

**E-platform for School Development
& Accountability (ESDA)
Version 5.3.x**

Installation and Data Migration Guide

July 2025

Table of Contents

About this Guide	3
Chapter 1 Installing ESDA	4
1.1 ESDA Installation	4
Chapter 2 Testing after Installation.....	8
2.1 Login Test	8
2.2 Login by Default User Account	9
2.3 System Registration.....	9
2.4 System Update.....	10
Chapter 3 System Setting	12
3.1 School Setting	12
3.2 Upload School Badge.....	13
3.3 School Year Setting.....	13
3.4 Advanced System Setting.....	14
3.5 System Version Information	14
3.6 Set up e-Certificate.....	15
Appendix 1 Setup ESDA to Use Other Port	22
Appendix 2 Setup Self-signed e-Certificate at Client Side	23
Appendix 3 Verify ESDA's port availability	32
Appendix 4 Solution for the failure to connect SQL server	33
Appendix 5 Enable Port 443 on Windows	36
Appendix 6 Uninstalling ESDA	39
Appendix 7 Cross-Platform Data Migration Procedures.....	40

About this Guide

This Installation and Data Migration Guide aims to provide the details on the installation of ESDA for System Administrator or any staff member authorised to install and manage ESDA. System Administrator can get installation and data migration instructions, and information on post-installation and post-migration testing for ESDA v5.0.x in this guide or through the self-learning videos on the ESDA webpage (<https://www.edb.gov.hk/en/sch-admin/sch-quality-assurance/performance-indicators/esda/self-learning.html>).

Contact us

Education Bureau (EDB) welcomes schools to share with us their opinions and good practices in using ESDA. Please contact the Indicators Section of the EDB to express any views and suggestions, or to share experiences by phone, fax or email.

You can contact the Indicators Section of the EDB by the following methods for enquiring about the technical problem of ESDA.

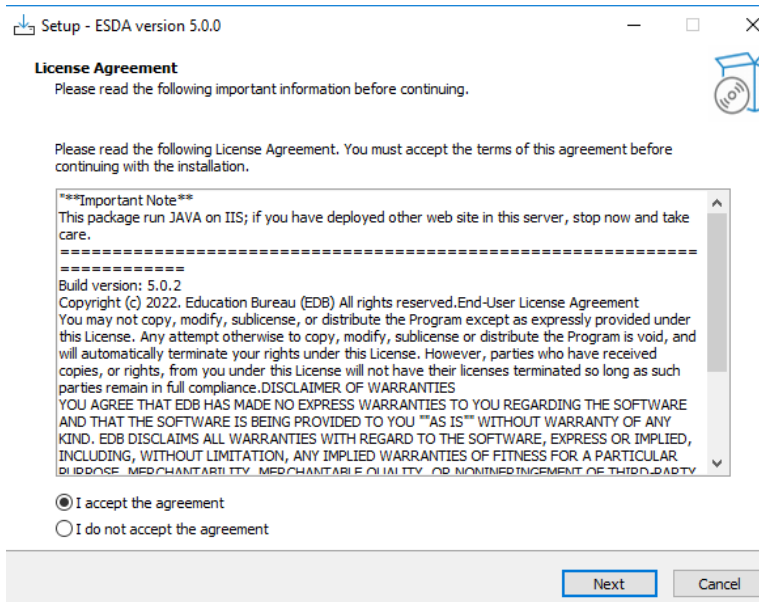
- Telephone: 2892 6577 / 2892 6476 / 2892 6544 / 2892 6507
- Fax: 2119 9074
- Email: indicators@edb.gov.hk

Note: For enquiries by email or fax, please state the technical problem encountered, school name and contact person with phone number.

Chapter 1 Installing ESDA

1.1 ESDA Installation

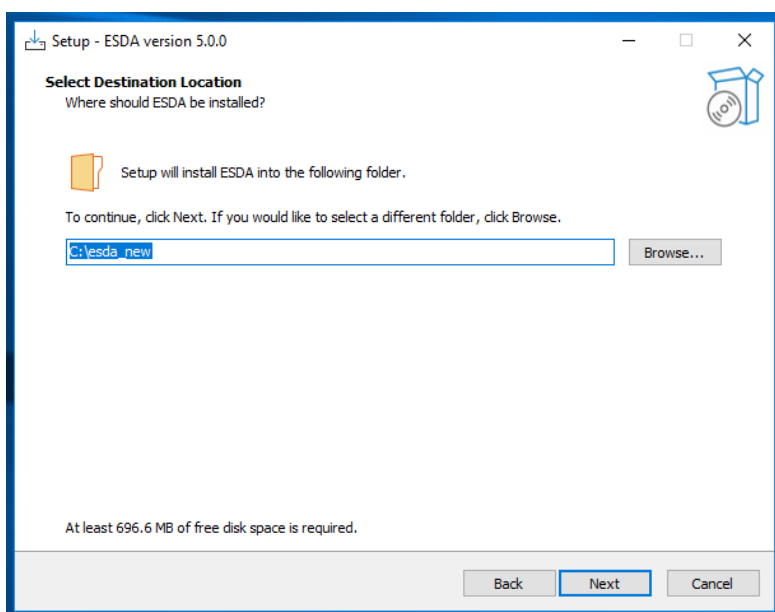
1) Double-click “esda-v5.0.x.exe”. Select “I accept the agreement” and click “Next”.



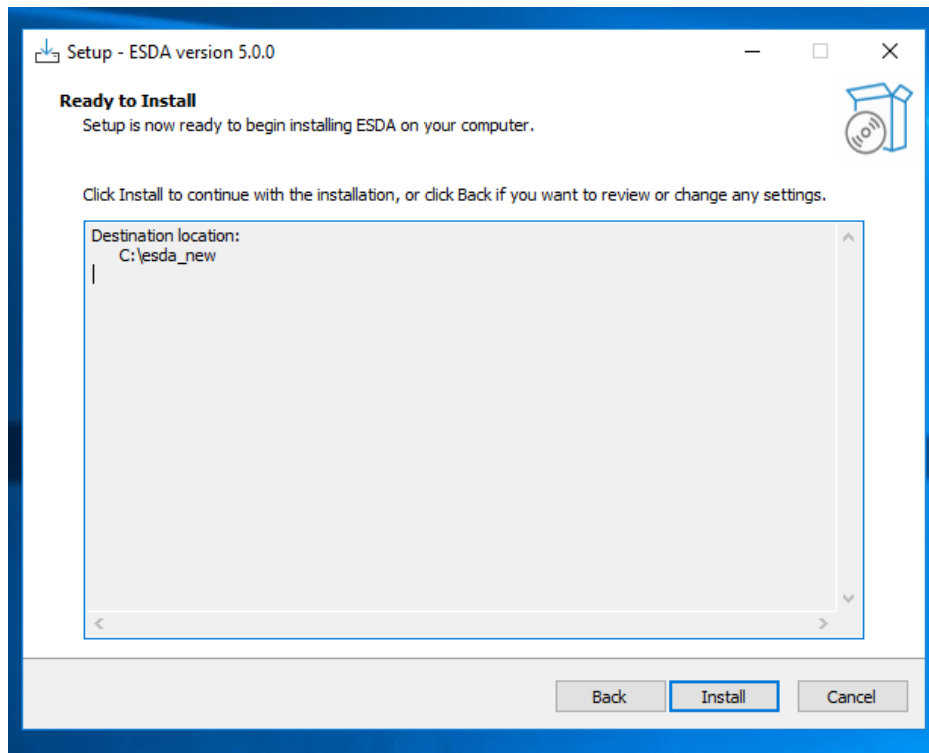
2) The ESDA v5.0.x will be installed in a default folder, click “Next”.

Note:

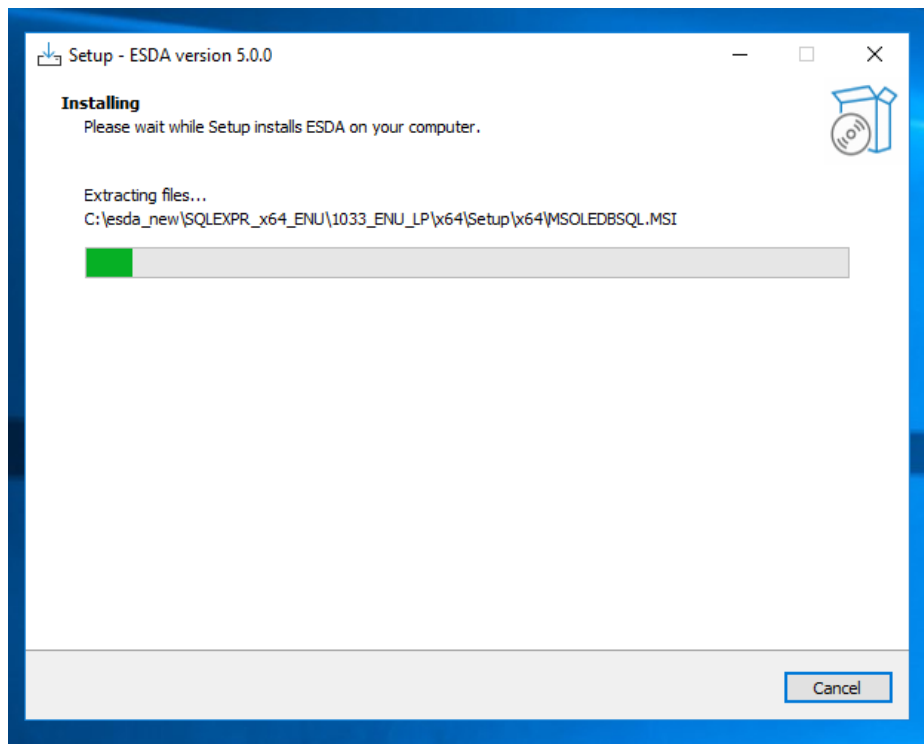
System Administrator can change the destination folder by clicking the “Browse” button.



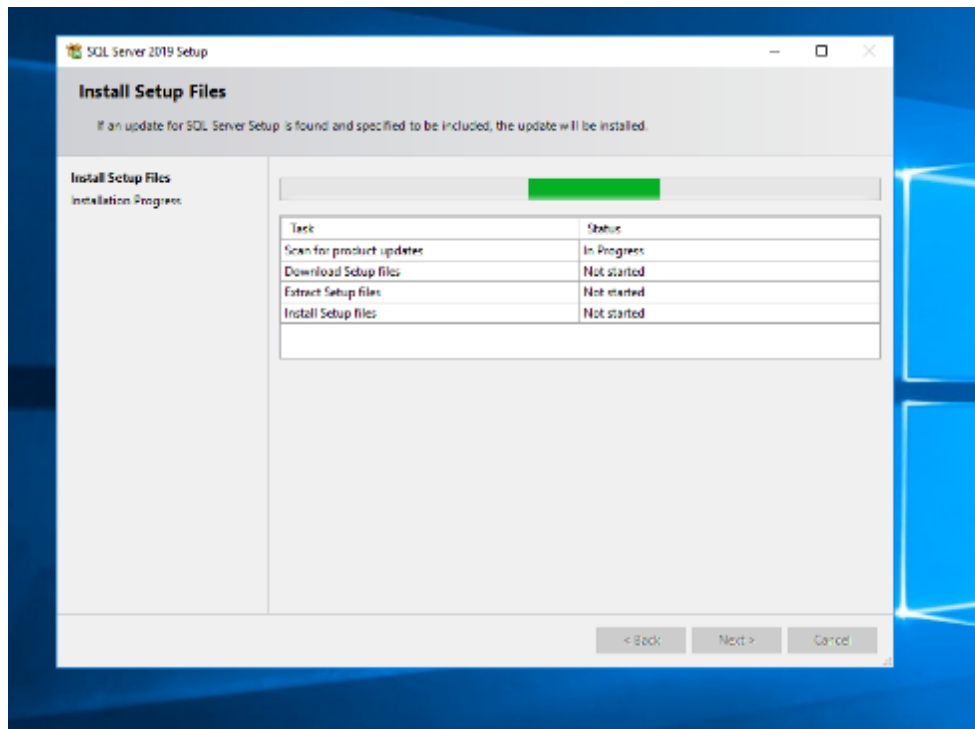
3) Click “Install” to start the installation.



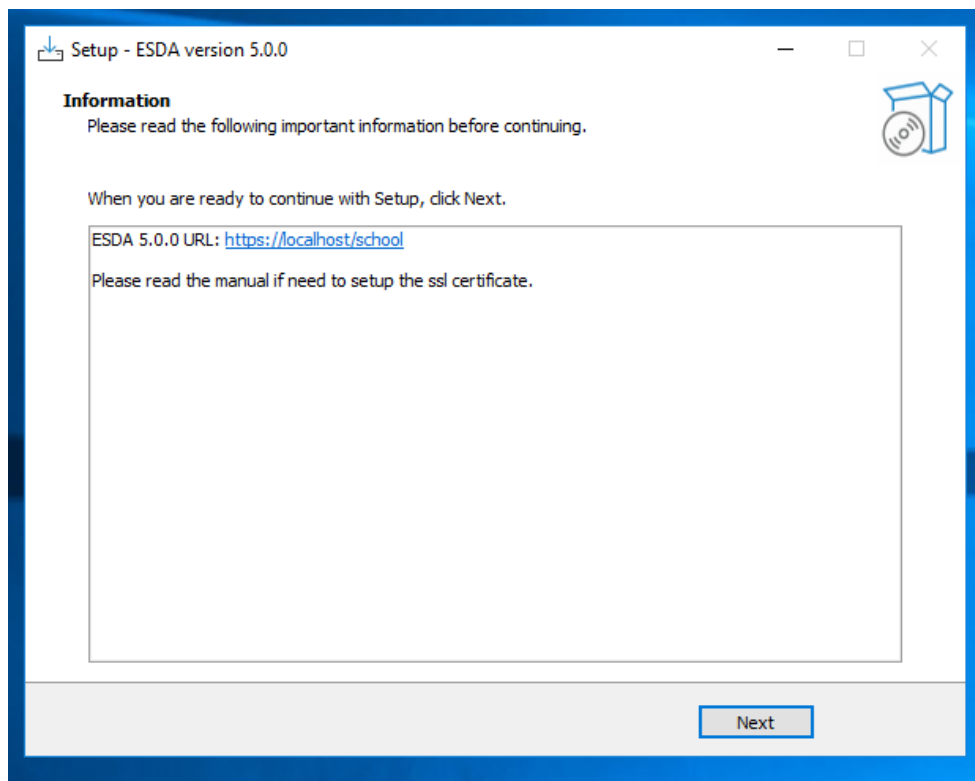
4) Installing ESDA v5.0.x.



5) Installing the MSSQL.

