

Certificate Issue Web Site Manual: Internet Explorer Edition

Revision History			
Rev.	Date (YYYY/MM/DD)	Description	Editor
V. 1.0	2015/4/1	First revision	NII
V. 1.1	2016/12/26	Amendment with addition of [NII Open Domain S/MIME CA] as a new Certificate Authority	NII
V. 2.2	2018/2/26	Addition of steps to change the language in the certificate retrieval procedure and amendment associated with the operating environment change.	NII
V. 2.3	2021/10/12	Change of issuance method by web enrollment.	NII

Table of Content

- [1. Setting the Browser](#)
 - [1-1. Internet Explorer Settings](#)
- [2. Retrieving the Certificate](#)
 - [2-1. Prerequisites](#)
 - [2-2. Certificate Retrieval](#)
 - [2-2-1. Notification of URL for the Certificate Retrieval](#)
 - [2-2-2. Retrieving the Certificate Using Internet Explorer](#)

1. Setting the Browser

Sections to follow discuss how to set up the browser prior to using this system.

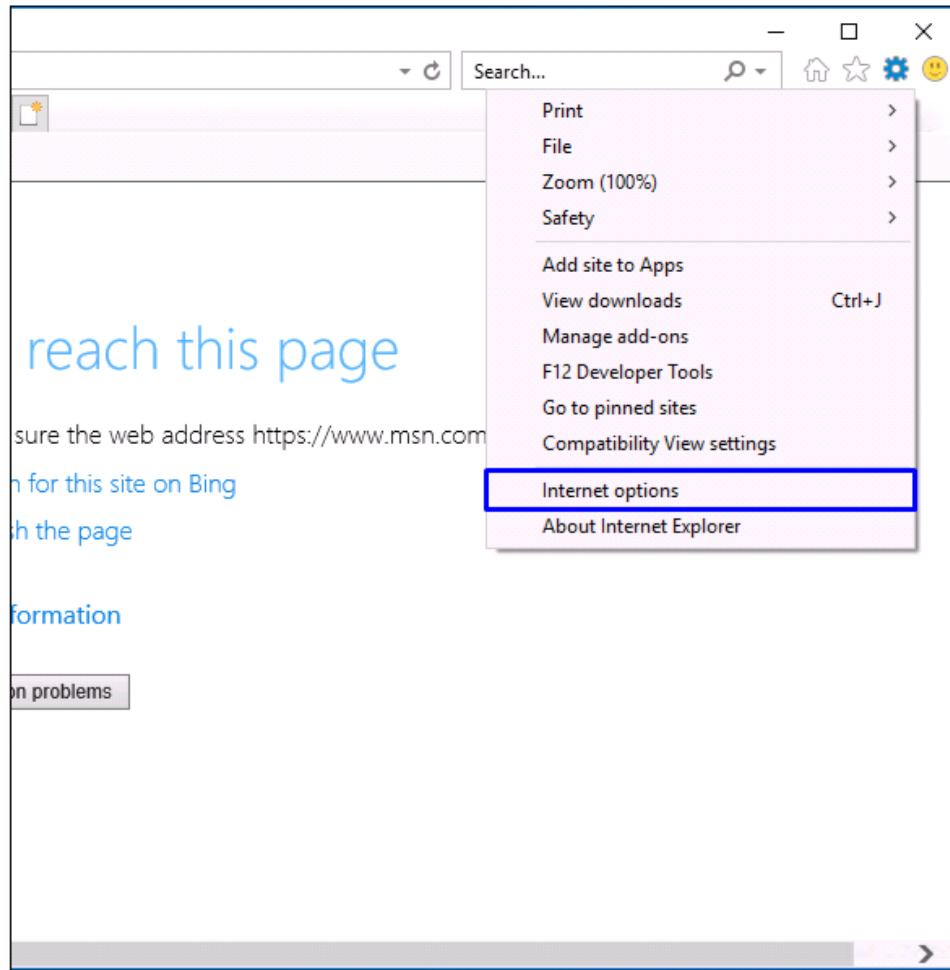
1-1. Internet Explorer Settings

You have to enable JavaScript and ActiveX in [Internet options], add [https://scia.secomtrust.net] to the Trusted sites and set up the Compatibility View.

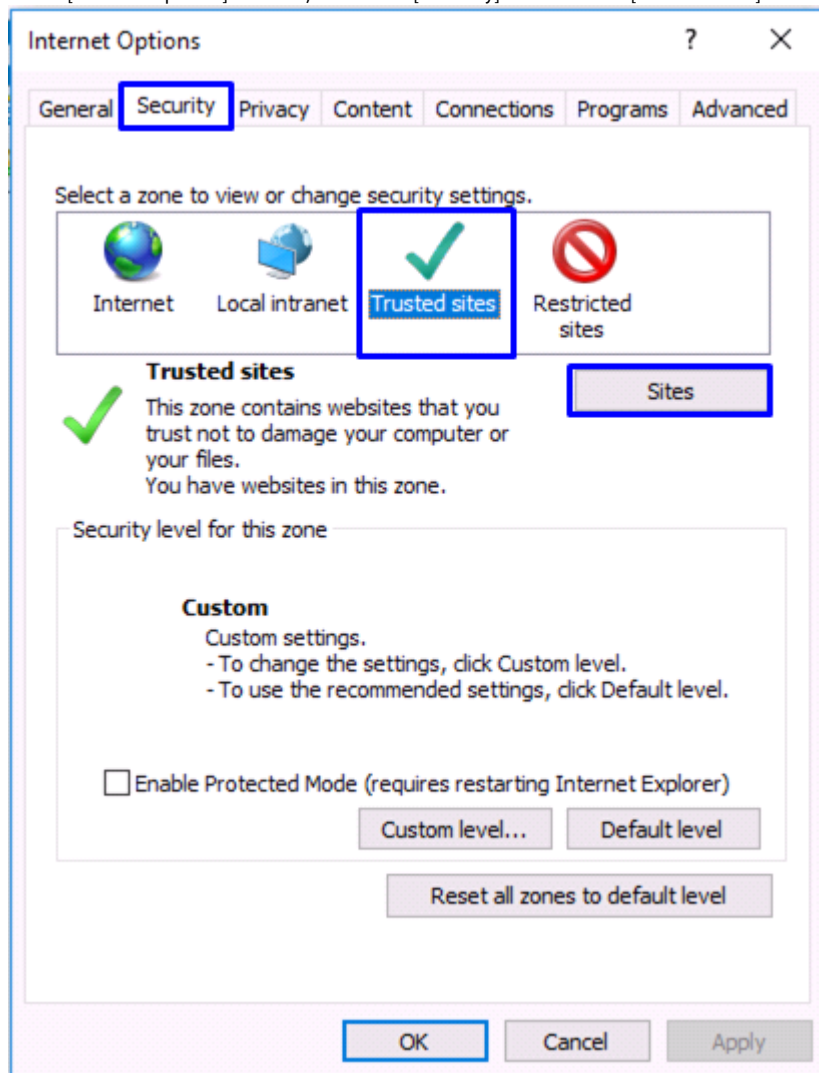
See below for the procedures for these settings.

