KYOCERA

kyoceradocumentsolutions.com

Data Encryption/Overwrite
OPERATION GUIDE

Introduction

This function can be used by installing the optional HD-6 / HD-7 (SSD).

This Setup Guide explains the procedures for installing and operating the Data Encryption/Overwrite Functions (hereinafter called Security Functions) and the procedure for system initialization.

Organization administrators should read and understand this manual.

- Nominate a reliable person for the machine administrator when installing the security functions.
- Sufficiently supervise the nominated administrator so that it can observe the security policy and operation rules at the organization to which it belongs and properly operate the machine in accordance with the operation guide of the product.
- Sufficiently supervise the general users so that they can operate the machine while observing the security policy and operation rules at the organization to which they belong.

■Instructions for General Users (for Both General Users and Administrators)

- Security Functions 2
- Touch Panel Display after the Security Functions is Installed....... 3

■Instructions for Administrators (for Those in Charge of Installation and Operation of the Security Functions)

- Installing the Security Functions 4
- Changing Security Functions... 8
- System Initialization 9
- Warning Message 10
- Disposal 10
- Appendix.. 11

Instructions for General Users (for Both General Users and Administrators)

Security Functions

The security functions enables overwriting and encryption.

Overwriting

Multi-functional products (MFPs) temporarily store the data of scanned originals and print jobs, as well as other data stored by users, in the SSD, and the job is output from that data. Users can also store various types of data in the SSD. As the data storage area used for such data remains in the SSD as is until it is overwritten by other data, the data stored here remains restorable using special tools for undesirable use.

The security functions deletes and overwrites (hereinafter collectively referred to as *overwrite(s)*) the unnecessary data storage area used for the output data or deleted data to ensure that data cannot be restored.

Overwriting is performed automatically, without user intervention.

CAUTION: When you cancel a job, the machine immediately starts overwriting the data that has been already stored in the SSD.

Encryption

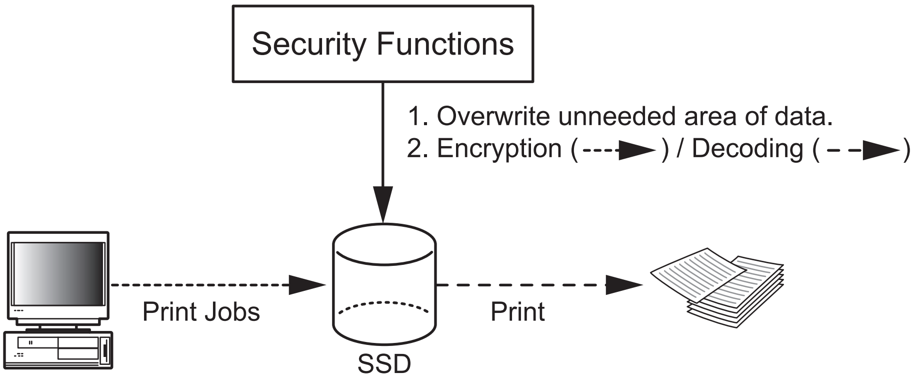
MFPs store the data of scanned originals and other data stored by users in the SSD. It means the data could be possibly leaked or tampered with if the SSD is stolen.

The security functions encrypts data before storing it in the SSD. It guarantees higher security because no data cannot be decoded by ordinary output or operations.

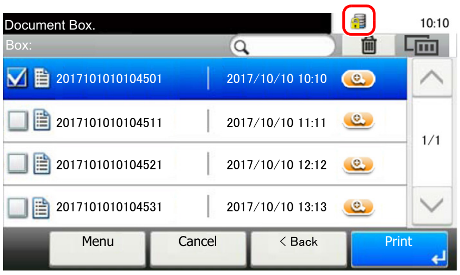
Encryption is automatically performed and no special procedure is required.

CAUTION: Encryption helps enhance security. However, the data stored in the Document Box can be decoded by ordinary operations. Do not store any strictly confidential data in the Document Box.

Functions of Security Functions


Security Functions
1. Overwrite unneeded area of data.
2. Encryption (---►) / Decoding (– –►)
Print Jobs
SSD
Print

Touch Panel Display after the Security Functions is Installed



☑	2017101010104501	2017/10/10 10:10
□	2017101010104511	2017/10/10 11:11
□	2017101010104521	2017/10/10 12:12
□	2017101010104531	2017/10/10 13:13

When the security functions has been installed and is running properly, Icon () appears in the touch panel while unneeded data is being overwritten.

CAUTION: Do not turn the power switch off during overwriting. It may crash the SSD.

NOTE: If you turn the machine off at the power switch during overwriting, data may not be overwritten completely from the SSD. Turn the machine back on at the power switch. Overwriting automatically resumes.

Instructions for Administrators (for Those in Charge of Installation and Operations of the Security Functions)

If any kind of problem occurs in the installation or use of the security functions, contact your dealer or service technician.

