

FLProtection[®]

User's Manual



FOURTHLOGIC

CONTENTS

4 GETTING STARTED

- 4 What is FLProtection®?
- 4 Product Contents
- 4 System Requirements
- 5 Installation

8 FLPROTECTION® FEATURES

- 8 User Interfaces
- 9 User registration
- 10 Signing In
- 11 Protecting a software
- 13 Generating Product Certificates
- 14 Generating Rights Certificates
- 16 Insert R/C into Dongle
- 17 Eject R/C from Dongle
- 18 Dongle Firmware Update
- 19 Certificate Verification
- 23 Dongle Verification

25 CERTIFICATES

- 25 Developer Certificates
- 25 Product Certificates
- 25 Rights Granter Certificates
- 25 Rights Certificates

27 DONGLE SPECIFICATION

- 27 Overall Structure
- 27 Indicator Specification
- 28 Changing Dongle LED Status

29 HOW TO USE FLPROTECTION®

- 29 Protecting a software
- 31 Generating Rights Certificates
- 32 Running a protected software

34 TROUBLESHOOTING

- 34 When the Indicator is Red
- 34 When the Indicator has faded

GETTING STARTED

1. What is FLProtection®?

FLProtection® is a certificate-based software license protection platform that supports USB Dongle and Network certification simultaneously. FLProtection® uses RSA2048 and AES256 to encrypt software, protects memory and your software license from crackers with powerful anti-debugging techniques.

2. Product Contents

Check if the following contents are included in the product box. If there are any missing, please contact the retailer where you purchased the product. Actual products and accessories may differ from the illustrations in this user's manual.

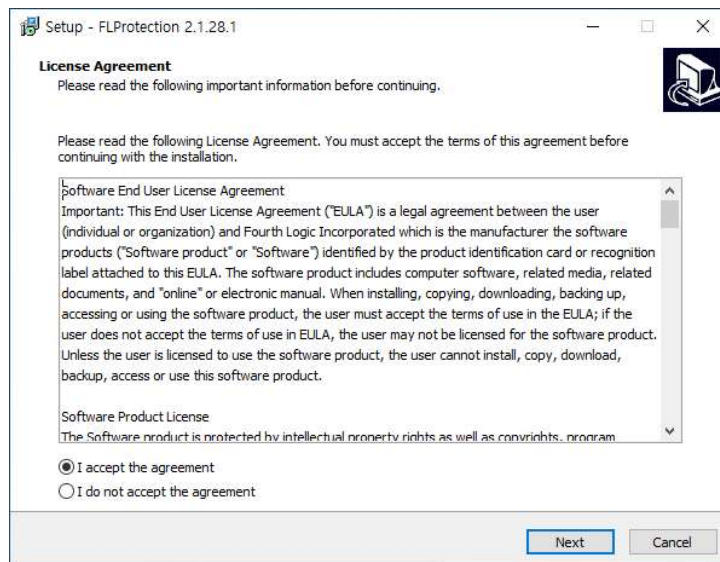
- FLProtection® USB Dongle
- FLProtection® USB Dongle cover
- User's Manual (PDF)

3. System Requirements

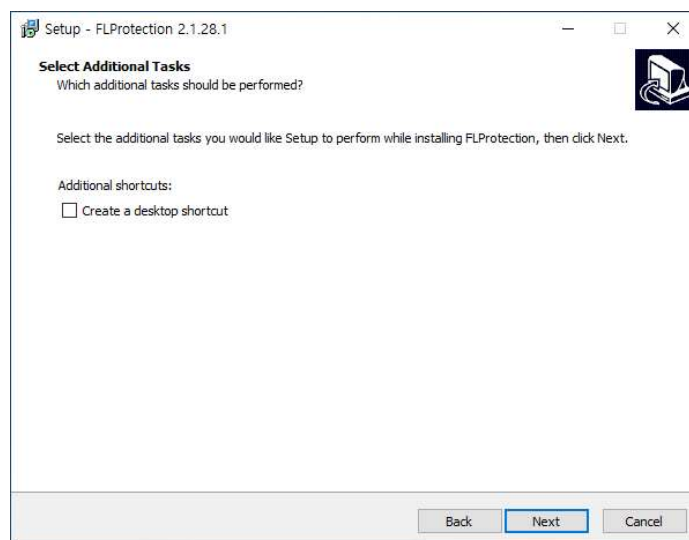
Device / Software	Minimum Requirements	Recommended
Operating System	Windows 7	Windows 10
System Memory	4GB	8GB
CPU	Sandy Bridge i3	Skylake i5
USB Port	USB 2.0 or over	USB 2.0 or over
Free Storage Space	50MB	1GB

4. Installation

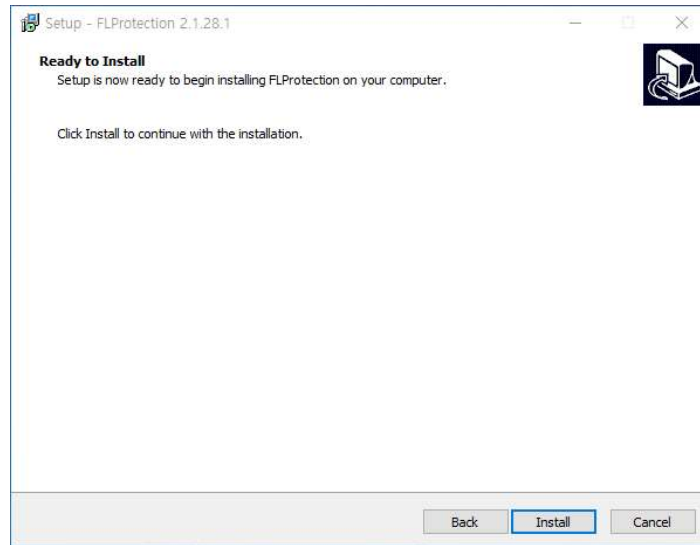
Go to <https://resource.fourthlogic.co.kr/flprotection/flprotectionsetuplatest.zip> to download the latest FLProtection® installation file.



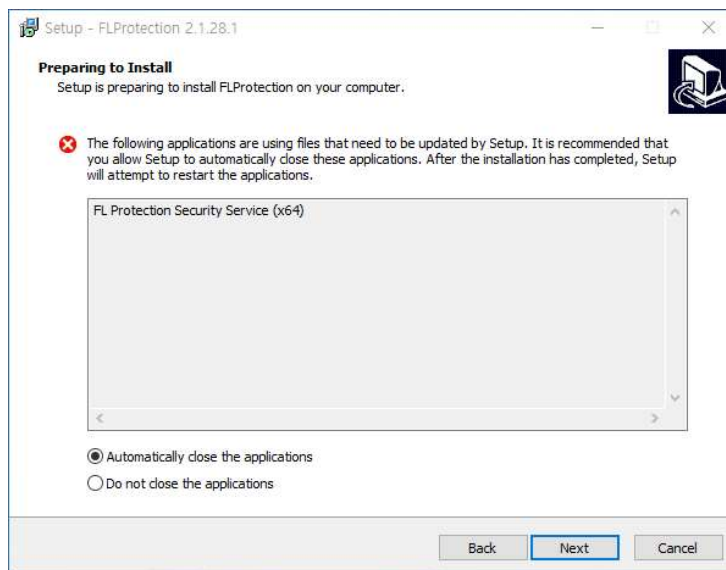
Launch the FLProtection® installation program. Read the license agreement carefully and agree to the License Agreement and click the “Next” button to proceed with the installation.



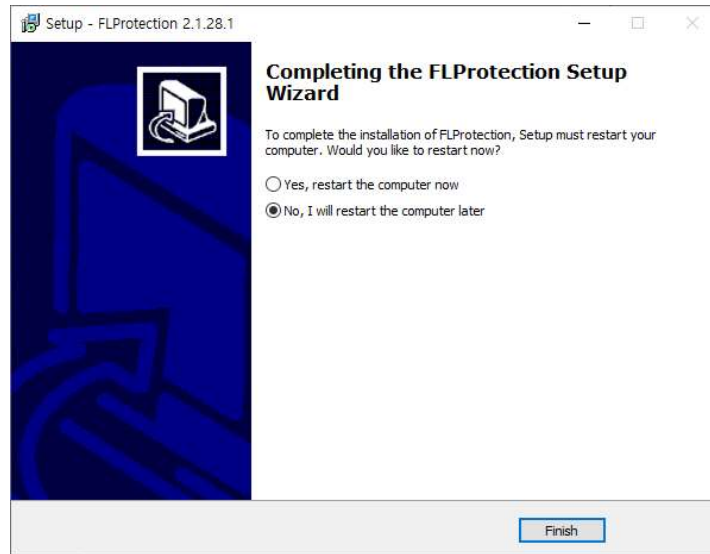
After setting the shortcut, click the “Next” button to proceed with the installation.



