HKSCC CCASS/ VaR Online/ RAP Installation Procedures

Version:	7.1
Date:	March 2025

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
4.0	Aug 2022	HKSCC	• Updated support of Google Chrome version for VaR Online • Remove support of Internet Explorer 11
5.0	Mar 2023	HKSCC	To prepare for launch of 2FA for CCASS Terminal • Section 4.7 for CCASS and add Section 4.9 • Installation of Smartcard reader and Smartcard Client software will not be required after 2FA enablement • Updated support of Google Chrome version for VaR Online
6.0	Jul 2023	HKSCC	After 2FA enablement, the requirement of Smartcard reader and Smartcard Client software and their installation procedures are removed.
7.0	Apr 2024	HKSCC	Updated support of Google Chrome version for VaR Online
7.1	Mar 2025	HKSCC	Rename to HKSCC CCASS/VaR Online/RAP Installation Procedures Support Windows 11 for CCASS Terminal and VaR Online and update PC requirements Add CCASS/CCMS report access for Participants and DBs to RAP

TABLE OF CONTENTS

1 OVERVIEW

1.1 Background

This document serves as a CCASS technical guide for HKSCC's Participants other than Investor Participants ("Participants") and Designated Banks (DBs) to install and configure their PC terminals to access CCASS via SDNet. Section 2 provides a summary of system requirements, while sections 3 & 4 documented the communication line & network setup requirement.

HKSCC Participants and DBs should refer to Section 5 for the hardware, software requirements and configuration for installing CCASS Terminals and should also access to Report Access Platform (RAP) for CCASS, CCMS and risk-related[1] reports. Respective requirements are documented in Section 6.

HKSCC Participants should also access to VaR Online for margin & stress test simulation purposes. Respective requirements are documented in Section 7.

[1] CCMS and risk-related reports are not applicable to DBs

2 System Requirements

2.1 PC Configuration Requirements

Highlighted below are the minimum PC configurations for CCASS Terminals and VaR Online (not applicable to DBs). There is no minimum PC configuration requirements for RAP.

Item	CCASS	VaR Online
CPU	1GHz	2.4GHz
Memory	4GB	8GB
Harddisk	64GB	64GB
Operating System	Win 11 Pro (64 bit)[2]	Win 11 Pro (64 bit)
Browser	MS Edge[3] version 94 or above	Google Chrome[4]
Java Plugin[5]	Oracle JRE 8u441[6] (both x86 and x64)	N/A
Software	• Anti-virus	• Anti-virus
Bandwidth[7]	1Mbps	1Mbps

[2] Existing *Windows 10 Pro version will be supported until Microsoft ends it support by October 14, 2025*

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

[4] *Please install Google Chrome version 130.0.6723.117 for VaR Online. The version for VaR Online will in general be aligned with HKATS*

[5] Java Plugin will become optional after CCASS/CCMS reports are available for download via RAP from mid-July 2025. It is only required for downloading CCASS/CCMS reports from CCASS Terminal Report Download function. JRE is not required for downloading CCASS/CCMS reports via RAP.

[6] *One needs proper license subscription to download Oracle JRE 8u441. 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 8u441 from (https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html).*

[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 (not applicable to DBs) to protect it from computer virus or worms attacks. Participants and DBs 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' and DBs' 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 and DBs 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 and DBs 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 and DBs are also advised to regularly review the latest Microsoft security patches and install them on their dedicated PCs accordingly. CPs and DBs 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 and DBs 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:

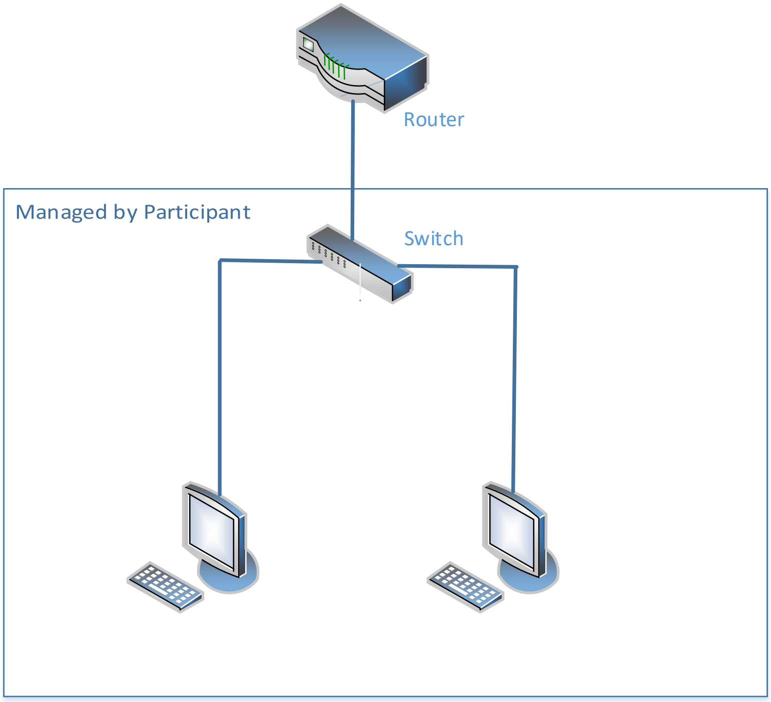
Participants and DBs must not perform any unauthorized access or security scanning (no matter at network, system or application level) on HKEX systems and any related network device not owned by them. Any such attempt will be regarded as illegal access or malicious intrusion and their access to HKEX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

3 Communication Line Setup

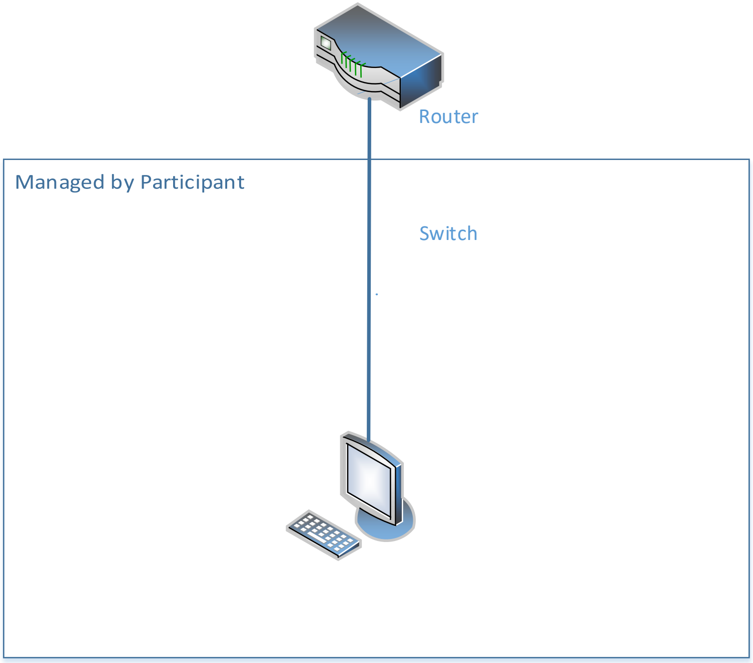
3.1 Connect PC Terminal with Router

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.

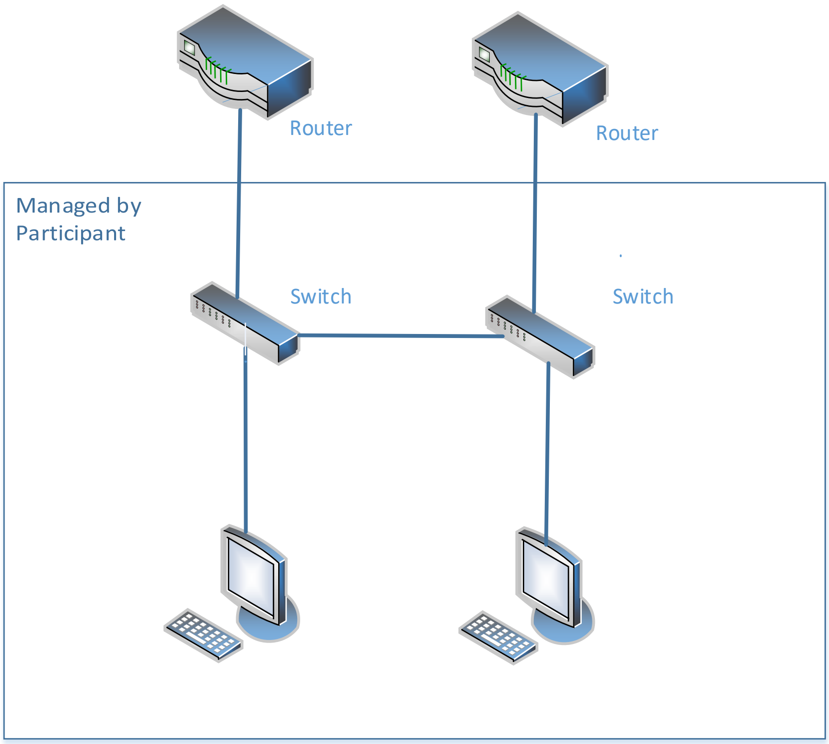
Option 1: Single Link Connection



Option 2: Single Link Connection with Direct Connection to Router



Option 3: Dual Link Connection



To maintain robustness, Participants and DBs 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 (not applicable to DBs); please follow procedures below for the PC setup.

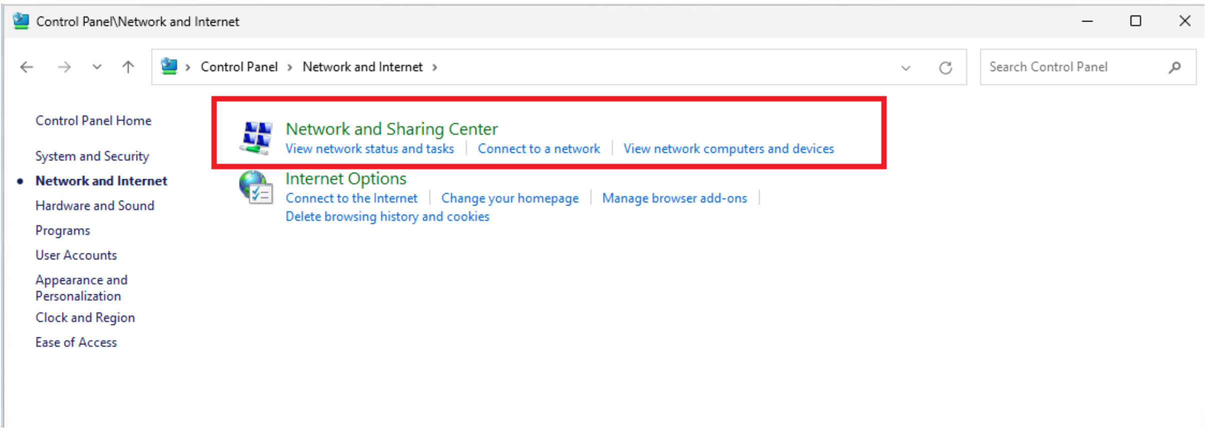
4.1 Windows IP address Configurations

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.

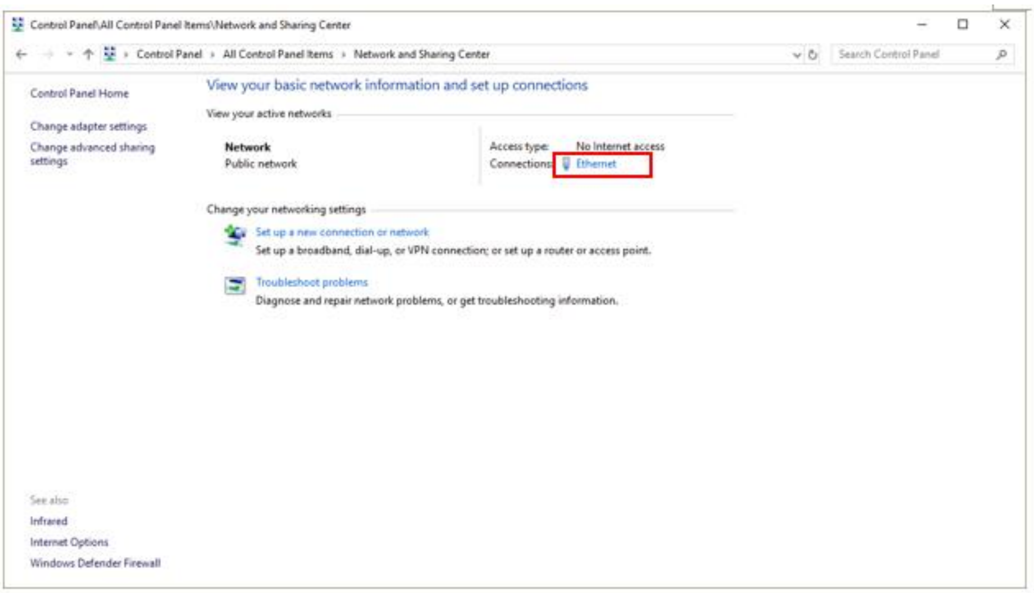
2. Click “Search” and input “Control Panel”

3. Select “Control Panel”

4. Click on "Network and Sharing Centre"


Control Panel\Network and Internet
Control Panel › Network and Internet ›
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Internet Options
Connect to the Internet | Change your homepage | Manage browser add-ons |
Delete browsing history and cookies

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


Control Panel\All Control Panel Items\Network and Sharing Center
Control Panel › All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Infrared
Internet Options
Windows Defender Firewall

View your basic network information and set up connections

View your active networks

Network
Public network

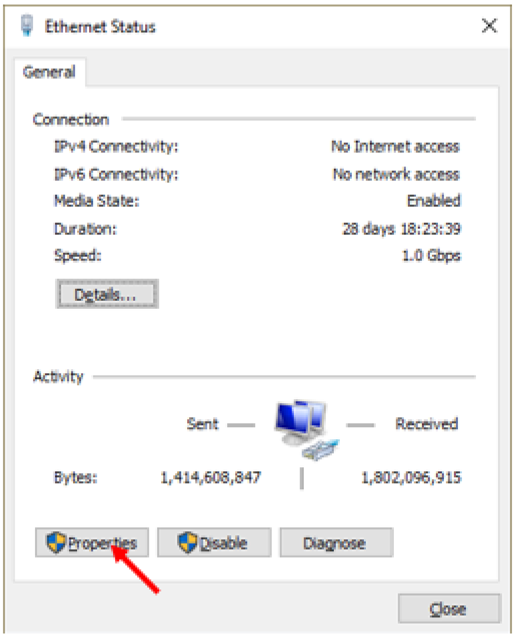
Access type: No Internet access
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

6. Click “Properties”



Connection

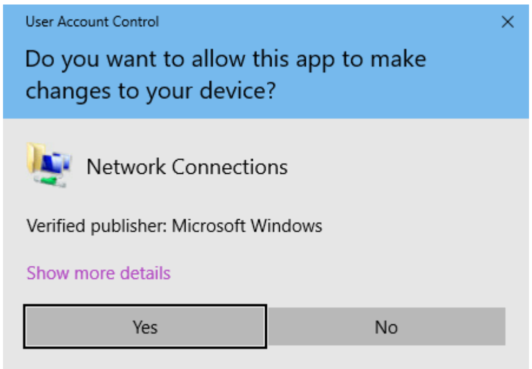
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 28 days 18:23:39
Speed: 1.0 Gbps

Activity

Sent — Received

Bytes: 1,414,608,847 | 1,802,096,915

7. Click “Yes” in for alert message.



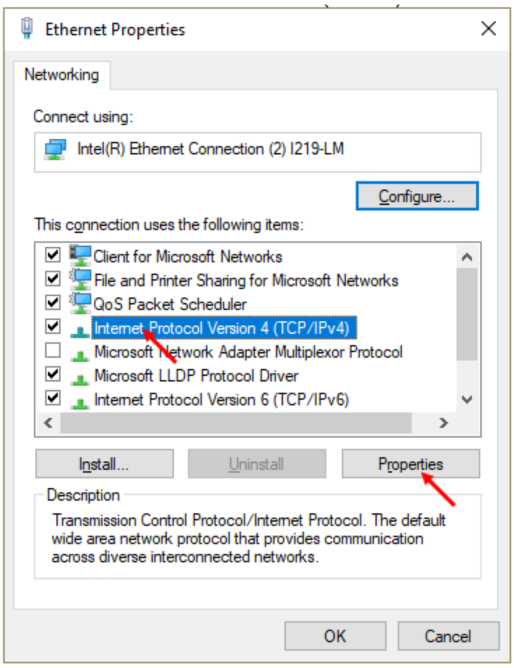
User Account Control

Do you want to allow this app to make changes to your device?