Setting Internet Options (O)

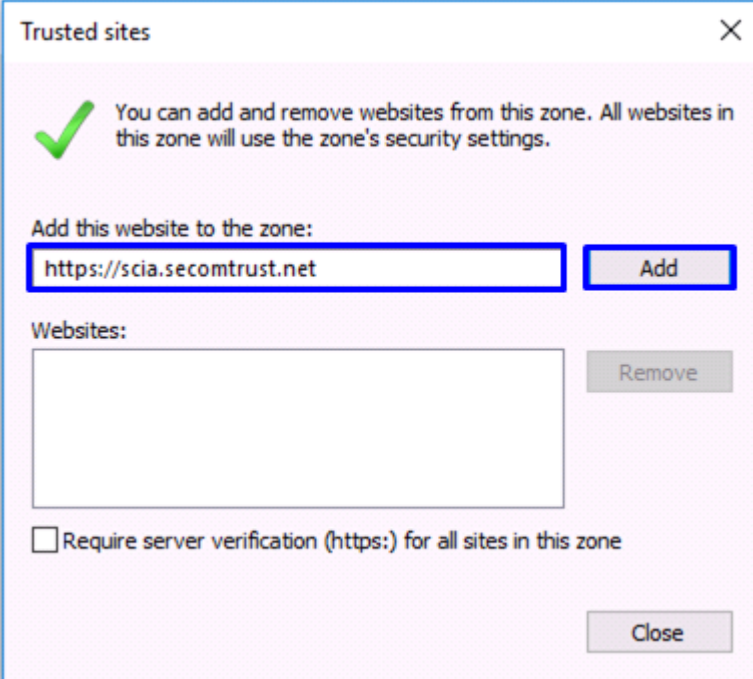
1. You have to add the URL in the Trusted sites first. Open your Internet Explorer, click the [Tools] button, and then click [Internet options (O)].



2. In the [Internet options] window, select the [Security] tab and then [Trusted sites]. Click the [Sites (S)] button.



3. In the Trusted sites dialog box, Enter [https://scia.secomtrust.net] in the [Add this website to the zone:] box and click [Add (A)].<https://scia.secomtrust.net>



Trusted sites

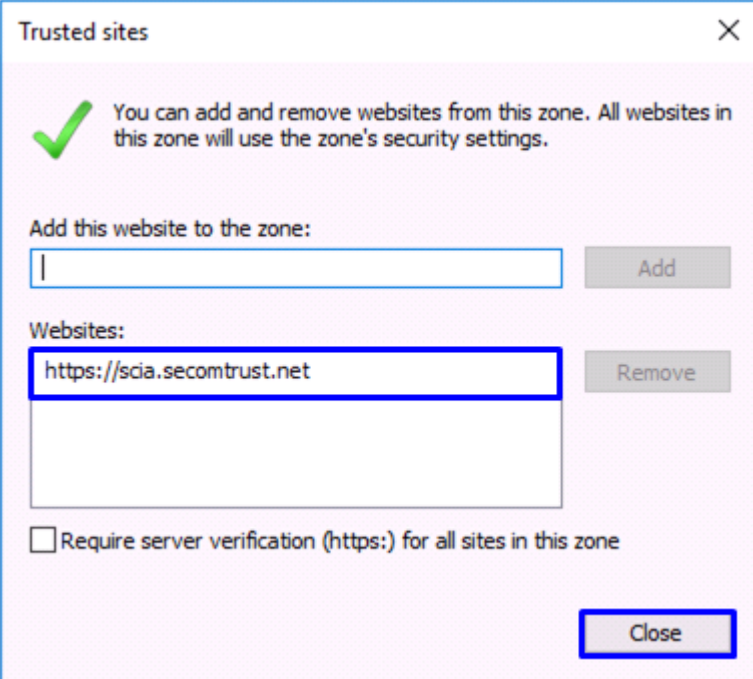
✓ You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

