TOSHIBA

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

High Security Mode

e-STUDIO2020AC/2520AC/2021AC/2521AC
e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC
e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A
e-STUDIO6526AC/6527AC/7527AC
e-STUDIO6529A/7529A/9029A

Preface

Thank you for purchasing our product.

This manual explains about the conditions and settings for using the Multifunctional Digital Systems which complies with CC Certification.

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 CC Certification, refer to "Security Precautions" in the "Safety Information".

Keep this manual within easy reach and use it to maintain the equipment complying with CC Certification.

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 described 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 objects.
⚠ CAUTION	Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury, partial damage to the equipment or surrounding objects, or loss of data.
Note	Indicates information to which you should pay attention when operating the equipment.
Tip	Describes handy information that is useful to know when operating the equipment.
📖	References describing items related to what you are currently doing. See these references as required.

❑ Target audience for this manual

This is the manual for equipment administrators. It is not necessary for general users to read this manual.

❑ 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
e-STUDIO2020AC/2520AC/2021AC/2521AC	e-STUDIO6525AC Series
e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC	
e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A	e-STUDIO6528A Series
e-STUDIO6526AC/6527AC/7527AC	e-STUDIO7527AC Series
e-STUDIO6529A/7529A/9029A	e-STUDIO9029A Series

❑ Options

For available options, see the reference below:
Information About Equipment - Information About Equipment - Options

❑ Trademarks

For trademarks, refer to the **Safety Information**.

CONTENTS

1

THE HIGH SECURITY MODE

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 CC Certification.

- User Authentication Setting function
- Role Management function
- Log collecting and browsing function
- Communication function with TLS1.2
- Integrity Check function
- Management functions such as:
  Log, Passwords, User, Password Policy, Date & Time, Auto Clear, Session Timer, Enable/disable of TLS

ISO/IEC15408 Certificate has been or will be obtained for the equipment (with the fax unit installed and IPv4 used) which has the combination of the OS and browser below and has been being operated in Japanese or English.

PP Identifier: HCD-PP

OS:	Windows 10
Browser:	Microsoft Edge
MFP:	e-STUDIO2020AC/2520AC/2021AC/2521AC*
	e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC*
	e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A*
	e-STUDIO6526AC/6527AC/7527AC*
	e-STUDIO6529A/7529A/9029A*

*   Certification pending (as of Jan. 2024)

To operate the equipment complying with CC Certification under the high security mode, configurations according to the use environment, such as 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 CC Certification.

Tip

For details of each security function and how to set the related items, see the reference below:
TopAccess

■ Confirmation of the mode

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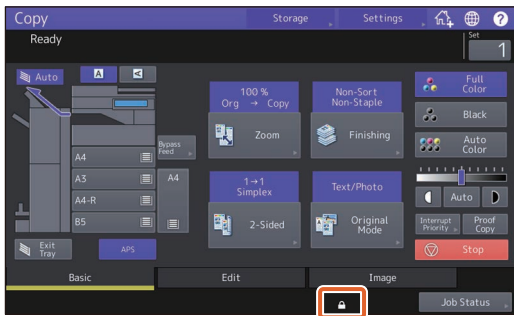
Note

When your service technician attempts maintenance, an administrator should confirm it beforehand and join in the operation.

After the operation is completed, confirm that 🔒 is displayed on the touch panel of this equipment.
Moreover, by referring to the initial value list, confirm that the settings have been made correctly.

If an administrator could not join in the operation, perform "Initialization" of this equipment and confirm that 🔒 is displayed on the touch panel. Then set the values again by referring to the initial value list.
📖 P.19 "Initial value list"

Tip

• The internal storage device of the equipment which is operated under the high security mode is encrypted.
• To confirm the SYS version, check the display at the top right of the [Counter] screen on the touch panel of the equipment.
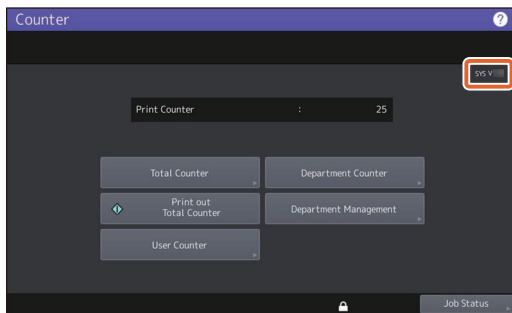
■ Operational conditions

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 CC Certification.

