Panasonic

Programmable Controller

FP7 CPU Unit

User's Manual

Security Functions

WUME-FP7CPUSEC-01

2013.12 | panasonic.net/id/pidsx

Introduction

Thank you for buying a Panasonic product. Before you use the product, please carefully read the installation instructions and the users manual, and understand their contents in detail to use the product properly.

Types of Manual

- There are different types of users manual for the FP7 series, as listed below. Please refer to a relevant manual for the unit and purpose of your use.
- The manuals can be downloaded on our website: http://industrial.panasonic.com/ac/e/dl_center/manual/ .

Unit name or purpose of use	Manual name	Manual code
FP7 Power Supply Unit	FP7 CPU Unit Users Manual (Hardware)	WUME-FP7CPUH
FP7 CPU Unit	FP7 CPU Unit Command Reference Manual	WUME-FP7CPUPGR
	FP7 CPU Unit Users Manual (Logging Trace Function)	WUME-FP7CPULOG
	FP7 CPU Unit Users Manual (Security Function)	WUME-FP7CPUSEC
Instructions for Built-in LAN Port	FP7 CPU Unit Users Manual (LAN Port Communication)	WUME-FP7LAN
Instructions for Built-in COM Port	FP7 series Users Manual (SCU communication)	WUME-FP7COM
FP7 Extension Cassette (Communication) (RS-232C/RS485 type)		
FP7 Extension Cassette (Communication) (Ethernet type)	FP7 series Users Manual (Communication cassette Ethernet type)	WUME-FP7CCET
FP7 Extension (Function) Cassette Analog Cassette	FP7 Analog Cassette Users Manual	WUME-FP7FCA (Upcoming)
FP7 Digital Input/Output Unit	FP7 Digital Input/Output Unit Users Manual	WUME-FP7DIO
FP7 Analog Input Unit	FP7 Analog Input Unit Users Manual	WUME-FP7AIH
FP7 Analog Output Unit	FP7 Analog Output Unit Users Manual	WUME-FP7AOH
FP7 High-speed counter Unit	FP7 High-speed counter Unit Users Manual	WUME-FP7HSC
FP7 Pulse Output Unit	FP7 Pulse Output Unit Users Manual	WUME-FP7PG (Upcoming)
FP7 Positioning Unit	FP7 Positioning Unit Users Manual	WUME-FP7POSP
FP7 Serial Communication Unit	FP7 series Users Manual (SCU communication)	WUME-FP7COM
PHLS System	PHLS System Users Manual	WUME-PHLS
Programming Software FPWIN GR7	FPWIN GR7 Introduction Guidance	WUME-FPWINGR7

Selection of CPU Units

Note the following points when selecting a CPU unit.

■ Specification changes of CPU unit

- The firmware version of CPU units has been changed in accordance with the extension of the specifications. Specify units with new model numbers.

		Conventional model number (Ver.1)		New model number (Ver.2)	
Program capacity	**Ethernet function**	**With Encryption function**		**No Eencryption function**	**With Encryption function**
196K steps	Available	AFP7CPS4E	→	AFP7CPS41E	AFP7CPS41ES
120K steps	Available	AFP7CPS3E	→	AFP7CPS31E	AFP7CPS31ES
	Not available	AFP7CPS3	→	AFP7CPS31	AFP7CPS31S

- The CPU units Ver.2 are upward compatible with the conventional Ver.1.
- For using CPU units Ver.2, Ver.2.0 or later version of FPWIN GR7 is required.
- For using the projects (programs, comments and configuration data) created for the conventinal CPUs Ver.1, the projects must be converted to the projects for CPU units Ver.2 using the "Convert PLC Type" function of the tool software.
- For using the units released after December 2013 or add-on cassettes, Ver.2 or later version of CPU unit is required.
- The layout of the operation monitor LEDs on the CPU units has been changed.

■ Regulations on Encryption function in China

- Some CPU units have the encryption function which encrypts a part or all parts of programs in projects.
- In China, the types equipped with the encryption function cannot be used as they are subject to "Regulation of Commercial Encryption Codes". For using machines or systems incorporating FP7 series in China, or exporting and importing them, select the types without the encryption function.

Table of Contents

1

Security Function

1.1 Overview of Security Function

1.1.1 Precautions on Using Security Function

- Security information set for each function can be cleared using the tool software, however, performing the clearing operation also deletes project data. Fully confirm before determining the operations of each security function.
- Although the encryption function encrypts programs to make them unreadable, it cannot protect projects from being read or rewritten. Use the password protection function in combination as necessary.

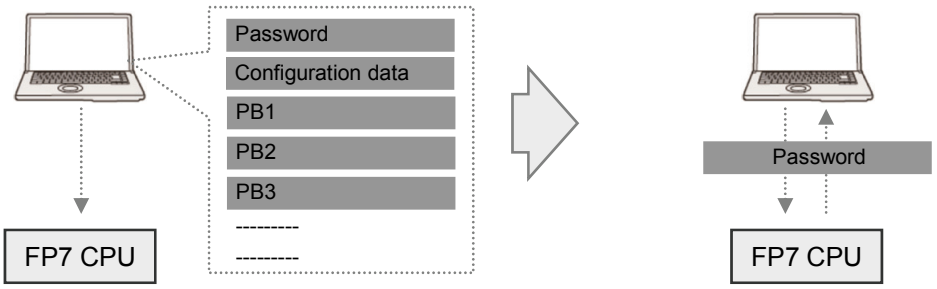
1.1.2 Type of Security Functions

■ **Password function（1）**

- This is a function to set a password for project data downloaded to the PLC for preventing data from being read and written. Using this function prevents unnecessary rewrting or leak of know-how.
- The password is valid for configuration data, ladder programs and comments.
- Operation memories can be read or written even when a password has been set.
- A project for which a password has been set is saved as a password-protected file even when it is saved on a PC. (Available in FPWIN GR7 Ver.1.3 or later)