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

4. Make sure that the entered URL now appears in the [Websites (W)] list and click [Close (C)] to finish.



Trusted sites

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

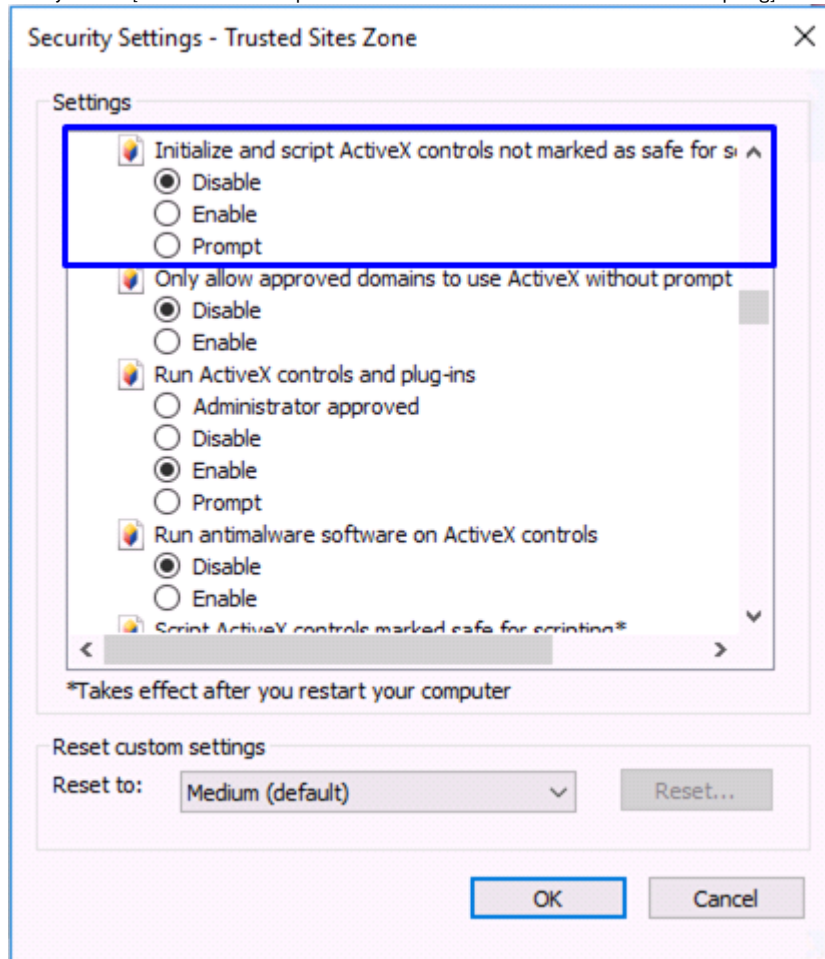
Add this website to the zone:

Websites:

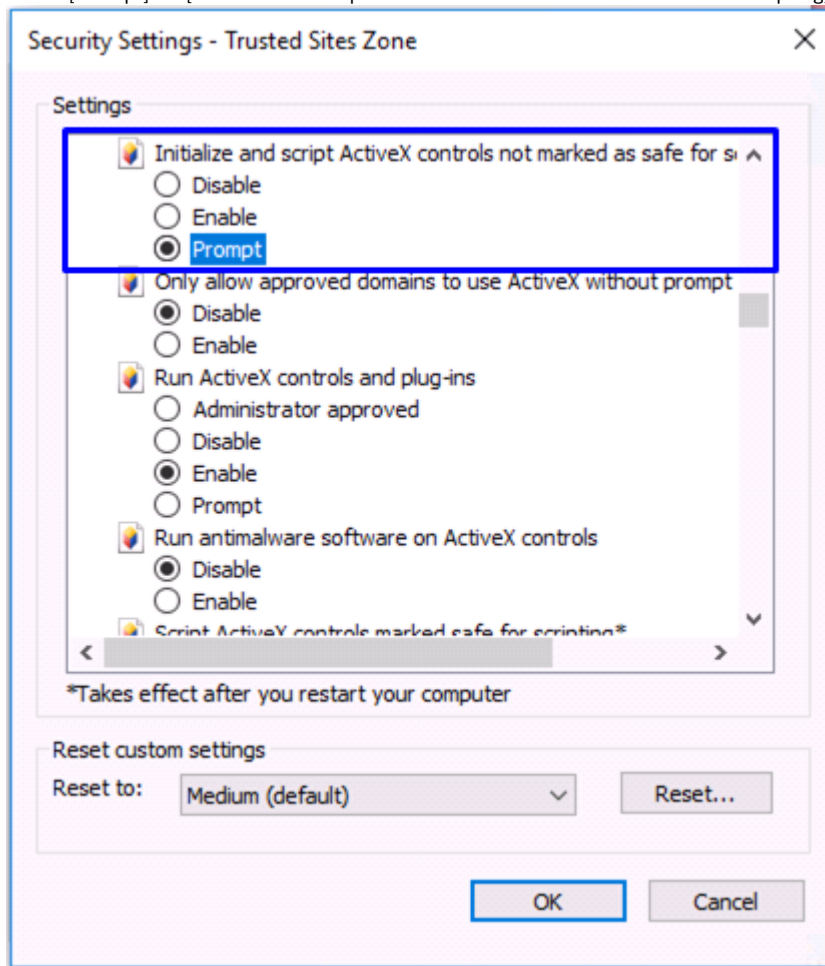
☐ Require server verification (https:) for all sites in this zone

This completes addition of the URL in the Trusted sites.

5. You have to set up JavaScript and ActiveX next. Return to the [Internet options] window and click [Custom level (C)...]. In the [Security Settings - Trusted Sites Zone] window, scroll down the Settings field until you see [Initialize and script ActiveX controls not marked as safe for scripting].



6. Select [Prompt] for [Initialize and script ActiveX controls not marked as safe for scripting].



7. Scroll the Settings field further down to make sure that the [Active scripting] and [Scripting of Java applets] is [Enabled] and then click [OK]. (If [Enabled] is not selected, select it and then click [OK].)