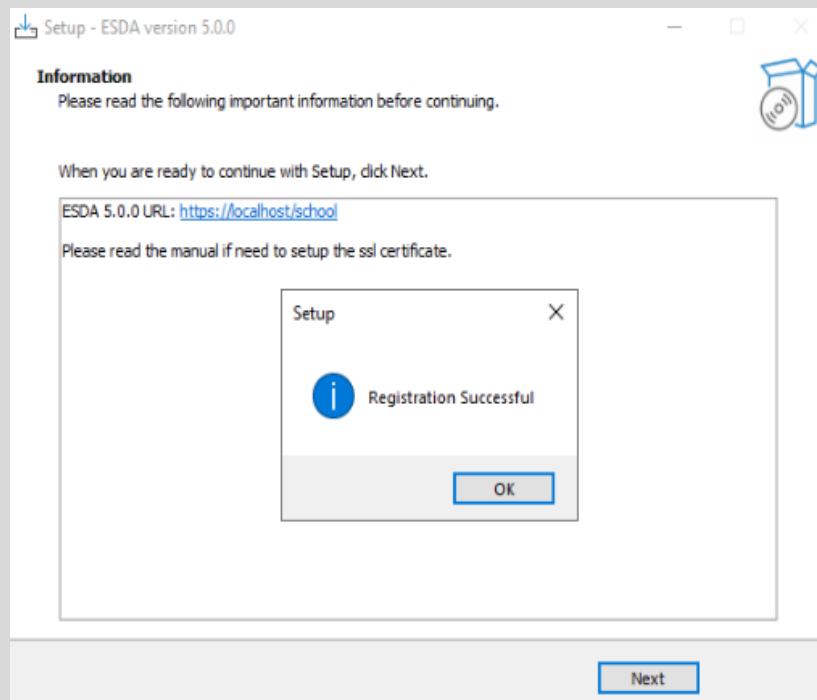


6) Click “Next” when the installation is completed.

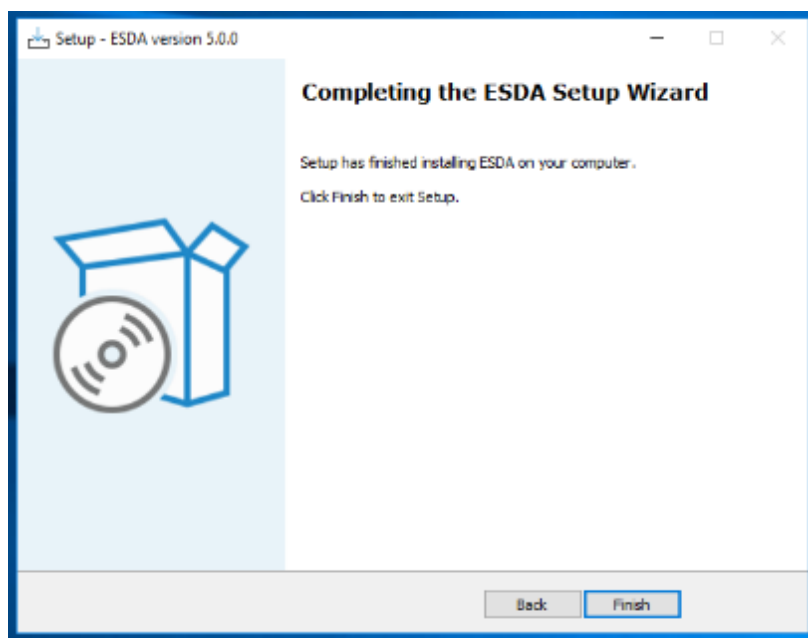


Note:

If ESDA v4.x.x is detected on the same server during installation, ESDA v5.0.x will be registered automatically.



7) Click “Finish” to close the installation programme.

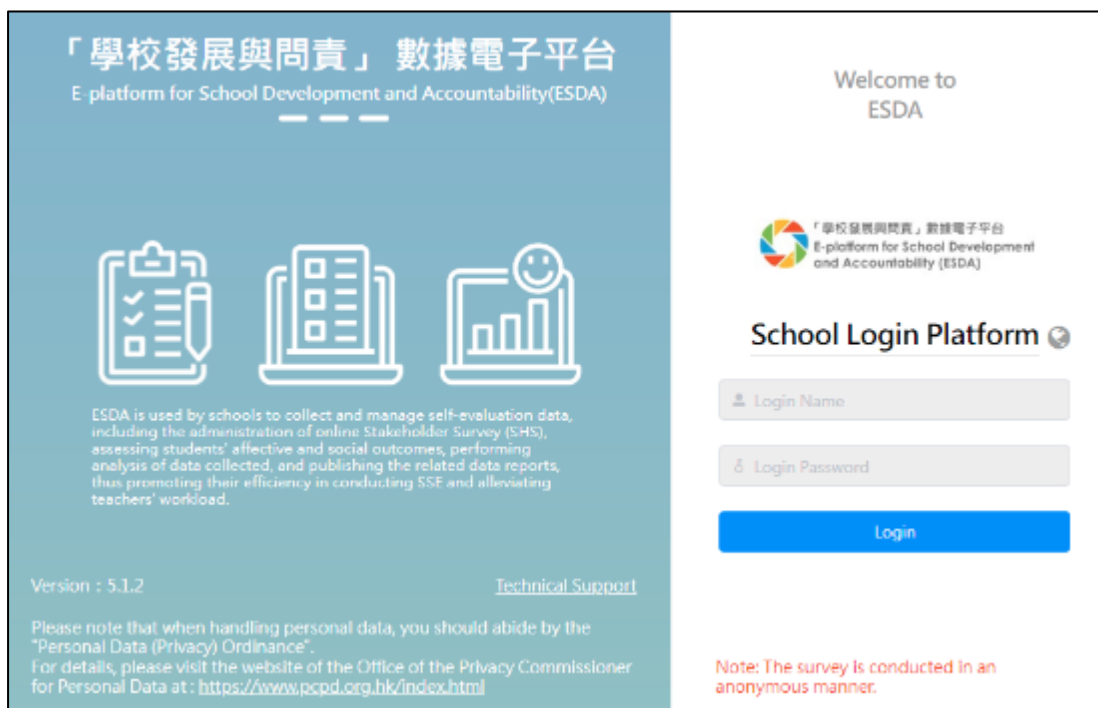


8) Restart the Windows Server after the installation is completed.

Chapter 2 Testing after Installation

2.1 Login Test

- 1) Login as an Administrator to the Windows Server where ESDA v5.0.x is installed.
- 2) Launch a supported browser (e.g. Google Chrome, Mozilla Firefox, Microsoft Edge, etc.) to “**https://127.0.0.1/school**” or “**https://<IP address or domain name>/school**”.
- 3) Login as a System Administrator to the ESDA v5.0.x system.



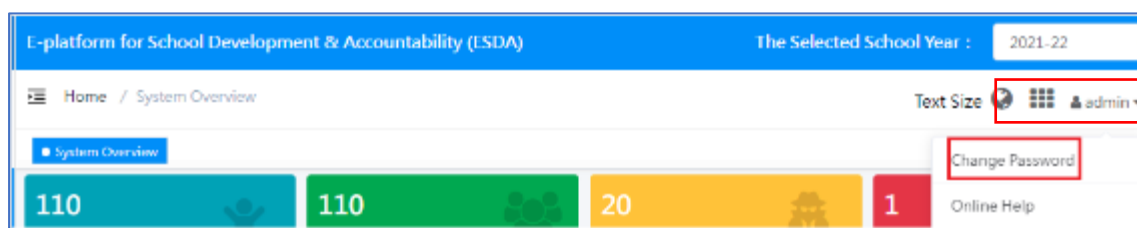
Note:

If ESDA cannot be accessed after installation, please check again whether the port used (e.g. default port 443) for ESDA v5.0.x is available. Please refer to Appendix 3 for details.

2.2 Login by Default User Account

The default username of a System Administrator account is **admin** and the password is **P@ssw0rd**. For security reason, please change the password of the default administrator account at once. Besides, all the user passwords used in ESDA v4.6.0 or before are not applicable for ESDA v5.0.x system. The System Administrator have to use the “Reset User Password” function in the “User Management” Module to assist all users in setting the passwords applicable for ESDA v5.0.x system. For details, please refer to Section 3.8 of the Operation Manual.

- 1) Click “admin” and then click “Change Password”.
- 2) Enter the “Old Password” and “New Password”, and then click “Confirm”.
- 3) The new password would be effective from the next login.



2.3 System Registration

System Administrator have to complete the registration for ESDA v5.0.x before using any functions in the system. System Administrator should obtain a registration key from the Indicators Section of the EDB for system registration so that the ESDA system could start be used. If the ESDA v4.6.0 and ESDA v5.0.x systems are installed on the same server, ESDA v5.0.x will be registered automatically. If the ESDA v4.6.0 and ESDA v5.0.x systems are installed on different servers, please send an email to the Indicators Section of EDB (indicators@edb.gov.hk) to request a registration key and follow the steps below for system registration.

- 1) Mouse over “System Tools” and then click “System Setting”.
- 2) Select the school level in “School Level” section.

- 3) Enter the registration key.
- 4) Click “Register”.

Note:

The registration key of ESDA v4.x.x is not applicable to ESDA v5.0.x.

The screenshot shows the 'School Badge Upload' and 'System Registration' sections. The 'School Badge Upload' section has 'Reset' and 'Upload' buttons, with a note: 'Upload image of 250 x 100 Pixels or 250% ratio size (JPG/JPEG/PNG file Format)'. The 'System Registration' section includes a 'School Level' dropdown menu, a 'Registration Key' field with five input boxes separated by hyphens, and a 'Register' button.

2.4 System Update

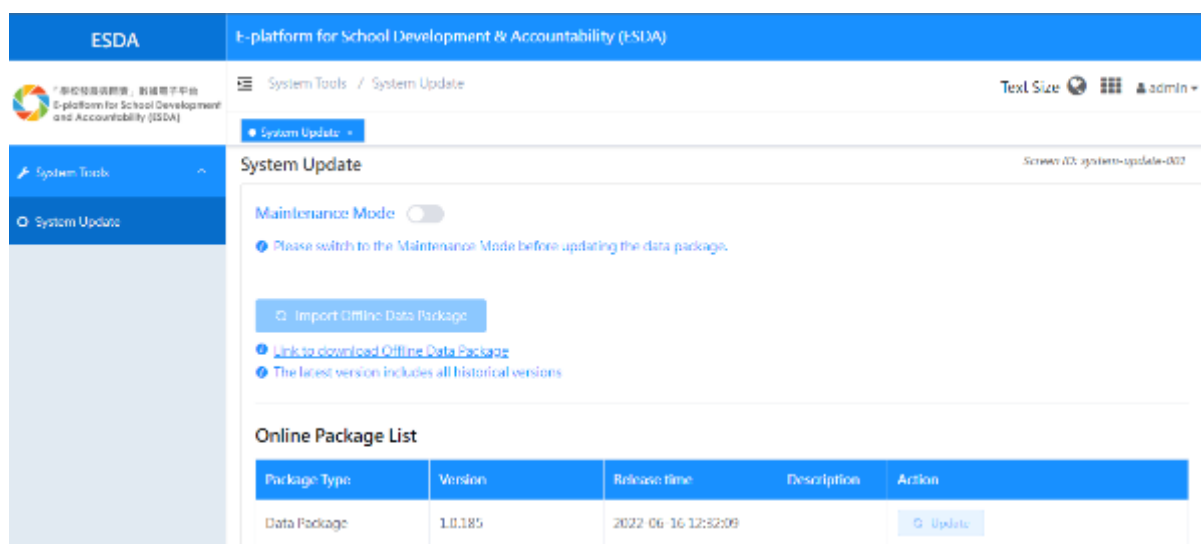
Please conduct a system update after the registration of ESDA v5.0.x.

- 1) Mouse over “System Tools” and then click “System Update”.
- 2) Switch on the “Maintenance Mode”.

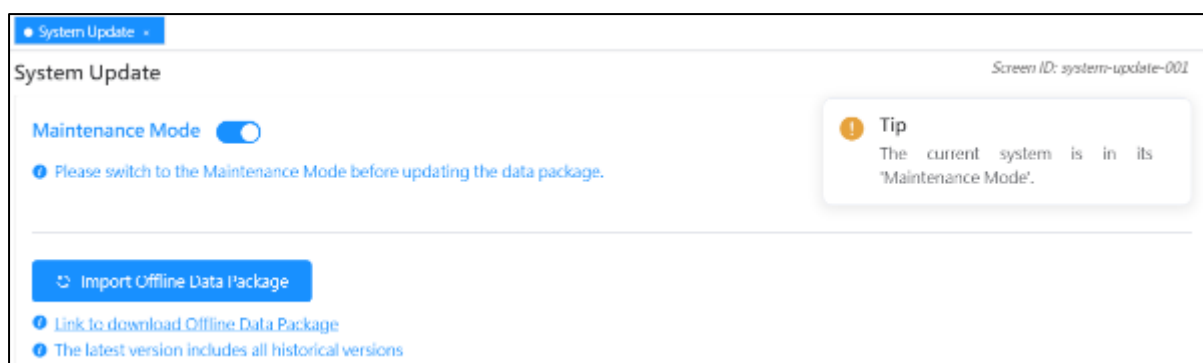
The screenshot shows the 'System Update' section. At the top, there are tabs for 'System Overview' and 'System Update'. Below the tabs, the 'System Update' section is active. It features a 'Maintenance Mode' toggle switch, which is currently turned off. A red box highlights the 'Maintenance Mode' label and the toggle. Below the toggle, there is a message: 'Please switch to the Maintenance Mode before updating the data package.' At the bottom, there is a button labeled 'Import Offline Data Package' and two links: 'Link to download Offline Data Package' and 'The latest version includes all historical versions'.

- 3) Click “Update” in the Online Package List section. “Updating” will be prompted when the system update is started. It takes about 15-20 minutes.

ESDA v5.3.x Installation and Data Migration Guide



4) Switch off the “Maintenance Mode” after the system update is completed.

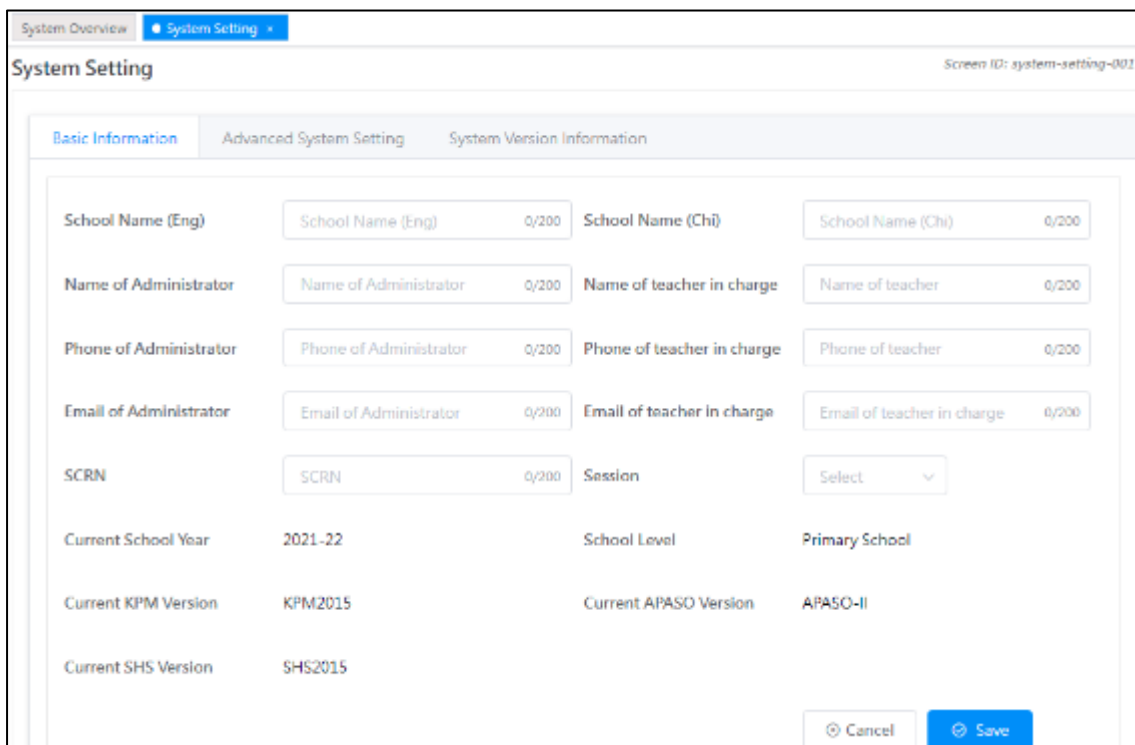


Chapter 3 System Setting

3.1 School Setting

The basic school information such as school name, SCRIN, school session etc. is recorded in the System Setting.