Network Connections

Verified publisher: Microsoft Windows

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



Ethernet Properties

Networking

Connect using:

Intel(R) Ethernet Connection (2) I219-LM

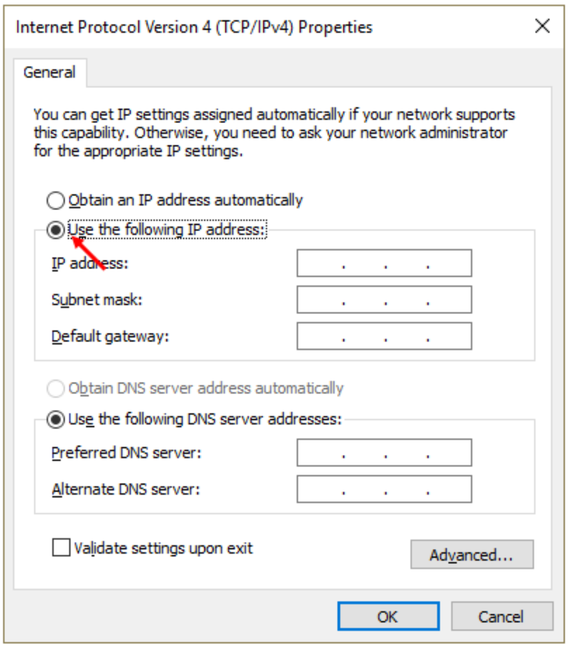
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

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
3. VaR DA Platform – https://idm.hkexposttrade.com.hk/user-management/

4.3 Disaster Recovery

During Disaster Recovery (DR) failover, Participants and DBs 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.

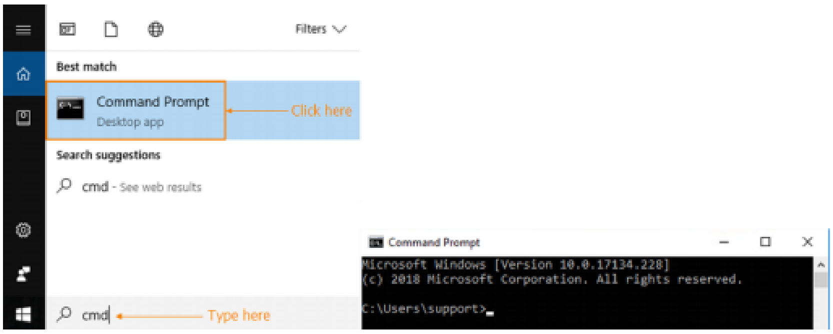
4.4 Source IP Address

Each SDNet circuit is assigned with a pre-defined range of IP addresses. Participants and DBs 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, CPs and DBs 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

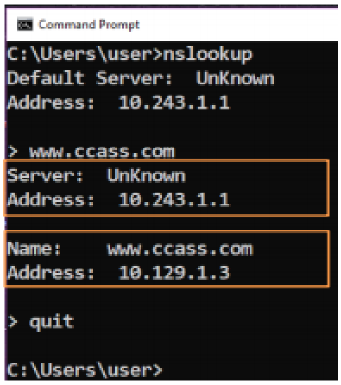
Please follow steps below to verify your DNS settings after completion of DNS setup (section 4.2).

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



```
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\support>_
```

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



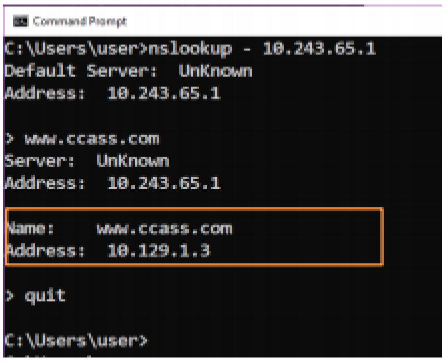
```
C:\Users\user>nslookup
Default Server:  UnKnown
Address:  10.243.1.1

> www.ccass.com
Server:  UnKnown
Address:  10.243.1.1

Name:    www.ccass.com
Address:  10.129.1.3

> quit

C:\Users\user>
```

DNS Address should be 10.243.1.1

The IP address of "www.ccass.com" should be resolved as "10.129.x.3", where x can be 1, 2, 3 or 4

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



```
C:\Users\user>nslookup - 10.243.65.1
Default Server:  UnKnown
Address:  10.243.65.1

> www.ccass.com
Server:  UnKnown
Address:  10.243.65.1

Name:    www.ccass.com
Address:  10.129.1.3

> quit

C:\Users\user>
```

The same IP address of www.ccass.com in step 3 should be returned

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 and VaR Online 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 and DBs 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[8] www.ccass.com	TCP: 441, 442, 443	CCASS Web[9] (PR & DR)

[8] *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.*

[9] *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*

HTTPS	10.243.2.15 sso.hkexposttrade.com.hk	TCP:443	CCASS 2FA Logon (PR)[10]
HTTPS	10.243.66.15 sso.hkexposttrade.com.hk	TCP:443	CCASS 2FA Logon (DR)

VaR Online (not applicable to DBs):

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)

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 and DBs 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 CPs' and DBs' 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

[10] *Participants and DBs will be redirected to CCASS 2FA Logon for authentication and then switch back to CCASS Online functions or Security Management functions automatically.*

[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.*

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. CCASS 2FA Logon
c. VaR Online (not applicable to DBs)
d. VaR Logon and DA Platform (not applicable to DBs)

The manual changes is be prone to error and is not recommended. Participants and DBs 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 and DBs 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.

- **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 5.1** to **Section 5.8** below

- **Java Plugin**[13]: 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.

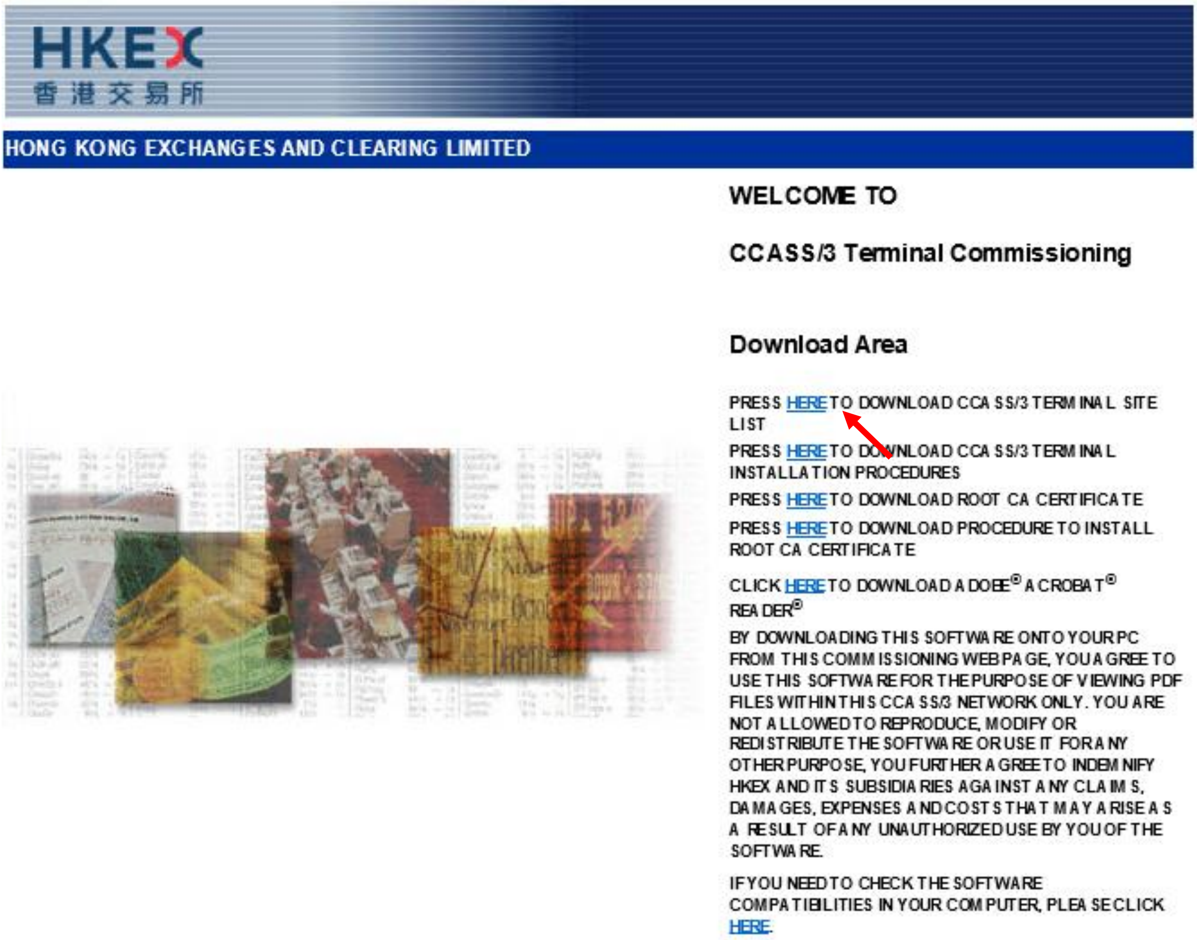
5.1 Internet browser Settings

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

[13] Java Plugin will become optional after CCASS/CCMS reports are available for download via RAP in July 2025. It is only required for downloading CCASS/CCMS reports from CCASS Terminal Report Download function. It is not required for downloading CCASS/CCMS reports via RAP



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

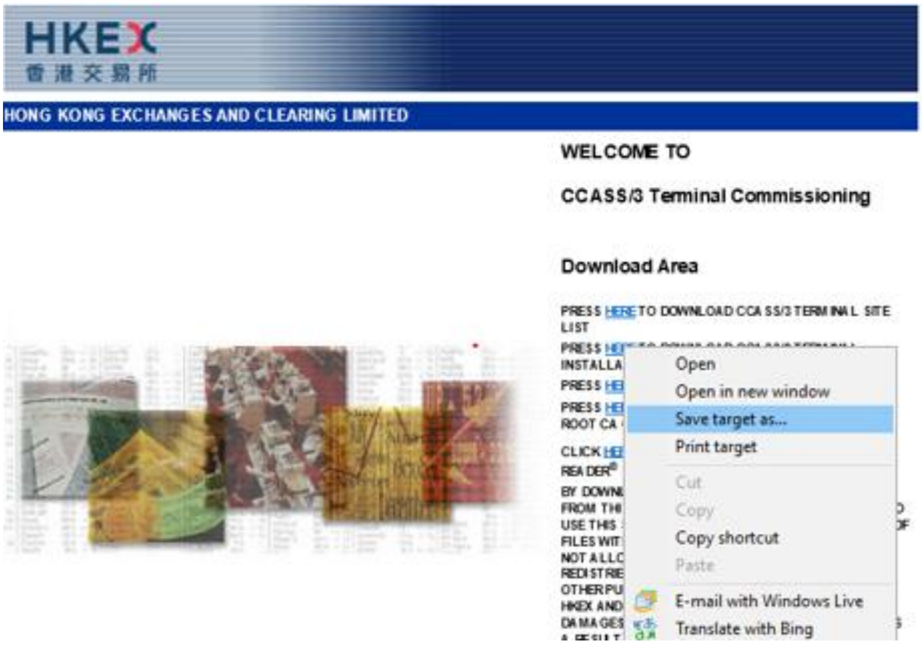
PRESS HERE TO DOWNLOAD PROCEDURE TO INSTALL ROOT CA CERTIFICATE

CLICK HERE TO DOWNLOAD ADOBE® ACROBAT® READER®

BY DOWNLOADING THIS SOFTWARE ONTO YOUR PC FROM THIS COMMISSIONING WEBPAGE, 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. Right click “HERE” on “PRESS HERE TO DOWNLOAD CCASS/3 TERMINAL SITE LIST, and select “Save target as…”



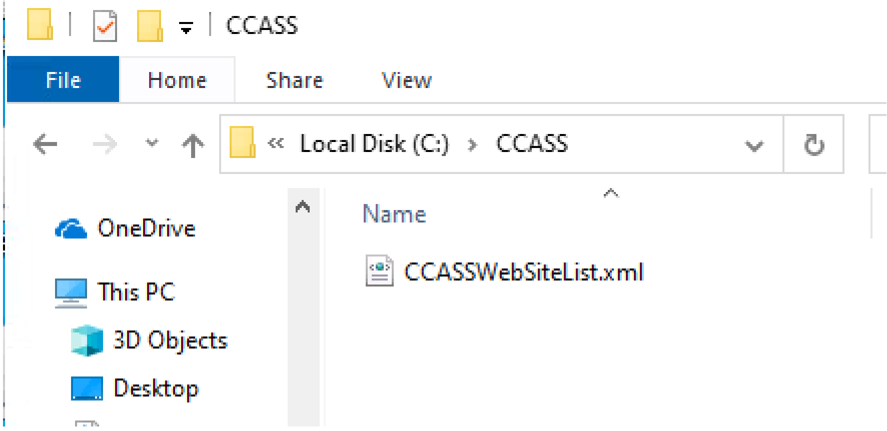
WELCOME TO

CCASS/3 Terminal Commissioning

Download Area

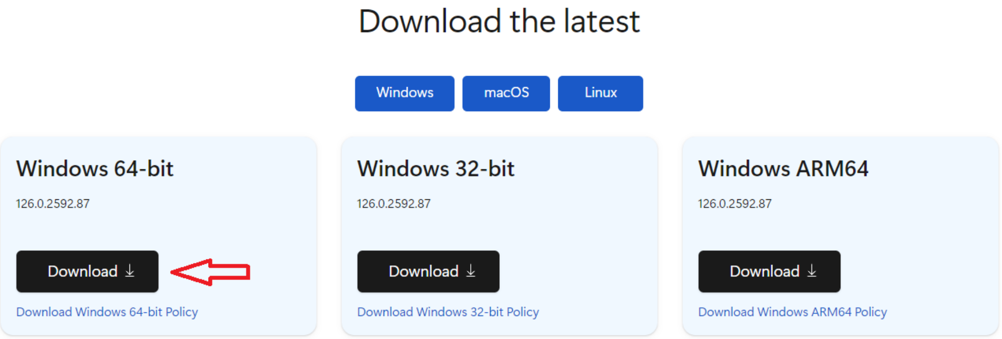
PRESS HERE TO DOWNLOAD CCASS/3 TERMINAL SITE LIST

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”



Download the latest

Windows 64-bit
126.0.2592.87

Download Windows 64-bit Policy

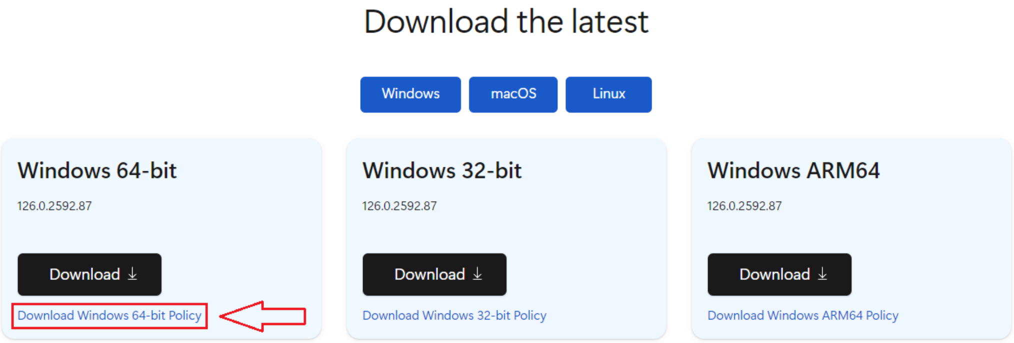
Windows 32-bit
126.0.2592.87

Download Windows 32-bit Policy

Windows ARM64
126.0.2592.87

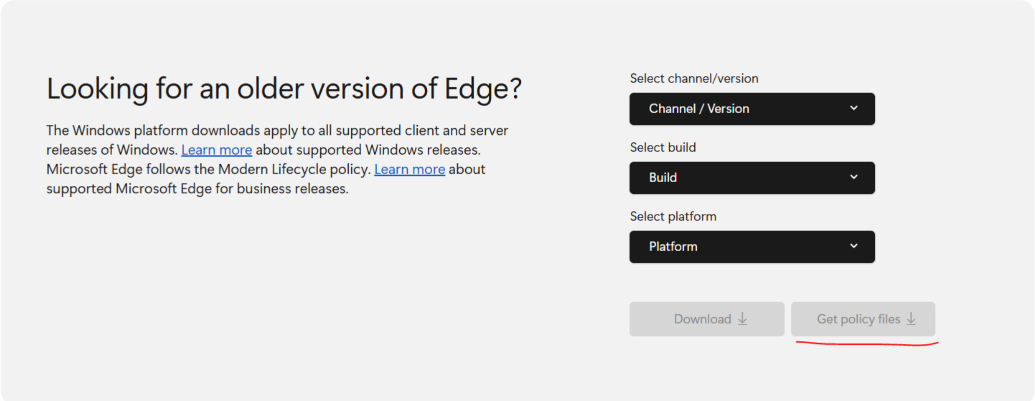
Download Windows ARM64 Policy

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



OR

Download edge Policy Files by selecting the Edge browser version (show as below)

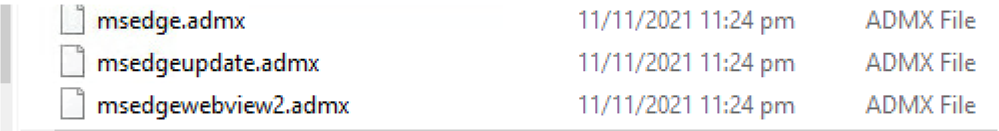


Looking for an older version of Edge?

