[Important notice] To the customers those who use SSL client authentication

Please follow the steps below when using SSL client authentication.

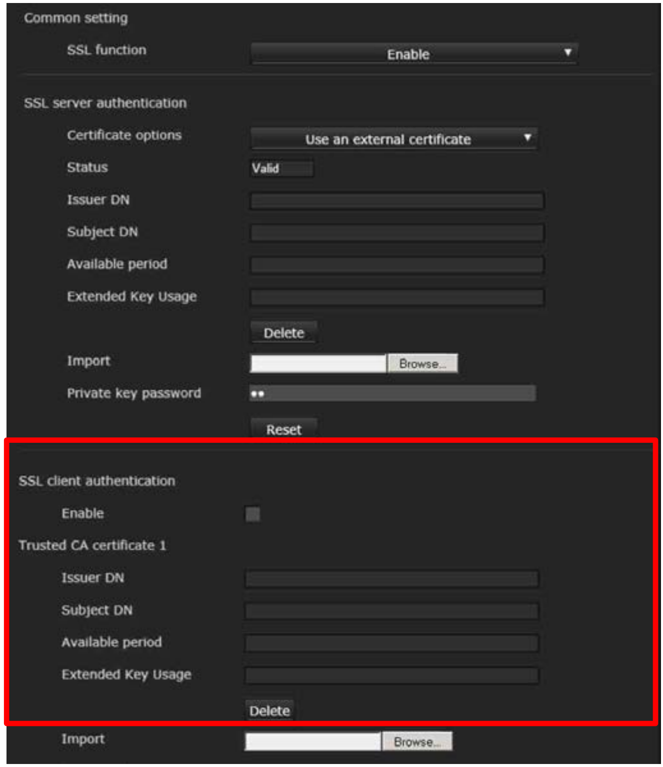
■If you enable SSL client authentication for the first time after updating camera firmware to V3.0, please follow [Step-1] and [Step-2] in order.

■If you already enabled SSL client authentication with camera firmware version earlier than V3.0, please make sure to follow [Step-2] BEFORE updating camera firmware to v3.0.

【Step-1】

Configure SSL client authentication

You can manage the CA certificate needed for the camera to use SSL client authentication in the [SSL] tab. Please refer to the existing user's guide regarding [Common setting] and [SSL server authentication] in this [SSL] tab.



Common setting

SSL function: Enable

SSL server authentication

Certificate options: Use an external certificate

Status: Valid

Issuer DN

Subject DN

Available period

Extended Key Usage

Delete

Import: Browse...

Private key password: ••

Reset

SSL client authentication

Enable ☐

Trusted CA certificate 1

Issuer DN

Subject DN

Available period

Extended Key Usage

Delete

Import: Browse...

Configure [SSL client authentication]

Note

- When using the client authentication, the personal certificate must be successfully installed on the PC being used. If it’s not installed, do NOT configure this tab or you may not be able to connect to the camera. For more detail, please refer to the [Step-2] Import personal certificate.
- The setting of SSL client authentication is available only when SSL server authentication certificates are uploaded.

1. Open [SSL] tab from the [Security] under [Setting] for administrator.

2. Click [Browse…] button for [Trusted CA certificate 1] and select the CA certificate to be imported to the camera.

3. Click [OK] button in the pop-up dialog, and the selected file will be imported to the camera.
   Up to 4 CA certificates can be imported to one camera. Supported file type of certificate is PEM.

4. Check the checkbox to enable SSL client authentication and click [OK] button.

Note

Importing process will be invalid if the selected file is not a CA certificate.

To display the information of the CA certificate

When the CA certificate has been successfully stored in the camera, its information appears on [Issuer DN], [Subject DN], [Available period], and [Extended Key Usage] for your reference.

To delete the CA certificate

Click [Delete] to delete the selected CA certificate from the camera.

Tip

When enabling the client certificate, the following steps in order are recommended.

1. Import the necessary CA certificates.
2. Check the [Enable] checkbox for SSL client authentication and click [OK].

Note

Once you check the [Enable] checkbox for SSL client authentication and click [OK], the camera will immediately enable the client authentication.
Therefore make sure that the personal certificate on your PC is successfully installed before you enable SSL client authentication.

For more detail, please refer to the [Step-2] Import personal certificate.

【Step-2】

Import personal certificate

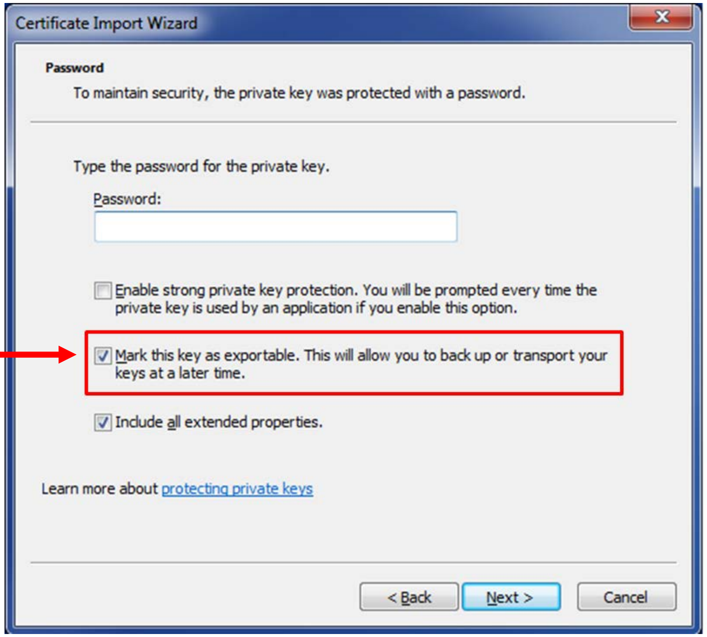
Please follow the steps below to import the personal certificate when using SSL client authentication.

1. Double click the stored personal certificate on your PC.

2. [Certificate Import Wizard] will pop-up.

3. Check the [Mark this key as exportable] checkbox in the middle.

4. Follow the instruction to complete the import.



Certificate Import Wizard

Password

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

Type the password for the private key.

Password:

□ 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.

☑ Include all extended properties.

Learn more about protecting private keys

☑ Check