In order to maintain the security status complying with CC Certification, when a self-signed certificate is created, use "RSA2048" for Public Key and "SHA256", "SHA384" or "SHA512" for Signature Algorithm.

Manually select [FULL] and perform the integrity check at the time of installation and during use periodically.
*   For details of the integrity check, see the reference below:
     User Functions - SETTING ITEMS (Admin) - Security - Performing the integrity check

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

In any of the following cases, contact your service technician.
*   The displayed SYS version differs from the actual one.

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
*   Disabling log authentication
*   Mailbox
*   E-mail reception print
*   Disabling POP3 setting
*   Data Backup/Restore

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/TLS to communicate with this equipment.

When IPP printing is performed, use the port created by entering "https://[IP address]:[SSL/TLS port number]/Print" into the URL field.
(e.g.: https://192.168.1.2:631/Print)
*   For details, see the reference below:
     Installation - INSTALLING PRINTER DRIVERS FOR WINDOWS - Other Installations - IPP printing

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] 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.

The Integrity Check function is automatically performed at the startup of this equipment. When "Call For Service" appears, contact your service technician.

In order to operate this equipment under the high security mode, a Syslog server which supports TLS1.2 is necessary.

Printing, copying, scanning and fax transmission/reception are subject to an access restriction by means of a user authentication function. All users can confirm the lists of jobs in processing and in waiting. However, as for the list of fax reception jobs, only users whose role is Administrator or FaxOperator can confirm it. Corresponding to the role privilege of users, they can operate outputting, deletion, pause or change orders of jobs. When the role of the users is Administrator or User, they can create jobs. When the role of the users is FaxOperator, they can create, output and delete fax transmission/reception jobs. However, as for fax transmission jobs, the users can output and delete only their account jobs. When the role of the users is User, jobs, they can output and delete only their account jobs. When the role of the users is Administrator, they can delete, pause and change the order of all jobs in waiting. However, if the role of the users is AccountManager or AddressBookRemoteOperator, outputting, deleting, pausing or changing orders of printing, copying or fax jobs is not available.

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

Note

Perform the setting correctly, see the reference below:
📖 P.19 "Initial value list"

- 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 MFP LOCAL since no password can be set.
- Administrators must regularly export and store the logs.
- Do not enable [Auto] of Email Direct Printing.
- Be sure to reboot the equipment when CA certification is uploaded or removed.

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 any local folder of this equipment.

An administrator should always confirm that communication with the Syslog server is being connected.

When disposing of an MFP, be sure to contact your service technicians to erase the data in the internal storage device completely.

2

UNIQUE FUNCTIONS

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

- You can display the preview of the fax image received on the touch panel before printing the fax. For details, see the reference below:
  Fax - USING THE FAX UNIT (BASIC OPERATION) - Receiving a Fax - Reception mode - Displaying the preview of a received fax
- If a job is in the [Hold (Fax)] queue, the Memory Rx lamp blinks.
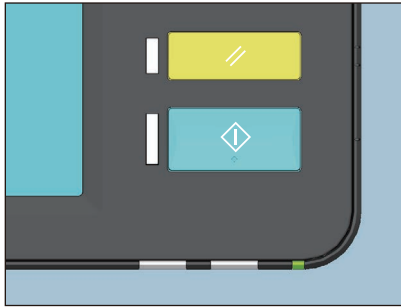
■ Printing a job in the Hold (Fax) queue

1 **Log in to the equipment as a user having the [Fax Received Print] privilege.**