The Windows platform downloads apply to all supported client and server releases of Windows. Learn more about supported Windows releases. Microsoft Edge follows the Modern Lifecycle policy. Learn more about supported Microsoft Edge for business releases.

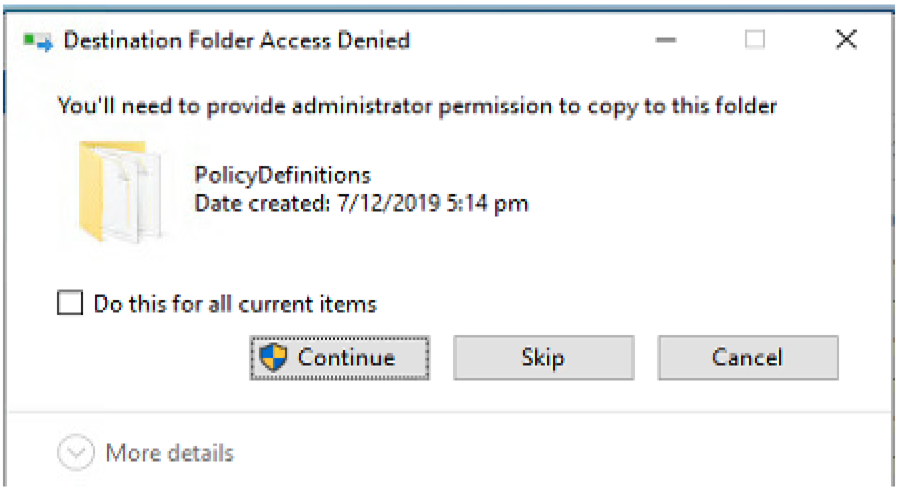
5. Unzip MS Edge policy files to a temporary folder (e.g. C:\TEMP\). To extract, double click the .cab file and extract the .zip to your location.

6. 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:



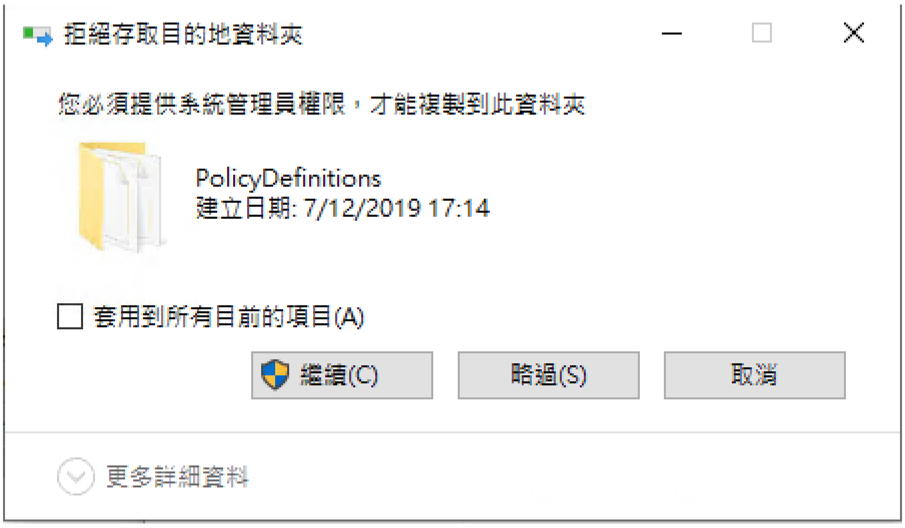
Destination Folder Access Denied

You'll need to provide administrator permission to copy to this folder

PolicyDefinitions
Date created: 7/12/2019 5:14 pm

□ Do this for all current items

For Chinese Windows OS:



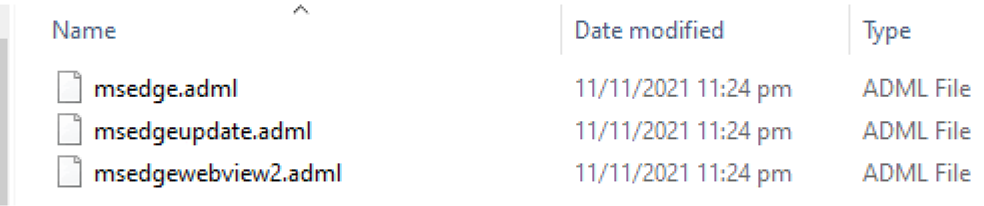
拒絕存取目的地資料夾

您必須提供系統管理員權限，才能複製到此資料夾

PolicyDefinitions
建立日期: 7/12/2019 17:14

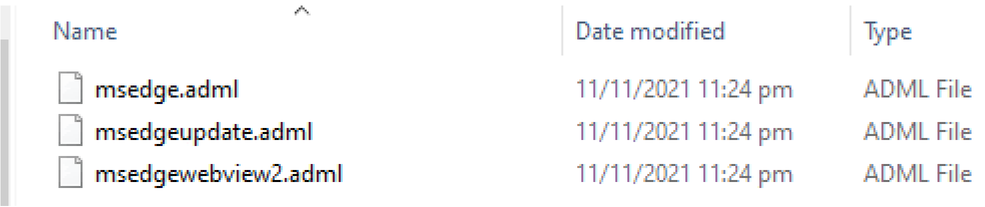
□ 套用到所有目前的項目(A)

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



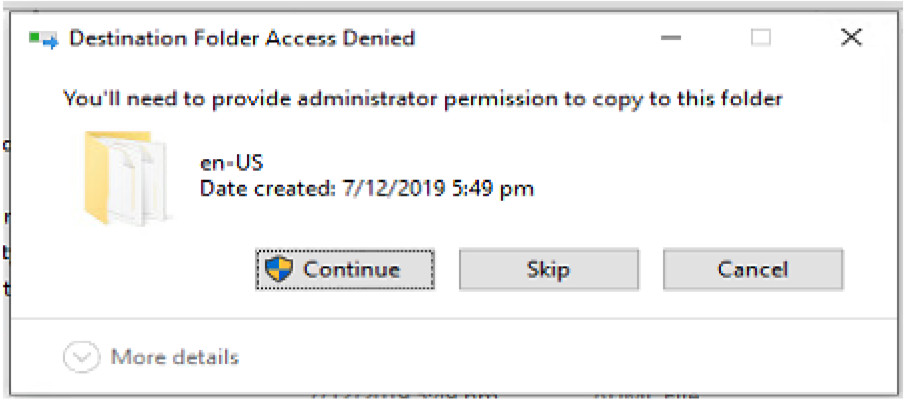
Name	Date modified	Type
msedge.adml	11/11/2021 11:24 pm	ADML File
msedgeupdate.adml	11/11/2021 11:24 pm	ADML File
msedgewebview2.adml	11/11/2021 11:24 pm	ADML File

Copy the following 3 files under MicrosoftEdgePolicyTemplates\windows\admx\zh-TW\ to C:\Windows\PolicyDefinitions\en-US (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:

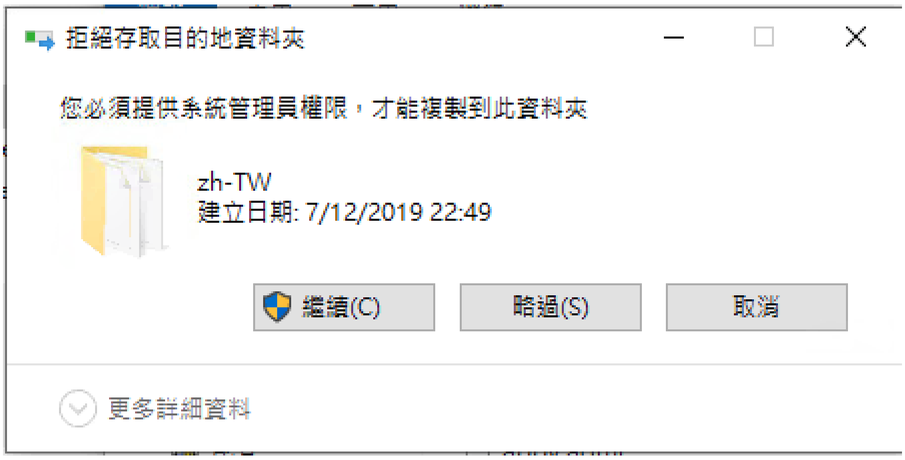


Destination Folder Access Denied

You'll need to provide administrator permission to copy to this folder

en-US
Date created: 7/12/2019 5:49 pm

For Chinese Windows OS:

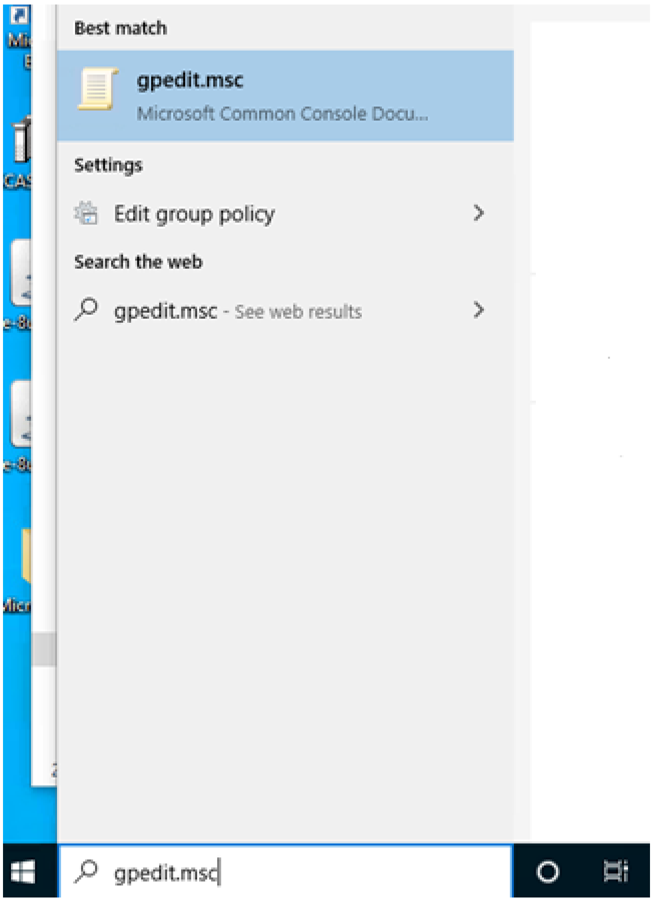


拒絕存取目的地資料夾

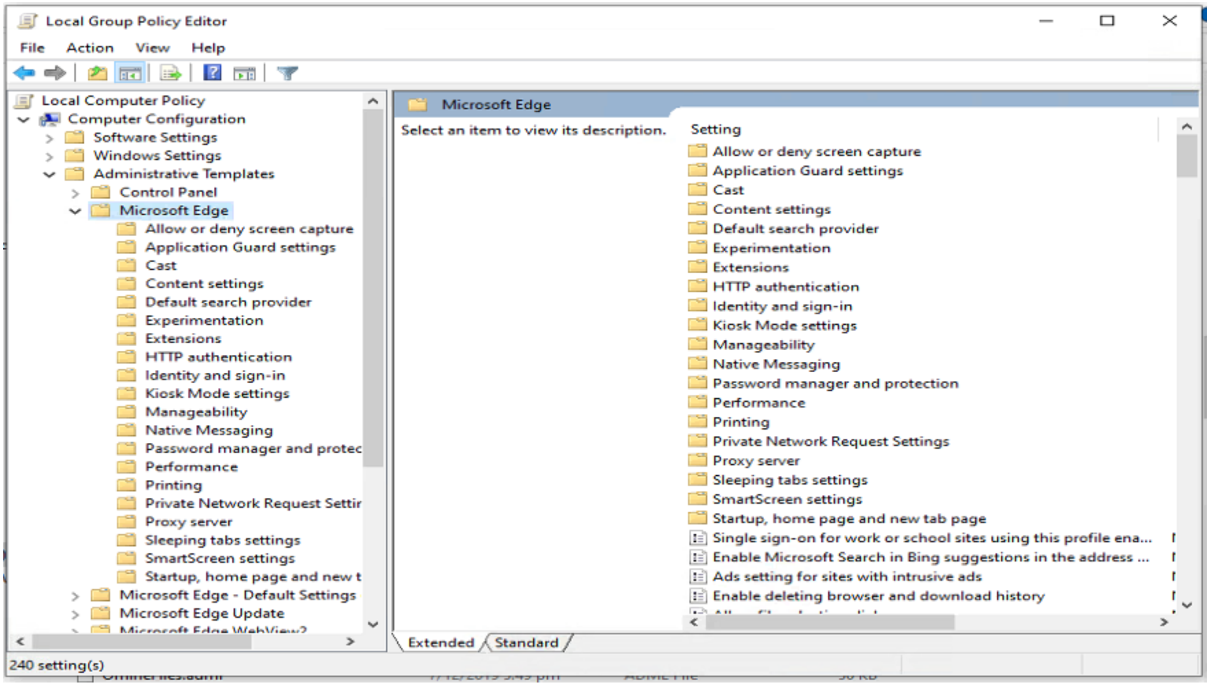
您必須提供系統管理員權限，才能複製到此資料夾

zh-TW
建立日期: 7/12/2019 22:49

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

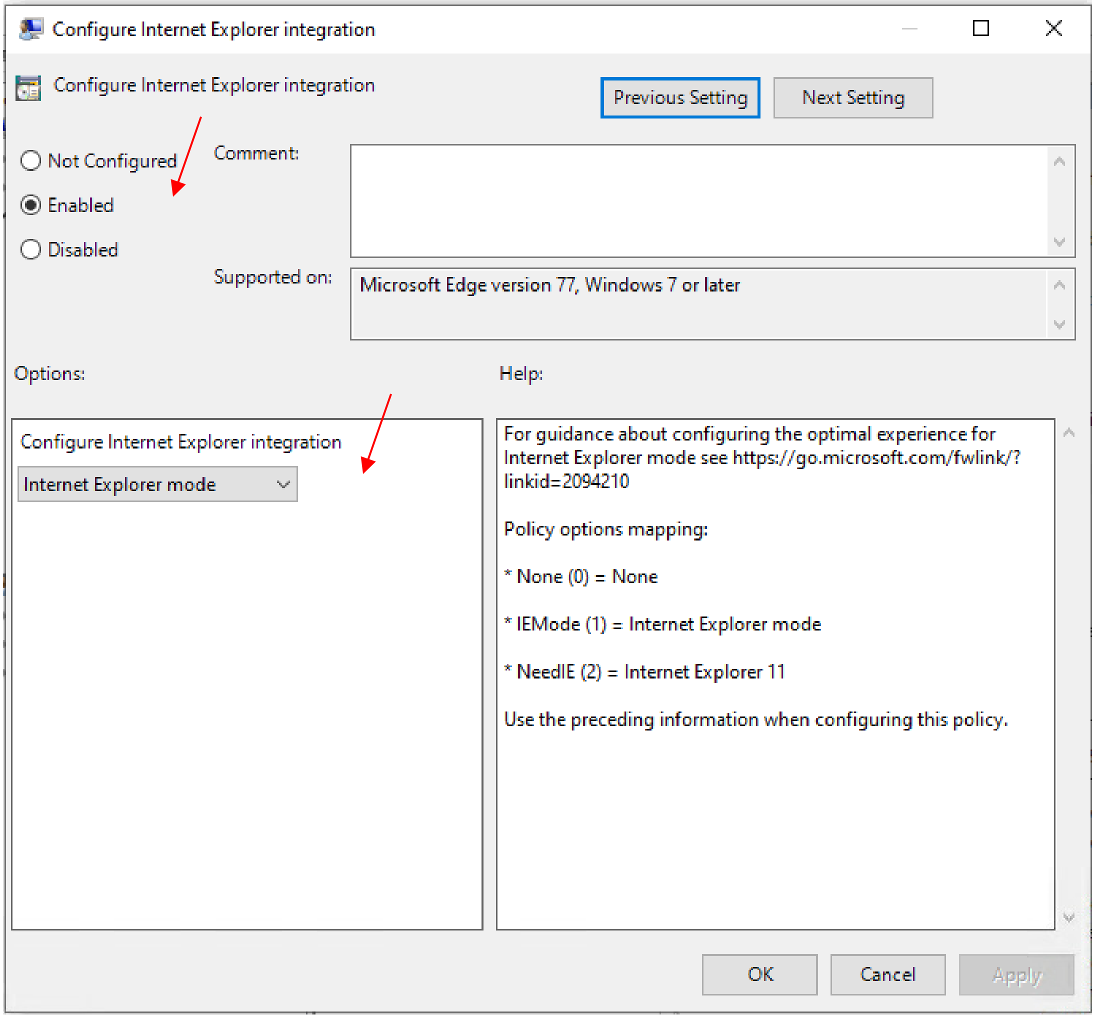


9. Browse to “Computer Configuration” > “Administrative Templates” > “Microsoft Edge”



10. Change Setting “Configure Internet Explorer Integration”

11. 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:

Configure Internet Explorer integration

Internet Explorer mode

Help:

For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Policy options mapping:

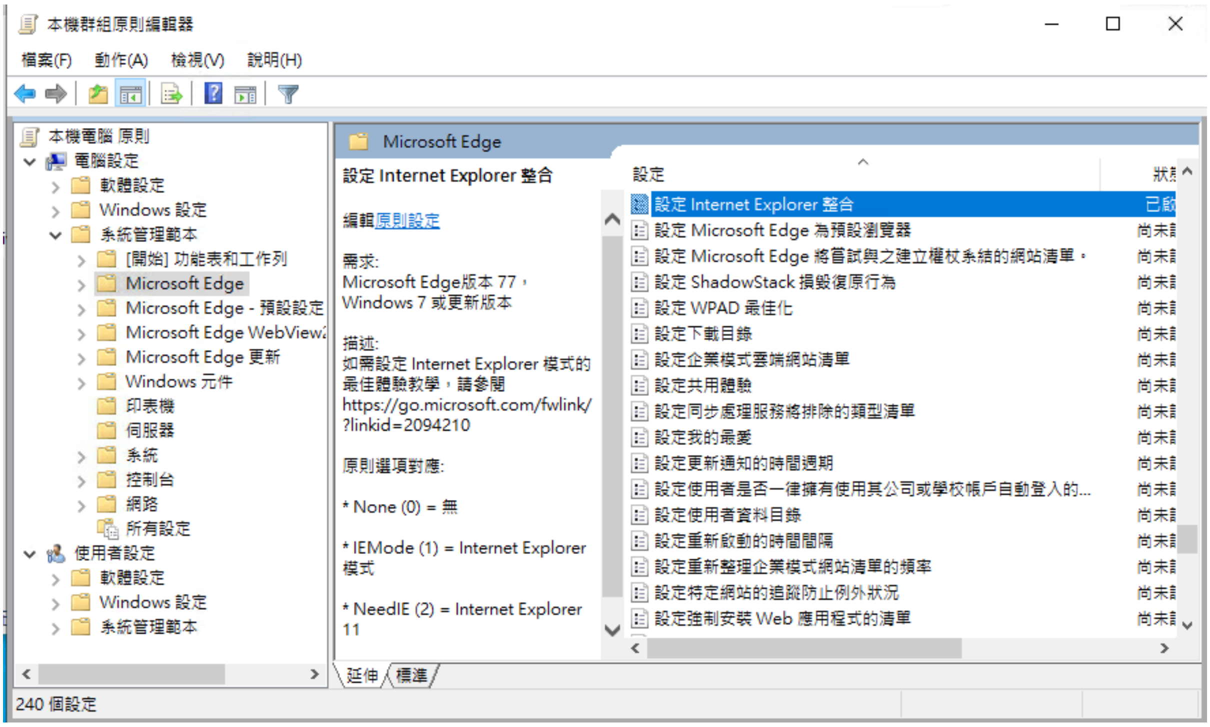
* None (0) = None

* IEMode (1) = Internet Explorer mode

* NeedIE (2) = Internet Explorer 11

Use the preceding information when configuring this policy.

For Chinese Windows OS:



- 本機電腦 原則
  - 電腦設定
    - 軟體設定
    - Windows 設定
    - 系統管理範本
      - [開始] 功能表和工作列
      - Microsoft Edge
      - Microsoft Edge - 預設設定
      - Microsoft Edge WebView
      - Microsoft Edge 更新
      - Windows 元件
      - 印表機
      - 伺服器
      - 系統
      - 控制台
      - 網路
      - 所有設定
  - 使用者設定
    - 軟體設定
    - Windows 設定
    - 系統管理範本

Microsoft Edge

設定 Internet Explorer 整合

編輯原則設定

需求:
Microsoft Edge版本 77，Windows 7 或更新版本

描述:
如需設定 Internet Explorer 模式的最佳體驗教學，請參閱 https://go.microsoft.com/fwlink/?linkid=2094210

原則選項對應:

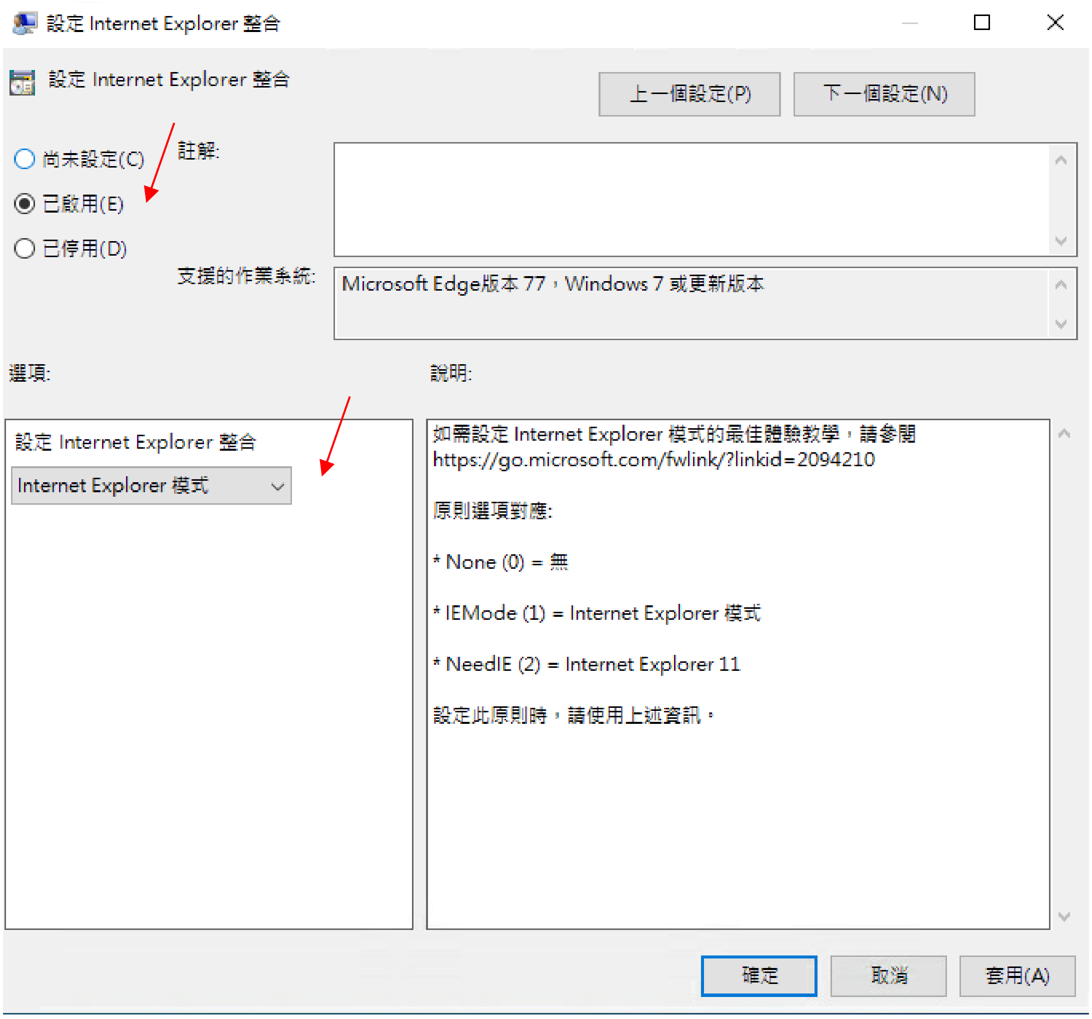
* None (0) = 無

* IEMode (1) = Internet Explorer 模式

* NeedIE (2) = Internet Explorer 11

設定	狀
設定 Internet Explorer 整合	已啟
設定 Microsoft Edge 為預設瀏覽器	尚未
設定 Microsoft Edge 將嘗試與之建立權杖系結的網站清單。	尚未
設定 ShadowStack 損毀復原行為	尚未
設定 WPAD 最佳化	尚未
設定下載目錄	尚未
設定企業模式雲端網站清單	尚未
設定共用體驗	尚未
設定同步處理服務將排除的類型清單	尚未
設定我的最愛	尚未
設定更新通知的時間週期	尚未
設定使用者是否一律擁有使用其公司或學校帳戶自動登入的...	尚未
設定使用者資料目錄	尚未
設定重新啟動的時間間隔	尚未
設定重新整理企業模式網站清單的頻率	尚未
設定特定網站的追蹤防止例外狀況	尚未
設定強制安裝 Web 應用程式的清單	尚未

240 個設定



設定 Internet Explorer 整合

○ 尚未設定(C)
● 已啟用(E)
○ 已停用(D)

註解:

支援的作業系統: Microsoft Edge版本 77，Windows 7 或更新版本

選項:

設定 Internet Explorer 整合
Internet Explorer 模式

說明:

如需設定 Internet Explorer 模式的最佳體驗教學，請參閱 https://go.microsoft.com/fwlink/?linkid=2094210

原則選項對應:

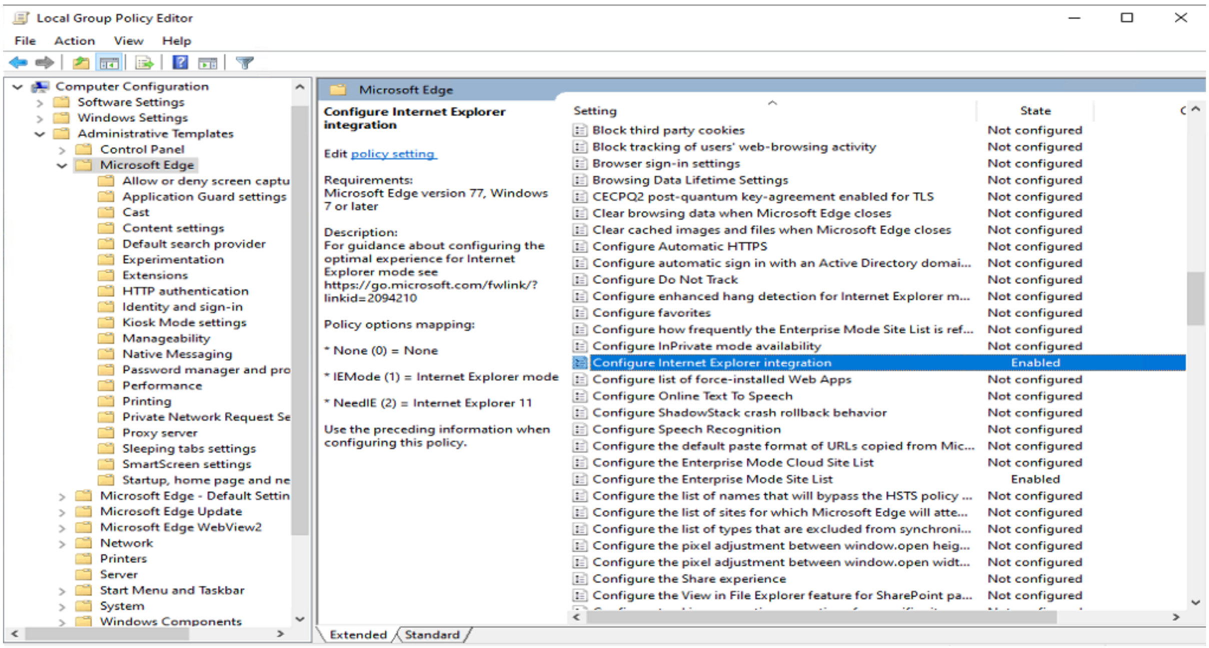
* None (0) = 無

* IEMode (1) = Internet Explorer 模式

* NeedIE (2) = Internet Explorer 11

設定此原則時，請使用上述資訊。

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



Configure Internet Explorer integration

Edit policy setting

Requirements:
Microsoft Edge version 77, Windows 7 or later

Description:
For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Policy options mapping:

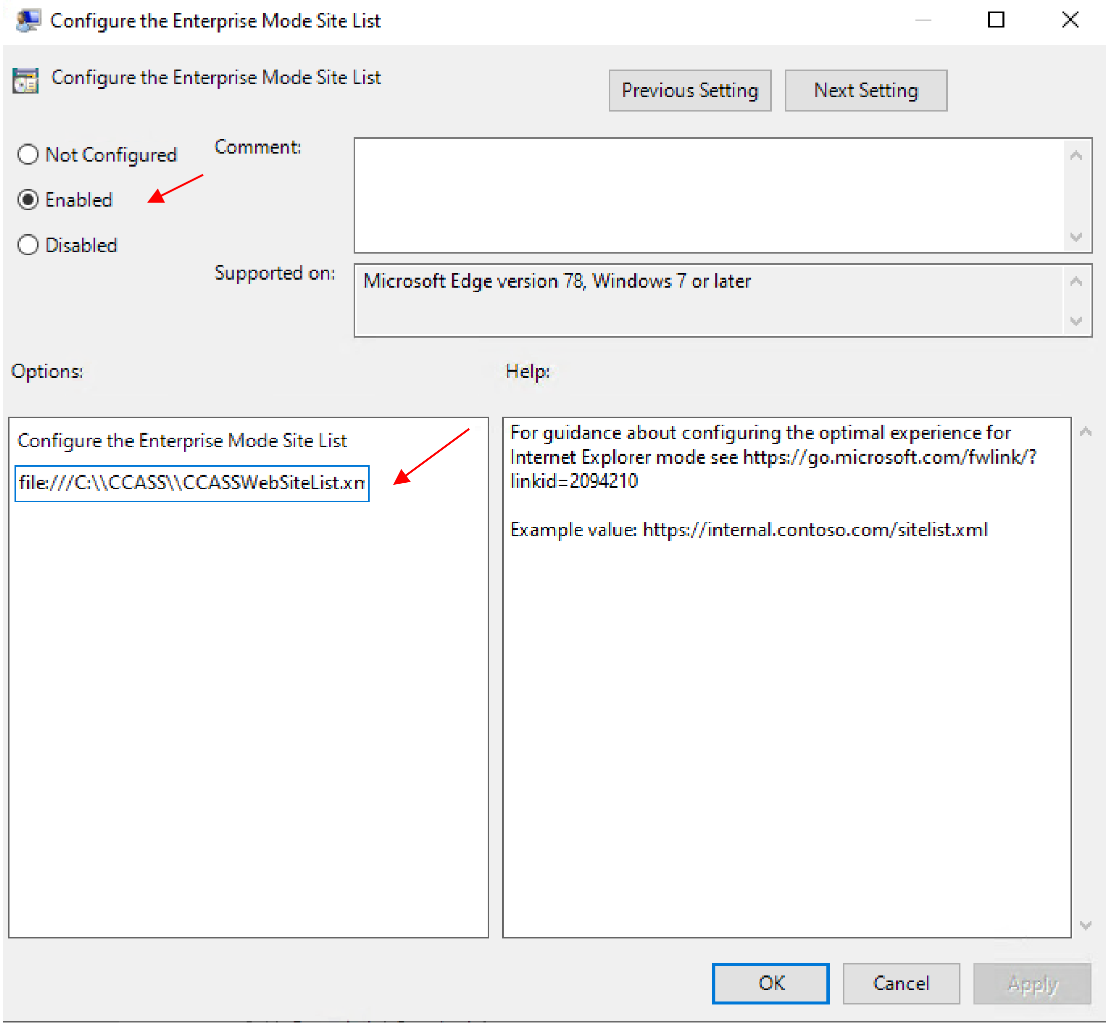
* None (0) = None

* IEMode (1) = Internet Explorer mode

* NeedIE (2) = Internet Explorer 11

Use the preceding information when configuring this policy.