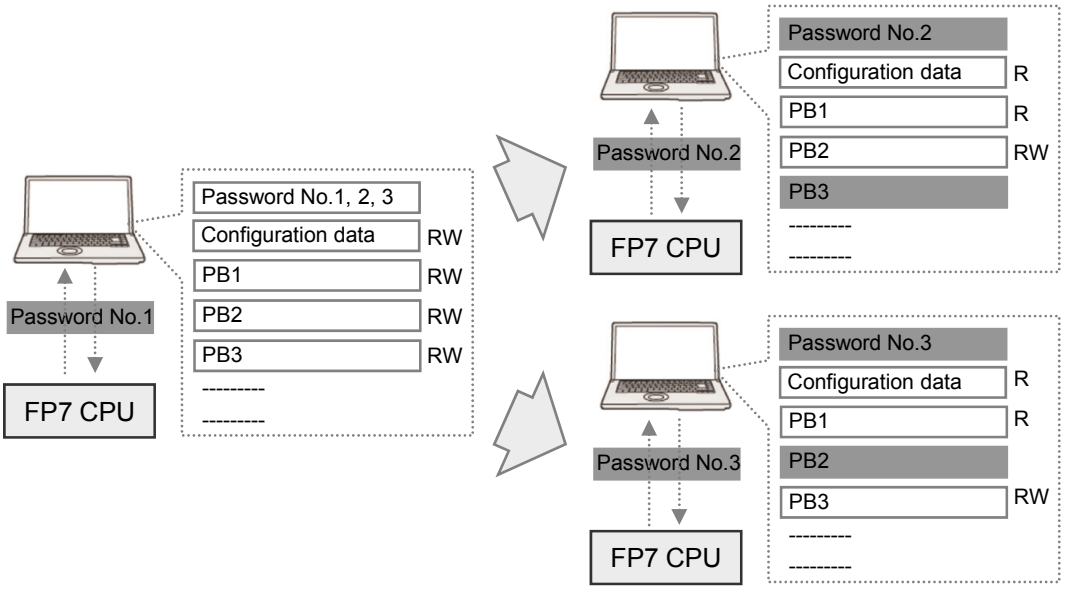
Item	Specifications
No. of registerable passwords	16 (Settable as administrator or users) (Note)
No. of characters	8 to 16 characters
Open and close for each communication route	Only connected port is allowed to access.
Limit on number of failed open request	Access is blocked when opening operation failed three times. It is recovered when the power turns on again.
Status when power is on	All passwords are closed when the power turns on.

(Note) The number one password is set with administrator privileges.



■ Password function（2）User-level password

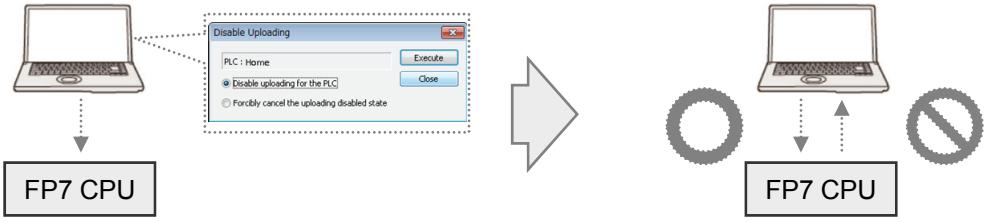
- This is a function to set passwords for administrator or each user, which enables to change levels of access.
- All operations can be performed with administrative privileges as in the case no password is set.
- For user-level passwords, it is possible to specify the allowable range of PB numbers of program blocks accessible when reading or writing.
- This function is available from FPWIN GR7 Ver.1.3 and CPU Ver.1.3.



Item	Privileges		Remarks
	Administrator	User	
Registration, deletion of passwords, limited distribution setting Upload protection setting, encryption setting, security forced reset	●		
Reading configuration data	●	●	
Writing or changing configuration data	●		
Reading files from PC	●	○	With user privileges, executable only in the range specified in the password setting dialog box
Saving files into PC	●	○	
Uploading program blocks from PLC	●	○	
Downloading program blocks to PLC	●	○	
Converting program blocks	●	○	
Converting projects	●	●	
Reading operation memories	●	●	
Writing operation memories	●	●	

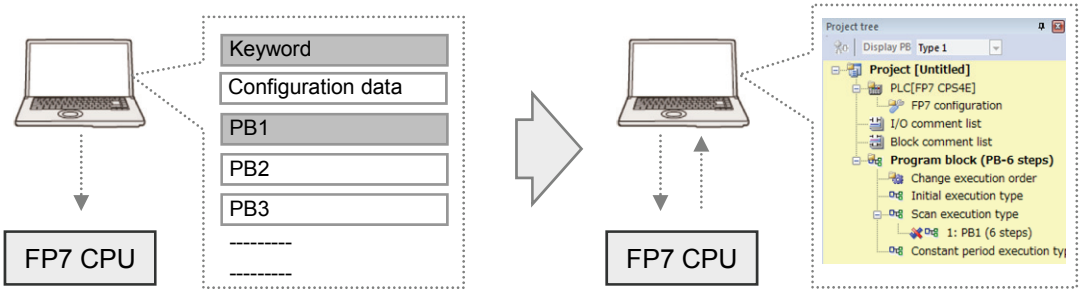
■ Upload protection function

- This is a function to prevent downloaded projects from being uploaded. This function prevents the leak of programs and know-how.
- The upload protection function is valid for configuration data, ladder programs and comments.
- Even when the upload protection function has been set, projects can be downloaded and overwritten.
- This function can be used in combination with the password function.