Click “Install” to proceed with the installation.



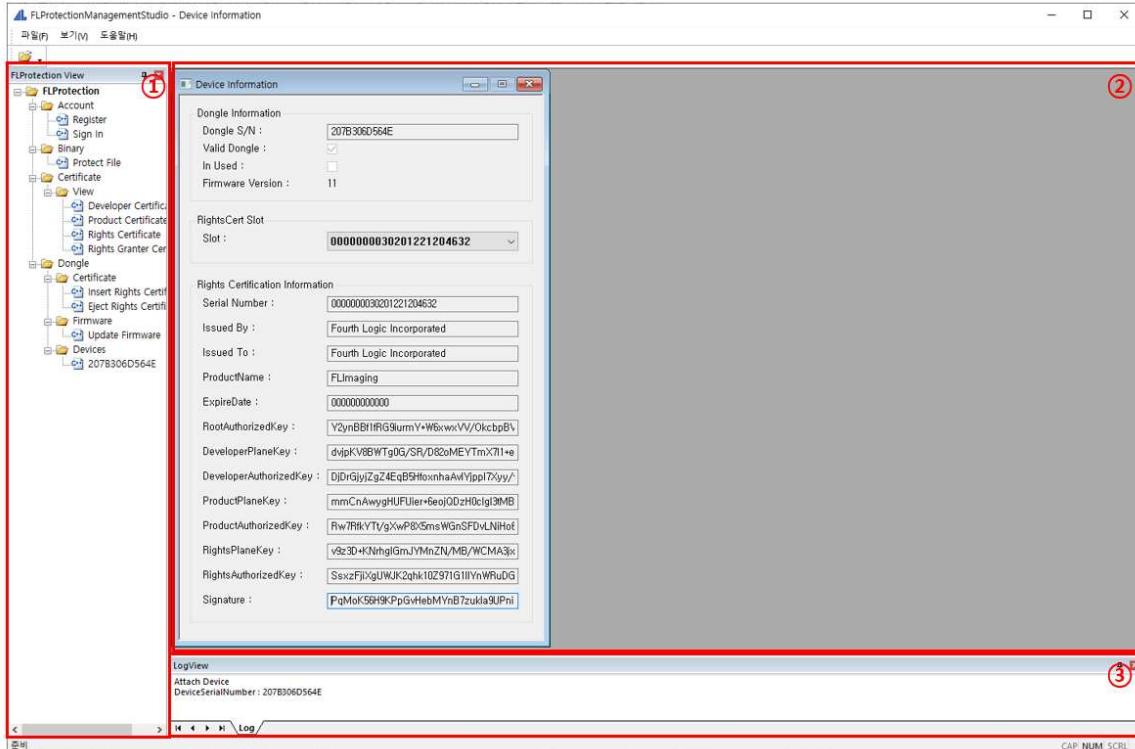
If FLProtection® is running, select “Automatically close the applications” in the next window and click the “Next” button to close FLProtection® and proceed with the installation.



When the installation is successfully completed, select whether to restart the computer to complete the installation (not necessary).

FLPROTECTION® FEATURES

1. FLProtection® User Interface



The composition of FLProtection® user interface is as follows.

① Menu Tree

You can use each FLProtection® function by selecting a menu item in the Menu Tree.

② Main Window

In the Main Window, windows related to the function selected in the Menu Tree are displayed.

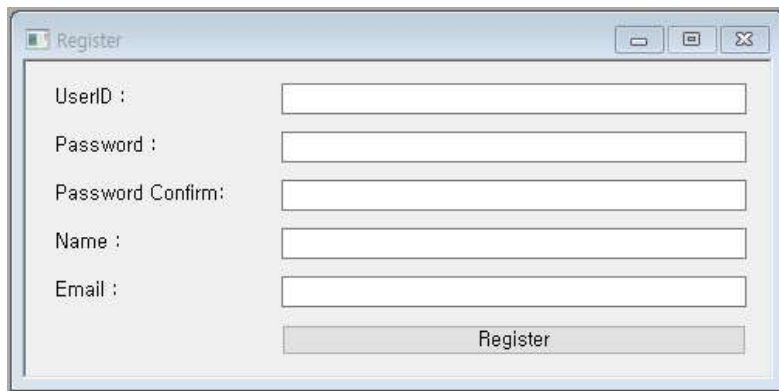
③ Log View

You can check the log of FLProtection® in Log View.

2. User registration



Double-click **Account > Register** in the Menu Tree to open the Register window.

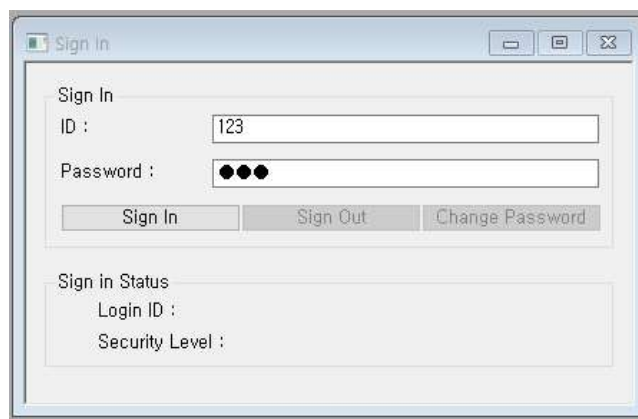
A screenshot of a "Register" dialog box. It contains five input fields stacked vertically, each with a label to its left: "UserID :", "Password :", "Password Confirm:", "Name :", and "Email :". Below these fields is a single button labeled "Register". The dialog box has a standard Windows-style title bar with minimize, maximize, and close buttons.

Enter User ID, Password, Confirm Password, Name, Email in the Register window and click the **“Register”** button to register.

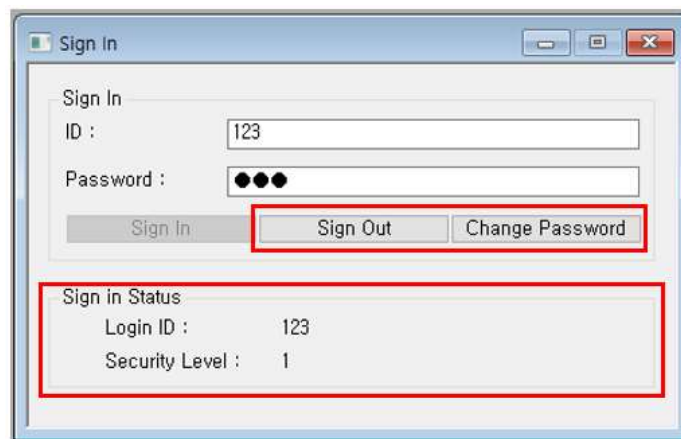
3. Signing in



Double-click **Account > Sign In** in the Menu Tree to open the Sign in window.



Enter your User ID and Password in the Sign In window and click the “**Sign In**” button to sign in.

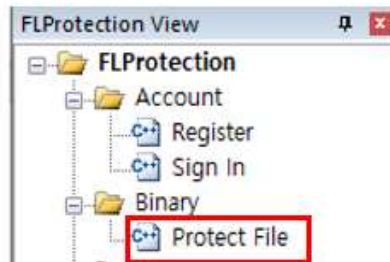


If signing in is successful, **Login ID** and **Security Level** are displayed in the Sign in Status below, and the “**Sign Out**” and “**Change Password**” buttons are activated. You can sign out by clicking the “**Sign Out**” button or change the password by clicking the “**Change Password**” button.