Security Settings - Trusted Sites Zone



Settings

☒ Enable
☐ Prompt

Scripting

Active scripting
☐ Disable
☒ Enable
☐ Prompt

Allow Programmatic clipboard access
☐ Disable
☐ Enable
☒ Prompt

Allow status bar updates via script
☐ Disable
☒ Enable

Allow websites to prompt for information using scripted windows
☐ Disable

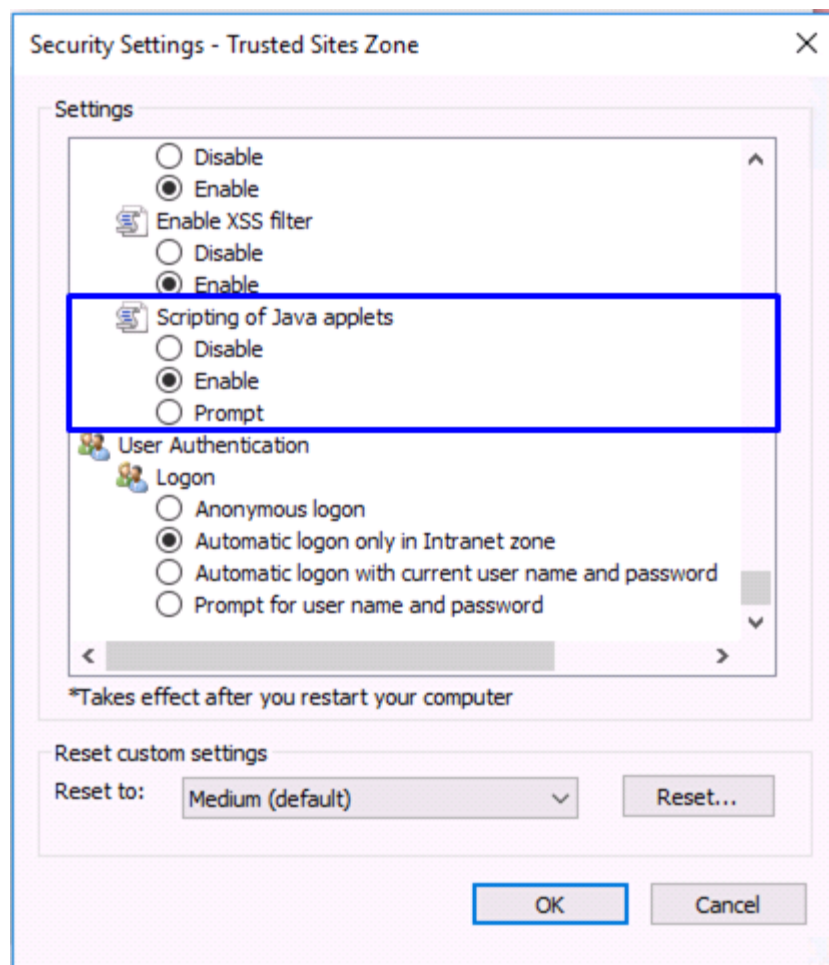
*Takes effect after you restart your computer

Reset custom settings

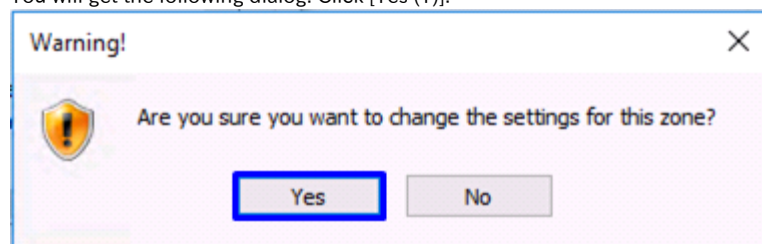
Reset to: Medium (default) v Reset...

