Service Manual

Canon BW
iR Security Kit-A2

Canon

Feb 10 2005

Application

This manual has been issued by Canon Inc. for qualified persons to learn technical theory, installation, maintenance, and repair of products. This manual covers all localities where the products are sold. For this reason, there may be information in this manual that does not apply to your locality.

Corrections

This manual may contain technical inaccuracies or typographical errors due to improvements or changes in products. When changes occur in applicable products or in the contents of this manual, Canon will release technical information as the need arises. In the event of major changes in the contents of this manual over a long or short period, Canon will issue a new edition of this manual.

The following paragraph does not apply to any countries where such provisions are inconsistent with local law.

Trademarks

The product names and company names used in this manual are the registered trademarks of the individual companies.

Copyright

This manual is copyrighted with all rights reserved. Under the copyright laws, this manual may not be copied, reproduced or translated into another language, in whole or in part, without the written consent of Canon Inc.

Caution

Use of this manual should be strictly supervised to avoid disclosure of confidential information.

Symbols Used

This documentation uses the following symbols to indicate special information:

Symbol	Description
	Indicates an item of a non-specific nature, possibly classified as Note, Caution, or Warning.
	Indicates an item requiring care to avoid electric shocks.
	Indicates an item requiring care to avoid combustion (fire).
	Indicates an item prohibiting disassembly to avoid electric shocks or problems.
	Indicates an item requiring disconnection of the power plug from the electric outlet.
	Indicates an item intended to provide notes assisting the understanding of the topic in question.
	Indicates an item of reference assisting the understanding of the topic in question.
	Provides a description of a service mode.
	Provides a description of the nature of an error indication.

The following rules apply throughout this Service Manual:

1. Each chapter contains sections explaining the purpose of specific functions and the relationship between electrical and mechanical systems with reference to the timing of operation.

   In the diagrams, ▅▌▐▅ represents the path of mechanical drive; where a signal name accompanies the symbol , the arrow ⟶ indicates the direction of the electric signal.

   The expression "turn on the power" means flipping on the power switch, closing the front door, and closing the delivery unit door, which results in supplying the machine with power.

2. In the digital circuits, '1'is used to indicate that the voltage level of a given signal is "High", while '0' is used to indicate "Low".(The voltage value, however, differs from circuit to circuit.) In addition, the asterisk (*) as in "DRMD*" indicates that the DRMD signal goes on when '0'.

   In practically all cases, the internal mechanisms of a microprocessor cannot be checked in the field. Therefore, the operations of the microprocessors used in the machines are not discussed: they are explained in terms of from sensors to the input of the DC controller PCB and from the output of the DC controller PCB to the loads.

The descriptions in this Service Manual are subject to change without notice for product improvement or other purposes, and major changes will be communicated in the form of Service Information bulletins.

All service persons are expected to have a good understanding of the contents of this Service Manual and all relevant Service Information bulletins and be able to identify and isolate faults in the machine."

Contents

Chapter 1   Specifications

Contents

1.1 Product composition

1.1.1 Product Components

This kit consists of:

[1] License Access Number Certificate Sheet   1pc.
[2] Reference Guide   1pc.
[3] Caution sheet for Users   1pc.
[4] License Registration Booklet   1pc.

> **Memo:**
> Using this kit, you can get a license key from the License Management System (LMS) and register it in an iR/ imageRUNNER to activate the specific feature included in the System Software.

Note:What's LMS?
A license server system to activate software options of iRs/imageRUNNERs, provided by Canon Inc. Collectively manages options in the form of licenses and protects copy rights of optional products. The options are activated with license keys being different from conventional activation measures that use dongles and PCs. Whereas the details of its management differ among countries and regions, it is designed assuming the users access it and activate licenses by themselves respectively. Per optional product, the license access number certificate sheet is supplied. Per license access number, a user can get a license key and activate the feature on an iR/imageRUNNER. To get a license key, a user accesses the Web server of the LMS.

URL for LMS:
http://www.canon.com/lms/ir/

When a user enters the license access number and the serial number for an iR/imageRUNNER in the LMS, 24-digit figure of a license key is generated. The license key includes the information of serial number for the iR/ imageRUNNER so that the key cannot be used for iRs/imageRUNNERs. Once the option is activated, the option information is saved as the backup in the iR/imageRUNNER. Parts replacement will not deactivate the feature.

The staff in each regional headquarters can access the administrator's pages of the LMS. They can view the license number issued for each iR/imageRUNNER and can reissue the license. The procedures are the same as the license management system for MEAP except for the point the license key is used instead of the license file.

Transfer of a License
An optional function that has been enabled by the LMS may be used on a different device by transferring its license, as when the original iR device needs to be replaced, say at the end of its lease arrangement. Specifically, individual licenses registered for optional functions must first be invalidated in user mode before transfer may take place. Doing

so will invalidate the optional functions on the source iR device and, at the same time, proof of invalidation will be generated within the device in the form of an invalidation license key. The user may then communicate the indicated invalidation license key, the serial number of the original iR device, and the serial number of the new iR device to the Sales Company, which in turn may issue a new license key for the new iR device. The user now may register the new license key to the new iR device in user mode, thereby enabling the optional function on the new iR device. For details of transferring a license in service mode, see the descriptions of service mode that come later.

Notes:

Security kit requires that a license key is obtained/registered, and optional PCI bus extension kit, security extension board (USB) and 256MB extension RAM are installed. If these options are not installed, "There are not enough required features for install." is displayed at the license registration, and this function cannot be enabled.

1.2 Specifications

1.2.1 Overview

<u>0008-5635</u>

This kit is an option to add the security function which is enabled by the license.

Characteristics:
- Since the security extension board and increasing memory are required, this kit is installed by the service man.
- HDD data can be protected, and Job Log can be not displayed.
- Encryption processing is conducted by the encryption accelerator, so there is not much influence on the machine performance.
- The security is secured since there is no method to take the key for encryption to the outside of HDD.
- When the data needs to be deleted at the damage on the device, the user can regenerate the encryption key, so that the data can be deleted easily.

For details of installation procedures, please refer to Installation procedure.

Protection of HDD data

Device's HDD records temporally image data like scanned images and PDL data, etc. at any time. Also, the image data is always saved in the user box, FAX box, etc. If the user information like the image data is stolen by extracting HDD, the original data can be recovered easily by directly accessing and analyzing with Disk Editor, etc. For the security, HDD encryption and full initialization of the HDD are used.

HDD encryption

Regarding the HDD dealing with images and PDL data, the information is written by encrypting, and it is read by decoding. Therefore, information within the HDD is always encrypted. Even when the HDD is stolen, recovering the data is too hard. For details, refer to New Functions in the later chapter.

Full initialization of the HDD

When the data which is recorded temporality (e.g. images and PDL data) is not necessary, 0 data or random data is overwritten in the areas where the data exists. By doing so, recovering the original data is too hard. For details, refer to New Functions in the later chapter.

Enabling/Disabling Display of Job Log

By not displaying Job Log to the third party, contents of the PDL printing and contents of transmission/reception using Send function can be prevented from leaking. By setting Service mode, User mode of whether to display Job Log is displayed. For details, refer to New Functions in the later chapter.

Chapter 2   Functions

Contents

2.1 New Function

2.1.1 Security Function

When the Security function is enabled using this kit, the following functions can be validated.
 - HDD encryption
 - Full initialization of the HDD
 - Enabling/Disabling display of Job Log

2.1.2 HDD Encryption

Device's HDD records temporally image data like scanned images and PDL data, etc. at any time. After the printing operation is completed, the normal operation is that only management information is deleted, so the image data information remains on HDD. Therefore, it is concerned that HDD is taken by the third party, the data is analyzed by accessing directly using Disk Editor, and the original data is recovered. As the countermeasure, information is always encrypted in the areas where the data like images and PDL data are saved temporarily. By doing so, recovering the original image data in the HDD will be too difficult. This function is automatically enabled when the license key registration of the security kit is completed. You cannot disable this function.

Mechanism of data encryption

Data encryption uses 3DES encryption algorism with a data encryption key. When the security kit is started its operations, the data encryption key is generated, based on random numbers in the device. Then, when information is read and written in the encrypted area of HDD, the data encryption key is used for encrypting and decoding. There is no way to take this data encryption key to the outside of the HDD. This key is saved in the separate locations other than HDD, so it is too hard to obtain this data encryption key.

Data encryption key to be regenerated

User can execute the regeneration of the data encryption key used for the HDD encryption from the following User mode. When the device itself is damaged or HDD is stolen by the third party, the user can regenerate the data encryption key, so that the current HDD data cannot be accessed.

