# Service Manual

# Canon BW
# Universal Send Kit-D1

**Canon**

## 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. |
| Memo | Indicates an item intended to provide notes assisting the understanding of the topic in question. |
| REF. | Indicates an item of reference assisting the understanding of the topic in question. |
| | Provides a description of a service mode. |
| Error | 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 configuration

<u>0008-4667</u>

**This kit consists of:**

- License access number certificate sheet
- Sending and Facsimile Guide
- License Key notice

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 Addtional Functions 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 Addtional Functions, 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.

# 1.2 Specifications

## 1.2.1 Specifications

<SEND function basic specifications>

**E-mail transmission**

- Transmission protocol: SMTP, POP3
- Transmission authentication: SMTP AUTH, POP before SMTP
- Reception authentication: POP3, APOP, POP AUTH
- Encoded transmission: Corresponds to SSL communication in each protocol when SMTP transmission and SMTP and POP reception. (The server side needs to correspond.)
- Key and certificate: Server certificate that the device has is used when SSL communication.
- Supported formats: TIFF (monochrome), PDF (monochrome), PDF (OCR) = Searchable PDF
However, encrypted PDF and searchable PDF are the options.
- PDF files can be split and sent page by page.
- Resolution: 100 X 100, 150 X 150, 200 X 100, 200 X 200, 200 X 400, 300 X 300, 400 X 400, 600 X 600 (dpi)
- Document size: A3 to A5
A3, B4, A4 (I-Fax Tx/Rx, A3/B4 transmission possible by setting other party's reception conditions)
- Addresses available from LDAP server (e-mail address and FAX telephone number)
Max. number of searching: 2000; The number of broadcasting selection after searching: 64
- No E-mail reception function. Error mails can be printed out.
When broadcasting transmission, display/write all the addresses in the To: field and separate every 100 addresses to send.

**I-Fax Tx/ Rx function**

- Transmission protocol: SMTP (Tx/ Rx), POP3 (Rx), I-Fax (Simple mode, Full mode)
- Transmission authentication: SMTP AUTH, POP before SMTP
- Reception authentication: POP3, APOP, POP AUTH
- Encoded transmission: Corresponds to SSL communication in each protocol when SMTP transmission and SMTP and POP reception. (The server side needs to correspond. When the server-less transmission, the encoded transmission is not executed. )
- Key and certificate: Server certificate that the device has is used when SSL communication.
- Supported formats: TIFF (monochrome: MH, MR MMR) , Not supported when sending/receiving the color data.
- Resolution: 100 X 100, 150 X 150, 200 X 100, 200 X 200, 200 X 400, 300 X 300, 400 X 400, 600 X 600 (dpi)
- Document size: A3 to A5
- Reception sizes: A3, B4, A4
- Server-less transmission supported
- Addresses available from LDAP server (e-mail address and FAX telephone number)
Max. number of searching: 2000; The number of broadcasting selection after searching: 64
- When broadcasting transmission, display/write all the addresses in the To: field.

**File transmission function**

- Transmission protocol: SMB (NetBios over TCP/IP), FTP(TCP/IP), NCP(IPX)
- Supported formats: TIFF (monochrome), PDF (monochrome), PDF (OCR)
However, encrypted PDF and searchable PDF are the options.
- PDF files can be split and sent page by page.
- Resolution: 100 X 100, 150 X 150, 200 X 100, 200 X 200, 200 X 400, 300 X 300, 400 X 400, 600 X 600 (dpi)
- Document sizes: A3, B4, A4
- CanonFTP automatically distinguishes responses from the server and switches operation accordingly.

**E-mail/I-fax operation confirmed server applications**
SMTP server
Sendmail 8.93 or later
Exchange Server 5.5+SP1 or later
Exchange 2000
Domino R4.6 or later

SMTP AUTH-enabled SMTP server
Sendmail 8.12.5 or later + Cyrus SASL API 1.5.28 combination
Exchange Server 5.5+SP1 or later
Exchange 2000

POP server
Qpopper 2.53 or later
Exchange Server 5.5+SP1 or later
Domino R4.6 or later
Exchange 2000
Qpop v4.0.5

POP before SMTP
Sendmail 8.12.5 or later +DRAC 1.11 or later +Qpopper 2.53 or later combinations

POP authentication function-enabled server
Exchange 2000Server: NTLM authentication when the integration authentication operation:
Qpop v4.0.5: STLS, APOP. However, OpenSSL and Popauth need to be installed.

POP authentication function of main PC mail clients
Outlook 2000:NTLM
Outlook Express 6:NTLM
Becky 2.05:APOP
WinBiff 2.42:APOP
Eudora 5.1:STLS, APOP, Kerberos

**File transmission operation confirmed operating environments**
SMB

Windows 98/ME

Windows NT 4.0 Workstation/Server SP6a

Windows 2000 Professional/Server SP1

Windows XP Home/Professional

Windows Server 2003

Sun Solaris (SPARC) 2.6 or later

RedHat Linux7.2

MacOS 10.2.x

MacOS 10.3.x

FTP

Windows NT 4.0 Server + IIS4.0

Windows 2000 Professional/Server + IIS5.0

Windows XP Professional + IIS5.1

Windows Server 2003

Sun Solaris (SPARC) 2.6 or later

RedHat Linux7.2

Mac OS 10.x.x

NCP

NetWare 3.20

NetWare 4.1, 4.11, 4.2

NetWare 5 +SP1a

NetWare 5.1

# Chapter 2    Functions

# Contents

# 2.1 New Function

## 2.1.1 Authentication at TX

When the mail server is set on the internet, you need to prevent from Third Party Mail Relay that the third party uses the false name. Third Party Mail Relay means that the third party sends large amount of spam mails using the mail server which other people are operating. If you do not take any measures for this, resources like server and network lines are exhausted and at the same time, you will get the claim from the user who received the spam mail. As a measure, the authentication operation when SMTP transmission is prepared.

In case of the inner network (LAN), you can prevent from Third Party Mail Relay by restricting the IP address and the domain name. In order to send from the outside domain using the mail address or securely use the mail server set on the internet which the provider prepares, the authentication is indispensable at the transmission. This machine uses two authentication methods, POP Before SMTP and SMTP AUTH and they enable to send i-FAX and e-mail to SMTP server which requests the sender's authentication.

**POP before SMTP**

With this method, before SMTP transmission is performed, the POP server is logged into. SMTP transmission can only be continued once the POP server has confirmed the IP address of the connected client as authorized within a specific period of time. After user authentication is carried out at the POP server, the authenticated client IP address is relayed to the SMTP server, where it is processed. The process requires a certain amount of time. Taking this processing time into consideration, there is an idle period of 300msec, from POP authentication to the start of SMTP transmission. If a POP before SMTP transmission is generated during POP reception, POP authentication is made to wait until the reception is finished and then POP authentication and SMTP transmission are performed. Errors occurring while the POP server is connected are treated as transmission errors.

With regard to the actual programming, all that is necessary is for **System Settings > Network Settings > E-Mail/ I-Fax > Authent./ Encryption > POP Authentication bofore Sending** to be set to ON.

Related new user error codes are #810 and #813. For details, refer to Troubleshooting.

**SMTP AUTH**

In SMTP AUTH, user authentication is performed when the SMTP server is connected, so that mail can only be received from registered users. This method was standardized in March, 1999, as RFC2554. SMTP AUTH uses ESMTP protocol, which is an extension of SMTP, and uses the SASL (Simple Authentication and Security Layer) authentication mechanism, standardized as RFC2222, to authenticate the user by sending the user name and password information in response to the server challenge data.

**<Authentication mechanisms>**

The SMTP server can have multiple authentication mechanisms and the most suitable authentication mechanism is programmed in accordance with the security policy decided by the SMTP server administrator. The client E-Mail client application selects the authentication algorithm from among the available authentication mechanisms and performs authentication upon transmission.

This model supports the following five types of authentication mechanism.

CRAM-MD5

Challenge-Response Authentication Mechanism, computed by using the key-protected MD5 algorithm by HMAC-MD5 (RFC2104)

NTLM

Windows NT authentication method

User name must be set in the form 'username@NTdomainname'

E.g.:

Windows2000 or earlier: username\\CANON (domain name may be omitted, depending on the environment)

Windows2000: username@canon.co.jp (domain name may be omitted, depending on the environment)

GSSAPI

Authentication system using Kerberos Version 5 (RFC1510)

User name must be set in the form 'username@realmname'.

username@CANON.CO.JP

(In Exchange2000, realm name = domain name)

PLAIN

Assumes that user name and password are sent as plain text (BASE64 encoded) and the communication packet is encoded. (RFC2595) Allows secure authentication when used in combination with the encoded transmission described later.

LOGIN

Sends the user name and password as plain text (BASE64 encoded). Actual transaction is the same as with PLAIN. Similarly, allows secure authentication when used in combination with encoded transmission.

**<SMTP AUTH transmission operation>**

Even if the unit is programmed for transmission with SMTP AUTH, if the mail server does not support SMTP AUTH and the encoding system supported by the server does not match that supported by this model, SMTP AUTH transmission will not be possible. In that case, even if SMTP AUTH is programmed, transmission will be by normal SMTP and there will be no transmission error generated. If an unauthenticated mail transmission is attempted to a server that will not allow such transmission, subsequent SMTP protocols will generate an error in the mail server. Unauthenticated mail can be transmitted to a server that will accept such transmission. These security policies are determined by the server so, even if SMTP AUTH is not programmed, it is impossible to tell whether transmission is possible without checking with the customer's server administrator.

**<Authentication protocol>**

Examples of transmission protocol using SMTP AUTH are given below.

The EHLO response from the client tells whether SMTP AUTH is supported by the server and the authentication algorithm being used at that time is described. In the event that there are multiple authentication algorithms, multiple algorithm names are described. The client selects one of the relayed authentication algorithms and then relays it on to the server. Server challenge data come from the server and coded data made up from the server challenge data, user name and password are returned in response for authentication. In general, the authentication algorithm to be

used can be selected on the server side and PLAIN and LOGIN authentication and others which are undesirable from the perspective of security can be blocked by the server setting.  (Security policy is determined by the server.)