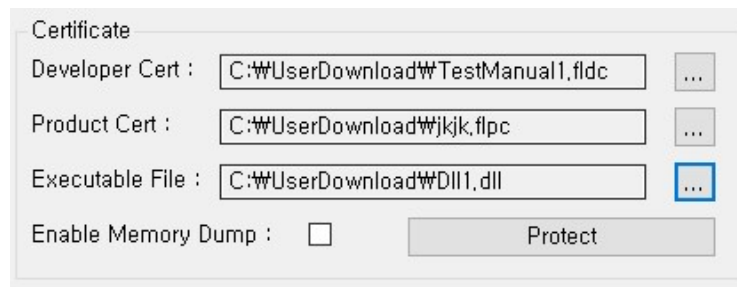
4. Protecting a software

Protecting a software requires a **Developer Certificate** and a **Product Certificate**, and can be performed only when a **Security Level 3 or higher account** is signed in.

Sign in with a Security Level 3 or higher account.



Double-click **Binary > Protect File** in the Menu Tree to open the Protect File window.



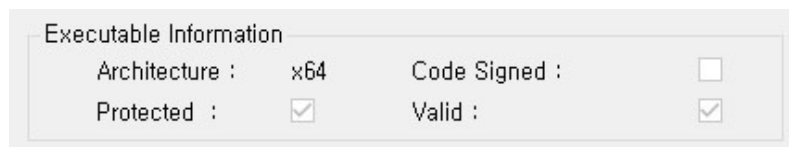
Click the “...” button to the right of the “**Developer Cert**” and enter the file path of the Developer Certificate file (*.fldc).

Click the “...” button to the right of the “**Product Cert**” and enter the file path of the Product Certificate file (*.flpc).

Click the “...” button to the right of the “**Executable File**” and enter the path of the program to be protected. Programs to be protected must not be code signed.

You can select whether or not to enable creating a dump file by checking or unchecking the “**Enable Memory Dump**” check box.

When the “**Protect**” button is activated, press the button to perform program protection.



You can check whether the program is code signed, protected, or valid through the contents of the “**Executable Information**” group box.

Certificate Information	
Serial Number :	0000000441210217165005
Issued By :	Fourth Logic Incorporated
Issued To :	jkjk
ProductName :	jkjk
RootAuthorizedKey :	Y2ynBBf1fRG9iurmY+W6xwxVV/Okcb
DeveloperPlaneKey :	RF9g83MiMydEb3DkJC/Df3aVtCWxe8
DeveloperAuthorizedKey :	cx1O1K9Z25iR9xmcY3OzqWUd3tSQB
ProductPlaneKey :	voDTpYGDtWw+J3WOi7r3AqbMfcU\
ProductAuthorizedKey :	u7gtMr8L5gOwLjHa0AeD5SOqaGa6aw
Signature :	IA8vvtg48Puao6ZtxARpuhhaXID8kyWfC

You can check the contents related to the certificate of the currently encrypted program through the contents of the “Certificate Information” group box.

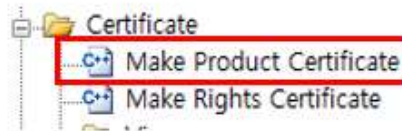
When the program encryption process is completed successfully, “Protected” and “Valid” items are checked.

Note: When signing an EV(Extended Validation) code to a program, you must sign the EV code after encrypting the program with FLProtection®.

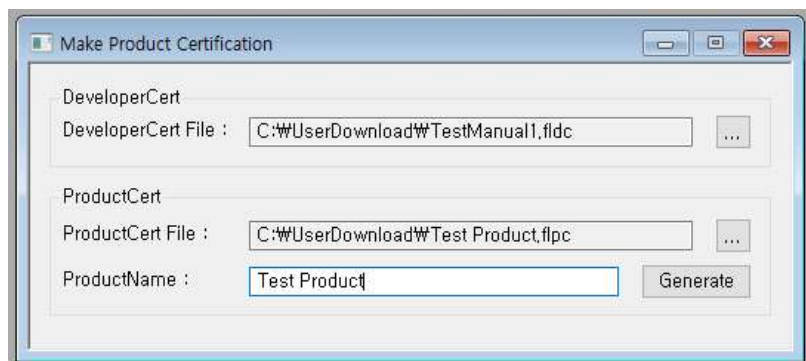
5. Generating Product Certificates

Generating Product Certificates requires a **Developer Certificate**, and can be performed only when a **Security Level 3 or higher account** is signed in.

Sign in with a Security Level 3 or higher account.



When signing into an account with Security Level 3 or higher, the **Certificate > Make Product Certificate** menu item appears in the Menu Tree. Double-click on the **Make Product Certificate** menu item to open the Make Product Certificate window.



Click the “...” button to the right of the “**DeveloperCert File**” and enter the file path of the Developer Certificate (*.fldc).

Click the “...” button to the right of the “**ProductCert File**” and enter the file path of the Product Certificate that will be created (*.flpc).

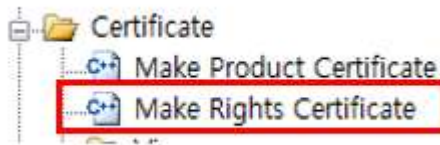
Enter the Product Certificate name in the Edit box and click the “**Product Certification**” button to create a Product Certificate.

After entering the product name, click the “**Generate**” button to generate a Product Certificate.

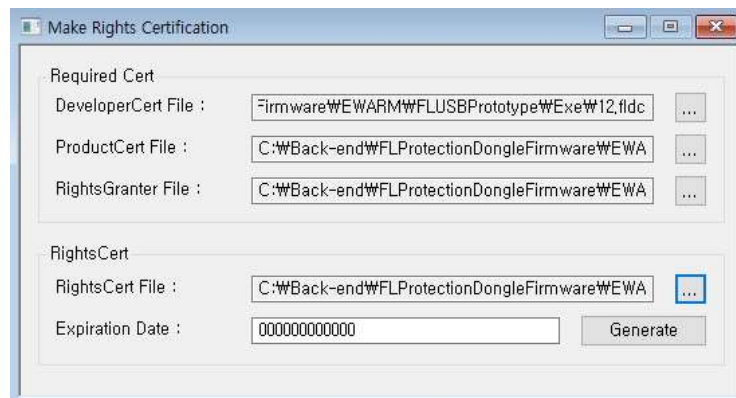
6. Generating Rights Certificates

Generating Rights Certificates requires a **Developer Certificate**, a **Product Certificate** and a **Rights Granter Certificate**, and can be performed only when a **Security Level 3 or higher account** is signed in.

Sign in with a Security Level 3 or higher account.



When signed in with a Security Level 3 or higher account, the **Certificate > Make Rights Certificate** menu item appears in the Menu Tree. Double-click the **Make Rights Certificate** menu item to open the Make Rights Certificate window.



Enter the path of the Developer Certificate (*.fldc), Product Certificate (*.flpc), and Rights Granter Certificate (*.flrgc) by clicking the “...” button to the right of each lists.

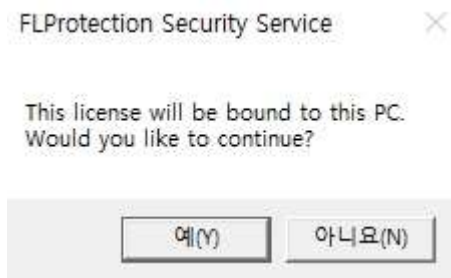
Click the “...” button to the right of the “**RightsCert File**” item and enter the file path of the Product Certificate that will be created (*.flrc).

Set the Expire Date at the “**Expired Date**” item. The format is YYYYMMDDHHmm, for example, if the Expiration Date is January 2, 2021 at 1:40 PM, enter 202101021340. If the Expiration Date is 000000000000, it is set permanent.

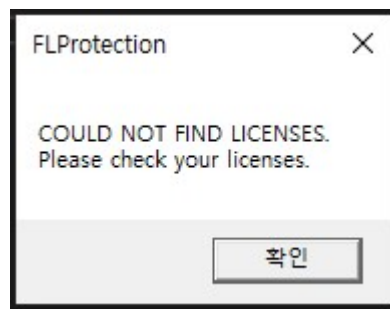
Click the “**Generate**” button to generate a Rights Certificate (*.flrc).

