Renesas Flash Programmer V3.25

Software Manual

All information contained in these materials, including products and product specifications, represents information on the product at the time of publication and is subject to change by Renesas Electronics Corp. without notice. Please review the latest information published by Renesas Electronics Corp. through various means, including the Renesas Electronics Corp. website (http://www.renesas.com).

Renesas Electronics
www.renesas.com

Rev. 1.00 Oct 2026

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.
   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.
(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan

www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit: www.renesas.com/contact/.

© 2026 Renesas Electronics Corporation. All rights reserved.

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)
   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on
   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state
   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins
   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals
   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin
   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses
   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products
   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Preface

The Renesas Flash Programmer is software used to program the on-chip memories of Renesas microcontrollers and external memories on the same system.

If you have any questions or requests about the Renesas Flash Programmer, submit your opinions or impressions by using the Give Feedback form or contact your local distributor.

For technical support, select [Help] → [Technical Support] from the menu bar to jump to the [Technical Support] page on the Renesas Web site.

You can download the latest manuals from the Renesas Tools homepage (https://www.renesas.com/rfp).

User Registration

Renesas Electronics recommends that customers who are using Renesas tool products register as users.

For details, refer to “Information about Tool User Registration” at the link below.

Tool User Registration: https://www.renesas.com/software-tool/tool-user-registration

User registration is available through “My Renesas”: https://www.renesas.com/myrenesas

How to Use This Manual

Purposes and Target Readers

The purpose of this manual is to give users an understanding of the basic specifications and correct use of the Renesas Flash Programmer. This manual is intended for users who are using the programmer in designing and developing a system that employs a Renesas Electronics microcontroller equipped with on-chip memory.

It is assumed that the readers of this manual have a basic knowledge of microcontrollers, Windows, Linux, and macOS, and some knowledge of electrical and logic circuits.

Use this software after sufficiently confirming the manual of the microcontroller in use.

Conventions

- Note: Footnote for item marked with “Note” in the text.
- Caution: Information requiring particular attention
- Remark: Supplementary information
- Numeral representations: Binary ... xxxx or xxxxB
  Decimal ... xxxx
  Hexadecimal ... 0xXXXX or xxxxH
- “ ”: Any character or item on the screen that can be selected or input
- [ ]: Name of a button
- [ ]: Name of a command, dialog box, tabbed page, option, or area on the screen

Terminology

The meanings of the terms used in the Renesas Flash Programmer manual are as follows.

(1/2)

Term	Meaning
RFP	Abbreviation of “Renesas Flash Programmer”
MCU	Abbreviation of “microcontroller unit”
E1/E20/E2/E2 Lite	Abbreviation of “the E1, E20, E2, or E2 emulator Lite”
J-Link	SEGGER-produced debug probe for MCUs
Tool used	A general term for tools such as the E1, E20, E2, E2 Lite, and J-Link.
Target device	Renesas Electronics MCU with on-chip memory and external memories on the same system.
Target system	User-designed board on which the target device is mounted
Input clock	A clock from an oscillator or a resonator which is externally input to the target device
Project file	Project files hold the data required to write programs. In the RFP, a project file holds the settings related to the programming environment, such as target device settings and command option specifications. Project files have the filename extension *.rpj.
Parameter file	Parameter files include information required to program the memory of the target device, and are created by acquiring information from the target device. Parameter files have the extension *.fcf.
Lock bit	One of the safety functions of the MCU. For details, refer to the manual of the target device.
HEX file	A program file in Intel HEX format or Motorola S-record format that does not contain flash option data.
HCUHEX file	Program file containing a combination of a HEX file generated by using the HEX Consolidation Utility (HCU) to produce ROM code for ordering preprogrammed flash memory devices from Renesas Electronics and flash option data
RPI file	RPI files are image files generated by the RFP that combine usable HEX files and flash options data.
RPE file	An encrypted program file that has been generated by the encryption utility program
SFP file	An encrypted program file that has been generated by the Security Key Management Tool
Program file	“Program file” refers to a file that contains a program to be written to the target device. The RFP supports the following program file formats. a. HEX files in Intel HEX format b. HCUHEX files in Intel HEX format c. HEX files in Motorola S format d. HCUHEX files in Motorola S format e. RPI files Refer to section 1.5.1, RPI File. The only supported character code is ASCII (one byte). Unicode (two bytes) is not supported. f. RPE files Refer to section 1.5.2, RPE File. g. Binary files h. SFP files

(2/2)

Term	Meaning
COM port	COM port is a serial interface port of the host PC. When writing data to the target system by using a serial interface of the host PC, select the COM port (COMx) as the tool to be used. Any value from 1 to 256 can be specified for *x*.
USB Direct	USB Direct is a method of writing to the MCU in the USB boot mode by using the USB interface port of the host PC.
FINE	FINE is a single- or dual-line communications interface operating through the FINE pin or pins of an MCU. Some of our MCUs support writing via single line FINE.
ID code	Authentication code used for memory programming and on-chip debugging. For details, refer to the manual of the target device.
ID authentication mode	One of the security functions of the MCU. Connection of the programmer is protected by ID authentication.
OTP	A security function of the MCU. For details, refer to the manual of the target device.
Access window (AW)	This is also referred to as the “flash shield window”. The specified range is selected as the access window (and window area), and functionality in other ranges is restricted to a degree which depends on the operating mode. For details, refer to the manual of the target device.
Flash options	Flash options are settings which determine the state after the MCU is reset, and is a general term for settings which must be specified separately from the HEX file.
TSIP	Dedicated hardware secure IP (trusted secure IP) for managing the encryption key. For details, contact a Renesas Electronics sales office.
DLM	Management to maintain security in the entire life cycle of the device (device life-cycle management). For details, refer to the manual of the target device.
Authentication code	A collective term for authentication codes, including ID codes, passwords, and DLM keys.
Renesas Partition Data File	File including the information on the boundary setting output from the e^2 studio for the RA Family
SWD	Two-wire communications interface using the debug communications pins of the MCU
Security Key Management Tool	The Security Key Management Tool is a key-wrapping tool for use with key-management systems that use security IP modules incorporated in Renesas MCUs and MPUs. For details, refer to the following Web page. https://www.renesas.com/software-tool/security-key-management-tool
External Memory Loader	A file generated by building the External Flash Library and converting it into a format that can be loaded by the tool. For details, refer to the following Web page. https://www.renesas.com/document/apn/ra-familly-external-flash-library-tools
Boot Image File	A firmware file that is downloaded to SRAM and used for memory programming. Examples include Provisioning SW with a certificate added by the Security Key Management Tool. For details about Provisioning SW, refer to the following Web page. https://www.renesas.com/software-tool/security-key-management-tool

Replacing Terms

Some terms used in this application should be replaced as shown in the table below, depending on the target device to be used.

Term in This Application	To be Replaced with
USB Direct	USB interface mode

- When an RL78 is to be used:

Term in This Application	To be Replaced with
Access window (AW)	Flash shield window

- When an RH850 is to be used:

Term in This Application	To be Replaced with
Boot mode	Serial programming mode

- When an RH850 with an extended user area is to be used:

Term in This Application	To be Replaced with
User Boot Area	Extended user area

- When an RH850 with an extended data area is to be used:

Term in This Application	To be Replaced with
Data Flash	Extended data area

- When an RH850 with a double map mode is to be used:

Term in This Application	To be Replaced with
Dual mode	Double map mode
Linear mode	Single map mode

- When an RH850, RA, RX, RISC-V MCU, or Renesas Synergy™ is to be used:

Term in This Application	To be Replaced with
Config Area	• RH850 (*1) Configuration setting area • RA, RX, RISC-V MCU, or Renesas Synergy™ Option-setting memory (*1): The term differs with the target device.

- When an MCU with MRAM is to be used:

Term in This Application	To be Replaced with
Flash memory	MRAM
Flash area	MRAM area

Table of Contents

1. Overview....12
1.1 Features....12
1.2 Supported Microcontrollers....12
1.3 System Overview....13
1.3.1 Connection with the Target System....13
1.4 Operating Environments....14
1.4.1 Hardware Environment....14
1.4.2 Software Environment....14
1.5 Formats of Program Files....15
1.5.1 RPI File....16
1.5.2 RPE File....16
1.6 Relative Paths for Files....16

2. Descriptions of Functions....17
2.1 Main Window....17
2.2 Creating a New Project....18
2.2.1 [Create New Project] Dialog Box....18
2.2.2 [Tool Details] Dialog Box....20
2.2.3 [Set Clock] Dialog Box....23
2.2.4 [Authentication] Dialog Box....23
2.2.5 [Set Boot Image] Dialog Box....24
2.3 Operating the Tabbed Pages....25
2.3.1 [Operation] Tabbed Page....26
2.3.2 [Operation Settings] Tabbed Page....30
2.3.3 [Block Settings] Tabbed Page....34
2.3.4 [Flash Options] Tabbed Page....35
2.3.5 [Connect Settings] Tabbed Page....35
2.3.6 [Unique Code] Tabbed Page....38
2.3.7 [External Memory Settings] Tabbed Page....41
2.4 Features of the Flash Options....42
2.4.1 “Set Option” (Common to Each Flash Option)....42
2.5 Menu Bar....48
2.5.1 [File] Menu....48
2.5.2 [Target Device] Menu....51
2.6 Simple Use of Project Files from a Command Line....56
2.6.1 Exit Code....56
2.6.2 Restriction....56
2.6.3 Command-line Syntax....56
2.6.4 Start Options....57
2.6.5 Example of Command-line Statements....62
2.7 Command Line for Windows, Linux, or macOS....62
2.8 Encryption Utility Program....63
2.8.1 Exit Code....63
2.8.2 Command-line Syntax....63
2.8.3 Start Options....63
2.9 Renesas Flash Programmer Utility Program....64

3. Operating the RFP....65
3.1 Flow of Operations....66

4. Troubleshooting 76
4.1 Problems during Startup 76
4.2 Problems during Operation 77
4.3 Problems during Communications 84
4.4 Error Messages 86
4.4.1 List of Security and Safety Functions of the Target Device that May Affect the Operation of the Programmer 94

5. Points for Caution 95
5.1 Manipulating the User Boot Mat 95
5.2 Host PC 95
5.3 Check before Connection 95
5.4 Erasing a Chip 95
5.5 Auto-padding with 0xFF 95
5.6 Verification after Protecting the target device 96
5.7 Switching to Dual Mode 96
5.8 Switching to Double Map Mode 97
5.9 RL78/F2x 97
5.10 SWD Interface Connection 98
5.11 DA14xxx / RA6Wx 98
5.12 Security Memory Protection Unit (MPU) 99
5.13 Erase Command 99

1. Overview

The Renesas Flash Programmer (hereafter referred to as the RFP) is software that uses an E2 emulator Lite (hereafter referred to as the E2 Lite), E2 emulator (hereafter referred to as the E2), E1 emulator (hereafter referred to as the E1), or E20 emulator (hereafter referred to as the E20) via a serial or USB interface or a J-Link debug probe (hereafter referred to as the J-Link) to erase, write, and verify programs for a target device on a target system.

1.1 Features

- Writing controlled by the host PC
- High-speed writing by using an emulator
- Simple operation for writing with a simple GUI specific to development
- Automatic writing from a command line
- Programming of a unique code to a designated area of flash memory
- Support of encrypted program files

1.2 Supported Microcontrollers

For information on additional supported target devices and external flash memories, refer to Renesas Flash Programmer V3 Release Note. For information on other supported target devices, refer to List of MCUs supported by Renesas Flash Programmer V3.

1.3 System Overview

An overview of the RFP system is illustrated in the following diagram.

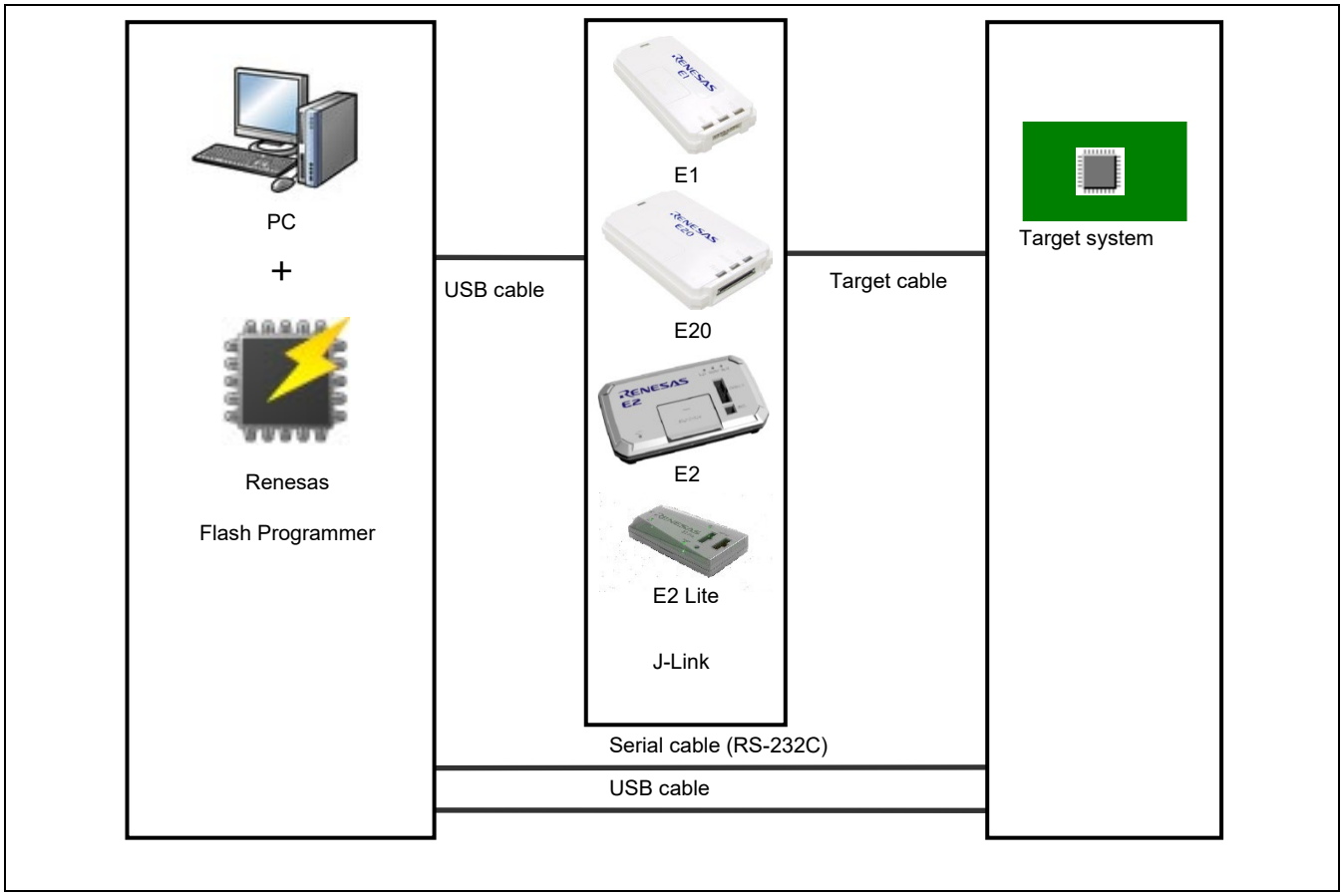


Figure 1-1 RFP Connection Image

1.3.1 Connection with the Target System

For examples of recommended connections between the RFP and the target devices, refer to the PG-FP6, Renesas Flash Programmer Additional Document for User's Manual (Recommended Circuits for Connecting the Flash Programmer).

1.4 Operating Environments

1.4.1 Hardware Environment

(1) Host PC

- Processor: 1 GHz or faster
- Main memory: At least 2 Gbytes; 4 Gbytes or more recommended
- Display: 1,024 x 768 or higher
- Interface: USB 2.0 (when using E1, E20, E2, E2 Lite, USB Direct, or J-Link)
  Serial interface (RS-232C, when using a COM port)

(2) Tools supported

- E1 emulator
- E20 emulator
- E2 emulator
- E2 emulator Lite
- J-Link debug probe from SEGGER (*1)
- USB (*2, *3, and *4)
- Serial port

Note: Support for the J-Link (*1)
For the J-Link supported by the RFP, refer to the Web page at the following link.
https://www.renesas.com/rfp_users

Remark: Recommended product for use as a USB-to-serial converter (*2): FT232R from FTDI
With a USB-to-serial converter, the PC recognizes the tool as being connected through a virtual COM port. Select “COM port” as the tool for the RFP.

Remark: The supported target devices differ with the tool. For the target devices supported by the different tools, refer to List of MCUs supported by Renesas Flash Programmer V3.

Remark: Connection through USB Direct (*3)
Applicable devices: RX71x, RX64x, RX63x, RX62x, RX61x, RX200, and RX100

Remark: USB connection (with serial communications through a virtual USB COM port) (*4)
Applicable devices: RX65x, RX66x, RX67x, RX72x, RA, RE, and Renesas Synergy™
With a USB connection, the PC recognizes the tool as being connected through a virtual COM port. Do not select “USB Direct” but select “COM port” as the tool for the RFP.

Remark: JTAG connections are not supported.

1.4.2 Software Environment

(1) OSs supported

- Windows 10 (32-bit and 64-bit)
- Windows 11
- Linux (Ubuntu 22.04 LTS, x64/ARM32/ARM64) (*1)
- Linux (Ubuntu 24.04 LTS, x64/ARM64) (*1)
- macOS 15 Sequoia (only supported on machines with Apple silicon) (*2)
- macOS 26 Tahoe (only supported on machines with Apple silicon) (*2)

Remarks:
1. We recommend having the latest version of Windows installed.
2. A point for caution applies with regard to the security function of Windows. For details, refer to item (4) in section 4.2, Problems during Operation.
3. The GUI (RFPV3.exe) does not run. (*1), (*2)
4. The E1 emulator and E20 emulator are not supported. (*1), (*2)
5. The USB boot mode connection with RA devices is not supported. (*2)
6. In some cases, the UART (serial port) connection may not correctly operate or certain restrictions may apply according to the version of the OS. (*2)
7. ARM32 is not supported by Ubuntu 24.04 LTS and later versions.

(2) Required software

- Linux and macOS: Refer to the guide “rfp-cli.md”, which is separately provided. Note that this is a markdown-format English file.

(3) USB drivers

Installing the RFP in Windows also leads to the following USB drivers being installed.

For Linux and macOS, refer to “rfp-cli.md”.

For details on the target devices supported by each of the USB drivers (tools), refer to List of MCUs supported by Renesas Flash Programmer V3.

- USB driver for the E1 or E20 emulator
  USB driver for the E1 or E20 emulator (for 32-bit and 64-bit Windows).
- USB driver for Renesas MCU tools
  USB driver for 32-bit versions of the Windows OS, which supports the IE850, IE850A, E2 emulator, E2 emulator Lite, and PG-FP5.
- USB driver for MCU tools
  USB driver for 64-bit versions of the Windows OS, which supports the IECUBE, IE850, IE850A, MINICUBE, MINICUBE2, E2 emulator, E2 emulator Lite, and PG-FP5.
- USB driver for USB-boot MCU Type A
  USB driver for the Renesas Flash Programmer for USB-boot MCU Type A, which supports devices of the RX Family (RX100, RX200, RX62x, RX63x, RX64x, and RX71x groups).
- USB driver for USB-boot MCU Type B
  USB driver for the Renesas Flash Programmer for USB-boot MCU Type B, which supports Renesas Synergy™ microcontrollers, devices of the RX Family (excluding the RX100, RX200, RX62x, RX63x, RX64x, and RX71x groups), RA Family, and RE Family.

1.5 Formats of Program Files

For a HEX file to be readable by the RFP, it must have the correct format and satisfy the following conditions. If a program file with a non-supported format is read, an error will occur.

(1) Intel HEX format

- The format file ends with the end record.
- All lines consist solely of record types 00 to 05.

(2) Motorola S format

- The format file ends with the end record (S7, S8, or S9).

- All lines consist solely of record types S0 to S9 (excluding S4).

1.5.1 RPI File

An RPI file is an image file that the RFP can generate. An RPI file combines program code and flash options data. Refer to section 2.5.1.4, [Save Image File], for the generation of these files.

1.5.2 RPE File

An RPE file is a file generated by using the encryption utility program to encrypt a program file. Refer to section 2.8, Encryption Utility Program, for the generation of such files.

1.6 Relative Paths for Files

When the following files are registered in a project, the RFP automatically uses relative paths in saving the files under the project directory.

- Program file
- Unique code file
- Key file
- Renesas Partition Data File
- Boot Image File

2. Descriptions of Functions

This chapter describes the window structure and functions of the RFP.

2.1 Main Window

After the RFP is started, the main window as shown below will appear.

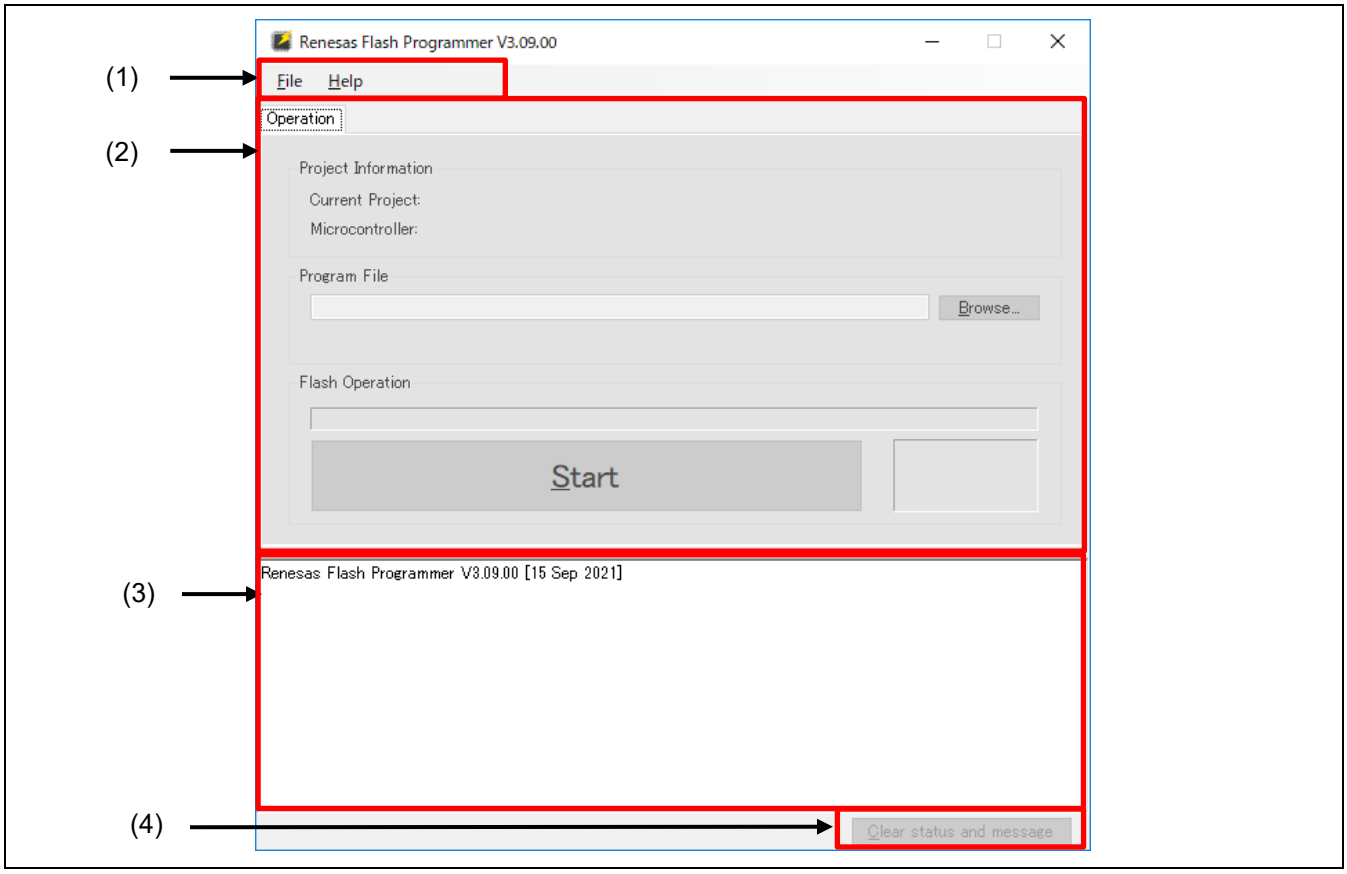


Figure 2-1 Main Window

(1) Menu bar

For the menu bar, refer to section 2.5, Menu Bar.

(2) Tabbed pages

Operations on the tabbed pages enable controlling the RFP for writing, setting options, and so on. For details on the individual tabbed pages, refer to section 2.3, Operation of the Tabbed Pages.