Server:220 smtp.example.com ESMTP server ready
Client(iR):EHLO ifax.example.com
S: 250-smtp.example.com
S: 250-DSN
S: 250-EXPN
S: 250 AUTH CRAM-MD5 DIGEST-MD5 : <- server declares authentication algorithm
C: AUTH CRAM-MD5 : <- client selects CRAM-MD5
S: 334 : <- server response (subsequently, authentication begins with CRAM-MD5.)
S: PENCeUxFREJoU0NnbmhNWitOMjNGNndAZWx3b29kLmlubm9zb2Z0LmNvbT4=
C: ZnJlZCA5ZTk1YWVlMDljNDBhZjJiODRhMGMyYjNiNiYmFlNzg2ZQ==
S: 235 Authentication successful.

**<Authorisation algorithm selection>**
Where the SMTP has multiple authentication mechanisms, selection is made in the order of the priority list given below.

1) CRAM-MD5
2) NTLM
3) GSSAPI
4) STARTTLS operation PLAIN
5) STARTTLS operation LOGIN
6) STARTTLS non-operation LOGIN
7) STARTTLS non-operation PLAIN

Authentication methods can be disabled in service mode.  When the service mode value is set to '1', the encoding system can be disabled.  (The default setting is all enabled.)
Ordinarily, the default setting is used, but if the server administrator wants to disable a particular encoding system, the settings need to be changed by the service mode settings.

**<SMTP AUTH related user modes>**
For the actual SMTP AUTH settings, system administrator settings > network settings > E-Mail/ I-Fax > Authent./ Encryption > **SMTP** Authentication (**SMTP AUTH**) should be set ON and the required user names and passwords for SMTP AUTH need to be entered.  If SSL permission, which is the encoded transmission setting, described later, is ON, with PLAIN and LOGIN authentication, the authentication encoded by the STARTTLS command  can be used.

**<Outlook Express example>**
For reference, this section describes what happens to the Outlook Express settings when using an SMTP server that supports SMTP AUTH. Outlook Express PLAIN authentication only.
1) From the Outlook Express tools menu, select Accounts.  In the example, pop3.canon.com is selected.

2) From Internet Accounts, select the desired account and click on Properties.  In the example, the pop3.canon.com server tab has been selected from the Properties window.

3) Put a check in the 'My server requires authentication' box against the OutGoing mail server.



F-2-1

4) Press the settings button that has been made active.

5) Programme the transmission mail server window's logon information.  In the default, 'use same settings as my incoming server' is selected.  This setting uses the POP3 authentication account name and password entered against the reception mail server in the previous window and performs SMTP AUTH operation.

**Outgoing Mail Server** ? X

Logon Information

⊙ Use same settings as my incoming mail server

○ Log on using

Account name: [          ]

Password: [          ]

☑ Remember password

☐ Log on using Secure Password Authentication

[ OK ]  [ Cancel ]

F-2-2

If 'Log on using' is selected, the account and password to be used with SMTP AUTH can be specified individually. In that case, if 'Log on using Secue Password Authentication' is selected, encoding is carried out by TSL(SSL), using the STARTTTLS command.

<SMTP AUTH related user error codes>
The related new user error codes are #839 and #843.  For details, refer to the section on Troubleshooting.

## 2.1.2 Encrypted transmission

0008-4676

**Transmission packet encryption (SSL)**
When Additional Functions > System Settings > Network Settings > E-Mail/ I-Fax > Authnt. /Encryption > allow SSL(SMTP send) is set to ON, and the mail server supports the SMTP protocol's STARTTLS command, SSL (TLS) is used for transmission packet encryption.  Not only the user name and password are encrypted, but also all of the mail transmission data.  Therefore, the transmission speed is slower.
If  'allow SSL(SMTP Semd)' is set to OFF, or the mail server does not support the SMTP protocol's STARTTLS command, the transmission packet is not encrypted.

**<STARTTLS command>**
STARTTLS is an SMTP command that tells the server that encrypted transmission (SSL/ TLS) is about to start.  The command is standardized in RFC2487.  Following is an example of the protocol flow during STARTTLS.
The EHLO response from the client declares that STARTTLS is supported from the server.  When the client generates the STARTTLS command, the operation is reprocessed from the starts and negotiation is initiated and the packet data are encrypted.

S: 220 mail.imc.org SMTP service ready
C: EHLO mail.example.com
S: 250-mail.imc.org offers a warm hug of welcome
S: 250-8BITMIME

**S: 250-STARTTLS : <- Shows that the server supports STARTTLS.**

S: 250 DSN

**C: STARTTLS : <- Declares to server that SSL/TLS are to be performed.**

S: 220 Go ahead

-- All subsequent transmission packets will be encrypted.

C: <starts TLS negotiation>

C&S: <negotiate a TLS session>

C&S: <check result of negotiation>

C: EHLO mail.example.com

S: 250-mail.imc.org touches your hand gently for a moment

S: 250-8BITMIME

S: 250 DSN


**<User error>**

Related new user errors are #841 and #842. For details, refer to the section on Troubleshooting.


# 2.1.3 Authentication at RX

The username and the password flow by the plaintext in  the reception form by past POP3. And POP3 logs in POP server at a short cycle. Therefore, the password is  easily stolen in POP3.

Enable the password to encrypt and to be attested by  using APOP and POP AUTH. APOP is defined by RFC1939, and  executed with UNIX system POP server, and POP AUTH is  defined by RFC2449, and executed with the MS Exchange  server.In addition, if POP server supports the SSL(TLS) encryption by the STLS instruction, not only the password but also the entire reception packet can be encrypted.


"POP AUTH Method " exists in Aditional Function >Network Settings >E-mail/I FAX >Authent./Encryption , and it is possible to select it from Standard / APOP / POP AUTH .

APOP and POP AUTH are executed respectively when APOP and POP AUTH are selected, and when Standard is specified, the authentication by the username and the password is executed.

Default: It is Standard.

**APOP**

APOP authentication procedures are as follows.

(1) As a greeting message when connecting to POP server, the server returns the character strings consisting of the time stamp and the host name to the client. The client links these character strings with the password character strings, and creates the message digest by MD5 from the linked character strings.

(2) With the APOP command, the client returns the message digest created with the user name to the server.

(3) Message digest is created in the POP server with the same algorism. By comparing this created digest and the digest from the client, if both digests are the same, the password is considered as the correct one.


Greeting message when connecting to the server includes the time stamp, so analyzing is difficult since the created message digest changes every time.


Different from the POP AUTH described later, there is no protocol to check whether or not the server is supporting

APOP from the client, so the user have to decide whether or not APOP is used and set User mode.

If the server does not support APOP and the user uses APOP, an error occurs. When the error occurs at the APOP authentication, "APOP Authentication Error" is displayed on the status line for certain time.

Following items are the examples of communication.

S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>

C: APOP mrose c4c9334bac560ecc979e58001b3e22fb

S: +OK maildrop has 1 message (369 octets)

C: :

When the server connection, the password "tanstaaf" character strings of the user mrose is linked after "<1896.697170952@dbc.mtview.ca.us>" message. Character strings of "<1896.697170952@dbc.mtview.ca.us>tanstaaf" is hashed by MD5, then it becomes "c4c9334bac560ecc979e58001b3e22fb".

For actual settings, set as follows. System Settings > Network Settings > E-mail/I-Fax > Authent./ Encryption > POP AUTH Method >APOP.


**POP AUTH**

POP AUTH uses the authentication mechanism of SASL(Simple Authentication and Security Layer) provided in RFC2222 and conducts the user authentication by returning the user name and password information as a response to the server challenge and its data from the server. This is standardized as RFC1734 "POP3 AUTHentication command". By the CAPA command extended in RFC2449 "POP3 Extension Mechanism", you can know the capability which the server has, and SASL authentication algorism which the server supports is included in one capability and returned by the SASL tag.


<Authentication mechanism>

In the POP server, multiple authentication mechanisms can be possessed and the authentication mechanism is set according to the security policy which the server administrator decides. E-mail client application selects the authentication algorism from the specified authentication algorism and performs the authentication at the transmission. This device supports the following authentication algorism.

**CRAM-MD5**

Challenge-Response Authentication Mechanism calculated using MD5 algorism with the key based on the HMAC-MD5 (RFC2104).

> **Note:**
> Currently, POP AUTH server in the field are mostly made by Microsoft and NTLM authentication is used. CRAM-MD5 is installed, but there is no server which the operations are checked, so the evaluation has not performed. For this reason, POP AUTH operations with CRAM-MD5 are not supported.

**NTLM**

Authentication method of Windows NT

User name has to be set in the form of "User name@ NT domain name".

> **Example:**
> Windows2000 or former: User name\\CANON (Domain name can be omitted according to the environment.)
> Windows 2000: User name@canon.co.jp (Domain name can be omitted according to the environment.)


**PLAIN**

Authentication method that user name and password are transmitted in plaintext (BASE64 encode) and the packet is encrypted. (RFC2595) By applying with the later "Encrypted transmission", the authentication is secured.

**LOGIN**

User name and password are transmitted in plaintext (BASE64 Encode). Actual method of communicating information is same as PLAIN. By applying with the later "Encrypted transmission", the authentication is secured.

> **Note:**
>
> When SSL is not operated, the authentication of PLAIN and LOGIN is not encrypted, so there is no difference from the authentication of the plaintext USER/PASS. For this reason, there is no meaning of using POP AUTH. This operation gives misunderstanding that it is encrypted, so operations with POP AUTH are prohibited.

< POP AUTH reception operations>

Even POP AUTH is set to be used for receiving, if the mail server does not support POP AUTH, the server supporting-authentication method and the device supporting-authentication method are different, the reception with POP AUTH is impossible. In this case, "POP AUTH Encryption Error" is displayed on the status line.