OK

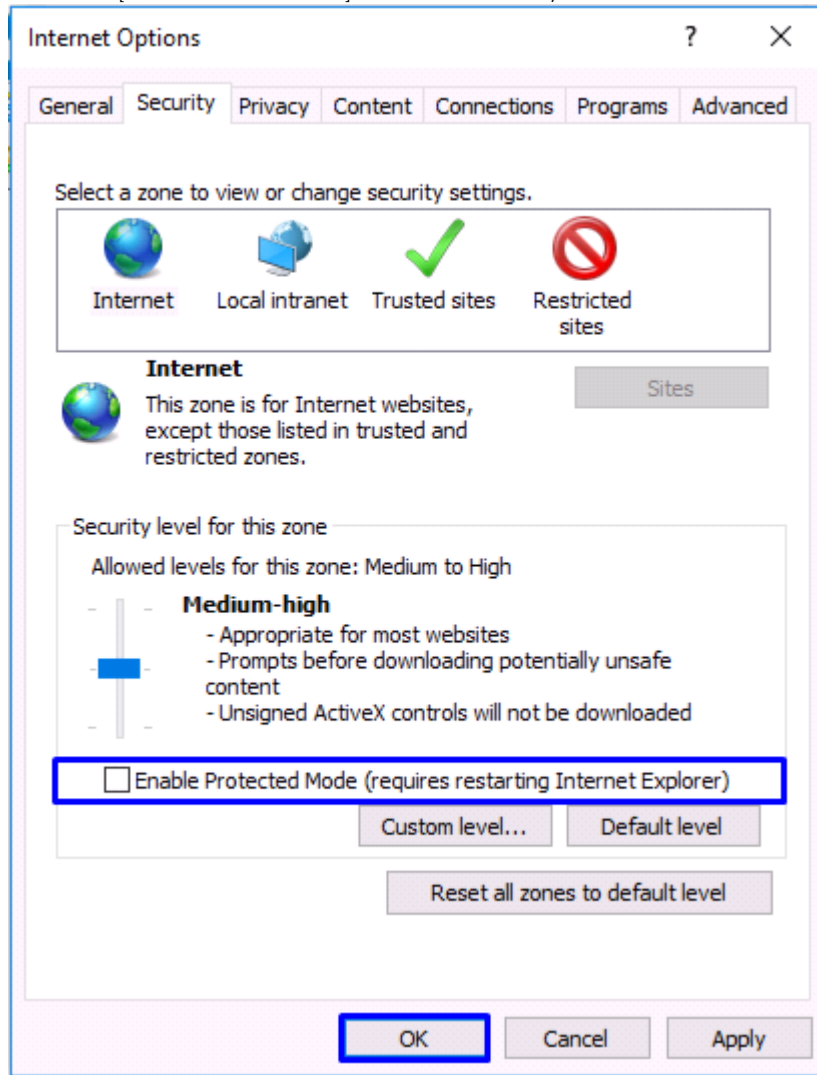
Cancel



8. You will get the following dialog. Click [Yes (Y)].

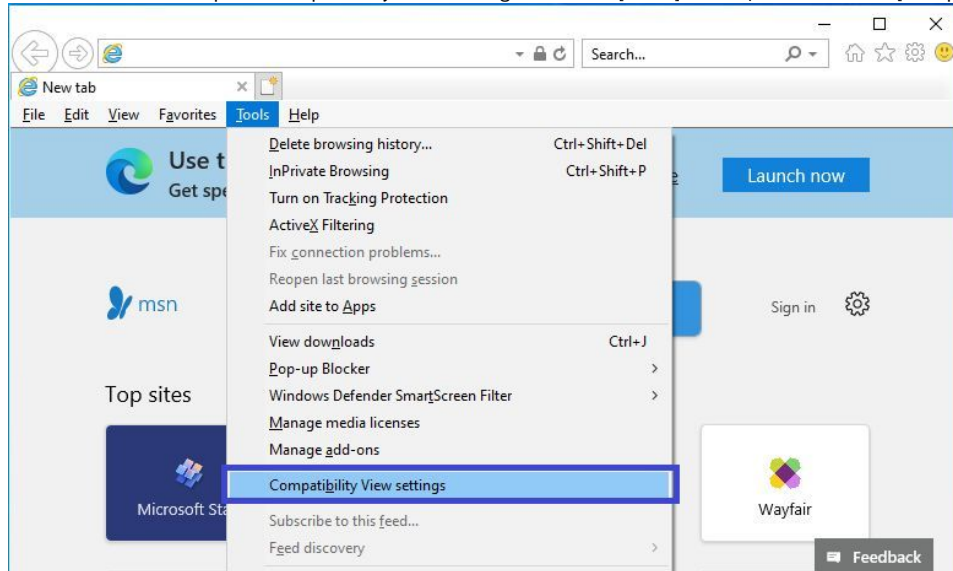


9. Returning to the [Internet options] window, click [OK] to finish.
Note: If the [Enable Protected Mode] checkbox is checked, uncheck it.

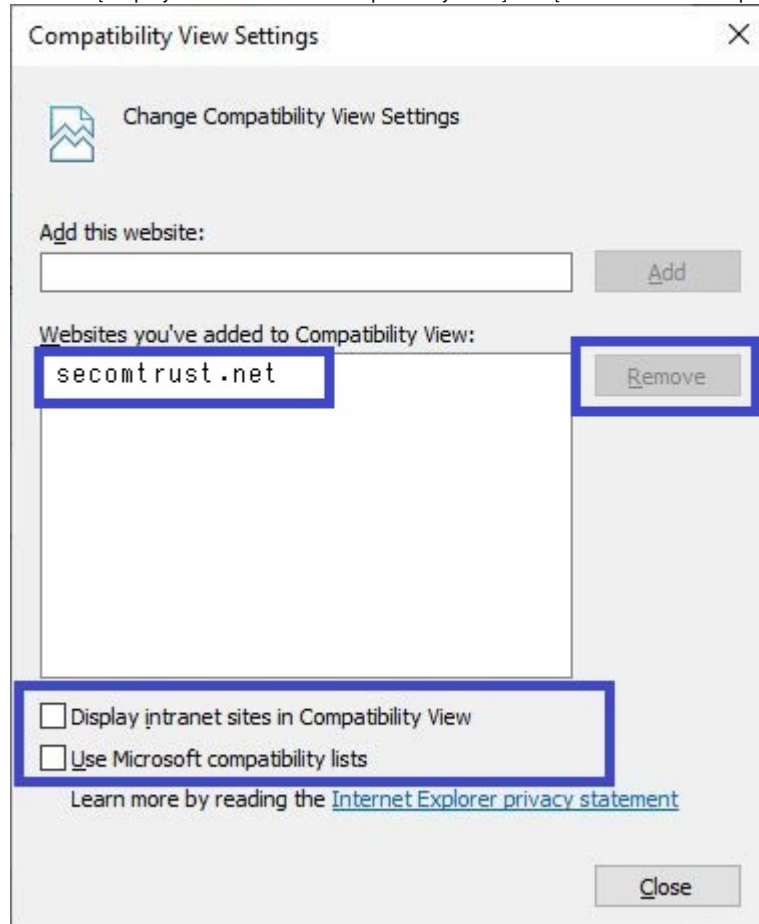


This completes the JavaScript and ActiveX settings.

10. You now have to set up the Compatibility View settings. Click the [Tools] button, and then click [Compatibility View settings].



11. If "secomtrust.net" is included in "Websites you've added to Compatibility View", click [Remove].
Uncheck [Display intranet sites in Compatibility View] and [Use Microsoft Compatibility Lists] if they are checked, and then click [Close].



This completes the Compatibility View settings.

If the compatibility view is set, the error message "SPKAC analysis failed." will be displayed when the certificate is issued.

2. Retrieving the Certificate

2-1. Prerequisites

The prerequisites for retrieving the Certificate are described. Replace the technical terms according to the user environment in which the Certificate will be retrieved.