- 1) Mouse over “System Tools” and then click “System Setting.
- 2) Click “Basic Information” tab.
- 3) Enter the required information and then click “Save”.

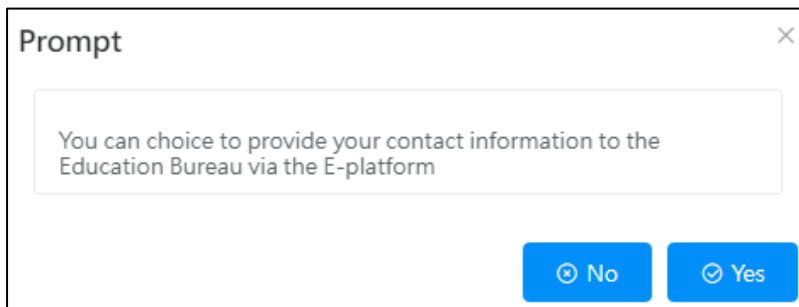


The screenshot shows the 'System Setting' window with the 'Basic Information' tab selected. The window has a title bar with 'System Overview' and 'System Setting' tabs. The 'System Setting' tab is active, and the 'Basic Information' sub-tab is selected. The form contains the following fields:

Field	Value	Field	Value
School Name (Eng)	School Name (Eng) 0/200	School Name (Chi)	School Name (Chi) 0/200
Name of Administrator	Name of Administrator 0/200	Name of teacher in charge	Name of teacher 0/200
Phone of Administrator	Phone of Administrator 0/200	Phone of teacher in charge	Phone of teacher 0/200
Email of Administrator	Email of Administrator 0/200	Email of teacher in charge	Email of teacher in charge 0/200
SCRIN	SCRIN 0/200	Session	Select
Current School Year	2021-22	School Level	Primary School
Current KPM Version	KPM2015	Current APASO Version	APASO-II
Current SHS Version	SHS2015		

At the bottom right, there are 'Cancel' and 'Save' buttons.

- 4) School may choose to provide relevant contact information to the EDB. If click “Yes”, the contact information will be saved at both school and EDB server. If click “No”, the contact information will be saved at the school server only.



The screenshot shows a 'Prompt' dialog box with a close button (X) in the top right corner. The text inside the dialog box reads:

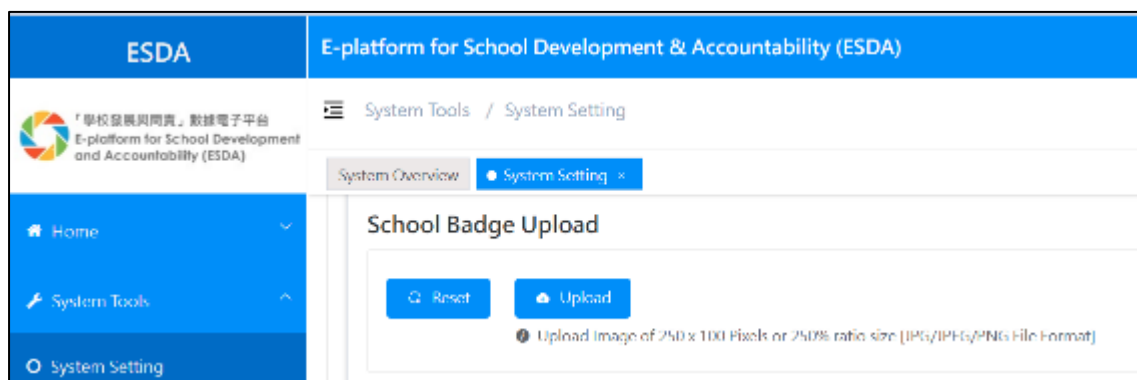
You can choice to provide your contact information to the Education Bureau via the E-platform

At the bottom, there are two buttons: 'No' and 'Yes'.

3.2 Upload School Badge

System Administrator can upload the school badge at “System Setting”.

- 1) Mouse over “System Tools” and then click “System Setting”.
- 2) Click “Basic Information” tab.
- 3) Click “Upload” to upload in “School Badge Update” section.
- 4) Select the school badge image file and click “Open”.
- 5) System Administrator may click “Reset” to set the badge to the default picture.



3.3 School Year Setting

System Administrator should set an appropriate school year as the “Current School Year”.

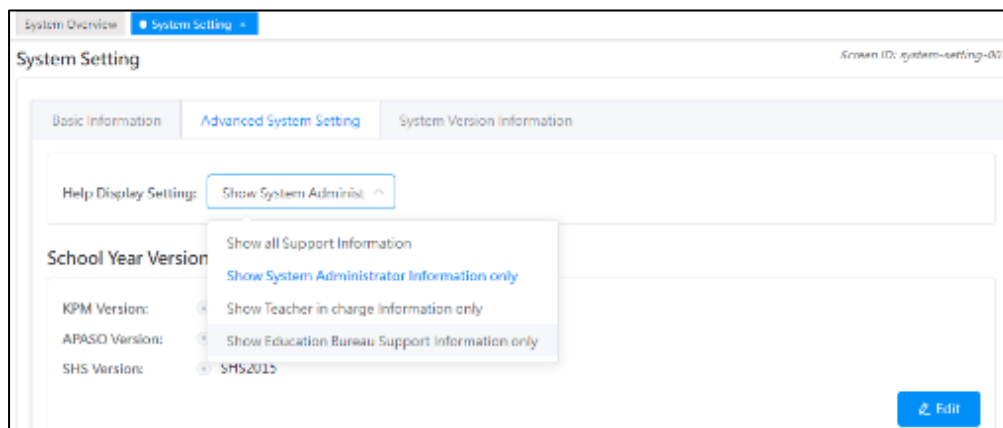
- 1) Mouse over “System Tools” and then click “School Year Setting”.
- 2) Select an appropriate school year as “Current School Year”.

School Year Setting				
School Year Name	KPM Version	APASO Version	SHS Version	Current School Year
2021-22	KPM2015	APASO-II	SHS2015	<input checked="" type="checkbox"/>
2020-21	KPM2015	APASO-II	SHS2015	<input type="checkbox"/>
2019-20	KPM2015	APASO-II	SHS2015	<input type="checkbox"/>

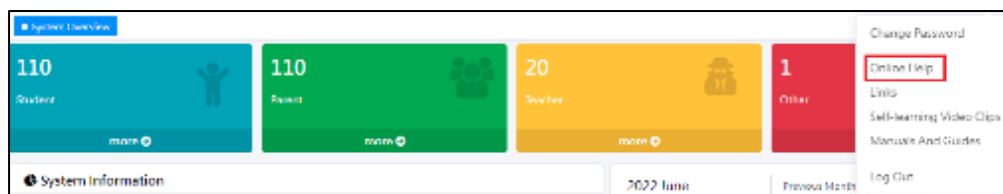
3.4 Advanced System Setting

System Administrator can choose the information to be displayed at the “Online Help”.

- 1) Mouse over “System Tools” and then click “System Setting”.
- 2) Click “Advanced System Setting” tab.
- 3) Select the “Help Display Setting” type.



- 4) All users can get the related help information from the “Online Help”.



3.5 System Version Information

System Administrator can check the system version information from “System Setting”.

- 1) Mouse over “System Tools” and then click “System Setting”.
- 2) Click the “System Version Information” tab to check the related information.

The screenshot shows the 'System Setting' page with the 'System Version Information' tab selected. It displays a table with version and installation details.

	Local Version	Installation Time	Latest Version	Published Time
ESDA System Version	v5.1.2	2022-05-26 15:59:16	v5.1.2	2022-05-26 17:22:54
Package Version	v1.0.220	2022-05-26 09:00:02	v1.0.220	2022-05-25 18:14:53

3.6 Set up e-Certificate

In order to set up ESDA v5.0.x to run on port 443, a valid e-Certificate is required. Schools can purchase a valid e-Certificate from a recognised Certification Authority (CA) or create a self-signed certificate:

A) Using an e-Certificate that purchase from a Certification Authority

- 1) **Make sure the purchased e-Certificate is in PKCS#12 format (the extension is “.p12”)**. If the e-Certificate is not in PKCS#12 format, please use other tools to convert the e-Cert to the PKCS#12 format first, for example using openssl to convert the e-Cert to “.crt” file to “.p12” file. Please refer to the website <https://www.openssl.org/> for download and use openssl.

Notes:

If schools use openssl version 3.0.x or above to convert the e-Certificate from “.crt” format to “.p12” format, schools should add the options -legacy and -provider-path “path of legacy.dll installed by openssl” into the command to prevent errors from the convention of “.keystore” file in following steps. (e.g. openssl pkcs12 -export -out cert.p12 -inkey key.key -in cert.crt -certfile cacert.crt -legacy -provider-path “C:\Program Files\OpenSSL-Win64\bin”)

- 2) Use a System Administrator account to login to the server where the ESDA v5.0.x is installed.
- 3) Copy the e-Certificate in PKCS#12 format (e.g. “cert.p12”) to the server (e.g. C:\temp\cert.p12).
- 4) Open “Windows Command Prompt” and enter the following command to convert the e-Certificate in PKCS#12 format into “.keystore”

```
"%JAVA_HOME%\bin\keytool" -importkeystore -srckeystore  
C:\temp\cert.p12 -srcstoretype PKCS12 -destkeystore C:\temp\keystore -  
deststoretype JKS
```

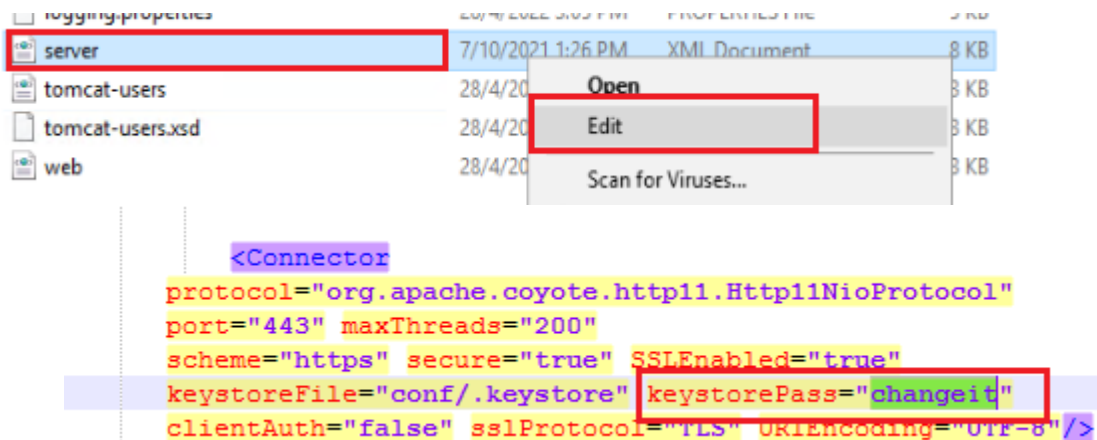
- 5) Enter a new password for the “.keystore” file, **the password should be the same as the password for the e-Certificate in PKCS#12 format.**

```
C:\Users\Administrator>"%JAVA_HOME%\bin\keytool" -importkeystore -srckeystore C:\temp\cert.p12 -srcstoretype PKCS12 -des  
tkeystore C:\temp\keystore -deststoretype JKS  
Importing keystore C:\temp\cert.p12 to C:\temp\keystore...  
Enter destination keystore password:  
Re-enter new password:
```

- 6) Enter the password for the e-Certificate in PKCS#12 format.

```
C:\Users\Administrator>%JAVA_HOME%\bin\keytool -importkeystore -srckeystore C:\temp\cert.p12 -srcstoretype PKCS12 -destkeystore C:\temp\keystore -deststoretype JKS
Importing keystore C:\temp\cert.p12 to C:\temp\keystore...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
```

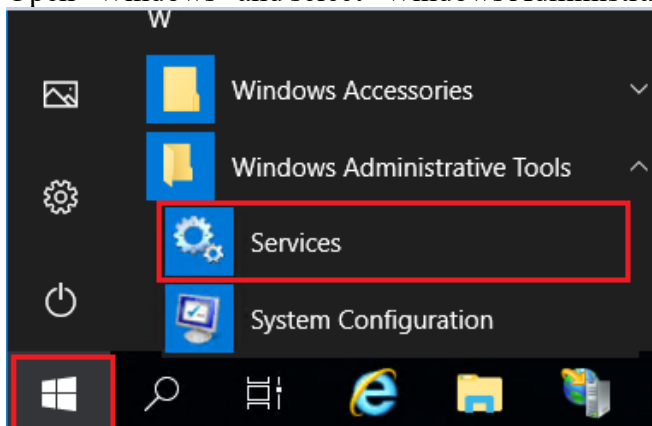
- 7) Please copy the certificate “.keystore” in the above path (e.g. C:\temp\keystore) to the installation path “C:\esda_new\apache-tomcat-9.0.xx\conf”.
- 8) Edit the Apache Tomcat configuration file (e.g. C:\esda_new\Apache_Tomcat_9.0\conf\server.xml) with a text editor (e.g. Notepad) and change the attribute keystorePass from “changeit” to the password entered in step5.



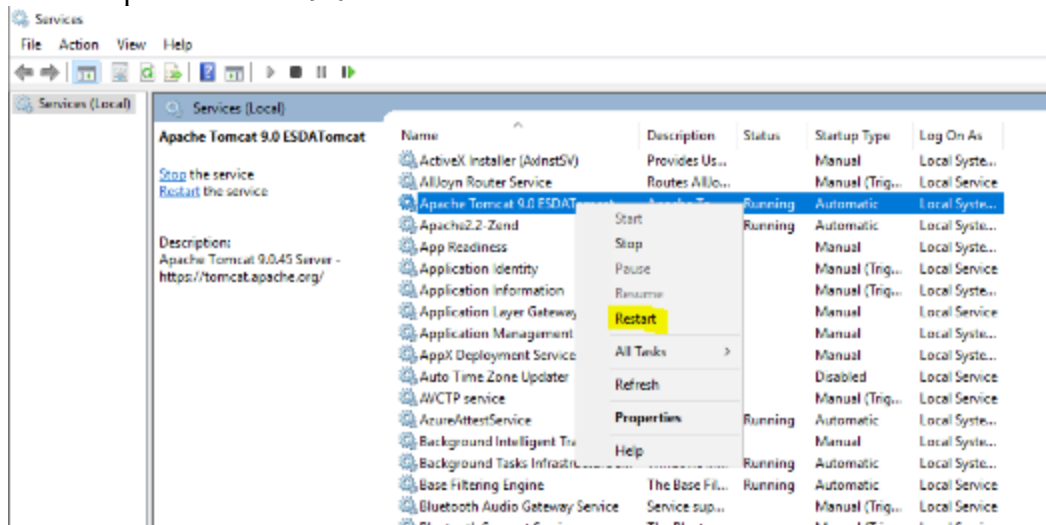
Notes:

If you need to re-establish the e-Certificate in PKCS#12 format to “.keystore” file, please first delete the certificate “.keystore” in the path of step 7 and start over with step 4.