<Authentication protocol example>

Examples of transmission protocol when using POP AUTH are shown below.

With the CAPA response from the client, supporting SASL is informed from the server. At this time, usable authentication algorism is described. If multiple authentication algorisms are possessed, multiple algorism names are described. Client selects one algorism from the authentication algorisms which the server informed and the selected authentication algorism is informed to the server. The server sends the server challenge data, and performs authentication by returning this data and the encrypted data created from the user name and password as a response. Generally, the authentication algorism can be selected on the server side whether to be used. If it is not suitable to be used for the security, it can be prohibited by the settings on the server side. (Security policy can be determined by the server.)

Server: +OK POP3 v2001.78 server ready <4a61.3e55cd70@test.canon.co.jp>
Client(iR): CAPA
S: +OK Capability list follows:
S: TOP
S: LOGIN-DELAY 180
S: UIDL
S: STLS
S: USER
S: SASL CRAM-MD5 LOGIN
S: .
C: AUTH CRAM-MD5
S: + PDE5MDQ0LjEwNDU4MTEyMThAYmFiYS5jY20uY2Fub24uY28uanA+
C: ZnJlZCA5ZTk1YWVlMDljNDBhZjJiODRhMGMyYjNiYmFlNzg2ZQ==
S: +OK Authentication successful....
...

<Selection of the authentication algorism>

When SMTP server possesses multiple authentication mechanisms, the authentication method is determined in the following priority order.

1) CRAM-MD5 (Not supported)

2) NTLM

3) PLAIN when STLS (SSL) operation

4) LOGIN when STLS(SSL) operation

From Service mode, you can prohibit the usage of each authentication method. If you set Service mode setting to "1", you can prohibit the usage of the authentication method. (All defaults: usable)

Usually, the device is used with the default settings, but if the server administrator prohibits the usage of the specific authentication method, you can change the setting by Service mode.

< POP AUTH-related Addtional Settings>

Actual POP AUTH-related setting is selected in the order of System Settings > Network Settings > E-mail/I-Fax > Authent./ Encryption > POP AUTH, and then you want to enter the user name and password necessary for POP address and POP password. When enabling "SSL Allow (POP)" (the setting of encryption communication), the encrypted authentication by STLS command can be used at PLAIN and LOGIN authentication.

## 2.1.4 Encrypted reception

0008-5788

There are two types of encrypted reception methods available - encrypted POP and SMTP email receptions.

**Encrypted POP Reception**

When Allow SSL (POP) control is turned on in Authentication/Encryption Settings window* and the POP server supports STLS command, defined in POP3 protocol, the imageRUNNER/iR can communicate with encrypted packets using SSL (TLS). The communications slows down since not only the user name and password but also the entire communication data for email reception are encrypted. If Allow SSL (POP) control is turned on but the POP server does not support STLS command of POP3 protocol, it results in an error. If an error occurs in POP SSL communications, the status line displays **"SSL Error (POP)."**

* Authentication/Encryption Settings window: opens by selecting Additional Functions > System Settings > Network Settings > Email/I-Fax > Authent./ Encryption.

**STLS**

An extended SMTP command, defined in RFC 2487. RFC 2449 -- POP3 Extension Mechanism -- specifies that STLS must support CAPA command. If a server supports STLS, it states the support in response to CAPA command.

The following lines exemplify communications when STLS is enabled.

...

S: +OK POP3 v2001.78 server ready <4a61.3e55cd70@test.canon.co.jp>

C: CAPA

S: +OK Capability list follows:

S: TOP

S: LOGIN-DELAY 180

S: UIDL

**S: STLS :<-- Indicates the server supports STLS.**

S: USER

S: SASL CRAM-MD5 LOGIN

S: .

C: STLS

S: +OK Begin TLS negotiation

<TLS negotiation, further commands are under TLS layer>

S: +OK POP3 v2001.78 server ready 4a61.3e55cd70@test.canon.co.jp

**Encrypted SMTP Reception**

The iR 2270 and later models support SSL (TLS) encryption for receiving email messages from SMTP servers. To use this feature, a valid server certificate is required. When SSL or On option is selected for Allow SSL (SMTP Receive)* and the email server supports STARTTLS command, the imageRUNNER/iR can communicate with encrypted packets using SSL (TLS). When Off option is selected for Allow SSL (SMTP Receive) control, the imageRUNNER/iR does not include STARTTLS in a response for EHLO. The communications slows down since not only the user name and password but also the entire data for email sending are encrypted. When Off option is selected for Allow SSL (SMTP Receive) or the email server does not support STARTTLS command of SMTP protocol, the communication packets are not encrypted.

*Allow SSL (SMTP Receive) control: is displayed by selecting Additional Functions > System Settings > Network Settings > Email/I-Fax > Authent./ Encryption.

**STARTTLS Command**

An extended SMTP command that notifies a start of encrypted communications in SSL/TLS to the SMTP server, defined in RFC 2487.

The following lines exemplify communications when STLS is enabled.

...

S: 220 mail.imc.org SMTP service ready

C: EHLO mail.example.com

S: 250-mail.imc.org offers a warm hug of welcome

**S: 250-STARTTLS :<-- Indicates the server supports STARTTLS.**

S: 250 DSN

**C: STARTTLS : <--Declares the use of SSL/TLS.**

S: 220 Go ahead

C: <starts TLS negotiation>

C & S: <negotiate a TLS session>

C & S: <check result of negotiation>

-- The communication packets are encrypted from now on --

C: EHLO mail.example.com

S: 250-mail.imc.org touches your hand gently for a moment

S: 250 DSN

C: MAIL FROM <ifax@mail.example.com>

S: 250 Sender OK

...

The client is notified with the response of EHLO that the server supports STARTTLS. When the client issues STARTTLS command, the server and client perform TLS negotiation and resume communications from the beginning with encrypted packet data.

If SSL option is selected for Allow SSL (SMTP Receive) control and the client carry on communicating in plain text, without using STARTTLS, the imageRUNNER/iR replies "530 Must issue a STARTTLS command first" of SMTP mail command and terminates the SMTP connection with the error. The user interface indicates "SSL Error (SMTP RX Reject)" in the status line.

If On option is selected for Allow SSL (SMTP Receive) control, the imageRUNNER/iR accepts communications with the client in plain text, without using STARTTLS. If an SSL processing results in an error, for example the imageRUNNER/iR does not feature an encryption algorithm common to the client, the user interface indicates "SSL Error (SMTP Receive)" and terminates the SMTP connection with the error.

Allow SSL (SMTP Receive) control defaults to Off.

## 2.1.5 MAC Address Block Function
0008-5789

**Receiving MAC Address Settings**

Limits network packets to receive by MAC address. To enable this function, select Additional Functions > System Settings > Network Settings > Email/I-Fax > On for Receiving MAC Address Settings. Up to 100 MAC addresses can be registered to allow communicating with the imageRUNNER/iR. If a conflict occurs between Receiving MAC Address Settings and IP Address Settings, Receiving MAC Address Settings overrides IP Address Settings.

This function filters packets in the network layer and the reception logs for applications are not recorded.

## 2.1.6 URL Send
0008-5791

It is function to transmit URL information with E-Mail to be able to refer the image with remote UI. Image preserved in box including fax box instead of transmitting.
The E-mail address where URL is notified can be set by selecting one address or one group address of each box from the address table.

Set the notified mail address by "URL Sending" of "box specification setting."
E-mail automatically notified that the image is stored in the box of the URL sending setting ending is transmitted.

## 2.1.7 Setting for communicate SSL

<span style="float:right">0008-5795</span>

To communicate SSL, this machine can register the key pair and the certificate. The key pair and the server authentication book self-signed by default have registered as DefaultKey.

## 2.1.8 Initialization of all data and settings

<span style="float:right">0009-6674</span>

**Purpose:**

Previous devices did not have the function to erase all the user data collectively. However, the following function was newly added: The user data in the device including the hard disk can be initialized by the user's operation.

In order to maintain the confidential information, we provide the function to erase all the user data stored in the iR device (image data, various logs, Address Book, Additional Functions settings, etc.) collectively.

**Limitations:**

**a. Confirmation of the erased data**

The function to confirm if all the data are erased collectively is not provided.

Verification after erasing the hard disk, such as Verification Check, is not performed.

**b. SoftID(License Registraton/License key)**

SoftID is controlled by LMS License Manager, and this is the BIT information for the validation/invalidation of the software options. SoftID is not deleted by the function described above (erasing of all the data collectively). LMS License Manager invalidates (uninstalls) the option functions.

**c. Limitation of the device**

When erasing all the user data collectively, LAN and FAX lines are disconnected, so you cannot access from the outside.

**d. Limitation of the job**

When erasing all the user data collectively, all jobs in the device are erased.

**Data to be erased**

 -Image data

 -Address Book

 -Temporary data

 -Fonts and profiles which the user installed

**Data not to be erased**

 -Counter

 -SoftID(License Registraton/License key)

 -Values in Service mode which are adjusted in the factory

 -System software

 -System data (such as the preinstalled font data)

All the data related with the printer are erased collectively. Then, the data are restored from the backup data, so the data will be the state of the default settings. Therefore, the fonts which the user installed will be erased.

**How to erase**
 -Without Security Kit
Only the logical information of FAT(File Allocation Tables) is erased.

 -With Security Kit
All the data are erased in the magnetic level according to the Erase mode in Security Kit.
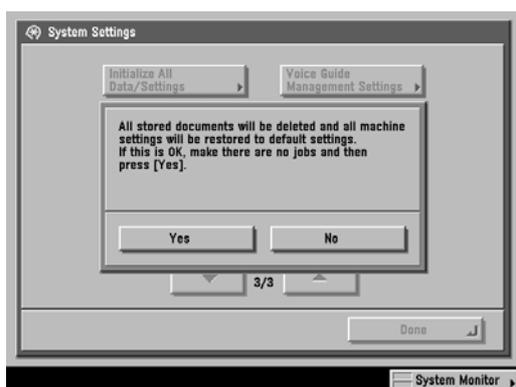
**How to erase the data collectively:**
 -Select "Additional Functions", "System Settings" and "Install All Data/Settings" in order.