Setting	State
Block third party cookies	Not configured
Block tracking of users' web-browsing activity	Not configured
Browser sign-in settings	Not configured
Browsing Data Lifetime Settings	Not configured
CECPQ2 post-quantum key-agreement enabled for TLS	Not configured
Clear browsing data when Microsoft Edge closes	Not configured
Clear cached images and files when Microsoft Edge closes	Not configured
Configure Automatic HTTPS	Not configured
Configure automatic sign in with an Active Directory domai...	Not configured
Configure Do Not Track	Not configured
Configure enhanced hang detection for Internet Explorer m...	Not configured
Configure favorites	Not configured
Configure how frequently the Enterprise Mode Site List is ref...	Not configured
Configure InPrivate mode availability	Not configured
Configure Internet Explorer integration	Enabled
Configure list of force-installed Web Apps	Not configured
Configure Online Text To Speech	Not configured
Configure ShadowStack crash rollback behavior	Not configured
Configure Speech Recognition	Not configured
Configure the default paste format of URLs copied from Mic...	Not configured
Configure the Enterprise Mode Cloud Site List	Not configured
Configure the Enterprise Mode Site List	Enabled
Configure the list of names that will bypass the HSTS policy ...	Not configured
Configure the list of sites for which Microsoft Edge will atte...	Not configured
Configure the list of types that are excluded from synchroni...	Not configured
Configure the pixel adjustment between window.open heig...	Not configured
Configure the pixel adjustment between window.open widt...	Not configured
Configure the Share experience	Not configured
Configure the View in File Explorer feature for SharePoint pa...	Not configured



Configure the Enterprise Mode Site List

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Microsoft Edge version 78, Windows 7 or later

Options:

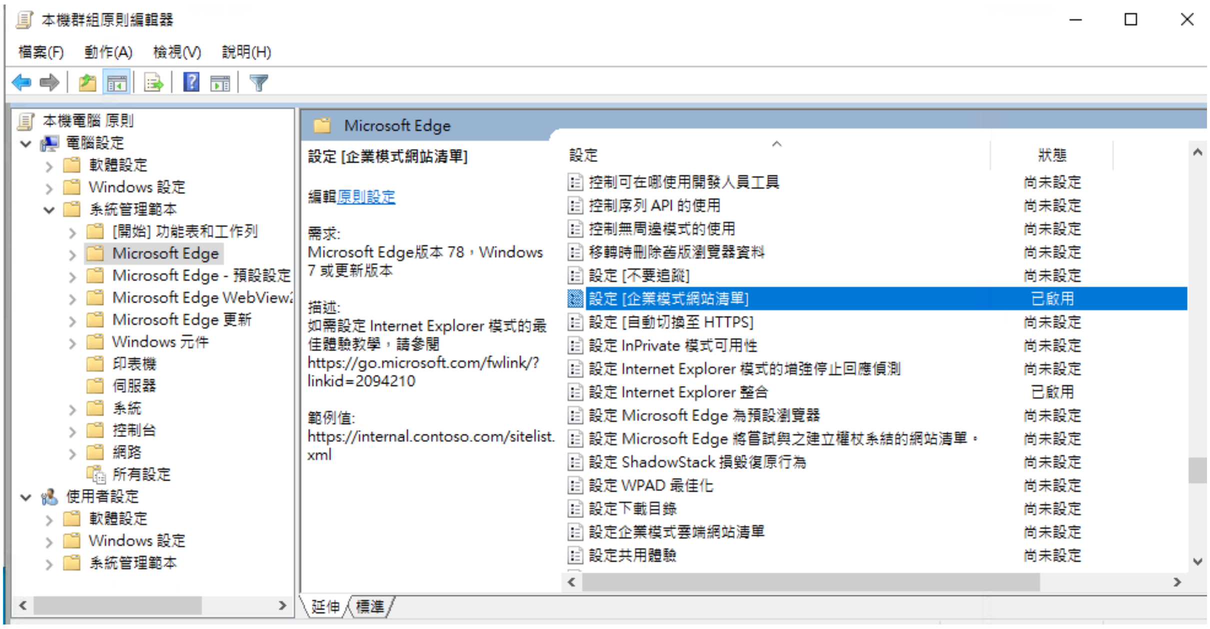
Configure the Enterprise Mode Site List
file:///C:\\CCASS\\CCASSWebSiteList.xn

Help:

For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Example value: https://internal.contoso.com/sitelist.xml

For Chinese Windows OS:



Microsoft Edge

設定 [企業模式網站清單]

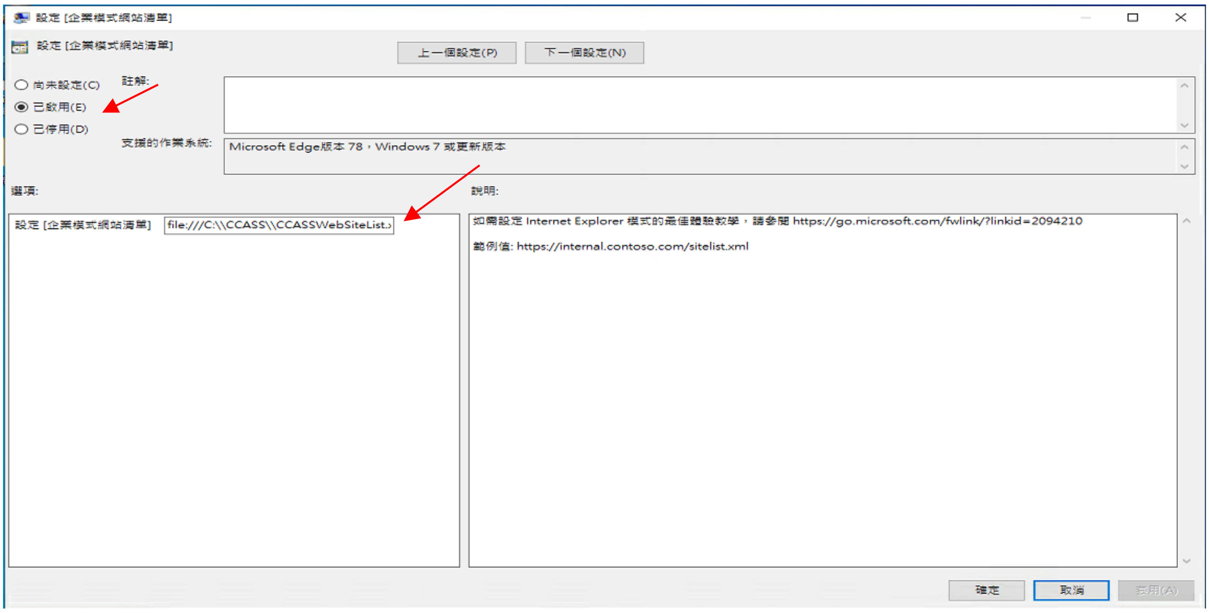
編輯原則設定

需求:
Microsoft Edge版本 78，Windows 7 或更新版本

描述:
如需設定 Internet Explorer 模式的最佳體驗教學，請參閱 https://go.microsoft.com/fwlink/?linkid=2094210

範例值:
https://internal.contoso.com/sitelist.xml

設定	狀態
控制可在哪使用開發人員工具	尚未設定
控制序列 API 的使用	尚未設定
控制無周邊模式的使用	尚未設定
移轉時刪除舊版瀏覽器資料	尚未設定
設定 [不要追蹤]	尚未設定
設定 [企業模式網站清單]	已啟用
設定 [自動切換至 HTTPS]	尚未設定
設定 InPrivate 模式可用性	尚未設定
設定 Internet Explorer 模式的增強停止回應偵測	尚未設定
設定 Internet Explorer 整合	已啟用
設定 Microsoft Edge 為預設瀏覽器	尚未設定
設定 Microsoft Edge 將嘗試與之建立權杖系結的網站清單。	尚未設定
設定 ShadowStack 損毀復原行為	尚未設定
設定 WPAD 最佳化	尚未設定
設定下載目錄	尚未設定
設定企業模式雲端網站清單	尚未設定
設定共用體驗	尚未設定



設定 [企業模式網站清單]

○ 尚未設定(C)
● 已啟用(E)
○ 已停用(D)

註解:

支援的作業系統: Microsoft Edge版本 78，Windows 7 或更新版本

選項:

設定 [企業模式網站清單] file:///C:\\CCASS\\CCASSWebSiteList.›

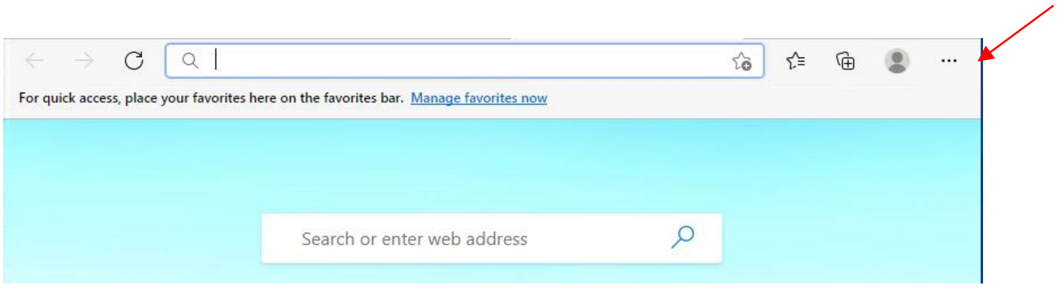
說明:

如需設定 Internet Explorer 模式的最佳體驗教學，請參閱 https://go.microsoft.com/fwlink/?linkid=2094210

範例值: https://internal.contoso.com/sitelist.xml

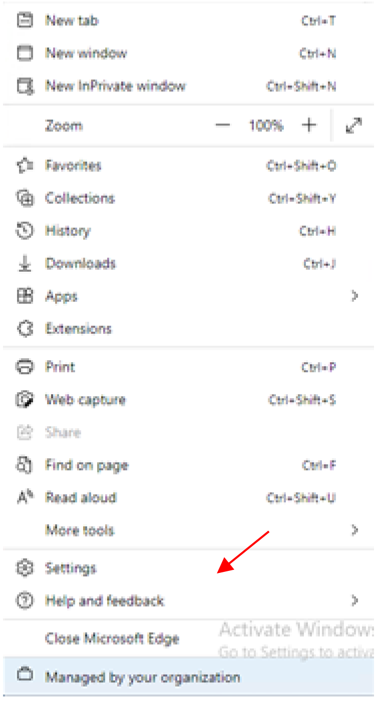
15. Click OK to save
16. Enable Pop-Up https://www.ccass.com:443 and https://www.ccass.com:442 in MS Edge browser

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

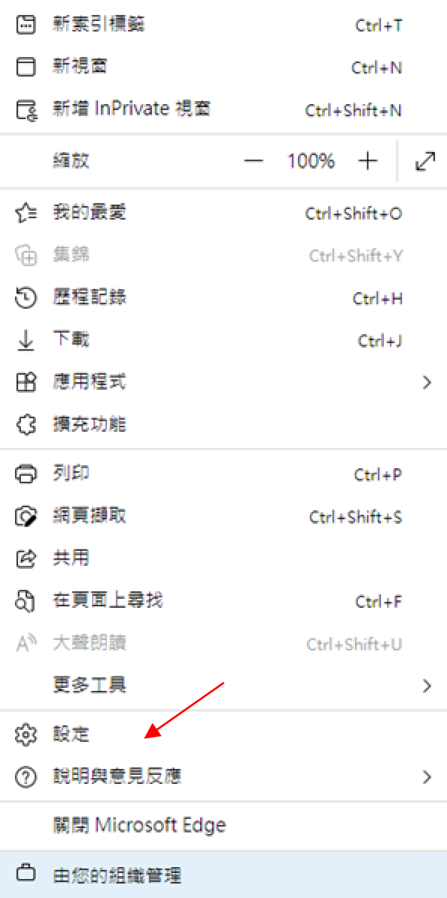


For quick access, place your favorites here on the favorites bar. Manage favorites now

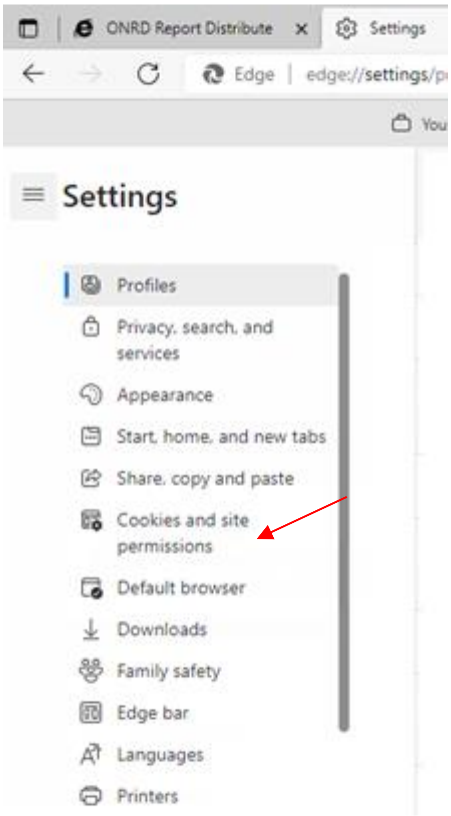
b. Go to Settings



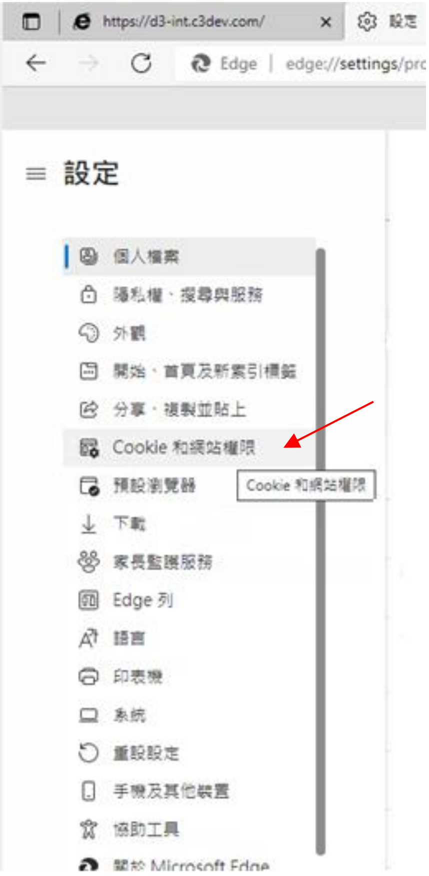
For Chinese Windows OS:



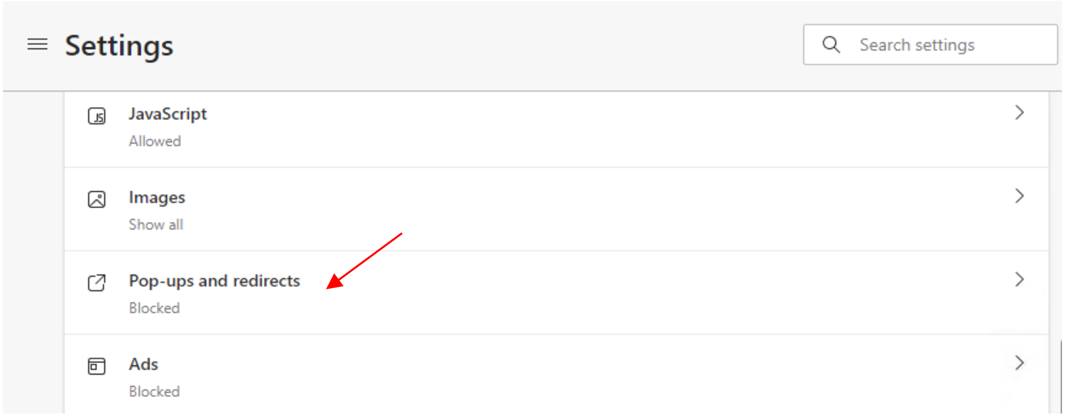
c. Click “Cookies and site permissions”



For Chinese Windows OS:



d. Go to “Pop-ups and redirects”



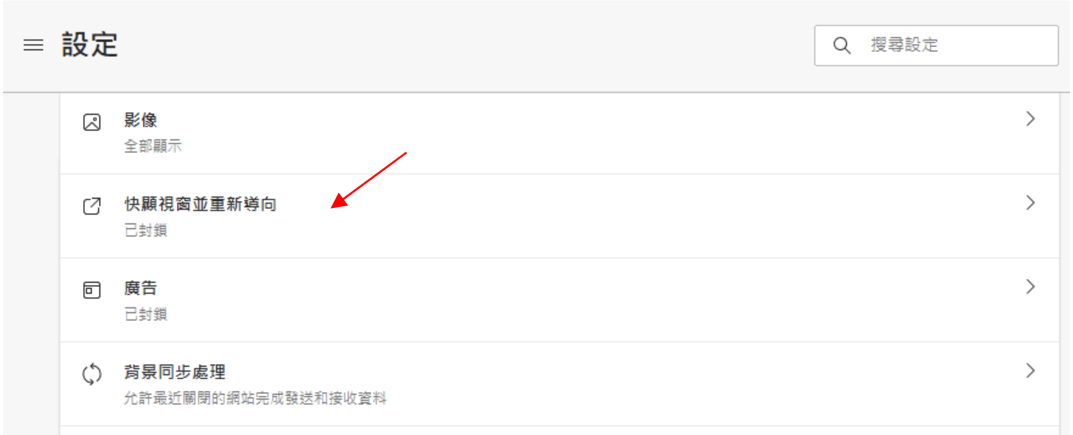
JavaScript
Allowed

Images
Show all

Pop-ups and redirects
Blocked

Ads
Blocked

For Chinese Windows OS:



設定

搜尋設定

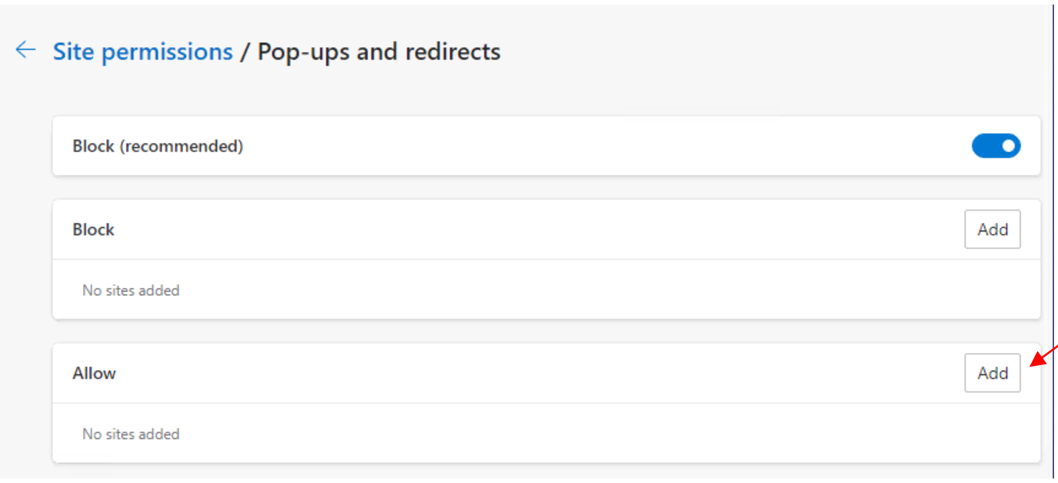
影像
全部顯示

快顯視窗並重新導向
已封鎖

廣告
已封鎖

背景同步處理
允許最近關閉的網站完成發送和接收資料

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



Site permissions / Pop-ups and redirects

Block (recommended)

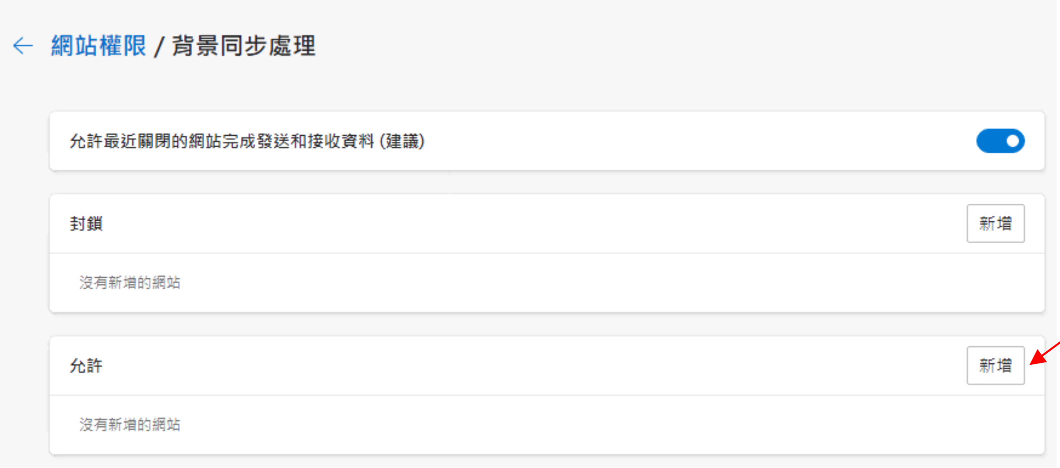
Block

No sites added

Allow

No sites added

For Chinese Windows OS:



網站權限 / 背景同步處理

允許最近關閉的網站完成發送和接收資料 (建議)

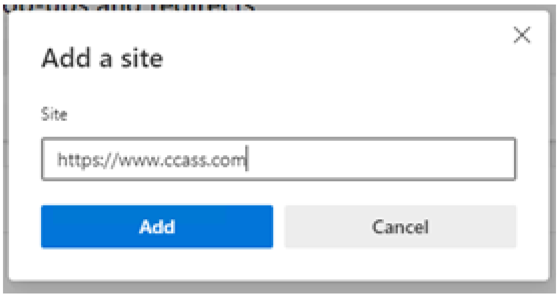
封鎖

沒有新增的網站

允許

沒有新增的網站

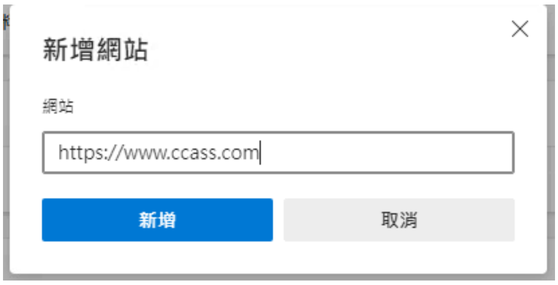
f. Input https://www.ccass.com and click “Add”



Add a site

Site: https://www.ccass.com

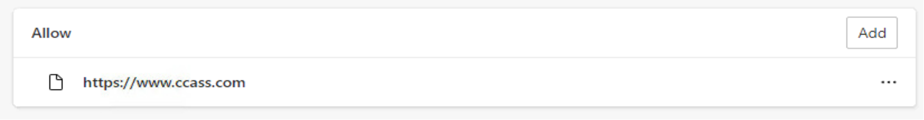
For Chinese Windows OS:



新增網站

網站: https://www.ccass.com

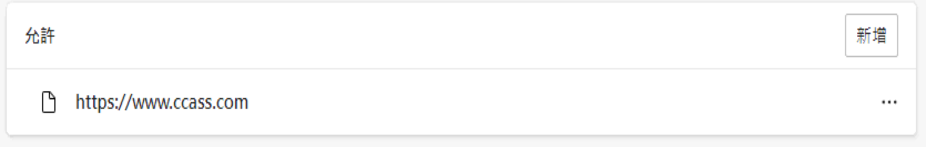
g. Confirm to see the website https://www.ccass.com is added



Allow

https://www.ccass.com

For Chinese Windows OS:



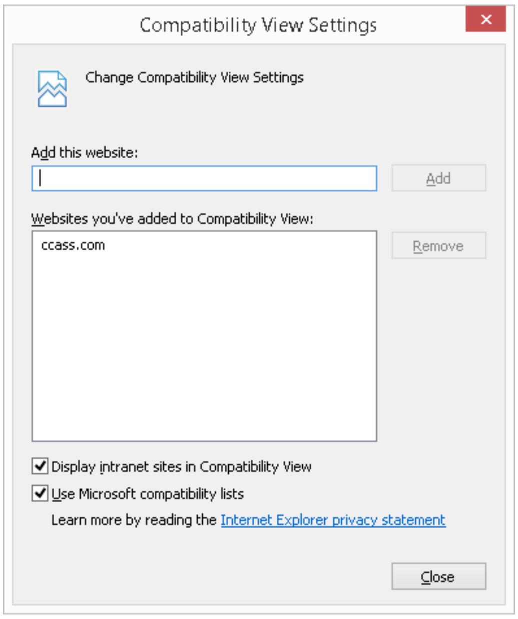
允許

https://www.ccass.com

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, if available)

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:”


Compatibility View Settings
×
Change Compatibility View Settings
Add this website:
Add
Websites you've added to Compatibility View:
Remove
Close

ccass.com

☑ Display intranet sites in Compatibility View

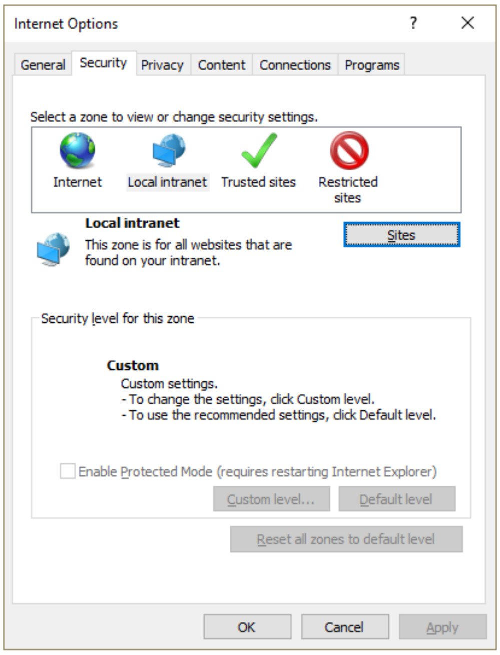
☑ Use Microsoft compatibility lists

Learn more by reading the Internet Explorer privacy statement

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”



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

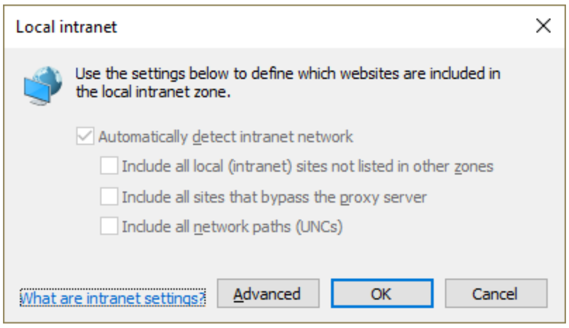
Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

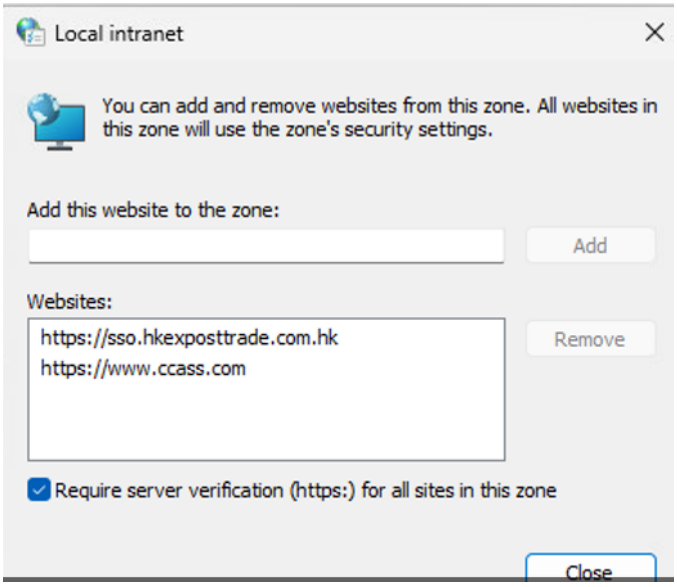
3. Click “Advanced”.



Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network
□ Include all local (intranet) sites not listed in other zones
□ Include all sites that bypass the proxy server
□ Include all network paths (UNCs)

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



Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:
https://sso.hkexposttrade.com.hk
https://www.ccass.com

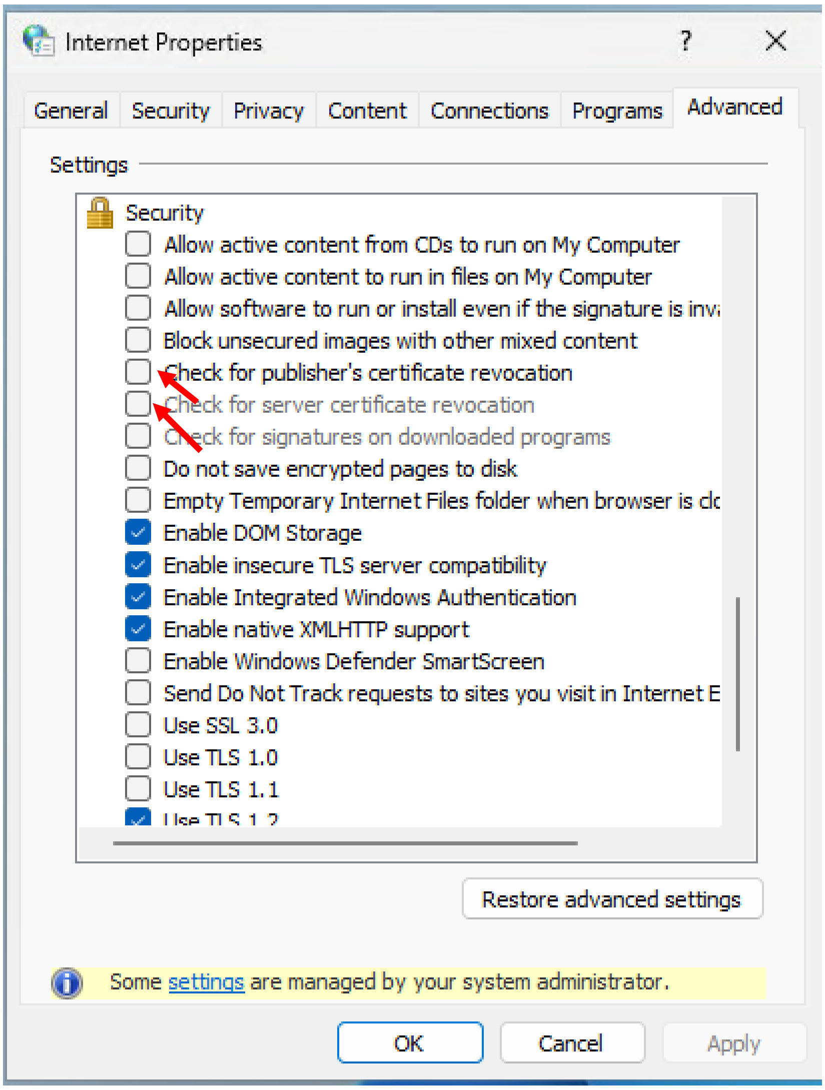
☑ Require server verification (https:) for all sites in this zone

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 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



Security

- □ Allow active content from CDs to run on My Computer
- □ Allow active content to run in files on My Computer
- □ Allow software to run or install even if the signature is inv
- □ Block unsecured images with other mixed content
- □ Check for publisher's certificate revocation
- □ Check for server certificate revocation
- □ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is cl
- ☑ Enable DOM Storage
- ☑ Enable insecure TLS server compatibility
- ☑ Enable Integrated Windows Authentication
- ☑ Enable native XMLHTTP support
- □ Enable Windows Defender SmartScreen
- □ Send Do Not Track requests to sites you visit in Internet E
- □ Use SSL 3.0
- □ Use TLS 1.0
- □ Use TLS 1.1
- ☑ Use TLS 1.2

Some settings are managed by your system administrator.

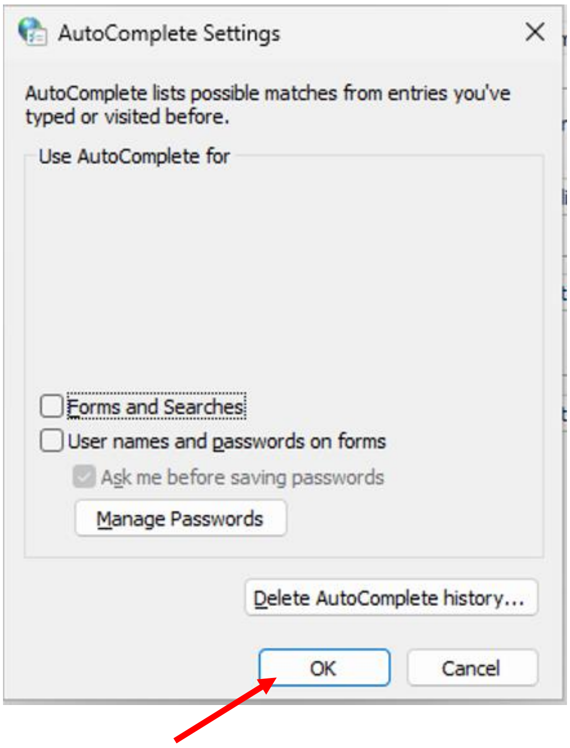
3. Click “Apply” and OK to close the window to complete the setting

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



AutoComplete Settings

AutoComplete lists possible matches from entries you've typed or visited before.