- 9) Open “Windows” and select “Windows Administrative Tools”, then click “Services”.



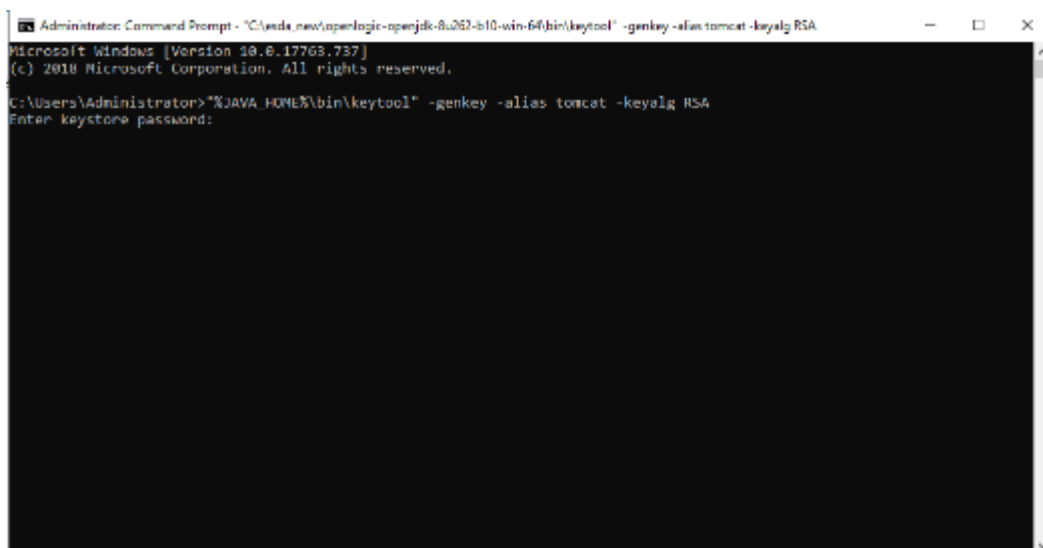
- 10) Select “Apache Tomcat 9.0 ESDA” and then click “Restart”.



B) Creating a self-signed e-Certificate

- 1) Login as a System Administrator to the server where the ESDA v5.0.x system is installed.
- 2) Enter the following command at “Windows Command Prompt”:
“%JAVA_HOME%\bin\keytool” -genkey -alias tomcat -keyalg RSA -ext san=dns:<domain name>”
(e.g. “%JAVA_HOME%\bin\keytool” -genkey -alias tomcat -keyalg RSA -ext san=dns:esda.schoola.edu)

Enter a password, e.g. “password”



3)

Enter the password for the steps above:
Enter the domain name, e.g. esda.schoola.edu
Enter the organizational unit, e.g. esda
Enter the organization, e.g. Testing Primary School A
Enter the city, e.g. Hong Kong
Enter the state, e.g. China
Enter the country code (two-letter), e.g. CN

```
C:\Users\Administrator>"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA -ext san=dns:esda.schoola.edu
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: esda.schoola.edu
What is the name of your organizational unit?
[Unknown]: esda
What is the name of your organization?
[Unknown]: Testing Primary School A
What is the name of your City or Locality?
[Unknown]: Hong Kong
What is the name of your State or Province?
[Unknown]: China
What is the two-letter country code for this unit?
[Unknown]: CN
```

4)

Enter "yes" to confirm the input.

```
C:\Users\Administrator>"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA -ext san=dns:esda.schoola.edu
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: esda.schoola.edu
What is the name of your organizational unit?
[Unknown]: esda
What is the name of your organization?
[Unknown]: Testing Primary School A
What is the name of your City or Locality?
[Unknown]: Hong Kong
What is the name of your State or Province?
[Unknown]: China
What is the two-letter country code for this unit?
[Unknown]: CN
Is CN=esda.schoola.edu, OU=esda, O=Testing Primary School A, L=Hong Kong, ST=China, C=CN correct?
[no]: yes
```

5)

Enter the password for the steps above, e.g. "password"

```
C:\Users\Administrator>"%JAVA_HOME%\bin\keytool" -genkey -alias tomcat -keyalg RSA -ext san=dns:esda.schoola.edu
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: esda.schoola.edu
What is the name of your organizational unit?
[Unknown]: esda
What is the name of your organization?
[Unknown]: Testing Primary School A
What is the name of your City or Locality?
[Unknown]: Hong Kong
What is the name of your State or Province?
[Unknown]: China
What is the two-letter country code for this unit?
[Unknown]: CN
Is CN=esda.schoola.edu, OU=esda, O=Testing Primary School A, L=Hong Kong, ST=China, C=CN correct?
[no]: yes

Enter key password for <tomcat>
(RETURN if same as keystore password):
Re-enter new password:
```

6)

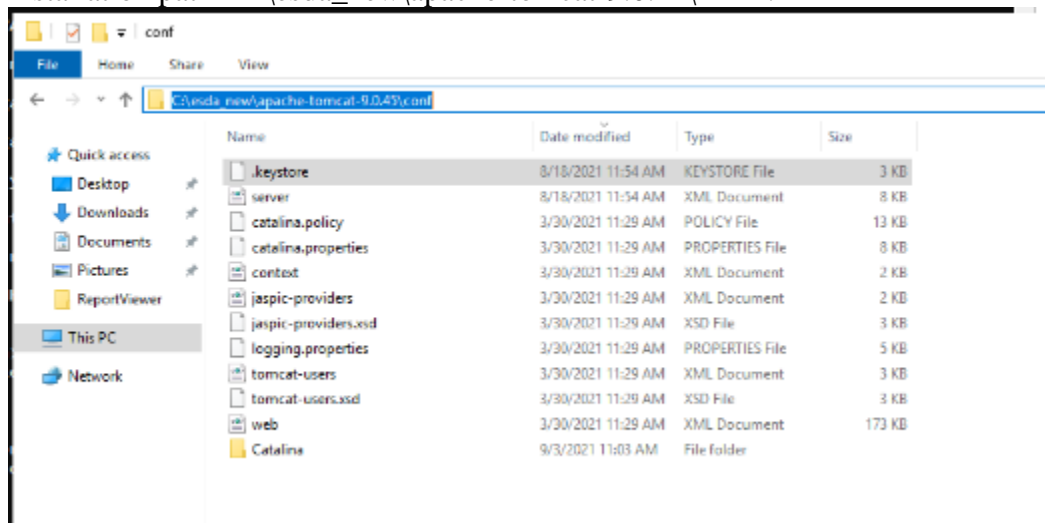
The certificate is generated in the above path (e.g. C:\Users\Administrator)

```
C:\Users\Administrator>%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA -ext san=dns:esda.schoola.edu
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: esda.schoola.edu
What is the name of your organizational unit?
[Unknown]: esda
What is the name of your organization?
[Unknown]: Testing Primary School A
What is the name of your City or Locality?
[Unknown]: Hong Kong
What is the name of your State or Province?
[Unknown]: China
What is the two-letter country code for this unit?
[Unknown]: CN
Is CN=esda.schoola.edu, OU=esda, O=Testing Primary School A, L=Hong Kong, ST=China, C=CN correct?
[no]: yes

Enter key password for <tomcat>
(RETURN if same as keystore password):
Re-enter new password:

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format
using "keytool -importkeystore -srckeystore C:\Users\Administrator\.keystore -destkeystore C:\Users\Administrator\.keystore
-deststoretype pkcs12".
```

7) Copy “.keystore” from the above path (e.g. C:\Users\Administrator\.keystore) to the installation path “C:\esda_new\apache-tomcat-9.0.xx\conf”.



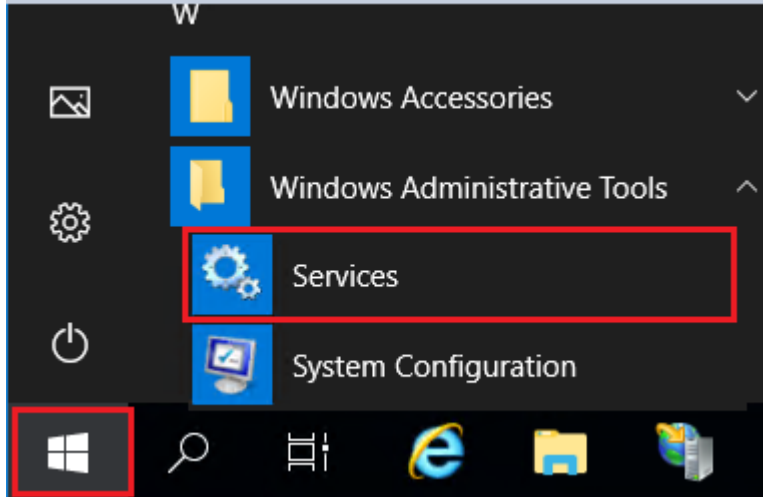
8) Edit Apache Tomcat configuration by using a word processor (e.g. Notepad) (e.g. “C:\esda_new\Apache_Tomcat_9.0\conf\server.xml”). Change the attribute “keystorePass” from “changeit” to the password entered in step 5 (e.g. password).

```
<Connector
protocol="org.apache.coyote.http11.Http11NioProtocol"
port="443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="conf/.keystore" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS" URIEncoding="UTF-8"/>
```

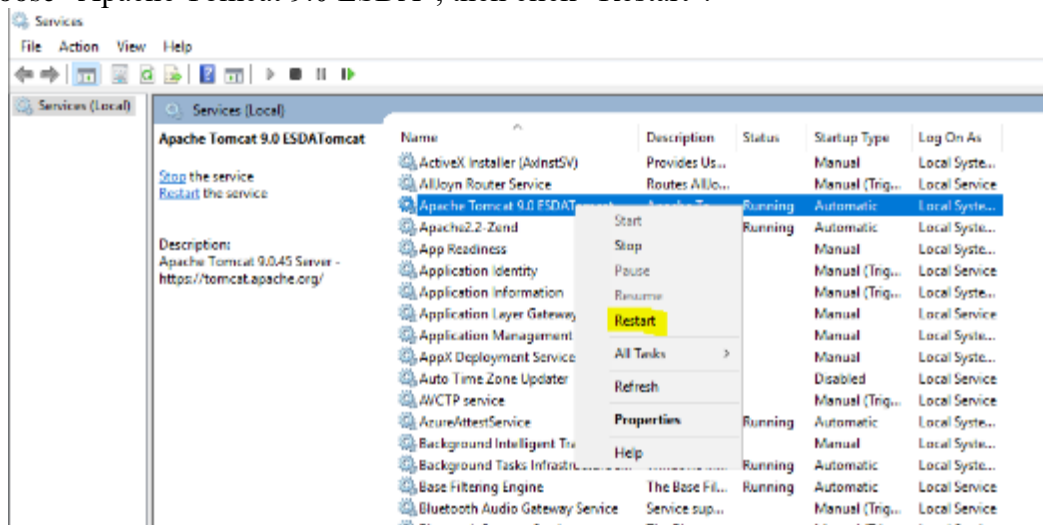
Note:

To re-establish a self-signed e-Certificate, please delete the e-Certificate, “.keystore” generated in the path of step 6 and then restart from step 2.

- 9) Open “Windows” and select “Windows Administrative Tools”, and click “Services”.

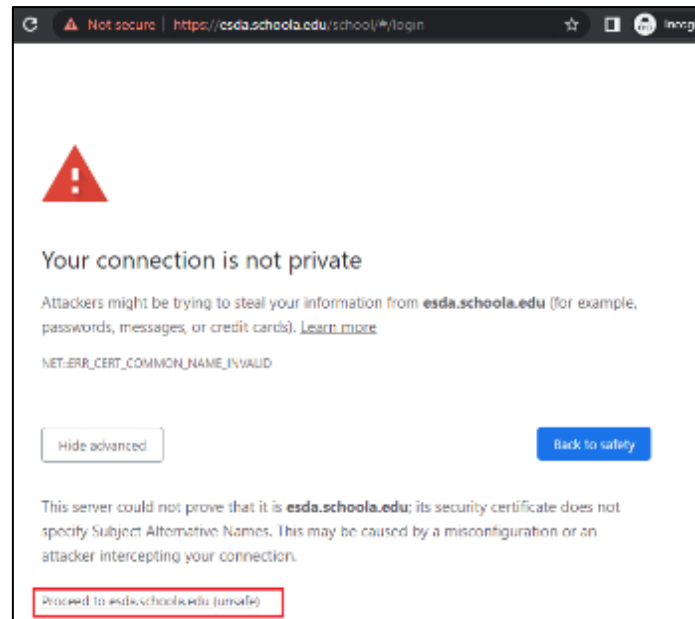


- 10) Choose “Apache Tomcat 9.0 ESDA”, then click “Restart”.



Note:

As the self-signed e-Certificate is not signed by a recognised CA, the website will be marked as “Not Secure” by the browser when users enter ESDA website (for example, the following screen will appear when using Google Chrome). Users must click “Proceed to” to access the website or refer to Appendix 2 to set up the self-signed e-Certificate at the client side.

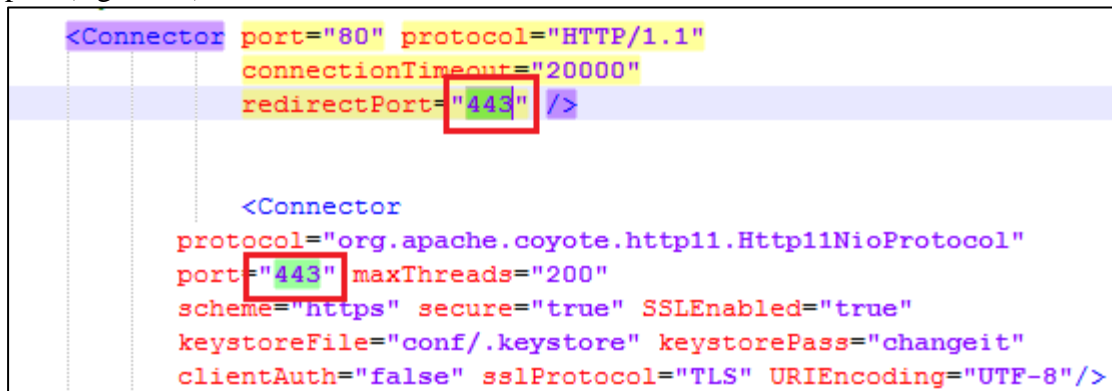


Please consider purchasing a valid e-Certificate from a recognised Certification Authority (“CA”) (e.g. Hongkong Post) to improve the security.