(The procedures required for Microsoft Internet Explorer 11 are described in this document.)

Prerequisites

1. You have the Access PIN issued by the certificate use administrator;
2. you have received the e-mail designating the certificate retrieval URL; and
3. Microsoft Internet Explorer is installed.

2-2. Certificate Retrieval


2-2-1. Notification of URL for the Certificate Retrieval

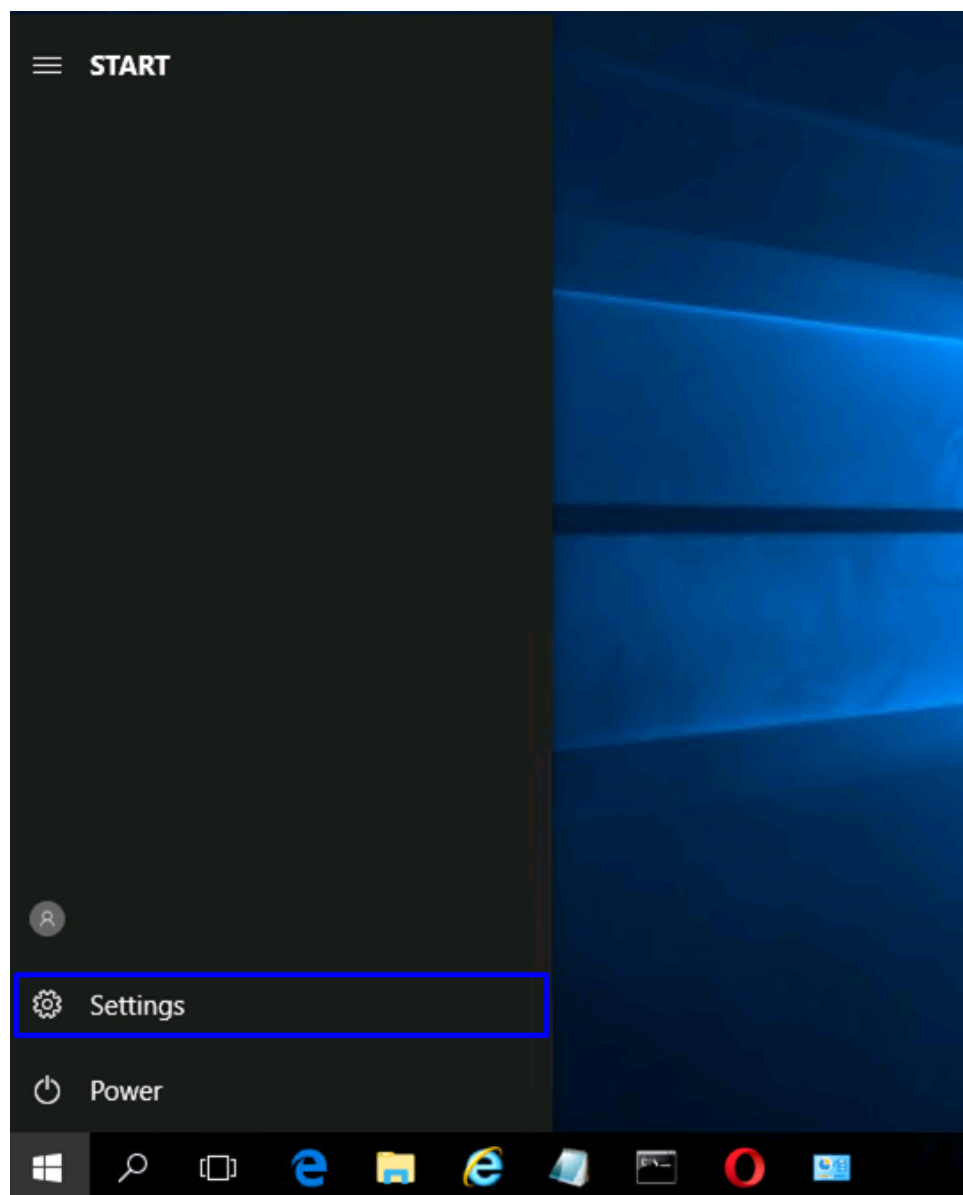
Once you complete the certificate application, you will receive the e-mail from this system that notifies the certificate retrieval URL for the certificate download.
Access the certificate URL in the e-mail message and retrieve the certificate.

