

Internet Explorer/ Edge/ Chrome/ Opera (Windows) Edition

Revision History			
Rev.	Date (YYYY/MM/DD)	Description	Editor
V.1.0	2015/4/1	First revision	NII
V.2.0	2018/2/26	Operating environment updates: Microsoft Internet Explorer 11 or later Microsoft Edge 38 or later Google Chrome 56 or later Opera 40 or later	NII
V.2.1	2021/4/7	Update: 1-3. Install Procedure	NII

Table of Content

1. Installing the Certificate (PKCS#12 file)

1-1. Operating Environment

1-2. Prerequisites

1-3. Install Procedure

2. Checking the Certificate (PKCS#12 file)

2-1. Using Microsoft Internet Explorer

2-1-1. Operating Environment

2-1-2. Confirmation Procedure

2-2. Using Microsoft Edge

2-2-1. Operating Environment

2-2-2. Confirmation Procedure

2-3. Using Google Chrome

2-3-1. Operating Environment

2-3-2. Confirmation Procedure

2-4. Using Opera

2-4-1. Operating Environment

2-4-2. Confirmation Procedure

1. Installing the Certificate (PKCS#12 file)

1-1. Operating Environment

The procedures only in the following environment are described in this document:

Supported environment:
Microsoft Internet Explorer 11 or later (Windows) Microsoft Edge 38 or later (Windows) Google Chrome 56 or later (Windows) Opera 40 or later (Windows)

1-2. Prerequisites

The prerequisites for installing the Certificate (PKCS#12 file) in Microsoft Internet Explorer, Microsoft Edge, Google Chrome or Opera are described.

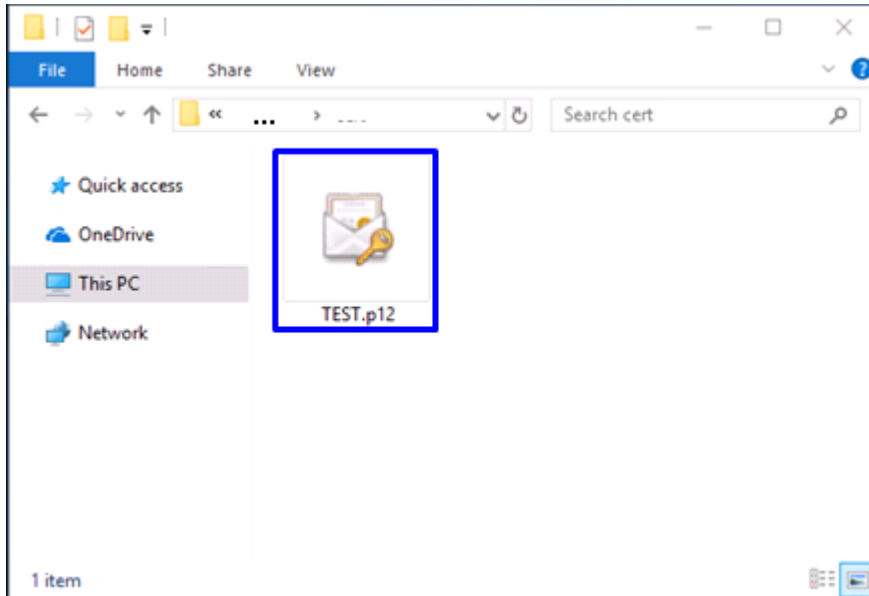
Replace the technical terms according to the user environment in which the Certificate will be used.

Prerequisites
1. The Certificate (PKCS#12 file) has been obtained; 2. the access PIN for the Certificate has been also obtained; and 3. the Operation System is Windows; and 4. Microsoft Internet Explorer, Microsoft Edge, Google Chrome or Opera has been installed.

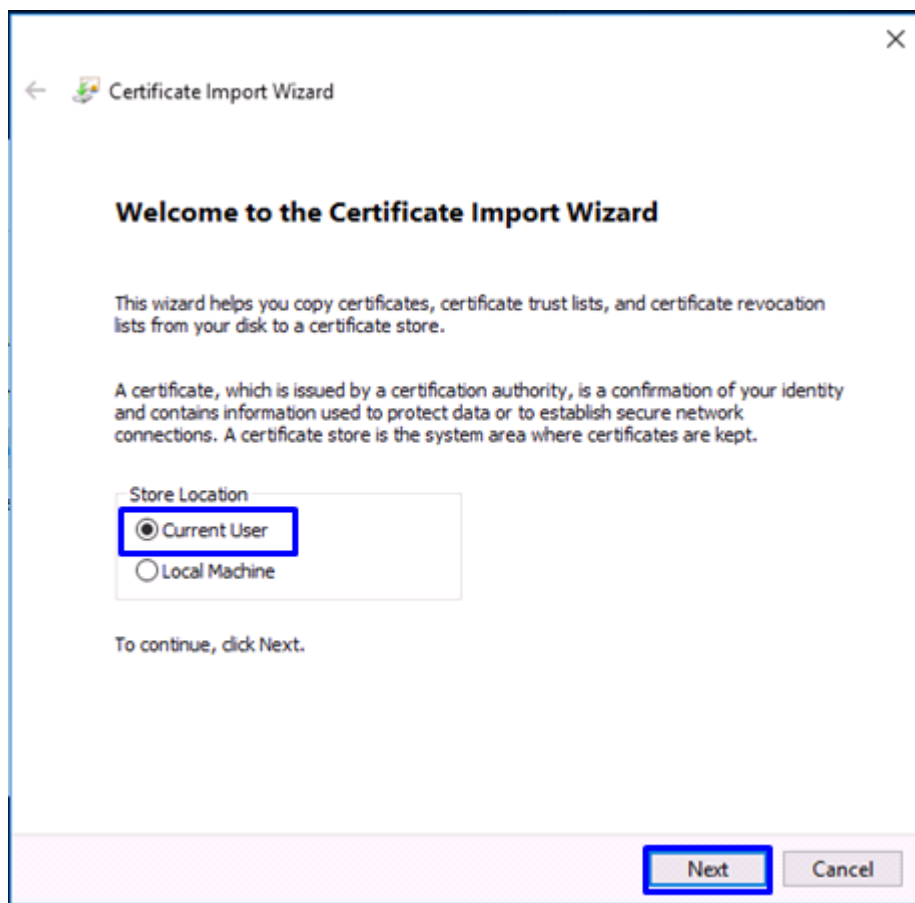
1-3. Install Procedure

Procedure to Install the Certificate (PKCS#12 file)

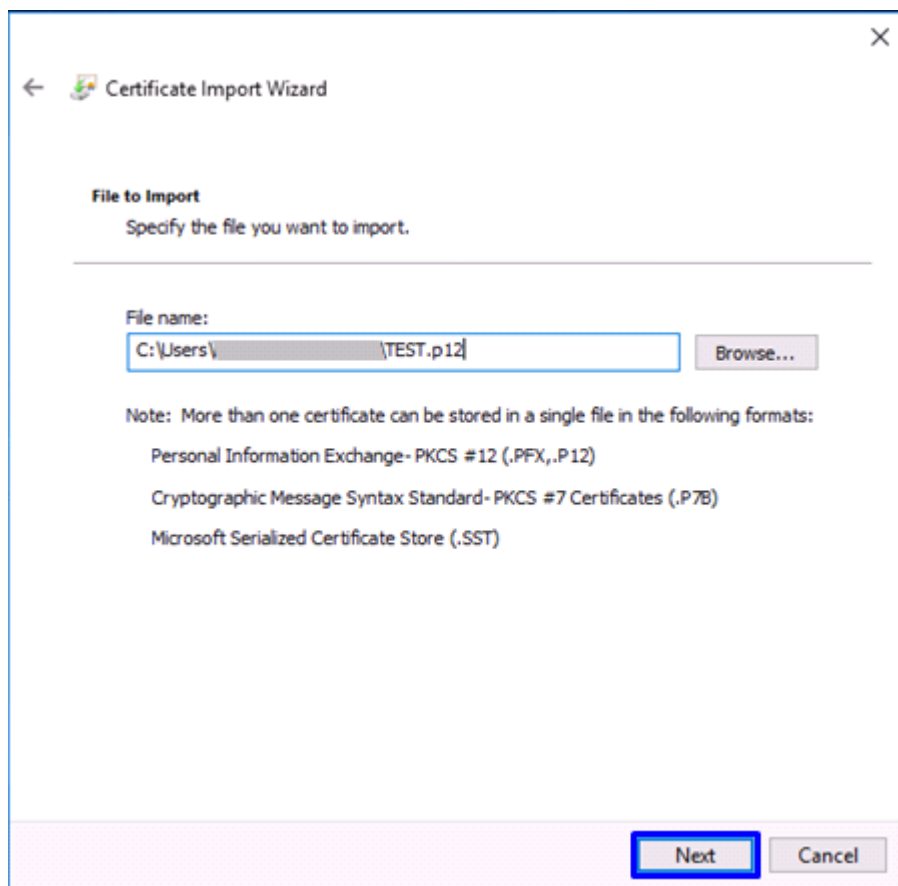
1. Select the Certificate (PKCS#12 file) issued by this Service.