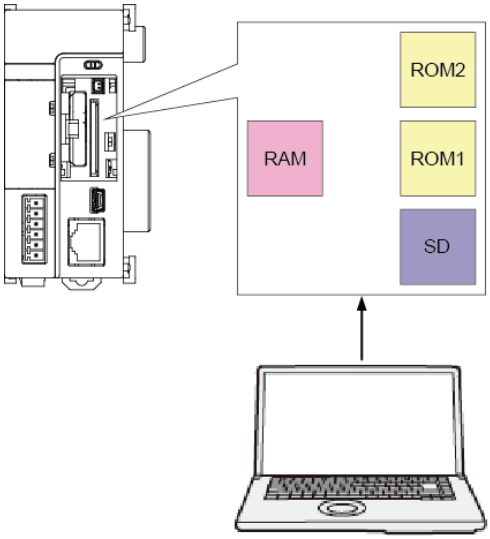
■ Encryption function (Models with the encryption function only)

- This is a function to encrypt a part or all parts of programs in projects.
- Encryption is valid for ladder programs and comments.
- Encryption can be performed for each program block (PB).
- Encrypted programs become valid only when an encryption key has been set to the PLC and it matches.
- A project for which an encryption keyword has been set is saved as a file with the encrypted keyword even when it is saved on a PC.
- This function can be used in combination with the password function.



1.1.3 Target Items of Security Functions

Available operations for each security function vary depending on target memories.



■ **Operations for projects in operation program memories (RAM/ROM1)**

- Downloading project data containing passwords
- Opening and closing password-protected items
- Setting and changing passwords
- Setting the read protection
- Downloading and uploading encrypted projects
- Cancelling the security function

■ **Operations for projects in program memories for backup (RAM/ROM2)**

- Backing up and restoring encrypted projects

Password-protected projects cannot be backed up and restored.

■ **Operations for projects in operation program memories (RAM/ROM1) in SD memory card operation**

- Opening and closing password-protected items
- Copying data from SD memory cards using limited distribution passwords to operation program memories (RAM/ROM1) and SD memory card operation

It is not possible to edit project data, set or delete passwords.

1.2 Password Protection Function

1.2.1 How to Set Password (1) Administrative Previleges

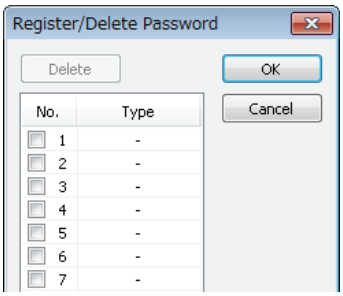
■ Setting method

- The following procedure describes the case that a project is created offline with FPWIN GR7.

◆ PROCEDURE

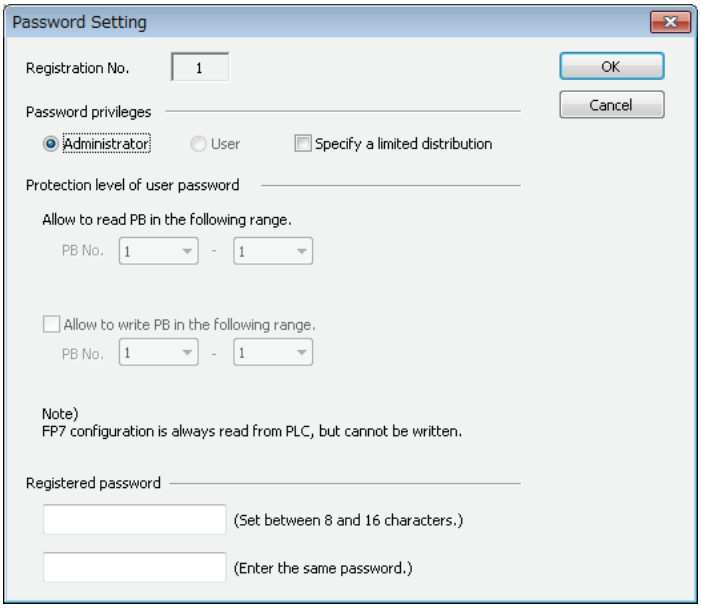
1. Select "Tools" > "PLC Security Settings" > "Register/Delete Password" in the menu bar.

The "Register/Delete Password" dialog box is displayed.



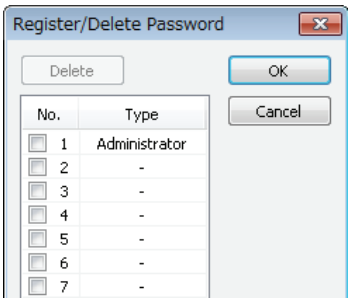
2. Select a desired number and double-click on it.

The "Password Setting" dialog box is displayed.