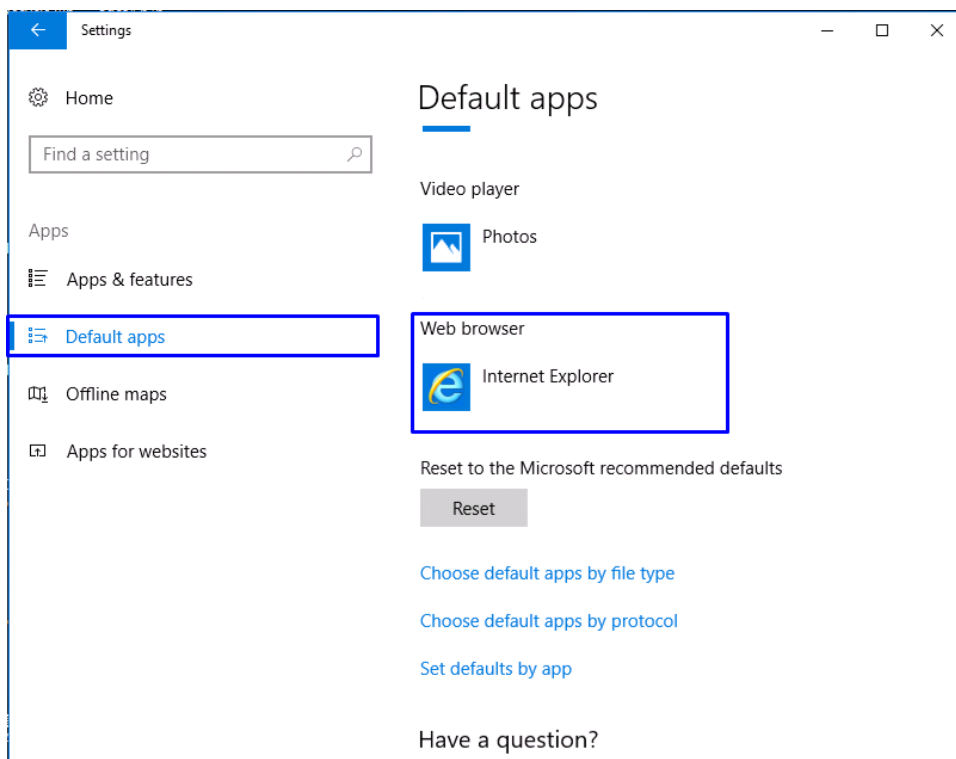
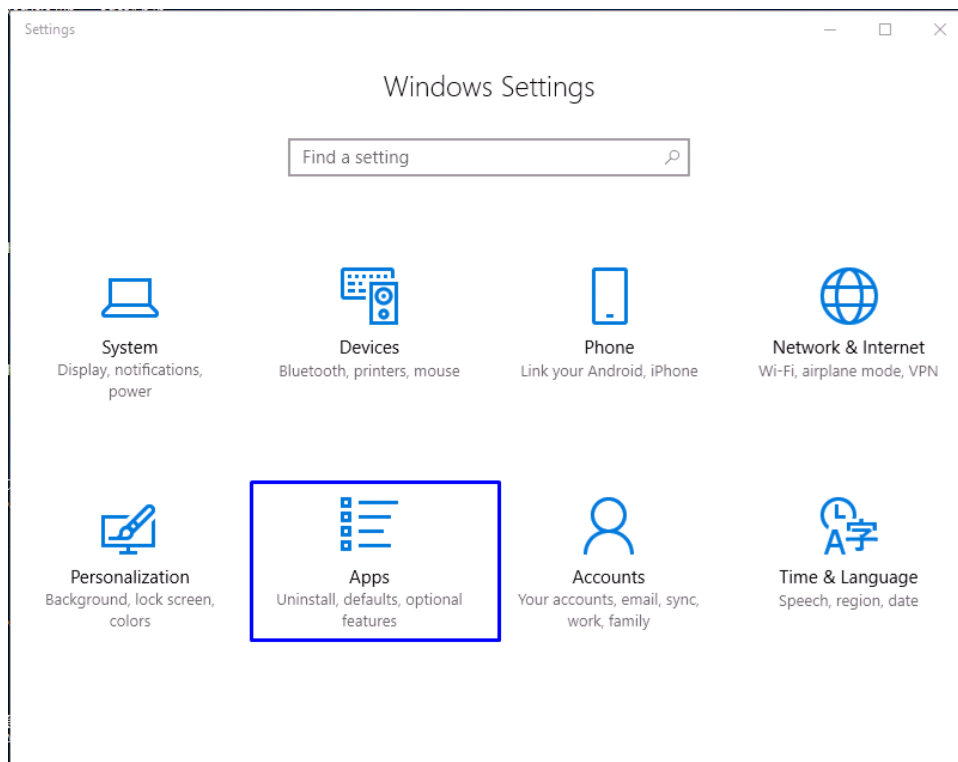
Notification of URL for the Certificate Retrieval
<div>[Title] client certificate issue acceptance notice</div> <div>snip</div> <div># Please find below the URL for the requested certificate retrieval.</div> <div>Please download a client certificate accessing the following certificate acquisition URL. Please correctly enter access PIN acquired at 1) for request of entering access PIN accessing the certificate acquisition URL. The download of a certificate is going to start as the authentication by the access PIN is completed.</div> <div>certificate acquisition URL:https://scia.secomtrust.net/~*(https://scia.secomtrust.net/~) + <- Access this URL to retrieve the Certificate.</div> <div>snip</div>

2-2-2. Retrieving the Certificate Using Internet Explorer

Retrieving the Certificate using [Internet Explorer] is described.

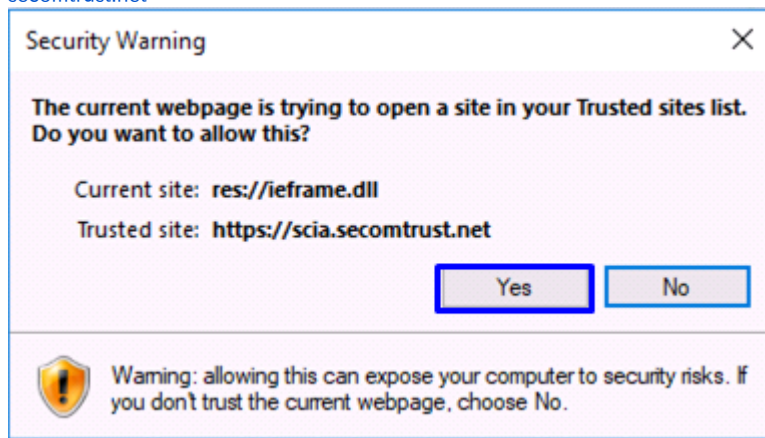
Process of Issuing the Certificate Using Internet Explorer
<div></div> <div>By specifying the web browser used for this system as the [Default] web browser, failure of the client authentication (including access failures) should be prevented.</div> <div>In this document, setting up the following prior to retrieving the certificate is recommended. Select [Settings] in the Windows Menu, and after getting the Settings window, make sure that Internet Explorer is specified as [Apps] > [Default apps] > [Web browser]. If not, specify [Internet Explorer]</div>