Actual operations are as follows.

Select in orders of User mode > System Settings > Hard Disk Data Complete Erase

After regenerating, all data is deleted since the full data initialization processing is executed like when the security is started.

2.1.3 Full Initialization of the HDD

Function

With the specific timing as files are deleted (e.g. management information data is deleted) from HDD, this function is to overwrite 0 (null) data and random data in file data areas and delete the data in HDD completely.

In addition to the above real time processing, processing at start-up is added as a new function. When the machine is

started, data which was not deleted when the power was turned OFF last time is deleted. In details, this is conducted when the power is turned OFF during copying and the Secured Print job remains. During the start-up processing, "Remaining data that is not needed is being erased. Do not turn off the main power" is displayed on the screen. When starting or stopping the security kit operation, note that data in the areas to be deleted are all deleted. If all data is deleted or there are much data remained when the power is turned OFF, it takes much time to start up.

Note: Data deletion at the installation

When the security kit is installed, processing to fully initialize HDD automatically is executed. Therefore, you need to backup beforehand.

The data deleted fully this way will be stored files (e.g. files in Boxes) and temporary files (copy files, not visible from outside but nevertheless stored inside). Files stored temporarily as PDL data (e.g. Network PDL Spool) will also be deleted.

If MEAP application is installed, you need to backup the license of MEAP application.

Depending on the Service mode settings, the deletion method is determined. As previous devices, there is no setting of ON/OFF in User mode, and if the security kit is installed, this will be enabled.

Service Mode Item

COPIER>OPTION>USER>HDCR-DSP

1:enable display in user mode/write "0" data once (default)

2:enable display in user mode/write random data once

3:enable display in user mode/write random data 3 times

Change the setting value according to the user's request.

Memo:

The higher the setting, the higher the level of security for the data on the hard disk. It is important to keep in mind, however, that since processing will take place in real time as part of ongoing job execution, the machine performance will drop. Especially when the security operation is started and the data encryption key is regenerated, all areas are deleted completely. Therefore, it takes for 20 minutes with the default setting and one hour with the setting of writing random data 3 times in order to initialize HDD fully.

2.1.4 Enabling/Disabling Display of Job Log

<u>0008-5639</u>

Function

You can disable the display of logs (Job Log) stored by the machine. It affects not only the local UI but also the remote UI. It is important to keep in mind that log collection (job account log/fax communication log) otherwise possible with a specific Canon application (NetSpot Accountant, etc.) will no longer be available, as there will be no response to a command for data collection. (Data in the form of a jam log, error log, and alarm log, however, will be available for collection.)

If the setting of the user mode item explained later is disabled, the display of the following will be disabled:

- System Monitor>copy>Log
- System Monitor>Send>Log
- System Monitor>Fax>Log
- System Monitor>Print>Log
- System Monitor>Receive>Activity Report (RX)
- Ad Func>Report Settings>Settings>Send>Activity Report
- Ad Func>Report Settings>Settings>Fax>Fax Activity Report

As needed, change the following settings:

- Ad Func>Report Settings>Settings: Send>Activity Report:Auto Print=off,Daily Activity ReportTime=off
- Ad Func>Report Settings>Settings: Fax>Fax Activity Report:Auto Print=off,Daily Activity Report Time=off

Whether or not the Job Log will be displayed depends on whether the function is enabled or disabled in user mode.

User Mode Items
Ad Func>System Settings>Job Log Display=on/off
on:enable display of Job Log (default)
off:disable display of Job Log

Service Mode Item
COPIER>Option>USER>LGSW-DSP
0:disable display in user mode (default)
1:enable display in user mode

Changing the setting from 0 to 1 enables to display in user mode.Change the setting value according to the user's request.

Chapter 3   Installation

Contents

3.1 Points to Note About Installation

3.1.1 Points to Note at Time of Installation

⚠ Caution

1. Required Accessories

To install the product, you will need the following separately available accessories: Expansion Bus-B1/C1, USB Application Interface Board-D1 (except US), iR 256MB Expansion RAM-B1 (except US). Be sure that these accessories have been properly installed before starting the work; otherwise, there will be a message to indicate the absence of resources when you attempt to register a license key. The special option may be needed with the copier product used.

2. Time Needed for HDD Initialization

-When the machine restarts for the first time after a license key has been registered, it may take more than 30 min to complete a restart run. It may take even longer if you have changed service mode settings to select 'write random data 3 times'.