2 **Press [Print Mode] on the home menu screen.**

3 **Select [Hold (Fax)].**
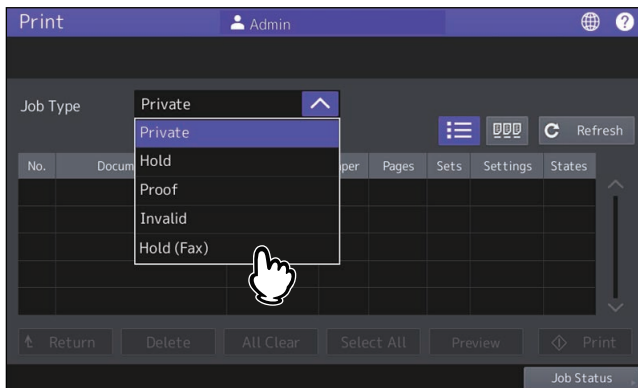
- All jobs in the [Hold (Fax)] queue are displayed.

4 **Select the desired job or [Select All], and then press [Print].**
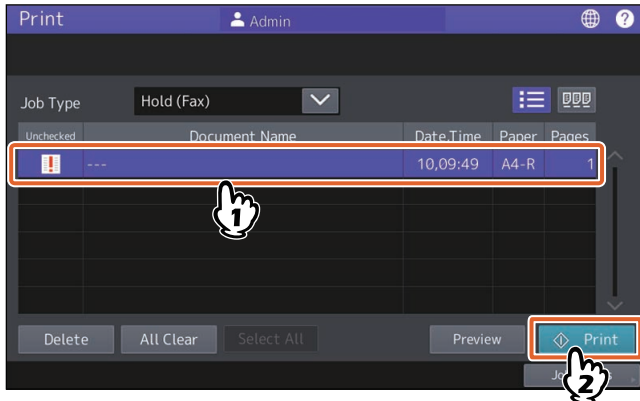
- The job that has been output is deleted from the [Hold (Fax)] queue.

3

THE INITIAL VALUES

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 this equipment complying with CC Certification, be sure to set the values again by referring to the initial value list described in this chapter at the start of use and keep them unchanged.

If this equipment has temporarily been operated with different settings from the initial value list, perform "Initialization" after the operation is completed. Then set the values again by referring to the initial value list described in this chapter at the start of use and keep them unchanged.

Note

*   For the initial and setting values in the normal security mode, see the references below:
    TopAccess
    User Functions
*   To reset all settings by performing "Initialization" of this equipment, back up the setting of this equipment and customers' data before initializing. For details, see the reference below:
    Information About Equipment - Information About Equipment - How to back up the data

■ Logging in

*   The [User Management] and [Administration] 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 Function] mode of the equipment as a user with the Administrator privilege.

■ Initial value list

Home screen:
[User Functions -User-] Menu
[Admin] Tab
[List/Report] Menu
[Report Setting] Menu

Item	Initial value for the high security mode	Remarks
[COMM. Report]		
Memory Tx	OFF	Do not change the setting to "ON".

* It is not possible to operate the above menus from TopAccess.

TopAccess:
[Administration]
[Setup] Menu
[General] Sub Menu

Item	Initial value for the high security mode	Remarks
Device Information		
USB Direct Print	Disable	
Functions		
e-Filing	Enable	Be sure to change the value to "Disable".
Save as FTP	Disable	
Save to USB Media	Disable	
Save as SMB	Disable	
Save as Netware	Disable	
iFax Send	Enable	
Fax Send	Enable	
Network iFax	Disable	
Network Fax	Disable	
Web Services Scan	Disable	
Twain Scanning	Disable	
Restriction on AddressBook Operation by administrator / AddressBookRemoteOperator		
Can be operated by Administrator / AddressBookRemoteOperator only		
Energy Save		
Auto Clear *	45 Seconds	The initial value is the same as in the Normal Security Mode; however, OFF cannot be selected.
Home Setting		
Public Home	Disable	
Sync Setting	Disable	

* The value can be changed in the [ADMIN] tab in the [User Functions -User-] menu in the touch panel of the equipment.