F-2-3

 -Select "Yes" in the confirmation dialog box.



F-2-4

 -After rebooting the device, erasing all the data is executed.

**Specification of erasing the data:**

SRAM

Select Service Mode, Copier, Function and Clear in order. Then, write whether the data are to be erased when erasing all the user data collectively.

Service Mode->Copier->Function->Clear

T-2-1

| Data to be erased | To be erased? |
|---|---|
| ERR | ○ |
| DC-CON | × |
| R-CON | × |
| SERVICE | ○ |
| JAM-HIST | ○ |
| ERR-HIST | ○ |
| E354-CLR | ○ |
| E355-CLR | ○ |
| PWD-CLR | ○ |
| ADRS-BK | ○ |
| CNT-MCON | × |
| CNT-DCON | × |
| OPTION | ○ |
| MMI | ○ |
| SOFT-CNT | × |
| CARD | ○ |
| ALARM | ○ |
| SLT-CLR | ○ |
| SND-STUP | ○ |

T-2-2

HDD

| Data to be erased | To be erased? |
|---|---|
| Stored compression image data | ○ |
| Temporary file, log data, others | ○ |

| PDL spool | ○ |
|---|---|
| FAX reception guaranteed | ○ |
| Address Book/Filter | ○ |
| MEAP application | ○ |
| General | ○ |
| Document management table, profile | ○ |
| Font used in PDL, others | ○ |
| Execution module, message file, RUI contents | × |

**The number of rewriting the hard disk**

Depending on whether there is Security Kit or not, the erasing method of the hard disk data when erasing all the user data collectively will change.

-Without Security Kit

Erase mode is fixed with NULL: 1 time. Other modes are not selectable.

-With Security Kit

From Service Mode, any Erase mode can be specified.

There are three patterns of the Erase mode; NULL: 1 time, Random: 1 time, Random: 3 times

# 2.1.9 Backup of Mail Box

0009-6675

**Purpose:**

In order to prevent from missing documents in MAIL BOX permanently because of the hard disk failure inside the iR device, the following function was added: Documents in Mail Box are backed up or restored to the file server connected on the network.

**System configurations:**

The following items are necessary.
-iR device
-SMB server connected on the network

The following types are supported as the SMB server.
Windows system
WIN2K/XP/2003
UNIX system
OS: Linux/RedHat
Server software: samba2.2.8/3.0

You can set the access right to the backup data stored in the server.

In this case, the appropriate user account is necessary.

**Data to be backed up:**

The following data are backed up.

- User Inboxes specification settings

- Image data of User Inboxes documents

- Setting information of User Inboxes documents



Mail Box documents backed up using this function can be used in the same model only. If the backup documents are used in the different model, we will not guarantee the operations.

**Data to be initialized at the restoration**

After folders and Mail Box documents in the iR device are all erased, the restoration is executed.

Data to be initialized at the restoration are as follows.

 -Information in Confidential Fax Inboxes and Memory RX Inbox

 -Mail Box documents created after the previous backup operation

 -Reception number (Target jobs: PDL print, copy, Mail Box Scan, Mail Box Print)

Mail Box documents backed up using this function can be used in the same model only. If the backup documents are used in the different model, we will not guarantee the operations.

**Data to be initialized at the restoration**

After folders and Mail Box documents in the iR device are all erased, the restoration is executed.

Data to be initialized at the restoration are as follows.

 -Information in Confidential Fax Inboxes and Memory RX Inbox

 -Mail Box documents created after the previous backup operation

 -Reception number (Target jobs: PDL print, copy, Mail Box Scan, Mail Box Print)

**Backup destination settings**

Specify "Host IP Address", "User Name", "Password" and "File Path" of the SMB server in which Mail Box documents are backed up. After clicking "Add. Func." of the remote UI, select "Custom Settings" from the menu and click "Backup Destination Settings".

**- Host IP Address**

Enter the server address which provides the SMB service.

Specify the setting value in the format of \\Server name\Name of the shared folder\.

If the correct value is not set, the backup operation cannot be proceeded.

Note: Set "User limit" of the shared folder in the server to "2" or more value or "Maximum allowed".

When you set "User limit" to "1", the restoration is not executed correctly.

**- User Name**

Enter the user name of the SMB server.

If you do not enter the account name which exists on the server, the backup operation cannot be proceeded.

**- Password**

Enter the password which corresponds to the server account name above.

If you do not enter the password which corresponds to the server account name above, the backup operation cannot be proceeded.

**- File Path**

Enter the file path which the data are backed up and stored.

If you do not enter the directory which exists on the server, the backup operation cannot be proceeded.

**Execution of the backup**

After clicking "Add. Func." of the remote UI, select "Custom Settings" from the menu and click "Backup". When you press the "Execute" button, the backup operation will be executed.

However, the error occurs when either of the following folders already exists on the file path: Mail Box folder which is previously backed up the data or BOX.tmp folder which is the folder for operations. Therefore, before executing the backup operation, you need to delete or rename the folders described above.

**Data of the backup destination**

In order to prevent from the failure during the backup operation, such as the device's power shutdown, start the backup operation by generating the following path on the SMB server:

\\<Host IP Address>\<File Path>\BOX.tmp\

This path will be renamed as follows when the backup operation is completed:

\\<Host IP Address>\<File Path>\BOX\

**Execution of the restoration**

After clicking "Add. Func." of the remote UI, select "Custom Settings" from the menu and click "Restore".

When you press the "Execute" button, the restoration which the backup data are read from the server set in "Backup Destination Settings" is executed.

In order to guarantee that the other functions are not executed during the restoration, the actual restoration is not executed until the device is started next time.

After all the Mail Box documents are restored, the auto-reboot is executed and the device is started normally. Then, the process will be the same as the normal operations.

**Security**

Since the communication between the device and the SMB server is not encrypted, you cannot secure the information of the Mail Box documents. Only the password is encrypted. Therefore, even though you use the hard disk encryption function of Security Kit, this backup operation of the Mail Box documents might become the security hole.

# Chapter 3  Installation

# Contents

# 3.1 Installation procedure

## 3.1.1 Overview of the Installation Procedure

As a rule, the user is expected to obtain a license key and register it to the device. Detailed instructions are found in the User's Guide. The following is an outline of the instructions:

1. Using the following URL, access the LMS, and obtain the license key by following the instructions shown on the screen:

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

  **Memo:**
  A license key is issued in exchange for the 24-digit number indicated on the License Access Number Certificate and the serial number of the device (e.g., ABC01234) to which the license will be registered. The device serial number will be indicated in response to a press on the Counter key on the iR device (under [Serial Number]).

2. Copy the 24-digit number shown on the Web browser screen in the space given for the purpose on the License Access Number Certificate sheet.

  **Caution:**
  Be sure to double-check the number to avoid an error. Be sure that the user is aware of the importance of the License Access Number Certificate and that it must be stored away in a safe place.

3. Make the following selections: user mode>system control setup>license control. Then, type in the 24-digit number, and click [Execute]. In response, the license key will be registered and the appropriate functions will be enabled. Otherwise, any of the following error messages will appear:

"The number of the license key is not correct. Check the license key."
 >> Make sure that the license key is not issued for a different device.
 >> Make sure that the number has been correctly typed in.
 >> Make sure that the license key is the correct one.

"The function has already been enabled."
 >> Make sure that the Kit has not already been enabled.

4. Hold down the control panel power switch for 3 sec or more. Follow the instructions shown on the screen for shut-down sequence so that the main power switch may be turned off. Turn off the main power switch, wait for 10 sec, and turn it back on.

5. The registered license will become valid when the device is turned back on. When it has started normally, press

the Counter key, and click the Device Configuration button to make sure that the Kit is indicated as part of the options.

# Chapter 4 Maintenance

# Contents

# 4.1 Notes when service

## 4.1.1 Points to Note

If it becomes necessary to perform memory clear (MMI CLEAR) during service, then in order to save the user's network settings and address settings, etc., always make sure that you print out the user data list (network) and address lists, etc., from user mode. And, before printing out any address lists, make sure that you explain the need for this to the user and obtain the user's consent. Further, if it is possible to use a remote UI, exporting and backing up address lists, transfer setting and other user mode contents will assist in recovery in the event of any problems. For a user who uses two or more imageRUNNERs/iRs, use of the device information delivery, new feature, will be a good solution.

# 4.2 Troubleshooting

## 4.2.1 Troubleshooting

<u>0008-4679</u>

**<Troubleshooting procedures>**

Basic troubleshooting procedures related to the SEND function are described below.

Where an error message or error code is displayed, refer to the appended error list and check the appropriate countermeasure. The error list is divided by function, as per the following.

E-mail transmission/ I-Fax transmission/ I-Fax reception/ transmission/FTP transmission/NCP transmission.

When a problem occurs, the first step is to identify with which function the problem occurred and then check the error list for the appropriate countermeasure.

If the location of the problem cannot be identified form the error message or the error code, the following information may be of help in determining whether the cause is in the network, server or iR.

**<Network causes>**

Check the following items.

- Use the Ping command to check whether the appropriate IP address (an address that can be used to check whether the DNS server, SMTP server, POP server, etc, are operating properly) responds.

- If there is a response, move on to check whether the cause is in the server. If there is no response, check the network cable connection, the network board status and the network hub status. If a PC can be used, take the cable that is connected to the iR and connect it to the PC and try connecting to the network from the PC. If connection fails, it may be assumed that there is a problem on the network side.

- With SMB transmission, it is sometimes the case that transmission on the PC to the network is possible but reference is not. In that case, it is necessary to gather information about the user's operating environment. The following is an example of the user's operating environment and possible cause and countermeasure, when it is not possible to reference.