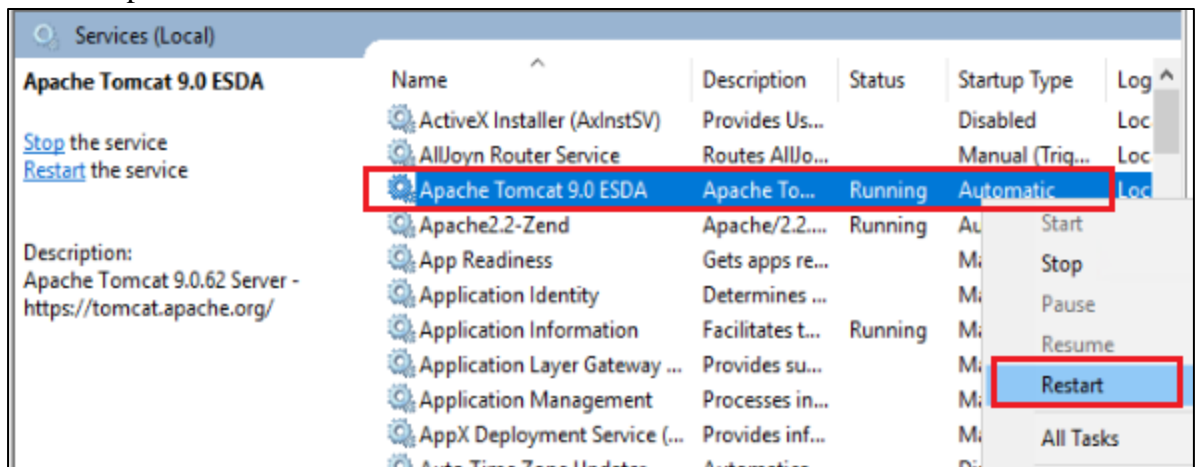
Appendix 1 Setup ESDA to Use Other Port

The ESDA system uses the “Port 443” by default. If the server has used the “Port 443” for other purposes, System Administrator can follow the steps below to set ESDA to use another port.

- 1) Follow the steps in Chapter 2 to install ESDA.
- 2) Edit Apache Tomcat configuration file (e.g. C:\esda_new\Apache_Tomcat_9.0\conf\server.xml), change the “Port 443” to other port (e.g. 8443).



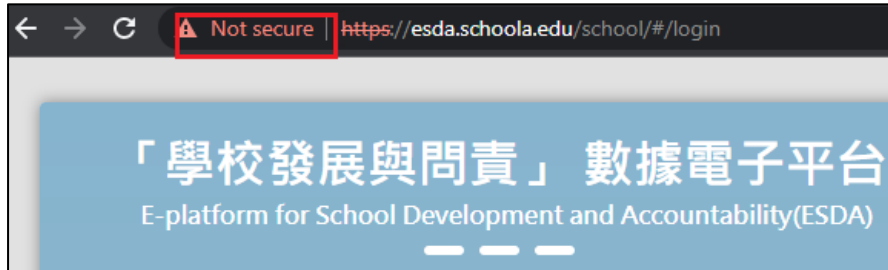
- 3) Restart Apache Tomcat server



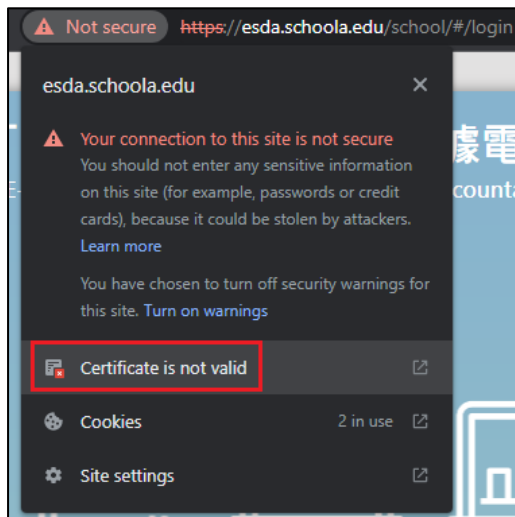
- 4) Follow the steps in Section 3.1 to test the system with the new port. (e.g. https://127.0.0.1:8443/school).

Appendix 2 Setup Self-signed e-Certificate at Client Side

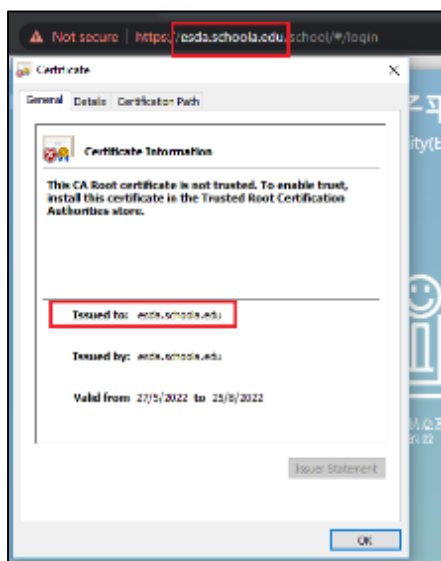
- 1) When accessing the website by Google Chrome, the website will be marked as “Not secure” by the browser. Click “Not secure”.



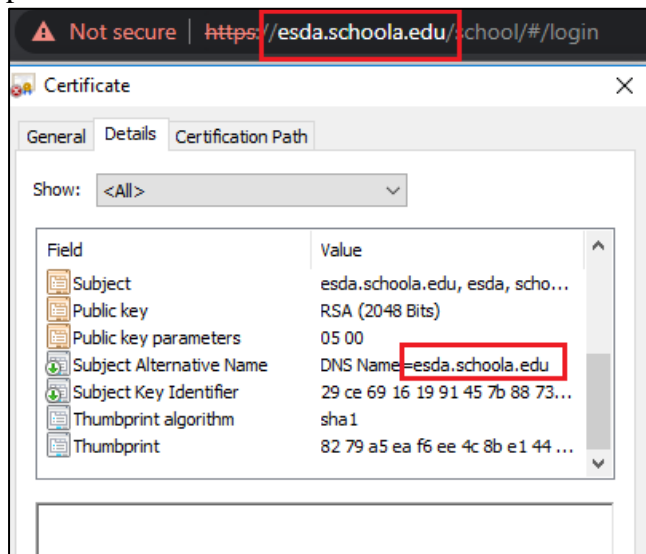
- 2) Click “Certificate is not valid”.



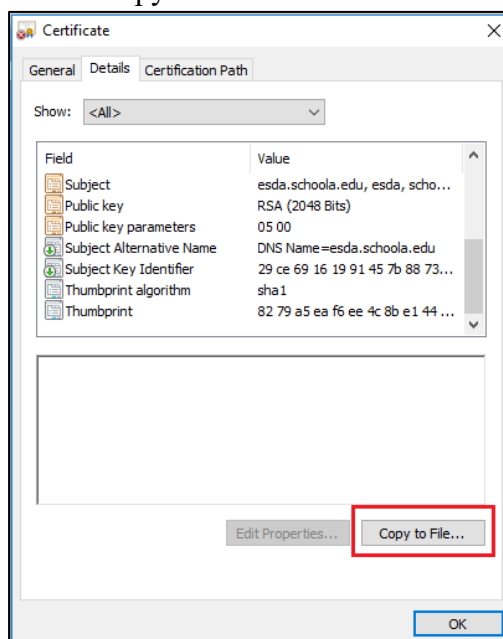
- 3) Ensure that the “Issued to” in the Certificate has the same domain name as the actual domain name. If the domain names are different, please refer to Section 2.3 to create a new Certificate.



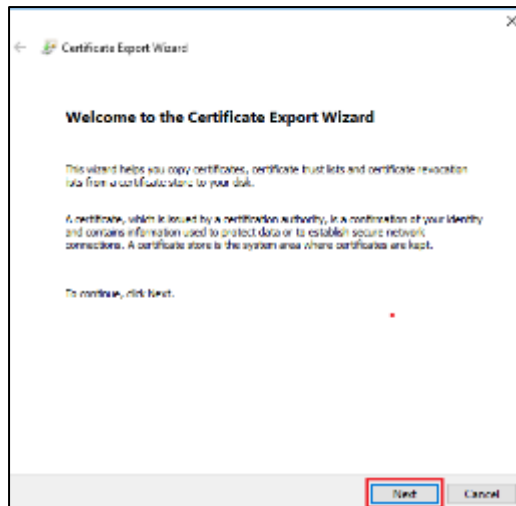
- 4) Click “Details” tab. Ensure the “Subject Alternative Name” in the Certificate has the same domain name as the actual domain name. If the domain names are different, please refer to Section 2.3 to create a new Certificate.



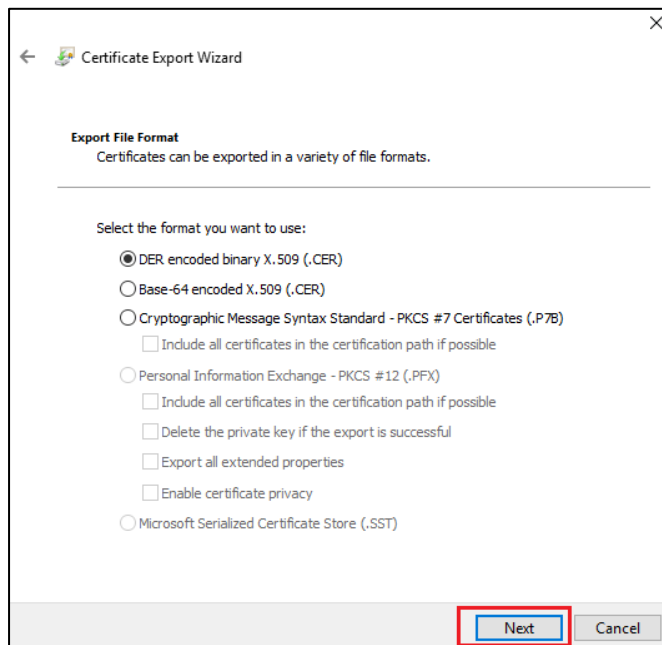
- 5) Click “Copy to File”.



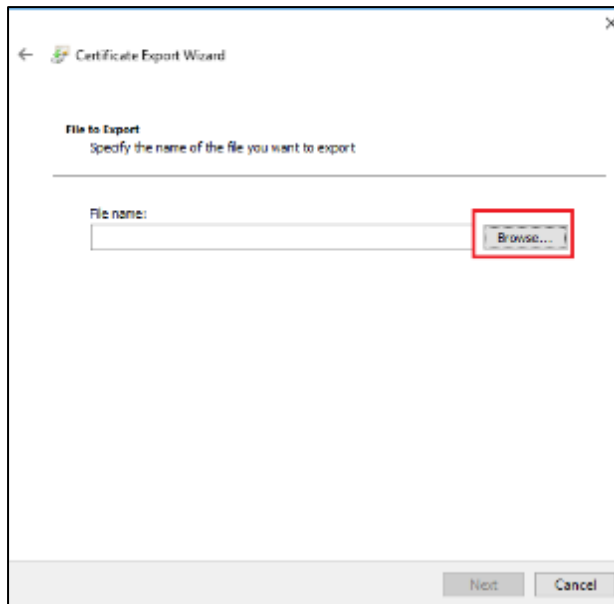
- 6) Click “Next”.



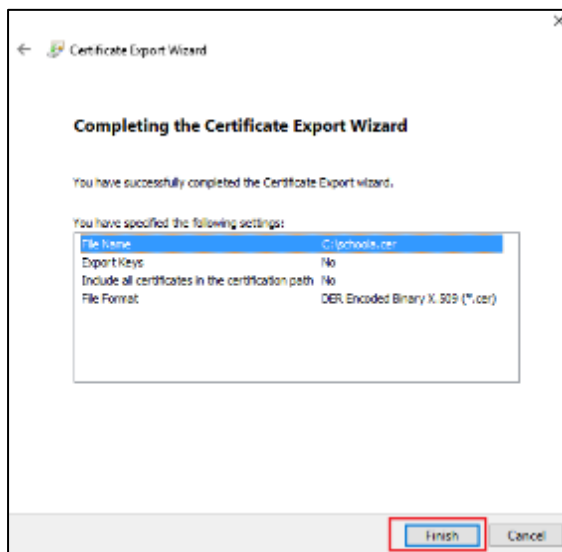
7) Click “Next”.



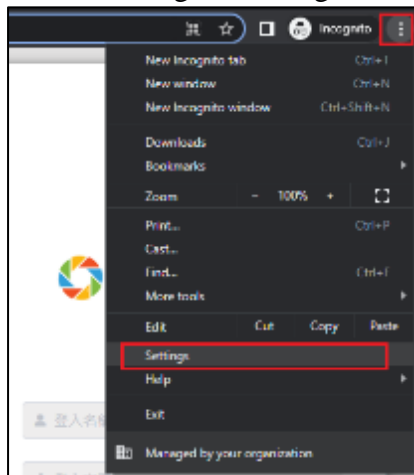
- 8) Click “Browse”, and save the Certificate to a specified path (e.g. C:\), and then click “Next”.



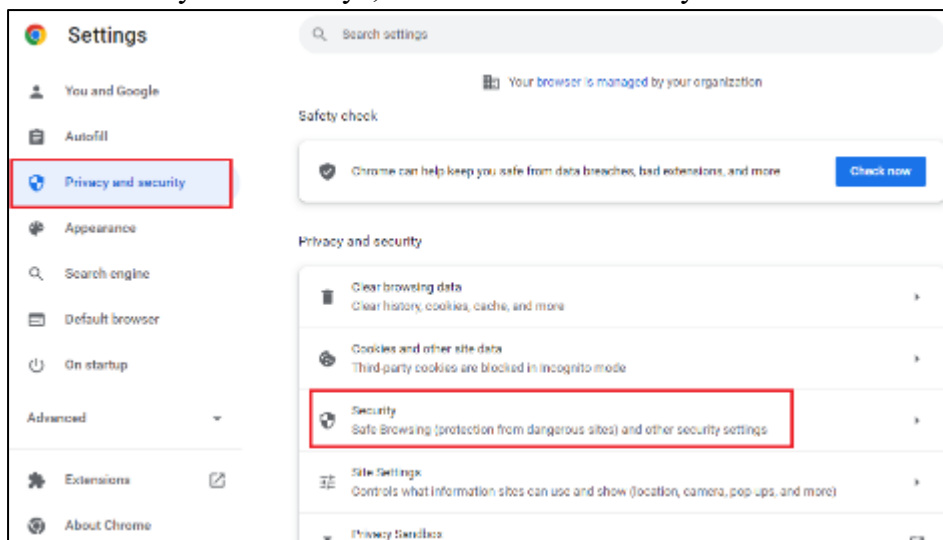
- 9) Click “Finish”.