2. Click [Next (N)] in the Security Import Wizard.



3. Make sure that the Certificate (PKCS#12 file) issued by this Service is selected in the [File name (F)] field and click [Next (N)].

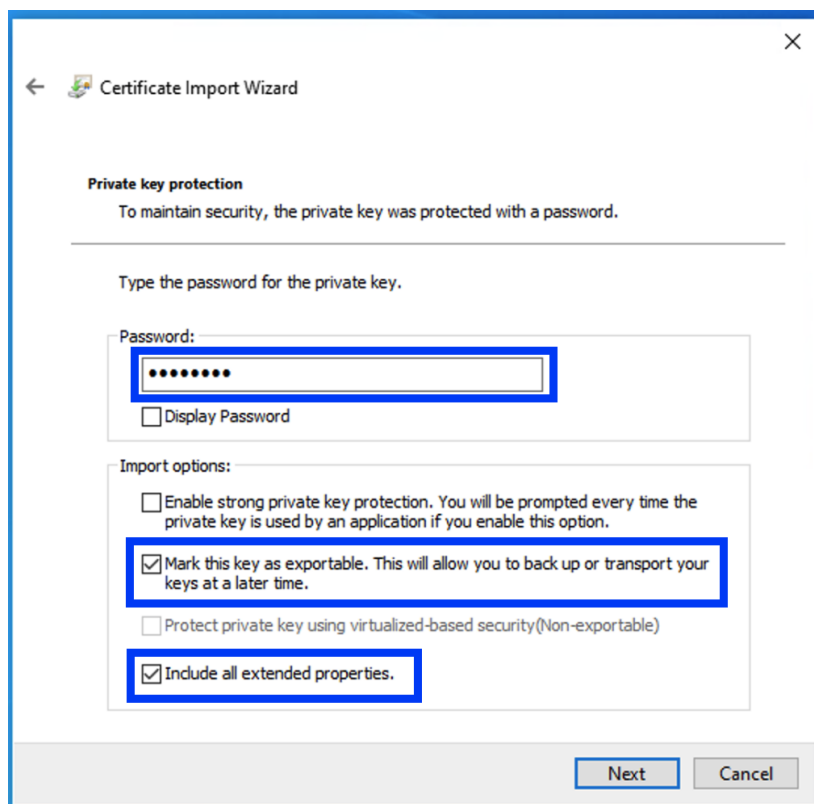


The image shows a Windows 'Certificate Import Wizard' dialog box. At the top, there is a back arrow, a small icon, and the title 'Certificate Import Wizard' with a close button (X) in the top right corner. Below the title bar, the section 'File to Import' is displayed with the instruction 'Specify the file you want to import.' A horizontal line separates this section from the input area. In the input area, there is a label 'File name:' followed by a text box containing 'C:\Users\ \TEST.p12'. To the right of the text box is a 'Browse...' button. Below the text box, a note states: 'Note: More than one certificate can be stored in a single file in the following formats:'. This is followed by three bulleted items: 'Personal Information Exchange- PKCS #12 (.PFX,.P12)', 'Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)', and 'Microsoft Serialized Certificate Store (.SST)'. At the bottom of the dialog, there are two buttons: 'Next' and 'Cancel'. The 'Next' button is highlighted with a blue rectangular border.

4. Enter the Access PIN issued by this Service in the [Password (P)] field.

Check the **[Mark this key as exportable (M)]** and **[Include all extended properties (A)]** checkboxes click [Next (N)].

Please do not check the [Enable strong private key protection (E)] . If checked, the client certificate will not work properly.



← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

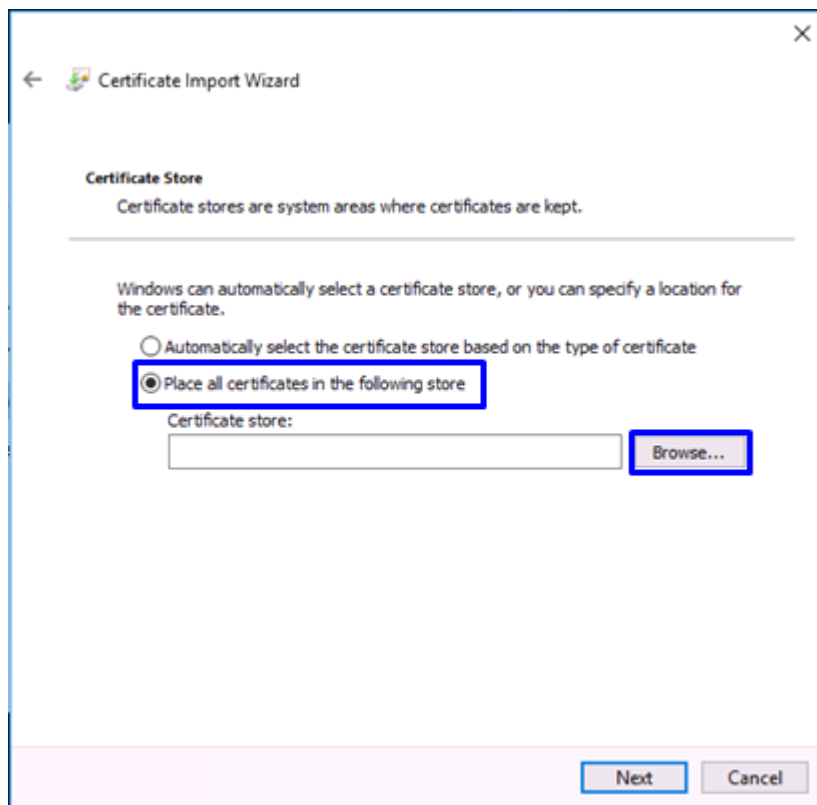
☐ Display Password

Import options:

- ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- ☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- ☐ Protect private key using virtualized-based security(Non-exportable)
- ☒ Include all extended properties.

Next Cancel

5. Select [Store all certificates in the following store (P)] and click [Browse...(R)].



← Certificate Import Wizard

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

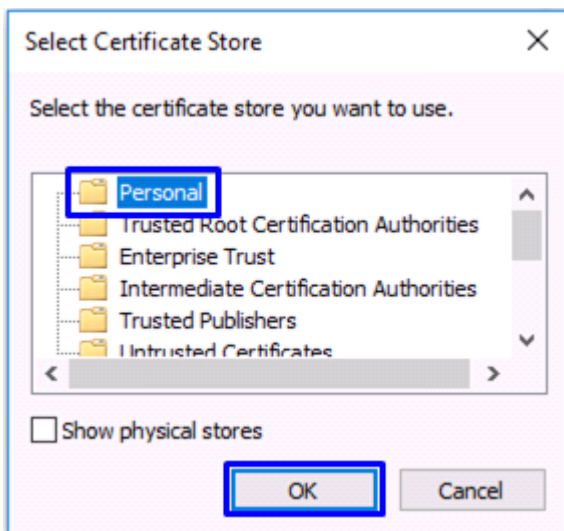
- ☐ Automatically select the certificate store based on the type of certificate
- ☒ Place all certificates in the following store

Certificate store:

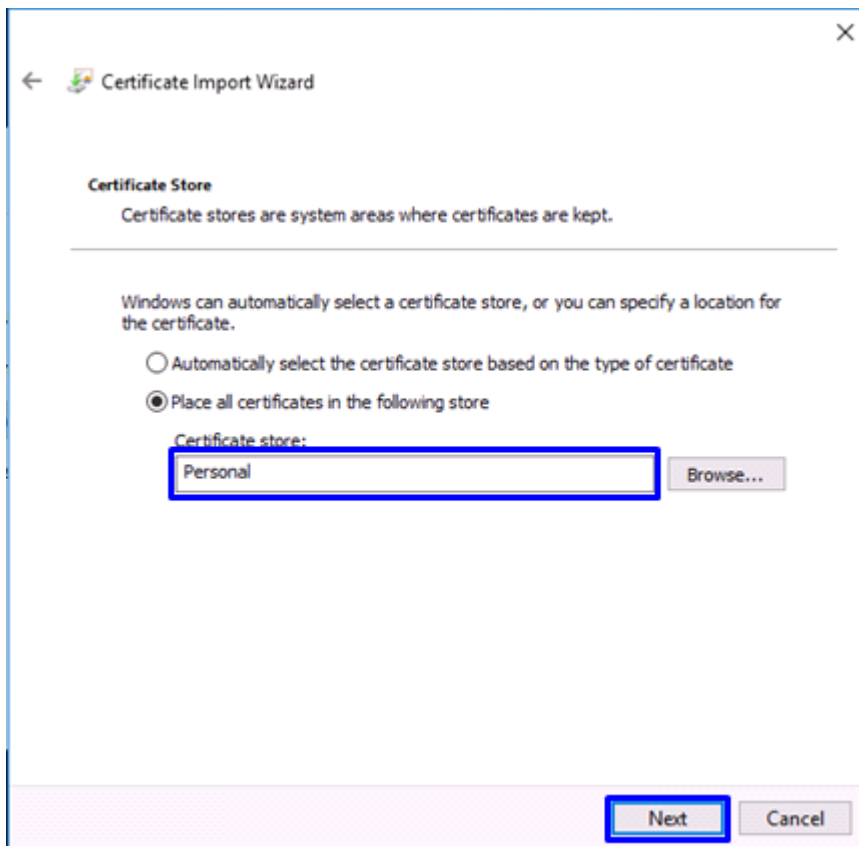
Browse...

Next Cancel

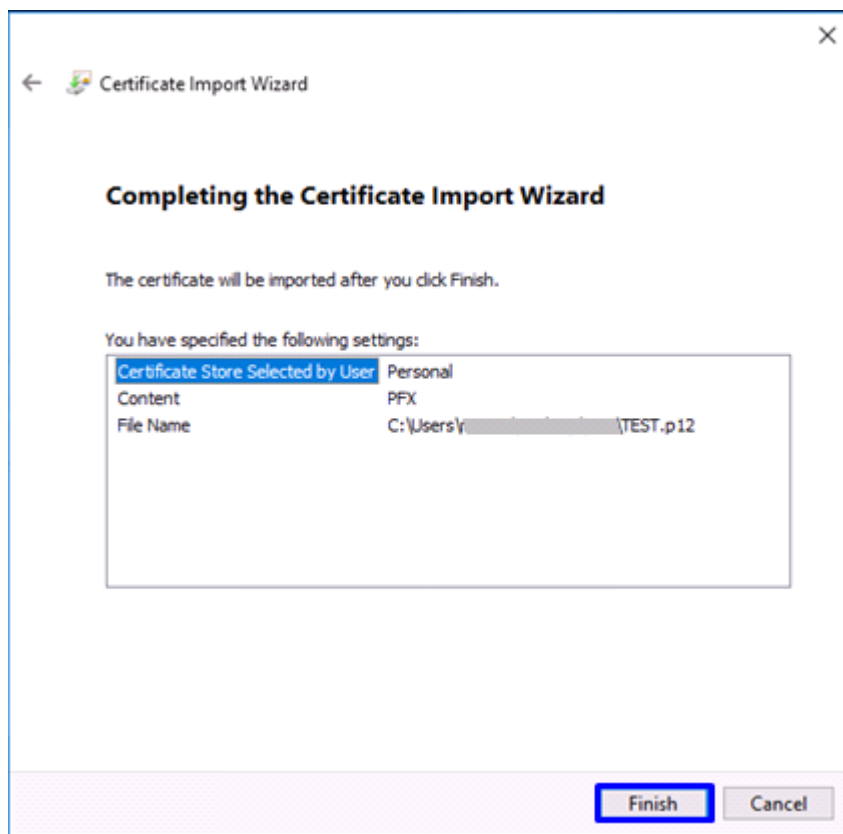
6. In the [Select Certificate Store] dialog, select [Personal] and click [OK].



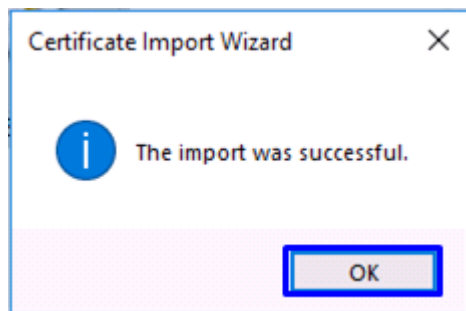
7. After confirming that [Personal] appears in the [Certificate store:] box, click [Next (N)].



8. Click [Finish].



9. Click [OK].



This completes installation of the Certificate (PKCS#12 file) into the web browser.

2. Checking the Certificate (PKCS#12 file)

2-1. Using Microsoft Internet Explorer

2-1-1. Operating Environment

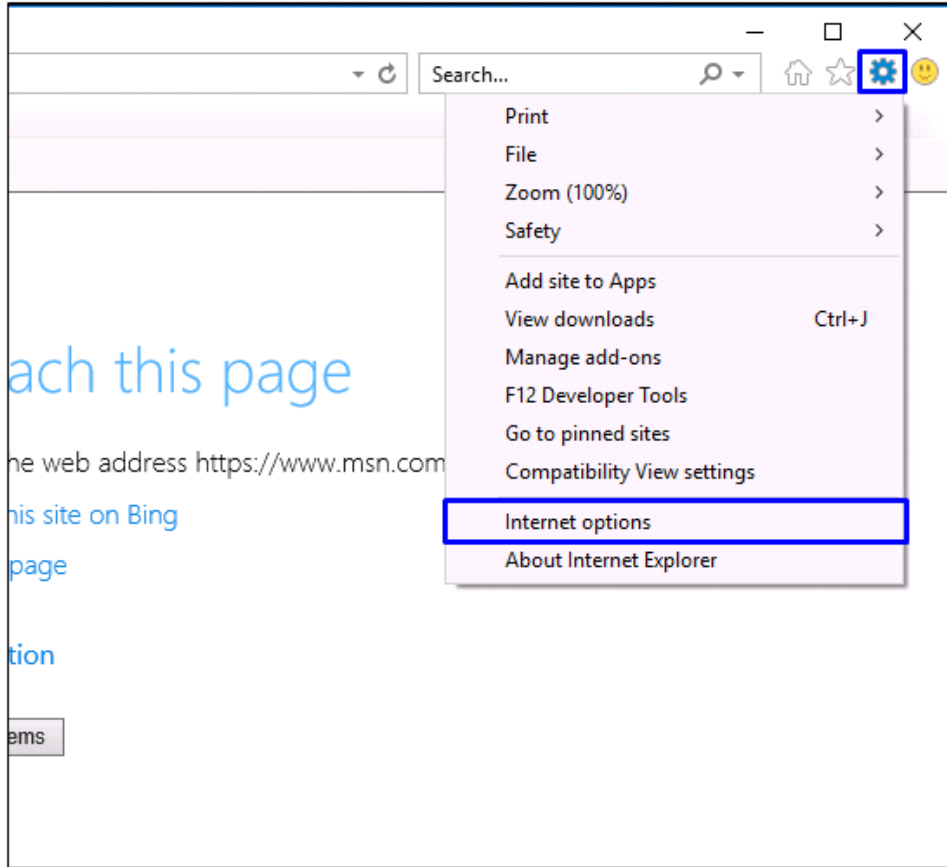
The procedures only in the following environment are described in this document:

Supported environment:

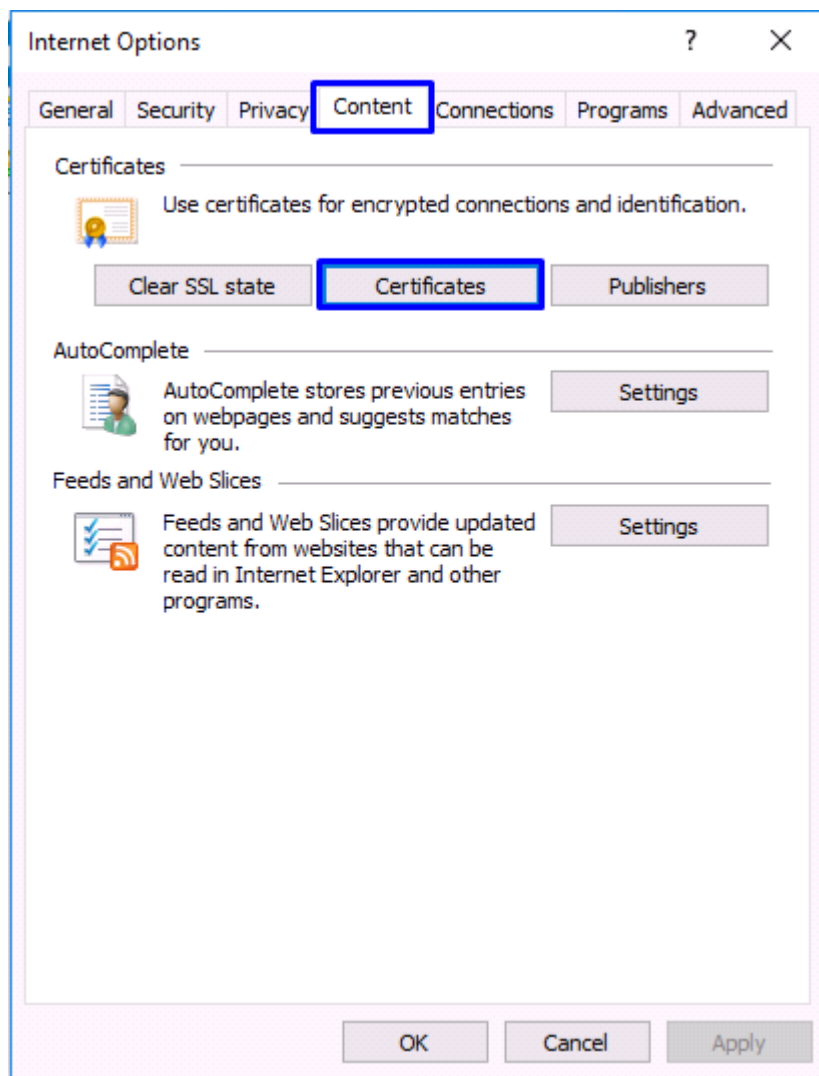
2-1-2. Confirmation Procedure

Checking the Certificate (PKCS#12 file)

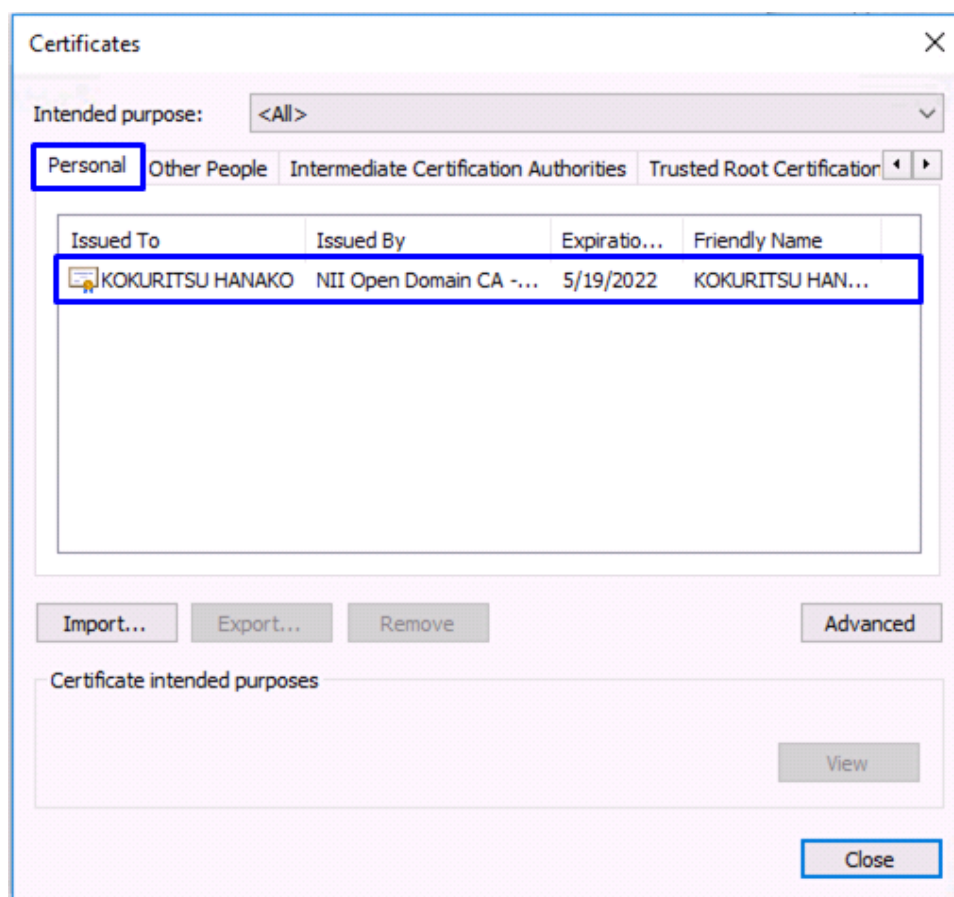
1. With Microsoft Internet Explorer, click on the [Tools] icon and select [Internet options (O)].



2. In the [Internet Options] dialog, select the [Content] tab and click [Certificates (C)]



3. Then, in the [Certificates] dialog, move to the [Personal] tab and make sure that the Certificate (PKCS#12 file) issued by this Service has been installed.



This completes confirmation of the Certificate (PKCS#12 file).

2-2. Using Microsoft Edge

2-2-1. Operating Environment

The procedures only in the following environment are described in this document:

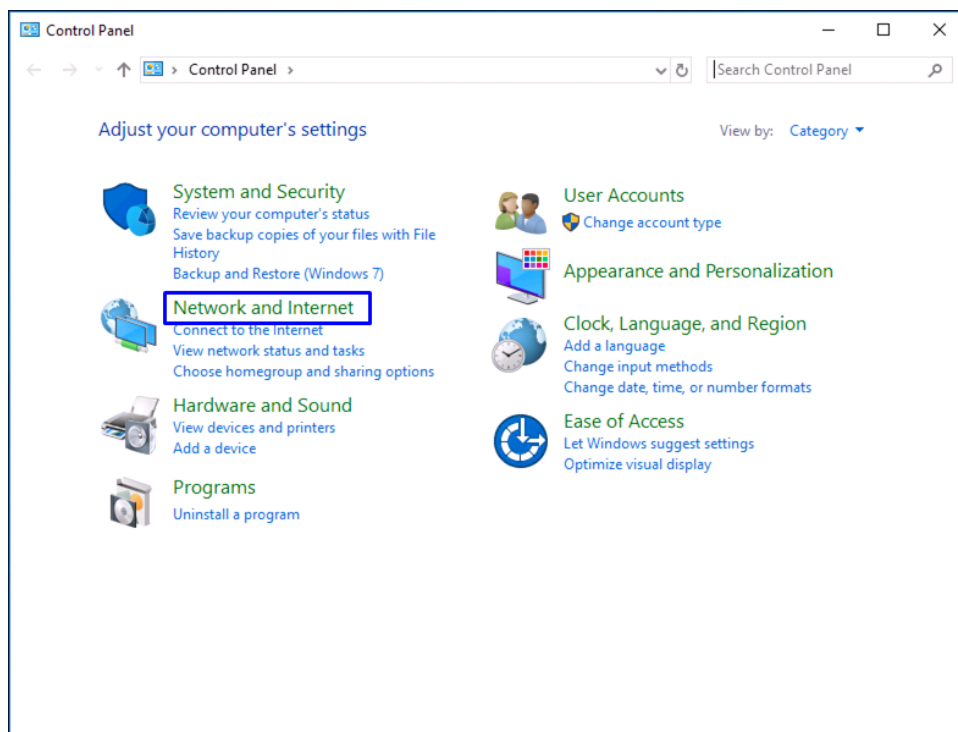
Supported environment:

Microsoft Edge 38 or later (Windows)

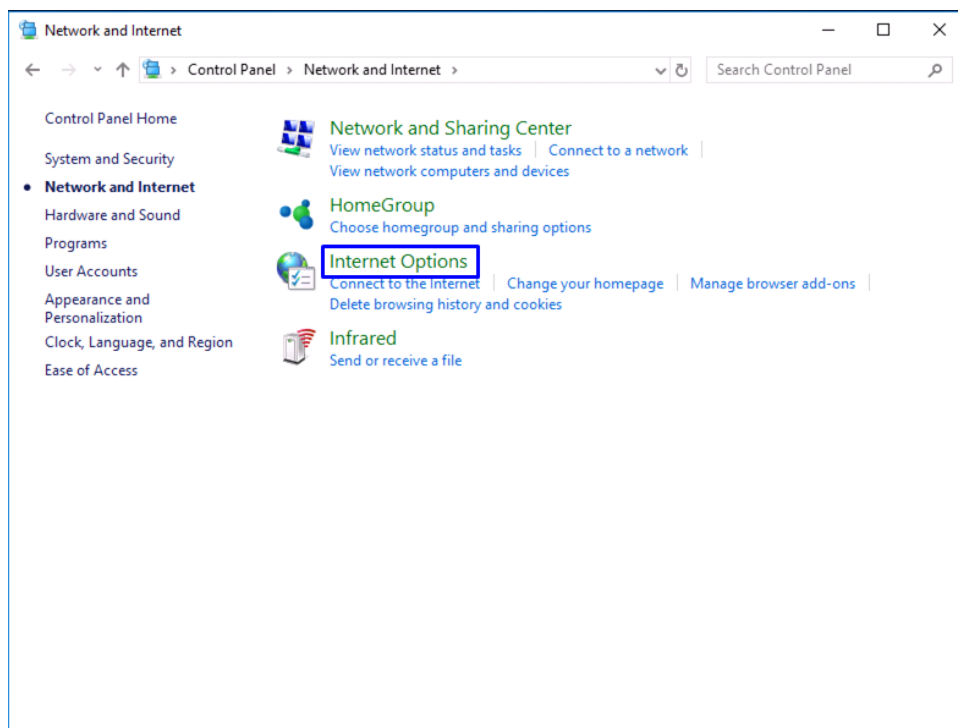
2-2-2. Confirmation Procedure

Checking the Certificate (PKCS#12 file)

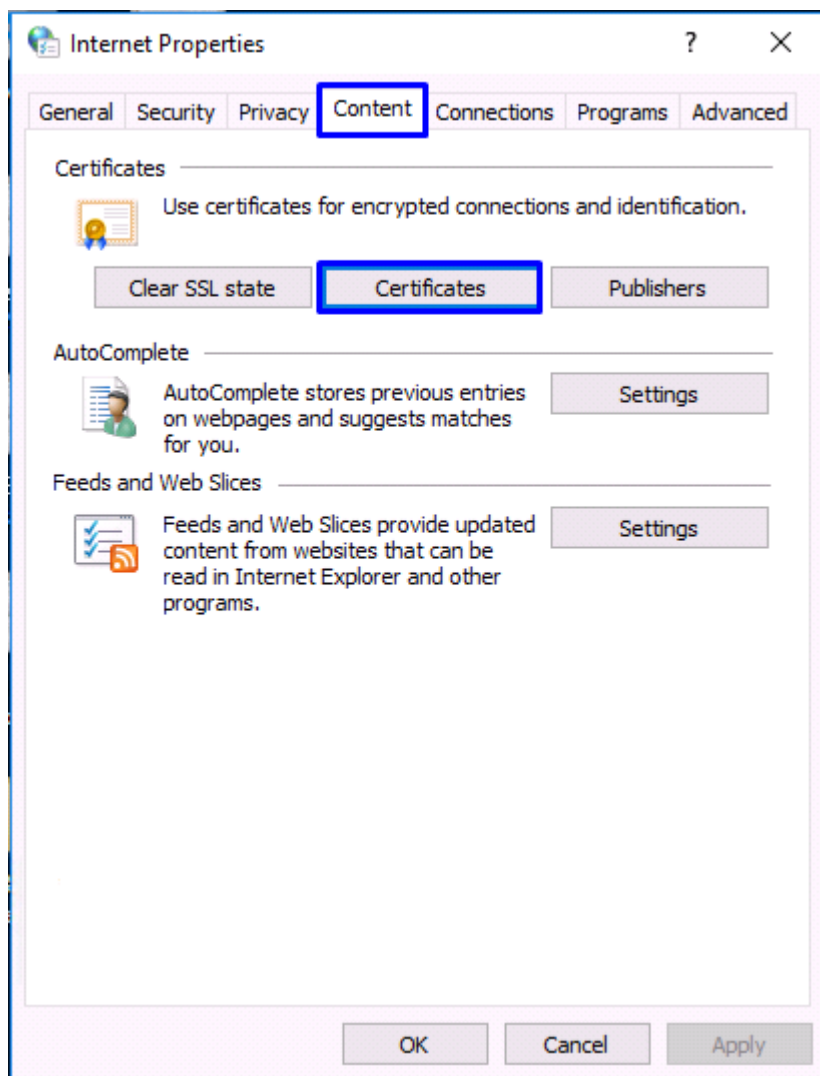
1. Open the [Control Panel] and select [Network and Internet].



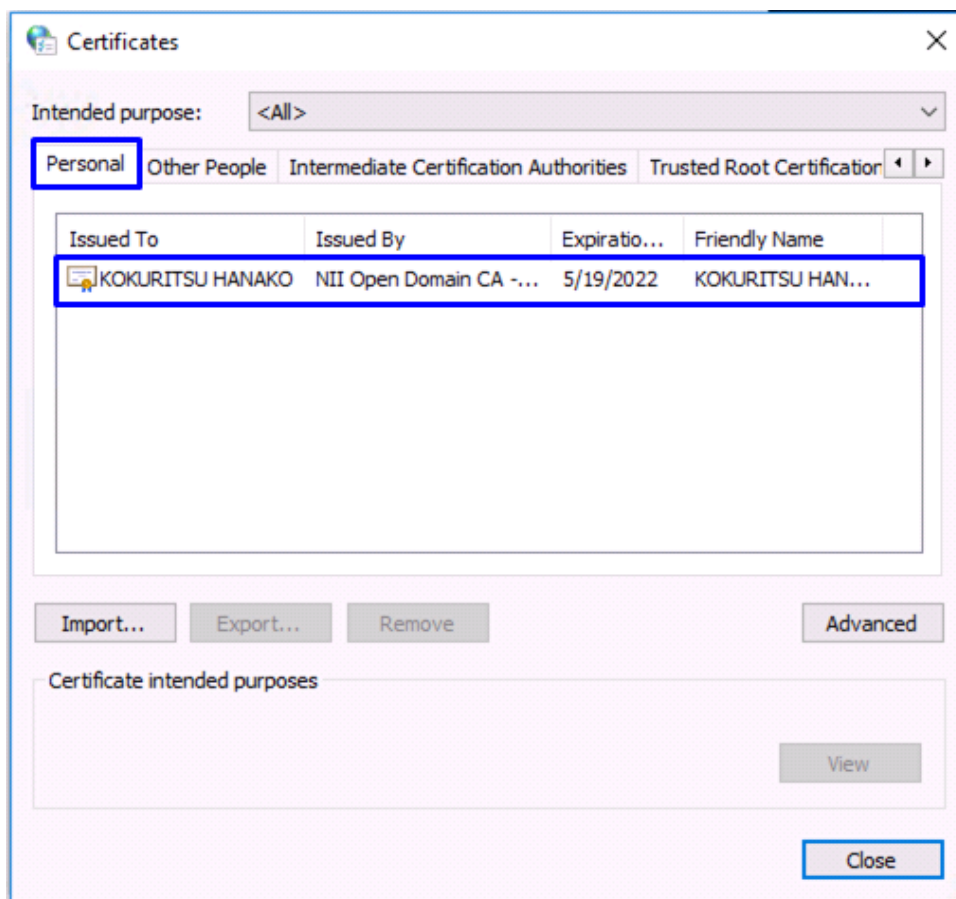
2. Choose [Internet Options].