**Reference information:**

**Operating environment when SMB browsing (reference) is not possible**

When transmitting files with SMB with the following operating environment, it is sometimes the case that the addressee's browsing (reference) function does not work well.

- Around 50 PCs (Windows XP/Windows 2000/Windows 98/Mac OS) all obtain IP addresses via DHCP. There is no domain controller or other server and the network is made up of 10 work groups.

Problems likely to occur with this kind of set up include, with regard to SMB browsing (reference) from iR,

- even if referencing is performed, there is absolutely no display,

- the function extends as far as the work groups, but some work groups are excluded.

**How this problem is caused**

The Windows network automatically assigns one machine in each work group as the master browser. However, in the above environment (each PC gets its IP address from DHCP and there is no server) the assignation of the master

browser may become unstable. The IP addresses obtained from DHCP sometimes change and there are periods where the master browser cannot be assigned because PCs are being switched off and on, so the information being held by the master browsers gets mixed up, leading to the problems described above. In this environment, even if a WINS server is programmed, in work group browsing there is no query made to the WINS server. This is because the WINS server does not return work group related lists or computer lists.

**Workaround**

There is no complete workaround, but the following measures may help to enable slightly more stable SMB browsing. If possible, the user's network administrator should be requested to perform these measures.

1) Set Additional Functions > System Settings > SMB Server Settings > Use SMB Server > Workgroup. This means that iR will always query the master browser of the programmed work group.

2) In the Windows 98 network properties in the work group, set the master browser 'invalid'.
This setting will stop Windows 98 from becoming the master browser. However, each work group will need to have Windows XP/Windows present and they must always be in operating condition.

3) Make Windows NT server and Windows 2000 server the domain controller, or as a stand alone server, run with a static IP address.
There may be difficulties, depending on the user's operating conditions, but these measures will help to make the SMB browser most stable.

**SMB FAQs**

Q1. Where does the work group name and domain name information come from?
A1. The work group name and domain name information comes from the master browser. Before the information is obtained, the master browser on the network needs to be retrieved. This search and retrieval sequence is as described below.

With no work group set in iR
1) Search (broadcast) for the master browser without specifying the work group.
2) Any work group master browser that exists within the scope of the broadcast will respond.
3) Select the first master browser that responds as the query address.

With a work group name specified in iR
1) Specify the work group name and search (broadcast) for the master browser.
2) Only the master browser in the specified work group will respond.
3) Set this master browser as the query address.

Q2. How is the computer name decided?
A2. The answer depends on whether you are talking about B-Node (Broadcast Node) or H-Node(Hybrid Node :when WINS is programmed).

For B-Node

1) A query is made in the broadcast.

2) If there is no response to step 1), a query is made to the DNS server (assuming that the DNS server has been programmed).

For H-Node

1) A query is made directly to the WINS server.

2) If an error is returned by the WINS server, a query is made in the broadcast.

3) If there is no query made in the broadcast, an attempt is made to verify whether the address server is designated in the IP address.  If the IP address is thus identified, direct communication begins.

4) If the IP address is not identified in step 3), a query is made to the DNS server (assuming that the DNS server has been programmed).

**\<Server causes\>**

Check the following items.

- Launch the PC's mail client application (Outlook Express, etc.) and use the POP account being used in iR to check whether mail can be sent and received.

- If mail can be sent and received, assume that the server is working properly and check for likely iR problems.  If mail cannot be sent, there is a problem with the SMTP and DNS server.  If mail cannot be received, the problem is with the POP server.  Note that, if SMTP reception is performed, there is a problem in the SMTP server and the DNS server.

- Attempt to access the folder to be transmitted by SMB from the PC.  If access is not possible, check the common settings of the folder.  To transmit files with iR, write privileges for the folder are required.

- When the WindowsXP firewall function is active or some application restricting port access has been installed, the port used in SMB can be made available.

- Settings in the user mode can enable 2 byte code to be used in the FTP server.  However, if this is not supported on the server side, it will not operate.  Therefore, check that the server side has been programmed to allow 2 byte code.

Following are descriptions of some of the kinds of problems that may be expected with the servers.

- Check that the SMTP server, DNS server is working properly.  If using POP before SMTP, also check the POP server operation.

- If the server itself is working, there may be errors in the settings.  Check whether mail transmission/ reception is possible from another mail account.  If mail transmission/ reception is possible from another mail account, reset the POP authentication or SMTP authentication account.  In the case of SMTP reception, if the iR host name is not recorded in the DNS server as an MX record, mail cannot be sent to iR, so it is necessary to check that DNS registration has been made.

**\<Likely problems with iR\>**

- If transmission from the PC is normal, check again whether those settings match the iR settings.

- If the registration contents of the primary DNS server do not match those of the secondary DNS server, in some cases operation with the PC will be normal while operation with the iR will not.  This is appears to be because, if the PC is not registered in the primary DNS, the secondary DNS is then referenced.  However, if iR is not found in the primary, the search ends at that point.

- When the SMTP server and the POP server are used with the host name (FQDN) entered, it may be possible that a

problem has arisen with the DNS not being able to solve the name.  In that case, when registering on the server, try entering the IP address directly, instead of the host name (FQDN).

- If the network connection Ethernet driver settings are on automatic, it may be that problems of affinity with the hub may cause improper operation.  In that case, using manual settings to change the network connection speed and semi-duplex/ full duplex settings may restore normal operation.  On the other hand, if the settings are manual, it may be that they do not match the network environment and communication is, therefore, disabled.

- If the problem still cannot be resolved, it may be possible to resolve the problem by capturing the iR communication packets.  In that case, it will be necessary to get the approval of the user.  When the packets are being filtered, it is the MAC address that is used for filtering, not the IP address.  If the IP address is used, some packets, such as broadcast, etc., cannot be captured.

# 4.3 Related Error code

## 4.3.1 E-mail Transmission errors

<E-mail transmission error message and error codes>
#713, #810, #813, #839, #841, #842, #843, #844, #845, #846 are new error codes.

T-4-1

| Message | Error code | Cause | Remedy |
|---------|-----------|-------|--------|
| No message | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |
| Transmission cancelled | #099 | A user canceled the transmission. | - Check Address Book. If the error insists, turn the power off and on. |
| The number of transmission standby documents must be reduced. | #702 | HD full (work area) | - Wait a while then retry.<br>- Stop broadcast transmission with other protocols. This sometimes helps to avoid this problem. |
| The number of transmission standby documents and BOX documents must be reduced. | #703 | HD full (work area) | - Wait a while then retry.<br>- Delete documents from the BOX to free up HD space. |
| The address is not in the address list. | #704 | Address book search error. | - Check the address book settings. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| Data size too big. | #705 | Transmission data size too big. | - Reduce number of pages for transmission or lower resolution.<br>- Reset user mode transmission upper limit. |
| Address table not available. | #706 | Address book locked. | - Address book cannot be referenced as it is being used by remote UI.<br>- Address book cannot be referenced as it is being used by other transmission components. |
| URL sending error | #713 | The document stored in Mail Box has been deleted before the URL transmission. | - Do not delete the document in Mail Box.<br>- Send the document again. |
| No connection | #752 | DNS/SMTP server setting error (SMTP connection error) | Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server) |
| No response | #753 | Network error(Socket Write,Selecterror, etc.) | - Check cable and connectors. |
| Check TCP/IP | #755 | - IP address set to 0.0.0.0. In the following two situations, the IP address is 0.0.0.0.<br>1) Address could not be obtained from DHCP, BOOTP, RARP.<br>2) Unit launched in IP fixed mode(keys 1+7 to enter FIXIPmode).<br>- TCP/IP protocol stack resources insufficient. Even with internal retry (5 times), transmission failed. | - Set the IP address correctly or set DHCP, RARP, BOOTP environments to operate properly.<br>- Turn power OFF/ON. |
| Check server | #801 | SMTP protocol error/ command timeout | - Check mail server<br>- Check the network traffic. |
| Cannot find server | #802 | DNS/SMTP setting error(DNS error) | Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server) |
| Check address | #806 | Incorrect address (address wrongly searched on SMTP protocol) | Check address |

| Message | Error code | Cause | Remedy |
|---------|-----------|-------|--------|
| POP server connection error | #810 | Cannot connect to POP server when attempting POP Before SMTP transmission. | - Reprogramme user mode settings (POP, DNS server name)<br>- Check POP server operation.<br>- Check DNS server operation. |
| POP server address error | #813 | Password, user account error when attempting POP Before SMTP transmission. | - Check POP user name, password.<br>- Check POP server account. |
| No display | #830 | DSN error notification received.  The DSN error notification is sent to the transmission source by the SMTP server and the iR machine programmed for SMTP reception during an ESMTP-enabled transfer path whenever the destination address and the other party's conditions settings are wrong, or when the transmitted document's data size exceeds the permitted SMTP server range. | - Check the destination address.<br>- Set the transmission data size so that it does not exceed the SMTP server's limit.<br>- Programme the transmission other party's conditions so that they can be processed by the receiver. |
| No display | #834 | MDN error notification received.  The MDN error notification is sent to the transmission source as a transmission result in the mail header when the final processing of a mail sent in I-Fax Full mode fails in the iR reception machine. | - Programme the transmission other party conditions so that they can be processed by the receiver.<br>- Check that the receiver memory is not full.<br>- Correct the cause of reception image decoding failure. |
| SMTP server authentication error | #839 | Error occurred with password, user name and/or account when attempting SMTP AUTH transmission. | - Check SMTP authentication user name, password.<br>- Check SMTP server account. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| SSL encoding error | #841 | Because there is no encoding algorithm in common with the mail server, error occurred when attempting SSL encoded transmission. | - Stop SSL encoded transmission.<br>- Change mail server settings and add encoding algorithm. |
| SSL encoding error | #842 | The mail server has requested client authentication, which is an unsupported function, and an error was generated when SSL transmission was attempted. | - Change the mail server settings so that client authentication is not requested.<br>- Stop using SSL encoded transmissions. |
| SMTP authentication error | #843 | In SMTP authentication using GSSAPI, there is a significant difference (more than 5 minutes) in the time set in the KDC (Key DistributionCenter) server and that set in the iR, causing SMTP authentication, using GSSAPI, to fail. | - Correct the time settings on the machine.<br>- Check the time zone and summer time settings.<br>- Correct the KDC server time settings. |
| SSL encoding error(POP) | #844 | In a transmission using POP Before SMTP, the device attempted SSL encryption communications but an error occurred in the communications and failed in POP authentication. | - Check the settings for encrypted SSL communications in the POP server.<br>- Turn Allow SSL (POP) option off in Additional Functions not to use SSL encryption function for communications with the POP server.<br>- Turn POP Authentication before Sending option off not to use POP Before SMTP. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| POP AUTH authentication error | #845 | In an email or I-Fax transmission using POP Before SMTP, the device attempted POP Auth but an error occurred in the POP server and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the POP authentication settings in the POP server.<br>- Cancel the selection of POP AUTH for POP AUTH Method.<br>- Turn POP Authentication before Sending option off not to use POP Before SMTP. |
| APOP authentication error | #846 | In an email or I-Fax transmission using POP Before SMTP, the device attempted APOP of POP authentication but an error occurred in the APOP authentication and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the APOP settings in the POP server.<br>- Cancel the selection of APOP for POP AUTH Method.<br>- Turn POP Authentication before Sending option off not to use POP Before SMTP. |
| No display | #899 | Operation completed normally. | This error code indicates that transmission as far as the SMTP server was completed normally, but delivery cannot be confirmed. Except when delivery confirmation is performed in I-Fax Full mode, confirmation is displayed on the I-Fax/E-Mail transmission side. The only way to judge whether transmission has been completed normally is to see whether there has been an error mail reception printout. |
| Cancelled. | #995 | Transmission cancelled | - Retransmit as necessary. |

<Memo>

This model does not have an E-Mail reception function, only an error mail reception function. Therefore, it can only print out text and i-Fax compliant TIFF attachments. PDF and JPEG files cannot be printed out.

## 4.3.2 I-Fax Transmission errors

<u>0008-4682</u>

<I-Fax transmission error message and error codes>
#810, #813, #839, #841, #842, #843, #844, #845, #846 are new error codes.

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No display | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |
| No display | #099 | A user canceled the transmission. | - Send the data again. |
| The number of transmission standby documents must be reduced. | #702 | HD full (work area) | - Wait a while then retry.<br>- Stop broadcast transmission with other protocols. |
| The number of transmission standby documents and BOX documents must be reduced. | #703 | HD full (work area) | - Wait a while then retry.<br>- Stop broadcast transmission with other protocols.<br>- Delete documents from the BOX to free up HD space. |
| The address is not in the address list. | #704 | Address book search error. | - Check the address book settings. |
| Data size too big. | #705 | Transmission data size too big. | - Reduce number of pages for transmission or lower resolution.<br>- Image data size for one page has exceeded the user mode setting.<br>- Reset user mode transmission upper limit. |
| Address table not available. | #706 | Remote UI or other transmission components using address book, so it cannot be referenced. | - Wait a while then retry. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No connection | #752 | DNS/SMTP server setting error (SMTP connection error) | - Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server) <br> - Check that the SMTP server is operating properly. |
| No response | #753 | Network error(Socket Write,Selecterror,etc.) | Check cable and connectors. |
| Check TCP/IP | #755 | - IP address set to 0.0.0.0. In the following two situations, the IP address is 0.0.0.0. <br> 1) Address could not be obtained from DHCP, BOOTP, RARP. <br> 2) Unit launched in IP fixed mode(keys 1+7 to enter FIXIPmode). <br> - TCP/IP protocol stack resources insufficient. Even with internal retry (5 times), transmission failed. | - Set the IP address correctly or set DHCP, RARP, BOOTP environments to operate properly. <br> - Turn power OFF/ON. |
| Check server | #801 | Error returned from SMTP server during SMTP session. Or, command timeout error generated. | -Check mail server <br> -Check the network traffic. |
| Cannot find server | #802 | DNS/SMTP setting error(DNS server connection error) | Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server)Check that the DNS server is operating normally. |
| Check address | #806 | Address wrongly searched on SMTP protocol. | Check address |
| POP server connection error | #810 | Cannot connect to POP server when attempting POP Before SMTP transmission. | - Reprogramme user mode settings (POP, DNS server name) <br> - Check POP server operation. <br> - Check DNS server operation. |
| POP server address error | #813 | Password, user account error when attempting POP Before SMTP transmission. | - Check POP user name, password. - Check POP server account. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No display | #830 | DSN error notification received. The DSN error notification is sent to the transmission source by the SMTP server and the iR machine programmed for SMTP reception during an ESMTP-enabled transfer path whenever the destination address and the other party's conditions settings are wrong, or when the transmitted document's data size exceeds the permitted SMTP server range. | - Check the destination address.<br>- Set the transmission data size so that it does not exceed the SMTP server's limit.<br>- Programme the transmission other party's conditions so that they can be processed by the receiver. |
| No display | #834 | MDN error notification received. The MDN error notification is sent to the transmission source as a transmission result in the mail header when the final processing of a mail sent in I-Fax Full mode fails in the iR reception machine. | - Programme the transmission other party conditions so that they can be processed by the receiver.<br>- Check that the receiver memory is not full.<br>- Correct the cause of reception image decoding failure. |
| SMTP server authentication error | #839 | Error occurred with password, user name and/ or account when attempting SMTP AUTH transmission. | - Check SMTP authentication user name, password.<br>- Check SMTP server account. |
| SSL error(SMTP Send) | #841 | Because there is no encoding algorithm in common with the mail server, error occurred when attempting SSL encoded transmission. | - Stop SSL encoded transmission.<br>- Change mail server settings and add encoding algorithm. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| SSL error(SMTP Send) | #842 | The mail server has requested client authentication, which is an unsupported function, and an error was generated when SSL transmission was attempted. | - Change the mail server settings so that client authentication is not requested.<br>- Stop using SSL encoded transmissions. |
| SMTP authentication error | #843 | In SMTP authentication using GSSAPI, there is a significant difference (more than 5 minutes) in the time set in the KDC (Key DistributionCenter) server and that set in the iR, causing SMTP authentication, using GSSAPI, to fail. | - Correct the time settings on the machine.<br>- Check the time zone and summer time settings.<br>- Correct the KDC server time settings. |
| SSL error(POP) | #844 | In a transmission using POP Before SMTP, the device attempted SSL encryption communications but an error occurred in the communications and failed in POP authentication. | - Check the settings for encrypted SSL communications in the POP server.<br>- Turn Allow SSL (POP) option off in Additional Functions not to use SSL encryption function for communications with the POP server. - Turn POP Authentication before Sending option off not to use POP Before SMTP. |
| POP AUTH encryption error | #845 | In an email or I-Fax transmission using POP Before SMTP, the device attempted POP Auth but an error occurred in the POP server and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the POP authentication settings in the POP server.<br>- Cancel the selection of POP AUTH for POP AUTH Method.<br>- Turn POP Authentication before Sending option off not to use POP Before SMTP. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| APOP encryption error | #846 | In an email or I-Fax transmission using POP Before SMTP, the device attempted APOP of POP authentication but an error occurred in the APOP authentication and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the APOP settings in the POP server.<br>- Cancel the selection of APOP for POP AUTH Method.<br>- Turn POP Authentication before Sending option off not to use POP Before SMTP. |
| No display | #899 | Operation completed normally. | This error code indicates that transmission as far as the SMTP server was completed normally, but delivery cannot be confirmed. Except when delivery confirmation is performed in I-Fax Full mode, confirmation is displayed on the I-Fax/E-Mail transmission side. The only way to judge whether transmission has been completed normally is to see whether there has been an error mail reception printout. |
| Cancelled. | #995 | Transmission cancelled | - Retransmit as necessary. |

## 4.3.3 I-Fax Reception errors

0008-4683

<I-Fax reception error message and error code list>

T-4-3

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| POP server UIDL error | | POP server UIDL commands not supported | - Change POP server. |
| POP server address error | | POP server error (account) | - Reprogramme user mode settings (account).<br>- Check POP server account. |
| POP server address error | | POP server error (password) | - Reprogramme user mode settings (password).<br>- Check POP server account. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| POP server connection error | | Cannot connect to POP server. | - Reprogramme user mode settings (POP, DNS server name)<br>- Check POP server operation.<br>- Check DNS server operation. |
| Check TCP/IP. | | Incorrect IP address. | - Reprogramme IP address and turn power OFF/ON.<br>- Check DHCP, RARP, BOOTP server operations and turn power OFF/ON. |
| Connect cable. | | SMTP initialisation error | - Check network and network card.<br>- Turn power OFF/ON. |
| No response | | Mail server error | - Check mail server operation. |
| Cannot receive | | Reception refused | - Clear any operator call error, such as no paper, etc.<br>- Receive reception JOBs into memory reception BOX.<br>- Delete transmitting JOBs. |
| SSL Error (SMTP Receive) | | Error in encrypting SSL to receive in SMTP | - Mismatched SSL algorithm. Check the server certificate and the settings in the SSL client. |
| SSL Error (SMTP RX Reject) | | The option that allows only SSL communications is selected. | - Change Allow SSL (SMTP Receive) setting from SSL to On or Off in Additional Functions.<br>- Change the settings to use SSL in the client. |
| SSL Error (POP) | | The device attempted to communicate with the POP server in SSL but an error occurred in SSL encryption communications and failed in POP authentication. | - Check the settings for encrypted SSL communications in the POP server.<br>- Turn Allow SSL (POP) option off in Additional Functions not to use SSL encryption function for communications with the POP server. |
| POP AUTH Encryption Error | | The device attempted POP Auth but an error occurred in the POP server and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the POP authentication settings in the POP server.<br>- Cancel the selection of POP AUTH for POP AUTH Method. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| APOP Authentication Error | | The device attempted APOP of POP authentication but an error occurred in the APOP authentication and failed in POP authentication. | - Check POP Address and POP Password settings of Additional Functions.<br>- Check the APOP settings in the POP server.<br>- Cancel the selection of APOP for POP AUTH Method. |
| The number of transmission standby documents must be reduced. | #702 | HD full(work area) | - Stop all jobs operating simultaneously.  Or, wait a while until the HD area is freed up. |
| The number of transmission standby documents and BOX documents must be reduced. | #703 | HD full(work area) | - Delete documents from the BOX to free up HD space and decrease number of transmission standby documents in the BOX. |
| Check server | #801 | Timeout (1KByte/ 10 sec.) during SMTP data reception. | - Check SMTP server operation.<br>- Check network traffic conditions. |
| Cannot find server | #802 | DNS/SMTP setting error(DNS error) | Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server) |
| POP server connection error | #810 | Timeout (1KByte/ 10 sec.) during POP data reception. | - Check user mode POP server settings.<br>- Check POP server operation.<br>- Check network traffic conditions. |
| No message. Error reason given on reception error report. | #818 | File attachment is in unprintable format. | - Contact sender and arrange for them not to transmit image data that is not supported by I-Fax. |
| No message. Error reason given on reception error report. | #819 | MIME information error | - Nothing in particular.Contact the sender and have them output the error information and error dump. |