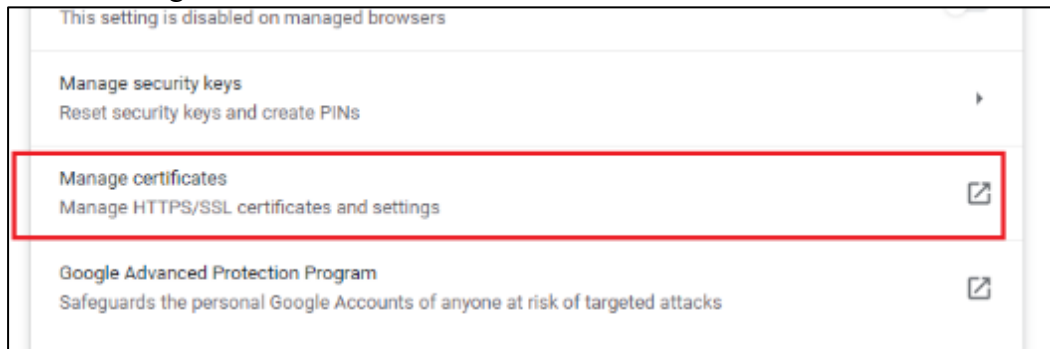
10) Go to “Settings” of Google Chrome.



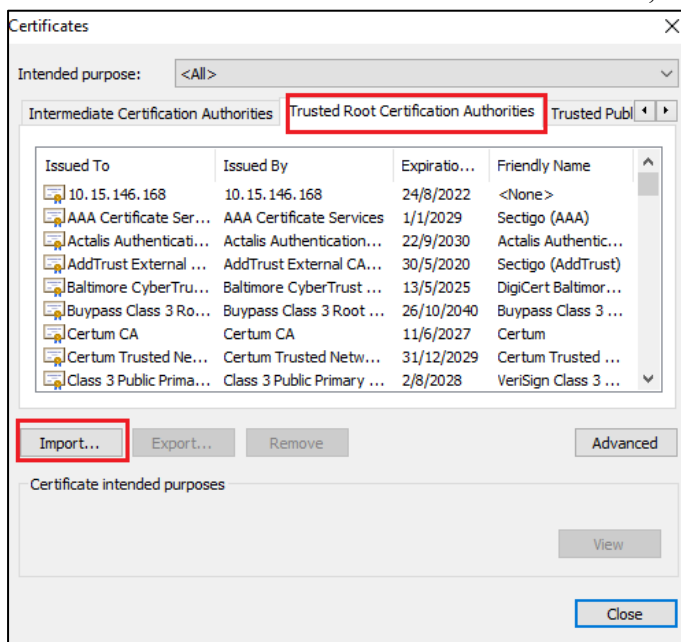
11) Click “Privacy and security”, and then click “Security”.



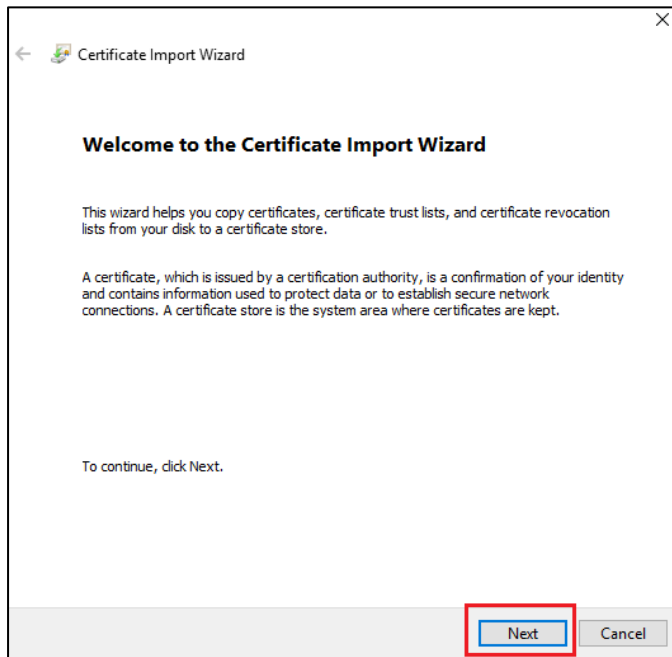
- 12) Click “Manage certificates”.



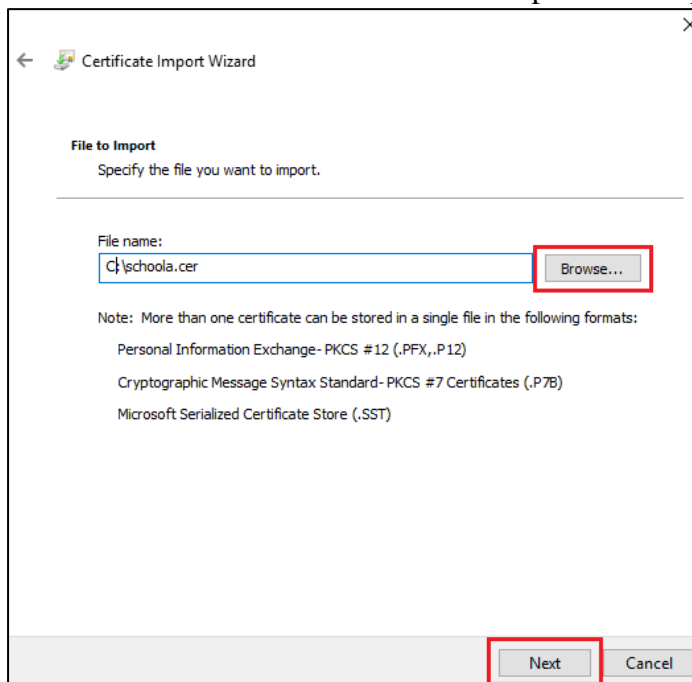
- 13) Click “Trusted Root Certification Authorities” tab, and then click “Import”.



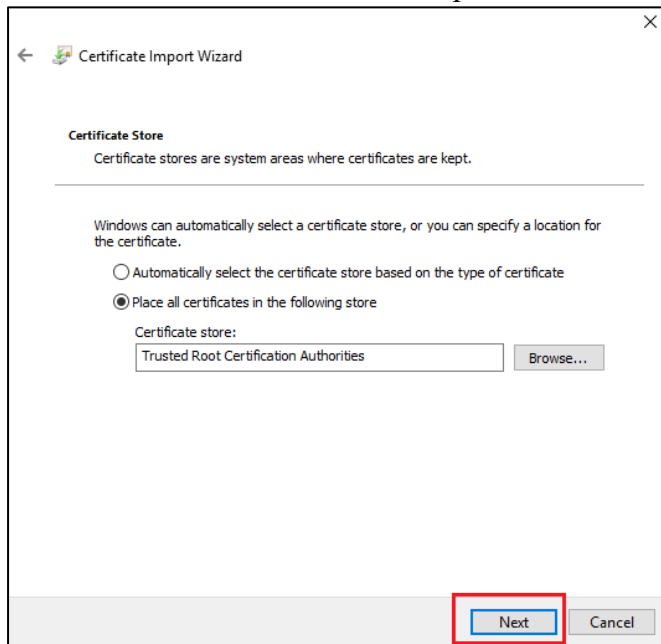
14) Click “Next”.



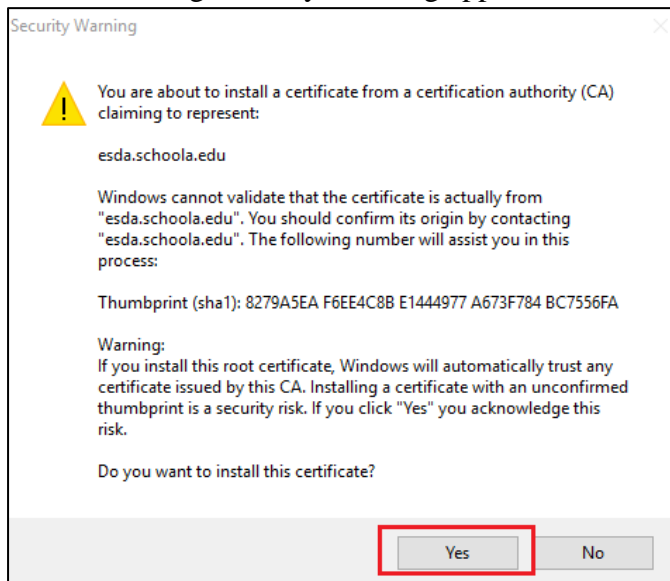
15) Click “Browse”. Select the certificate exported in step 8 and then click “Next”.



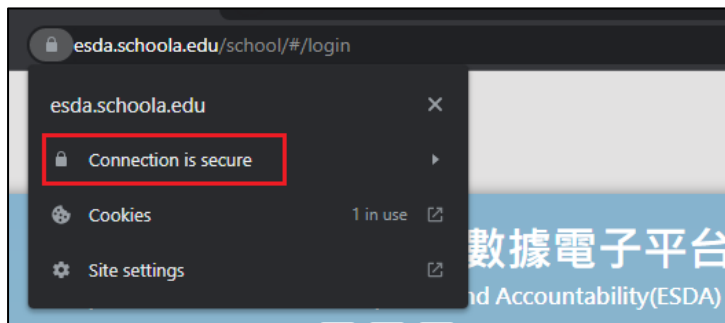
16) Click “Next”, and then click “Complete”.



17) If the following Security Warning appears, click “Yes”.



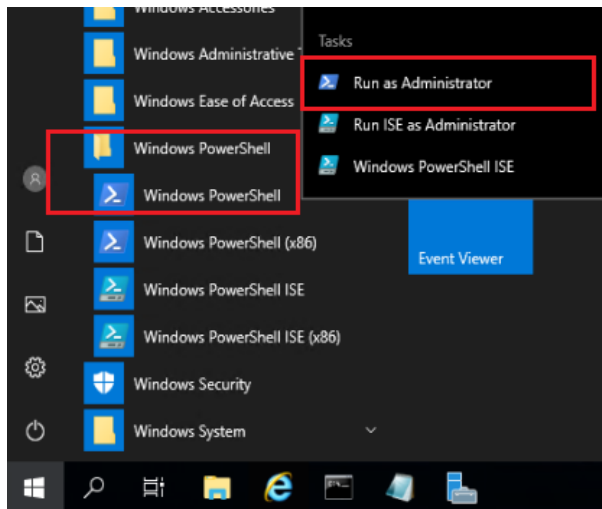
- 18) Restart the Google Chrome and access the website again. The browser will show that the connection is secure.



Appendix 3 Verify ESDA's port availability

If ESDA cannot be accessed after installation, System Administrator may follow the steps below to verify whether the port used (e.g. default port 443) by ESDA v5.0.x is available.

- 1) In a computer that can connect to ESDA v5.0.x, run the “Windows PowerShell” as an Administrator.



- 2) Execute the following command “Test-NetConnection [ESDA v5.0.x server IP address] -port [port]” (e.g. Test-NetConnection 10.15.7.91 -port 443) in “Windows PowerShell”.

```
PS C:\Windows\system32> Test-NetConnection 10.15.7.91 -port 443

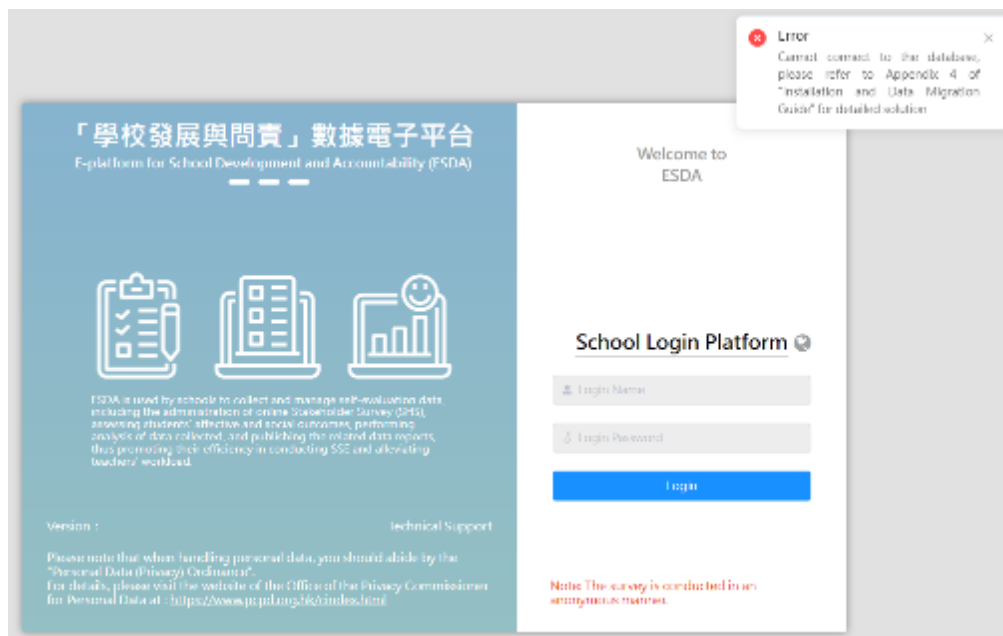
ComputerName           : 10.15.7.91
RemoteAddress           : 10.15.7.91
RemotePort              : 443
InterfaceAlias          : Ethernet0
SourceAddress           : 192.168.188.133
PingSucceeded           : True
PingReplyDetails (RTT) : 2 ms
TcpTestSucceeded        : True

PS C:\Windows\system32>
```

- 3) Ensure “TcpTestSucceeded” is “True”.
- 4) If “TcpTestSucceeded” is “False”, please check again whether the port used by ESDA v5.0.x is available or blocked by firewall, such as Windows Firewall, Antivirus software’s firewall or other firewall software installed in the server.

Appendix 4 Solution for the failure to connect SQL server

If ESDA cannot be accessed after installation or updating, System Administrator may follow the steps below to check ESDA v5.0.x.



A. After the first installation of ESDA, the message "unable to connect to the database" appears.

Did the school use the correct system installation tool?

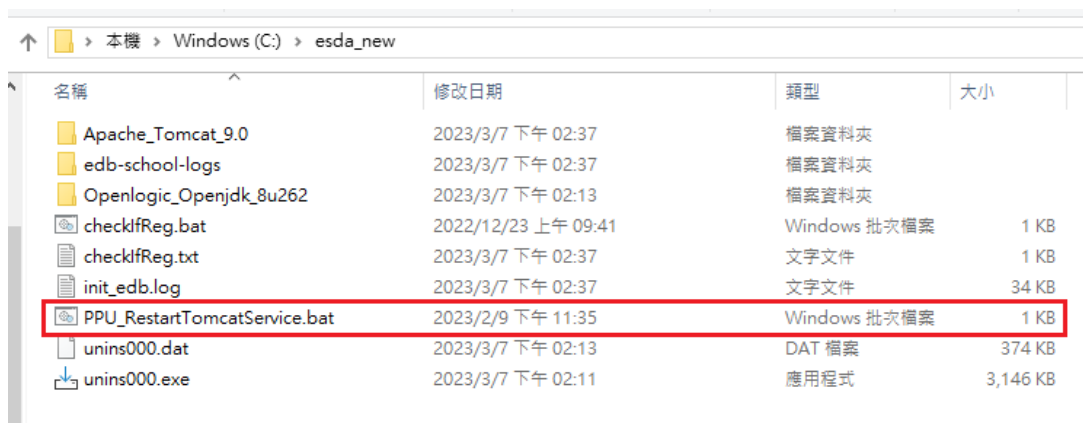
Full Installation Package (For Windows Server 2016 version or above / Windows 10 version or above)

If an incorrect version is installed, ESDA may fail to connect to the database. Please delete the ESDA version 5.0.x and reinstall ESDA by using the correct installation package.