The user data will be deleted from the hard disk for the following:

-when the security function is enabled by registering the product's license key

-when a data encryption key is re-generated

-when the product's license key is invalidated to stop using the security function

Before attempting any of the foregoing, be sure to inform the user's device supervisor that the items of data shown in the following table will be lost and it is important to make a backup of data as necessary. Making a backup, however, is not the work of the service person, as it inherently involves security issues. The instructions herein are for reference purposes only.

T-3-1

Data Erased	Able to Be Backed Up
Information registered in the Address Book	Yes
Settings made from the Additional Functions screen	Yes *1
Forwarding Settings	Yes
MEAP applications	Yes
License files for MEAP applications	Yes
Registered SDL (Simple Device Login) user authentication information	Yes
Data saved using MEAP applications	Yes *2

Data Erased	Able to Be Backed Up
MEAP SMS (Service Management Service) password (the password will return to its default password if it was changed)	No
Mode Memory settings registered in the Copy and Mail Box functions	No
Data stored in inboxes	No *3
Scan modes registered in the Send Function	No
Unsent documents (documents waiting to be sent with the Delayed Send mode)	No
Image forms stored in the Form Composition mode	No
Job logs	No

*1 Can only be backed up using the Remote UI or Device Information Delivery Settings mode.

*2 Depending on the MEAP application.

*3 In the case of the iR6570/5570 Series, a backup may be made using the remote UI (not applicable to address books).

 - attributes of boxes

 - image data of a box file

 - attributes of a box file

Items of data that can be backed up

T-3-2

The data can be backed up	Reference
Address Book Settings	See the Remote UI Guide.
Additional Functions Settings	
Forwarding Settings	
Information on exporting data	
License files for MEAP applications	See the MEAP SMS Administrator's Guide. .
Information on downloading license files	
User authentication information registered with SDL	See the MEAP SMS Administrator's Guide. .
Information on exporting user authentication information	

The data can be backed up	Reference
Information which can be delivered using the Device Information Delivery Settings mode	Can only be backed up if you have another imageRUNNER machine that is equipped with the Device Information Delivery Settings mode. It is not necessary to back up this information if you want to use it. For more information on the Device Information Delivery settings mode, see the Reference Guide.
Data saved by MEAP applications	Depending on the MEAP application. For information, see the documentation included with the application.

4. Work After Installing the Kit

-If you disable functions of the Security Kit, passwords set for User Inboxes, Confidential Fax Inboxes, and the Memory RX Inbox are erased. Set these passwords again.

-If you have logged in to the machine using a login service, such as SDL (Simple Device Login) or SSO (Single Sign-On) before disabling functions of the Security Kit, you must select the login service again in SMS (Service Management Service) after restarting the machine. For information on changing the login service, see the MEAP SMS Administrator's Guide.

3.2 Checking components

3.2.1 Checking Items in the Package
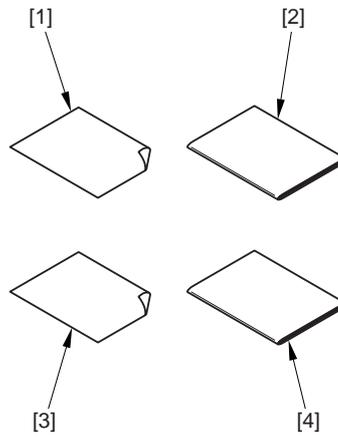
F-3-1

[1] License Access Number Certificate Sheet   1pc.
[2] Reference Guide   1pc.
[3] Caution sheet for Users   1pc.
[4] License Registration Booklet   1pc.

3.3 Installation procedure

3.3.1 Backing Up Data (reference only)

MEMO:

Points to note when the security kit and its iR machine are installed at a time.

Install the security kit first if the security kit and its iR machine are installed at a time. Backup work is unnecessary in this case. If the security kit is installed in a machine that is already set up, backup work is required.

Overview of backup procedures for each data is as follows.

Backup using the import/export function of Remote UI

Procedure for backing up address book information

(1) Access the following URL, and access Remote UI.

http:// [Device IP Address] /

(2) Click Add. Func., and select import/export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.

(3) Click Address Book and click Export.

(4) Select Address Book and file format, and click Start Export.

(5) Specify a storage location of the files according to the screens. Name files to easily identify a file and its page of address book.

MEMO:

All information in address book is included once Forwarding settings are exported.

Backup of Address Book is unnecessary if there is no need to backup pages individually

Procedure for exporting Forwarding settings

(1) Access the following URL, and access Remote UI.

http:// [Device IP Address] /

(2) Click Add. Func., and select import/export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.

(3) Click Forwarding settings.

(4) Click Export, and click Start Export.

(5) Specify a storage location of files according to the screens.

Procedure for exporting Additional Functions

(1) Access the following URL, and access Remote UI.

http:// [Device IP Address] /

(2) Click Add. Func., and select Import/Export from the menu displayed. A dialog box is displayed at this time if a system administrator ID and a password are set up. Enter a system administrator ID in the user name field, and a password in the password field. Click OK.

(3) Click Additional Functions and Click Export.

(4) Select Address Book, and click Start Export.

(5) Specify a storage location of files according to the screens.

Backup using the device information delivery function

If same iR machines connected on the network are installed more than two and they have the device information delivery function, it is possible to register one machine as a master and deliver same information to the other machines to synchronize settings.

Refer to [Device Information Delivery] in the Reference Guide.

(1) Make settings of a master machine (i.e., transmission side). Register destinations of device information to the master machine. Select Additional Functions>System Settings>Device Information Delivery Settings>Register Destinations.

(2) Register destinations manually/automatically. In the case of auto-search, select destinations from search results, and press OK.

(3) Check settings status of destinations to see if the master machine can send device information to slave machines.

(4) Make manual delivery settings. Make the settings when slave machines are not used on the network/Local UI.

(5) Select Additional Functions>System Settings>Device Information Delivery Settings>Transmitting and Settings>Manual Delivery. Set target information for delivery to ON from Add. function settings value, Dept. ID, and Address Book, and press Next.

If address book is selected, forwarding settings and favorites button settings are also delivered.

(6) Select destinations, and press Manual delivery start. Device information will be delivered to the specified slave machines. Check delivery results after delivery.

Backup of MEAP applications

If any of MEAP applications is already installed, data and a license stored in the MEAP application is deleted. However, you don't need to consider it if MEAP applications are not installed.

If a MEAP application has the backup function, be sure to backup data specific to the MEAP application using the function. For licenses, it is necessary to stop all applications from SMS (Service Management Service), disable the licenses, and download the disable license files.

⚠

MEAP backup function using SST

Concerning data backed up with MEAPback of SST before starting the security kit, it must not be re-written to the iR machine after the security kit starts to run. Also, if data backed up after the security kit starts to run is re-written to an iR machine that the security kit is yet to run, it does not work properly. It is absolutely necessary to match operating conditions of the security kit before and after backup work. For that reason, backup is impossible with the MEAP backup function while installing the security kit.

The following procedures are for stopping MEAP applications, disable licenses, and downloading license files. Refer to the MEAP SMS Administrator Guide for details.

Stopping/Disabling MEAP applications, Downloading license files, Uninstalling MEAP application.

(1) Select the following URL to access SMS.

http://[Device IP Address]:8000/sms

The default password is "MeapSmsLogin." If the user has changed the SMS password, ask him/her to change it to an appropriate one after the start of security implementation.

⚠

SMS password will be initialized after the security kit starts to run.

Therefore, be sure to ask user to change a password.

(2) Select the radio button of an application to be stopped from the Application list page, and click stop.

(3) Click name of application that a license is Installed, and access the Application License Information page.

(4) Click License Management, and click Disable. Click OK on the Disable license file confirmation screen.

(5) Click download from Download/Delete Disabled License File.

Specify a storage location of a file according to indications on the screens. At this time, name the file to easily identify an application and its disable license file.

Click deletion after the disable license file is downloaded to PC. Click OK on the Delete disabled license file confirmation screen.

(6) Go back to the application list page, and select the radio button of an application to be uninstalled. Then, click uninstall. Click OK on the uninstallation confirmation screen. Repeat the steps (1) to (6) if there are multiple applications.

(7) After the security kit starts to run, re-install applications using application files (jar file) of applications and the backed up disable license files (.lic file).

User authentication information registered in SDL (Simple Device Login)

When user changed a login application of MEAP to SDL, backup of user authentication information is necessary according to the following procedure.

(1) Access the following URL.

http:// [Device IP Address]:8000/sdl/

(2) Login using user name and a password registered in SDL as an administrator.

Defaults are as follows:

User name: Administrator

Password: password

(3) Click user management.

(4) Place a checkmark to Select All, and click Export.

(5) Click start without changing File Format and Encoding from defaults.

(6) Specify a storage location of file, and click save.

⚠

Data that backup is impossible

Data stored in the boxes, yet-to-be-transmitted documents, overlaid-image data are deleted since backup is impossible. Ask user how to handle data that backup is impossible, and take appropriate actions such as printing out the data if necessary.

Refer to Points to Note on Installation for details of data that backup is impossible.

3.3.2 Obtaining and Registering the license key

0008-3227

After completion of data backup, then move to next step: obtain a license key through LMS and register it. Basically users are supposed to operate obtaining their license keys by themselves following the License Registration booklet Guide, which offers the detailed procedures. The outline of the procedures is described below just for reference.

MEMO:

What is LMS?

The LMS (License Management System) is new license server system, which has been offered by Canon Inc. to be used as a mean of validating the iR software options. The purposes of the system are to centrally manage the options in the forms of license and to keep the options from being copied. Instead of conventional methods, such as a dongle or PC, in this new system, the license keys are used in order to validate the options. Basically users are supposed to do the operation, however, the situation will be various in countries or regions. When purchasing an option, a license access number certificate sheet is packaged with the option. The access number is used to obtain a license key, which is specific to the number. Users can access to the Web server, the LMS itself, with the number, and obtain the license key. With the license key is registered to the iR device, the function of the option is validated finally.

When users input both the number on the license access number certificate sheet and the device serial No. of the iR itself to the LMS, a license key composed of 16-digit number, which is specific to each option, is generated. The key includes the information of the device serial No., therefore, users cannot use the key to other devices. Additionally, when once the option information is validated, it will not be invalidated even if parts are replaced for repairs since the information is backed up and stored in the device.

Procedures to obtain and register the license key

(1) Access to the LMS clicking the URL below, and obtain a license key following instructions displayed on the screen step by step.

The URL of the LMS

http://www.canon.com/lms/ir/

⚠

When users obtain a license key, both the 16-digit number on the License Access Number Certificate Sheet and the serial No. (e.g.: ABC01234) of the device to be installed are required. The device serial No. is displayed in the "Serial Number" when the counter key of the iR is pressed.

(2) Write down the 16-digit number displayed on the Web in the space provided on the license access number certificate sheet.

MEMO:

The 16-digit license key number can be printed out last with LMS.

⚠

Make sure to transcribe correctly. Give an appropriate explanation to users so that they will keep License Access Number Certificate Sheet surely.

(3) Press the Additional function>System settings>License Registration, then input the license key in the designated space, and press Start key so that the license key is registered and the function of the option is validated.

If the function fails to be validated, an error message will be displayed. Refer to the followings what action to be required.

"There are not enough required features for install."

>> Check if the USB Application Interface Board-D1 is recognized correctly and also check if the RAM capacity is 512MB. The special option may be needed with the copier product used.

"The value for the license key is incorrect. Check the license key."

>>Check if the license key issued to another device is used.

>>Check if the license key is input wrongly.

>>Check if the license key is correct.

"This function has already enabled."

>>Check if the security function has already been enabled.

(4) Press the power switch on the control panel for 3 seconds or more. Following the instructions displayed on the shutdown sequence step by step with operations to select appropriate items on the touch panel so that the main switch can be ready for turning off. Turn the main power off, and after 10 seconds, turn it on again.

(5) The registered license will be validated when the power supply of the device itself is turned on once again.

At the first reboot after the license key registration, in some cases, it might take 30 min. or more in order to initialize the data in HDD. If the data erasing method of HDD of the device is set to "Overwrite random data 3 times", it might take longer than the cases above. Make sure not to turn off the power supply when the message, "Remaining data that is not needed is being erased. Do not turn off the main power.", is displayed.

(6) When the device starts normally, press counter key and then press the Device Configuration to check if the security kit is displayed in the space of options. Then, set the Service mode at user's request.

3.3.3 Setting the Service mode

When this kit is installed, the Service mode needs changing in response to the user's request.

1. Changing the setting of "Complete erasing of HDD"

Change the setting of complete erasing of HDD at user's request.

- Service mode level 2

COPIER>OPTION>USER>HDCR-DSP

Set value

1: Overwrite NULL data one time

2: Overwrite Random data one time

3: Overwrite Random data three times

Default value: 1

⚠

As the value is set higher, the security level becomes higher while the performance level becomes lower.