3. Select the [Content] tab in the [Internet Options] dialog, and click [Certificates (C)].



4. Then, in the [Certificates] dialog, move to the [Personal] tab and make sure that the Certificate (PKCS#12 file) issued by this Service has been installed.



This completes confirmation of the Certificate (PKCS#12 file).

2-3. Using Google Chrome

2-3-1. Operating Environment

The procedures only in the following environment are described in this document:

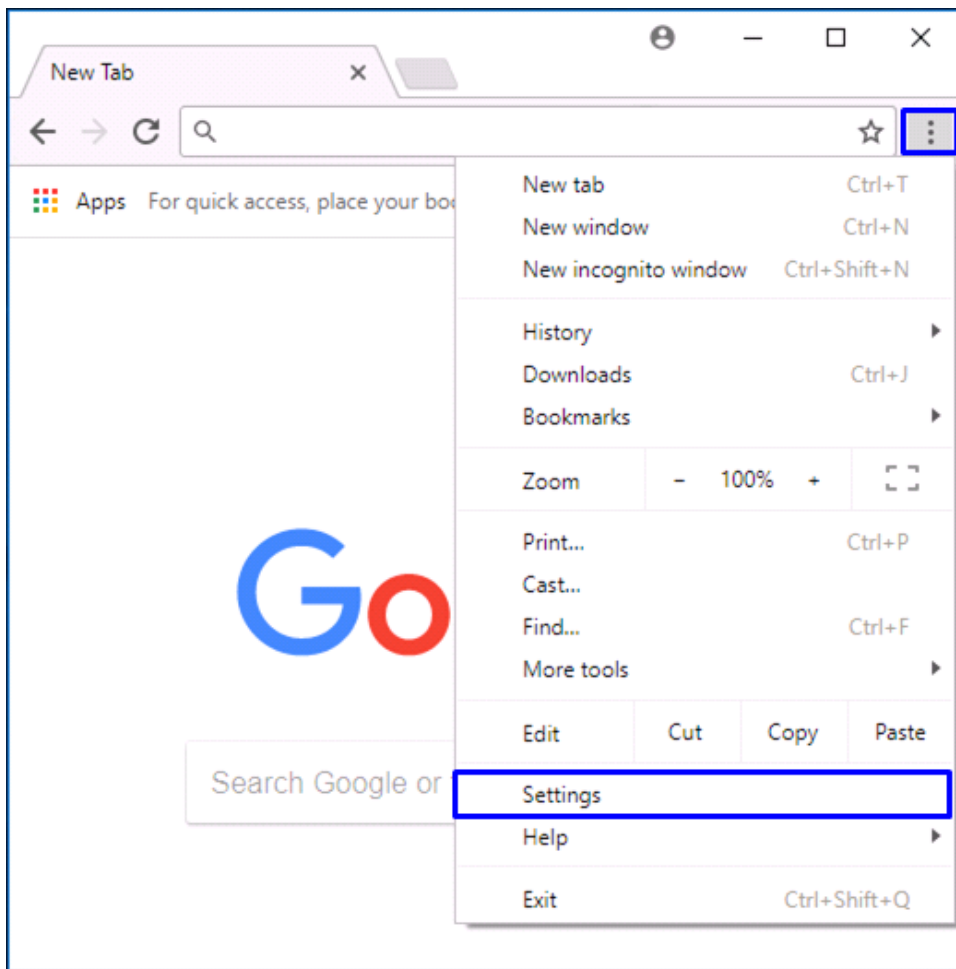
Supported environment:

Google Chrome 56 or later (Windows)

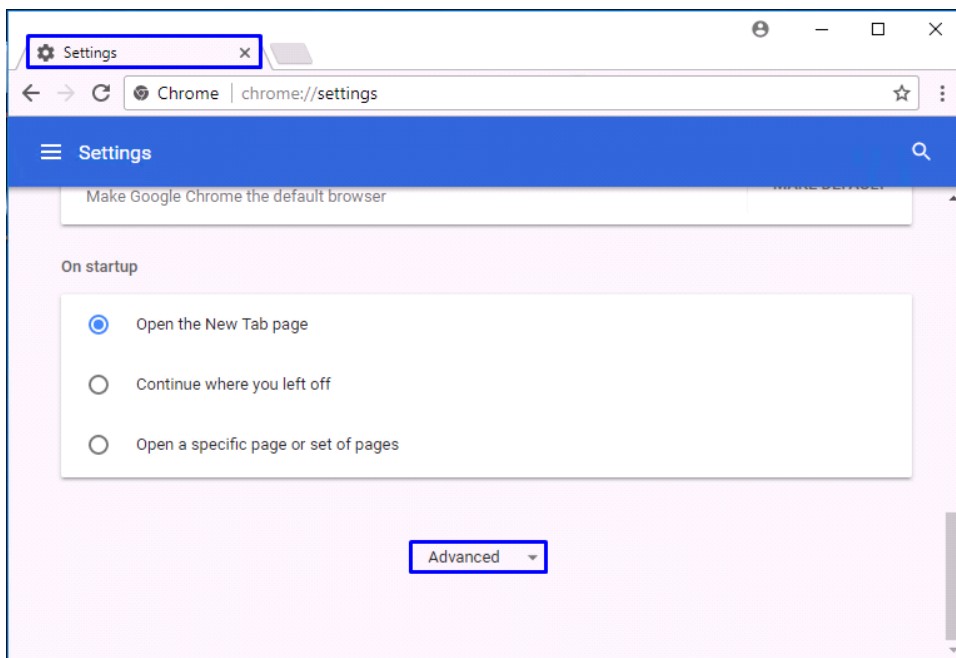
2-3-2. Confirmation Procedure

Checking the Certificate (PKCS#12 file)

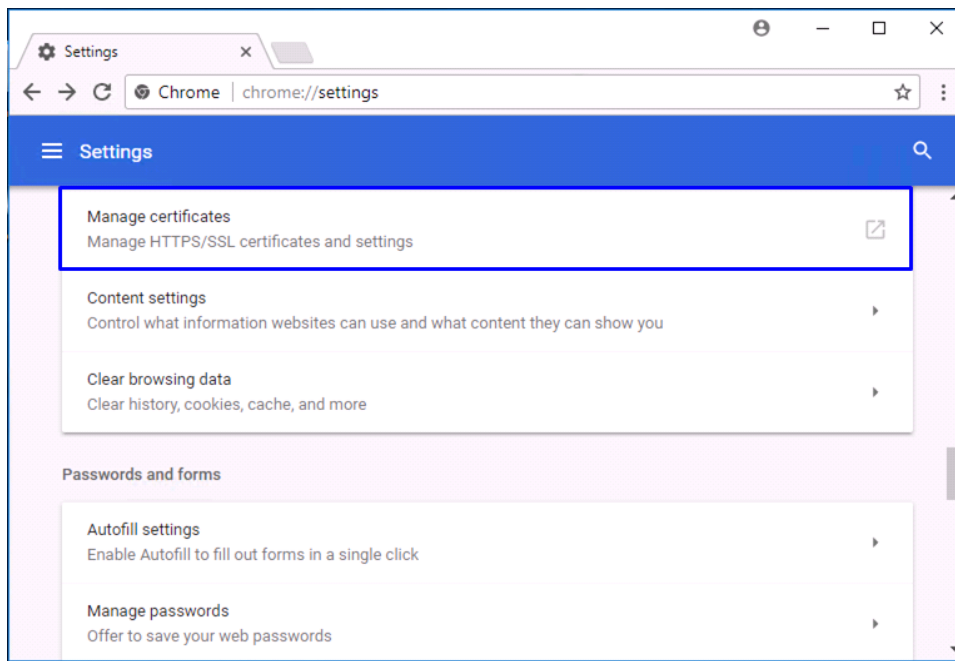
1. With Google Chrome, click the [Chrome Menu] on the browser toolbar and select [Settings (S)].