B. After updating the ESDA system, the message "unable to connect to the database" appears.

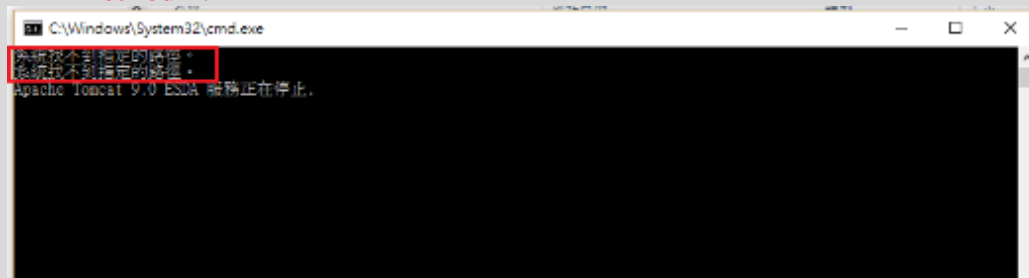
Method 1:

- 1) Login to the ESDA server.
- 2) In the File Explorer, open the path "C:\esda_new" and look for a file named "PPU_RestartTomcatService.bat". Run this file.



Note:

- If the system displays "The system cannot find the specified path" during execution, it means that the default "Apache Tomcat 9.0 ESDA" path cannot be found on the ESDA server to restart the service. Please proceed to **Method 2**.

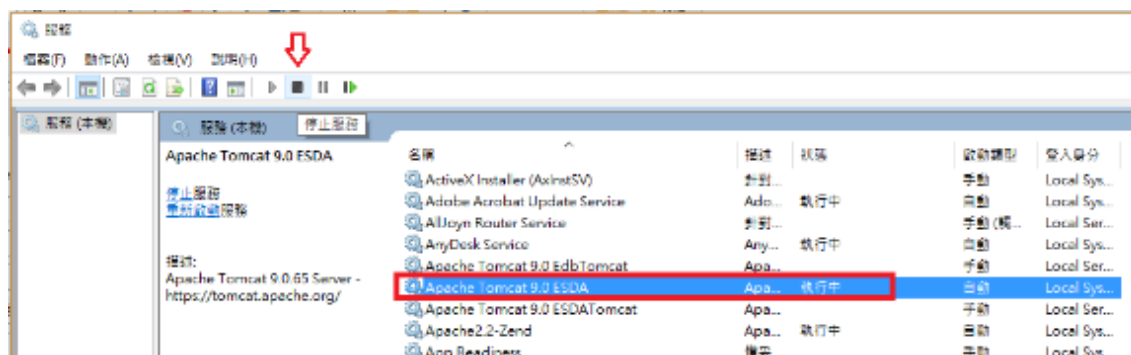


- If the execution file cannot be found, please proceed to **Method 2**.

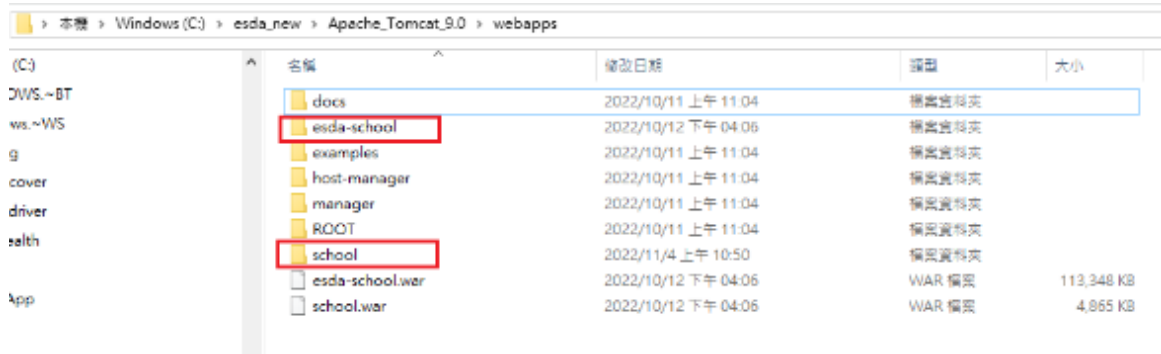
- 3) Wait for about 1 minute, then browse the ESDA system again (e.g., <https://localhost/school>).

Method 2:

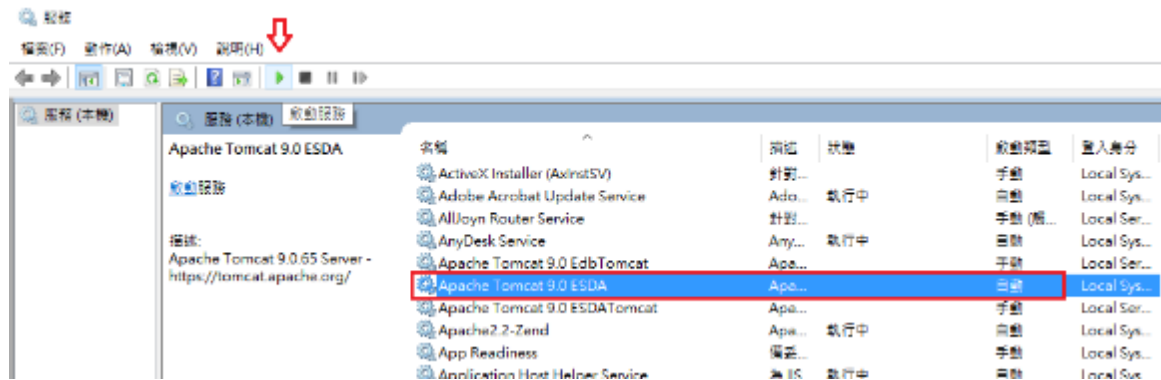
- 1) Login to the ESDA server.
- 2) Select "Apache Tomcat 9.0 ESDA" and click "Stop Service".



- 3) In the File Explorer, open the path "C:\esda_new\apache-tomcat-9.0\webapps". Delete the folders "esda-school" and "school".



- 4) Go to "Services", select "Apache Tomcat 9.0 ESDA", and click "Start Service".



- 5) Wait for about 1 minute, then browse the ESDA system again (e.g., <https://localhost/school>).

Note:

If the above methods cannot help solve the problem, please contact the Indicators Section of the EDB.

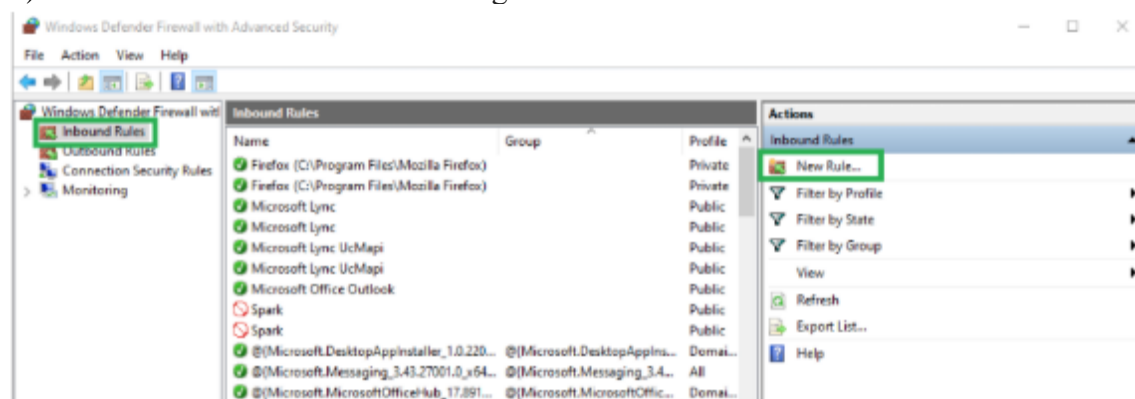
Appendix 5 Enable Port 443 on Windows

If ESDA cannot be accessed via the school intranet, please enable Port 443 on Windows. To enable Port 80, 443, you need to add these to the Windows Firewall.

- 1) Go to Firewall Control Panel by selecting “Start” > “Run”, and type “firewall.cpl”. Click “Advanced Settings” on the left side.



- 2) Click on “Inbound Rules” showing on left side.



- 3) Under the “Action”, click on “New Rule” on the right-side panel.
- 4) A new window pop-up, please choose “Port” and click the “Next” button.

5) Select “TCP” and “Specific local ports” and fill in “80, 443” and click “Next”.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains the following text and controls:

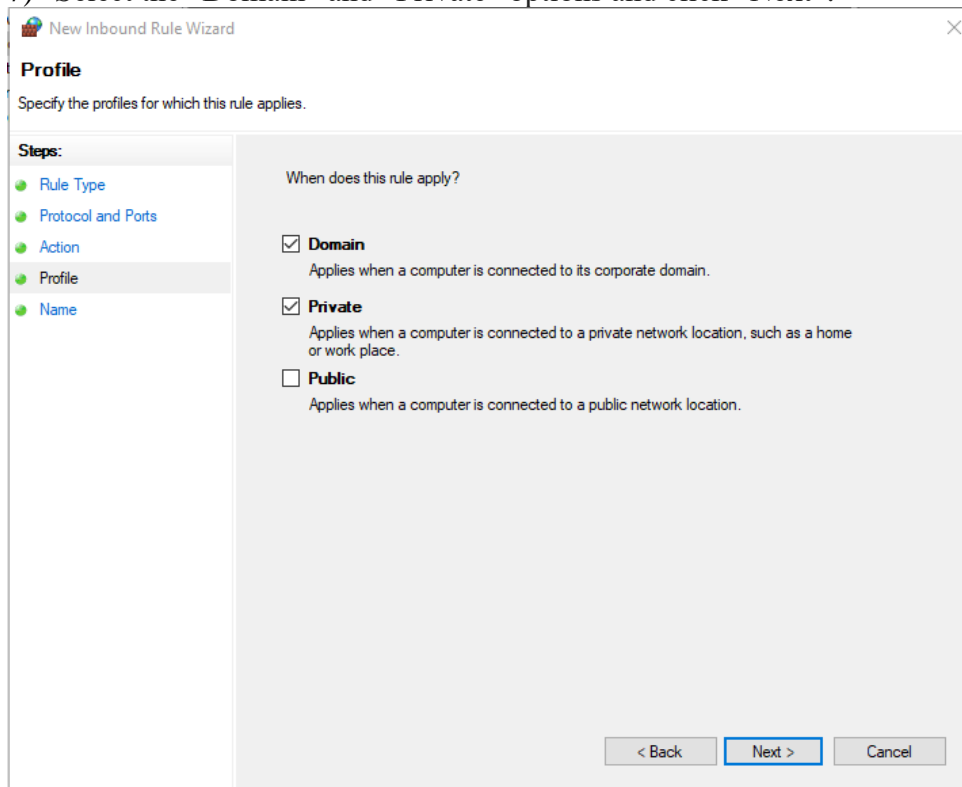
- Protocol and Ports**
Specify the protocols and ports to which this rule applies.
- Steps:**
 - Rule Type
 - Protocol and Ports
 - Action
 - Profile
 - Name
- Does this rule apply to TCP or UDP?
 - ☒ **TCP**
 - ☐ UDP
- Does this rule apply to all local ports or specific local ports?
 - ☐ All local ports
 - ☒ **Specific local ports:**
Example: 80, 443, 5000-5010
- Navigation buttons at the bottom: < Back, **Next >**, and Cancel.

6) Select “Allow the connection” and click “Next”.

The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains the following text and controls:

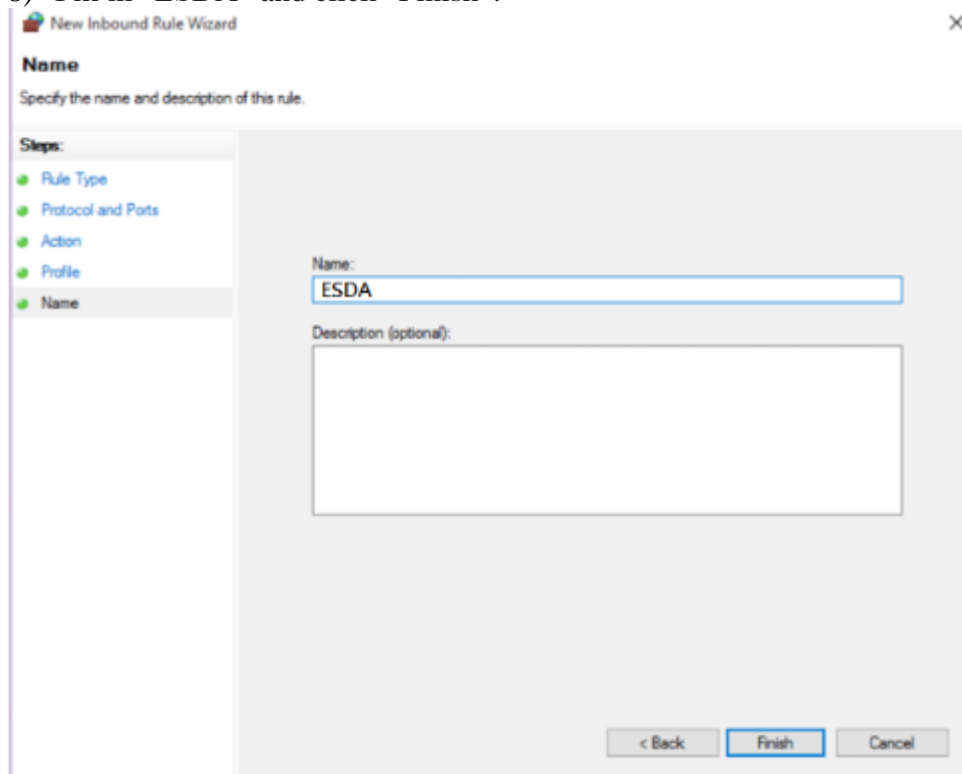
- Action**
Specify the action to be taken when a connection matches the conditions specified in the rule.
- Steps:**
 - Rule Type
 - Protocol and Ports
 - Action
 - Profile
 - Name
- What action should be taken when a connection matches the specified conditions?
 - ☒ **Allow the connection**
This includes connections that are protected with IPsec as well as those that are not.
 - ☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
 - ☐ **Block the connection**
- Navigation buttons at the bottom: < Back, **Next >**, and Cancel.

7) Select the “Domain” and “Private” options and click “Next”.



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile (selected), and Name. The main area is titled 'Profile' with the instruction 'Specify the profiles for which this rule applies.' Below this, it asks 'When does this rule apply?' and provides three options:
☒ **Domain**
Applies when a computer is connected to its corporate domain.
☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.
☐ **Public**
Applies when a computer is connected to a public network location.
At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

8) Fill in “ESDA” and click “Finish”.

