



MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS/
MULTIFUNCTIONAL DIGITAL SYSTEMS

High Security Mode Management Guide

ES9160 MFP/ES9170 MFP
ES9460 MFP/ES9470 MFP
CX3535 MFP/CX4545 MFP

Preface

Thank you for purchasing OKI Multifunctional Digital Systems.

This manual explains about the conditions and settings for using the Multifunctional Digital Systems which complies with IEEE Std 2600.1™-2009 *1.

Read this manual carefully before using your Multifunctional Digital Systems under the high security mode. For the security precautions on operating the equipment complying with IEEE Std 2600.1™-2009, refer to “Security Precautions” in the “Safety Information”.

Keep this manual within easy reach and use it to maintain the equipment complying with IEEE Std 2600.1™-2009.

■ How to read this manual

□ Symbols in this manual

In this manual, some important items are marked with the symbols shown below. Be sure to read these items before using this equipment.

 **WARNING** Indicates a potentially hazardous situation which, if not avoided, could result in death, serious injury, or serious damage, or fire in the equipment or surrounding assets.

 **CAUTION** Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, partial damage to the equipment or surrounding assets, or loss of data.

 **Note**

Indicates information to which you should pay attention when operating the equipment.

Other than the above, this manual also marks information that may be useful for the operation of this equipment with the following signs:

 **Tip**

Describes handy information that is useful to know when operating the equipment.



Pages describing items related to what you are currently doing. See these pages as required.

□ Applicable models

ES9160 MFP/ES9170 MFP

ES9460 MFP/ES9470 MFP

CX3535 MFP/CX4545 MFP

If the model name is written, precautions are applicable to the specified model. If no model name is written, precautions are applicable to the above models.

□ Explanation for control panel and touch panel

- The details on the touch panel menus may differ depending on the operating environment such as whether options are installed.
- The illustration screens used in this manual are for paper in the A/B format. If you use paper in the LT format, the display or the order of buttons in the illustrations may differ from that of your equipment.

□ Trademarks

- The official name of Windows XP is Microsoft Windows XP Operating System.
- The official name of Windows Vista is Microsoft Windows Vista Operating System.
- The official name of Windows 7 is Microsoft Windows 7 Operating System.
- The official name of Windows Server 2003 is Microsoft Windows Server 2003 Operating System.
- The official name of Windows Server 2008 is Microsoft Windows Server 2008 Operating System.
- Microsoft, Windows, Windows NT, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- Apple, AppleTalk, Macintosh, Mac, Mac OS, Safari, and TrueType are trademarks of Apple Inc. in the US and other countries.
- Adobe, Acrobat, Reader, and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Mozilla, Firefox and the Firefox logo are trademarks or registered trademarks of Mozilla Foundation in the U.S. and other countries.
- IBM, AT and AIX are trademarks of International Business Machines Corporation.
- NOVELL, NetWare, and NDS are trademarks of Novell, Inc.
- Other company and product names given in this manual or displayed in this software may be the trademarks of their respective companies.

CONTENTS

Preface	1
How to read this manual.....	1

Chapter 1 THE HIGH SECURITY MODE

Precautions on Using the High Security Mode	6
Confirmation of the mode	6
Operational conditions.....	7

Chapter 2 UNIQUE FUNCTIONS

Temporary Password	10
Conditions when a temporary password is used	10
Operation by a user when a temporary password is used	10
HOLD (FAX)	11

Chapter 3 THE INITIAL VALUES

Precautions on the Initial Values	14
Logging in.....	14
Initial value list.....	15

THE HIGH SECURITY MODE

Precautions on Using the High Security Mode	6
Confirmation of the mode	6
Operational conditions.....	7

Precautions on Using the High Security Mode

This operation mode protects customers' important information against unauthorized access to the equipment and leakage.

The following are the security functions when you operate the equipment complying with IEEE Std 2600.1™-2009.

- User Authentication Setting function
- Role Management function
- Encryption function of data to be written in HDD
- Log collecting and browsing function
- Overwriting function of the specified data in HDD when jobs are completed or the power is turned ON
- Communication function with SSL or TLS
- Integrity Check function
- Management functions such as:
Log, Passwords, User, Password Policy, Date & Time, Auto Clear, Session Timer, Enable/disable of SSL/LTS

To operate the equipment complying with IEEE Std 2600.1™-2009 under the high security mode, configurations according to the use environment, such as data or protocol encryption setting and setting for the connection only to the authorized server or client PC, are required.