(3) Log output panel

The version information of RFP and the contents and results of command execution are displayed here.

Caution: Log entries older than the 1500th line are automatically removed.

(4) Clear status and message

Pressing this button clears the contents of the log output window and the status information on the [Operation] tabbed page.

2.2 Creating a New Project

2.2.1 [Create New Project] Dialog Box

Selecting [File] → [Create a new project] in the menu bar makes the [Create New Project] dialog box appear. The configuration of the dialog box is shown below.

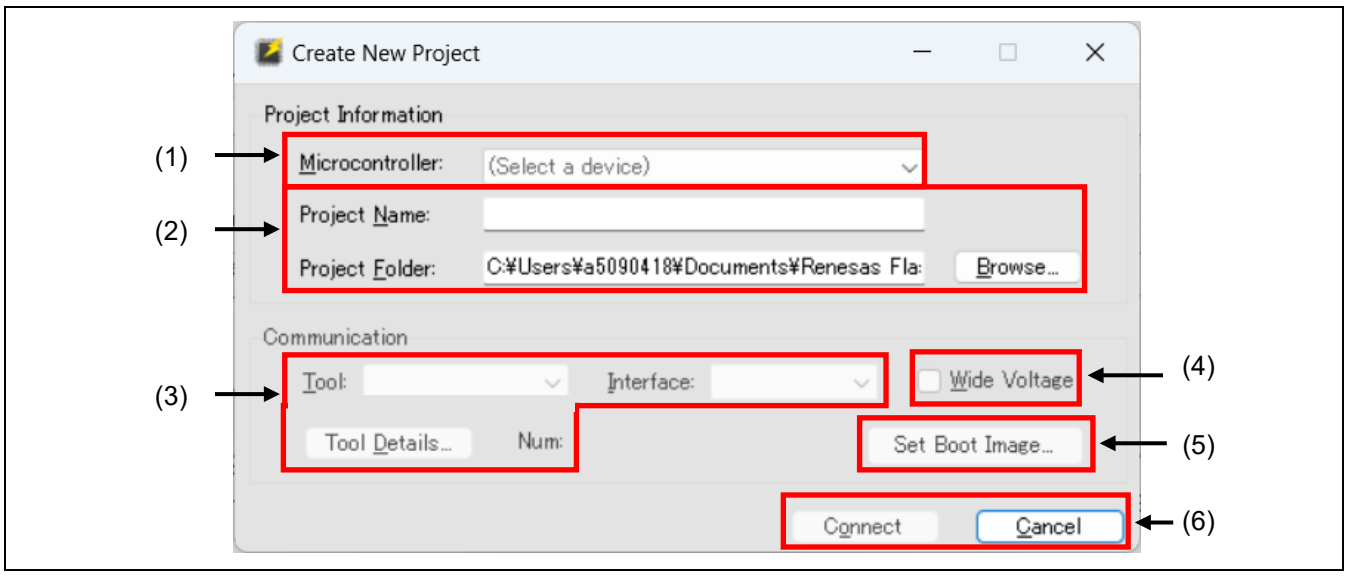


Figure 2-2 [Create New Project] Dialog Box

(1) Microcontroller

Select the type of target device to be used.

(2) Project Name and Project Folder

Specify the name of a project which is to be newly created and the project folder which will hold the created project file.

Remark: Since the project name is used in the file name, characters that are not usable in file names cannot be used.

(3) Communication

Set up communications with the target device.

- "Tool"
  Select the tool to be used for connection with the target device.

Caution: For the USB connection of some target devices, select "COM port", since serial communications are performed through a virtual USB COM port. For the applicable target devices, refer to remark in item (2) of section 1.4.1.

Remark: The usable tools may differ with the selected target device.

- "Interface"
  When this item is selectable, select the method for communicating with the target device.

- Tool Details…
  Make detailed settings for the tool to be used. The tool in use and the setting for the supply of power supply are shown to the right of Tool Details…. For details on Tool Details…, refer to section 2.2.2, [Tool Details] Dialog Box.

(4) Wide Voltage

When “Wide Voltage” is selected, each command can be executed with the target device set to wide voltage mode. When writing to the target device proceeds with a voltage lower than 2.4 V (or lower than 2.7 V in the case of an RL78/F2x device), deselect this checkbox. For details on the wide voltage mode, refer to the manual of the target device.

Remark: “Wide Voltage” is not displayed for those target devices which do not support it.

(5) Set Boot Image…

Sets the image file for memory programming. For details on Set Boot Image…, refer to section 2.2.5 [Set Boot Image] Dialog Box.

Remark: Set Boot Image… is not displayed for those target devices which do not support it.

(6) Connect

Clicking on Connect enables connection with the target device.

At this time, the following dialog boxes might be displayed according to the type of the target device; enter a value in each dialog box to continue processing to make the connection.

- [Set Clock] dialog box
- [Authentication] dialog box
  For details on these dialog boxes, refer to sections 2.2.3, [Set Clock] Dialog Box, and 2.2.4, [Authentication] Dialog Box.

Caution: If the connection is made with incorrect settings, the tool or the target system might be damaged. For details, refer to chapter 5, Points for Caution.

2.2.2 [Tool Details] Dialog Box

The [Tool Details] dialog box consists of the following tabbed pages.

- [Select Tool] tabbed page
- [Reset Settings] tabbed page
- [Mode Pin Setting] tabbed page
  The [Mode Pin Setting] tabbed page is only displayed when the E1, E20, E2, or E2 Lite is selected.

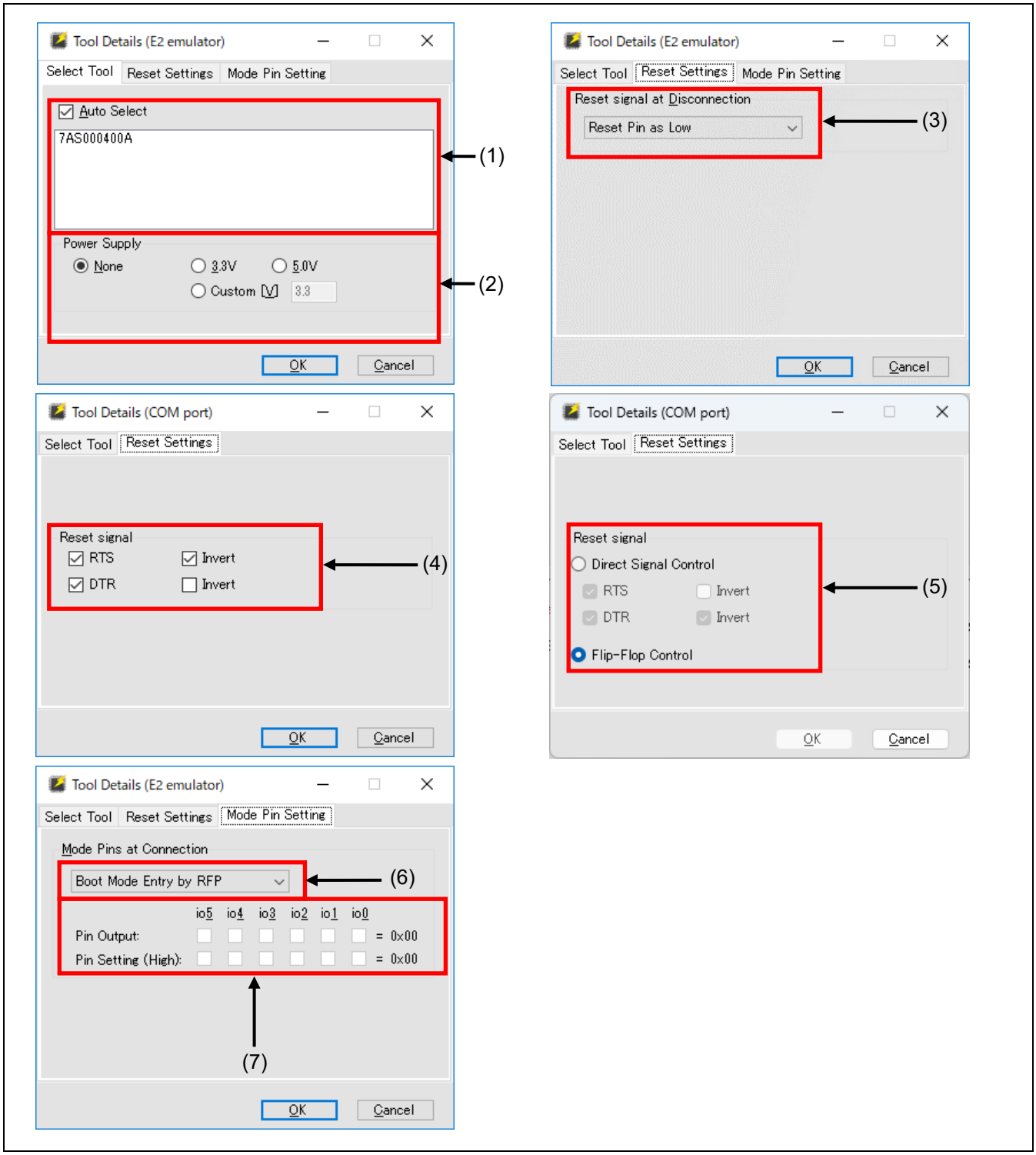


Figure 2-3 [Tool Details] Dialog Box

(1) [Select Tool]

Tools which are currently available are shown; select the tool to be used.

When the “Auto Select” checkbox is selected, the tool which is shown at the top of the list is automatically selected. To directly select the tool to be used, deselect the “Auto Select” checkbox and select a tool from the list.

Remark: For the E1, E20, E2, or E2 Lite, the serial number of the emulator is shown.

(2) Power Supply

Select the power-supply function of the tool.

Select “None” if no power is to be supplied from the tool in use.

Specify the voltage when the tool in use is to supply power.

For the power-supply function, refer to the manual of the tool you are using.

Caution: Do not use the power-supply function from the tool in processing for mass-production; instead, supply power which matches the target device’s specifications from the target system. Since the voltage supplied from the tool depends on the performance of the USB power supply of the host PC, its precision cannot be guaranteed.

Remark: [Custom] only appears in the [Tool Details] dialog box when the E2 emulator is selected. A voltage within the range from 1.8 V to 5.5 V can be specified.

(3) Setting of RESET

Sets the operation of the reset signal when the RFP is disconnected from the target device.

- Reset Pin as Low
  After the RFP is disconnected from the target device, the low level continues to be output from the RESET pin.
- Reset Pin as Hi-Z
  After the RFP is disconnected from the target device and the RESET pin has been at the low level, the RESET pin enters the hi-Z state. This setting is used when the user wishes to operate the target device on completion of processing with the RFP.

(4) Settings for reset signals - 1

Make settings for pins to be used for the output of reset signals to the target device.

Remark: Reset signals are only displayed when “COM port” is selected for the tool.

- Selection of the RTS or DTR signal
  Selected: The signal is used as a reset signal.
  Deselected: The signal is not used as a reset signal.
- Logic of the signal
  Selected: The RTS or DTR signal outputs the high level when the device is reset.
  Deselected: The RTS or DTR signal outputs the low level when the device is reset.

(5) Settings for reset signals - 2

Make settings for pins to be used for the output of reset signals to the target device or the output of reset signals with the use of the flip-flop circuit.

Remark: Reset signals are only displayed when a supported target device is selected.

- Selection of the RTS or DTR signal
  Selected: The signal is used as a reset signal.
  Deselected: The signal is not used as a reset signal.
- Direct Signal Control
  For details, see item (4), Settings for reset signals - 1.
- Flip-Flop Control
  Select this radio button when reset signals are to be output with the use of the flip-flop circuit.

(6) Setting of entry to boot mode

Make settings for pins when the target device is connected.

- “Boot Mode Entry by RFP”
  The settings of “Pin Output” and “Pin Setting” according to the recommended circuits of the tool in use are made automatically.

Remark: For the recommended circuit, refer to the manual of the tool you are using.

- “Boot Mode Entry by User”
  Manually make the settings for “Pin Output” and “Pin Setting”.

Remark: “Boot Mode Entry by User” might not be selectable depending on the target device or tool in use and the communications interface.

(7) Setting of outputs

Selecting “Boot Mode Entry by User” for boot mode entry enables the setting of outputs.

The boxes set the output of the io0 to io5 pins of the tool in use when the target device is connected.

- Pin Output
  Selected: The target pin is used as an output pin.
  Deselected: The target pin is used as hi-Z.
- Pin Setting (High)
  Selected: The high level is output.
  Deselected: The low level is output.

Remark: For pin assignments of io0 to io5 in the E1, E20, E2, and E2 Lite, refer to the PG-FP6, Renesas Flash Programmer Additional Document for User’s Manual (Recommended Circuits for Connecting the Flash Programmer).

2.2.3 [Set Clock] Dialog Box

The input clock must be set to suit the type of the target device.

If setting of the input clock is required, the [Set Clock] dialog box will appear.

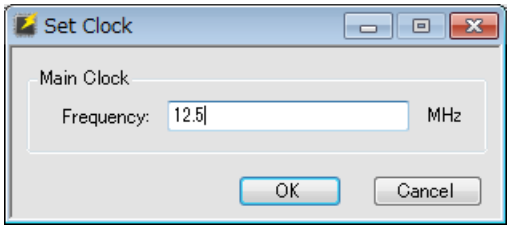


Figure 2-4 [Set Clock] Dialog Box

Enter the frequency of the input clock and click on OK.

The value for frequency is entered in MHz. If you want to enter a value in smaller units than MHz, use a decimal point.

2.2.4 [Authentication] Dialog Box

If entering an authentication code is required, the [Authentication] dialog box will appear.

Remark: Whether or not there is an authentication code function depends on the target device.

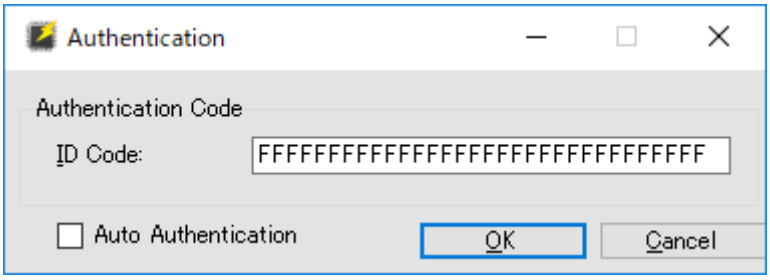


Figure 2-5 [Authentication] Dialog Box

- Authentication Code
  Enter the authentication code in hexadecimal notation (0 to 9 and A to F).
- Auto Authentication
  When this checkbox is selected, the authentication code is saved in the project file and authentication automatically proceeds from the next time the project is opened.

Caution

- If the value of the input field takes up fewer than the number of effective bytes, the RFP automatically pads the input data with 0xFF after the input value.
- When an RX Family device is connected via the RFP, input the value in the order ID1, ID2, ..., ID16. However, for a device with control code, enter the value of the code as the first of the effective bytes.
  Example:
  When the number of effective bytes = 16, control code = 0x45, ID code = ID1=0x01, ID2=0x02, ID3=0x03, ID4=0x04, ID5=0x05, ID6=0x06, ID7=0x07, ID8=0x08, ID9=0x09, ID10=0x0A,

ID11=0x0B, ID12=0x0C, ID13=0x0D, ID14=0x0E, and ID15=0x0F, the value will be '45010203040506070809 0A0B0C0D0E0F'.

- When RX72x, RX71x, RX67x, RX66x, RX65x, or RX64x device is connected via a debug tool which has been specified with the CS+ or e2 studio, the order for input of the authentication code changes to that shown below.
  ID4 ID3 ID2 ID1 ID8 ID7 ID6 ID5 ID12 ID11 ID10 ID9 ID16 ID15 ID14 ID13
- When an RA Family, Renesas Synergy™-microcontrollers, or RE Family device is connected to the RFP, input values to be specified for registers of the target device in order of bits 127 to 0 in byte units. Since the input specification may also differ with the tool, confirm the input specification of the tool you will be using.
- For an RH850 Family device, when the ID code for programming is to be generated in a program file instead of on the [Option Settings] tabbed page, enter the value set for the register in the target device from the higher-order bits in byte units. Example: For ID255 to ID0, the first byte is entered as ID255 to ID248 and the second byte is entered as ID247 to ID240.

Remark: The default authentication code in some target devices at the time of shipment is all FFs. For details, refer to the manual of the target device.

2.2.5 [Set Boot Image] Dialog Box

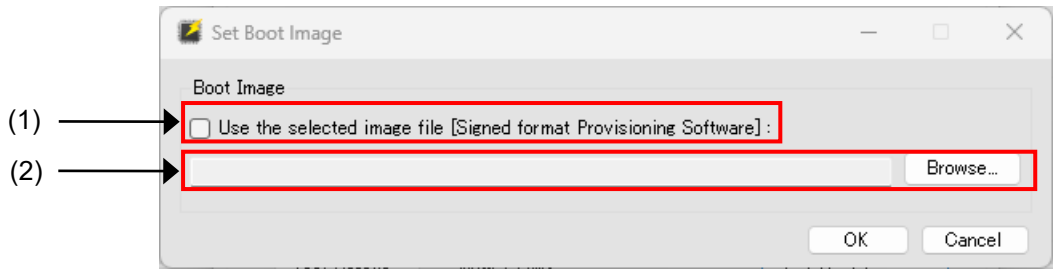


Figure 2-6 [Set Boot Image] Dialog Box

(1) Use the selected image file

When this checkbox is selected, the image file is used. The file type is also displayed on the right.

(2) Selected File

An image file for memory programming can be added by clicking the Browse… button or by drag and drop.

2.3 Operating the Tabbed Pages

When “Create New Project” is completed normally, the main window of the RFP is displayed.

Operating the tabbed pages in the main window allows you to make detailed settings of the RFP.

The tabbed pages consist of the seven listed below.

- [Operation] tabbed page
- [Operation Settings] tabbed page
- [Block Settings] tabbed page
- [Flash Options] tabbed page
- [Connect Settings] tabbed page
- [Unique Code] tabbed page
- [External Memory Settings] tabbed page

The following describes the configuration and operation of each tabbed page.

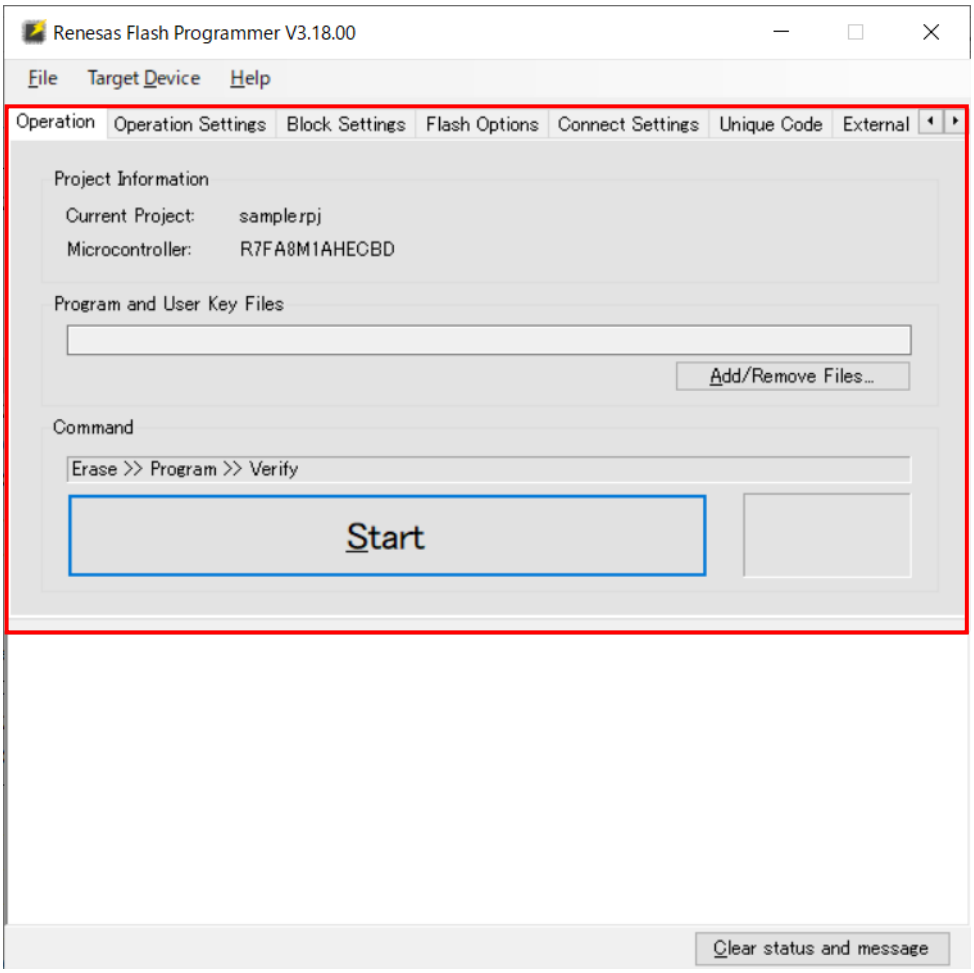


Figure 2-7 Main Window

2.3.1 [Operation] Tabbed Page

The [Operation] tabbed page shows information on the project and command.

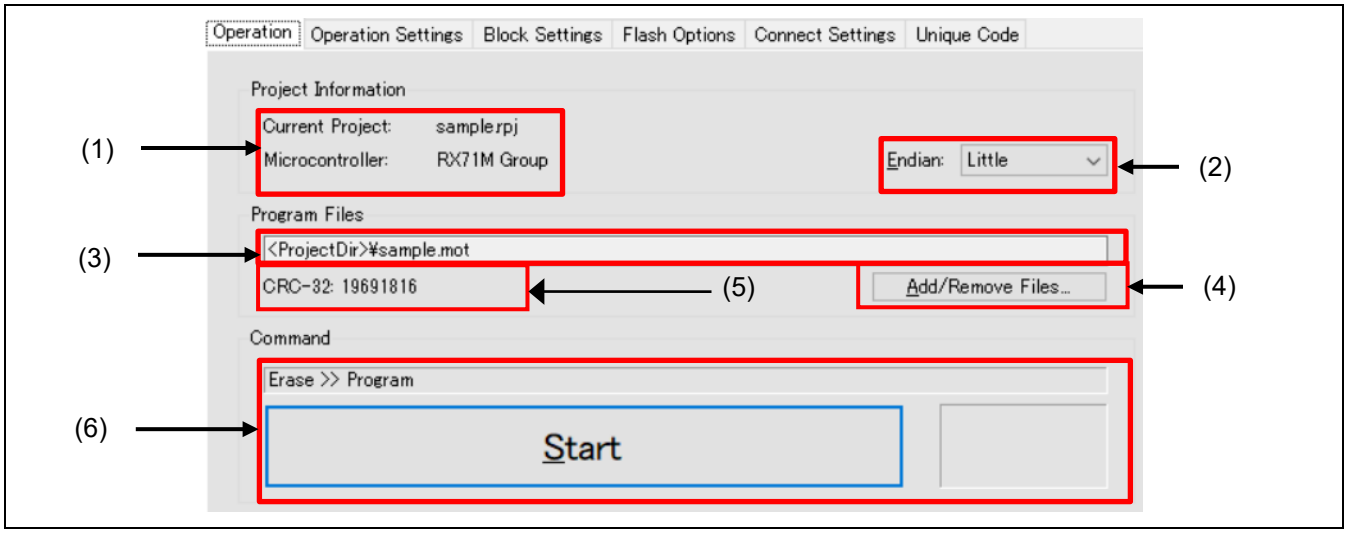


Figure 2-8 [Operation] Tabbed Page

(1) Project Information

Information on the selected project is shown.

(2) Endian

Select the endianness for the data of the program file.

This item does not appear for target devices which do not support changing the endianness in the RFP.

- "Little"
  Set the handling of files for programming as little endian.
- "Big"
  Set the handling of files for programming as big endian.

(3) Program Files/Program and User Key Files

Register a file to be programmed in the flash memory of the target device and a user key file. Drag and drop the file icon or click on Add/Remove Files… to select a file.

Multiple files for programming are also selectable simultaneously. Refer to 2.3.1.1, Selecting Multiple Program Files, for details.

Caution: The [Program and User Key Files] feature may be displayed for a target device that does not actually support user keys. Refer to the manual of the target device regarding whether or not the user key function is available.

Remarks: 1. For the type of user keys and the features, refer to the application note of the standard boot firmware.
2. For details on how to generate user key files, refer to Security Key Management Tool.

(4) Add/Remove Files

The [File Details] dialog box is displayed. Adding and removing files and changing the write addresses and offsets of files are possible. For details, refer to section 2.3.1.2, [File Details] Dialog Box.

(5) File Checksum

The CRC-32 checksum is displayed for a single selected program file and the number of files is displayed for two or more selected program files.

