

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

High Security Mode Management Guide

Preface

Thank you for purchasing Toshiba 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.
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.




Note

If you find any evidence of the suspicious opening of received cartons or you are not sure how it has been packed, contact your sales representative.

■ 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.

□ Model and series names in this manual

In this manual, each model name is replaced with the series name as shown below.

Model name	Series name in this manual
e-STUDIO2050C/2550C	e-STUDIO2550C Series
e-STUDIO2555C/3055C/3555C/4555C/5055C e-STUDIO2555CSE/3055CSE/3555CSE/4555CSE/5055CSE	e-STUDIO5055C Series
e-STUDIO287CS/347CS/407CS e-STUDIO287CSL/347CSL	e-STUDIO407CS Series
e-STUDIO477S/527S e-STUDIO477SL	e-STUDIO527S Series
e-STUDIO5560C/6560C/6570C	e-STUDIO6570C Series
e-STUDIO207L/257/307/357/457/507	e-STUDIO507 Series
e-STUDIO557/657/757/857	e-STUDIO857 Series

□ Explanation for control panel and touch panel

- Illustrations for the control panel and the touch panel shown in this manual are those of the e-STUDIO4540C Series.
The shape and location of some buttons on the control panel and the dimension of the touch panel of the other models differ depending on the model, however, the names and functions of the buttons and parts are the same.
- 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.

□ Options

For the available options, refer to "Options" in the **Quick Start Guide** for your equipment.

□ Trademarks

- 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 8 is Microsoft Windows 8 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.
- The official name of Windows Server 2012 is Microsoft Windows Server 2012 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, iPhone, iPod touch, and TrueType are trademarks of Apple Inc. in the US and other countries.
- AirPrint, AirPrint logo, and iPad are trademarks of Apple Inc.
- IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license.
- 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.
- TopAccess is a trademark of Toshiba Tec Corporation.
- 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	7
Operational conditions.....	8

Chapter 2 UNIQUE FUNCTIONS

Temporary Password	12
Conditions when a temporary password is used	12
Operation by a user when a temporary password is used	12
HOLD (FAX)	13

Chapter 3 THE INITIAL VALUES

Precautions on the Initial Values	16
Logging in.....	16
Initial value list.....	16

THE HIGH SECURITY MODE

Precautions on Using the High Security Mode	6
Confirmation of the mode	7
Operational conditions.....	8

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 *1
- 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*2 or TLS
- Integrity Check function
- Management functions such as:
Log, Passwords, User, Password Policy, Date & Time, Auto Clear, Session Timer, Enable/disable of SSL*2/TLS

*1 The function to encrypt the data to be written in the HDD for the e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507 and e-STUDIO557/657/757/857 series are not subject to the assessment of ISO/IEC15408.

*2 Only TLS is supported in the e-STUDIO5560C/6560C/6570C, e-STUDIO207L/257/307/357/457/507 and e-STUDIO557/657/757/857 series.

The ISO/IEC 15408 certification is applied or will be to the models operating with the following OS and browser combination as well as running in the English or Japanese mode.

OS: Windows XP

Browser: Internet Explorer 8

MFP:

e-STUDIO2050C/2550C

e-STUDIO2555C/3055C/3555C/4555C/5055C

e-STUDIO2555CSE/3055CSE/3555CSE/4555CSE/5055CSE

OS: Windows 7

Browser: Internet Explorer 9

MFP:

e-STUDIO5560C/6560C/6570C*

e-STUDIO207L/257/307/357/457/507*

e-STUDIO557/657/757/857*

* Certification pending (as of March, 2015)


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.

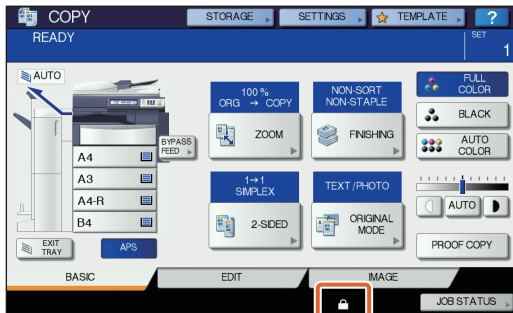
Pay attention that if the conditions given in this manual are not met, you may not be able to operate the equipment complying with IEEE Std 2600.1™-2009.

