEMNIFY HKEX AND ITS SUBSIDIARIES AGAINST ANY CLAIMS, DAMAGES, EXPENSES AND COSTS THAT MAY ARISE AS A RESULT OF ANY UNAUTHORIZED USE BY YOU OF THE SOFTWARE.

IF YOU NEED TO CHECK THE SOFTWARE COMPATIBILITIES IN YOUR COMPUTER, PLEASE CLICK [HERE](#).

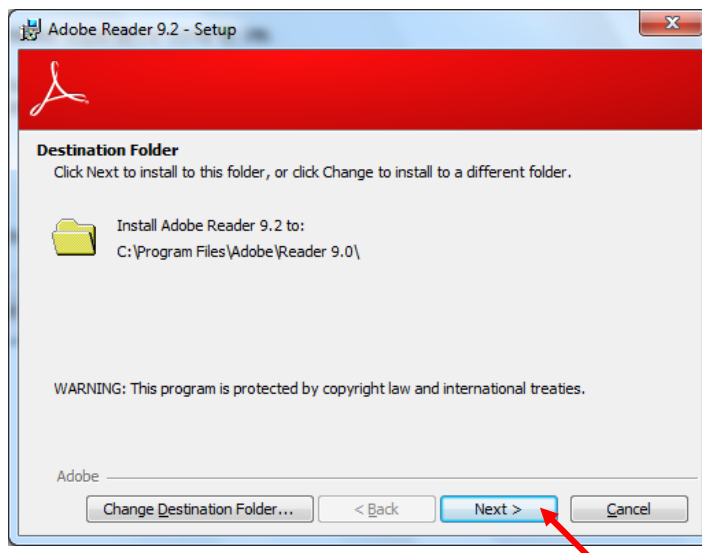
2. Click “Run” or “Open” button and wait for installation starting after the file to be downloaded to the PC



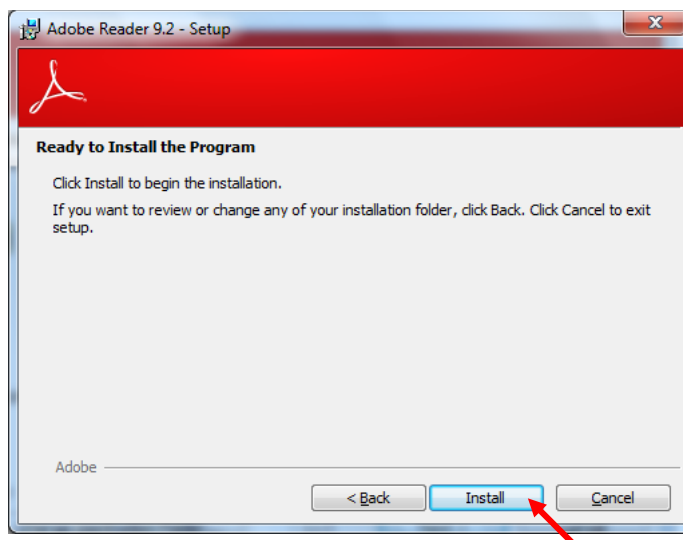
3. Click "Continue" button to continue and start to install Acrobat Reader



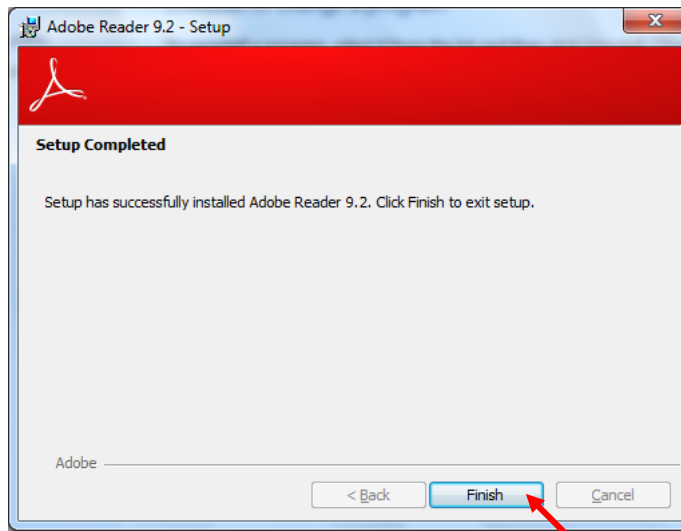
4. Click "Next" to proceed installation in default settings



5. Click "Install" to start installation



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



-- END --