Caution: This CRC-32 is a checksum for whole of file, not for HEX data. The file checksum is different from the checksum of the one obtained from the target device.

(6) Command

Clicking on Start leads to the execution of commands to handle the processing shown above Start.

Information on the state is indicated with color and characters in the status display to the right of Start. For the status display, refer to table 2-1.

The types of command can be changed on the [Operation Settings] tabbed page. For the [Operation Settings] tabbed page, refer to section 2.3.2, [Operation Settings] Tabbed Page.

Table 2-1 State Information

	Immediately after the RFP has been started or after clicking on the Clear button under the output panel
Run	A command is being executed.
OK	A command has been executed and ended normally.
Abort	Processing has stopped during the execution of a command.
NG	Processing failed after the execution of a command.

2.3.1.1 Selecting Multiple Files

When selecting multiple files, specify all desired files beforehand then start the command to run the actual programming.

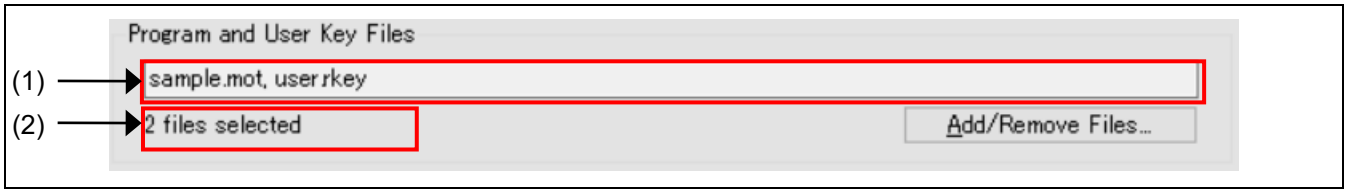


Figure 2-9 [Program and User Key Files] Group Box after the Selection of Multiple Files for Programming

(1) File Name

Only the file names are displayed when multiple files have been selected. When a selected file includes offset or address information, the information is appended as eight hexadecimal digits “XXXXXXXX” at the end of the displayed file name.

(2) File Information

The number of files for programming is displayed.

Caution

- An error occurs if an HCUHEX or RPE file is specified in the selection of multiple files.
- An error occurs when writing to the flash area in cases of overlapping between the addresses of the data files for programming.

2.3.1.2 [File Details] Dialog Box

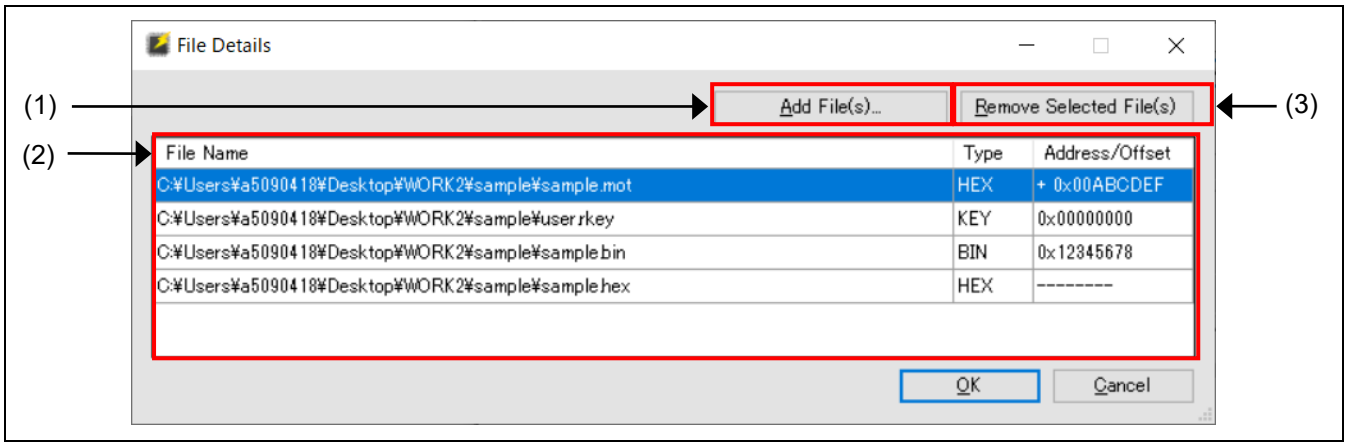


Figure 2-10 [File Details] Dialog Box

(1) Add Files

Clicking on the Add File(s)… button or dragging and dropping file icons enables the addition of program files.

(2) Changing [Address/Offset]

Selecting and double-clicking on the name of a target file opens the [File Offset] dialog box which enables specifying the write address or offset. For details, refer to section 2.3.1.3, [File Offset] Dialog Box.

Remark: An offset can be specified for a HEX file. The entry in the [Address/Offset] column for a HEX file shows “--------” if no offset is specified and “+xxxxxxxx” if an offset is specified.

(3) Remove Selected Files

Select a file or files to be removed. Clicking on the Remove Selected File(s)… button or pressing the delete key of Windows enables removal of the selected file(s).

2.3.1.3 [File Offset] Dialog Box

A binary file or a key file is shown in address mode and other types of file are shown in offset mode.

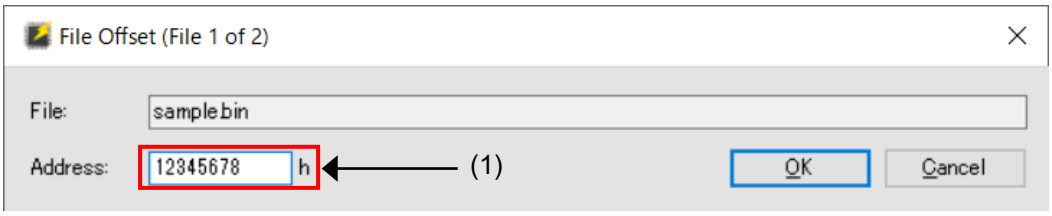


Figure 2-11 [File Offset] Dialog Box (Address Mode)

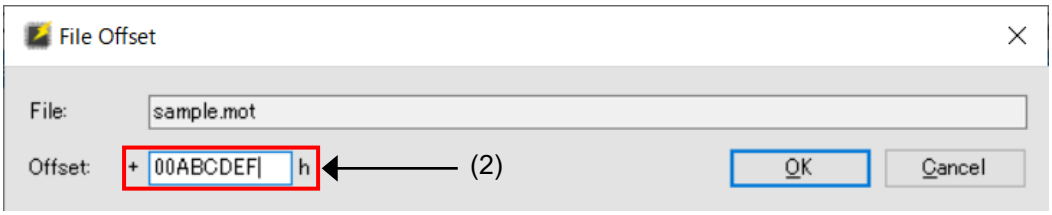


Figure 2-12 [File Offset] Dialog Box (Offset Mode)

(1) Address

Enter the write address of the file in hexadecimal.

(2) Offset

Enter the write offset (additive) of the file in hexadecimal. No entry will be regarded as 0.

2.3.2 [Operation Settings] Tabbed Page

Settings for the command can be changed on the [Operation Settings] tabbed page.

Remark: Some items will not be shown according to the selected program file or the type of the target device.

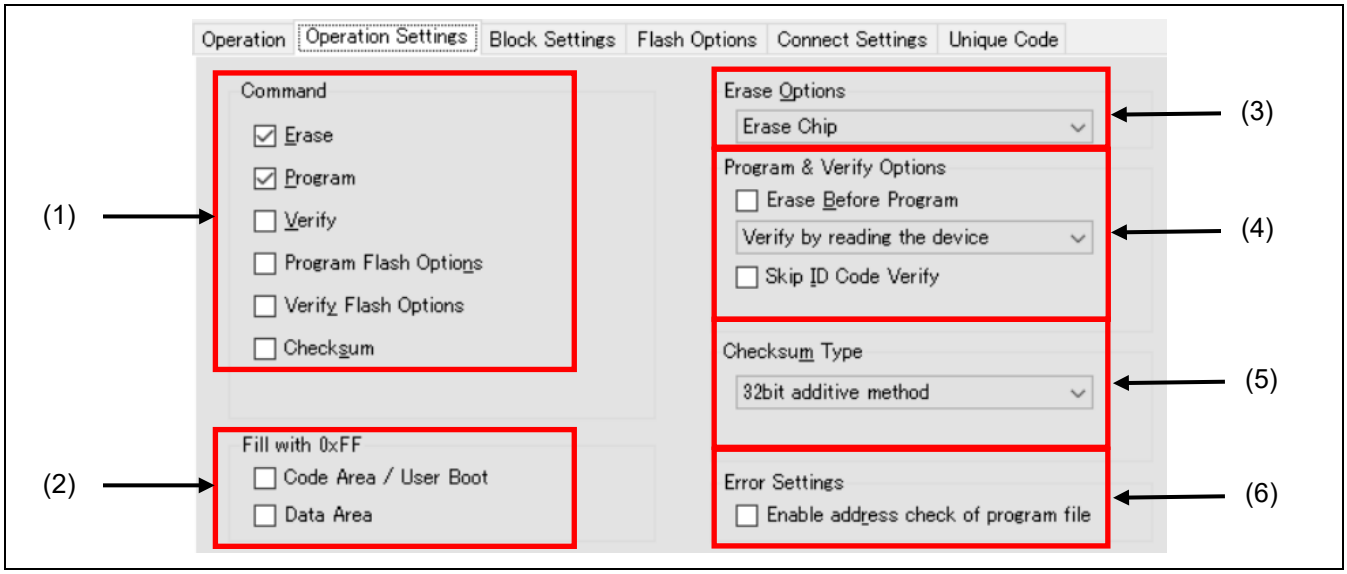


Figure 2-13 [Operation Settings] Tabbed Page

(1) Command

Specify the type of processing that will proceed after clicking on Start in the main window.

When multiple operations are specified for “Command”, each operation is executed from the top item in order.

The following five types of processing can be specified for “Command”, and are described in more detail following the summaries below.

- Erase
  Erase the flash area.
  The range of areas to be erased conforms to the setting made with “(3) Erase Option”.
  For details on a point for caution that applies to this command, refer to section 5.13, Erase Command.

- Program
  Program the flash area.
  The operation reflects the setting made under “(4) Program & Verify Option”.

- Verify
  Handle comparison between the program file and the data in the flash area.
  The operation reflects the setting made under “(4) Program & Verify Option”.

- Program Flash Options
  Set flash options such as “Lockbit”, “OTP”, “Access Window”, “Option Bytes”, and “Security”.
  The programming setting conforms to the settings made on the [Block Settings] and [Flash Options] tabbed pages.
  Note, however, that this command is not displayed if an HCUHEX file, RPI file, or RPE file generated by encrypting an HCUHEX file or RPI file is selected, in which case the flash options are always programmed.

- Verify Flash Options
  Select whether or not to verify values in the flash option area.

- Checksum
  Acquire the checksum.
  The checksum is calculated by the method selected under “(5) Checksum Type”.

Remark: The results are output in units of areas of flash memory. Use the verify command if you want to check the consistency of data in units of blocks.

(2) Fill with 0xFF

Select the method for handling ranges for which files have no data in each area of flash memory.

- Code Area/User Boot Area
  The target range is the code flash and user boot areas including the extended code flash area.

- Data Area
  The target range is the data flash area.

  When this option is selected:
  Programming: The value 0xFF is programmed to bytes in ranges for which the program file has no data.
  Verifying: Ranges containing no data from a program file are regarded as having the value 0xFF for comparison.

  When this option is not selected:
  Programming: Ranges for which the program file has no data are not programmed.
  Verifying: Ranges for which the program file has no data are not verified.

Caution: Even if “Fill with 0xFF” is not selected, when an amount of data is less than the minimum unit for writing to the target memory in the target device, the data are always padded with 0xFF.

(3) Erase Option

Set options when “Erase” is selected for “Command”.

- Erase Selected Blocks
  Erase only those blocks selected on the [Block Settings] tabbed page.
  For the [Block Settings] tabbed page, refer to section 2.3.3, [Block Settings] Tabbed Page.

- Erase All Blocks
  Erase all blocks.

Caution: Erasure processing may be skipped for certain blocks reserved by the target device due to security functions and so on.

- Erase Chip
  Erase all blocks. For devices other than DA and RA6Wx, flash options are also cleared.

Caution
- This processing does not restore the target device to its state at shipment. If correct settings are not programmed for the flash options after erasing the chip, the target device will not operate. When this processing is used on an RH850 Family product, be sure to refer to section 5.4, Erasing a Chip.
- When "Erase Chip" is executed, the chip erasure command, the security release command, or the configuration clear command will be executed after all blocks are erased. For details of these commands, refer to the manual of the target device.

(4) Program & Verify Option

Set options here when you have selected “Program” or “Verify” for “Command”.

- Erase Before Program
  The range where data are to be programmed is erased beforehand if this option is selected.

Caution: The range to be erased depends on the minimum unit of erasing by the target device.

- Verification type
  Select the type of verification as one of the following items. Depending on the target device, only one type may be available.

  — Verify by reading the device
  Data are acquired with a read command from the target device and the RFP handles comparison.
  Comparison cannot proceed if the target device is in a state such that reading is prohibited.

  — Verify in the device
  Data are re-sent to the target device by a verify command or the like, and comparison processing is performed inside the target device.
  Depending on the specifications of the verify command, the range for comparison may extend beyond the programmed data, and this may lead to an error in verification if “Fill with 0xFF” was not selected.
  Use this option if the execution of read commands is disabled by the security settings of the target device.

- Skip ID Code Verify
  In general, do not select the checkbox when this feature is displayed as an option. However, use this feature in cases of the following type.
  The security settings of the target device may make reading of the ID code impossible since the ID code in the target device is protected. This may lead to an error in verification processing. To avoid errors of this type, select this checkbox to use the feature.
  For details, refer to section 5.6, Verification after Protecting the target device.

- Create and write product/image headers
  Create and write a flash header with the program file data if this option is selected. For points for caution, refer to section 5.11, DA14xxx / RA6Wx.

(5) Checksum Type

Select the type of calculation when “Checksum” is selected for “Command”.

The available types of calculation differ according to the target device.

- Calculate block selection range
  Applies to: RL78
  - When this option is selected
    The range of calculation is limited to blocks that are selected in the [Select] column on the [Block Settings] tabbed page.
  - When this option is not selected
    The result for the whole area of the flash memory is output.

(6) Error Settings

Select the method for handling cases where the program file attempts access to data which is out of the range of memory in the target device.

- Enable address check of program file
  - When this option is selected
    In case of attempted access to data that are out of the range of memory, the RFP outputs an error message and stops processing.
  - When this option is not selected
    In case of attempted access to data that are out of the range of memory, the RFP outputs a warning message, ignores that data, and continues processing.

2.3.3 [Block Settings] Tabbed Page

The blocks for operations can be set on the [Block Settings] tabbed page.

Remark: The columns to be displayed differ according to the type of the target device.

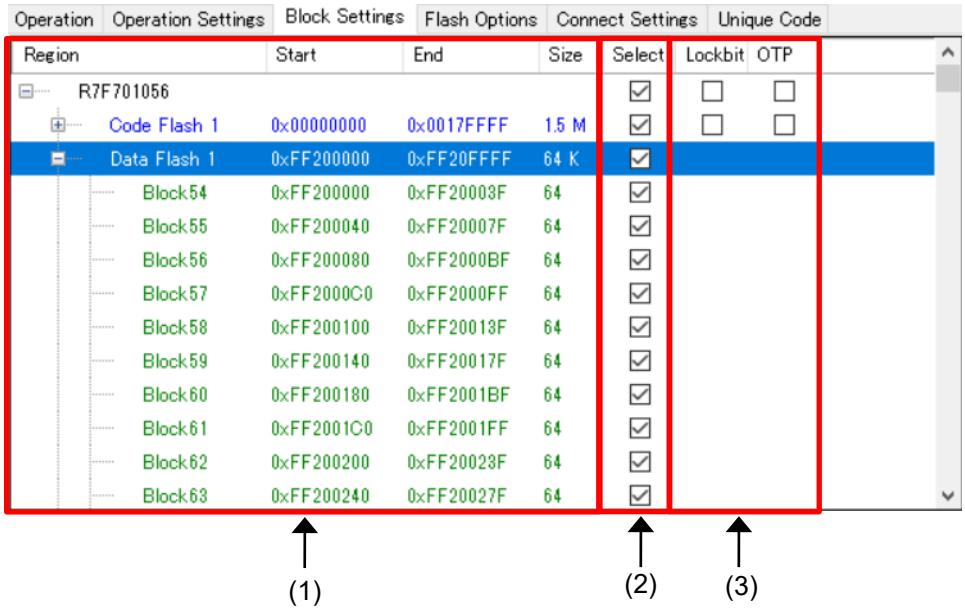


Figure 2-14 [Block Settings] Tabbed Page

(1) Information on the block areas

Information on the ranges of the block areas for the target device is shown.

Caution: Common area names and block numbers are used in the RFP; note that they may differ from those described in the manuals of the target devices.

(2) Select column

Specify blocks to be erased, programmed, or verified.

Blocks with checkboxes selected in the Select column are to be erased, programmed, or verified.

(3) Setting functions in units of blocks

Specify blocks for the setting of security or safety functions.

While “Program Flash Option” is selected, the settings are only reflected in the target device when the type of setting is enabled on the [Flash Options] tabbed page.

- Lockbit column
  Select blocks for which the lock bit is to be set.
  A lock bit is set for blocks with the checkbox selected.

- OTP column
  Select blocks to be set as OTP.
  Blocks with the checkbox selected are set as OTP.

2.3.4 [Flash Options] Tabbed Page

For individual items on the [Flash Options] tabbed page, refer to section 2.4, Features of the Flash Options.

2.3.5 [Connect Settings] Tabbed Page

The information required to connect the target device can be set on the [Connect Settings] tabbed page.

Remark: The items displayed differ according to the type of the target device.

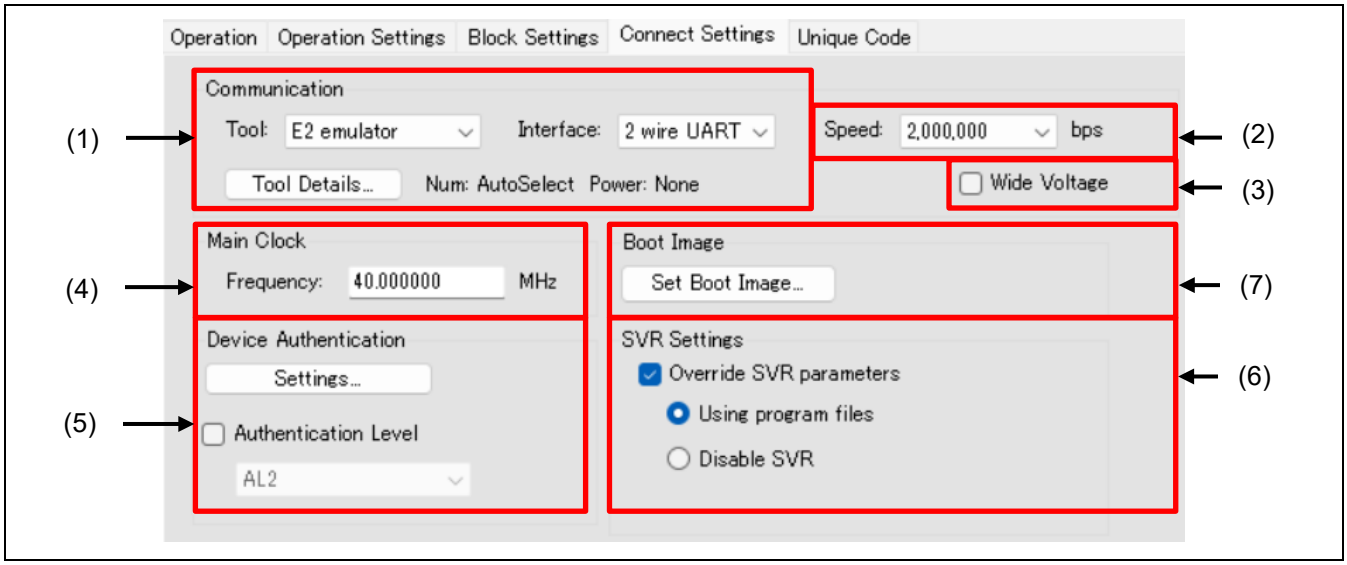


Figure 2-15 [Connect Settings] Tabbed Page

(1) Communication

Change the settings for communications.

For details, refer to section 2.2.1, [Create New Project] Dialog Box.

Remark: For the settings for communications, only options are displayed which are changeable in the current project. For example, when SWD has been selected to create a new project, changing the interface may not be possible for some connected devices. To change the settings, create a new project.

(2) Speed

Select the baud rate for use in communications with the target device.

The available baud rates differ according to the environment of the target device and the target system.

Cautions:

- The speed is only directly specifiable for a COM port connection. Since using this may lead to the RFP being unable to detect a baud-rate error, set the speed only after confirming that it will not cause a problem.
- If the target device operates at a low voltage, communications may only be possible with a relatively low baud rate (e.g., 9600 bps or 115200 bps).
- If the target device operates at a low voltage and a new project is created, the selectable baud rates will be restricted. If the target device does not operate at a low voltage, create a new project again.

Remark: The maximum rate that the E2 Lite can support is 1.5 Mbps. However, only rates which are selectable from the external clock of the target device or system are displayed for the RX Family. The baud rate which was selected for the E1, E20, or E2 emulator might not be selectable.

(3) Wide Voltage

For details, refer to section 2.2.1, [Create New Project] Dialog Box.

(4) Main Clock

Change the frequency of the input clock from that which was set when the project was created.

(5) Device Authentication

- "Settings…"
  When "Auto Authentication" is set to "Yes" in the dialog box which is displayed in response to clicking on the Settings… button, the ID code, access password, or DLM key that has been entered is used for authentication. To change the value used for automatic authentication, enter a new value.

Remark: If "Auto Authentication" is set to "No", the ID code, access password, or DLM key will not be saved in the project file.

- "Authentication Level (AL)"
  When this option is selected, authentication proceeds at the authentication level selected from the pull-down menu.

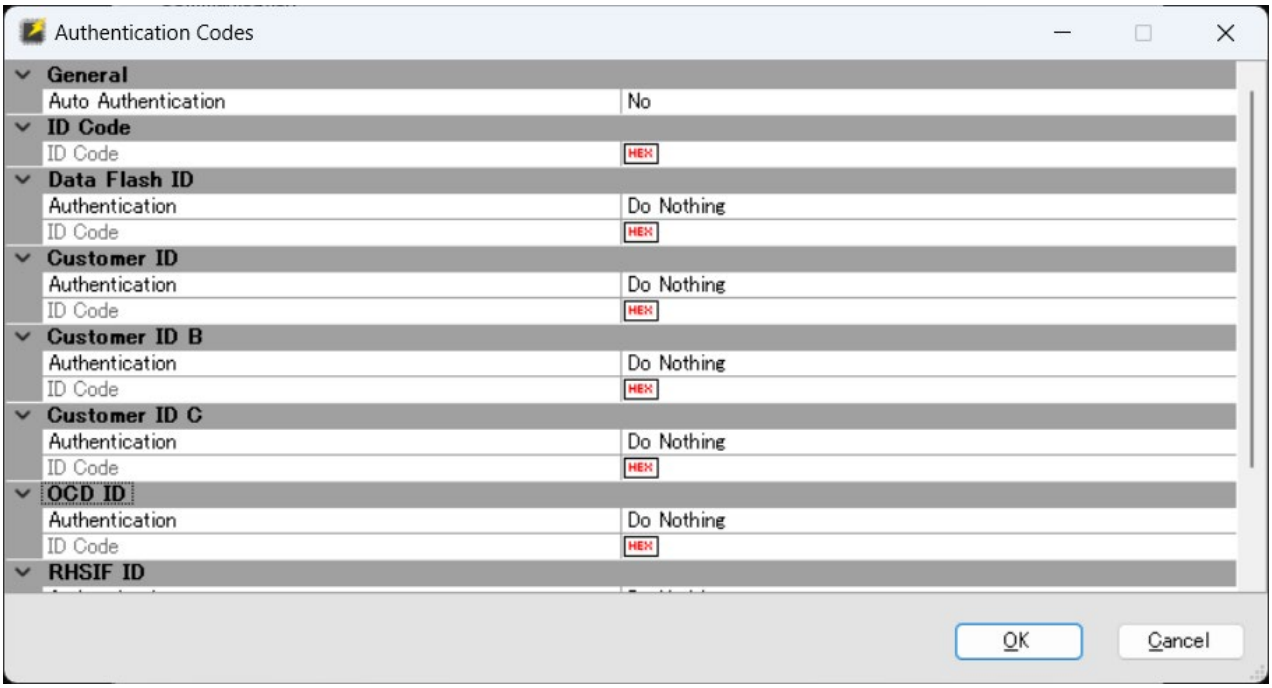


Figure 2-16 [Authentication Codes] Dialog Box

(6) SVR Settings

Make the settings to control the SVR parameters while the RFP is connected to the target device.