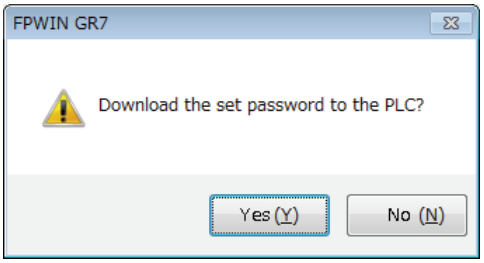


3. Enter a desired password, and press the [OK] button.

"Administrator" is displayed in the "Register/Delete Password" dialog box, and the password is registered.



When it is online, the following message box is displayed.



◆ **KEY POINTS**

- **Only an administrator password can be set in the password number one. User-level passwords cannot be set.**
- **An administrator password can be also set in numbers 2 to 16.**
- **If necessary, change passwords by a similar procedure as above.**

1.2.2 How to Set Password (2) User Privileges

■ Setting method

- The following procedure describes the case that an administrator password has been already set in the registration number one.

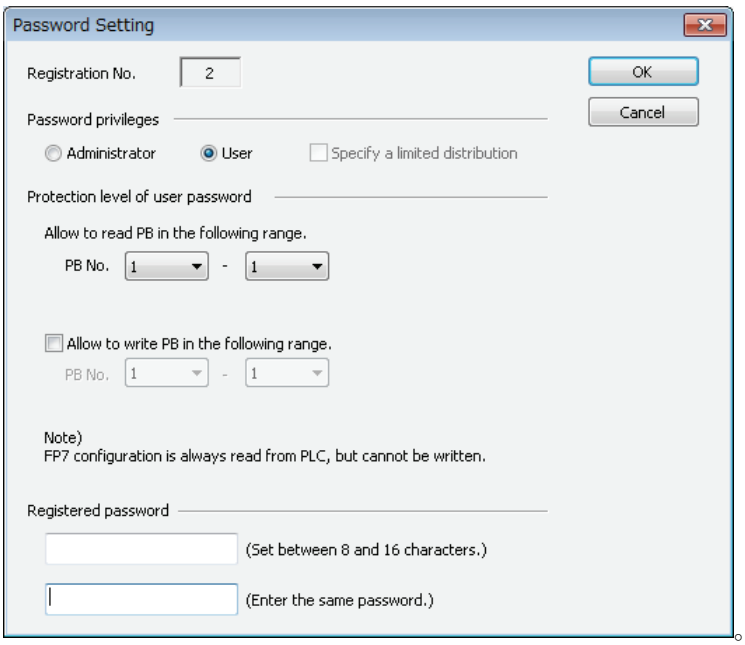
◆ PROCEDURE

1. **Select "Tools" > "PLC Security Settings" > "Register/Delete Password" in the menu bar.**

2. **Select a desired number and double-click on it.**

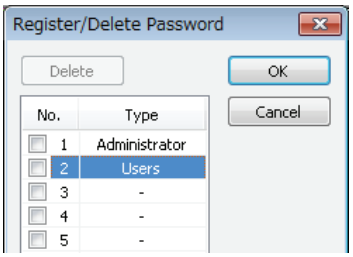
   The "Password Setting" dialog box is displayed.

3. **Change the password privileges to "User", and set the protection level.**

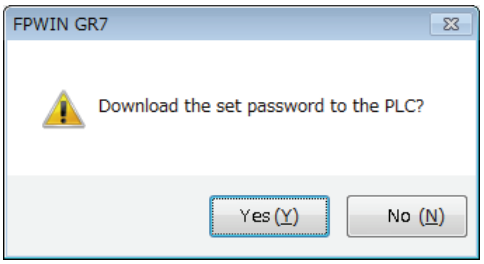


4. **Enter a desired password, and press the [OK] button.**

   "User" is displayed in the "Register/Delete Password" dialog box, and the password is registered.



When it is online, the following message box is displayed.



◆ KEY POINTS

- **User passwords and protection levels can be set only with administrative privileges.**
- **As for user passwords, the range of PB numbers that are readable or writable can be specified for each registration number.**

1.2.3 Reading Project that Password Has Been Set (1) Administrative Previleges

■ Setting method

- The following procedure describes the case that a project with a password is uploaded from the PLC.

◆ PROCEDURE

1. **Select "Online" > "Upload From PLC (Entire Project)" in the menu bar.**

   The "Input a Password" dialog box is displayed.

2. **Enter the registration number and the password, and press the [OK] button.**

   When the password matches, the project is uploaded from the PLC.

■ Optional settings of "Input a Password" dialog box

Item	Description
After completion, the PLC will revert to the protected state.	Uncheck the box for cancelling the protection of PLC temporarily or permanently after the completion of upload.
Open time	The PLC returns to the password protected state after the elapse of a specified time.
Number of retries	It indicates the allowable number of times for the entry of wrong password. The set value is always 3 times. If wrong passwords have been entered three times, you cannot enter a password any more unless the CPU unit is turned off and on again.

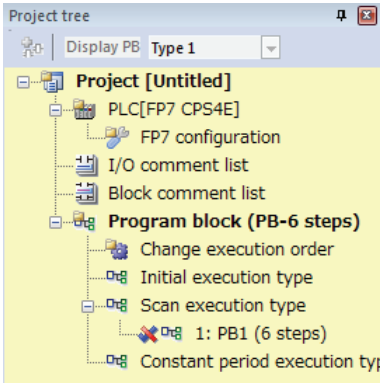
◆ KEY POINTS

- **When the read project has been changed, the "Input a Password" dialog box is displayed before downloading the changes to the PLC.**

1.2.4 Reading Project that Password Has Been Set (2) User privileges

■ **Operation when reading a project with user privileges**

- Reads the program blocks in the range of PB numbers that are allowed to be read.
- The background color of the project tree is cream when the project is read with user privileges.
- A red line is displayed at the PB number of the project tree in the range of PB numbers that are not allowed to be written.



◆ **KEY POINTS**

- **When the read project has been chagned, the "Input a Password" dialog box is displayed before downloading the changes to the PLC. With user privileges, only the range of program blocks that are allowed to be written is downloaded.**

1.2.5 Cancelling Password

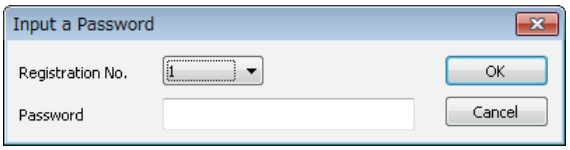
■ Setting method

- The following procedure describes the case that a project with a password has been uploaded from the PLC.

◆ PROCEDURE

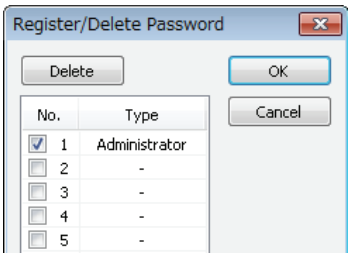
1. **Select "Tools" > "PLC Security Settings" > "Register/Delete Password" in the menu bar.**

   The "Input a Password" dialog box is displayed.



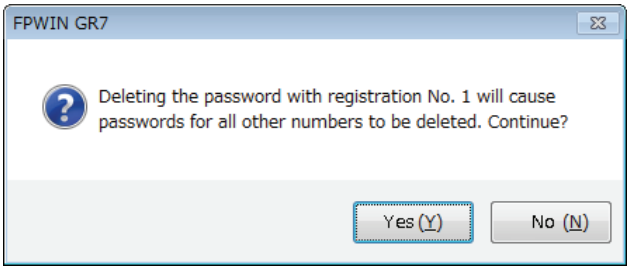
2. **Enter the password, and press the [OK] button.**

   The "Register/Delete Password" dialog box is displayed.



3. **Select the number for the password you want to delete, and press the [OK] button.**

   When the password is that with the registration No. 1, the confirmation message box appears.



4. **Press the [Yes] button.**

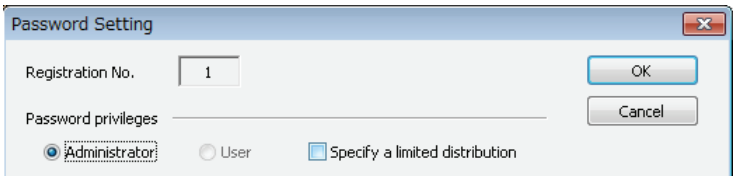
◆ **KEY POINTS**

- **Even when a password is deleted, project information will not be deleted.**
- **If the password with registration No.1 is deleted, all other passwords will be deleted.**

1.2.6 Limited Distribution Password

■ **Overview**

- Check the box of "Specify a limited distribution" in the "Password Setting" dialog box to set the limited distribution to the password.
- Projects can be downloaded with the limited distribution password only when the same password has been set to the PLC in advance.
- This is used as a matching condition for the SD card operation and copying projects in a SD memory card to the operation program memories (RAM/ROM1).



◆ **KEY POINTS**

- **The limited distribution password is used for checking if the passwords for the project stored in the operation memory and the project in a SD memory card match in such case the SD memory card operation is performed using the password-protected project.**
- **The limited distribution password can be set with administrative privileges only.**

1.3 Upload Protection Setting

1.3.1 Operation When Upload Protection Has Been Set

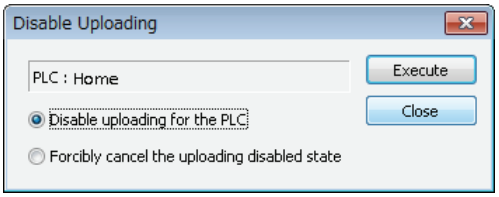
- All project information stored in the PLC (programs, comments, and configuration data) cannot be read.
- It is possible to download or edit project information online.
- It can be used in combination with the password protection function as necessary.

1.3.2 Setting Method

◆ **PROCEDURE**

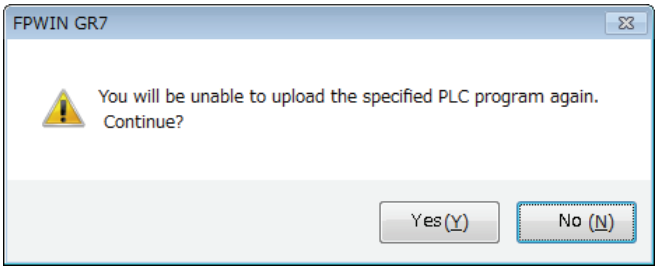
1. **Select "Tools" > "PLC Security Settings" > "Disable Uploading" in the menu bar.**

   The "Disable Uploading" dialog box is displayed.



2. **Select "Disable uploading for the PLC", and press the [Execute] button.**

   The following confirmation message is displayed.



3. **After confirmation of the message, press the [Yes] button.**

   A message indicating the execution result is displayed.

◆ **NOTE**

- **Once the above operation has been performed, project information cannot be uploaded. Fully confirm before determining the operation.**

1.3.3 Cancelling Upload Protection Setting

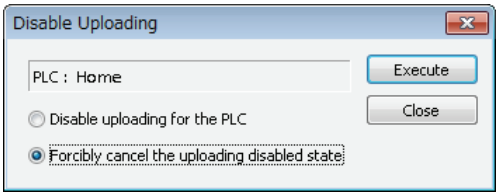
■ **Overview**

- The upload protection setting can be cancelled by the following procedure.

◆ **PROCEDURE**

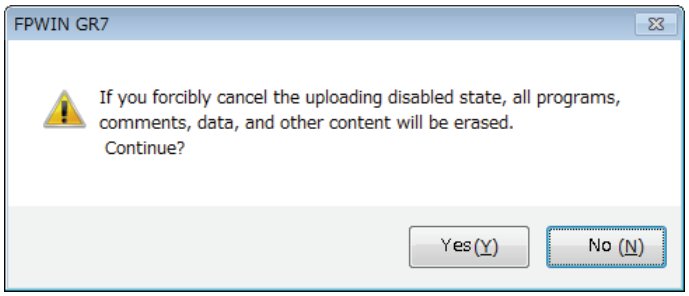
1. **Select "Tools" > "PLC Security Settings" > "Disable Uploading" in the menu bar.**

   The "Disable Uploading" dialog box is displayed.



2. **Select "Forcibly cancel the uploading disable state", and press the [Execute] button.**

   The following confirmation message is displayed.



3. **After confirming the message, press the [Yes] button.**

   A message indicating that the settings have been reverted to the factory defaults is displayed.

◆ **NOTE**

- **Performing the above operation erases not only the security setting information but also all project information. Confirm if there is no problem erasing all the information before performing the operation.**

1.4 Encryption Setting

1.4.1 Feature of Encryption Setting Function

- All or a part of project information is encrypted by an encryption keyword.
- Programs and comments can be encrypted for each program block (PB).
- The registered encryption keyword cannot be read.

◆ **NOTES**

- **The encryption keyword set in the PLC cannot be changed until it is cancelled by "1.5 Cancelling Security Setting". Executing the force cancel erases all project information. Please do not forget the encryption key.**
- **The encryption key must be registered in the PLC to enable the encryption function.**

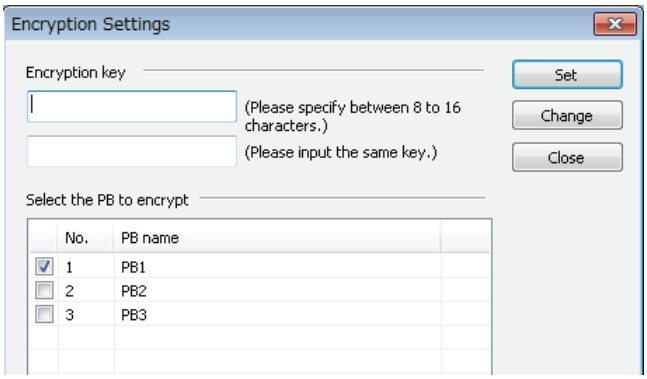
1.4.2 Encryption Setting for Program Blocks (PB)

- Program blocks (PB) to be encrypted are set with FPWIN GR7 online.
- The following procedure describes the case that three program blocks (PB) have been created in advance.

◆ **PROCEDURE**

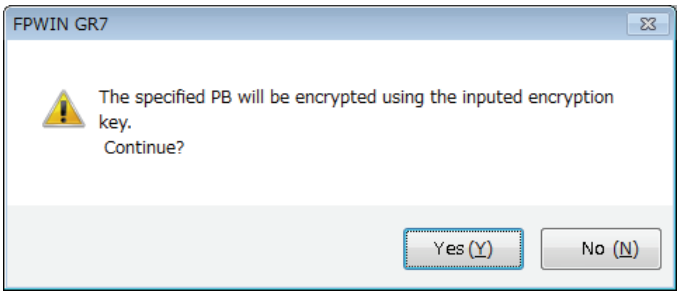
1. **Select "Tools" > "PLC Security Settings" > Encryption Settings" in the menu bar when the program blocks (PB) to be encrypted are active.**

   The "Encryption Settings" dialog box is displayed.



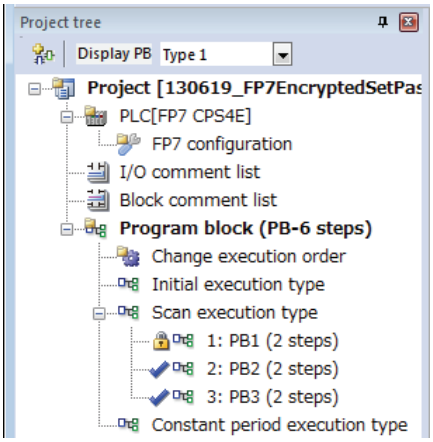
2. **Select the PB to be encrypted, enter the encryption key, and press the [Set] button.**

   The following confirmation message is displayed.



3. **After confirming the message, press the [Yes] button.**

   The icon for the encrypted program block (PB) on the project tree changes to a key mark.