Use AutoComplete for

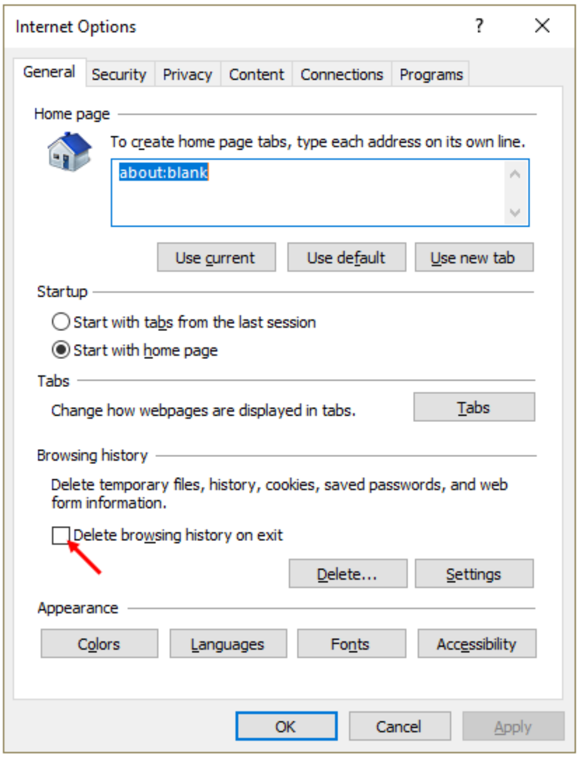
□ Forms and Searches

□ User names and passwords on forms

☑ Ask me before saving passwords

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 **<u>not checked</u>** (if any)



Internet Options ? ✕

General | Security | Privacy | Content | Connections | Programs

Home page

To create home page tabs, type each address on its own line.

about:blank

Use current | Use default | Use new tab

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs. Tabs

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

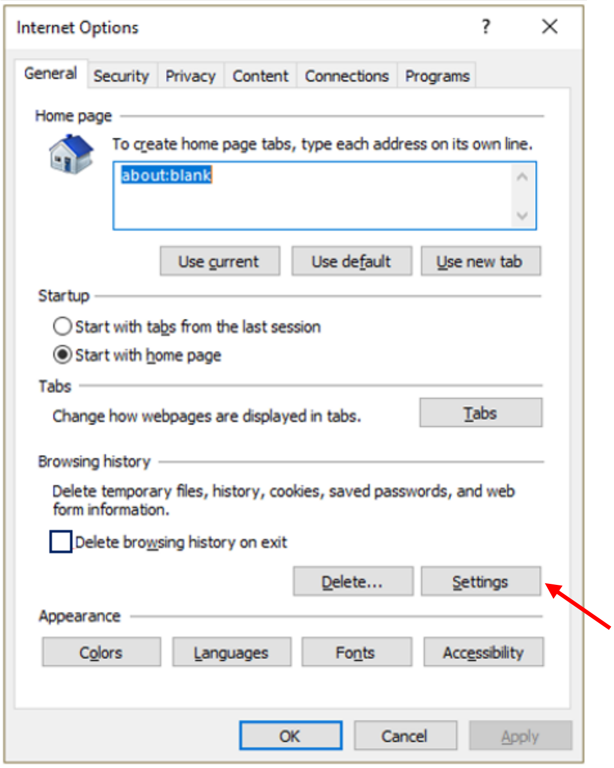
Delete... | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply

3. Then click on Settings



Internet Options ? ✕

General | Security | Privacy | Content | Connections | Programs

Home page

To create home page tabs, type each address on its own line.

about:blank

Use current | Use default | Use new tab

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs. Tabs

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

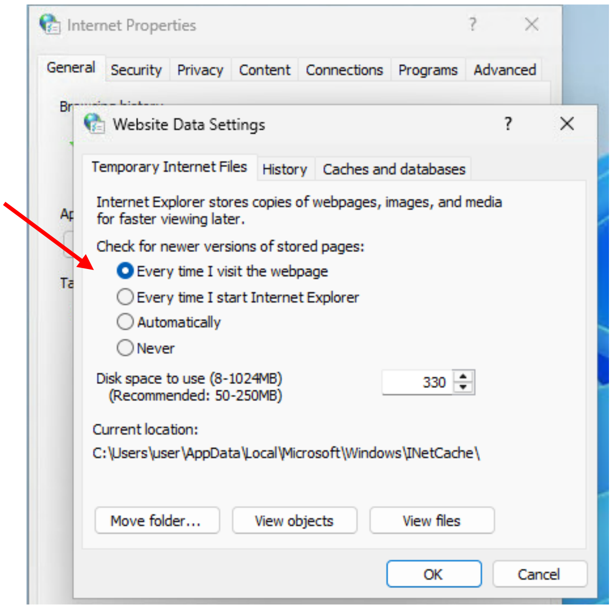
Delete... | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply

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



Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

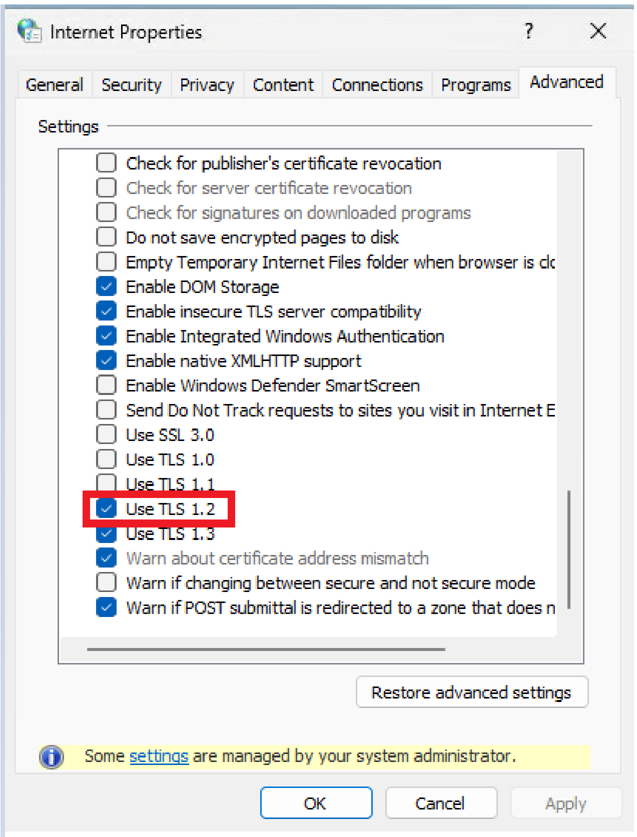
● Every time I visit the webpage
○ Every time I start Internet Explorer
○ Automatically
○ Never

Disk space to use (8-1024MB) (Recommended: 50-250MB) 330

Current location:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\

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.



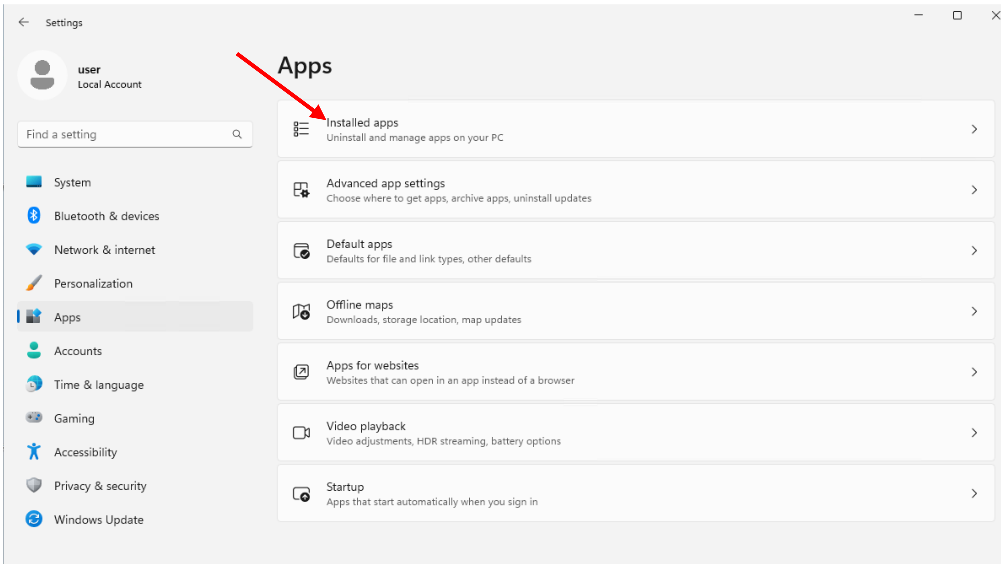
- ☐ Check for publisher's certificate revocation
- ☐ Check for server certificate revocation
- ☐ Check for signatures on downloaded programs
- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is clc
- ☑ Enable DOM Storage
- ☑ Enable insecure TLS server compatibility
- ☑ Enable Integrated Windows Authentication
- ☑ Enable native XMLHTTP support
- ☐ Enable Windows Defender SmartScreen
- ☐ Send Do Not Track requests to sites you visit in Internet E
- ☐ Use SSL 3.0
- ☐ Use TLS 1.0
- ☐ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Use TLS 1.3
- ☑ Warn about certificate address mismatch
- ☐ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does n

Some settings are managed by your system administrator.

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 -> Installed apps


Settings
user
Local Account
Find a setting
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
Apps
Installed apps
Uninstall and manage apps on your PC
Advanced app settings
Choose where to get apps, archive apps, uninstall updates
Default apps
Defaults for file and link types, other defaults
Offline maps
Downloads, storage location, map updates
Apps for websites
Websites that can open in an app instead of a browser
Video playback
Video adjustments, HDR streaming, battery options
Startup
Apps that start automatically when you sign in

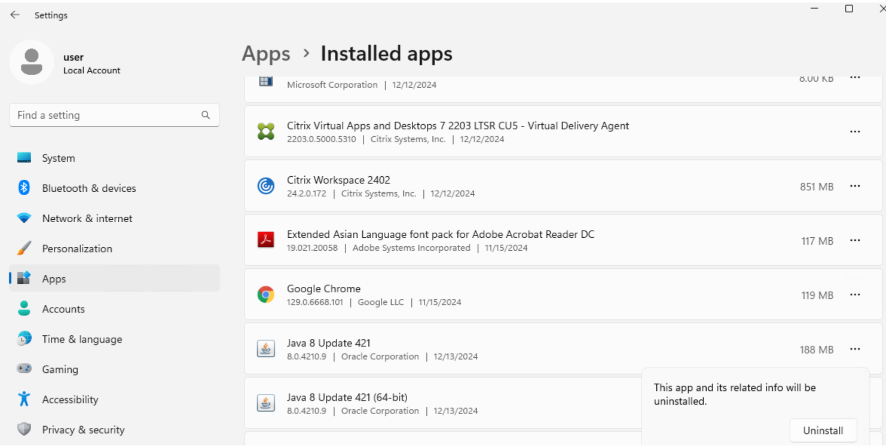
2. Find “Java X Update XX” in the list

- **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.



Microsoft Corporation | 12/12/2024 8.00 KB

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 - Virtual Delivery Agent
2203.0.5000.5310 | Citrix Systems, Inc. | 12/12/2024

Citrix Workspace 2402
24.2.0.172 | Citrix Systems, Inc. | 12/12/2024 851 MB

Extended Asian Language font pack for Adobe Acrobat Reader DC
19.021.20058 | Adobe Systems Incorporated | 11/15/2024 117 MB

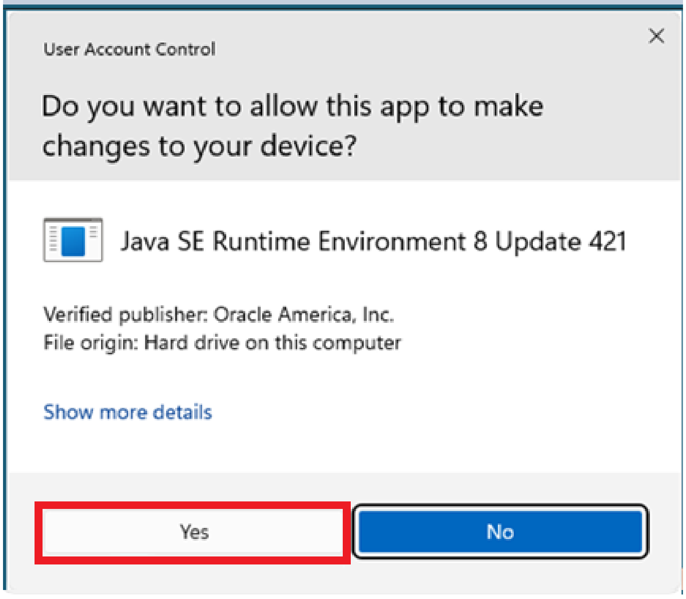
Google Chrome
129.0.6668.101 | Google LLC | 11/15/2024 119 MB

Java 8 Update 421
8.0.4210.9 | Oracle Corporation | 12/13/2024 188 MB

Java 8 Update 421 (64-bit)
8.0.4210.9 | Oracle Corporation | 12/13/2024

This app and its related info will be uninstalled.

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



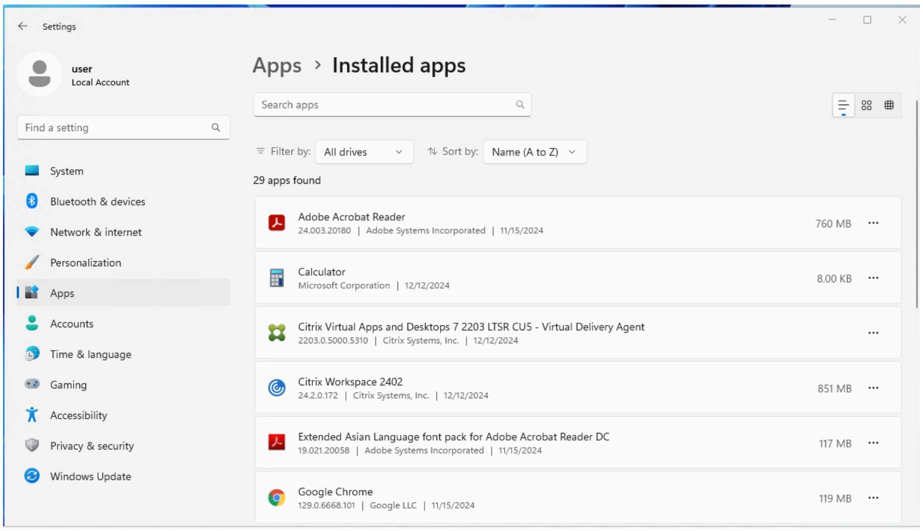
User Account Control

Do you want to allow this app to make changes to your device?

Java SE Runtime Environment 8 Update 421

Verified publisher: Oracle America, Inc.
File origin: Hard drive on this computer

5. Check again that all JRE items should be removed



Settings

user
Local Account

Find a setting

Apps › Installed apps

Search apps

Filter by: All drives Sort by: Name (A to Z)

29 apps found

Adobe Acrobat Reader
24.003.20180 | Adobe Systems Incorporated | 11/15/2024 760 MB

Calculator
Microsoft Corporation | 12/12/2024 8.00 KB

Citrix Virtual Apps and Desktops 7 2203 LTSR CU5 - Virtual Delivery Agent
2203.0.5000.5310 | Citrix Systems, Inc. | 12/12/2024

Citrix Workspace 2402
24.2.0.172 | Citrix Systems, Inc. | 12/12/2024 851 MB

Extended Asian Language font pack for Adobe Acrobat Reader DC
19.021.20058 | Adobe Systems Incorporated | 11/15/2024 117 MB

Google Chrome
129.0.6668.101 | Google LLC | 11/15/2024 119 MB

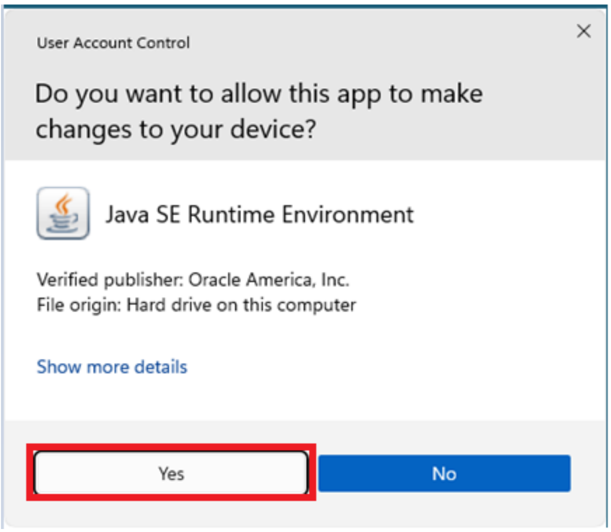
6. Restart the computer

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 8u441 from (https://www.java.com/en/download/ or https://www.oracle.com/java/technologies/javase/javase8u211-later-archive-downloads.html).

   jre-8u441-windows-i586.exe – for Windows x86

   jre-8u441-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



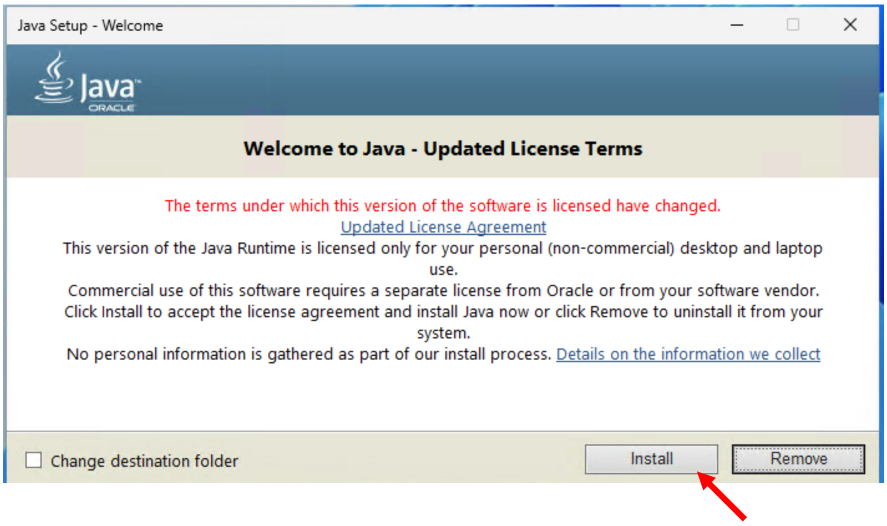
User Account Control

Do you want to allow this app to make changes to your device?