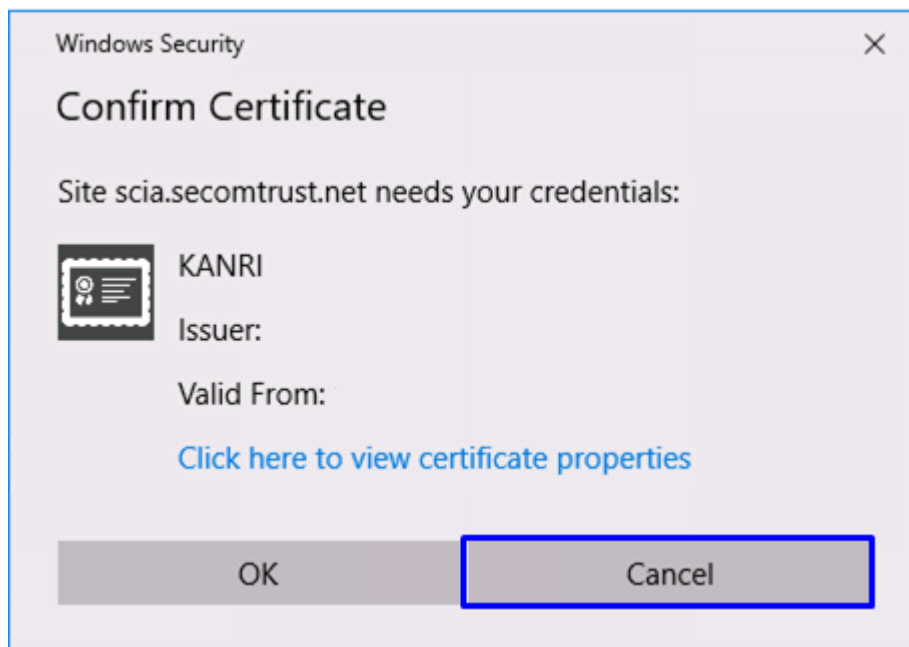


1. To retrieve the certificate using Internet Explorer, changing ActiveX controls in advance is required. For the details, see [1-1 Internet Explorer Settings].

2. According to the instruction in [2-2-1. Notification of URL for the Certificate Retrieval], access the certificate retrieval URL provided in the e-mail.
If the following dialog box pops up, make sure that [https://scia.secomtrust.net] is specified in the Trusted sites and click [Yes].<https://scia.secomtrust.net>



<<Getting the Windows Security dialog box instead?>>
If the selection dialog box of certificate pops up, click [Cancel].



3. In the password prompt, enter the Access PIN you have received.

The screenshot shows the 'Client Certificate Download [STEP1]' screen. At the top, the header includes the logo of the National Institute of Informatics and the text 'National Institute of Informatics UPKI Digital Certificate Issuance Service'. A language selector in the top right corner shows '日本語 / English'. The main content area has a heading 'Client Certificate Download [STEP1]' and instructions: 'To issue the certificate, follow the steps.' Below this, three steps are listed: '[STEP1] Enter the Password.' (highlighted in red), '[STEP2] Issue a certificate.', and '[STEP3] Take a Certificate.'. A second set of instructions follows: '[STEP1] Enter the Password.' and 'Please obtain the access PIN from the administrator and enter it below.' At the bottom, there is a 'Password' label next to a text input field, and a 'Next' button to its right.

- To change the language, click the link in the upper right corner.
Clicking [日本語] changes the language to Japanese.
Clicking [English] changes the language to English.

4. Now, the screen changes to the [Issue a Certificate] screen, make sure that the certificate is actually downloaded.

The screenshot shows the 'Client Certificate Download [STEP2]' screen. The header is identical to the previous screen. The main content area has a heading 'Client Certificate Download [STEP2]' and instructions: 'To issue the certificate, follow the steps.' Below this, three steps are listed: '[STEP1] Enter the Password.', '[STEP2] Issue a certificate.' (highlighted in red), and '[STEP3] Take a Certificate.'. A second set of instructions follows: '[STEP2] Issue a certificate.' and 'Please click the [issue] button. This process may take several minutes.' At the bottom, there are two buttons: 'Previous' and 'Issue' (highlighted with a blue box). Below the buttons, a red 'Caution' message reads: 'Once you click [Issue] button, please wait for until [STEP3] is shown. Please don't close your browser. And also, do not click the [Previous] button. The certificate might be unavailable.'

5. After the certificate is successfully issued, select "Save".

The screenshot shows a standard Windows file save dialog box. The text inside reads: 'Do you want to open or save [redacted] ([redacted] bytes) from [redacted]?' At the bottom, there are three buttons: 'Open', 'Save' (highlighted with a blue box), and 'Cancel'. A small dropdown arrow is visible to the right of the 'Save' button.

6. If the certificate is successfully issued, the certificate will start downloading.
When the download is complete, click the "X" button on your browser to close the browser.

情報・システム研究機構
国立情報学研究所
National Institute of Informatics

National Institute of Informatics
UPKI Digital Certificate Issuance Service

Client Certificate Download [STEP3]

To issue the certificate, follow the steps.

[STEP1] Enter the Password.
[STEP2] Issue a certificate.
[STEP3] Take a Certificate.

[STEP3] Take a Certificate.

The certificate has just been issued.
please exit the browser used.

7. In order to import the downloaded P12 file, please refer to the Please refer to the manual below to import it.
It is recommended that you back up this file. However, please handle it with care.

[Internet Explorer/ Edge/ Chrome/ Opera \(Windows\) Edition](#)

8. Checking the existence of the certificate
To check if the certificate import is complete, refer to the following manual.

[Checking Existence of the Certificate Using Internet Explorer](#)