When the creation of the Rights Granter Certificate is complete, the Rights Granter Certificate used at this time cannot be reused. Once the Rights Certificate is generated, the extension of the used Rights Granter Certificate is changed to ***.used**.

When using a program protected by FLProtection® with network certification, the Rights Certificate must be in the same folder as the protected program to run the program.



When using network certification, the first time you use a program protected by FLProtection®, you will be asked if you want to bind the Rights Certificate to your PC. If you proceed, the right certificate will be bound to the PC. If you do not, the protected program will not run.



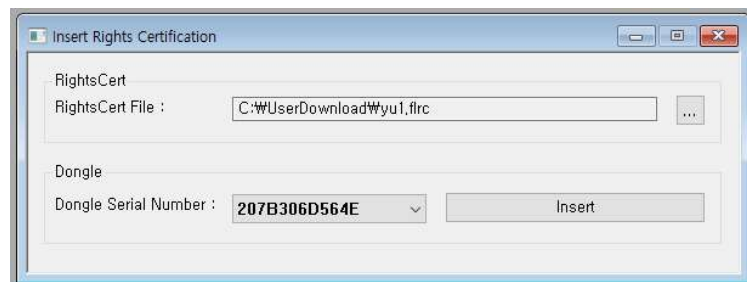
When running a program protected by FLProtection®, if the certificate cannot be found, the following pop-up window is displayed. In this case, you must check the certificates, Dongle, and the operating status of the FLProtection® service.

7. Insert R/C(Rights Certificate) into Dongle

If the Dongle is not connected to PC, connect it.



Double-click the **Dongle** > **Certificate** > **Insert Rights Certificate** menu item in the Menu Tree to open the Insert Rights Certificate window.



Click the “...” button to the right of the “**RightsCert File**” item and enter the path to the Rights Certificate (*.flrc).

Select the Dongle's **Serial Number** to insert the right certificate.

Click the “**Insert**” button to insert the right certificate into the Dongle.

Note: Network certification is not possible with the certificate inserted into the Dongle.

Note 2: Only up to 10 certificates can be inserted into the Dongle.

8. Eject Rights Certificate from Dongle

If the Dongle is not connected to PC, connect it.



Double-click the **Dongle > Certificate > Eject Rights Certificate** menu item in the Menu Tree to open the Eject Rights Certificate window.



Select the Dongle Serial Number of which you want to remove the right certificate.

Click the “...” button to the right of the “**RightsCert File**” item and specify the file path to save the Rights Certificate to be extracted.

Select the serial number of the right certificate to be ejected.

Click the “**Eject**” button to extract the Rights Certificate in Dongle.

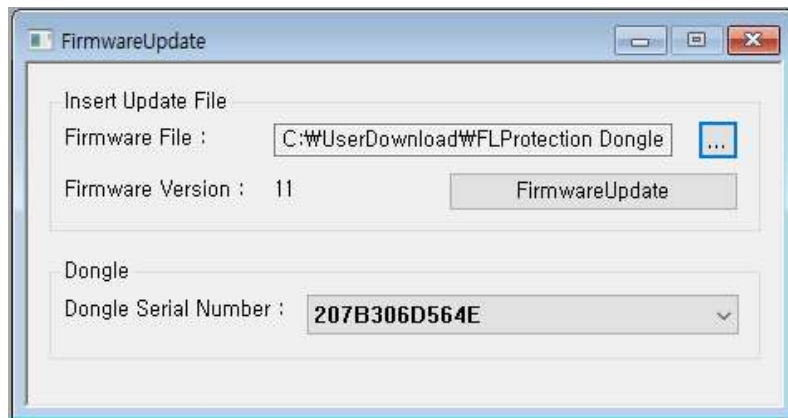
9. Dongle Firmware Update

Go to <https://resource.fourthlogic.co.kr/flprotection/flprotectionfirmwarelatest.zip> to download the latest Dongle firmware update file.

If Dongle is not connected to PC, connect it.



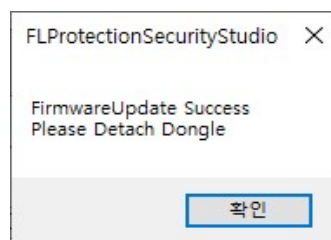
Double-click the **Dongle > Firmware Update** menu item in the Menu Tree to open the Firmware Update window.



Click the “...” button to the right of the “**Firmware File**” in the Firmware Update window and enter the path to the firmware update file (*.out).

After selecting the Serial Number of the Dongle to be updated, click the “**FirmwareUpdate**” button to update the firmware.

Note: Do not disconnect the Dongle or exit FLProtection® during the firmware update. It is a major cause of device failure, and A/S is not possible in this case.



After the firmware update is complete, press the OK button on the pop-up window to close the window, disconnect and reconnect the Dongle to the PC again to complete the firmware update.

10. Certificate Verification

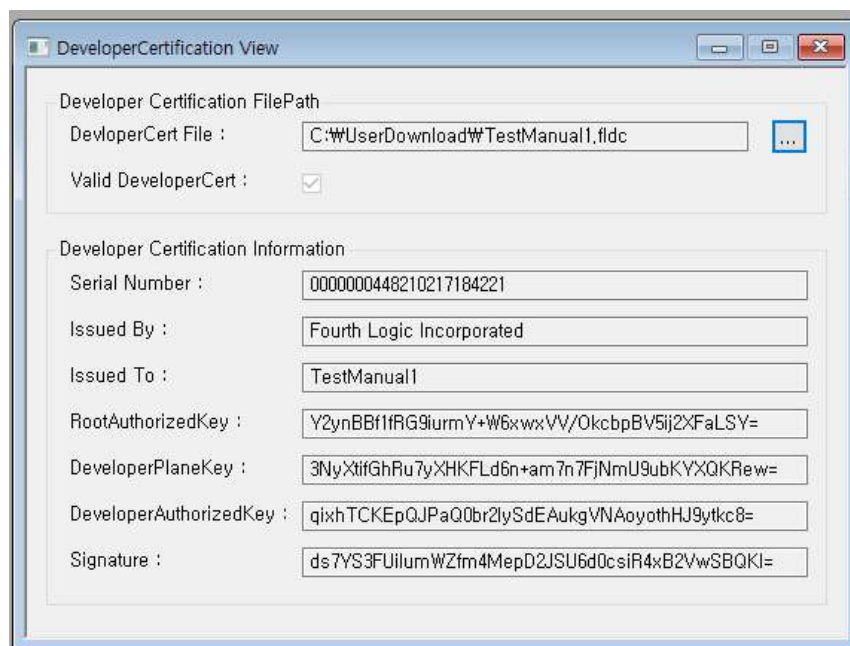


You can check the certificate by selecting the type of certificate you want to check from the sub-items of **Certificate** > **View** in the Menu Tree.

Enter the file path of the certificate (*.fldc, *.flpc, *.flrgc, *.flrc) to check the contents of the certificate.

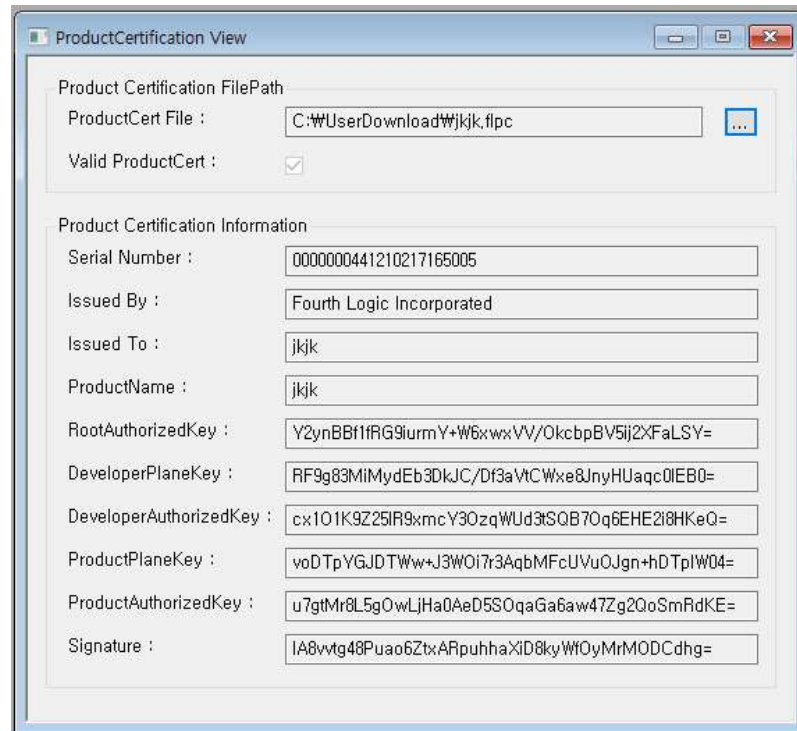
The contents that can be checked in each certificate are as follows.