4. **Repeat the "Encryption setting" operation as necessary.**

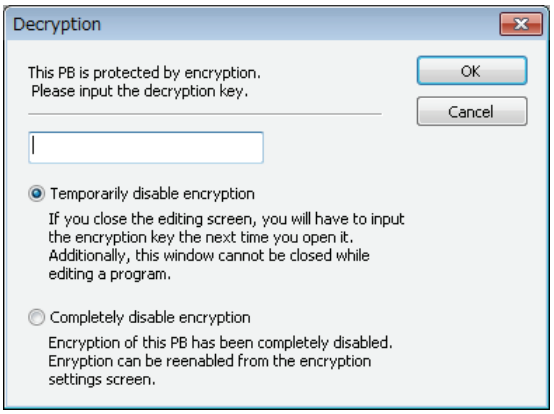
1.4.3 Confirming Encrypted State (Decryption)

- Confirm the contents of encrypted program blocks (PB) by the following procedure.

◆ PROCEDURE

1. **Double-click on the icon for the encrypted program block (PB) on the project tree.**

   The "Decryption" dialog box is displayed.

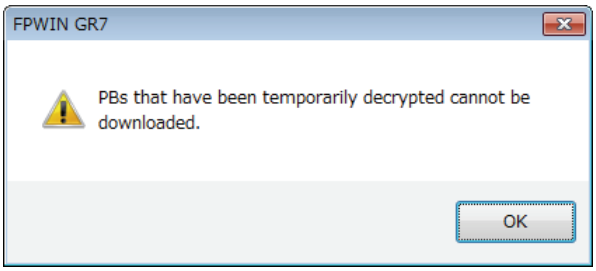


2. **Select a method of disabling encryption, enter the encryption key, and press the [OK] button.**

   The corresponding program block (PB) is open and becomes editable.

◆ KEY POINTS

- **By closing the program block (PB) whose encryption has been temporarily disabled, it returns to the encrypted state.**
- **The project cannot be downloaded to the PLC when a decrypted program block (PB) is open. Close the program block (PB), and download the project in the encrypted state.**



1.4.4 Changing or Deleting Encryption Key

■ Changing encryption key

- The encryption key of the program block (PB) encrypted offline can be changed or deleted by the following method.

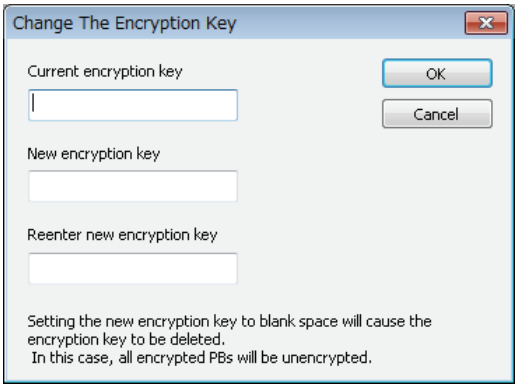
◆ **PROCEDURE**

1. **Select "Tools" > "PLC Security Settings" > "Encryption Settings" in the menu bar.**

   The "Encryption Settings" dialog box is displayed.

2. **Enter the encryption key, and press the [Change] button.**

   The "Change The Encryption Key" dialog box is displayed.



3. **Enter the encryption keys before and after change, and press the [Change] button. For deleting the encryption key, leave a new encryption key blank.**

   The confirmation dialog box is displayed.

4. **Press the [Yes] button.**

   The encryption key is changed and the corresponding program block (PB) is closed.

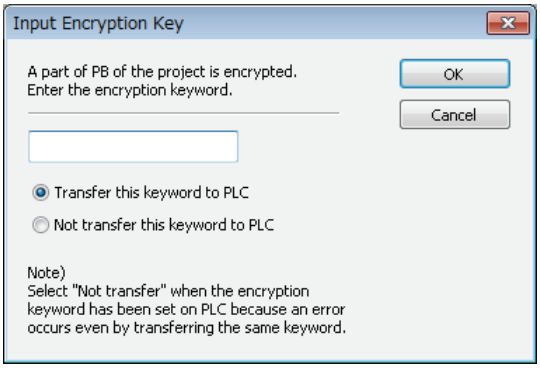
1.4.5 How to Set Encryption Keyword for PLC (1)

- The encryption setting for the PLC can be set only in online.
- Also, set the same encryption key for downloading a project containing encrypted blocks (PB). The following procedure describes the case that each program block (PB) has been encrypted offline.

◆ PROCEDURE

1. **Select "Online" > "Download To PLC (Entire Project)" in the menu bar.**

   The "Input Encryption Key" dialog box is displayed.



2. **Enter the encryption key, and press the [OK] button.**

   Project information is transferred together with the encryption key.

◆ KEY POINTS

- **When the encryption key does not match, "Passcode unmatch error" occurs.**
- **Double-clicking an encrypted program block (PB) online displays the "Decryption" dialog box. As necessary, the contents of the program blcok (PB) can be confirmed by entering the encryption key.**
- **It is not possible to edit only encrypted program blocks (PB) online. For changing them, switch to offline mode, edit and download them again.**

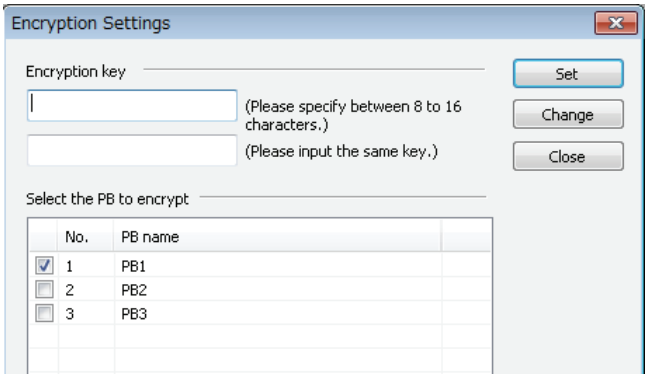
1.4.6 How to Set Encryption Keyword for PLC (2)

- The encryption setting for the PLC can be set only in online.
- For setting an encryption key before downloading a project containing encrypted program blocks (PB), the procedure is as follows.