Tips

- For details of each security function and how to set the related items, refer to the TopAccess Guide.
- The optional Hard Disk Kit (GE-1220) is required when e-STUDIO2050C/2550C with no hard disk is to be used in the high security mode.



Confirmation of the mode

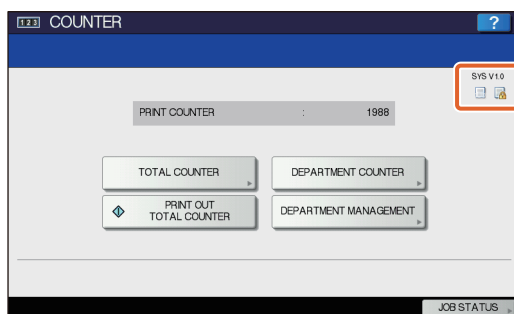
When this equipment is operated under the high security mode,  is displayed on the touch panel of the equipment.



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.

<p>The HDD is encrypted.</p>	<p> The icon is displayed. The HDD has been encrypted if this equipment is operated under the high security mode.</p>																
<p>The Data Overwrite Enabler is operating properly.</p>	<p> The icon showing that the Data Overwrite Enabler is correctly operating is displayed. The version of the system which is running is displayed.</p> <p>Tip</p> <p>The system version to be displayed differs depending on the equipment which is used.</p> <table> <tr> <td>e-STUDIO2550C Series:</td> <td>SYS V4.0</td> </tr> <tr> <td>e-STUDIO5055C Series:</td> <td>SYS V4.0</td> </tr> <tr> <td>e-STUDIO6570C Series:</td> <td>SYS V3.0 *</td> </tr> <tr> <td>e-STUDIO507 Series:</td> <td>SYS V3.0 *</td> </tr> <tr> <td>e-STUDIO857 Series:</td> <td>SYS V3.0 *</td> </tr> <tr> <td>e-STUDIO407CS Series:</td> <td>SYS V2.0</td> </tr> <tr> <td>e-STUDIO527S Series:</td> <td>SYS V2.0</td> </tr> <tr> <td>e-STUDIO307LP:</td> <td>SYS V2.0</td> </tr> </table> <p>* ISO/IEC15408 certification accession version</p>	e-STUDIO2550C Series:	SYS V4.0	e-STUDIO5055C Series:	SYS V4.0	e-STUDIO6570C Series:	SYS V3.0 *	e-STUDIO507 Series:	SYS V3.0 *	e-STUDIO857 Series:	SYS V3.0 *	e-STUDIO407CS Series:	SYS V2.0	e-STUDIO527S Series:	SYS V2.0	e-STUDIO307LP:	SYS V2.0
e-STUDIO2550C Series:	SYS V4.0																
e-STUDIO5055C Series:	SYS V4.0																
e-STUDIO6570C Series:	SYS V3.0 *																
e-STUDIO507 Series:	SYS V3.0 *																
e-STUDIO857 Series:	SYS V3.0 *																
e-STUDIO407CS Series:	SYS V2.0																
e-STUDIO527S Series:	SYS V2.0																
e-STUDIO307LP:	SYS V2.0																



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

■ Operational conditions

Follow the operating guidance above, otherwise your confidential information will not be protected from leakage or unauthorized access to this equipment.

Be sure to set [MFP Local Authentication] for [Authentication Method] in the [User Management] screen. If [Windows Domain Authentication] or [LDAP Authentication] is set for user authentication, the equipment will not be covered by IEEE Std 2600.1™-2009.

When connecting the equipment from any of e-Filing 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] and perform the integrity check at the time of installation and during use periodically.

* For details of the integrity check, refer to the MFP Management Guide/User's Manual Advanced 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 any of the following cases, contact your service technician.

- If the icon showing that the HDD is encrypted (🔒) is not displayed.
- If the icon showing that the Data Overwrite Enabler is operating properly (📄) is not displayed.
- The displayed system version differs from the actual one.