- Developer Certificate



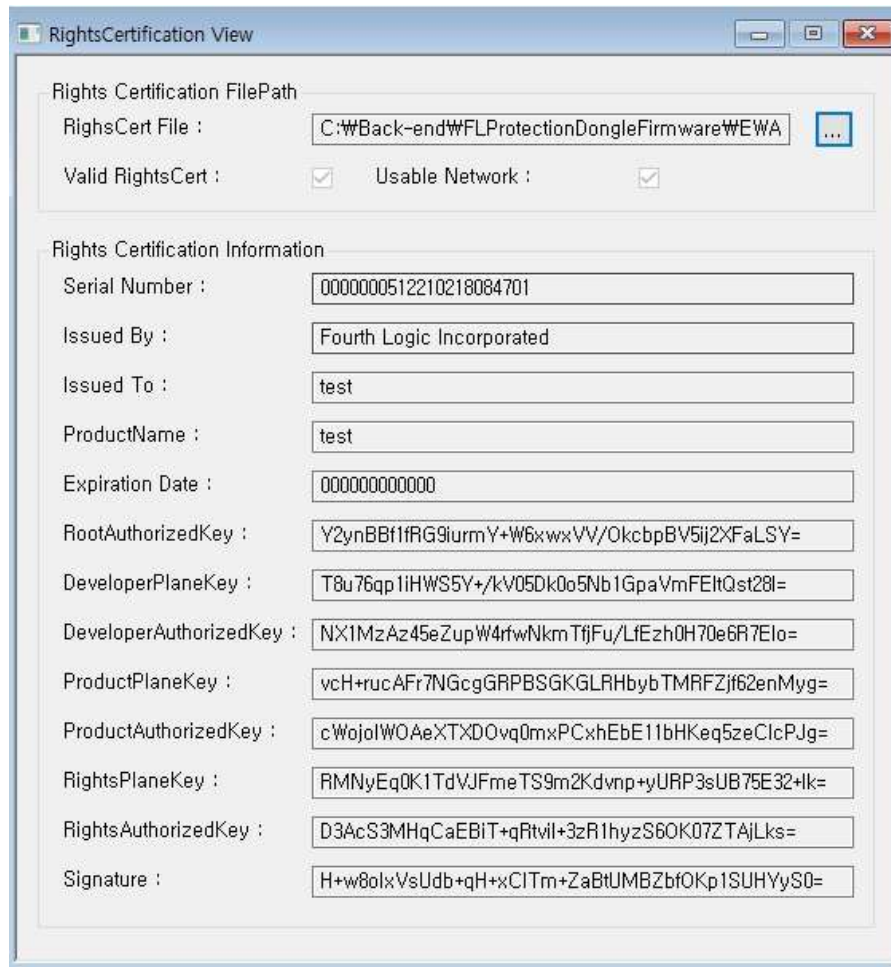
Contents	Description
Valid DeveloperCert	Checked if the Developer Certificate is valid.
Serial Number	Serial Number of the Developer Certificate.
Issued By	The organization that issued the Developer Certificate.
Issued To	The organization that the Developer Certificate is issued to.
RootAuthorizedKey	Root certificate identification authentication key.
DeveloperPlaneKey	Plaintext key of the Developer Certificate.
DeveloperAuthorizedKey	Identification authentication key of the Developer Certificate.
Signature	Signature of the Developer Certificate.

- Product Certificate



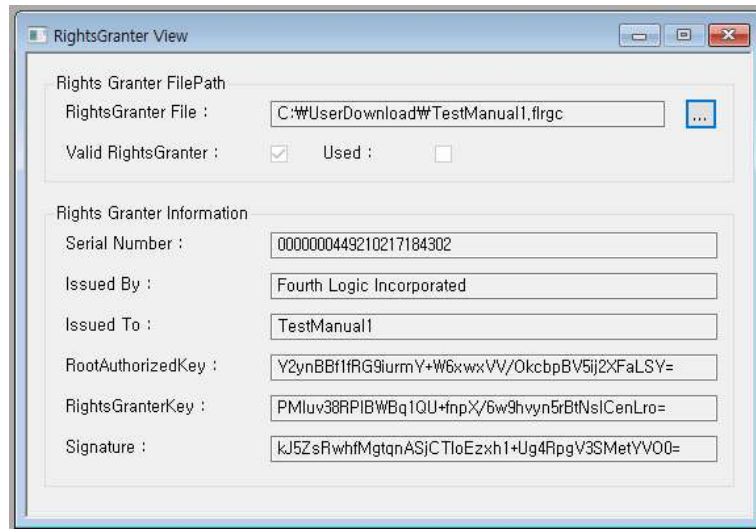
Contents	Description
Valid ProductCert	Checked if the Product Certificate is valid.
Serial Number	Serial Number of the Product Certificate.
Issued By	The organization that issued the Product Certificate.
Issued To	The organization that the Product Certificate is issued to.
ProductName	Name of the product.
RootAuthorizedKey	Root certificate identification authentication key.
DeveloperPlaneKey	Plaintext key of the Developer Certificate.
DeveloperAuthorizedKey	Identification authentication key of the Developer Certificate.
ProductPlaneKey	Plaintext key of the Product Certificate.
ProductAuthorizedKey	Identification authentication key of the Product Certificate.
Signature	Signature of the Product Certificate.

- Rights Certificate



Contents	Description
Valid RightsCert	Checked if the Rights Certificate is valid.
Usable Network	Checks whether network certification is available.
Serial Number	Serial Number of the Rights Certificate.
Issued By	The organization that issued the Rights Certificate.
Issued To	The organization that the Rights Granter is issued to.
ProductName	Name of the product.
ExpireDate	Expire date of the Rights Certificate.
RootAuthorizedKey	Root Certificate identification authentication key.
DeveloperPlaneKey	Plaintext key of the Developer Certificate.
DeveloperAuthorizedKey	Identification authentication key of the Developer Certificate.
ProductPlaneKey	Plaintext key of the Product Certificate.
ProductAuthorizedKey	Identification authentication key of the Product Certificate.
RightsPlaneKey	Plaintext key of the Rights Granter Certificate.
RightsAuthorizedKey	Identification authentication key of the Rights Granter Certificate.
Signature	Signature of the Rights Certificate.

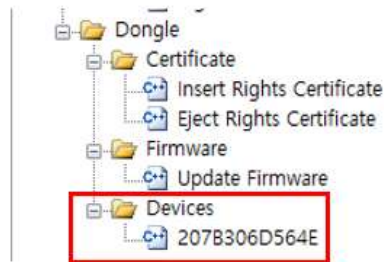
- Rights Granter Certificate



Contents	Description
Valid RightsGranter	Checked if the Rights Granter Certificate is valid.
Serial Number	Serial Number of the Rights Granter Certificate.
Issued By	The organization that issued the Rights Granter Certificate.
Issued To	The organization that the Rights Granter Certificate is issued to.
RootAuthorizedKey	Root certificate identification authentication key.
RightsGranterKey	Identification authentication key of the Rights Granter Certificate.
Signature	Signature of the Rights Granter Certificate.

11. Dongle Verification

If the Dongle is not connected to PC, connect it.



You can check the Dongle by selecting the serial number of the Dongle you want to check from the sub-item of **Dongle** > **Devices** in the Menu Tree.

The contents that can be checked in each Dongle are as follows.

Device Information

Dongle Information

Dongle S/N :

Valid Dongle :

In Use :

Firmware Version :

Dongle Led Status :

Rights Certificate Slot

Slot :

Rights Certificate Information

Serial Number :

Issued By :

Issued To :

Product Name :

Expiration Date :

Root Authorized Key :

Developer Plane Key :

Developer Authorized Key :

Product Plane Key :

Product Authorized Key :

Rights Plane Key :

Rights Authorized Key :

Signature :

Contents	Description
Valid Dongle	Checked if the Dongle is valid.
In Use	Checked if the Dongle is currently in use.
Firmware Version	Version of the Firmware installed.
Dongle LED Status	LED Status of the Dongle. Blinking, keep on, keep off status are available.
Slot	Serial Number of the Rights Certificate inserted.
Serial Number	Serial Number of the Rights Certificate of the slot.
Issued By	The organization that issued the Rights Certificate.
Issued To	The organization that the Rights Certificate is issued to.
ProductName	Name of the product.
ExpireDate	Expire date of the Rights Certificate.
RootAuthorizedKey	Root Certificate identification authentication key.
DeveloperPlaneKey	Plaintext key of the Developer Certificate.
DeveloperAuthorizedKey	Identification authentication key of the Developer Certificate.
ProductPlaneKey	Plaintext key of the Product Certificate.
ProductAuthorizedKey	Identification authentication key of the Product Certificate.
RightsPlaneKey	Plaintext key of the Rights Granter Certificate.
RightsAuthorizedKey	Identification authentication key of the Rights Granter Certificate.
Signature	Signature of the Rights Certificate.

CERTIFICATES

1. Developer Certificate

- The Developer Certificate is a certificate provided to the developer of the program to be protected.
- You can generate Product Certificates for products to be protected using Developer Certificates.
- The extension of the Developer Certificate is ***.fldc**.

2. Product Certificate

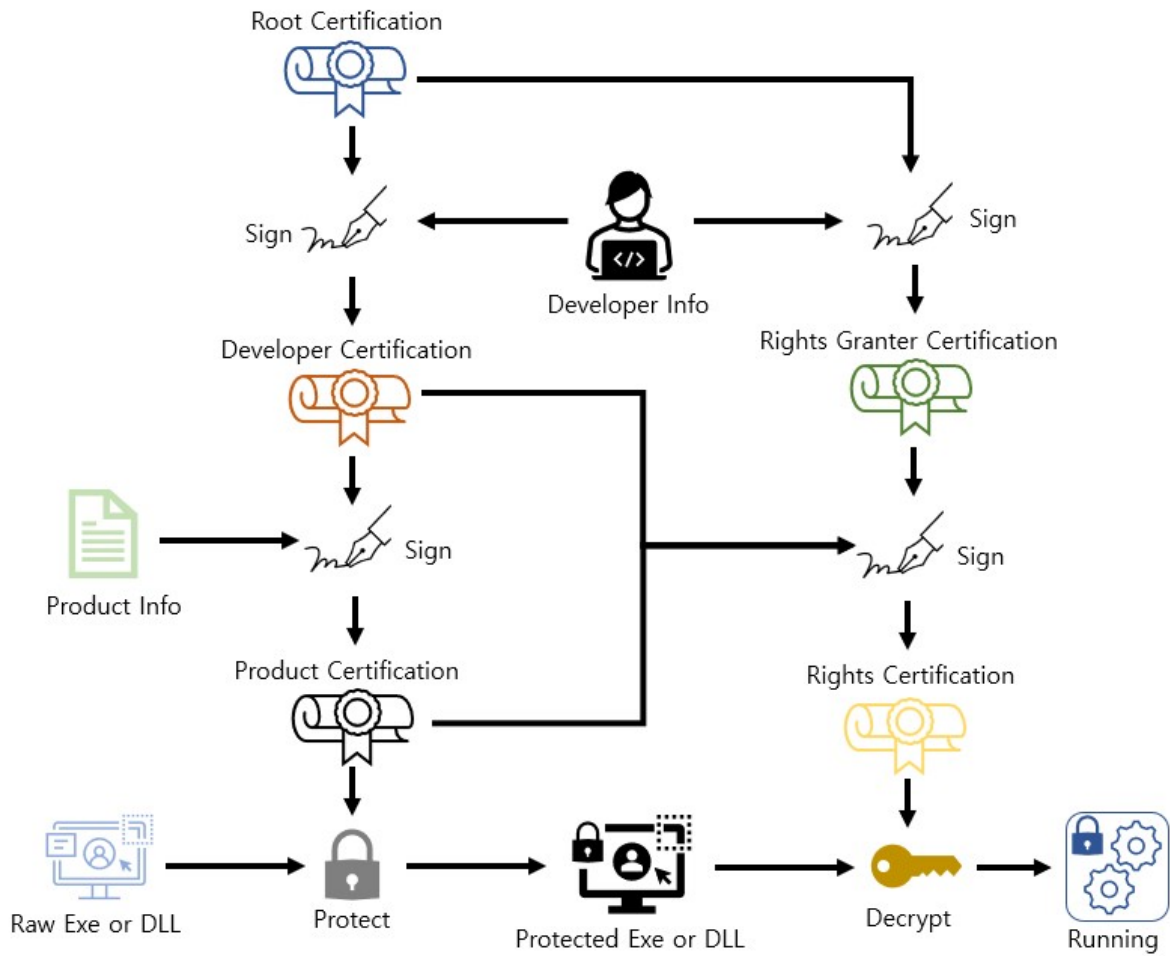
- The Product Certificate is the certificate provided to the program to be protected.
- The program can be encrypted using the Developer Certificate and Product Certificate.
- The extension of the Product Certificate is ***.flpc**.

3. Rights Granter Certificate

- The Rights Granter Certificate (RGC) is a one-time certificate designed to entitle users of encrypted programs to use.
- You can use Developer Certificates, Product Certificates, and RGCs to generate Rights Certificates that enable you to use the program.
- The extension of the RGC is ***.flrgc**.
- Once the Rights Certificate is generated, the RGC used to generate the Rights Certificate cannot be reused. The RGC used to create the Rights Certificate is renamed ***.used**.
- The certificate for granting rights is provided by FourthLogic Inc.

4. Rights Certificate

- The Certificate of Rights is a certificate that gives you the right to use programs protected by FLProtection®.
- You can use FLProtection®-protected programs on a PC with a Rights Certificate or on a PC connected to a Dongle.
- The Product Certificate has the extension ***.flrc**.



DONGLE SPECIFICATION

1. Overall Structure

The structure of Dongle is designed with a USB port at the bottom and an indicator light at the top. When the Dongle is connected to the PC, you can check the current FLProtection® status according to the color of the indicator at the top.



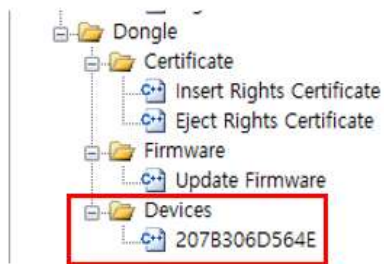
2. LED State Specification

You can check the current FLProtection® status according to the Dongle indicator status. The following is a table of FLProtection® status by indicator color.

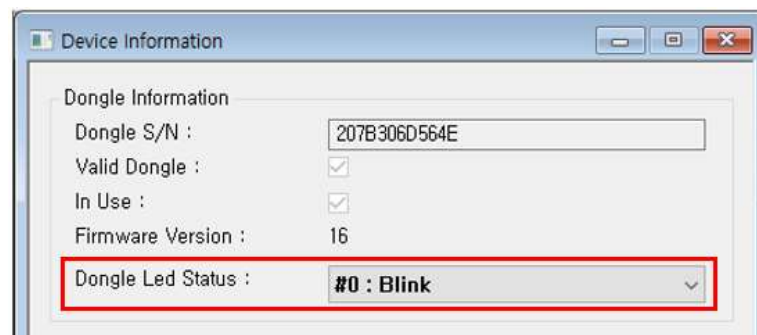
Indicator color	State
Blue	Displays the Dongle standby status.
Yellow	Indicates that a protected program is running.
Red or Faded	Indicates that there is an error in the Dongle or FLProtection® is not installed.
Purple	Indicates that Dongle firmware is being updated.
Blue Light Blinking rapidly	Indicates that Dongle firmware update is being completed.

3. Changing Dongle LED Status

You can change the LED Status of the Dongle. The steps are the following.



In the Menu Tree, select the serial number of the Dongle you want to check from the sub-item of **Dongle** > **Devices** to open the Device Information window.



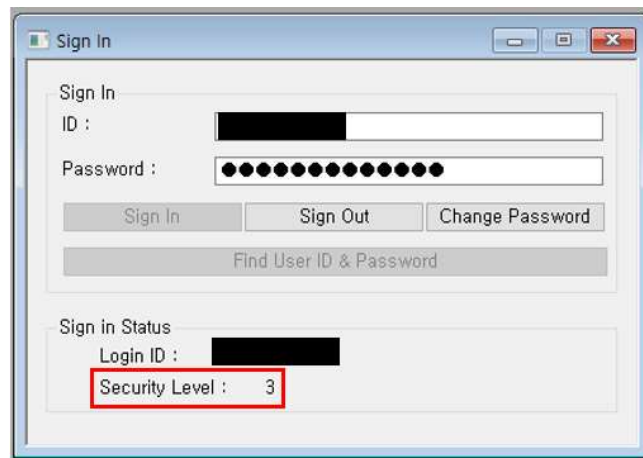
Select the status of the Dongle indicator from the Dongle LED status item.

FLPROTECTION® STEP BY STEP

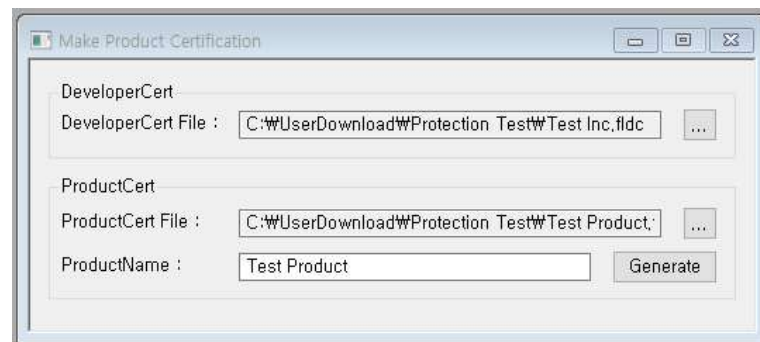
1. Protecting a software

Protecting a software requires a **Developer Certificate** and a **Product Certificate**, and can be performed only when a **Security Level 3 or higher account** is signed in. The process of creating a protected program is as follows.

Run the FLProtection® software.



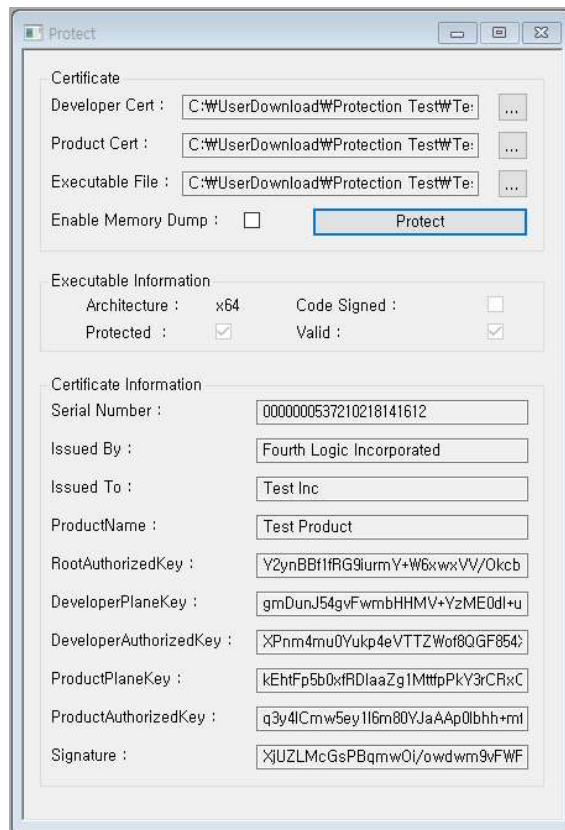
Log in with your FLProtection® Security Level 3 or higher account.



Name	Date modified	Type	Size
Test Inc.fldc	2021. 2. 18. 오후 4:47	FLDC File	1 KB
Test Product.flpc	2021. 2. 18. 오후 4:47	FLPC File	1 KB

After selecting **Certificate > Make Product Certificate**, enter the path to the Developer Certificate, path to the Product Certificate to be generated, and the product name. Then click the **“Generate”** button to proceed with the Product Certificate generation process.

By this process, a Product Certificate is created in the path with the name specified in **“ProductCert File”**.



After selecting the **Binary > Protect File** item, enter the Developer Certificate path, Product Certificate path, and program path to be protected, and then click the **“Protect”** button to proceed with the protection progress. When the program protection process is completed successfully, **“Protected”** and **“Valid”** items are checked.

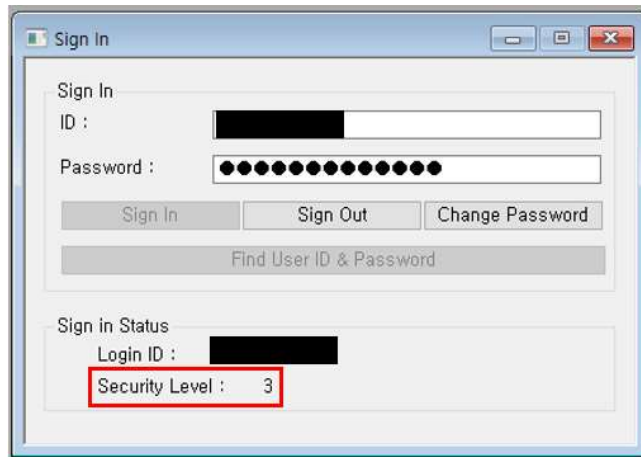
*Note: When signing an EV (Extended Validation) code to a program, you must sign the EV code **after** encrypting the program with FLProtection®.*

2. Generating Rights Certificates

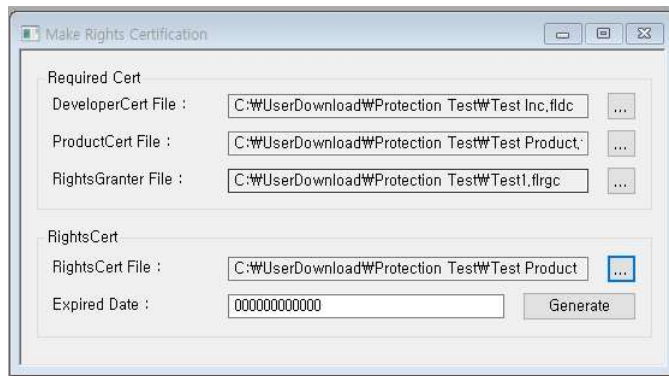
To run the program protected in step [1.Protecting a software], the **Rights Certificate** is required.

Generating Rights Certificates requires a **Developer Certificate**, a **Product Certificate**, a **Rights Granter Certificate**, and can be performed only when a **Security Level 3 or higher account** is signed in. The process of generating a Rights Certificate is as follows.

Run the FLProtection® software.



Log in with your FLProtection® Security Level 3 or higher account.



Name	Date modified	Type	Size
Test Inc.fldc	2021. 2. 18. 오후 4:47	FLDC File	1 KB
Test Product Rights Cert.flrc	2021. 2. 18. 오후 4:47	FLRC File	1 KB
Test Product.flpc	2021. 2. 18. 오후 4:47	FLPC File	1 KB
Test1.flrgc.used	2021. 2. 18. 오후 4:47	USED File	1 KB

After selecting the **Certificate > Make Rights Certificate** item, enter the Developer Certificate path, Product Certificate path, Rights Granter Certificate path, the Rights Certificate path to be generated, and the expiration date, click the “Generate” button to proceed with the Rights Certificate generation.

After this process, a Rights Certificate is created in the path with the name specified in “**RightsCert File**”, and the extension of the Rights Granter Certificate is changed to *.used.

3. Running a protected software

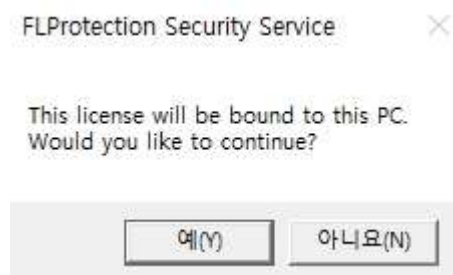
With the Rights Certificate created in [2. Generating Rights Certificates], the program protected by [1. Protecting a software] can be run.

There are two methods of execution, either through network authentication or by inserting a certificate into the Dongle.

1) Running through Network Certification

Name	Date modified	Type
DLL1.dll	2021. 2. 18. 오후 4:47	Application exten...
DLL1.lib	2021. 2. 18. 오후 4:47	Object File Library
Test Program - Copy.exe	2021. 2. 18. 오후 4:47	Application
Test Product rights Cert.flrc	2021. 2. 18. 오후 5:33	FLRC File

In order to run the program protected through Network Certification, move the Rights Certificate into the same path of the protected program.



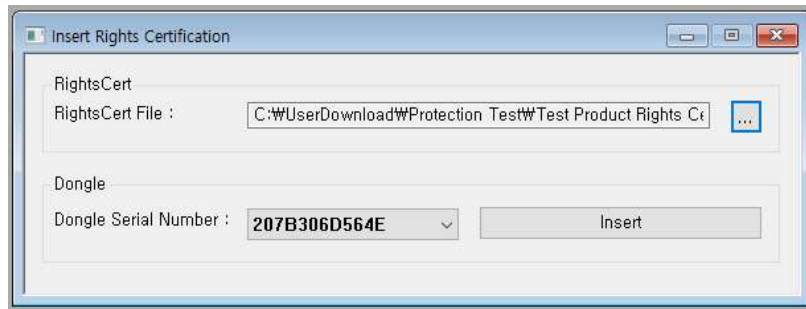
Run the protected program. Before the program runs you will be asked if you want to bind the Rights Certificate to your PC. Click “Yes” in the pop-up window to bind the Rights Certificate to the PC. After this step, the program will be running.

If you proceed with this process, the right certificate will be bound to your PC, and you will not be able to run programs protected with this Right Certificate on other computers.

2) Running through the Certificate inserted into the Dongle

To insert the certificate into the Dongle, you need the Dongle and the Rights Certificate. To insert a certificate in Dongle, follow the steps below.

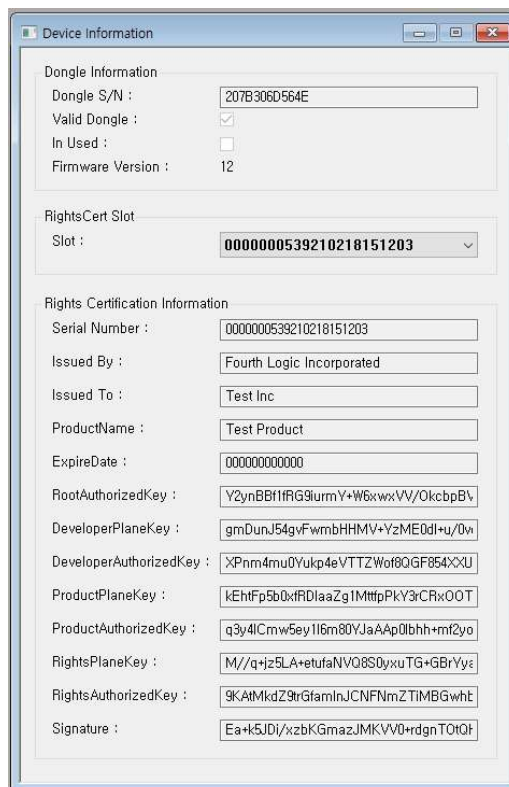
Run FLProtection® to insert the certificate into the Dongle and connect the Dongle with your PC.



Test Inc.fldc	2021. 2. 18. 오후 4:47	FLDC File
Test Product Rights Cert.flrc.used	2021. 2. 18. 오후 4:47	USED File
Test Product.flpc	2021. 2. 18. 오후 4:47	FLPC File

After selecting the **Dongle > Certificate > Insert Rights Certificate** item, enter the Rights Certificate path and Dongle serial number and click the “Insert” button to insert the Rights Certificate into the Dongle.

If you proceed with this process, the extension of the Right Certificate file inserted in Dongle will be changed to *.used.



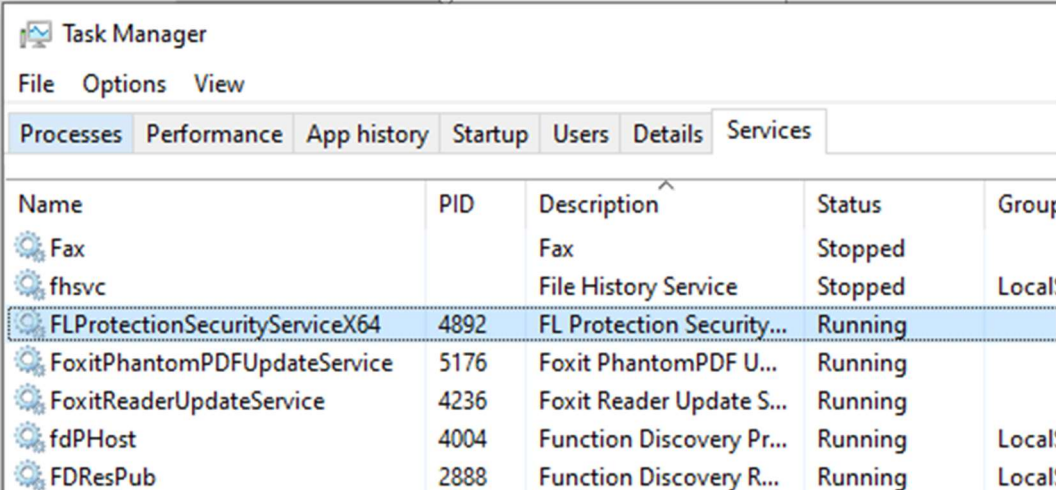
By selecting the Dongle with the Rights Certificate inserted in **Dongle > Device**, then selecting the inserted Rights Certificate serial number in the “Slot” item, you can check the contents of the Right Certificate.

Run the protected program with the PC and Dongle connected. If the PC and Dongle are disconnected, the protected program cannot be executed.

TROUBLESHOOTING

1. When the Indicator is Red

- 1) Disconnect and reconnect the PC and Dongle. Check the light to see if the blue light is on.
- 2) If the red light keeps on, check that the FLProtection® service is running in Task Manager.



The screenshot shows the Windows Task Manager window with the 'Services' tab selected. The 'Services' list is displayed with columns for Name, PID, Description, Status, and Group. The service 'FLProtectionSecurityServiceX64' is highlighted in blue and is in a 'Running' state. Other services listed include Fax (Stopped), fhsvc (Stopped), FoxitPhantomPDFUpdateService (Running), FoxitReaderUpdateService (Running), fdPHost (Running), and FDResPub (Running).

Name	PID	Description	Status	Group
Fax		Fax	Stopped	
fhsvc		File History Service	Stopped	Local!
FLProtectionSecurityServiceX64	4892	FL Protection Security...	Running	
FoxitPhantomPDFUpdateService	5176	Foxit PhantomPDF U...	Running	
FoxitReaderUpdateService	4236	Foxit Reader Update S...	Running	
fdPHost	4004	Function Discovery Pr...	Running	Local!
FDResPub	2888	Function Discovery R...	Running	Local!

- 3) If the red light keeps on, install the Dongle firmware update to the latest version.
- 4) If the red light keeps on, re-install the FLProtection®.
- 5) If the problem is not solved by the above, turn off the power to the PC and turn it on again to check the operation after booting.

If the problem is not solved by the above, please contact FourthLogic Inc. technical support(+82) 31-463-6902).

2. When the Dongle Indicator has faded

If the problem is not solved after taking the measures of [1. When the Indicator is Red], there is a high probability of a hardware problem. Please re-check the operations after checking your PC hardware conditions.

If the problem is not solved by the above, please contact FourthLogic Inc. technical support(+82) 31-463-6902).