Java SE Runtime Environment

Verified publisher: Oracle America, Inc.
File origin: Hard drive on this computer

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

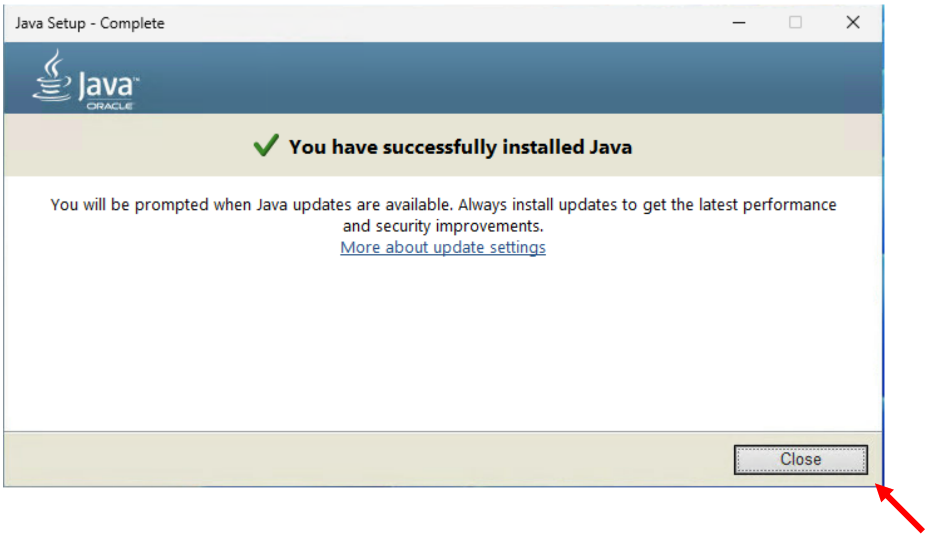


Welcome to Java - Updated License Terms

The terms under which this version of the software is licensed have changed.
Updated License Agreement
This version of the Java Runtime is licensed only for your personal (non-commercial) desktop and laptop use.
Commercial use of this software requires a separate license from Oracle or from your software vendor.
Click Install to accept the license agreement and install Java now or click Remove to uninstall it from your system.
No personal information is gathered as part of our install process. Details on the information we collect

□ Change destination folder

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

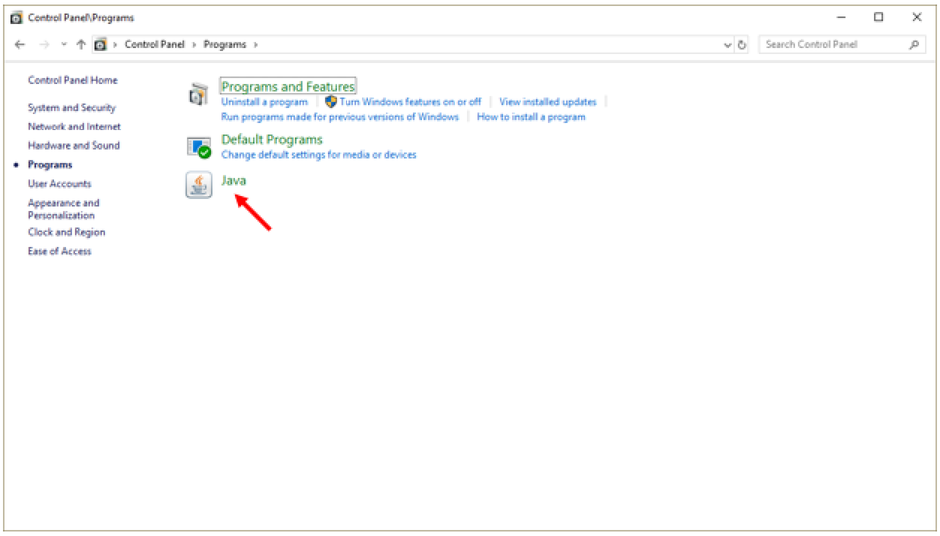


✓ You have successfully installed Java

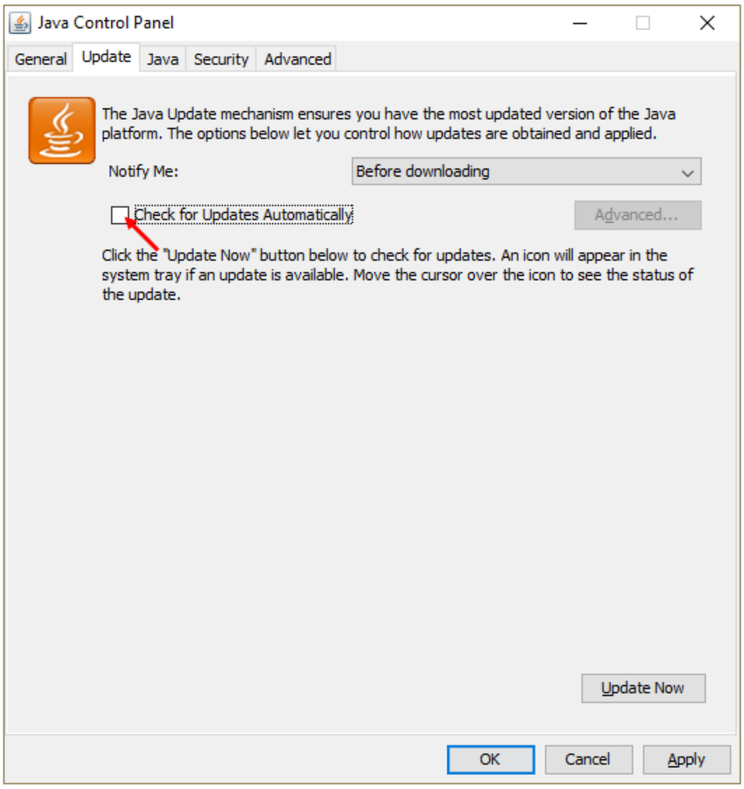
You will be prompted when Java updates are available. Always install updates to get the latest performance and security improvements.
More about update settings

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”.



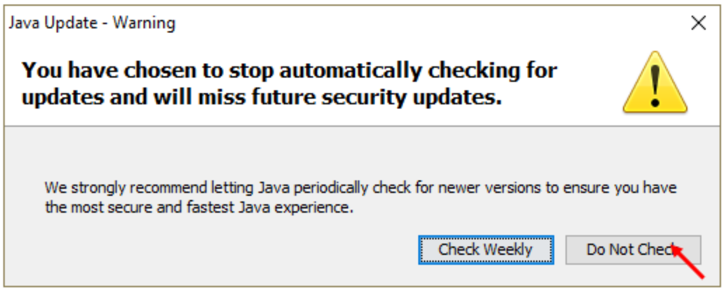
The Java Update mechanism ensures you have the most updated version of the Java platform. The options below let you control how updates are obtained and applied.

Notify Me: Before downloading

□ Check for Updates Automatically

Click the "Update Now" button below to check for updates. An icon will appear in the system tray if an update is available. Move the cursor over the icon to see the status of the update.

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

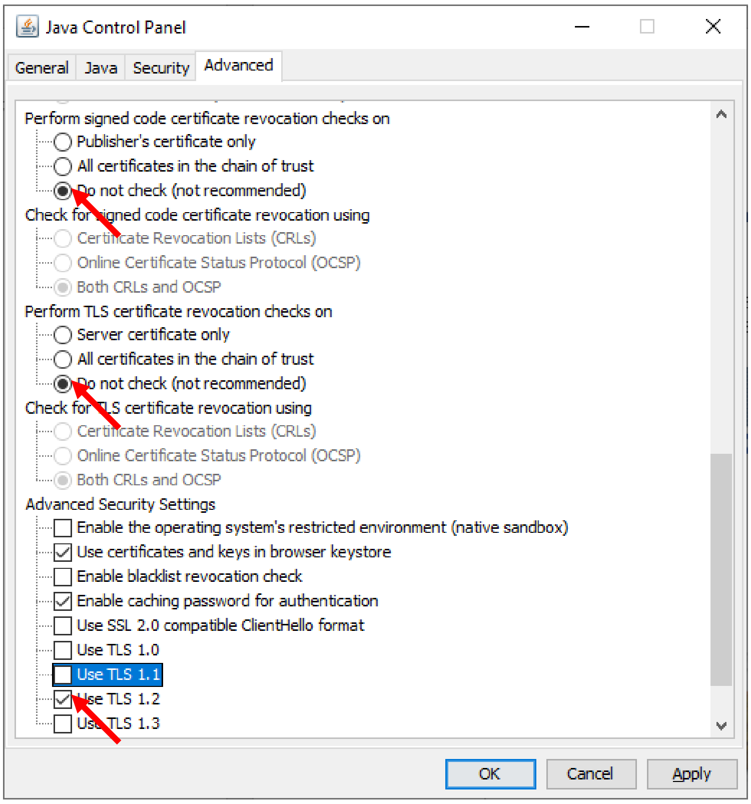


Java Update - Warning

You have chosen to stop automatically checking for updates and will miss future security updates.

We strongly recommend letting Java periodically check for newer versions to ensure you have the most secure and fastest Java experience.

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



Perform signed code certificate revocation checks on
- ○ Publisher's certificate only
- ○ All certificates in the chain of trust
- ● Do not check (not recommended)

Check for signed code certificate revocation using
- ○ Certificate Revocation Lists (CRLs)
- ○ Online Certificate Status Protocol (OCSP)
- ● Both CRLs and OCSP

Perform TLS certificate revocation checks on
- ○ Server certificate only
- ○ All certificates in the chain of trust
- ● Do not check (not recommended)

Check for TLS certificate revocation using
- ○ Certificate Revocation Lists (CRLs)
- ○ Online Certificate Status Protocol (OCSP)
- ● Both CRLs and OCSP

Advanced Security Settings
- □ Enable the operating system's restricted environment (native sandbox)
- ☑ Use certificates and keys in browser keystore
- □ Enable blacklist revocation check
- ☑ Enable caching password for authentication
- □ Use SSL 2.0 compatible ClientHello format
- □ Use TLS 1.0
- □ Use TLS 1.1
- ☑ Use TLS 1.2
- □ Use TLS 1.3

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

6 RAP Technical Setup

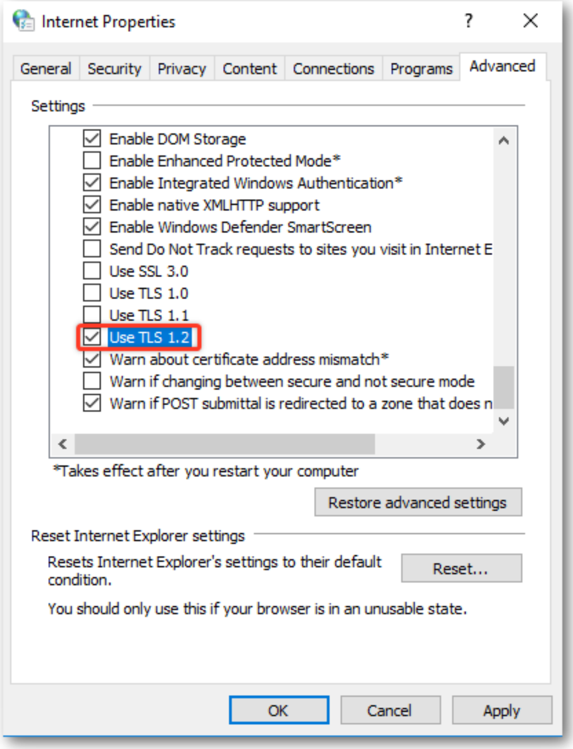
After the network setup is completed, HKSCC Participants and DBs should proceed to configure their RAP setup & connectivity according to the HKSCC Report Access Platform (RAP) Technical Guide available in Client Connect on HKEX Access Management Portal.

7 VaR Online (not applicable to DBs)

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.

7.1 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.



Internet Properties

Settings

☑ Enable DOM Storage
☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
☐ Send Do Not Track requests to sites you visit in Internet E
☐ Use SSL 3.0
☐ Use TLS 1.0
☐ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

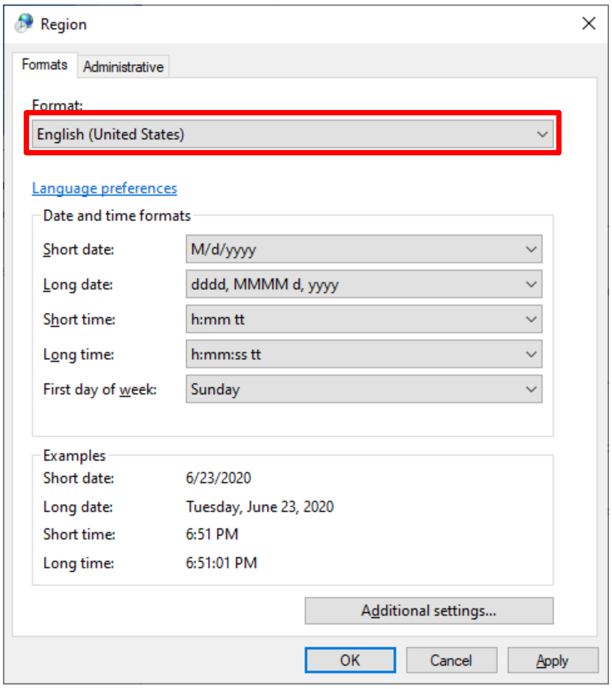
Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

7.2 Language Settings in Windows

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



Region

Format: English (United States)

Date and time formats

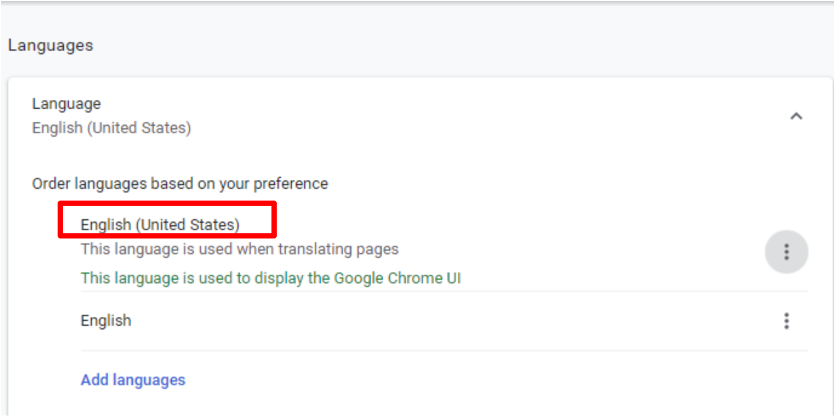
Short date:	M/d/yyyy
Long date:	dddd, MMMM d, yyyy
Short time:	h:mm tt
Long time:	h:mm:ss tt
First day of week:	Sunday

Examples

Short date:	6/23/2020
Long date:	Tuesday, June 23, 2020
Short time:	6:51 PM
Long time:	6:51:01 PM

7.3 Language Settings in Chrome

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



Languages

Language
English (United States)

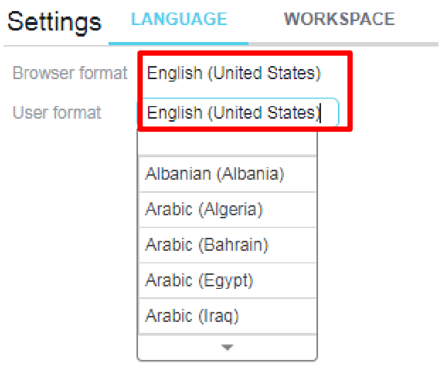
Order languages based on your preference

English (United States)
This language is used when translating pages
This language is used to display the Google Chrome UI

English

7.4 Language Settings for VaR Online

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



Settings LANGUAGE WORKSPACE

Browser format English (United States)

User format English (United States)