- "Override SVR parameters"
  - When this option is selected
    The RFP is connected to the target device after forcibly changing the SVR settings of the target device.
    - "Using program files": Parameters in the program file are used.
    - "Disable SVR": The SVR functions are disabled.
  - When this option is not selected
    The SVR parameters written to the option bytes of the target device are used.

Caution: Caution is required since the SVR settings are for the power supply. For details, refer to the manual of the target device.

(7) Boot Image

For details, refer to section 2.2.5, [Set Boot Image] Dialog Box.

2.3.6 [Unique Code] Tabbed Page

The [Unique Code] feature is for the embedding in a specified area of a unique code for the loaded program file. The feature becomes effective when a unique code and specified area are written to a unique code file, and the file name is set on the [Unique Code] tabbed page. A unique code file can contain a single specification of an area and multiple unique codes, with an index for each of the unique codes. The next index will be specified when a [Program] command ends normally; however, no index will be specified when a [Flash Option Program] command ends normally.

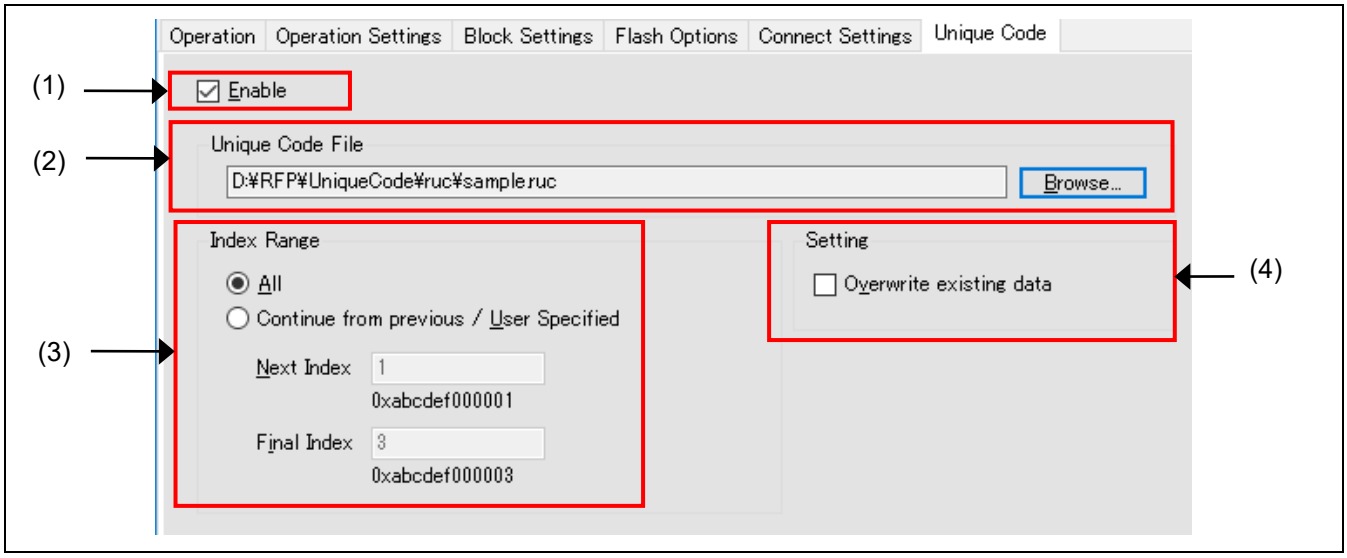


Figure 2-17 [Unique Code] Tabbed Page

(1) Enabling or Disabling the Use of Unique Codes

Usage or non-usage of the unique code feature can be set in this checkbox.

Check the box to select the use of unique codes.

(2) Unique Code File

Open the [Open] dialog box by clicking on Browse..., and specify a unique code file.

(3) Specifying a Range

Specify a range of indices in the unique code file.

- "All"
  Obtain the first and last indices from the unique code file. This starts from the first index when the RFP is rebooted.

- "Continue from previous/User Specified"
  The first and last indices are directly specifiable. Even if the RFP is rebooted, it will start from the previous point.
  - "Next Index": The next index is displayed or specified. The corresponding unique code will be shown under the box.
  - "Final Index": The last index of the range is displayed or specified. The corresponding unique code will be shown under the box.

(4) Operation Setting

- Allow the overwriting of data
  When embedding a unique code for a loaded program file, this button is used to allow or prohibit the overwriting of data if the area where the code is to be embedded already contains data (contention). Put a checkmark in the box to allow this and remove the checkmark to prohibit it.

[Remark] If the checkmark is removed, an error message is displayed and the process is cancelled, in cases of contention with existing data during embedding of the unique code.

2.3.6.1 Unique Code Files

This section describes unique code files.

(1) Filename Extension

*.ruc

(2) File Format

A unique code file is a text file. A file consists of a header and a code part. Write a list of the combinations of indices and unique codes after the header, which defines the location where the unique code is to be embedded. The only supported formats for the codes are ASCII (one byte) character codes. Unicode is not supported.

- Comment line
  Line starting with “//” are considered as comments and ignored in processing. Lines consisting only of blanks are also ignored.

- Separating characters
  Tabs, spaces, or commas can be used as separating characters in the header definitions and the settings of the indices and unique codes.

- Header part
  The header part has the following definitions that are case-insensitive.

Table 2-2 Header Definitions

Item	Definition of Unique Code
	Description
Specifying the format	format <hex | ascii>
	Specify the format of the unique codes. <hex>: Hexadecimal numerals <ascii>: ASCII characters (0x20 to 0x7e)
Specifying the address	address <address>
	Specify the address where the unique code is to start as a hexadecimal number preceded by “0” or “H”.
Specifying the size	size <size>
	Specify the size of each unique code.
	<size>: Specify a size in bytes (range: 1 to 2048)

Remark: An area specification (area) was necessary for the earlier versions. It is now ignored even if there is a statement in the file.

- Codes
  The list of unique codes consists of indices and codes, with only one code and index per line. Indices need not be prefixed by padding with“0” as in the example. They are assumed to be base-10 ordinal numbers in ascending order.

Table 2-3 Code Definitions

Item	Unique code definition
	Description
Declaration of unique codes (header of code part)	index data
	Declares that unique codes follow from the next line. This is case-insensitive.
Indices and unique codes	<index> <unique code>
	Each line specifies an index and a unique code. <index>: Specifies an index (integer in the range 0 to 2147483647) <unique code>: Specifies a unique code (big endian format, with the format and size specified in the header) If the format is ascii <unique code> A unique code can be enclosed in double quotation marks. If the code includes a space at its beginning or end, the quotation marks are required to distinguish such spaces from separating characters. If the code itself includes consecutive double quotation marks, they are handled as one double quotation mark.

- Limit on size
  The size of a unique code file should be no greater than 2 GB.

(3) Example of a File

```
//Sample unique code file

format hex

address 0xf000

size 6

index data

000001 abcdef000001

000002 abcdef000002

000003 abcdef000003
```

2.3.7 [External Memory Settings] Tabbed Page

Selecting the target board for use enables settings for the external memory mounted on the target board on the [External Memory Settings] tabbed page.

Remark: This tabbed page is only displayed if the RFP supports programming the external memory of the target device in use.

Remark: For information about the library used to control external flash memory connected to RA devices, refer to RA Familly External Flash Library for tools.

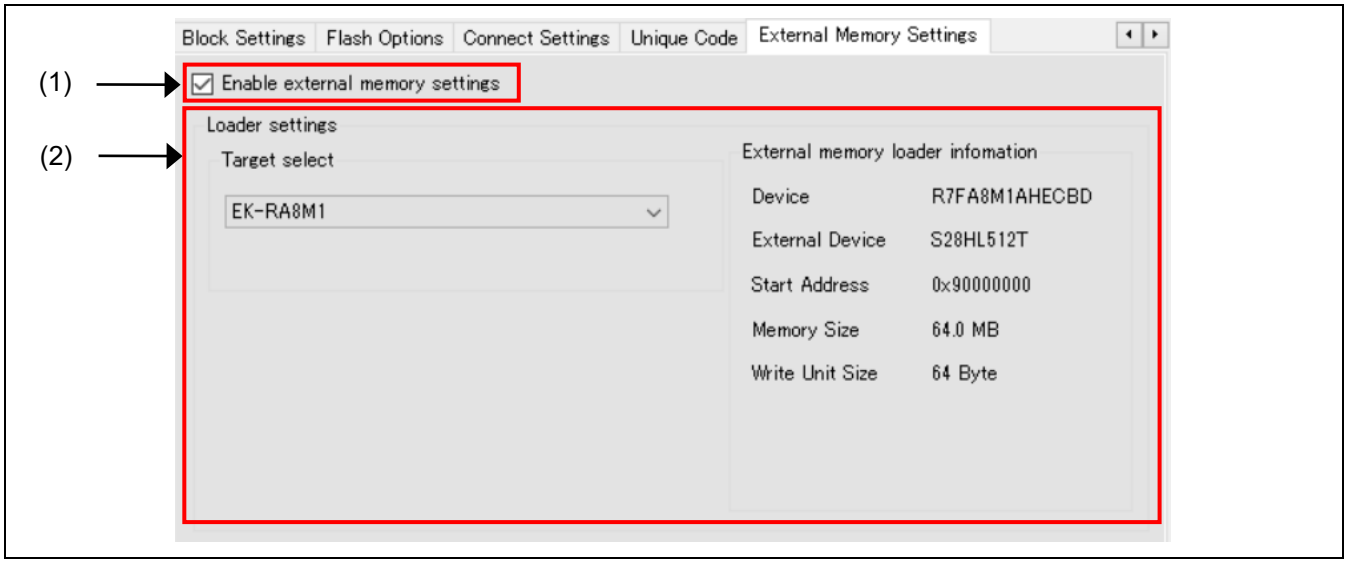


Figure 2-18 [External Memory Settings] Tabbed Page

(1) "Enable external memory settings"

Enabling or disabling the operation of external memory is set in this checkbox.

Select the checkbox to enable the operation of external memory according to the selected loader settings.

(2) "Loader settings"

Items on the settings of an external memory loader are displayed.

- "Target select"
  Select the external memory loader on the target board.
- "External memory loader information"
  This item displays information on the external memory loader specified in [Target select].

2.4 Features of the Flash Options

The flash options of the target device can be set in the [Flash Options] tabbed page.

Remark: Only those items the target device supports are shown. For the meanings and details of the settings of the individual items, refer to the manual of the target device in use.

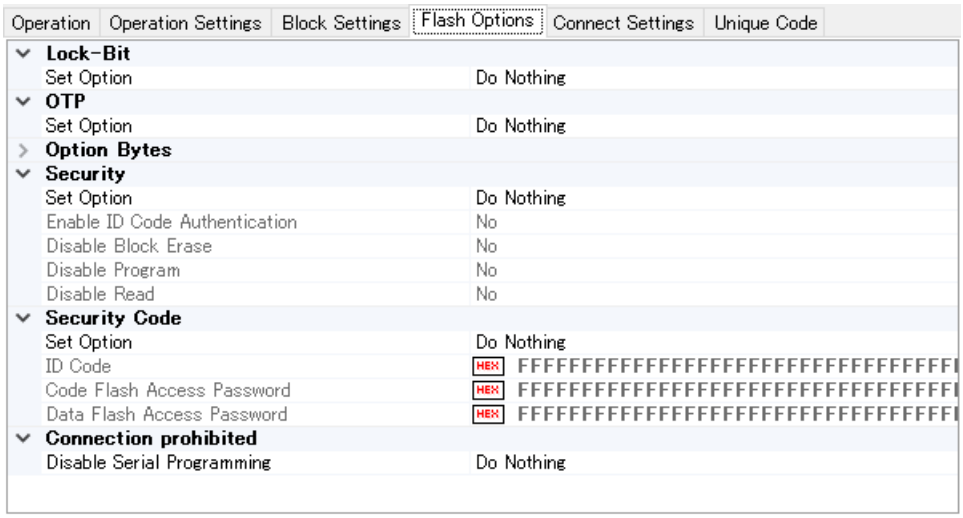


Figure 2-19 [Flash Options] Tabbed Page

2.4.1 “Set Option” (Common to Each Flash Option)

Each flash option has a "Set Option" that allows you to specify whether the setting is enabled or disabled using one of the following options.

- “Do Nothing”
  No settings are required for this item. Writing to the target device in relation to this flash option does not proceed and the current setting is not changed.
- “Set”
  The setting of this item is enabled and writing to the target device in relation to the specified setting proceeds. If “Set” is selected, specify the value to be set or file containing the setting as required.

Caution: Once certain options have been set for a target device, they cannot be reverted by the RFP. For details, refer to the descriptions of the individual items.

(1) Lock-Bit

Specify lock bits.

The blocks for which the lock bit is to be set are selected on the [Block Settings] tabbed page.

(2) OTP

Specify OTP.

The blocks to be set as OTP are selected on the [Block Settings] tabbed page.

(3) Access Window/Flash Shield Window

Specify access window.

- "Start Block/End Block"
  Select the start or end block from the pull-down menu.

- "Operation Setting"
  - "Prohibit outside the range": Programming or erasing of blocks outside the range from the start block to the end block is prohibited.
  - "Prohibit inside the range": Programming or erasing of blocks within the range from the start block to the end block is prohibited.

- "Disable Rewriting"
  - "No": Making changes within the access window is not disabled.
  - "Yes": Making changes within the access window is disabled.

(4) Option Bytes

Change the settings of option bytes.

- "Enable Extended Option Bytes"
  Select "Enable" or "Disable", respectively, to enable or disable setting of extended option bytes (OPBT8 and above) and acquisition of their values.

Caution: Since the extended option bytes contain important settings for the target device, take care with the data to be programmed if you enable this operation. Normally use this option as "disabled" unless you have a particular reason to do otherwise.

- "OPBT0~OPBT7"
  Enter the settings for option bytes in units of four bytes in hexadecimal notation (bit31....bit0).

- "OPBT8" and above
  Enter the settings for extended option bytes in units of four bytes in hexadecimal notation (bit31....bit0).

(5) ICU-S

Set ICU-S.

Caution: Once the ICU-S function is set for the target device, it cannot be reverted by the RFP.

(6) Security

Set security functions.

- "Enable ID Code Authentication"
  - "No": The ID authentication function is disabled.
  - "Yes": The ID authentication function is enabled.

- "Disable Block Erase / Disable Program / Disable Read / Disable Rewriting boot cluster / Disable Initialize Command / Disable Test Mode / Disable AL2 authentication / Disable AL1 authentication / Disable LCK_BOOT transition"
  - "No": The security function is not set for the target command.
  - "Yes": The use of the target command is prohibited.

Caution

- Once any of the functions for disabling commands has been set for a target device, some of the security settings cannot be reverted.
- To reverse the security settings for the target device, select “Erase Chip” for “Erase Options” to clear the flash options.

(7) Connection prohibited

Make the setting for disabling connection in serial programming mode or both the debugger and serial programming mode.

Caution: Once the Connection Prohibited function is set for a target device, the setting cannot be reverted.

(8) Security Code

Set the ID code or the access password.

- “ID Code”
  Enter the ID code in hexadecimal notation.
- “Code Flash Access Password”
  Enter the code flash access password in hexadecimal notation.
- “Data Flash Access Password”
  Enter the data flash access password in hexadecimal notation.

(9) DLM

Make the setting for DLM state transitions. Use this setting when a transition of the DLM state is made to suit other processing such as the writing of program files. If DLM state transitions require authentication, use the [DLM Transition] menu for the target device.

- “Target State”
  Select the destination of the DLM transition from the pull-down menu.

(10) DLM Keys

Specify the DLM key file for use in DLM authentication which is to be set for the target device.

For details on how to generate DLM keys, refer to Security Key Management Tool.

- DLM key file
  Open the [Open File] dialog box by clicking on [...], and specify a DLM key file.

Remarks: 1. If a DLM key file is not specified, programming of the flash memory will not proceed.
2. DLM key files in formats other than the Renesas Key File (.rkey) are not supported.

- “Change the storage area for AL1/AL2/RMA Key to OTP”
  — “No”: The settings for these options are not configured.
  — “Yes”: These options are to be set.

(11) Boundary

Set the size of the secure and non-secure callable areas of the target device.

- “Use Renesas Partition Data File”

— “No”: Boundaries are not to be set by using the Renesas Partition Data File.
— “Yes”: The setting of boundaries by using the Renesas Partition Data File is enabled.

- “Renesas Partition Data File”
  Open the [Open File] dialog box by clicking on [...], and specify the Renesas Partition Data File.
- “Secure Size [KB]”
  Enter the size of the secure area in KB units.
- “Non-secure callable Size [KB]”
  Enter the size of the non-secure callable area in KB units.

Note: Confirm the specifiable sizes in the manual of the target device since limits will apply.

(12) Flash Read Protection

Make the setting for flash read protection.

- “Start Block/End Block”
  Select the start or end block from the pull-down menu.

Remark: To enable reading of all blocks, select “Permitted All Blocks”.

- “Disable Rewriting”
  — “No”: Rewriting of flash read protection is not disabled.
  — “Yes”: Rewriting of flash read protection is disabled.

(13) Extra Option

Make the setting for an extra option.

- “Disable Rewriting”
  — “No”: Rewriting of an extra option is not disabled.
  — “Yes”: Rewriting of an extra option is disabled.

Caution: Once the Extra Option function is set for a target device, the setting cannot be reverted.

(14) Configuration Data Lock Bit

Make the setting for a configuration data lock bit.

- “Lock bits”: Enter the setting in hexadecimal notation.

Caution: Once the Configuration Data Lock Bit function is set for a target device, the setting cannot be reverted.

(15) Anti-Rollback Settings

Make the Anti-Rollback Settings.

- “ARCLS/ARCCS”: Enter the setting in hexadecimal notation.

Cautions:
- Once the Anti-Rollback Settings function is set for a target device, the setting cannot be reverted.

- "Anti-Rollback Settings" may be displayed for some target devices which do not support this function. For details on whether a target device has an Anti-Rollback Settings function, refer to the manual of the target device.

(16) OEM root public key

Make the setting for the OEM root public key.

- "OEM Root Public Key File x"
  Open the [Open File] dialog box by clicking on [...], and specify the OEM root public key file.

- "Disable Rewriting"
  — "No": Rewriting of an OEM root public key is not disabled.
  — "Yes": Rewriting of an OEM root public key is disabled.

Caution: "OEM root public key" may be displayed for some target devices which do not support this function. For details on whether a target device has an OEM root public function, refer to the manual of the target device.

(17) Certificate

Make the setting for a certificate.

- "Verification Method"
  Specify the authentication method.
  — "Signature": Signature mode
  — "CRC": CRC mode

- "Anti-Rollback Counter Mode"
  Specify the anti-rollback counter mode.
  — "Mode1": Anti-Rollback Counter for OEM boot loader
  — "Mode2": Anti-Rollback Counter for Secure application

- "Code Certificate / Key Certificate"
  Open the [Open File] dialog box by clicking on [...], and specify a certificate file.

(18) CPU Settings

Make the setting for the operation of the CPU.

- "Change master CPU from CPU0 to CPU1"/"Disable Security Extension for CPU1"
  — "No": The settings for these options are not configured.
  — "Yes": These options are to be set.

Caution: Once "Yes" is set for a target device, the setting cannot be reverted.

(19) Boot Cluster Size/Bank Swapping

Make the setting for the boot cluster size/bank swapping option.

Caution: When the swapping function of the target device is enabled (BTFLG = 0) and BTBLS is changed after programming of the flash memory, the result of programming may not be as expected if the swapping size is changed after the end of programming. To avoid this problem, following either of the methods below when flash memory is programmed with the swapping function enabled is recommended.

- Program the flash memory after BTBLS has been set.
- Program the flash memory after having restored all security states (including that of BTFLG) to their default values by erasing the chip.

- “Disable Rewriting BTBLS (BAPR)”
  - “Yes”: Rewriting the setting area for BTBLS is disabled (BAPR = 0).

Remark: When BTBLS is to be set, be sure to disable rewriting of the setting area for BTBLS.

(20) SiP Flash

Make the setting for the SiP flash memory.

- “Status Register”/“Protection Management Register”/: Enter the setting in hexadecimal notation.

(21) User Extra

Sets protection against accidental programming of the user extra area.

- “Enable Write protection for User Extra Area”
  - “No”: Write protection for the user extra area is disabled.
  - “Yes”: Write protection for the user extra area is enabled.

2.5 Menu Bar

2.5.1 [File] Menu

Menu items for processing related to projects can be selected.

2.5.1.1 [New Project]

Create a new project.

For details, refer to section 2.2, Creating a New Project.

2.5.1.2 [Open Project]

Open an existing project file.

2.5.1.3 [Save Project]

Save the changes to the current project.

2.5.1.4 [Save Image File]

Saves an image file (RPI file) that is a combination of a program file and flash options.

Select [Save Image File] from the [File] menu. This opens the [Save As] dialog box. Specify where the image file is to be saved.

Cautions:

- The memory ranges are in accord with those selected in the Select column on the [Block Settings] tabbed page.
- The setting of [Fill with 0xFF] on the [Operation Settings] tabbed page is applicable.
- Data which exceed the address range of the target device in use are not deleted.
- Only values which represent valid settings can be saved as flash options.

2.5.1.5 [File Checksum]

The checksum of the program file is displayed in the [Log output] panel.

Remarks:
1. For the checksum operation, use the method specified on the [Operation Settings] tabbed page.
2. Empty locations are included in the calculation as having the value 0xFF.

2.5.1.6 [Set File Password]

The password for decrypting an RPE file is encrypted and saved on the host PC.

(1) [File Password] Dialog Box (for Setting a Password)

Selecting [File] → [Set File Password] in the menu bar makes the [File Password] dialog box appear, allowing you to set the password for use in decryption. The password for decrypting an RPE file is encrypted and saved on the host PC.

Remark: You must run the RFP as an administrator to set a file password. The password cannot be set without administrator rights.

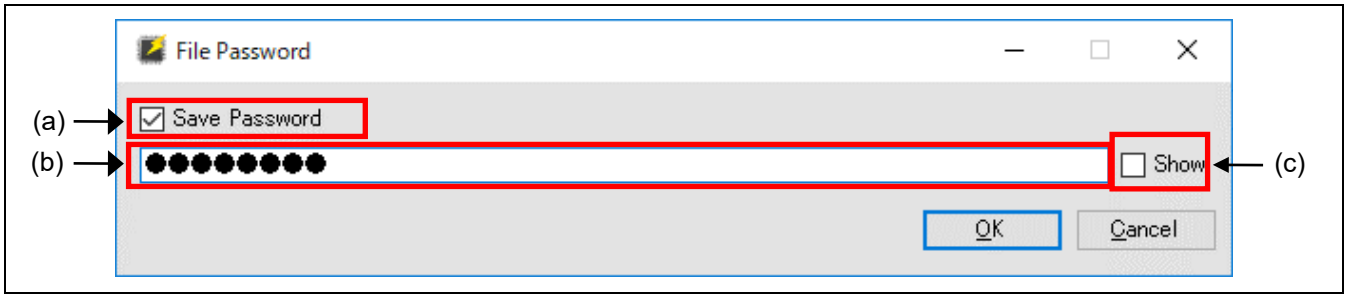


Figure 2-20 [File Password] Dialog Box (for Setting a Password)

(a) [Save Password]

- When the checkbox is selected
  The password is saved on the host PC.
- When the checkbox is deselected
  The password is deleted from the host PC.

(b) Entering a password

Enter a password made up of alphanumeric characters and symbols (up to 64 characters).

Remark: The alphanumeric characters are handled as case-sensitive; the usable symbols are as follows.

!, @, #, $, ^, &, *, (,), _, -, +, =, [,], {, }, ;, :, <, >, |, ., /, ?

(c) [Show]

When this checkbox is selected, the password being entered is shown.

(2) [File Password] Dialog Box (for Entering a Password)

When an RPE file is decrypted, the [File Password] dialog box appears to allow the entry of a password if a password has not been saved on the host PC or decryption of the file has failed.

Remark: The password that has been entered is only retained while the RFP is running.