[Network] Sub Menu

Item	Initial value for the high security mode	Remarks
IPv6		
Enable IPv6	Enable	Be sure to change the value to "Disable".
SSL/TLS		
TLS Versions	TLS 1.2	Do not change.
SMB		
SMB Server Protocol	Disable	
HTTP		
Enable SSL/TLS*	Enable	
WSD		
Enable SSL/TLS	Enable	
Web Services Print	Disable	
Web Services Scan	Disable	
SMTP Server		
Enable SMTP Server	Disable	
FTP Server		
Enable FTP Server	Disable	
Enable SSL/TLS	Enable	
SSL/TLS	Port Number 990	
SMTP Client		
Enable SSL/TLS	Verify with imported CA certification(s)	
Authentication	AUTO	Be sure to confirm that one of "CRAM-MD5", "Digest-MD5", "Kerberos" or "NTLM (IWA)" is applied to your use environment.
POP3 Client		
Enable POP3 Client	Enable	Be sure to change the value to "Disable".
Enable SSL/TLS	Verify with imported CA certification(s)	
FTP Client		
SSL/TLS Setting	Verify with imported CA certification(s)	
Bonjour		
Enable Bonjour	Disable	
SNMP		
Enable SNMP V1/V2	Disable	
Enable SNMP V3	Enable	
SLP		
Enable SLP	Disable	
Syslog Setting		

Item	Initial value for the high security mode	Remarks
Enable Syslog	Enable	
Enable SSL/TLS	Verify with imported CA certification(s)	
Severity - Error	Enable	
Severity - Warning	Enable	
Severity - Information	Enable	
Facility - Security/Authorization	Enable	
Facility - Local Use0	Enable	
Facility - Local Use1 (Job Log)	Enable	

* The value can be changed in the [ADMIN] tab in the [User Functions -User-] menu 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
Raw TCP Print		
Enable Raw TCP	Disable	
LPD Print		
Enable LPD	Disable	
IPP Print		
Enable SSL/TLS	Enable	
FTP Print		
Enable FTP Printing	Disable	

[ODCA] Sub Menu

Item	Initial value for the high security mode	Remarks
Network		
Enable Port (SOAP)	Disable	
Enable Port (REST)	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".
User Authentication According to Function	Disable	Do not change the setting to "Enable".
Use Password Authentication for Print Job	Disable	Do not change the setting to "Enable".
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".
Authentication Type	MFP Local Authentication	
PIN Code Authentication	Disable	Do not change the setting to "Enable".
Shared User Management	Disable	Do not change the setting to "Enable".
Public Box Authentication		
Public Box Authentication	Enable	

[Password Policy] Sub Menu

Item	Initial value for the high security mode	Remarks
Policy for Users		
Minimum Password Length	8 (digits)	Set a password longer than 15 digits with alphanumeric characters (including letters having an umlaut in German or a cedilla in French), symbols (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` {	} ~ \) and a space.
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)	Set a password longer than 15 digits with alphanumeric characters (including letters having an umlaut in German or a cedilla in French), symbols (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` {	} ~ \) and a space.
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, SecurePDF, SNMPv3, Cloning, Secure Receive		
Minimum Password Length (e-Filing Boxes), Minimum Password Length (SecurePDF, SNMPv3, Cloning, Secure Receive)	8 (digits)	Set a password longer than 15 digits with alphanumeric characters (including letters having an umlaut in German or a cedilla in French), symbols (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` {	} ~ \) and a space.
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	

4

APPENDIX

List of target events for monitoring and logs to be sent to the Syslog server

The following information will be sent to a Syslog server. Success or failure of the event can be confirmed by means of the Result field.

- Registration date
- Internal log memory date
- Code
- Message
- User name
- Domain name

Target events for monitoring		Logs to be sent to the Syslog server		
		Code	Result	Message
Start of the monitoring function	Turning ON of the equipment	D801	—	Turned on the power
End of the monitoring function	Turning OFF of the equipment	D800	—	The machine was shut down
End of jobs	End of printing jobs	4000	OK	job:Print jobId:6
	End of scanning jobs	2D01	OK	job:FTPStore jobId:8 to:
		2C00	OK	job:EmailSend jobId:33 to:
	End of copying jobs	4000	OK	job:Copy jobId:11
	End of fax transmission jobs	0000	OK	job:FaxSend jobId:9 to:1
	End of fax reception jobs	0000	OK	job:FaxReceive jobId:10 from:1
User authentication failure	Login failure	6001	NG	Failed user login
User identification failure				
User identification failure	Login failure (Print Job)	4041	NG	job:Print jobId:29
Use of the management functions	Addition of a user	7174	OK	Updated user information : New User created
		7129	NG	Failed to import User Information
	Setting and changing of a user ID	7175	OK	Updated user information : User Information modified
		717D	OK	Updated user information : Role/Group assignment modified
		7129	NG	Failed to import User Information
	Deletion of a user	7176	OK	Updated user information : User removed

Target events for monitoring			Logs to be sent to the Syslog server		
			Code	Result	Message
Use of the management functions	Changing of settings	Number of retries for the login password entry	7184	OK	Edited Security Setting
		Lockout time	7184	OK	Edited Security Setting
		Status of the locked out account	7175	OK	Updated user information : User Information modified
		User password policy information	7184	OK	Edited Security Setting
		Auto logout time	7182	OK	Edited Device Setting
		Registration of the address book	7160	OK	Added new contact
		Change of the address book	7166	OK	Edited Address Book
		Deletion of the address book	7170	OK	Removed a contact
		Network setting	7183	OK	Edited Network Setting
Modification of the user group which is a part of the role	Changing of the role information		717B	OK	Updated group information : Group information modified
Change of the time	Correction of the time		718A	OK	Edited Date & Time Setting
Session consolidation failure	TLS session consolidation failure		80C1	NG	Failed to establish the TLS session (bad record mac)
			80C5	NG	Failed to establish the TLS session (handshake failure)
Use of the management functions	Management of the software		7100	OK	Successfully updated Copier Firmware

Note

As for "End of jobs", if any codes other than the listed one appear, "NG" will be indicated in the Result field.

CC Certification obtained version list

The following table shows the combination of the CC Certification obtained version, operator's manual and options for each model. Be sure to confirm the identification number of the operator's manual and the information described on the equipment and the packing carton.

Series	Operator's Manual		SYS version	Required option
	Name	**Identification number**		**FAX unit**
e-STUDIO6525AC Series, e-STUDIO6528A Series	Quick Start Guide	OME210012B0	V5.2 or V6.2 [*1]	
	Safety Information	OME210014B0		
	Copy	OME210018B0		
	Scan	OME210020B0		
	User Functions	OME210028B0		
	Installation	OME210032B0		
	Print	OME210034B0		
	TopAccess	OME210036B0		
	Frequently Asked Questions	OME210030B0		
	Troubleshooting	OME210006B0		
	High Security Mode	OME210040E0		
	Preparation of Paper	OME210004B0		
	Information About Equipment	OME210016C0		
	Specifications	OME210038C0		
	Fax	OME210022B0		
	Information to our customers	OMM210083E0		For the U.S.A.: GD-1370NA-N[*2] For Europe: GD-1370EU [*2]
e-STUDIO7527AC Series, e-STUDIO9029A Series	Quick Start Guide	OME210012B0	V5.1 [*1]	
	Safety Information	OME210014B0		
	Copy	OME210018B0		
	Scan	OME210020B0		
	User Functions	OME210028B0		
	Installation	OME210032B0		
	Print	OME210034B0		
	TopAccess	OME210036B0		
	Frequently Asked Questions	OME210030B0		
	Troubleshooting	OME21001000		
	High Security Mode	OME210040E0		
	Preparation of Paper	OME21000800		
	Information About Equipment	OME210016C0		
	Specifications	OME210038C0		
	Fax	OME210022B0		

*1 For details about the combination of the SYS version and the firmware, see the reference below:
 📖 P.30 "Combination of the SYS version and the firmware"
*2 Be sure to confirm that the model name of the FAX unit is "GD-1370NA-N" or "GD-1370EU" by performing list printing by means of selecting [User Functions -User-] > [Admin] > [List/Report] > [List] > [Function] from the control panel.

■ Combination of the SYS version and the firmware

The combination of the firmware varies depending on the equipment used and the SYS version as the tables below.
For how to confirm the SYS version, see the reference below:
📖 P.9 "Confirmation of the mode"
For how to confirm the version of the firmware, see the reference below:
TopAccess - [Administration] - [Setup] Item List - Version

> Tip

For details about the difference of the SYS version, refer to **Information to our customers**.

❑ SYS V5.1

Firmware	e-STUDIO6526AC/6527AC/7527AC	e-STUDIO6529A/7529A/9029A
SYSTEM FIRMWARE	TS20SF0W1806	TS20SF0W1806
SYSTEM SOFTWARE	TS20SD0W1805	TS20SD0W1805
ENGINE FIRMWARE	TK180MWW06	TK183MWW06
SCANNER FIRMWARE	TK160SLGWW15	TK160SLGWW15
FAX1 FIRMWARE	FAXH625TA13	FAXH625TA13

❑ SYS V5.2

Firmware	e-STUDIO2020AC/2520AC	e-STUDIO2021AC/2521AC	e-STUDIO2525AC/3025AC/3525AC	e-STUDIO4525AC/5525AC/6525AC	e-STUDIO2528A/3028A/3528A/4528A
SYSTEM FIRMWARE	TS20SF0W1810	TS20SF0W1810	TS20SF0W1810	TS20SF0W1810	TS20SF0W1810
SYSTEM SOFTWARE	TS20SD0W1810	TS20SD0W1810	TS20SD0W1810	TS20SD0W1810	TS20SD0W1810
ENGINE FIRMWARE	TK160MWW62	TK240MWW04	TK162MWW62	TK166MWW62	TK170MWW62
SCANNER FIRMWARE	TK160SLGWW16	TK160SLGWW16	TK160SLGWW16	TK160SLGWW16	TK160SLGWW16
FAX1 FIRMWARE	FAXH625TA13	FAXH625TA13	FAXH625TA13	FAXH625TA13	FAXH625TA13

Firmware	e-STUDIO5528A/6528A
SYSTEM FIRMWARE	TS20SF0W1810
SYSTEM SOFTWARE	TS20SD0W1810
ENGINE FIRMWARE	TK174MWW61
SCANNER FIRMWARE	TK160SLGWW16
FAX1 FIRMWARE	FAXH625TA13

❑ **SYS V6.2**

Firmware	e-STUDIO2020AC/2520AC	e-STUDIO2525AC/3025AC/3525AC	e-STUDIO4525AC/5525AC/6525AC
SYSTEM FIRMWARE	TS20SF0W1810	TS20SF0W1810	TS20SF0W1810
SYSTEM SOFTWARE	TS20SD0W1810	TS20SD0W1810	TS20SD0W1810
ENGINE FIRMWARE	TK160MWW62	TK162MWW62	TK166MWW62
SCANNER FIRMWARE	TK160SLGWW16	TK160SLGWW16	TK160SLGWW16
FAX1 FIRMWARE	FAXH625TA13	FAXH625TA13	FAXH625TA13

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS
<u>**High Security Mode**</u>

e·STUDIO2020AC/2520AC/2021AC/2521AC
e·STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC
e·STUDIO2528A/3028A/3528A/4528A/5528A/6528A
e·STUDIO6526AC/6527AC/7527AC
e·STUDIO6529A/7529A/9029A

Toshiba Tec Corporation

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

QUALITY SERVICE