◆ **PROCEDURE**

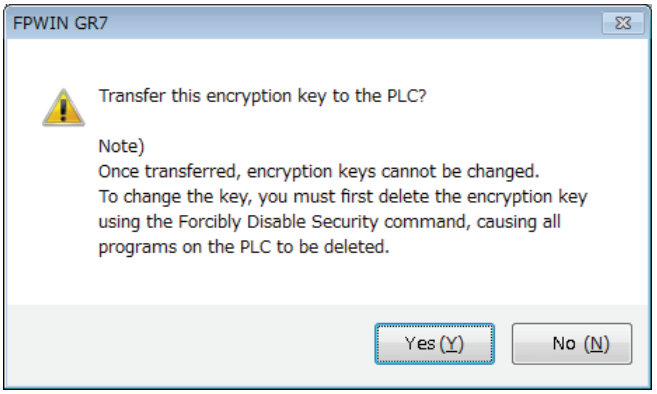
1. **Select "Tools" > "PLC Security Settings" > "Encryption Settings" in the menu bar.**

   The "Encryption Settings" dialog box is displayed.



2. **Enter the encryption key, and press the [Set] button.**

   The confirmation dialog box is displayed.



3. **Press the [Yes] button.**

   The encryption key is transferred to the PLC.

1.5 Cancelling Security Setting

1.5.1 Setting Method

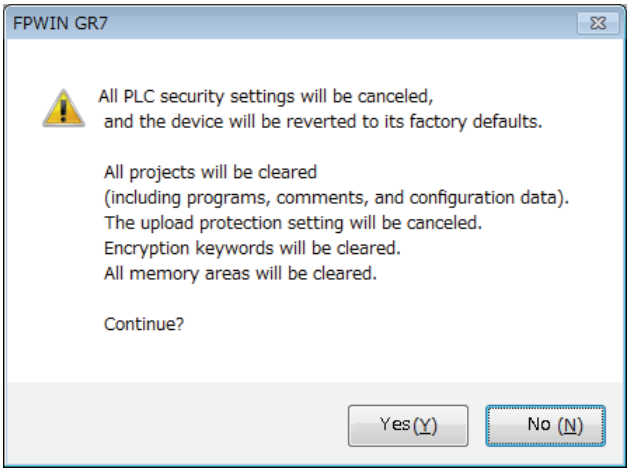
■ **Overview**

- Clears all password settings, upload protection settings and encryption keywords, and reverts them to the factory defaults.

◆ **PROCEDURE**

1. **Select "Tools" > "PLC Security Settings" > "Forcibly Disable Security" in the menu bar.**

   The following confirmation message is displayed.



2. **Press the [Yes] button.**

   A message indicating that the settings have been reverted to the factory defaults is displayed.

◆ **NOTE**

- **Performing the above operation erases not only the security setting information but also all project information. Confirm if there is no problem erasing all the information before performing the operation.**

1.6 Restrictions on SD Memory Card Operation and Copy Operation

1.6.1 SD Memory Card Operation and Copy Operation of SD Memory Card

■ SD memory card operation and execution project

Project status in SD memory card / Project status in PLC (ROM1)	Limited distribution password	Unlimited password	No password
Limited distribution password	Operable when matched	Not operable 1	Not operable 2
Unlimited password	Operable when matched	Operable when matched	Not operable 3
No password	Not operable	Operable	Operable

(Note 1) In the cases of the above "Not operable 1", "Not operable 2" and "Not operable 3", the operations become operable by disabling the password function of the execution project saved in the RAM/ROM1 of the CPU unit.

■ Copy operation of project in SD memory card

Project status in SD memory card / Project status in PLC (ROM1)	Limited distribution password	Unlimited password	No password
Limited distribution password	Copiable when matched	Not copiable 1	Not copiable 2
Unlimited password	Copiable when matched	Copiable when matched	Not copiable 3
No password	Not copiable	Copiable	Copiable

(Note 1) In the cases of the above "Not copiable 1", "Not copiable 2" and "Not copiable 3", the operations become operable by disabling the password function of the execution project saved in the RAM/ROM1 of the CPU unit.

◆ **KEY POINTS**

- **The download or online editing cannot be performed for the execution project memory (ROM1) during SD memory card operation regardless of the security function settings. Also, comments cannot be read when uploading.**

Record of changes

Manual No.	Date	Record of Changes
WUME-FP7CPUSEC-01	Dec.2013	First Edition

Please contact .....

Panasonic Industrial Devices SUNX Co., Ltd.

■ Overseas Sales Division (Head Office): 2431-1 Ushiyama-cho, Kasugai-shi, Aichi, 486-0901, Japan
■ Telephone: +81-568-33-7861 ■ Facsimile: +81-568-33-8591
panasonic.net/id/pidsx/global

About our sale network, please visit our website.

December, 2013 PRINTED IN JAPAN

WUME-FP7CPUSEC-01