Pay attention that if the conditions given in this manual are not met, you may not be able to operate the equipment complying with IEEE Std 2600.1™-2009.

Tip

For details of each security function and how to set the related items, refer to the TopAccess Guide.

Confirmation of the mode

When this equipment is operated under the high security mode,  is displayed on the touch panel of the equipment.



Tips

- The HDD inside the equipment which is operated under the high security mode is encrypted. Moreover, the Data Overwrite Option (GP-1070) is installed in such equipment.
To confirm that each function is operating, check the display at the top right of the [Counter] screen on the touch panel of the equipment.

The HDD is encrypted.	 The icon is displayed. Even in the case that it is not displayed, the HDD has been encrypted if this equipment has been operated under the high security mode.
The Data Overwrite Enabler is operating properly.	 The icon showing that the Data Overwrite Enabler is correctly operating is displayed. The version of the system (V1.0) is displayed.



- When the Data Overwrite Enabler is installed, the hard disk space temporarily used during job process will be used for another job after the data are overwritten.

Operational conditions

Select [MFP Local Authentication] for [Authentication Type] in [User Authentication]. If an SNTP server, LDAP server or DNS server is used for user authentication, the equipment is no longer complying with IEEE Std 2600.1™-2009.

When connecting the equipment from any of eFiling BackUp/Restore Utility, File Downloader, TWAIN Driver or Addressbook Viewer, enter an ID and password to log in. The password input is displayed in the blank symbols. In addition, you will be locked out if the password is input incorrectly a certain number of times.

Manually select [FULL] to perform integrity check.

* For details of the integrity check, refer to the MFP Management Guide.

Do not change the communication settings of the equipment from the initial values. Communication via a network can be protected by SSL if no such changes are made.

Set to OFF [MEMORY TX] under [USER FUNCTIONS] - [ADMIN] - [LIST/REPORT] - [REPORT SETTING] - [COMM. REPORT].

In the High Security Mode, the following functions cannot be used.

- Interrupt copy
- Network Fax
- Scheduled printing
- Storing to e-Filing from a printer driver*
 - * The function can be selected; however, an error occurs and the job is deleted. As a result, printing is not performed. When a job is deleted, it is recorded in the error log. Confirm it in the [Logs] tab on TopAccess or [JOB STATUS] - [LOG] - [PRINT] in the equipment.
- Disabling log authentication

The automatic log-in function in the client software which comes with this equipment is not available. Be sure to enter the user name and password when using client software.

Any data sent to this equipment, such as a Fax and Internet Fax printed or received from a printer driver*, can be outputted only when a user with the printing privilege is logged in.

* Use IPP SSL or SSL of WS Print for the communication with the equipment.

When IPP printing is performed, use the port created by entering “https://[IP address]:[SSL port number]/Print” into the URL field.

(e.g.: https://192.168.1.2:443/Print)

* For details, refer to [IPP printing] under [Installing the Printer Drivers] - [Other Installations] in the Software installation guide.

Do not use any applications which need a setting change of the [ODCA] sub menu in the [Setup] menu on the [Administration] tab under TopAccess.

To securely operate this equipment, we recommend you to observe the following items.

- Use the encrypted PDF format when saving or sending a file and the encryption level shall be 128 bit AES.
- Specify a reliable remote PC for the saving destination of the scan data.
- Do not use PUBLIC BOX in e-Filing since no password can be set.
- Do not use MFP LOCAL since no password can be set.
- When printing a Report by InternetFax, do not select “Print 1st page image” so that no copy of the original will be added.
- Use SMP Submission in [Print Share].
- Disable [Enable Raw TCP] and [Enable LPD] in Print Service.
- Administrators must regularly export and store the logs.
- Select [Disable] in [Twain Scanning].

UNIQUE FUNCTIONS

Temporary Password	10
Conditions when a temporary password is used	10
Operation by a user when a temporary password is used	10
HOLD (FAX)	11

Temporary Password

In the high security mode, a password, tentatively assigned by an administrator to allow a user access, is treated as a temporary one. To use the equipment, you need to register your password after accessing it with the temporary one.

Note

The security level is insufficient if you continue to use the temporary password. Register your password as soon as possible.