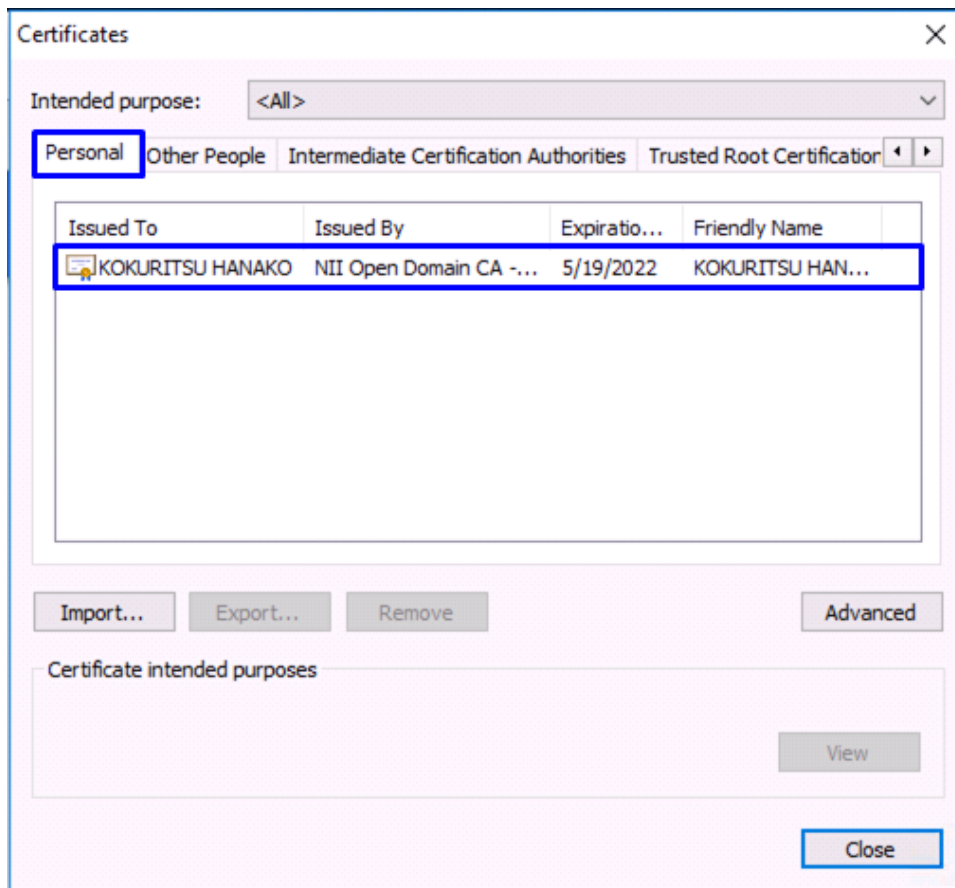
2. In the [Settings] tab, click [Advanced].



3. Click [Manage certificates].



4. Then, in the [Certificates] dialog, move to the [Personal] tab and make sure that the Certificate (PKCS#12 file) issued by this Service has been installed.



This completes confirmation of the Certificate (PKCS#12 file).

2-4. Using Opera

2-4-1. Operating Environment

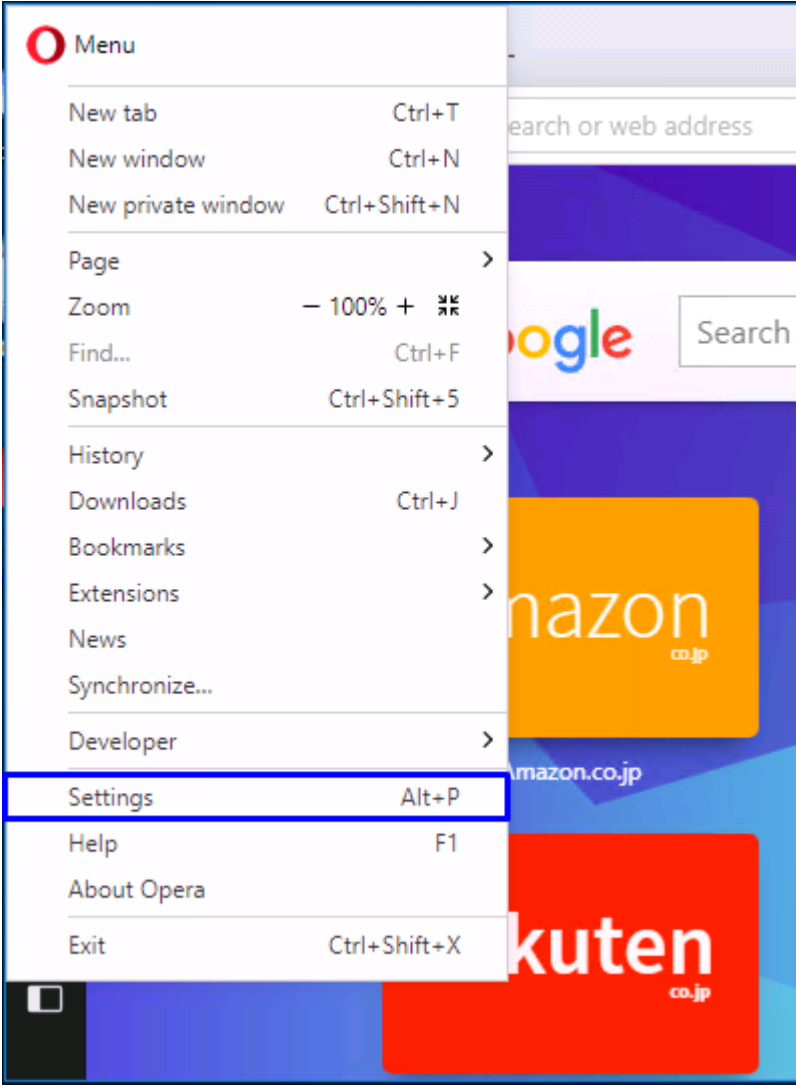
The procedures only in the following environment are described in this document:

Supported environment:
Opera 40 or later (Windows)