When SNMPV3 is used, be sure to set "General User" in the [Permission Level] box during the creation of the SNMP V3 user information in the following menu: [Administration] tab page -> [Setup] menu -> [Network] submenu -> [SNMP] -> [Create SNMP V3 User Information] screen

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

- Interrupt copy
- Network Fax
- AddressBook Viewer
- File Downloader
- TWAIN Driver
- e-Filing BackUp/Restore Utility
- 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 to communicate with this 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.

When importing the data such as address book, be sure to use the data exported from this equipment.

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.

Do not enable [Use Password Authentication for Print Job] when printing is performed from this equipment with any of these printer drivers; Universal Printer 2, Universal PS3 and Universal XPS.

To operate this equipment securely, be sure to set the following items:

Note

Perform the setting correctly referring to Initial value list (📖 P.16).

- Select [Disable] in [Enable Raw TCP] and [Enable LPD] in the [Print Service] submenu.
- 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.
- Administrators must regularly export and store the logs.
- Select [Disable] in [Twain Scanning].
- Select [Disable] in [Enable SLP].
- Select [Disable] in [Web Services Print].
- Select [Disable] in [SMB Server Protocol].
- Select [Disable] in [Enable Bonjour].
- Select [Disable] in [Enable FTP Server].

An administrator should explain to users that the high security mode is operating in this equipment as well as the following items so that they will keep to them appropriately.

- Printing should be performed by using the printer driver settings of IPP print.
- Specify a reliable remote PC for the saving destination of the scan data.
- Do not use a shared folder in e-Filing.
- Do not use any local folder of this equipment.

UNIQUE FUNCTIONS

Temporary Password	12
Conditions when a temporary password is used.....	12
Operation by a user when a temporary password is used	12
HOLD (FAX)	13

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.

- Registering your password on the control panel
Enter the user name and a temporary password in the User Authentication menu. When you press [OK] in the confirmation screen for the temporary password, the password entry screen appears. Enter the temporary password in [OLD PASSWORD]. Enter your new password in [NEW PASSWORD] and [RETYPE NEW PASSWORD], and then press [OK]. The new password is registered and you can log in to the equipment.
- Registering your password in TopAccess
When you access the equipment from TopAccess, the log-in screen appears. Enter the user name and a temporary password in the log-in screen, and then press [Login]. When the registration screen appears, enter your new password in [NEW PASSWORD] and [RETYPE NEW PASSWORD], and then press [SAVE]. The new password is registered and you can log in to TopAccess.

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.

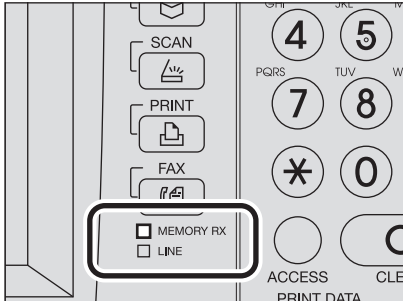
- Remote Scan driver
- e-Filing Web Utility

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.

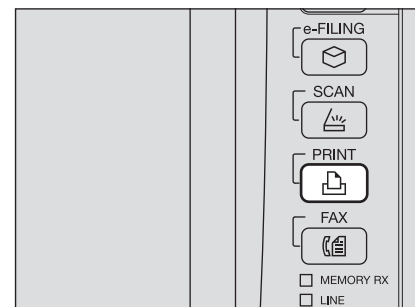
Tip

If a job is in the [HOLD (FAX)] queue, the MEMORY RX lamp blinks.