| Message | Error code | Cause | Remedy |
|---------|-----------|-------|--------|
| No message. Error reason given on reception error report. | #820 | BASE64 or uuencode error | - Nothing in particular.Contact the sender and have them output the error information and error dump. |
| No message. Error reason given on reception error report. | #821 | TIFF analysis error | - Nothing in particular.Contact the sender and have them output the error information and error dump. |
| No message. Error reason given on reception error report. | #822 | Image decode error | - Nothing in particular.Contact the sender and have them output the error information and error dump. |
| No message. Error reason given on reception error report. | #827 | Unsupported MIME | - Contact sender and ask them not to transmit data that cannot be received. |
| No message. Error reason given on reception error report. | #828 | HTML format file attachment | - Contact sender and ask them not to transmit data that cannot be received. |
| No message. Error reason given on reception error report. | #829 | Reception document exceeds 1000 pages. | - Contact the sender and have them limit the number of pages in a single transmission to 999. |
| No message. | #831 | SMTP connection cut by IP block function. | - Reprogramme the IP address of the IP block function that allows SMTP connection. |
| No message. | #832 | Problem with receiving unit's transmission settings. DSN transmission failed. | - Check the SMTP/DNS server, domain name, host name, E-Mail address, IP address, netmask and default gateway settings in user mode.<br>- Check mail server/ DNS server operation. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No message. | #833 | Problem with receiving unit's transmission settings. MDN transmission failed. | - Check the SMTP/DNS server, domain name, host name, E-Mail address, IP address, netmask and default gateway settings in user mode.<br>- Check mail server/ DNS server operation. |
| No message. | #835 | Text reception line count error. | - Have the sender reduce the number of lines in the text. |

## 4.3.4 SMB Transmission errors

0008-4684

<SMB transmission error message and error code list>

T-4-4

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No message | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |
| Transmission cancelled | #099/ #995 | - Transmission cancelled by user. | Resend. |
| Address does not appear in address list. | #704 | - An error occurred when address information was being obtained from the address list.  (Address deleted from list after scanning, etc.) | - Check address list settings. Or, turn unit OFF/ON. |
| HD full | #702 | Operation stopped because HD full (work area). | - Wait a while then retry.<br>- Stop broadcast transmission with other protocols.  This sometimes helps to avoid this problem. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| HD full | #703 | Operation stopped because HD full (image area). | - Wait a while then retry.<br>- Stop broadcast transmission with other protocols.  This sometimes helps to avoid this problem. |
| Address table not available | #706 | - Address table being imported/ exported from RUI.<br>- Address book usage doubled up with other transmission component (Fax, etc.). | - Quit access from RUI.<br>- Wait a while and then retry |
| No response | #751 | - Server has not booted up.<br>- Network disconnected. (If connection cannot be made with transmission destination, connection is sometimes cut mid-way.)<br>- Reset caused by internal error.  Processing interrupted. | - Check transmission destination and network settings.<br>- Transmission jobs whose processing has stopped for some reason or other are forced to quit by assigning an internal error code (#751).  As a result, after rebooting, the job is not run. |
| TCP/IP error | #755 | - IP address set to 0.0.0.0. In the following two situations, the IP address is 0.0.0.0.<br>1) Address could not be obtained from DHCP, BOOTP, RARP.<br>2) Unit launched in IP fixed mode(keys 1+7 to enter FIXIPmode).<br>- TCP/IP protocol stack resources insufficient. Even with internal retry (5 times),transmission failed. | - Set the IP address correctly or set DHCP, RARP, BOOTP environments to operate properly.<br>- Turn power OFF/ON. |

| Message | Error code | Cause | Remedy |
|---------|-----------|-------|--------|
| Check server | #801 | - Error generated due to cause on server side. <br> - SMB server side file capacity not sufficient. <br> - In WindowsNT/2000 server, password was incorrect. <br> - In WindowsNT SMB, common file name did not match. <br> - In SMB, a user exists but no write privileges. <br> - SMB transmission made to write-prohibited file of the same name. | - Reset server. <br> - Check server status and settings. <br> - Check the network traffic. |
| Cannot find server | #802 | DNS/SMTP setting error(DNS error) | Reprogramme the user mode settings. (domain name, E-Mail address, DNS, mail server) |
| Check address | #804 | - No match for specified directory name. <br> - In SMB, a user exists but no write privileges. | - Check that the destination directory name is correct. <br> - Set directory access privileges in the server. |
| Check address. | #806 | - Wrongly specified user name. <br> - Wrongly specified password. (Excl. Windows NT.) | - Change address book user name or password. |
| No messag | #807 | No access rights for the specified directory | - Check the access rights to the server. |

<Memo>

From iR C3200 onward, including this model, NTLM authentication (NTLM 0.12) is supported.

In SMB transmission, in place of plain text authentication, NTLM encoded authentication is supported. This means that by specifying the user name as "domain name\user name" in file transmission, the transmission can be carried out with the user privileges of the specified domain. Also, transmission can be made to access mode common folders at user level in Win9x OS.

Note: With this function, NAS (Network Attached Stage) and Linux SAMBA folders can now be transmitted. However, this is not guaranteed for all environments, so it is essential to check transmission in the user's operating environment, before delivery.

# 4.3.5 FTP Transmission errors

0008-4685

<FTP transmission error message and error code list>

T-4-5

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No message | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |
| Transmission cancelled | #099/ #995 | - Transmission cancelled by user. | Resend. |
| HD full | #702 | Operation stopped because HD full (work area). | - Wait a while then retry. Stop broadcast transmission with other protocols. This sometimes helps to avoid this problem. |
| HD full | #703 | Operation stopped because HD full (image area). | - Wait a while then retry. Stop broadcast transmission with other protocols. This sometimes helps to avoid this problem. |
| Address does not appear in address list. | #704 | - An error occurred when address information was being obtained from the address list. (Address deleted from list after scanning, etc. ) | - Check address list settings. Or, turn unit OFF/ON. |
| Address table not available | #706 | - Address table being imported/ exported from RUI.<br>- Address book usage doubled up with other transmission component (Fax, etc.). | - Quit access from RUI.<br>- Wait a while and then retry |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No response | #751 | - Server has not booted up.<br>- Network disconnected.<br>(If connection cannot be made with transmission destination, connection is sometimes cut mid-way.)<br>- No Tree name entered.<br>- Reset caused by internal error. Processing interrupted. | - Check transmission destination and network settings.<br>- Enter Tree name.<br>- Transmission jobs whose processing has stopped for some reason or other are forced to quit by assigning an internal error code (#751). As a result, after rebooting, the job is not run. |
| TCP/IP error | #755 | - IP address set to 0.0.0.0. In the following two situations, the IP address is 0.0.0.0.<br>1) Address could not be obtained from DHCP, BOOTP, RARP.<br>2) Unit launched in IP fixed mode(keys 1+7 to enter FIXIPmode).<br>- TCP/IP protocol stack resources insufficient. Even with internal retry (5 times), transmission failed. | - Set the IP address correctly or set DHCP, RARP, BOOTP environments to operate properly.<br>- Turn power OFF/ON. |
| Check server | #801 | - Error generated due to cause on server side.<br>- In NetWare,a user exists but no read or write privileges.<br>- Transmission made to write-prohibited file of the same name. | - Reset server.<br>- Check server status and settings.<br>- Check the network traffic. |
| Cannot find server | #802 | - The IP address for DNS server is not set up.<br>- DNS Server is not running.<br>- No appropriate host name is found in the DNS server. | - Check the DNS server. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| Check address | #804 | - No match for specified directory name.<br>- No access privileges for that directory. | - Check that the destination directory name is correct.<br>- Set directory access privileges in the server.<br>- Send to different directory with access privileges. |
| Check address. | #806 | - Wrongly specified user name.<br>- Wrongly specified password.<br>- In NetWare, the host name is incorrect. | - Change address book user name or password. |
| No message | #807 | No access rights for the specified directory | - Check the access rights to the server. |
| No connection | #815 | - Login is made from this unit in NetWare's Pserver mode (NDS/ Bindery common) and login is attempted again for NCP, while the server is printing. | - Wait a while and try again.<br>- Change the destination NetWare server.<br>- Stop Pserver. |

# 4.3.6 NCP Transmission errors

0008-4686

<NCP transmission error message and error code list>

T-4-6

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No message | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| Transmission cancelled | #099/ #995 | - Transmission cancelled by user. | Resend. |
| Address does not appear in address list. | #704 | - An error occurred when address information was being obtained from the address list. (Address deleted from list after scanning, etc.) | - Check address list settings. Or, turn unit OFF/ON. |
| HD full | #702 | Operation stopped because HD full (work area). | - Wait a while then retry. Stop broadcast transmission with other protocols. This sometimes helps to avoid this problem. |
| HD full | #703 | Operation stopped because HD full (image area). | - Wait a while then retry. Stop broadcast transmission with other protocols. This sometimes helps to avoid this problem. |
| Address table not available. | #706 | - Address table being imported/ exported from RUI. <br> - Address book usage doubled up with other transmission component (Fax, etc.). | - Quit access from RUI. <br> - Wait a while and then retry |
| No response | #751 | - Server has not booted up. <br> - Network disconnected. (If connection cannot be made with transmission destination, connection is sometimes cut mid-way.) <br> - No Tree name entered. <br> - Reset caused by internal error. Processing interrupted. | - Check transmission destination and network settings. <br> - Enter Tree name. <br> - Transmission jobs whose processing has stopped for some reason or other are forced to quit by assigning an internal error code (#751). As a result, after rebooting, the job is not run. |
| Net Ware error | #756 | NetWare option is turned off in Additional Functions. | Turn NetWare option on in Network Settings, System Settings, Additional Functions. |

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| Check server | #801 | - Error generated due to cause on server side.<br>- In NetWare, a user exists but no read or write privileges.<br>- Transmission made to write-prohibited file of the same name. | - Reset server.<br>- Check server status and settings.<br>- Check the network traffic. |
| Check address | #804 | - No match for specified directory name.<br>- No access privileges to the directory. | - Check that the destination directory name is correct.<br>- Set directory access privileges in the server.<br>- Send to different directory with access privileges. |
| Check address. | #806 | - Wrongly specified user name.<br>- Wrongly specified password.<br>- In NetWare, the host name is incorrect. | - Change address book user name or password. |
| No message | #807 | No access rights for the specified directory | - Check the access rights to the server. |
| No connection | #815 | - Login is made from this unit in NetWare's Pserver mode (NDS/ Bindery common) and login is attempted again for NCP, while the server is printing. | - Wait a while and try again.<br>- Change the destination NetWare server.<br>- Stop Pserver. |

# 4.3.7 Box Transmission errors

0008-5758

<BOX transmission error message and error code list>

| Message | Error code | Cause | Remedy |
|---|---|---|---|
| No message | #022 | Address deleted or invalidated during transmission reservation. | - Retransmit deleted address.<br>- Check that a group address is specified as the transfer destination and that it contains a valid address.<br>- Check that a group address is specified as the transfer destination and whether it contains local print or fax box only.<br>- Check whether the specified transfer destination address has been deleted. |
| Transmission cancelled | #099/ #995 | - Transmission cancelled by user. | Resend. |
| Address table not available. | #706 | - Address table being imported/ exported from RUI.<br>- Address book usage doubled up with other transmission component (Fax, etc.). | - Quit access from RUI.<br>- Wait a while and then retry |
| No message | #711 | Full in memory for User Inboxes | Delete stored documents in Mail Boxes. |
| No message | #712 | The number of documents for a box reaches to the maximum | Delete stored documents in Mail Box that contains the maximum number of documents. |

# 4.4 Related Service Mode

## 4.4.1 Related Service Modes List

Following is an overview of the service modes related to the SEND function.

**Preconditions:**

- These service modes are found in COPIER>OPTION>BODY.

- All are Level 2 service modes.

- Service modes marked with an asterisk (*) are new service modes.

T-4-8

| Item | Setting name | Description |
|------|--------------|-------------|
| I-Fax reception raw data print | RAW-DATA | 0: Ordinary reception mode(default) <br> 1: Received I-Fax content printed out as is (in order to judge whether data are correct). |
| I-Fax reception output line count limit | IFAX-LIM | When large volume data (error mail, etc.) are received via I-Fax, the output line count is restricted (default: 500). <br> NB: If the setting is 0, there is no restriction. |
| No limitation on file size for I-Fax serverless transmission. | IFAX-SZL* | 0: Enables Limitation on file size for serverless transmission. <br> 1: Disables Limitation on file size for serverless transmission. |
| Divided page transmission in I-Fax simple mode | IFAX-PGD* | 0: Does not allow divided page transmission in I-Fax simple mode <br> 1: Allows divided page transmission in I-Fax simple mode |
| SMTP transmission port number | SMTPTXPN | TCP port number used by SMTP transmission (default:25) |
| SMTP reception port number | SMTPRXPN | TCP port number used by SMTP reception (default:25) |
| POP3 port number | POP3N | TCP port number used by POP (default:110) |
| FTP transmission port number | FTPTXPN | TCP port number used by FTP transmission (default:25) |
| CRAM-MD5 authentication restrictions with SMTP / POP AUTH authentication | NS-CMD5* | 0: Permit CRAM-MD5 authentication when performing SMTP / POP AUTH authentication. (Default) <br> 1: Prohibit CRAM-MD5 authentication when performing SMTP authentication. |

| NTLM authentication restrictions with SMTP / POP AUTH authentication | NS-NTLM5* | 0: Permit NTLM authentication when performing SMTP / POP AUTH authentication. (Default)<br>1: Prohibit NTLM authentication when performing SMTP / POP AUTH authentication. |
|---|---|---|
| GSSAPI authentication restrictions with SMTP / POP AUTH authentication | NS-GSAPI* | 0: Permit GSSAPI authentication when performing SMTP POP AUTH authentication. (Default)<br>1: Prohibit GSSAPI authentication when performing SMTP POP AUTH authentication. |
| PLAIN, LOGIN authentication restrictions with SMTP POP AUTH authentication when communication packets are encoded | NS-PLNWS* | When communication packets are encoded,<br>0: Permit PLAIN, LOGIN authentication when performing SMTP POP AUTH authentication. (Default)<br>1: Prohibit PLAIN, LOGIN authentication when performing SMTP POP AUTH authentication. |
| LOGIN authentication restrictions with SMTP POP AUTH authentication | NS-LGN* | 0: Permit LOGIN authentication when performing SMTP POP AUTH authentication. (Default)<br>1: Prohibit LOGIN authentication when performing SMTP POP AUTH authentication. |
| PLAIN, LOGIN authentication restrictions with SMTP POP AUTH authentication when communication packets are not encoded | NS-PLN* | When communication packets are not encoded,<br>0: Permit PLAIN, LOGIN authentication when performing SMTP POP AUTH authentication. (Default)<br>1: Prohibit PLAIN, LOGIN authentication when performing SMTP POP AUTH authentication. |

<Memo>

With regard to the new SMTP authentication-related user modes, usually there is no need to change these settings. These settings should be changed only when a particular authentication system is to be prohibited, depending on the server administrator's security policy.

## 4.4.2 Invalidating the License for Transfer to a Different Device (Level 2)

<span style="float:right">0008-5796</span>

**Service Mode Item Used to Invalidate a License for Transfer to a Different Device (Level 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 Level 2 so that the following is true:

COPIER>OPTION>LCNS-TR

The following screen appears, showing the current status of various options:
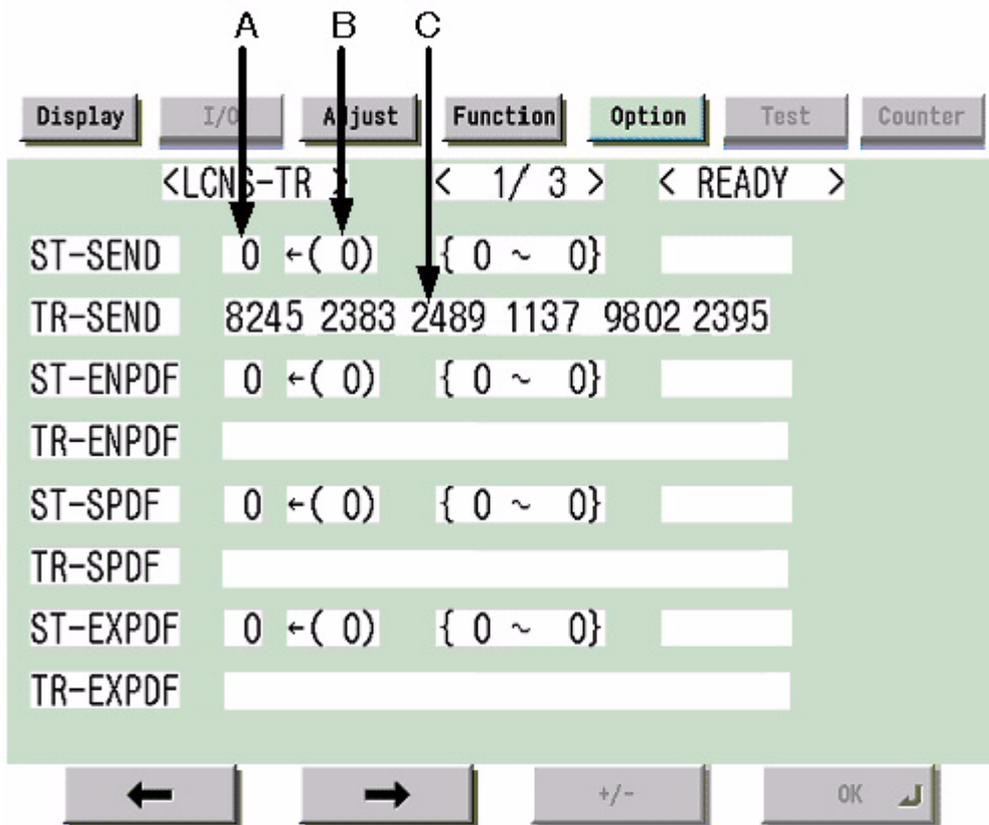


F-4-1

**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

**PDFDR:** PDF Direct print function

**SCR:** encryption secured printing (for future use)

**HDCLR:** HDD encryption + full deletion (Security Kit)

**BRDIM:** BarDIMM (for future use)

**VNC:** Remote Operators Software

**WEB:** Web Browser

**Memo:**
Not all foregoing options are available in all countries and regions.

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 22 2005

Canon