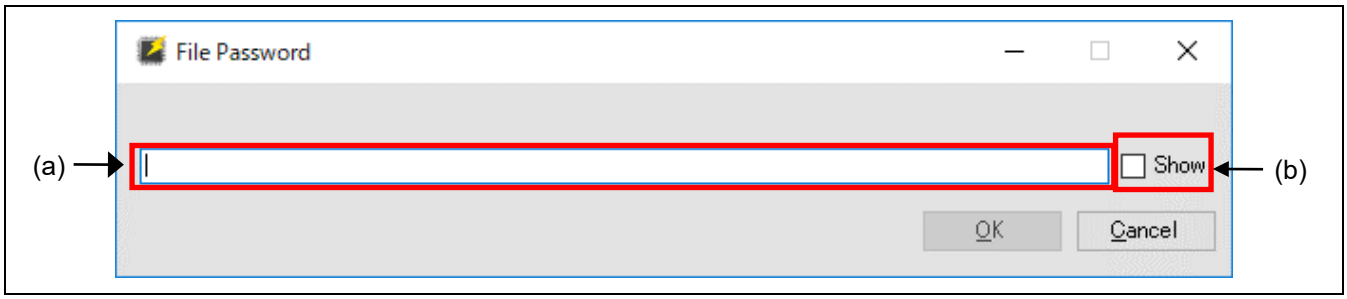


Figure 2-21 [File Password] Dialog Box (for Entering a Password)

(a) Entering a password

Enter a password made up of alphanumeric characters and symbols (up to 64 characters).

Remark: The alphanumeric characters are handled as case-sensitive; the usable symbols are as follows.

!, @, #, $, ^, &, *, (,), _, -, +, =, [,], {, }, ;, :, <, >, |, ., /, ?

(b) [Show]

When this checkbox is selected, the password being entered is shown.

2.5.1.7 [Recently used projects]

The names of project files that have recently been used are displayed. The name of the most recently used file is displayed at the top of the menu.

2.5.1.8 [Exit]

Exit the RFP.

2.5.2 [Target Device] Menu

Processing for the target device can be selected.

Caution: Selecting items from the [Target Device] menu leads to transfer to and from the target device to acquire information. Before selecting an item, check the connection between the host PC and the target device. If a connection is not found, an error will occur.

Remark: Some menu items will not be usable according to the type of the target device.

2.5.2.1 [Read Device Information]

Read information on the device while a target device is connected.

The information that has been read is displayed in the log output panel.

Remark: For the target device information that can be obtained using this function, refer to section 2.5.2.9, List of Target Device Information.

2.5.2.2 [Blank Check]

Connect the target device for blank checking.

2.5.2.3 [Initialize Device]

For a connected target device, initialize the settings for flash memory, boundaries and so on, and cause the DLM state to change to SSD or OEM_PL2.

2.5.2.4 [SWAS Recover]

Execute the SWAS Recover command in the target device. For the SWAS Recover command, refer to the Flash Boot Firmware Manual.

2.5.2.5 [Read Memory]

Connect the target device and read and save the contents of the flash areas.

When [Target Device] → [Read Memory] is selected from the menu bar, the [Save As] dialog box will appear. Specify the file and folder where the data that have been read are to be stored.

Clicking on the Save button shows the [Read Memory Information] dialog box. Specify the range of the flash area to be read.

Remark: The Motorola S format or the Intel HEX format is selectable as the file format for saving.

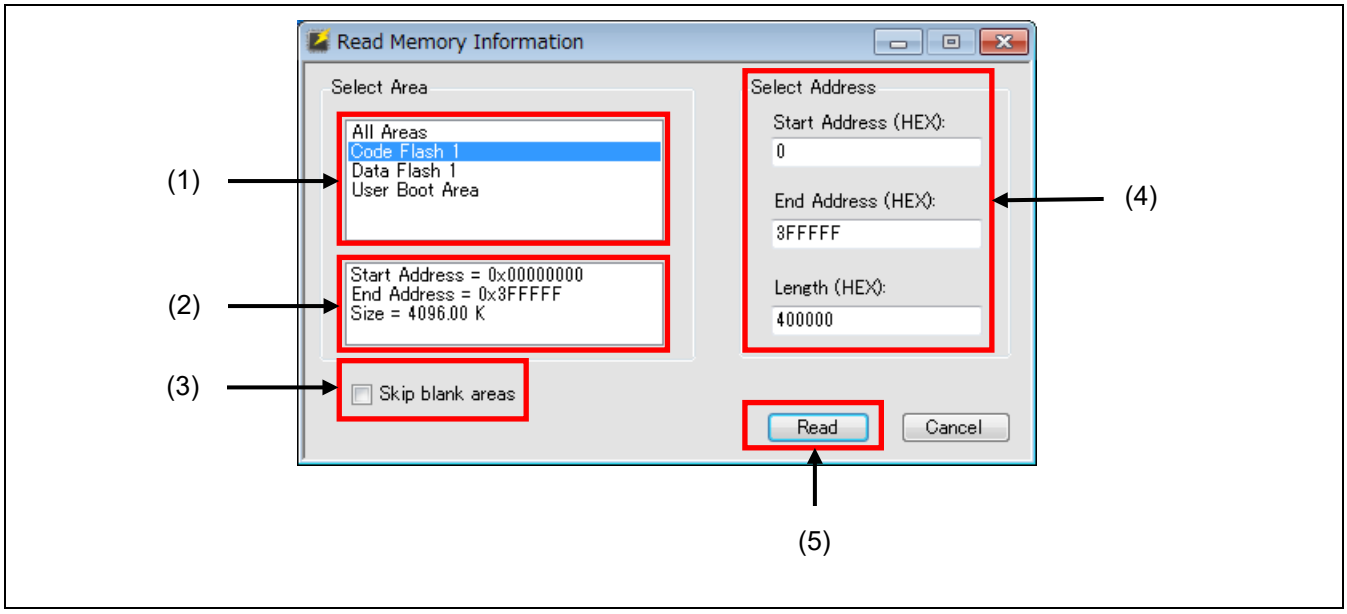


Figure 2-22 [Read Memory Information] Dialog Box

(1) Area list

Select the area to be read or all areas.

(2) Area information

Information on the area that has been selected from the list of areas or on all areas is shown.

(3) Skip blank areas

Reading of blank areas of the target device is skipped if this checkbox is selected.

Remark: The size of the area for judging whether a range is blank or not differs according to the target device. Furthermore, in some target devices, selecting this option will significantly increase time for reading.

(4) Select Address

Change items when only a specific range is to be read.

(5) Read

Connect the target device, start reading the range specified in “Select Address”, and save the data in the specified file and folder.

2.5.2.6 [Read Block Information]

Connect the target device and read the information on the blocks. The read block information can be reflected in the current project.

When [Target Device] → [Read Block Information] is selected from the menu bar, the [Read Block Information] dialog box will appear after connecting the target device, and information on blocks, including lock bits, and OTP flags, will be read. Note that the columns to be shown differ according to the type of the target device in use.

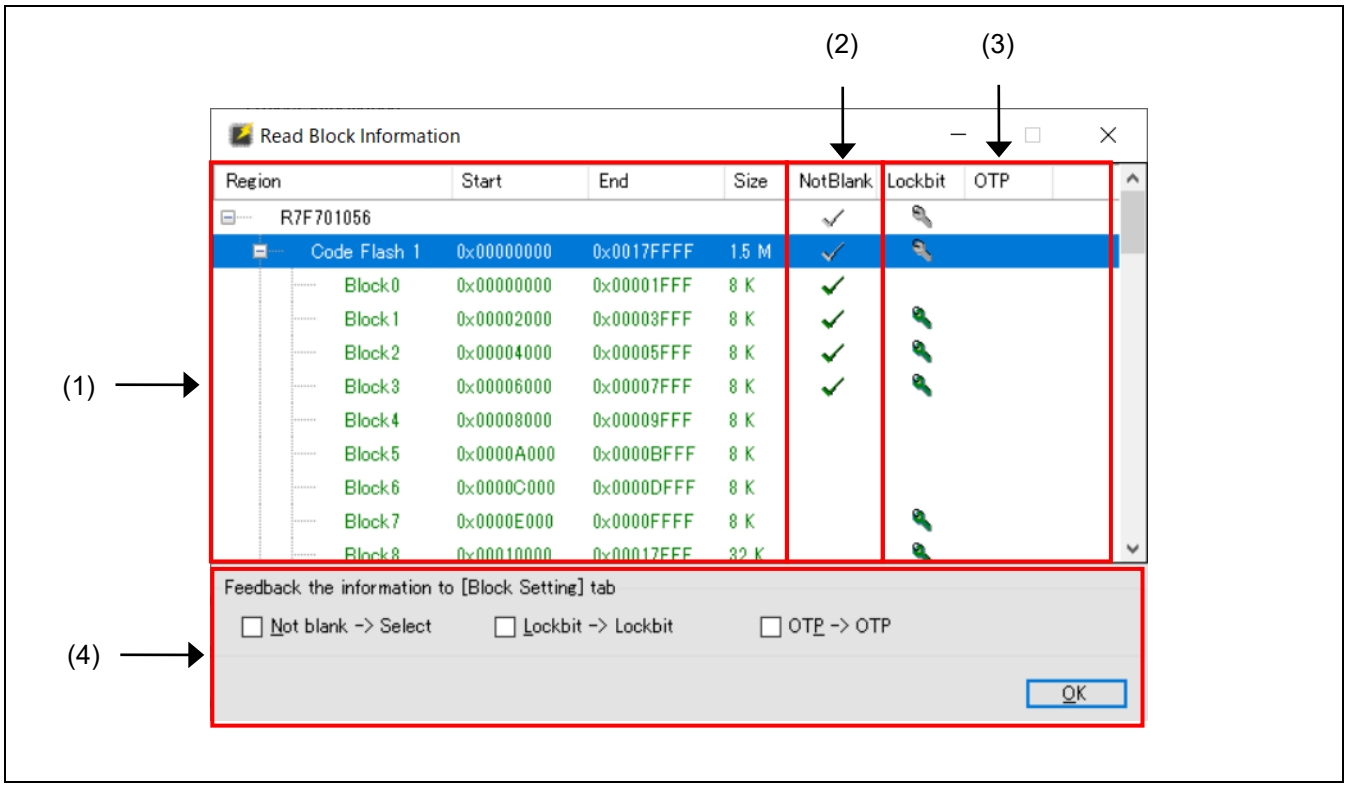


Figure 2-23 [Read Block Information] Dialog Box

(1) Information on block areas

Information on the block areas for the target device is shown.

(2) "NotBlank" Column

Information on blank blocks in the target device is shown.

Blocks with check marks are not blank.

(3) Information on options in units of blocks

Information on the target device in units of blocks is shown.

For details on each item, refer to section 2.3.3, [Block Settings] Tabbed Page.

(4) Reflecting read information

Clicking on OK reflects the read contents of the checked items in the corresponding columns of the [Block Settings] tabbed page.

2.5.2.7 [Read Flash Option]

Connect the target device and read the flash options. The read flash option information can be reflected in the current project.

When [Target Device] → [Read Flash Option] is selected from the menu bar, the [Read Flash Option] dialog box will appear after connecting the target device and information on Option Bytes and Security will be read out. Note that the items to be shown differ according to the type of the target device in use.

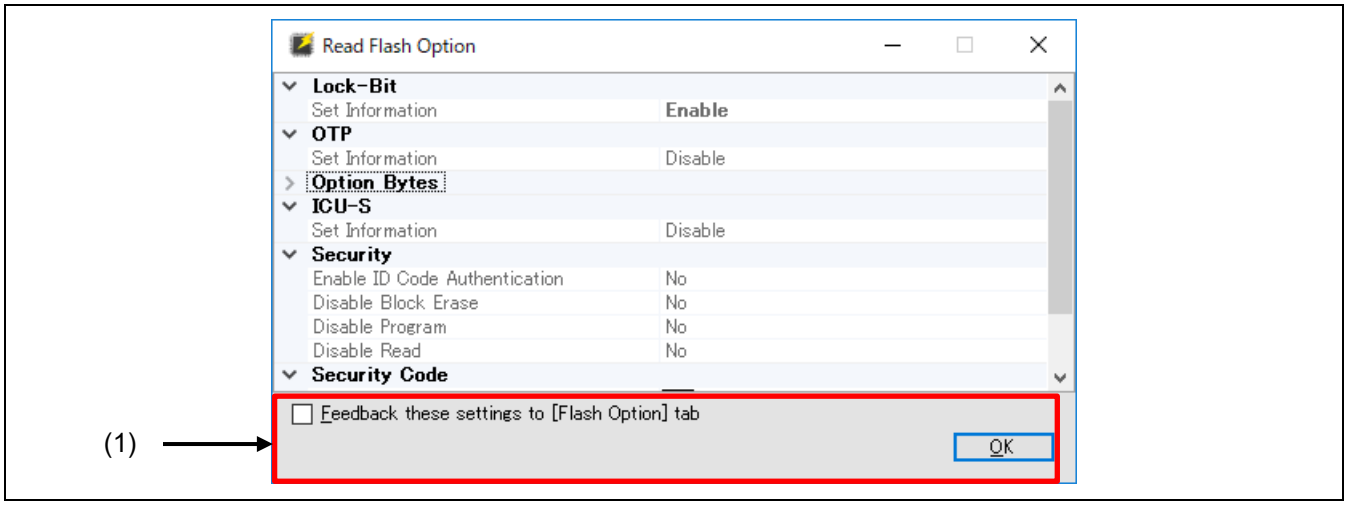


Figure 2-24 [Read Flash Option] Dialog Box

(1) Reflecting the set information

Selecting the checkbox and clicking on OK reflects the read contents on the [Flash Options] tabbed page.

2.5.2.8 [DLM Transition]

Cause a transition of a connected target device to the DLM state.

In the dialog box that is displayed by selecting [Target Device] → [DLM Transition] from the menu bar, selecting the target DLM state and clicking on Transition cause the required transition of the DLM state.

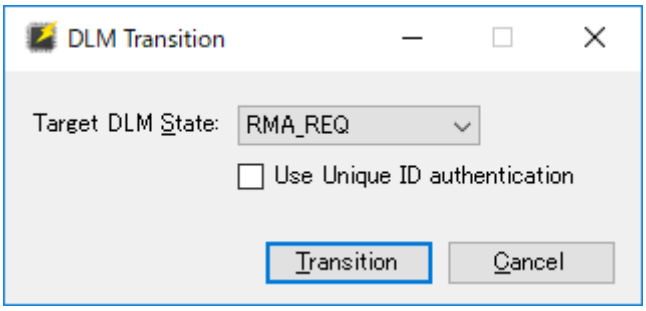


Figure 2-25 [DLM Transition] Dialog Box

- Target DLM State

Caution: Returning to a state may not be possible depending on the state of DLM for the target. For details, refer to the manual of the target device.

Remark: The current DLM state can be checked using [Target Device] → [Read Device Information].

- Use Unique ID authentication
  When this checkbox is selected, the unique ID authentication feature is enabled.

Remark: This item is only displayed when the DLM state of the target device is “RMA_REQ”.

2.5.2.9 List of Target Device Information

The following list shows the device information that can be obtained from the target device using the [Target Device] → [Read Device Information] function.

- Device Name
- Device Code
- Boot Firmware Version
- Unique ID
- DLM State
- Authentication Level
- DLM Key Injection
- OEM Root Public Key

Remark: The device information that can be obtained depends on the target device. For details, refer to the manual of the target device.

2.6 Simple Use of Project Files from a Command Line

RFPV3.exe can be run from the command line, with options prefixed by '/'.

An option may have one or more parameters; the number of parameters is determined by the option.

The name of a project file can be specified.

2.6.1 Exit Code

When the operation was successful, exit code 0 is returned.

Otherwise, 1 is returned.

2.6.2 Restriction

When command-line statements specifying the same project file are started at the same time, the same value may be written as the index of the unique code.

2.6.3 Command-line Syntax

The command-line syntax is as follows:

RFPV3.exe [Option...] [ProjectFile] [Option…]

RFPV3.Console.exe [Option...] [ProjectFile] [Option…]

The following table gives descriptions of each item.

Table 2-4 Command-line Syntax

Item	Description
RFPV3.exe	A name of a file to be executed.
RFPV3.Console.exe	A name of a file to be executed with the standard output facility. This file always starts the RFP in silent mode.
Option…	Option names prefixed by a slash (/). • Specify parameters as required. • If [Option…] is omitted, operation of the RFP is the default. • Options and parameters are not case sensitive. • Absolute or relative paths can be used for the name of the file.
ProjectFile	Specifies the name of a project file. • If this item is omitted, operation of the RFP is as follows.* When there is a project that has been recently used, that project will be opened. When no such project has been set up yet, the RFP is started without opening a project. • Absolute or relative paths can be used for the name of the file. Note: An error will occur if RFPV3.Console.exe is used.

Caution: Pathnames that include spaces must be enclosed in double-quotation marks (").

2.6.4 Start Options

The following lists start options for the RFP. If a command that cannot be used with the specified project file is specified, the E0002101 error message will be displayed.

Table 2-5 Start Options

Option	Parameter	Default	Description
silent	None	None	Starts the RFP in silent mode. After the specified project file is opened and processing which is equivalent to execution in response to pressing the [Start] button once is done, the RFP is closed. If the device requires ID authentication, automatic ID authentication is performed. When no project file is specified, this option is ignored. • Silent mode In this mode, the GUI, progress bars, and dialog boxes are not displayed.
log	File Path	None	Saves a log in a file. If the specified file already exists, the log is appended to the contents of the file. Encoding in saving of the log depends on the encoding option.
encoding	Encode	UTF8	Specifies the character encoding for the log file. If a parameter other than UTF8 or ASCII is specified for Encode, an error will occur.
force	None	None	A facility for interlinking with the CS+ integrated development environment from Renesas. • When a project file is specified, the project file is loaded and the RFP is started. • When no project file is specified, the specified path is used and the dialog box for creating a new project is opened. Note that this option is ignored both in silent mode and when no project file is specified.
lang	jp/en	Automatically selected by default	Specifies the language for display of the RFP. • jp: Japanese • en: English

The following options for the command can only be specified in silent mode.

Table 2-6 Start Options Specific to Silent Mode (1/2)

Option	Parameter	Default	Description
file	File Path	Setting in the project	Used to specify one or more program files. Flash memory in the target device is programmed by replacing the program file specified as the parameter with the program file in the project file. Refer to the caution in section 2.3.1.1.
bin	Address File Path	None	Used to specify one or more binary files. If the addresses of the data files for programming are overlapped, no error occurs and the data files are overwritten in the order of execution of the commands.
tool	SerialNo	Setting in the project	Selects the tool specified in the project. • SerialNo: (1) Emulator*1 Serial No. on the body e.g. “7AS000400A” (2) COM port*1 “COMx” (3) USB Direct*1 USB instance path*2 e.g. "VID_045B&PID_0025¥6&3234B9D9&0&3" Notes: *1: Select the tool in the project file in advance. It cannot be changed from the command line. *2: The USB instance path must be enclosed in double-quotation marks (”).
auth	IDType:IDCode	Setting in the project	Specifies the ID code for use in authentication. One or more auth options can be specified. • IDType: Specifies the character string that identifies each ID code. If a parameter other than id, cfpw, dfpw, seckey, nonseckey, rmakey, al2key, al1key, oid, cid, cida, cidb, cidc, ctid, sifid, or dfid is specified, an error will occur. • IDCode: Specifies the ID code for use in authentication as a hexadecimal number.
blankcheck	blank/notblank	None	Performs blank checking. Note that this command is executed first and an error occurs if the device does not support it. • Specifying blank: Execution of the command is only successful when the flash memory in the device is blank. • Specifying notblank: Execution of the command is only successful when the flash memory in the device is not blank.

Option	Parameter	Default	Description
userkey	Address File Path	Setting in the project	Used to specify one or more user key files. Flash memory in the target device is programmed by replacing the user key file specified as the parameter with the user key file in the project file. If the addresses of the user key files are overlapped, an error occurs.

Table 2-7 Start Options Specific to Silent Mode (2/2)

Caution

- Only one of the following options can be specified.
- If any of the following options is specified, processing which is equivalent to execution in response to pressing the [Start] button will not proceed.

Remark: The read, read32, write32, and writebit options are not supported for devices of the RL78 Family.

Option	Parameter	Default	Description
read	Format Address Size File Path	None	Reads memory of the device. • Format: Select one of the following formats for saving data in the file: — srec: S-record — hex: Intel hex — bin: Binary file • Address: Specify the start address as a hexadecimal number. • Size: Specify the size for acquisition as a decimal number. • File Path: Specify the name of the destination file for saving.
read32	Address Size	None	Reads memory of the device in 32-bit units and saves the result in a log. The endianness is specified by the settings for the project. If the endianness is not specified for the project, little endian will be used. • Address: Specify the start address as a hexadecimal number. • Size: Specify the size for acquisition as a decimal number (multiples of 4 up to 1024 are specifiable).
write32	Address Data…	None	Writes data to the device in 32-bit units. The endianness is specified by the settings for the project. If the endianness is not specified for the project, little endian will be used. • Address: Specify the start address as a hexadecimal number. • Data…: Specify the 4-byte data to be written in hexadecimal. When multiple data are to be specified, separate them with spaces (up to 64 units of 4-byte data are specifiable).

writebit	Address BitPos BitData	None	Writes data to the device in 1-bit units. The endianness is specified by the settings for the project. If the endianness is not specified for the project, little endian will be used. • Address: Specify the start address as a hexadecimal number. • BitPos: Specify the start bit number (0 to 31). For 4-byte data, the most significant bit is 31 and the least significant bit is 0. • BitData: Specify the data to be written in binary. Write the bit data in descending order from the specified bit number to the least significant bit (up to 32 characters are specifiable).
Command	Command	Setting in the project	Specifies processing to be executed. This depends on the settings in the project. When the read option is specified, the command option is ignored. Select the commands to be executed from among the following. Some commands can be specified in combination but their order is ignored. • Commands e: Erase p: Program* v: Verify o: Program Flash Options* y: Verify Flash Options s: Checksum e.g. /command epv Note: When the selected file is an HCUHEX file, RPI file, or RPE file generated by encrypting an HCUHEX file or RPI file, *p* forcibly includes *o*. Executing *o* on its own is not possible.
dlm	State	None	Causes a transition of the DLM state. Refer to the cautionary note in section 2.5.2.8. • State: SSD, NSECSD, DPL, LCK_DBG, LCK_BOOT, RMA_REQ, OEM_PL2, OEM_PL1, or OEM_PL0
initialize	None	None	Initializes the device.

2.6.5 Example of Command-line Statements

The following is an example of command-line statements in a batch file.

- Example of a whole file
  RFPV3.exe /silent "d:\rfp\project\sample.rpj" /file "d:\rfp\hex\sample_1.hex" /file "d:\rfp\hex\sample_2.hex" /log "d:\rfp\log\sample.log"
  ECHO Result Code: %ErrorLevel%
  PAUSE

- Example of the [write32] option
  The following command writes 0x01020304 and 0x05060708 to addresses 0xFF200000 and 0xFF200004, respectively.
  RFPV3.exe /silent "d:\rfp\project\sample.rpj" /write32 FF200000 01020304 05060708

- Example of the [writebit] option
  The following command writes 0xAAAA to the 16 lower-order bits (bits 15 to 0) of address 0xFF200000.
  RFPV3.exe /silent "d:\rfp\project\sample.rpj" /writebit FF200000 15 1010101010101010

2.7 Command Line for Windows, Linux, or macOS

Programming can be controlled from the command line alone without the use of project files.

Regarding the usage of the command line, refer to the separate guide in the directory where the RFP has been installed: “docs*.md”.

rfp-cli.md: Guide for the command line

rpe.md: Guide for the encryption utility program

2.8 Encryption Utility Program

rpe.exe, which is bundled with this product, can be used to encrypt or decrypt program files.

Remarks: 1. rpe.exe is stored in the same location as that for RFPV3.exe in the folder where the RFP has been installed.
2. The Advanced Encryption Standard (AES) with a 128-bit block length is used for encryption.

Caution: In this utility program, encryption is not for protecting communications between the tool and the target device but for protecting program files.

2.8.1 Exit Code

When the operation was successful, exit code 0 is returned.

Otherwise, 1 is returned.

2.8.2 Command-line Syntax

The command-line syntax is as follows:

rpe <file> /password <password> [options...]

2.8.3 Start Options

The following lists start options for the encryption utility program.

Table 2-8 Start Options

Option	Description
file	Specifies the file to be input (this specification is mandatory). • The file can be specified as a relative path from the working directory. • Files to be encrypted: Intel Hex, S-Record, HCUHEX, and RPI • Files to be decrypted: RPE
password	Specifies the password for use in encrypting or decrypting the file (this specification is mandatory). If the password includes symbols, enclose each in double-quotation marks (”).
decrypt	Decrypts an encrypted file (RPE). If this option is not specified, the file is encrypted.
output	Specifies the destination for output of a file. If this option is not specified, the directory holding the input files is used. • The file can be specified as a relative path from the working directory.
nooverwrite	Prohibits overwriting of output files.
?	Displays help information on the options.

Caution: Pathnames that include spaces must be enclosed in double-quotation marks (”).

Remark: Enter a password made up of alphanumeric characters and symbols (up to 64 characters). The usable symbols are as follows.
!, @, #, $, ^, &, *, (,), _, -, +, =, [,], {, }, ;, :, <, >, |, ., /, ?

Example:

```
> rpe "out.hex" /password "0123456789"
```

```
> rpe "out.hex" /password "0123456789" /output "out.rpe"

> rpe "out.rpe" /decrypt /password "0123456789" /output "D:\outputdir\"
```

2.9 Renesas Flash Programmer Utility Program

The Renesas Flash Programmer utility program, rfp-util.exe, which had been bundled with this product from RFP V3.11, has been discontinued. Use the Security Key Management Tool as the successor software.

3. Operating the RFP

This chapter describes the basic operation of the RFP (the flow until a file is programmed) so that the user understands the series of basic operations using the RFP from activation of the system to programming of the target device.

The operations of creating, erasing, programming, and verifying a new project file are explained here. The conditions for the series of operations used in the examples are as follows.

- Target device: R5F104PJ (RL78/G14)
- Tool used: E1 emulator
- Connection method: 1-wire UART (single-wire UART)
- Communications speed: 1,000,000 bps
- Clock supply: No external clock (internal clock oscillator)
- Power supply: E1 (5.0 V, from USB VBUS)
- Flash options: Not used

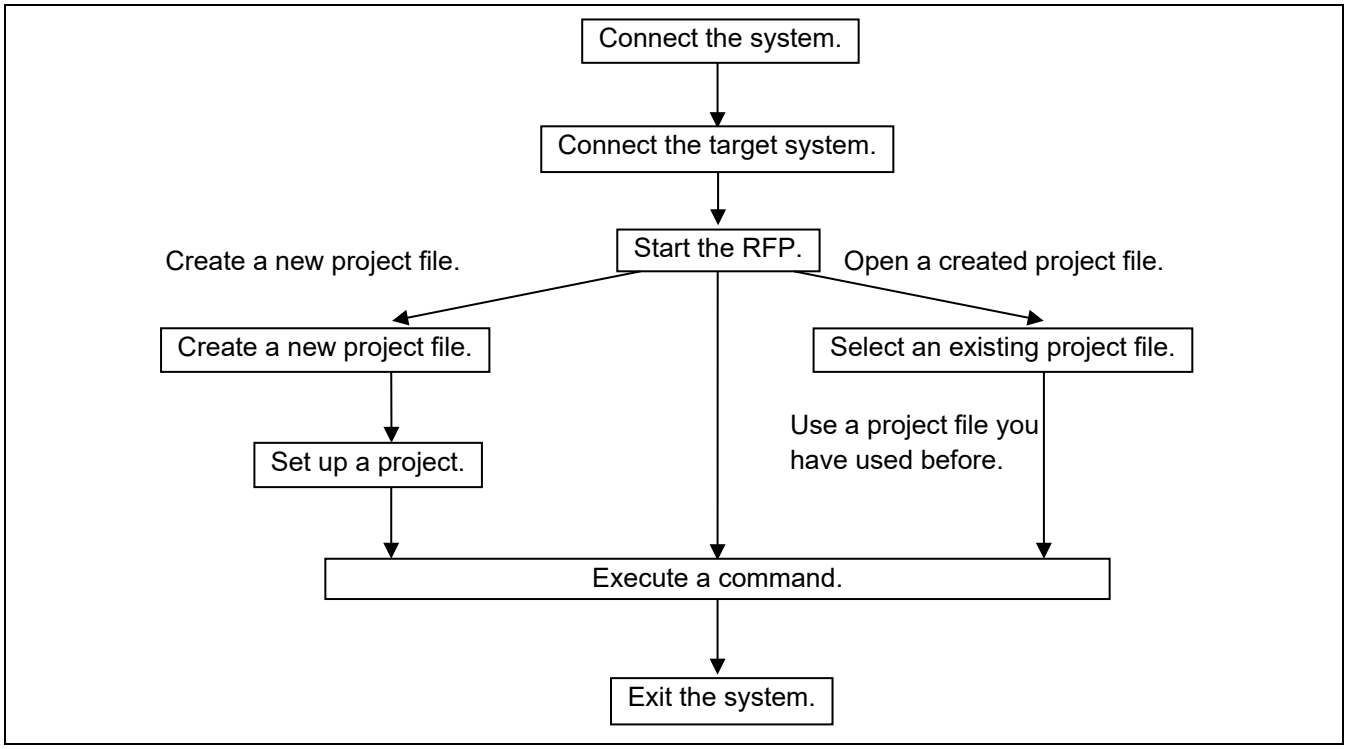


Figure 3-1 Flow of Operations

3.1 Flow of Operations

(1) Connecting the system

Connect the USB port of the host PC to the tool you will be using via the USB cable.

(2) Connecting the target system

Connect the target cable of the tool to the target system.

Caution: If power is to be supplied on the target system, be sure to connect the tool in use to the target system before switching the power on.

(3) Creating a project file

(1) When the RFP is started, the main window opens.
When [File] → [Create a new project] is selected from the menu bar, the [Create New Project] dialog box will appear.

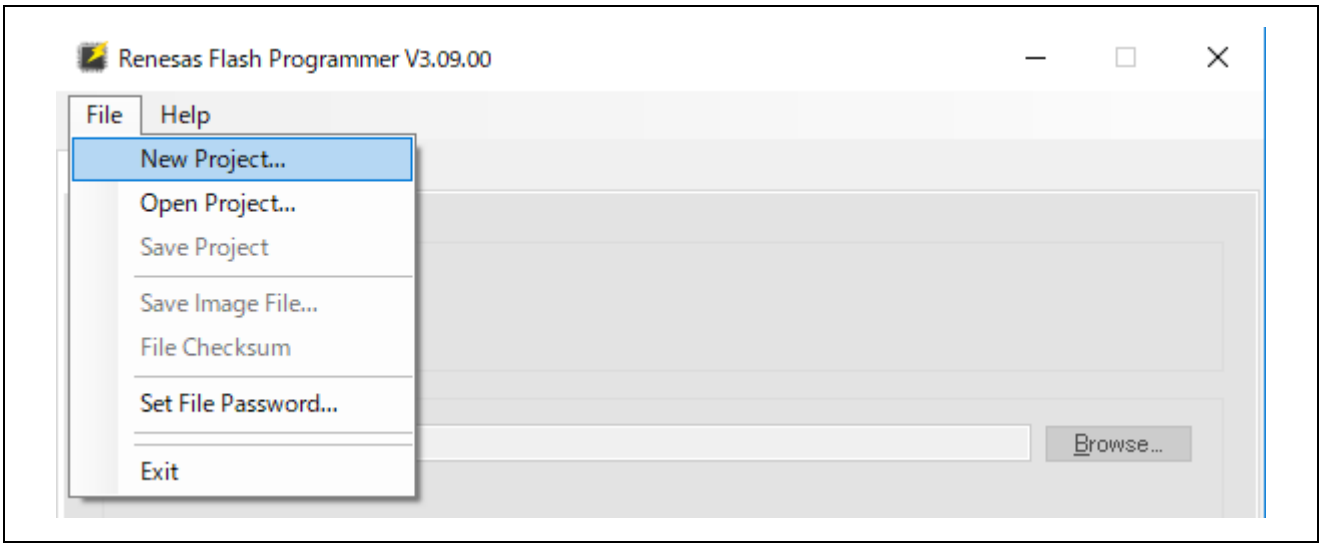


Figure 3-2 File Menu

(2) Select “RL78” for [Microcontroller].
Enter any project name (in this example, “sample”) for [Project Name] and specify any folder (e.g. D:\rfp\sample) for [Project Folder].
Select “E1” for [Tool]. For the RL78 Family, [Interface] is fixed to “1 wire UART”.
Clicking on the Tool Details… button opens the [Tool Details] dialog box.

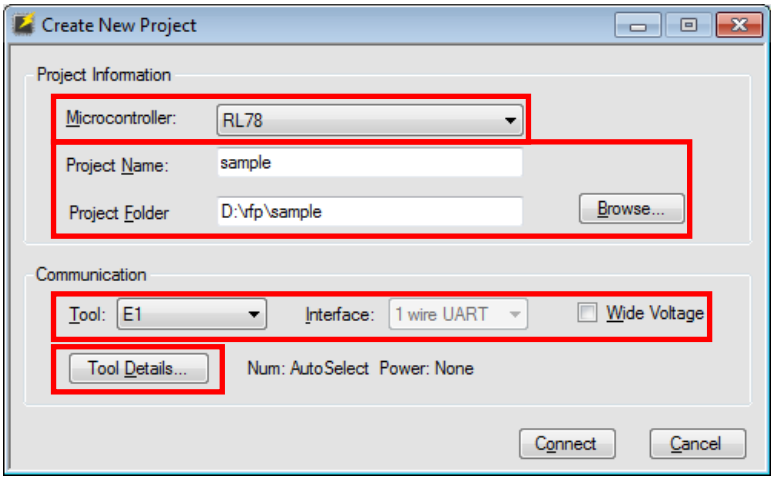


Figure 3-3 [Create New Project] Dialog Box

(3) Select the [Select Tool] tabbed page and the [Auto Select] checkbox.
After that, select “5.0V (USB VBUS)” in [Power Supply].
Click on OK.

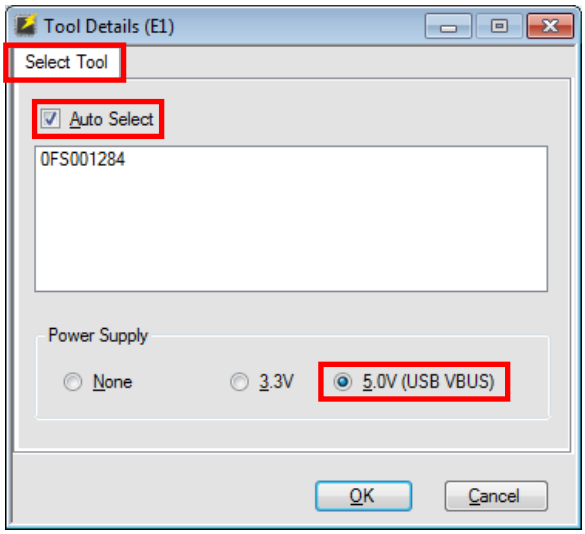


Figure 3-4 [Select Tool] Tabbed Page

(4) Information on the specified tool is displayed.
Check the contents (in this example, “Num: AutoSelect Power: 5.0V (USB VBUS)”) and click on Connect.
A project is created and the Main Window is shown.

Caution: Clicking on Connect starts the connection to the target device.

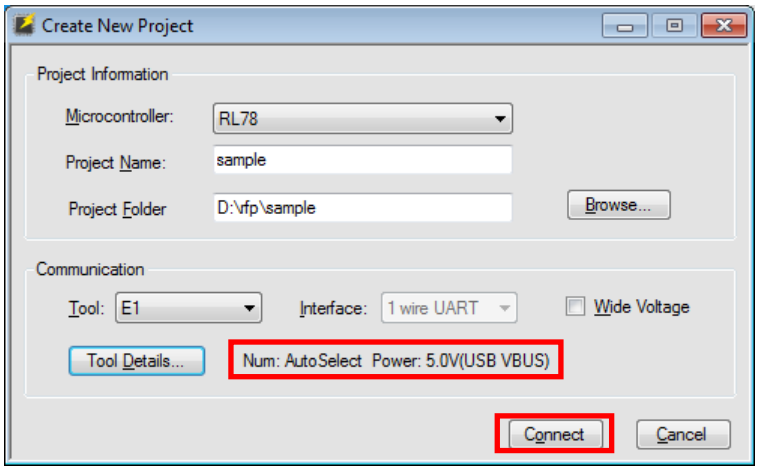


Figure 3-5 [Create New Project] Dialog Box

(5) When a project is created, the display of the main window changes with the addition of new tabbed pages. Check the information displayed in Project Information.

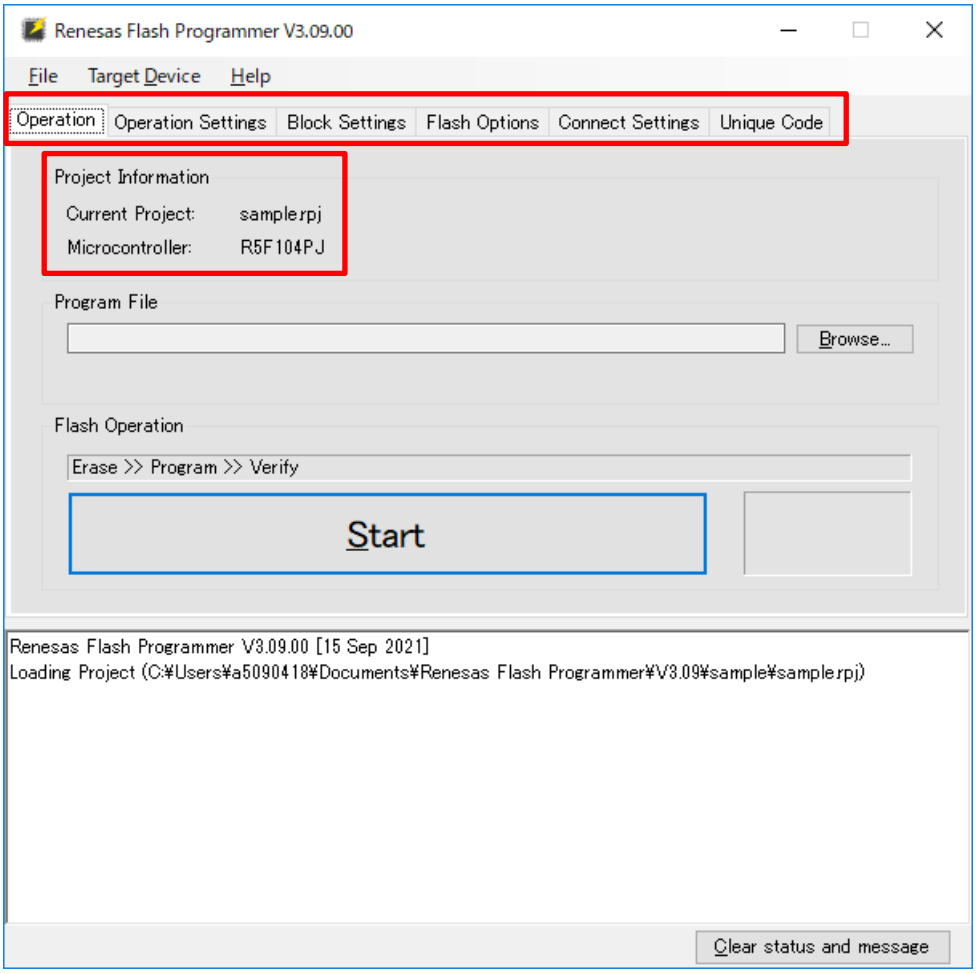


Figure 3-6 Main Window

(4) Detailed settings of the RFP

Operate the tabbed windows to make detailed settings of the RFP.

(1) Set the [Operation Settings] tabbed page.
Refer to “Command” and check that the “Erase”, “Program”, and “Verify” checkboxes have been selected, then click on the [Block Settings] tabbed page.

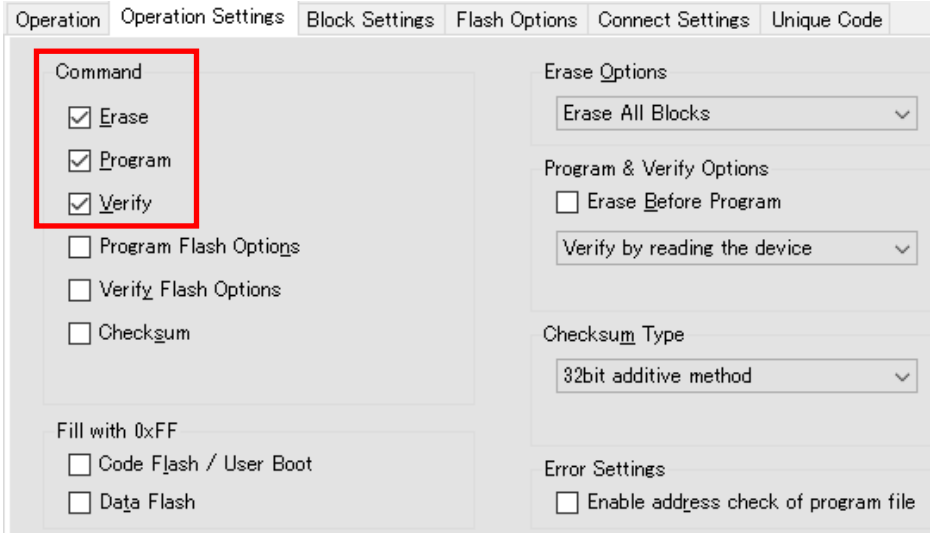


Figure 3-7 [Operation Settings] Tabbed Page

(2) Set the [Block Settings] tabbed page.
Check that all checkboxes in the “Select” column have been selected.
Then click on the [Connect Settings] tabbed page.

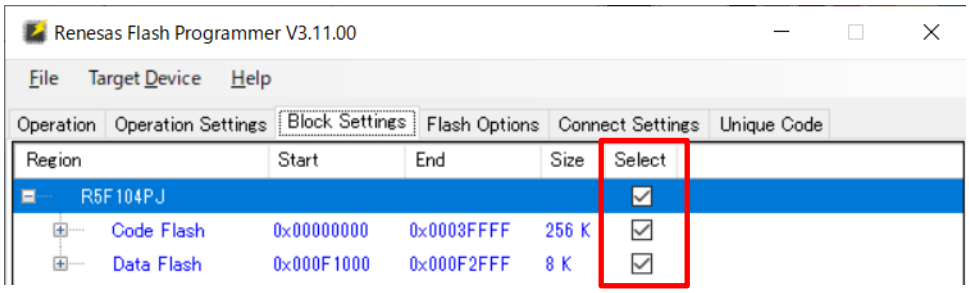


Figure 3-8 [Block Settings] Tabbed Page

(3) Set the [Connect Settings] tabbed page.
Specify 1,000,000 bps for “Speed”, then click on the [Operation] tab.

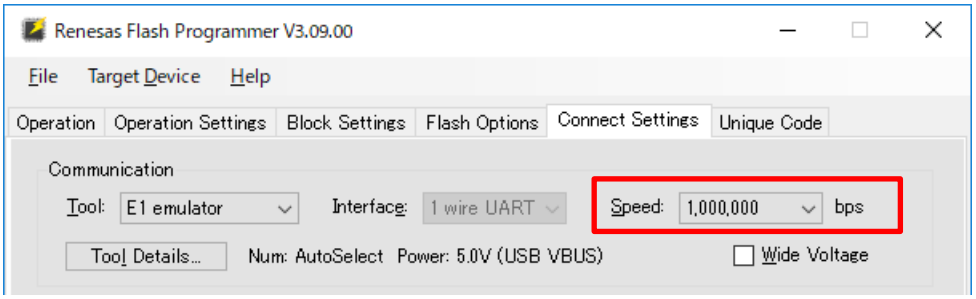


Figure 3-9 [Connect Settings] Tabbed Page

(4) Check that the commands above Start are displayed as “Erase >> Program >> Verify”.

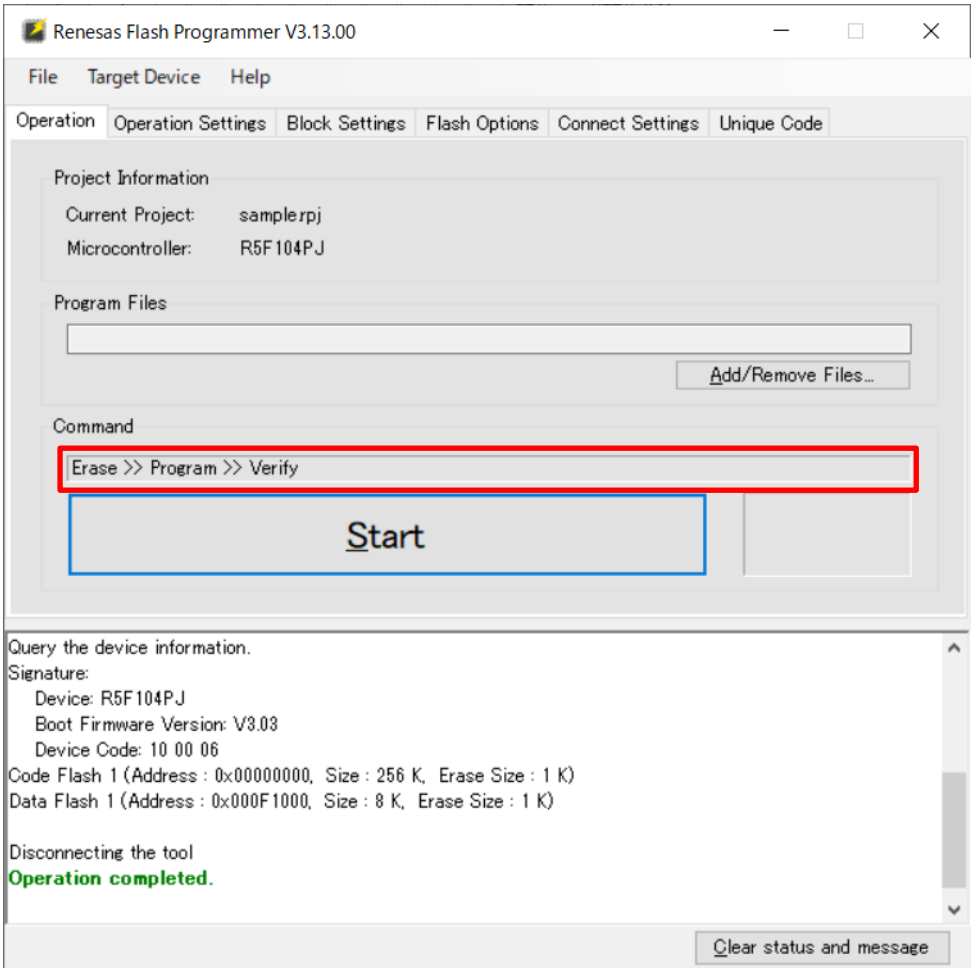


Figure 3-10 Main Window

(5) Selecting a program file

Click on Browse… in “Program File” on the [Operation] tabbed page and select a program file from among those displayed in the dialog box (in this example, “C:\RFP_ProgramFile\sample.mot”).

Check that the path to the program file selected in the “Program File” box is indicated.

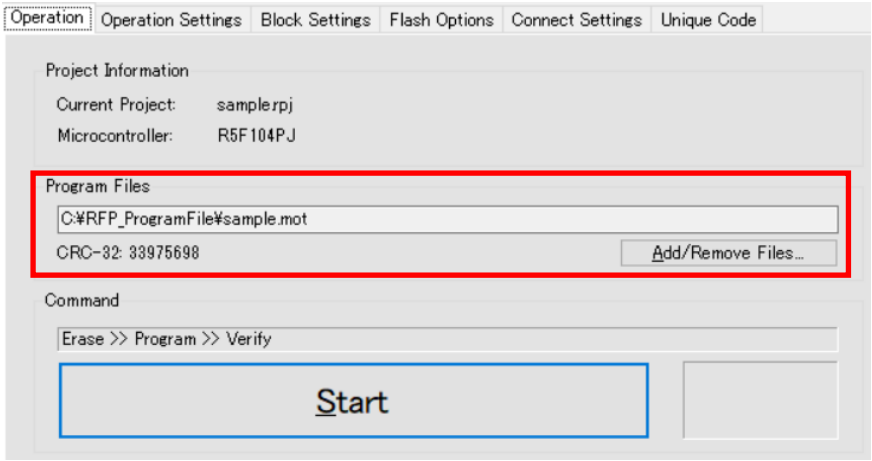


Figure 3-11 [Operation] Tabbed Page

(6) Executing a command

(1) Click on Start to execute the commands indicated above Start.
When sending of the commands is started, the [Progress Report] dialog box will appear.