2. Switching the key of "Job Log Display ON/OFF" between display and not display

Switch the key of "Job Log Display ON/OFF" between display and not display.

- Service mode level 2

COPIER>OPTION>USER>LGSW-DSP

Set value

0: Not display the key

1: Display the key

Default value: 0

⚠

When this key is set to "1", the device will always respond "0" to the demands of job history reference from the remote applications. Therefore, software, such as NetSpot Accountant, which manages the device using the job history, cannot be used.

3. OFF/ON of connection devices

Re-start procedure may change with connection apparatus used.

1) When the setting of the Service mode is changed, need to turn off/ on the power of connection devices.

⚠

Turning Off the Main Power

When turning off the main power, be sure to go through the following in strict sequence to protect the machine's hard disk:

1. Hold down on the power switch on the control panel for 3 sec or more.

2. Operate on the touch panel according to the shut-down sequence indicated so that the main power switch may be turned off.

3. Turn off the main power switch.

4. Disconnect the power cable (for the power outlet).

<iR4570/3570,2870/2270 Series>
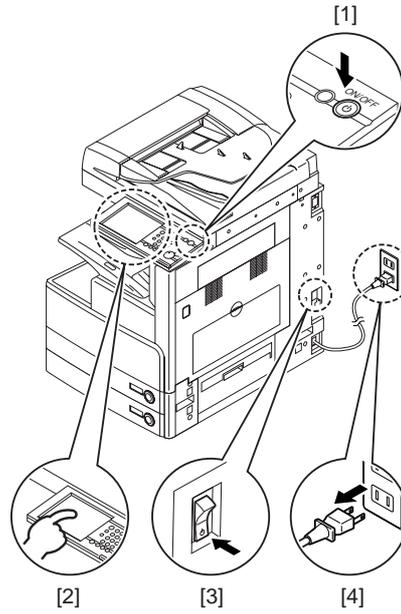
F-3-2

<iR6570/5570 Series>
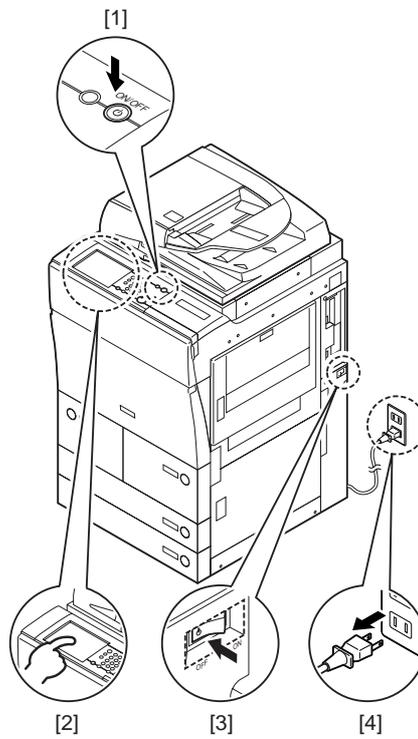
F-3-3

2) Turn the main power on.

MEMO:

If the target data to be erased completely remain in the HDD at the time of turning off the main power, the erasing operation will be carried out at the start-up.

Chapter 4   Maintenance

Contents

4.1 Related Service Mode

4.1.1 Invalidating the License for Transfer to a Different Device (Category 2)

Service Mode Item Used to Invalidate a License for Transfer to a Different Device (Category 2)

Possible Situation

A license may be used on a different device through transfer, as when replacing the device at the end of a lease agreement. To do so, the user must first invalidate the existing license by performing a set of steps referred to as "invalidation of a license" using service mode. At times, both source and target of transfer may be the same device, and a license therefore may also be invalidated only temporarily. It is important to note that the user must contact the Sales Company to make a license good regardless of whether it has been invalidated intentionally or inadvertently.

Invalidation Procedure

Invalidation consists in invalidating the license in service mode and generating an invalidation certificate that proves the completion of invalidation. Invalidation may take place for individual optional functions, and a specific function becomes no longer available as soon as an invalidation certificate is issued. The user contacts the Sales Company and provides the following: the invalidation certificate, the device serial number of the source of transfer, the device serial number of the target of transfer, reason of transfer. In response, the Sales Company may issue a license key for new installation on a different device. The user must take note of the new license key in writing, and keep it as a record after registering it to the target device.