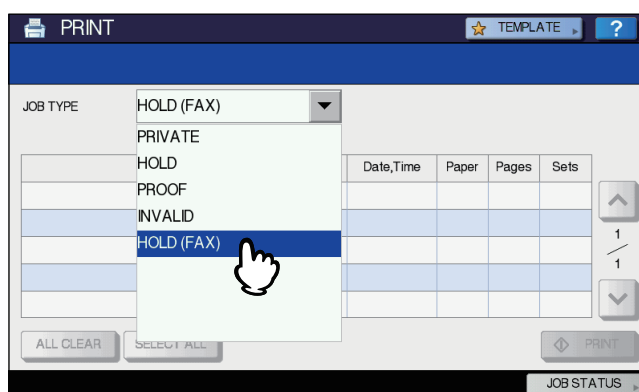


Printing a job in the HOLD (FAX) queue

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

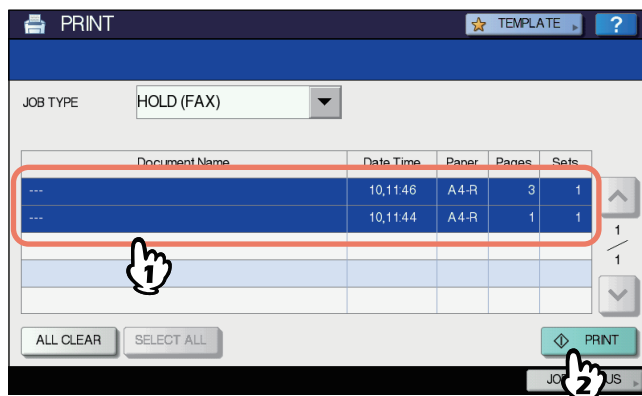


- 3 Select [HOLD (FAX)].



- 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	16
Logging in	16
Initial value list	16

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.

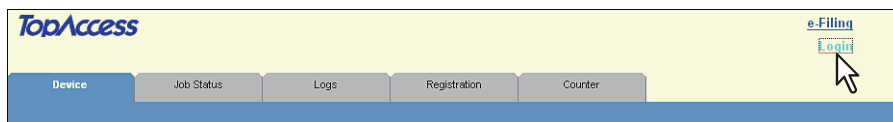
To operate equipment complying with IEEE Std 2600.1™-2009, be sure to change the initial values for the high security mode listed in this chapter following the instructions described in the remarks column at the start of use and keep them unchanged.

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 [Administration] 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 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

Item	Initial value for the high security mode	Remarks
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

Item	Initial value for the high security mode	Remarks
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 FTP Server	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable]
Enable SSL	Enable	
SNMP Network Service		
Enable SNMP V1/V2	Disable	
Enable SNMP V3	Enable	
Web Services Setting		
Enable SSL	Enable	
Web Services Print	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable].
Web Services Scan	Disable	
SLP Session		
Enable SLP	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable].
SMB Session		
SMB Server Protocol	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable].
Bonjour		
Enable Bonjour	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [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

Item	Initial value for the high security mode	Remarks
General Setting		
Restriction for Print Job	Only Hold	

[Print Service] Sub Menu

Item	Initial value for the high security mode	Remarks
IPP Print		
Enable SSL	Enable	
FTP Print		
Enable FTP Printing	Disable	
Raw TCP Print		
Enable Raw TCP	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable].
LPD Print		
Enable LPD	Enable	Although [Enable] is set by default in the same manner as the normal security mode, be sure to set it to [Disable].

[ODCA] Sub Menu

Item	Initial value for the high security mode	Remarks
Network		
Enable Port	Disable	

[Security] Menu

[Authentication] Sub Menu

Item	Initial value for the high security mode	Remarks
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".
PIN Code Authentication	Disable	Do not change the setting to "Enable".
Use Password Authentication for Print Job	Disable	Do not change the setting to "Enable".

[Password Policy] Sub Menu

Item	Initial value for the high security mode	Remarks
Policy for Users		
Minimum Password Length	8 (digits)	
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 (digits)	
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, Secure Receive		
Minimum Password Length	8 (digits)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	

FC-2050C/2550C
FC-2555C/3055C/3555C/4555C/5055C
FC-287CS/287CSL/347CS/347CSL/407CS
DP-4710S/5210S
FC-5560C/6560C/6570C
DP-2072/2572/3072/3572/4572/5072
DP-5570/6570/7570/8570
OME100078P0

**MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS**
High Security Mode Management Guide

TOSHIBA TEC CORPORATION

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN