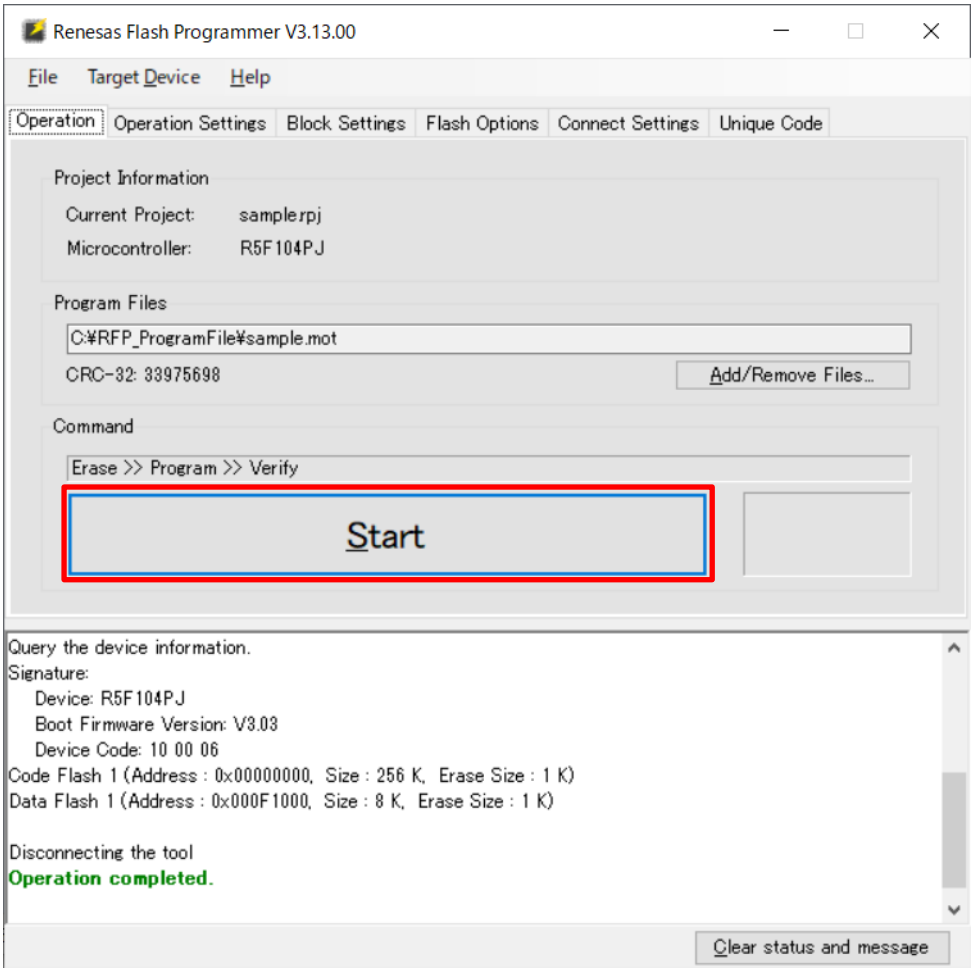


Figure 3-12 Main Window

(2) The [Progress Report] dialog box shows the state of command execution.

The state information is changed to “Run” and details of the processing are output as a log in the log output panel of the main window.

When command execution is completed, the [Progress Report] dialog box is automatically closed and the main window is displayed.

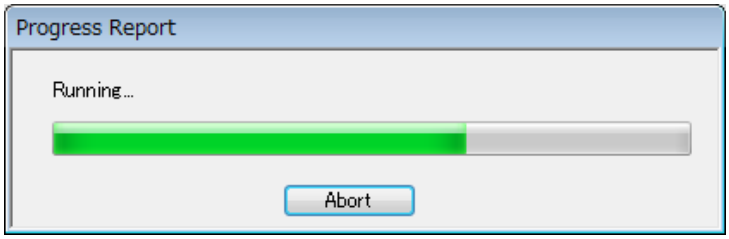


Figure 3-13 [Progress Report] Dialog Box

(3) When command processing is completed normally, the message “Operation completed.” is displayed in the log output panel and the state information is displayed as “OK”.

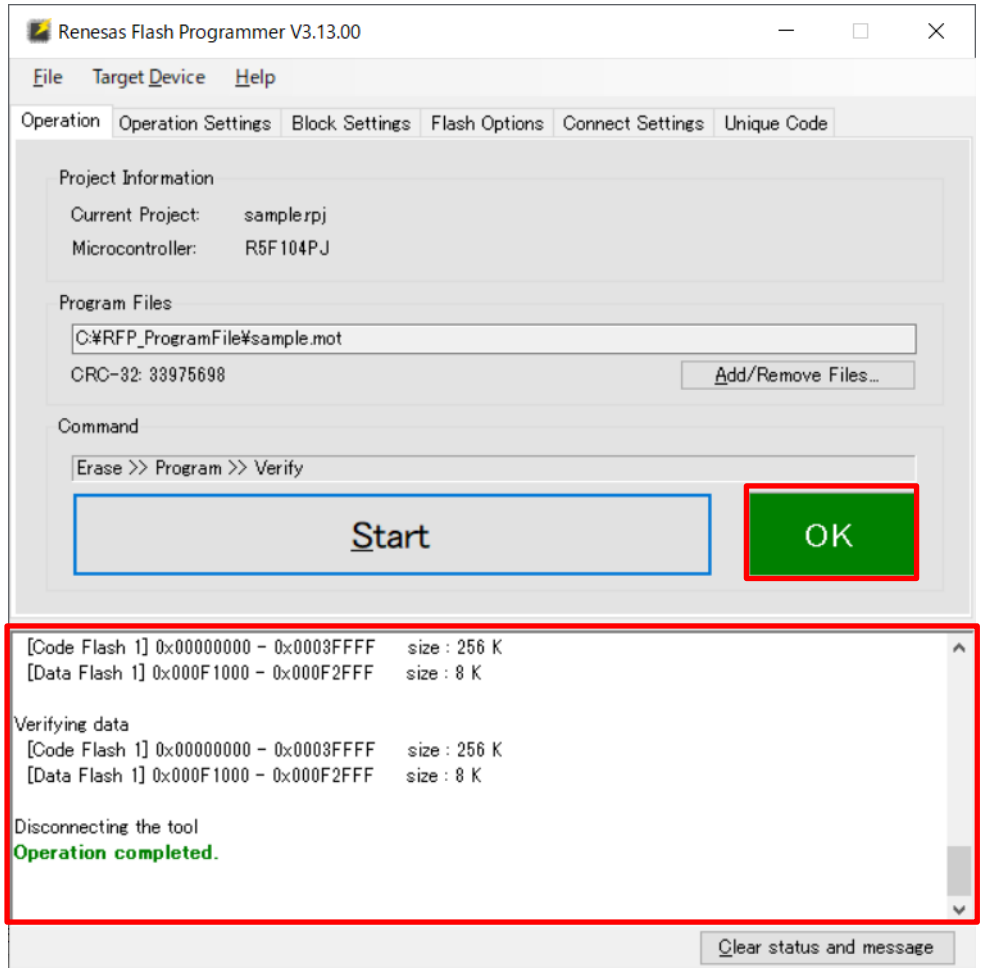


Figure 3-14 Main Window

(7) Exiting the system

(1) Remove the target cable of the tool in use from the target system.

Caution: If VDD is being supplied on the target system, turn off the supply power before removing the target cable of the tool in use from the target system.

(2) If you do not need to program another target device, select [File] → [Exit] and exit the RFP. Since all settings that you have made are saved in the project file, they can be reused when the RFP is restarted.
When you intend to continue to program other target devices, connect the target system (step (2)) and execute the required commands (step (6)).

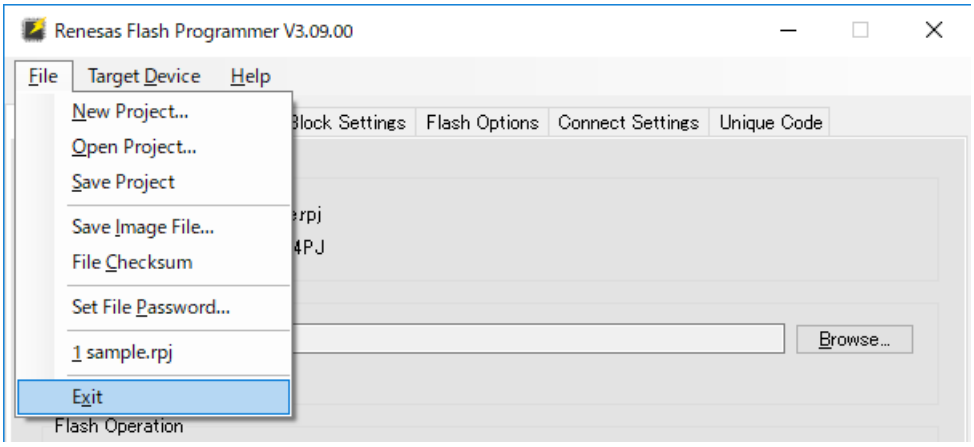


Figure 3-15 Main Window

(3) Remove the USB cable from the tool.

4. Troubleshooting

This chapter explains how to troubleshoot the RFP.

Remark If an error occurs during the sequence of a procedure, refer to this chapter and the manual of the target device. Also refer to the manual of the tool you are using and execute diagnostic tests. If this still does not resolve the problem, refer to the FAQ (https://www.renesas.com/rfp/faq-en). If you need technical support, contact Renesas via the Renesas Web site (http://www.renesas.com/contact) after writing down the PID number printed on the Renesas Development Tool License Certificate for the RFP.

4.1 Problems during Startup

This section explains how to troubleshoot problems that might occur in the processes from installation to startup.

(1) When the tool is connected to the host PC via a USB interface, plug and play does not recognize the driver.

Cause:

The USB connector might not be inserted properly into the USB port of the host PC.

Action:

Check that the USB connector is fully inserted into the USB port of the host PC. Alternatively, disconnect the USB connector, and then insert the USB connector again after a while.

(2) The tool is connected to the host PC but the power LED on the tool is not turned on.

Cause:

The USB port of the tool or the host PC might be defective.

Action:

Check the tool for defects by using the diagnostic tool for the tool in use. If you find a defect, consider repairs. If there is no defect, try connecting the tool to another host PC.

4.2 Problems during Operation

This section describes troubleshooting for problems that may occur during operation.

(1) When an error produces the message 'E3000105 There is no response from the device.'

Cause 1:

The connection with the target system might be wrong.

Action 1:

(1) Check that the connection with the target system is in accord with the recommended circuits shown in the manual of the tool in use. Also check that all required pins of the tool have been connected.
(2) For the RL78 Family, check that the EMVDD pins of the E1, E20, E2, or E2 Lite have been correctly connected.

Cause 2:

The operating mode of the target device might be wrong.

Action 2:

(1) Refer to the manual of the target device and check that all required mode pins are being handled correctly.
(2) For the RX Family, check that the settings for I/O signals in the [Tool Details] dialog box match the wiring of the target system.

Cause 3:

The wrong target device might be selected in the [Create New Project] dialog box.

Action 3:

Select the same device as the connected target device.

Cause 4:

The target device might not be receiving a clock signal.

Action 4:

Check the clock supply on the target system.

Cause 5:

Power might not be being supplied normally to the target device.

Action 5:

(1) Check the power supply setting.
(2) If the power is being supplied from the tool in use, the power might not be sufficient. In such cases, supply power from the target system. Confirm that the supply of power on the target system is possible.

Cause 6:

The security functions of the target device may restrict the connection to the RFP.

Action 6:

None. Change the target device if this is required.

Cause 7:

The RFP may not be connected to the target device due to the compatibility with the host PC or the USB-to-serial converter.

Action 7:

We do not recommend the use of a USB-to-serial converter because it may cause delays in timing and data being lost due to the specifications of the converter. Check the operation of the USB-to-serial converter you are using. If timing is delayed or data are being lost, you may consider using a different USB-to-serial converter.

Remark Recommended product for use as a USB-to-serial converter: FT232R from FTDI

Cause 8:

The target device may not have been reset.

Action 8:

When the connection is through a COM port or USB Direct, the RFP does not control the reset pin of the target device. Reset the target device in advance when connecting to it. If the target device has been started in boot mode by a power-on reset and connected or disconnected by the RFP, it must also be reset in advance when re-connecting with the target device.

(2) When an error produces the message 'E3000107 This device does not match the connection parameters.'

Cause 1:

An attempt was made to connect a target device which differs from that when the project was created.

Action 1:

Create a new project or use the correct project with the target device.

Cause 2:

The memory structure might have been changed by the option settings of the target device.

Action 2:

When the target device has a function for changing the memory mapping, such as a dual-bank structure, the RFP recognizes the target device as a different device before and after the change in memory mapping. Accordingly, after a change to the memory mapping of the target device, the error "E3000107 This device does not match the connection parameters." will occur. In the RFP, create projects corresponding to the states before and after the memory mapping change, and switch between the projects for use.

(3) When an error produces the message 'E4000003 A timeout error occurred.'

Cause 1:

The connection to the target system may be wrong.

Action 1:

Confirm that the connection to the target system is correct according to the recommended circuits shown in the manual of the tool you are using.

Remark Good communications may not be possible if you are using a USB-to-serial converter or a self-made target cable for connection with a tool.

Cause 2:

Settings of the target system and RFP may not match.

Action 2:

(1) Baud rate: Check the operating frequency of the target device to see if the baud rate exceeds the allowable communications rate and if the baud rate is appropriate.
(2) Clock settings: Check if the clock settings for the target device in the RFP match the actual clock of the target system.

Cause 3:

The target device might have been reset during communications.

Action 3:

(1) Power supply of the target device: An internal reset might occur in the target device due to voltage fluctuations during communications with the RFP. Check that the power supply is free of problems.
(2) External reset: A reset might have been applied to the target device by an external reset circuit during communications with the RFP. Check that the reset circuit is free of problems.

Cause 4:

The settings of switches of the 20-pin to 14-pin conversion adapter (RTE0T00020KCA00000R) for the E2 emulator may be wrong.

Action 4:

Refer to the E2 emulator manual and confirm that the settings of switches of the 20-pin to 14-pin conversion adapter for the E2 emulator are correct.

(4) When USB Direct of the RX device does not work

A target device which is connected by a USB cable is not selectable for the RFP.

Cause:

The driver for USB Direct has not been loaded in Windows Device Manager.

Action:

Install USB driver V2.00.00 for USB-boot MCU Type A by using the installer for the Renesas Flash Programmer. Furthermore, USB driver V1.00.02 for USB-boot MCU Type A is also usable only in an environment where “Memory integrity” in “Core isolation” of the security function of Windows is disabled.

(5) Forgetting the ID code of the RX or entering the wrong ID code

Action:

Refer to the address in the program file at which the ID code was set.

For details, refer to the manual of the target device.

When the control code for the ID code is set so that the whole flash memory is erased after consecutively entering a wrong ID code three times, you can program the flash memory after returning to boot mode.

(6) When a USB-boot device is not recognized by Renesas Flash Programmer V3.20.00 or an earlier version or the Flash Development Toolkit after this product has been installed

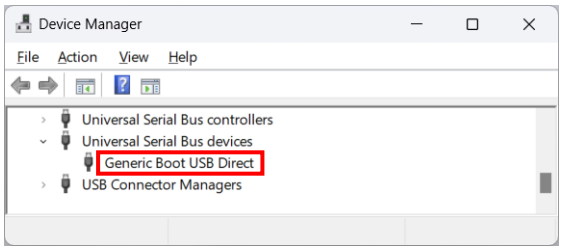
Cause 1:

The USB driver for USB Direct for the RX device has been replaced by the new version.

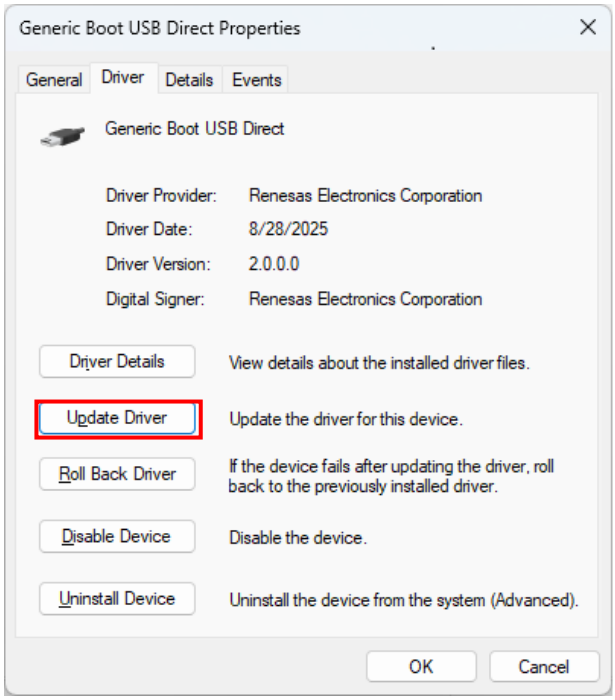
Action 1:

Change the USB driver to V1.1.9.0 or an earlier version by following the steps below.

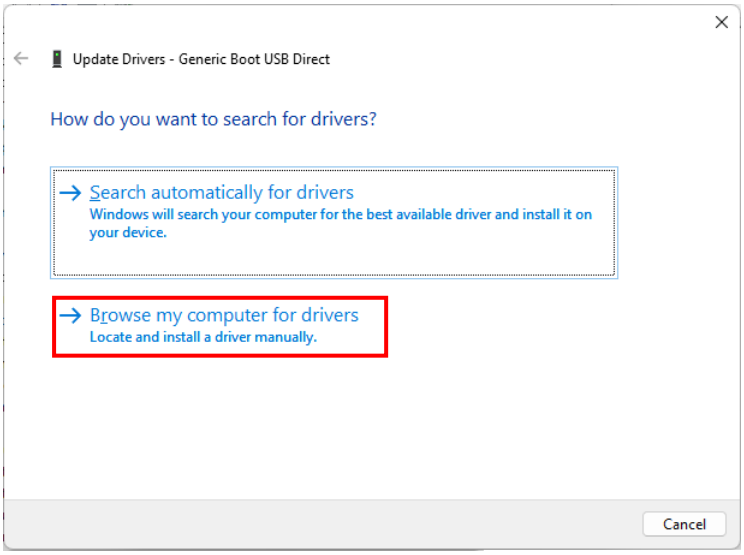
1. Open the Device Manager.
2. Right-click on “Generic Boot USB Direct” to open the properties.



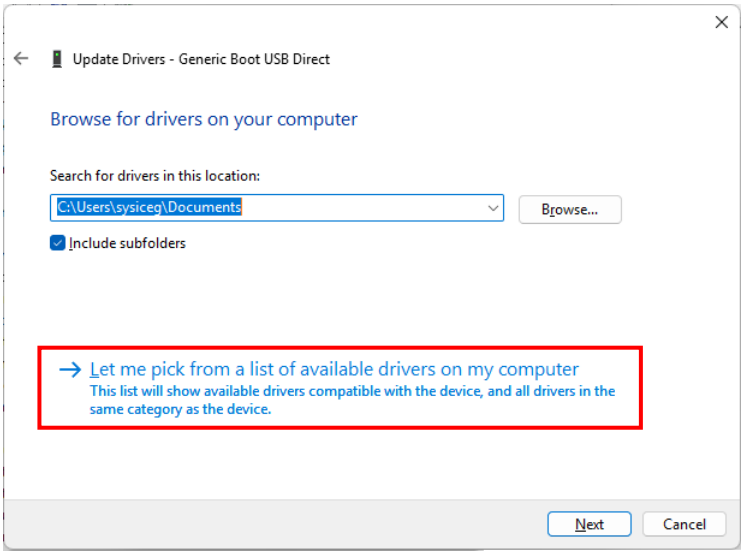
3. Click on [Update Driver] on the [Driver] tabbed page (doing so requires the administrator privilege).



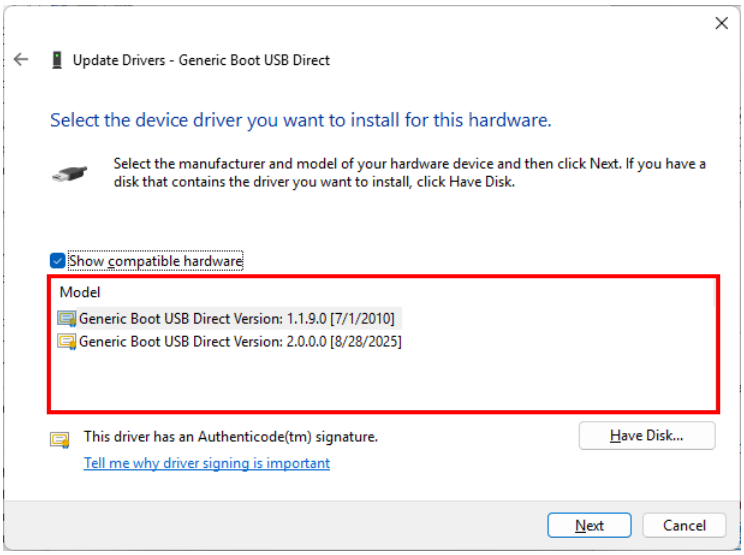
4. Click on [Browse my computer for drivers].



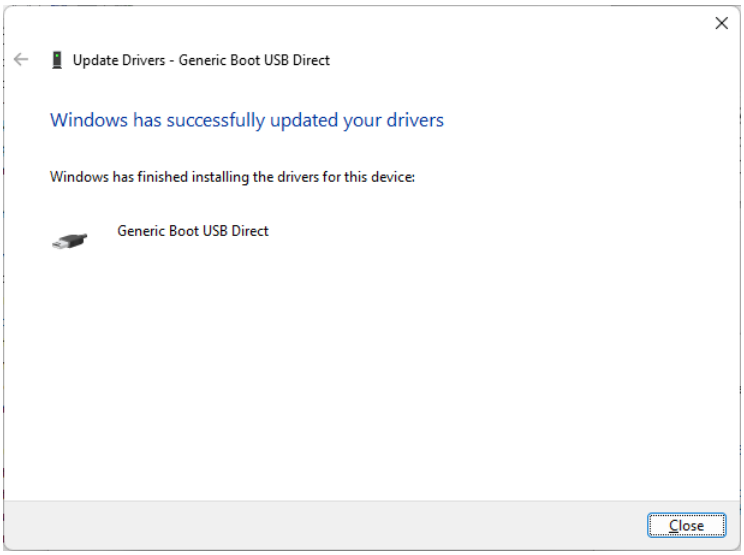
5. Click on [Let me pick from a list of available drivers on my computer].



6. Select the driver you want to use and click on [Next].
   Earlier version of the USB driver: 1.1.9.0 [7/1/2010]
   New version of the USB driver: 2.0.0.0 [8/28/2025]



7. Click on [Close].



Action 2:

Remove “Renesas USB Driver for USB Boot MCU TypeA V2.00” from [Apps]->[Installed apps] of Windows.

4.3 Problems during Communications

This section describes troubleshooting for problems that may occur during communications with the tool or the target device.

(1) When the following errors occur while the tool is connected

- E3000203: An error occurred while connecting to the tool.
- E3000204: An error occurred while communicating with the tool.
- E3000205: An error occurred while updating the tool firmware.
- E3000206: An error occurred while initializing the tool.

Action 1:

The tool you are using might have locked up. Try disconnecting and then reconnecting the USB cable.

Action 2:

The host PC might be unstable or the USB port might be broken. Restart the host PC or connect the tool to a USB port other than that you are trying to use.

Action 3:

On the E1, E20, E2, or E2 Lite the tool might be damaged. Refer to the manual of the tool you are using and run the self-diagnostic test.

Action 4:

If the power is being supplied from the tool, the power might not be sufficient. In such cases, supply power from the target system.

(2) When the following errors occur during communications

- E300010C: Data received from the device are corrupted.
- E4000004: A framing error occurred while receiving data.
- E4000005: A parity error occurred while receiving data.
- E4000006: An overrun error occurred while receiving data.
- E1000004: A transmission data error occurred in the device.
- E5000003: An error occurred during communications with the device.

Action 1:

The setting of the target device might be wrong or communications might not be stable. Check the following items.

- Check that there is no noise on the communications line.
- Check that the tool in use is properly connected with the target system.
- Check that unused pins are being handled correctly.
- Confirm that the correct input clock and transfer rate are selected. Stable programming might be achieved by setting a lower value for the transfer rate.
- A target device which differs from the one in use when the project was created is connected.

Remark Good communications may not be possible if you are using a USB-to-serial converter, a self-made cable, a self-made extension cable, or the like for connection with a tool.

Action 2:

When the RFP is connected to RL78/G10, G1M, G1N, G15, or G16 via the USB-to-serial converter, a parity error may occur due to the hardware. In such a situation, consider the use of another USB-to-serial converter.

4.4 Error Messages

This section describes error messages generated while the RFP is in use.

For error messages not listed above, refer to the target device manual or the Boot Firmware manual.