Installation Procedure

1. Start service mode, and activate Category 2 so that the following is true:
COPIER>OPTION>LCNS-TR
The following screen appears, showing the current status of various options:
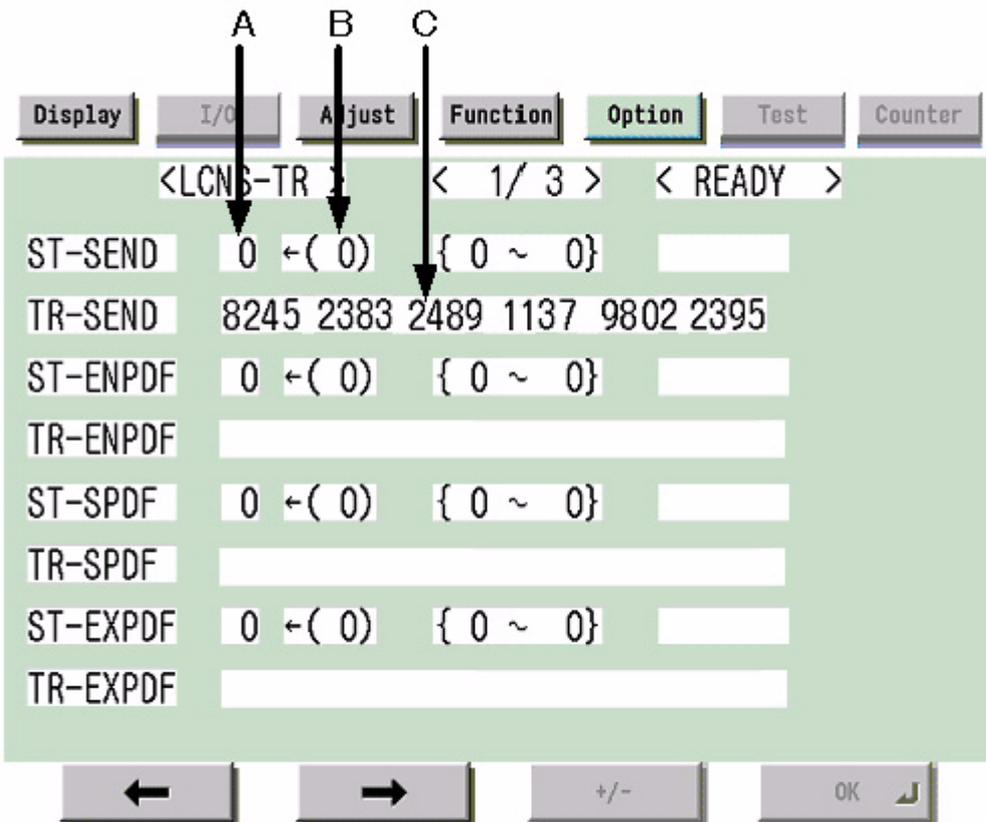
F-4-1

Screen Design:

SET-xxxx: indicates the license status. If installed, the option is identified as '1' under A.

To invalidate an option for transfer, select it, and type in '0' under B; then, click [OK] so that the option will be invalidated and an invalidation certificate will be issued.

TR-xxxx: indicates any invalidation certificates that have been generated under C.

xxxx may be any of the following:

SEND: SEND function

ENPDF: encryption PDF

SPDF: searchable PDF

EXPDF: PDF function expansion (encryption PDF + searchable PDF)

LIPS: LIPS function

SCR: encryption secured printing (for future use)

HDCLR: HDD encryption + full deletion (Security Kit)

BRDIM: BarDIMM (for future use)

Memo:

Not all foregoing options are available in all countries.

2. If an option has already been installed, '1' will be indicated under A. If you want to invalidate it, select it, and type in '0' so that the indication under B will change to '0'.

3. Thereafter, when [OK] is pressed, the indication under A will change to '0' and, at the same time, an invalidation certificate will be indicated in the form of a number. Take note of it in writing together with the serial number of the target device.

4. When the target device is ready, check its serial number.

5. Contact the Sales Company, and provide the following: invalidation certificate for transfer, serial number of the source device, serial number of the target device. The Sales Company, in response, may issue a new license key that may be registered on the target device.

6. Register the new license key to the target device, and check to make sure that the function has been enabled.

Feb 10 2005

Canon