■ Conditions when a temporary password is used

A user temporary password is used in the following cases:

- For the first time to log in to the equipment after being registered by an administrator.
- When an administrator resets the user's password.
- When the user information password imported by an administrator is plain text.

Note

When an administrator resets users' passwords, they must be so notified and prompted to change them to ones of their own choosing.

Tip

To prevent user information exported from an equipment from being altered, it is hashed. If you change the password for the exported user information, plain text is used for the password.

■ Operation by a user when a temporary password is used

If your password can be registered when accessing.

When you access the equipment from the control panel or the following utilities, you can immediately register your password. After the registration, you can use the functions for which you have the privilege.

- Control panel
- TopAccess

When you access the equipment with a temporary password from the control panel or TopAccess, a message indicating that you are using a temporary password is displayed. After the confirmation, a window to register your new password is displayed. Enter a new password in this window, do so again for confirmation, and then press [OK] (control panel) or [Save] (TopAccess) to register it. You can log in to the equipment with this registered password from the next time.

If you cannot register a new password when accessing the equipment.

In the following utilities, an error occurs when you try to log in to the equipment with a temporary password. Therefore a new password cannot be registered either. Before using these utilities, register a new password on the control panel or in TopAccess.

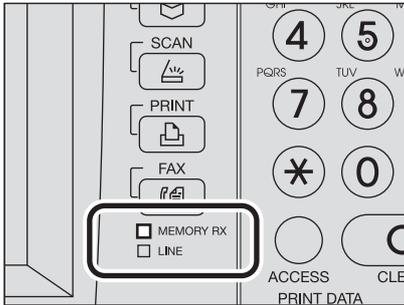
- Remote Scan driver
- e-Filing Web Utility
- Back Up/Restore Utility
- File Downloader
- TWAIN Driver
- AddressBook Viewer

HOLD (FAX)

In the high security mode, when an email to which a FAX, Internet FAX or image is received, it is not automatically output. These jobs are stored in the [HOLD (FAX)] queue and only a user having the [Fax Received Print] privilege can print the job.

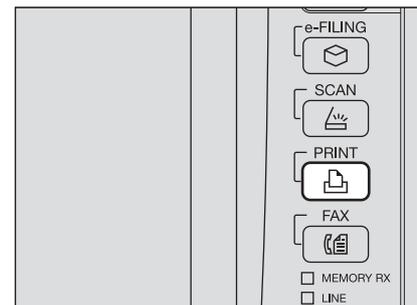
Tip

If a job is in the [HOLD (FAX)] queue, the MEMORY RX / LINE lamps blink.

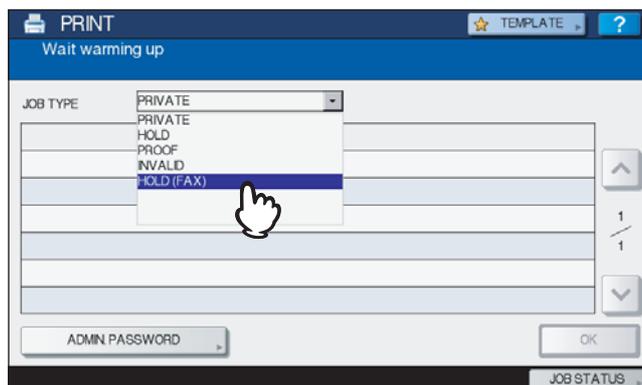


Printing a job in the HOLD (FAX) queue

- 1 Log in to the equipment as a user having the [Fax Received Print] privilege.
- 2 Press the [PRINT] button on the control panel.

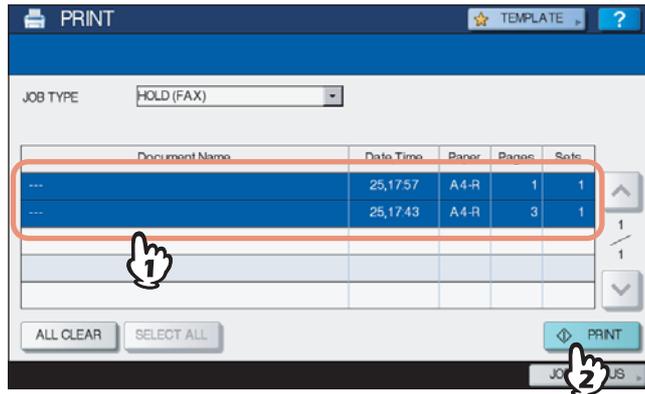


- 3 Select [HOLD (FAX)].



- All jobs in the [HOLD (FAX)] queue are displayed.

4 Select the desired job or [SELECT ALL], and then press [PRINT].



- The job that has been output is deleted from the [HOLD (FAX)] queue.

THE INITIAL VALUES

Precautions on the Initial Values	14
Logging in	14
Initial value list	15

Precautions on the Initial Values

To securely operate the equipment, the initial and selectable values in the equipment under the high security mode may differ from those under the normal security mode. This manual only explains about the initial values and setting items which are different from those under the normal security mode.

To operate the equipment complying with IEEE Std 2600.1™-2009, do not change the initial settings described in this manual.

Notes

- For the initial and setting values in the normal security mode, refer to the TopAccess Guide and MFP Management Guide.
- To reset all settings by performing “Initialization” of this equipment, back up the setting of this equipment and customers’ data before initializing. For details, refer to the TopAccess Guide and MFP Management Guide.

■ Logging in

- The [User Management] and [Administrator] tabs in TopAccess are displayed by logging in as a user with the administrator privilege. Open TopAccess, click “Login” on the top right, and then enter the user name and password to log in.



- Be sure to log in the [ADMIN] tab in the [USER FUNCTIONS] mode of the equipment as a user with the Administrator privilege.

■ Initial value list

[Administration] Tab

[Setup] Menu

[General] Sub Menu

Functions		
Save as FTP	Disable	
Network iFax	Disable	
Network Fax	Disable	
Web Services Scan	Disable	
Twain Scanning	Enable	The initial value is the same as that of in the Normal Security Mode; however, be sure to set to OFF.
Restriction on Address Book Operation by Administrator		
Can be operated by Administrator only		
Energy Save		
Auto Clear *	45 Seconds	The initial value is the same as in the Normal Security Mode; however, OFF cannot be selected.

* The value can be changed in the [ADMIN] tab in the [User Function] mode in the touch panel of the equipment.

[Network] Sub Menu

HTTP Network Service		
Enable SSL *	Enable	
SMTP Client		
Enable SSL	Verify with imported CA certification(s)	The secure setting is "Verify with imported CA certification(s)" or "Accept all certificates without CA".
Authentication	AUTO	Be sure to confirm that one of "CRAM-MD5", "Digest-MD5", "Kerberos" or "NTLM (IWA)" is applied to your use environment.
SMTP Server		
Enable SMTP Server	Disable	
POP3 Network Service		
Enable SSL	Verify with imported CA certification(s)	
FTP Client		
Enable SSL	Verify with imported CA certification(s)	
FTP Server		
Enable SSL	Enable	
SNMP Network Service		
Enable SNMP V1/V2	Disable	
Enable SNMP V3	Enable	
Web Services Setting		
Enable SSL	Enable	
Web Services Scan	Disable	

* The value can be changed in the [ADMIN] tab in the [User Function] mode in the touch panel of the equipment.

[Printer] Sub Menu

General Setting		
Restriction for Print Job	Only Hold	

[Print Service] Sub Menu

IPP Print		
Enable SSL	Enable	
FTP Print		
Enable FTP Printing	Disable	

[Security] Menu

[Authentication] Sub Menu

User Authentication Setting		
User Authentication	Enable	You cannot change the setting to "Disable".
Authentication Type	MFP Local Authentication	
Enable Guest User	No check mark (Disable)	The initial value is the same as in the Normal Security Mode; however, it cannot be set to "Enable".

[ODCA] Sub Menu

Network		
Enable Port	Disable	

[Password Policy] Sub Menu

Policy for Users		
Minimum Password Length	8 (digit)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	
Available Period	Disable	(Same as in the Normal Security Mode)
Expiration day(s)	90 (days)	
Policy for Administrator, Auditor		
Minimum Password Length	8 (digit)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	
Available Period	Disable	(Same as in the Normal Security Mode)
Expiration day(s)	90 (days)	
Policy for e-Filing Boxes, Template Groups, Templates, SecurePDF, SNMPv3, Cloning		
Minimum Password Length	8 (digit)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	

Oki Data Corporation
4-11-22 Shibaura, Minato-ku, Tokyo
108-8551, Japan

www.okiprintingsolutions.com