Table 4-1 Error Messages

E0000001	Message	Operation with a file failed.
	Description	The file name exceeds the available number of characters or includes characters that are not usable in Windows, or the permission settings for the specified file or folder may not allow the operation. Change the file name or the location.
E0000002	Message	A file was not found.
	Description	This error code and message are displayed when the specified file was not found. Specify a new file that actually exists.
E0000003	Message	The file cannot be opened.
	Description	This error occurs in response to an attempt to open a corrupted, non-supported, or non-existent file. Create a new file or select the correct file.
E0000004	Message	The file cannot be saved.
	Description	Change the file or folder to a location which allows saving files.
E0000301	Message	This file cannot be read.
	Description	This error occurs when a program file that is corrupted or is in a non-supported format is specified. For the supported program file formats, refer to section 1.5, Formats of Program Files.
E0000302	Message	This file cannot be read. This file is corrupt.
	Description	This error occurs when a corrupted file is opened. Create a new file or select the correct file.
E0000303	Message	This file cannot be read. It was created with a non-supported version.
	Description	Create a new file.
E0000304	Message	This file cannot be read. This file was created with an older version and contains settings that cannot be converted.
	Description	Create a new file.
E0000305	Message	Specified file contains data outside the device's memory area.
	Description	This error occurs when a file that includes data that are out of the range of memory in the target device has been selected. If you do not wish this situation to produce an error, e.g. ignoring the data beyond the range of the memory does not create a problem, it can be changed to a warning. Regarding changing error messages to warnings, refer to “(6) Error Settings” in section 2.3.2, [Operation Settings] Tabbed Page.
E0001001	Message	The input value is not correct.
	Description	The value entered is wrong. Enter the value in the correct format.

E0001002	Message	The combination of file type is incorrect.
	Description	This error occurs when an RPI, HCUHEX, or RPE file is included in a multiple program file selection. Specify these file types exclusively of each other.
E0001003	Message	The specified crystal frequency is out of range.
	Description	The value entered exceeds the valid range. Refer to the manual of the target device and enter a correct value.
E0001004	Message	No program file has been specified.
	Description	A program file must be specified before the start of programming or verification processing.
E0001005	Message	No command(s) has been selected in the Operation Settings tab.
	Description	Select one or more commands on the [Operation Settings] tabbed page.
E0001006	Message	No blocks have been selected for the current operation.
	Description	Check one or more blocks for the operation on the [Block Settings] tabbed page.
E0001007	Message	No flash options have been set.
	Description	There are no target options when flash options are to be programmed. Change at least one setting to [Set] on the [Flash Options] tabbed page.
E0001008	Message	No unique code file specified.
	Description	This error occurs when a unique code file is not specified on the [Unique Code] tabbed page. For specifying the unique code file, refer to section 2.3.6, [Unique Code] Tabbed Page.
E0001009	Message	This file is not supported by this device.
	Description	For the supported program files, refer to the description of “Program file” under “Terminology” in “How to Use This Manual”.
E0002101	Message	The specified command line option cannot be used in this project file.
	Description	• This error code and message are displayed when the specified project file includes a command that is not available. • This error code and message are displayed when a project file set for RPI or HCUHEX files is in use and a command with a HEX file specified is executed from the simple command line. • This error code and message are displayed when a project file set for HEX files is in use and a command with an RPI or HCUHEX file specified is executed from the simple command line.
E0004002	Message	The ID code does not match.
	Description	This error code and message are displayed when an ID code different from the security code set in the target device is authenticated. If you have forgotten the configured ID code, connection to the target device for serial programming is basically disabled. However, erasure of the whole flash memory is enabled as an exception in some target devices; for details, refer to the manual of the target device.
E0009001	Message	Not enough memory.
	Description	Processing cannot be continued since there is not enough memory in the host PC.

E0009002 E0009003	Message	An unexpected error occurred.
	Description	Reinstall the RFP.
E3000008	Message	This file is corrupt and cannot be opened (line X).
	Description	This error occurs when a program file which contains a line that is corrupted, is in a non-supported format, or contains entries in a non-supported format is specified. Check the format of the program file.
E3000101	Message	The data at 0xXXXXXXXX already exist and cannot be overwritten.
	Description	This error occurs when an attempt is made to handle data having overlapping addresses. Check for data having overlapped addresses in the program file.
E3000103	Message	The format of option data is invalid.
	Description	The target device does not support the format of the option data in the specified program file. Specify the correct RPI file or review the specification of the flash options.
E3000104	Message	The data address is outside the 32-bit address space.
	Description	This error occurs when processing of data beyond the 32-bit address space for the code is attempted in the programming of a unique code. Check the address and the amount of data specified for the unique code file.
E3000105	Message	The device is not responding.
	Description	The target device is not connected or has not returned a response. Confirm that the connection to the target device and the operating mode are correct. The security functions of the target device may have prevented the connection. Refer to section 4.2, Problems during Operation.
E3000106	Message	This device is not supported.
	Description	An attempt was made to connect a non-supported target device. For the supported target devices, refer to section 1.2, Supported Microcontrollers.
E3000107	Message	This device does not match the connection parameters.
	Description	An attempt was made to connect the target device which differs from that when the project was created or the memory structure might have been changed by the option settings of the target device. Create a new project. Refer to section 4.2, Problems during Operation.
E3000108	Message	There is no data in the operation range.
	Description	This error occurs when there are no data in the range of memory of the target device specified by the program file.
E300010A	Message	The data at address 0xXXXXXXXX do not match.
	Description	The data in the program file might be different from that programmed in the target device.
E300010B	Message	The option data do not match.
	Description	The flash option data in the program file might be different from that programmed in the target device. This error will occur when the flash option data is reflected in the target device after a reset.
E300010C	Message	Data received from the device are corrupted.
	Description	Refer to section 4.3, Problems during Communications.

E300010D	Message	The device sent an unrecognized response. (0xXX)
	Description	This error occurs when unexpected data were received from the target device. Check that the target device was reset before connection. Refer to cause 8 of item (1) in section 4.2, Problems during Operation.
E300010E	Message	There are no SVR parameters in the data.
	Description	This error occurs when [Using program files] under [Override SVR parameters] is enabled but data include no SVR parameters in the specified program file.
E300010F	Message	This external flash device is not supported.
	Description	This error occurs when connection was attempted to an external flash device that is not supported. For the supported external flash devices, refer to section 1.2, Supported Microcontrollers.
E3000110	Message	No data found in the operation range, or the operation is not supported for the target.
	Description	This error occurs when the range of memory of the target device specified for the program file contains no data or an operation that is not supported was attempted.
E3000201	Message	Cannot find the specified tool.
	Description	Confirm that the tool specified by the project has been connected to the host PC and that the device driver of the OS has been recognized.
E3000202	Message	The specified tool is already in use.
	Description	This error occurs when the specified tool is already in use by another program.
E3000203	Message	An error occurred while connecting to the tool.
	Description	Refer to section 4.3, Problems during Communications.
E3000204	Message	An error occurred while communicating with the tool.
	Description	Refer to section 4.3, Problems during Communications.
E3000205	Message	An error occurred while updating the tool firmware.
	Description	Refer to section 4.3, Problems during Communications.
E3000206	Message	An error occurred while initializing the tool.
	Description	Refer to section 4.3, Problems during Communications.
E3000207	Message	Power is not being supplied to the user system.
	Description	Turn on the target system before connecting the tool. Check the connection of the tool after you have turned the target system on. When power is supplied from an emulator, confirm that VCC LED of the emulator is lit up.
E4000001	Message	Power is already been supplied on the user system.
	Description	This error occurs when the power-supply function of the tool is selected for use but a power-supply voltage that is already present is detected on the user board. Refer to “(2) Power Supply” in section 2.2.2, [Tool Details] Dialog Box.
E4000002	Message	Cannot release a reset signal.
	Description	This error occurs when the reset signal of the target device going to the high level has not been detected while the E1, E20, E2, or E2 Lite is in use and the target device is connected. Check the reset signal of the target system.

E4000003	Message	A timeout error occurred.
	Description	A timeout occurred when a problem in communications between the target device and the RFP arose for some reason. Check the connection to the target device and confirm that the target device has not been reset. Refer to section 4.2, Problems during Operation.
E4000004	Message	A framing error occurred while receiving data.
	Description	Refer to section 4.3, Problems during Communications.
E4000005	Message	A parity error occurred while receiving data.
	Description	Refer to section 4.3, Problems during Communications.
E4000006	Message	An overrun error occurred while receiving data.
	Description	Refer to section 4.3, Problems during Communications.
E5000001	Message	The device cannot be connected to the RFP since debugging the device is prohibited.
	Description	This error occurs when the target device is not in secure state and is connected through SWD communications. Confirm the security state of the target device. For non-secure state, connect the device through UART communications.
E5000002	Message	The device cannot be connected to the RFP since it is in non-secure state.
	Description	Refer to the description of error message (E5000001).
E5000003	Message	An error occurred during communications with the device.
	Description	Refer to section 4.3, Problems during Communications.
E6000001	Message	An error occurred during setting of the CPU clock.
	Description	This error occurs when the CPU clock is stopped. Check that the clock is correctly being supplied to the target device. If there are no problems with the clock, the device will be in snooze mode or software standby mode. Erase flash memory in the target device through UART or USB communications.
E6000101	Message	Uploading flash programmer firmware failed.
	Description	This error occurs when uploading of the flash programmer firmware to the RAM on the target device failed. Confirm the connection to the target device or reset the target device.
E6000102	Message	Communication with flash programmer firmware failed.
	Description	This error occurs when command communications with the flash programmer firmware uploaded to the RAM on the target device failed. Confirm the connection to the target device or reset the target device.

Table 4-2 Error Messages Due to Errors in the target device

E1000002	Message	A fatal error occurred during control of the flash memory. (Response XX:XX)
	Description	The target device might be malfunctioning or temporarily in an abnormal state. If this error occurs repeatedly, contact a Renesas Electronics sales representative or distributor.
E1000004	Message	A transmission data error occurred in the device. (Response XX:XX)
	Description	Refer to section 4.3, Problems during Communications.
E1000005	Message	An input frequency error occurred in the device. (Response XX:XX)
	Description	This error occurs when the value specified for the input clock signal cannot be used in the target device. For details, refer to the manual of the target device.
E1000006	Message	A frequency error occurred in the device. (Response XX:XX)
	Description	This error occurs when the target device failed to make the clock settings. Check the value of the input clock or the settings of the target device. For details, refer to the manual of the target device.
E1000007	Message	An authentication code error occurred in the device. (Response XX:XX)
	Description	Refer to the description of error message (E0004002).
E1000008	Message	An address error occurred in the device. (Response XX:XX)
	Description	This error occurs when an address range that the target device does not support has been specified. Refer to the manual of the target device and specify the correct range.
E1000009	Message	A baudrate error occurred in the device. (Response XX:XX)
	Description	This error occurs when a baud rate which the target device cannot generate is selected. Check the settings for the baud rate and the clock.
E100000A	Message	A sequencer error occurred in the device. (Response XX:XX)
	Description	This error will occur in the following cases. • An operation was attempted in an area to which a security function is applying a restriction. • The target device is malfunctioning (including defects in or deterioration of the flash memory).
E100000C	Message	A serial programming connection is prohibited for this device.
	Description	This error occurs when the security setting to prohibit connection has been made. The serial programming function then cannot be used. In some target devices, this error does not occur even if connection has been prohibited but the E3000105 error occurs instead.
E100000D	Message	A flow error occurred in the device. (Response XX:XX)
	Description	This error occurs when an operation executed does not match the security state of the target device. Reset the target device or re-check the security state of the target device.

E100000E	Message	A protection error occurred in the device. (Response XX:XX)
	Description	This error will occur in the following cases. • The specified operation is prohibited by a security function of the target device. • An attempt was made to change an operation prohibited by a security function of the target device to be permitted.
E100000F	Message	A blank error occurred in the device. (Response XX:XX)
	Description	This error occurs when there are areas that cannot be erased during erasure of the chip. Re-confirm the security settings of the target device.
E1000010	Message	A verification error occurred in the device. (Response XX:XX)
	Description	This error code and message are displayed when verification of flash memory in the target device was attempted but failed. Possible causes of the error include: (1) Different data have been written to the program file and the target device. (2) The power-supply voltage for the target device not being correct. (3) Data cannot be read from flash memory in the target device because of the pin settings or processing of the target device. Check the items (1) through (3) above. If this error is not resolved even if there are none of the problems described in (1) through (3) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
E1000011	Message	A write error occurred in the device. (Response XX:XX)
	Description	This error code and message are displayed when programming of flash memory in the target device was attempted but failed. Possible causes of the error (failure to program) include: (1) Programming was attempted in an area where the flash memory had not been erased. (2) The power-supply voltage for the target device not being correct. (3) Flash memory in the target device cannot be programmed because of the pin settings or processing of the target device. (4) An operation was attempted in an area to which a security function is applying a restriction. Check the items (1) through (4) above. If this error is not resolved even if there are none of the problems described in (1) through (4) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).
E1000012	Message	An erasure error occurred in the device. (Response XX:XX)
	Description	This error code and message are displayed when erasure of flash memory in the target device was attempted but failed. Possible causes of the error (failure to erase) include: (1) The power-supply voltage for the target device not being correct. (2) Flash memory in the target device cannot be erased because of the pin settings or processing of the target device. (3) An operation was attempted in an area to which a security function is applying a restriction. Check the items (1) through (3) above. If this error is not resolved even if there are none of the problems described in (1) through (3) above, the target device may be malfunctioning (including defects in or deterioration of the flash memory).

E1000014	Message	A dirty error occurred in the device. (Response XX:XX)
	Description	This error code and message are displayed when the state of the switch area is dirty during programming of flash memory in the target device. Execute [SWAS Recover] to restore the state of the switch area to valid.

4.4.1 List of Security and Safety Functions of the Target Device that May Affect the Operation of the Programmer

The following lists the security and safety functions of the target device that may affect the error messages with descriptions that include security functions.

- Access window
- Flash shield window
- OTP
- Disable Debugger and Serial Programming
- Disable Serial Programming
- DLM
- Disable Initialize Command
- Disable Chip Erase
- Disable Block Erase
- Disable Program
- Disable Rewriting boot cluster
- ICU
- Disable Read

Remark: The security functions included in a target device and the operation when the security function has been set depends on the target device. Some security functions may not be cleared by using the [Erase Chip] option or the [Initialize Device] menu. For details, refer to the manual of the target device.

5. Points for Caution

This chapter describes points for caution regarding the RFP.

5.1 Manipulating the User Boot Mat

Applies to: RX610

If a connection is made while the ID code protection is disabled, manipulation of the user boot mat is disabled after the connection is completed. To enable manipulation of the user boot mat, connect to the target device with the ID code protection enabled.

5.2 Host PC

Applies to: All target devices

Some tools (the E1, E20, E2, E2 Lite, serial interface, and USB interface) may not work with the host PC you are using. Check the connection between the tool and the host PC. If the tool still does not work, you may need to use a different host PC.

5.3 Check before Connection

Applies to: All target devices

Connection of the target device in the cases listed below may damage the tool in use or the target system due to conflicts between signals. Be sure to check that the settings and circuit connection are correct.

- The type of the target device to be connected was mistaken.
- The wrong recommended circuit was used for the target device or the circuit being used was in error.
- The output setting of an I/O port pin was wrong while the setting is for manual entry to boot mode.
- The power-supply setting of the tool was wrong.

5.4 Erasing a Chip

Applies to: RH850 Gen1

When a chip is erased, the configuration data are cleared after all other data have been erased. In other words, the option settings of the target device are all erased. Since all settings, including the settings at the time of shipment, are erased at this time, be sure to make the required settings at the same time.

In addition, processing to clear the configuration data is prohibited in some target devices. When you wish to erase a chip, refer to the manual of the target device in use and determine whether the processing is available.

Applies to: RA

Erasing external flash devices as a chip is not supported. When the -erase-chip option is specified in rfp-cli, external flash devices are not erased on the RA8 series. On the RA4 and RA6 series, all blocks of the external flash device are erased.

5.5 Auto-padding with 0xFF

Applies to: All target devices

Even if “Fill with 0xFF” is not selected, when an amount of data is less than the minimum unit for writing to the target memory in the target device, the data are always padded with 0xFF — especially when writing to the configuration setting area.

5.6 Verification after Protecting the target device

Applies to: RH850 Gen1, RX72T, RX71x, RX66T, RX660, RX64x

Setting the following protection functions of the target device restricts the verification function.

- ID code protection
  Proceeding with verification (“Verify by reading the device”) without issuing a reset after the ID code protection bit has been set (written) will cause a protection error. To avoid this type of error, be sure to reset the target device after setting (writing to) the ID code protection bit. The RFP enters the ID authentication mode and verification is enabled.

- Read command protect (Reading prohibited)
  After the read command protection bit has been set, the ID code written to the target device cannot be verified. However, the setting of the read command protection bit becomes effective immediately after a new setting has been written.

5.7 Switching to Dual Mode

Applies to: All MCUs with flash memory in a dual-bank structure

For MCUs that support a dual-bank structure, the RFP recognizes MCUs in the dual and linear modes as different MCUs. Thus, when the bank mode of an MCU has been changed, the error “E3000107 This device does not match the connection parameters.” will occur. In the RFP, newly create and change projects if you change the bank mode.

Remark: This point for caution applies to all MCUs in cases where the configuration of flash memory is changed after programming. The way this is indicated, such as “dual mode”, “linear mode”, or “Bank Mode Select bits” will differ with the MCU Family in use. For details, refer to the manual of the MCU you are using.

The bank mode for the MCU is changed by the following actions.

- Resetting the MCU after a setting for bank mode which differs from the current setting has been written to the Bank Mode Select bit
- Resetting the MCU after selecting [Erase Chip] to erase a chip that is currently in dual mode

The following describes the steps in switching a chip from the linear mode to the dual mode.

(1) Programming an application at the same time as switching to dual mode

Applies to: RA, RX

- Condition: Do not program area 2 in Figure 5-1.

1. Connect the target device in the linear mode and create a new project for the linear mode.
2. Program the program file for the option-setting memory that specifies the dual mode and the program file (application) for area 1 in Figure 5-1.
3. Reset the target device.

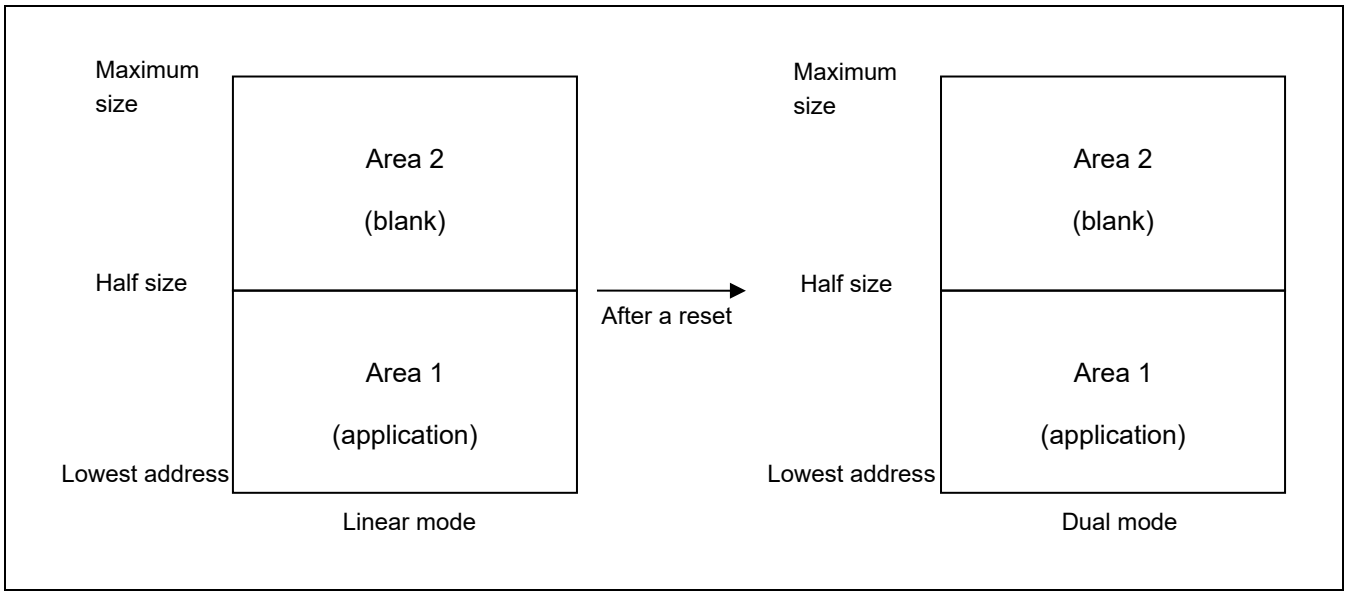


Figure 5-1 Programming an Application for Use in Dual Mode in Linear Mode

Remark: When switching from linear mode to dual mode is to proceed, it is recommended that area 2 in Figure 5-1 be blank.

(2) Only switching to dual mode

Applies to: RH850, RA, RX

1. Connect the target device in the linear mode and create a new project for the linear mode.
2. Program the option-setting memory with a file that specifies the dual mode.
3. Reset the target device.
4. Since the connection of the target device in the project for the linear mode is not possible after this step, create a new project for the dual mode.

5.8 Switching to Double Map Mode

This method is the same as that for switching to dual mode.

For details, refer to section 5.7, Switching to Dual Mode.

5.9 RL78/F2x

Applies to: RL78/F2x

- Writing to the code flash memory for secure boot
  Before writing to the code flash memory of a target device of the type stated above for secure boot by the GUI with specification of the key and MAC passwords, generate an RPI file for which a password has been set by using rfp-cli.
- Procedure for erasing data flash memory
  When data flash memory in a target device of the type stated above is to be erased, set bit 0 in the security option byte to 0. If this procedure was not observed and data flash memory was erased, an error may occur during erasure.

— Procedure

1. Write a program file in which bit 0 in the security option byte (000C4H/040C4H) is set to 0.
2. Reset the target device.
3. Erase data flash memory.

- Operation at low voltage
  When a target device of the type stated above is to operate with a voltage lower than 2.7 V, be sure to select the checkbox for “Wide Voltage” in the GUI. When rfp-cli is in use, be sure to specify the -widevoltage option.

- Writing to the code flash memory
  When a program file is written to the code flash memory in a target device of the type stated above, data must be written to the entire area. Select the [Fill with 0xFF] option (Code Area) of the RFP.

5.10 SWD Interface Connection

Applies to: RA

For the SWD interface connection, handle the pins on the user system so that the startup mode of the MCU is single-chip mode. In single-chip mode, the MD pin is at the high level. The RFP does not operate normally in SCI boot mode or USB boot mode.

For the MCUs supported by the SWD interface, refer to List of MCUs supported by Renesas Flash Programmer V3.

Applies to: RA4E1, RA4M2, RA4M3, RA6E1, RA6M4, RA6M5, RA6T2
Applies to: RA2L2 (*1)

The following functions cannot be used with an SWD interface connection. If options for these functions are specified with rfp-cli, the option settings will be ignored or an error will occur. This also applies in cases where the options are specified in an RPI file. Use these functions through UART or USB communications.

- Programming, verifying, or reading flash options
- Writing or verifying user keys
- Checksums (including file checksums)
- Settings or acquisition in relation to TrustZone
- Initializing devices
- Connecting the RFP while the MCU is in non-secure state

(*1) Of the functions listed above, only the checksum function is supported for the applicable device.

5.11 DA14xxx / RA6Wx

Applies to: DA1459x, DA1469x, DA1470x, DA1453x, DA148xx, RA6W1, RA6W2

- If a program file does not contain a product header or image header, the data of these headers will not be verified even if a verify command is executed.
- If the “Create and write product/image headers” feature is enabled during the execution of the program and verify options, the ranges for which files have no data will be padded with the value 0xFF. Note that DA1459x, RA6W1, and RA6W2 devices do not support the “Create and write product/image headers” feature.
- Changing the external flash device after a project has been created may lead to an error. When changing the external flash device, create a new project.

Applies to: RA6W1, RA6W2

- Target devices of the types stated above do not require erasure of the flash memory in advance; flash memory can be rewritten by writing operations alone.

5.12 Security Memory Protection Unit (MPU)

Applies to: RA

After the security MPU has been enabled, the RFP will not operate correctly on the target device.

5.13 Erase Command

Applies to: RA, RH850, RX, Renesas Synergy™

Areas that do not support erasure, such as MRAM areas and Config Area will not to be erased even if “Erase” is selected for “Command” on the [Operation Settings] tabbed page. Note that erasure is skipped for these areas. Check the log to see the areas which were actually erased.

Revision History	Renesas Flash Programmer V3.25 Software Manual

Rev.	Date	Description	
		Page	Summary
1.00	Oct.01.26	—	The following items were updated on the basis of the contents of document No. “R20UT5820EJ0100”.
		8	Descriptions in the Terminology section were modified.
		9	Descriptions in the Replacing Terms section were modified.
		16	Descriptions in section 1.6, Relative Paths for Files, were modified.
		32	Descriptions in section 2.3.2, [Operation Settings] Tabbed Page, (3) Erase Option, were modified.
		47	Descriptions in section 2.4, Feature of the Flash Options, (21) User Extra, were modified.
		98	Descriptions in section 5.10, SWD Interface Connection, were modified.

Renesas Flash Programmer V3.25 Software Manual

Publication Date: Rev.1.00 Oct.01.26

Published by: Renesas Electronics Corporation

Renesas Flash Programmer V3.25

Renesas Electronics Corporation

R20UT5866EJ0100