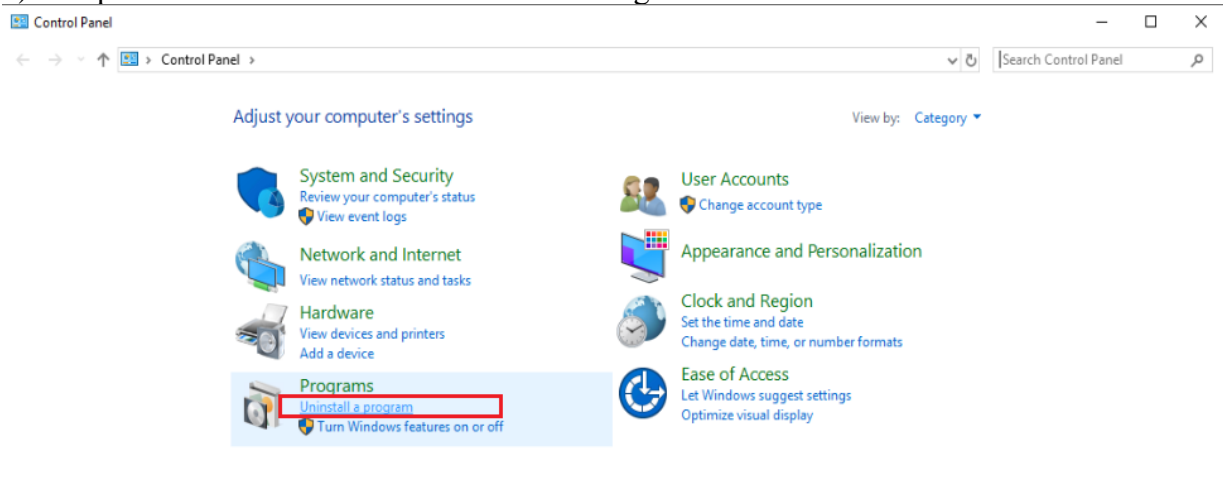


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name (selected). The main area is titled 'Name' with the instruction 'Specify the name and description of this rule.' Below this, there is a 'Name:' label followed by a text box containing 'ESDA'. Below that is a 'Description (optional):' label followed by a larger empty text box. At the bottom right, there are three buttons: '< Back', 'Finish' (highlighted with a blue border), and 'Cancel'.

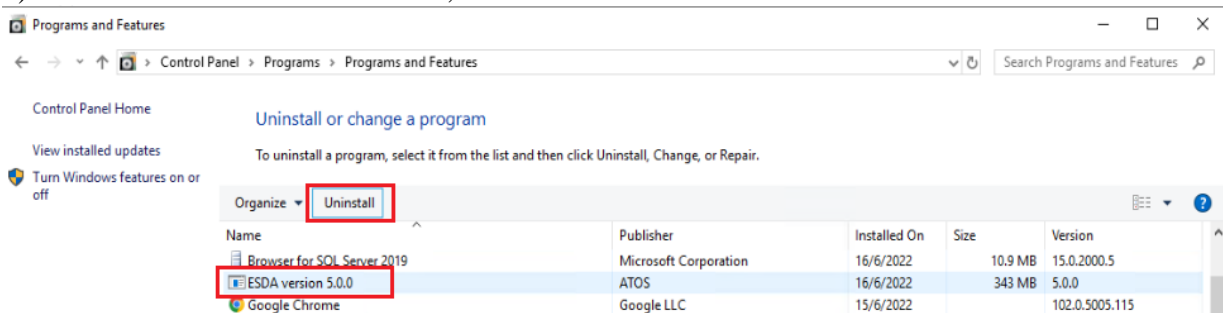
Appendix 6 Uninstalling ESDA

System Administrator may follow the procedures below to uninstall ESDA.

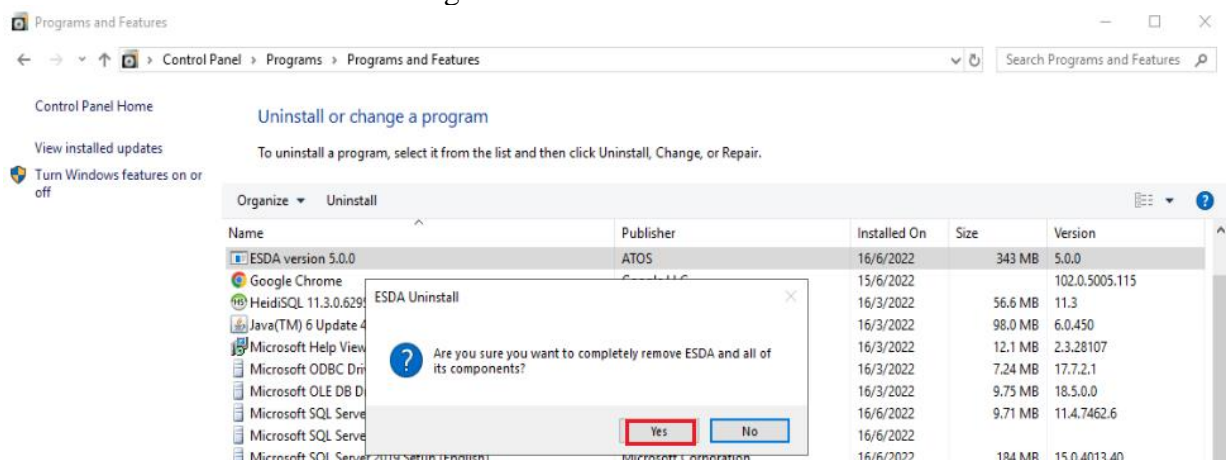
- 1) Open Control Panel and click “Remove Programs”.



- 2) Select “ESDA version 5.0.x”, click “Uninstall”.

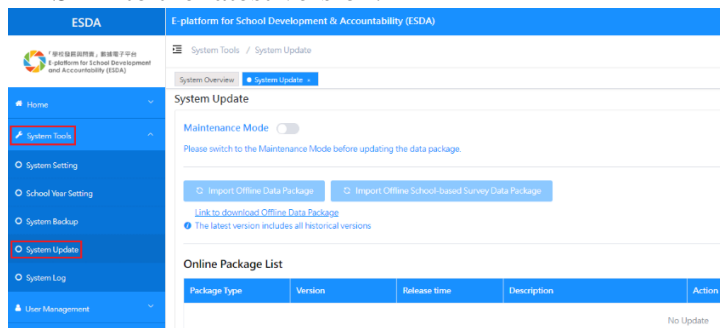


- 3) Click “Yes” to confirm uninstalling ESDA.

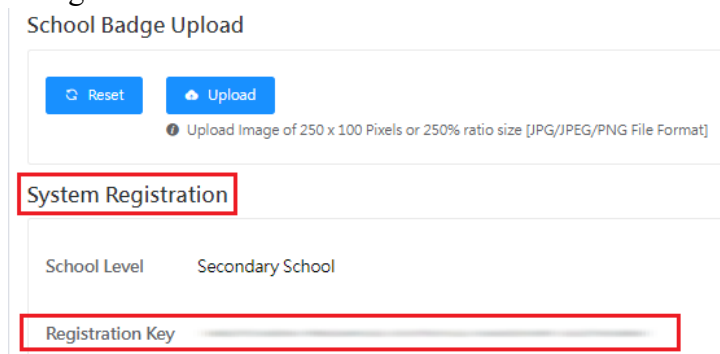


Appendix 7 Cross-Platform Data Migration Procedures

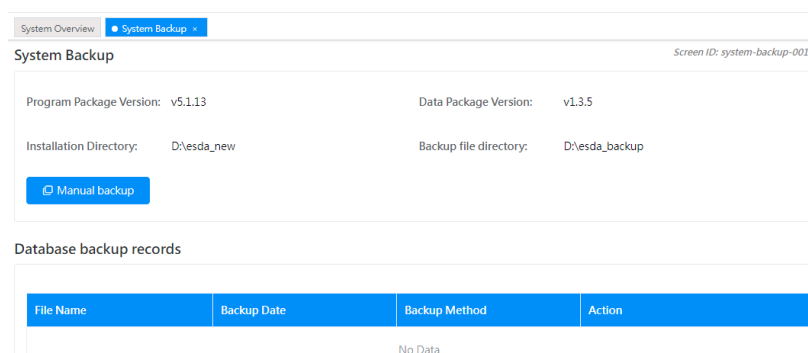
- 1) Login system as System Administrator.
- 2) In the left directory, click “System Tools” and then click “System Update” to upgrade ESDA to the latest version.



- 3) Click “System Setting”. The school’s Registration Key can be obtained under “System Registration”.



- 4) Click “System Backup” and click “Manual Backup”. The system will generate a backup file to the backup file directory.



Note:

- System Administrator, please move the backup file to a safe place.

- 5) Install ESDA on a new server. Please refer to Section 1.2 for details.

- 6) Select the “School Level” and paste the Registration Key obtained from Step 3, then click “Register”.

School Badge Upload

[Reset](#) [Upload](#)

Upload Image of 250 x 100 Pixels or 250% ratio size [JPG/JPEG/PNG File Format]

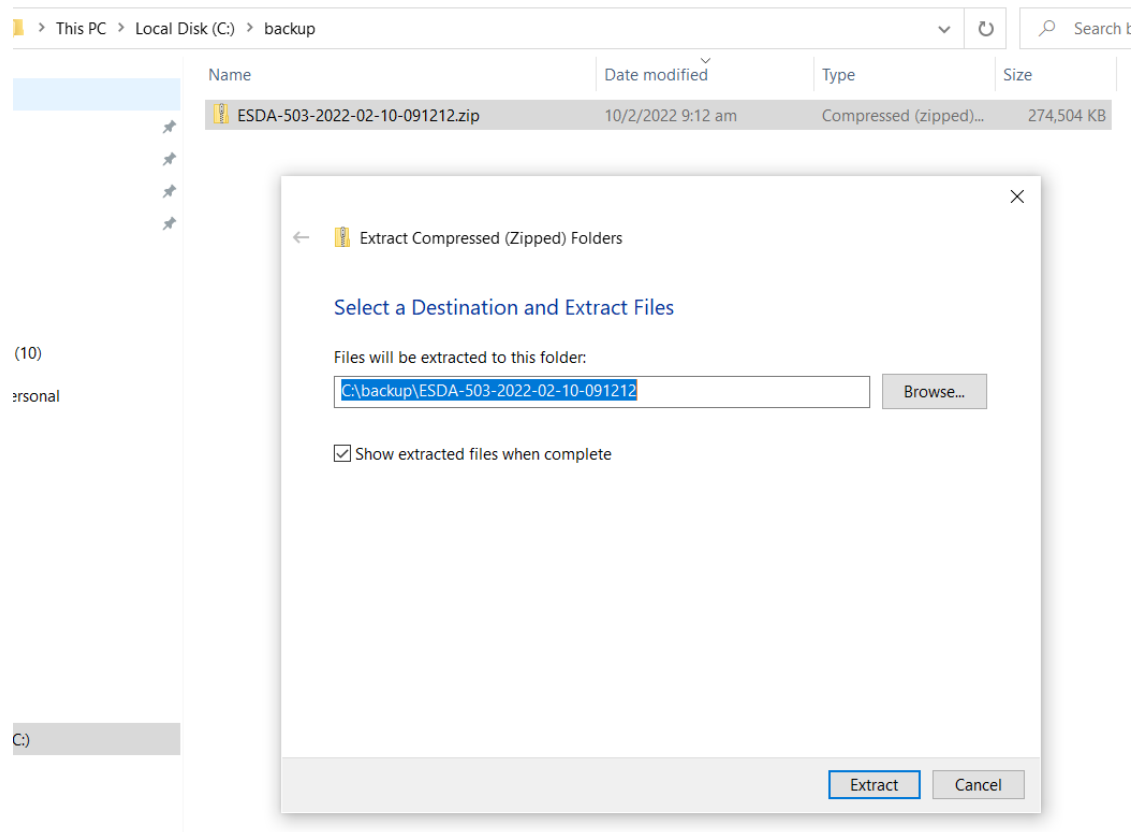
System Registration

School Level

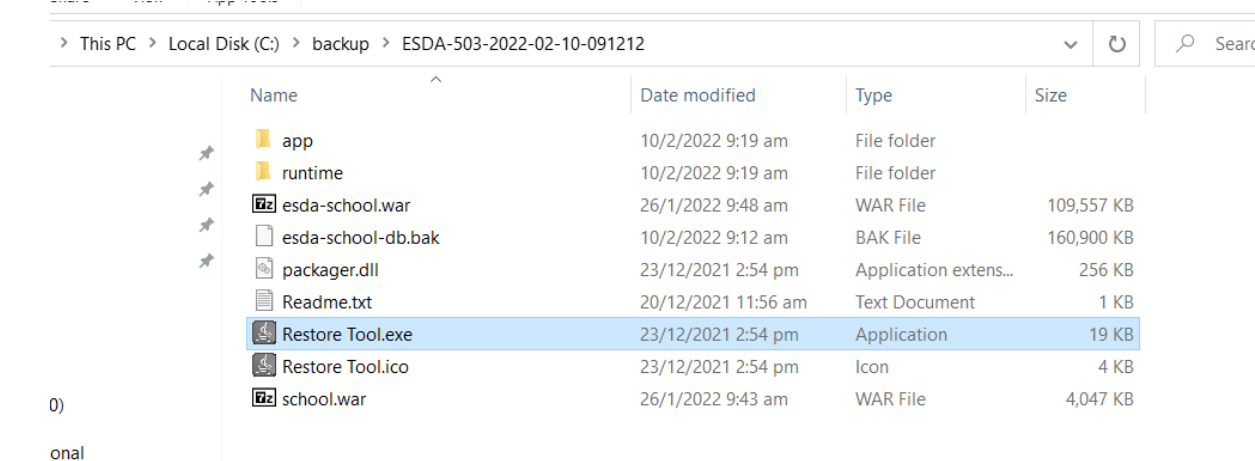
Registration Key - - - -

[Register](#)

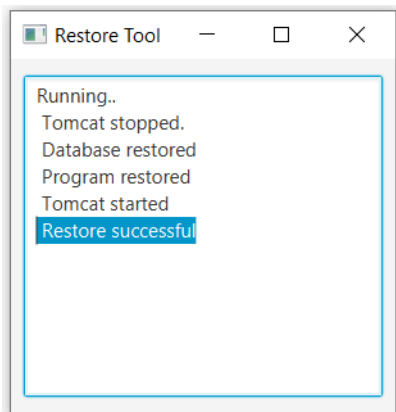
- 7) Repeat Step 2 to upgrade ESDA to the latest version on the new server.
- 8) Repeat Step 4 to generate a backup file directory on the new server.
- 9) Save the backup file obtained from Step 4 of the old server to the backup file directory of Step 8, then unzip the backup file.



10) Run Restore Tool.exe as System Administrator.



11) The data recovery will be started.



Note:

- If error is found during the restoration, please send the log file (\app\log.txt) to the Indicators Section of EDB.

The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > New Volume (D:) > esda_backup > ESDA-519-2022-06-20-220011 > app'. The file list contains the following items:

Name
JavaFXApp.jar
log.txt
mssql-jdbc-9.4.0.jre8.jar
Restore Tool.cfg

The 'log.txt' file is highlighted in blue. The 'app' folder name in the address bar is also highlighted with a red box.

-- End --