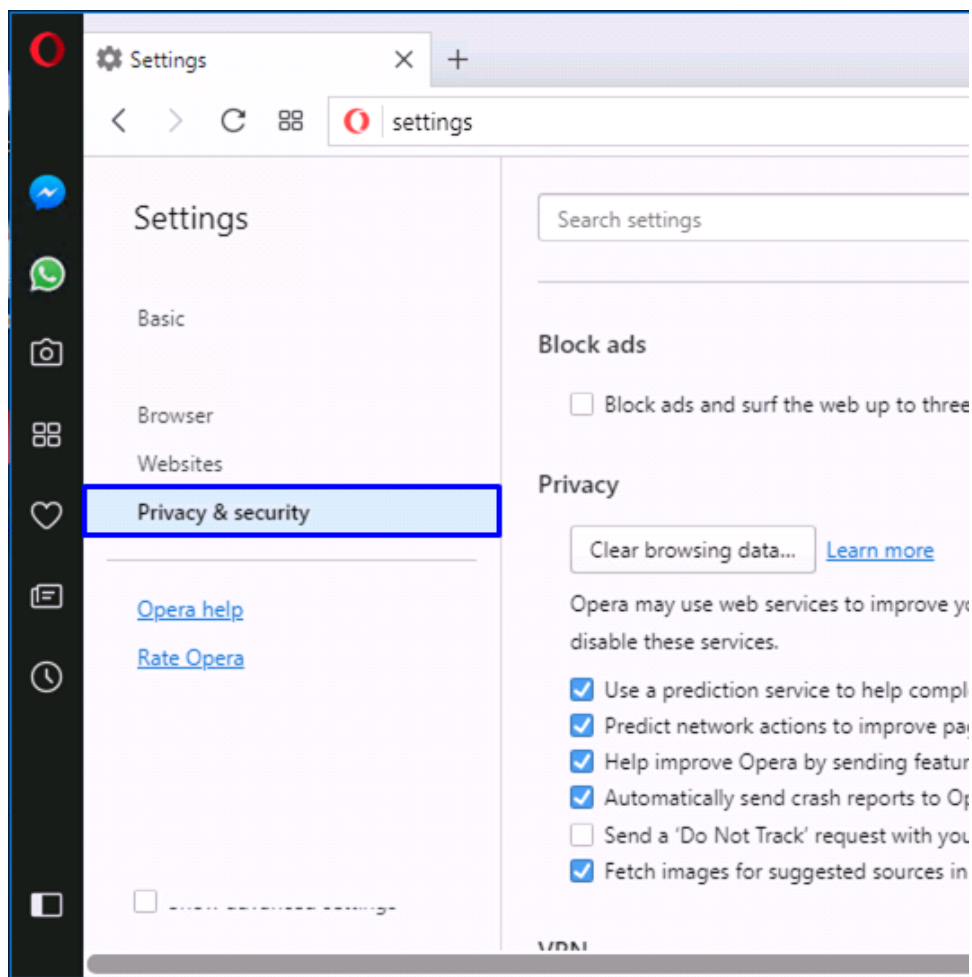
2-4-2. Confirmation Procedure

Checking the Certificate (PKCS#12 file)

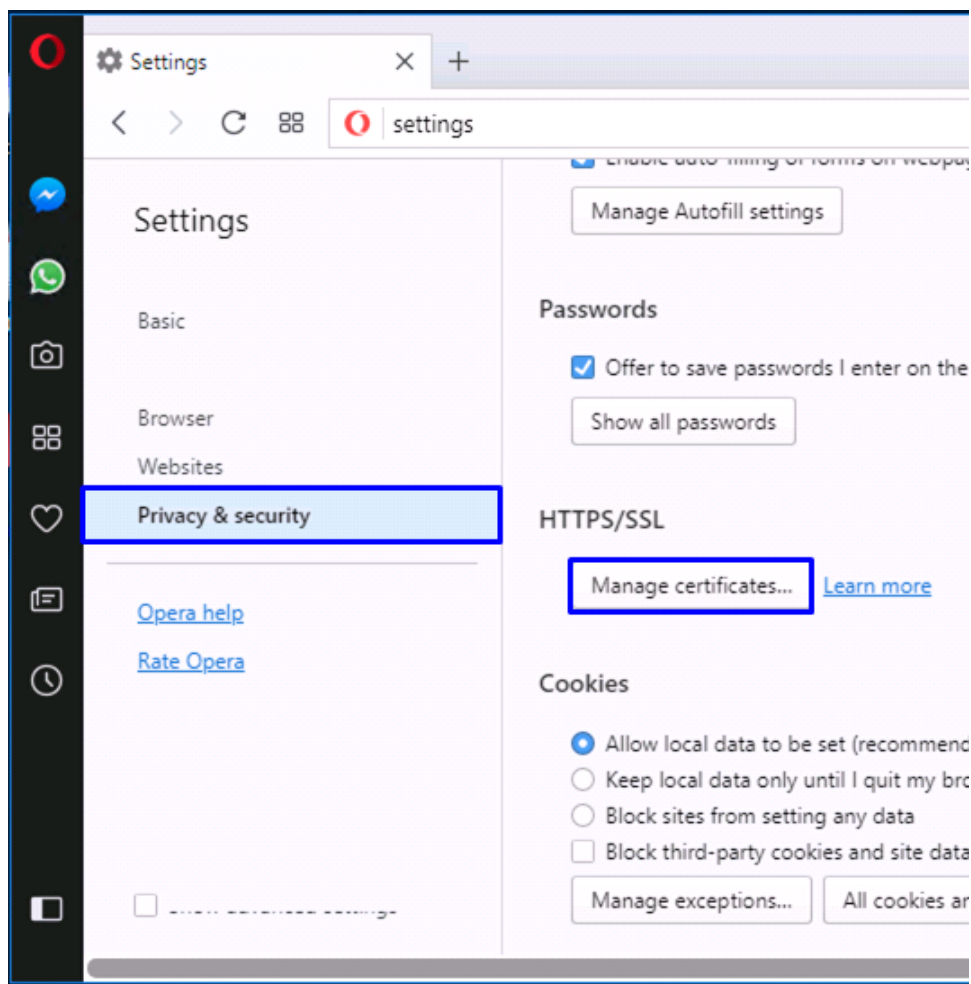
1. Select [Settings (S)] in the [Menu] tab.

A screenshot of the Opera browser's menu. The menu is open, showing various options. The 'Settings' option is highlighted with a blue border. The menu items include: New tab (Ctrl+T), New window (Ctrl+N), New private window (Ctrl+Shift+N), Page, Zoom (- 100% +), Find... (Ctrl+F), Snapshot (Ctrl+Shift+5), History, Downloads (Ctrl+J), Bookmarks, Extensions, News, Synchronize..., Developer, Settings (Alt+P), Help (F1), About Opera, and Exit (Ctrl+Shift+X). The background of the browser shows a search bar and several website thumbnails, including Google, Amazon.co.jp, and Rakuten.co.jp.

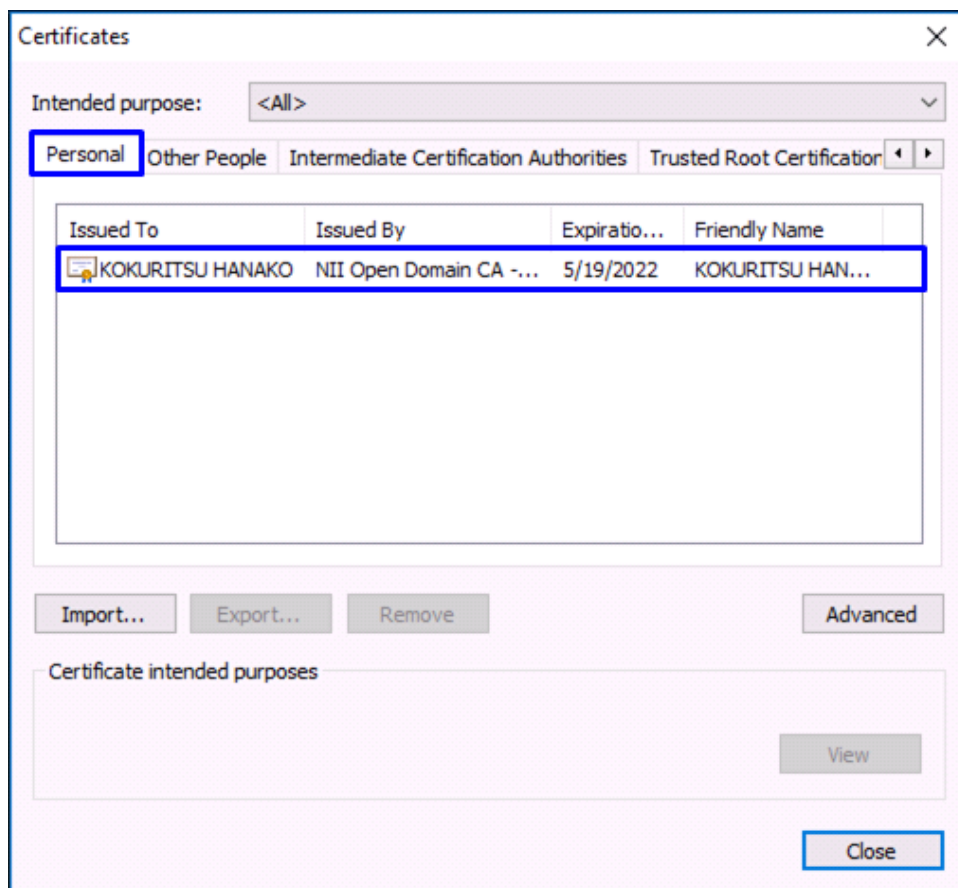
2. Select [Privacy & security].



3. Click [Manage certificates...].



4. Then, in the [Certificates] dialog, move to the [Personal] tab and make sure that the Certificate (PKCS#12 file) issued by this Service has been installed.



This completes confirmation of the Certificate (PKCS#12 file).