Installing the Security Functions

Before Installation

- Make sure that the service representative must be a person who belongs to the supplying company.
- Install the machine in a safe location with controlled access, and unauthorized access to the machine can be prevented.
- The system will be initialized during installation of the security functions. This means that the data stored in the SSD will be all overwritten. Special attention should be given if you install the security functions on the MFP currently used.
- The network to which the machine is hooked up must be protected by a firewall to prevent extraneous attacks.
- When installing the security functions, change the machine settings as follows.

Item			Value
User Login/Job Accounting	User Login Setting	Local User List	Change the administrator password.
System Menu	Date/Timer/Energy Saver	Date/Time	Set the date and time.

Installation

Installation of the security function is performed by the service person or the administrator. The service person or the administrator should log in the system menu to enter the encryption code.

Encryption Code

An encryption code of 8 alphanumeric characters (0 to 9, A to Z, a to z) to encrypt data needs to be entered. By default, the code is set *00000000*.

As an encryption key is then created from this code, it is safe enough to continue using the default code.

CAUTION: Be sure to remember the encryption code you entered. If you need to enter the encryption code again for some reason and you do not enter the same encryption code, all the data stored on the SSD will be overwritten as a security precaution.

Installation Procedure

Use the procedure below to select the interface.

1. Press the [System Menu/Counter] key.

2. Press [∨] and [System/Network].

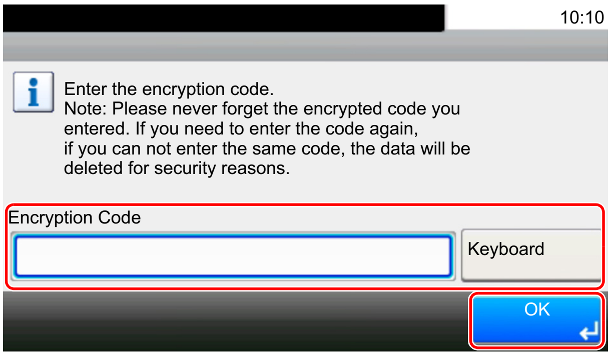
   If user login is disabled, the user authentication screen appears. Enter your login user name and password and then press [Login]. For this, you need to log in with administrator privileges. Refer to the machine's Operation Guide for the default loginuser name and password.

3. Press [∨] and [Optional Function].

4. The optional function screen is displayed. Select [Data Encr./Overwrite] and press [Activate].

5. This function will be activated. The data saved in the large capacity storage will be deleted and the storage will be formatted and encrypted. If there is no problem, press [Yes].

6. Turn the power switch on again following to the indication in the panel screen. The screen for entering the encryption code is displayed.



10:10

Enter the encryption code.
Note: Please never forget the encrypted code you entered. If you need to enter the code again,
if you can not enter the same code, the data will be deleted for security reasons.

7. Enter the encryption code, and press [OK]. Hard disk/SSD formatting begins.

8. When formatting finishes, follow the on screen instructions to turn the Power Switch off and on again.

9. After the opening screen is displayed, confirm that a hard disk icon (Overwritten completion icon of unnecessary data in the hard disk) is shown in the lower right corner of the screen.

After Installation

Change the machine setting as follows to securely operate it. If the system in the machine is initialized, it returns to the settings before installation, so make changes in the same way. If you allow service personnel to conduct maintenance operations, confirm the set values.

Items changed in Command Center RX

Item						Value
Device Settings	Energy Saver/Timer	Energy Saver/Timer Settings		Timer Settings	Auto Panel Reset	On
					Panel Reset Timer	Setting any value
Function Settings	Printer	Printer Settings	Google Cloud Print Settings (Select [Settings])	Privet(Cloud Device Local Discovery Protocol and API)	Local Discovery	Off
					Local Print	Off
	Forwarding	Forward Settings			Forward	Setting any value
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	Off
				IPSec Settings	IPSec	On
	Protocol	Protocol Settings		Print Protocols	NetBEUI	Off
					LPD	Off
					FTP Server (Reception)	Off
					IPP	Off
					IPP over SSL	On
					IPP Authentication	Off
					Raw	Off
					WSD Print	Off
					POP3 (E-mail RX)	Off
				Send Protocols	SMTP (E-mail TX)	On
					FTP Client (Transmission)	On
					SMB	Off
					WSD Scan	Off
					eSCL	Off
					eSCL over SSL	Off
				Other Protocols	SNMPv1/v2c	Off
					SNMPv3	Off
					HTTP	Off
					HTTPS	On
					Enhanced WSD	Off
					Enhanced WSD over SSL	On
					LDAP	Off
					IEEE802.1X	Off
					LLTD	Off
					REST	Off
					REST over SSL	Off

Item						Value
Security Settings	Device Security	Device Security Settings	Edit Restriction		Address Book	Administrator Only
					One Touch Key	Administrator Only
			Authentication Security Settings	User Account Lockout Settings	Lockout Policy	On
	Network Security	Network Security Settings	Secure Protocol Settings	SSL		On
				Serverside Settings	TLS Version	SSL3.0/TLS1.0: Disable TLS1.1: Disable TLS1.2: Enable
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
				Clientside Settings	TLS Version	SSL3.0/TLS1.0: Disable TLS1.1: Disable TLS1.2: Enable
					Certificate Verification	On
Management Settings	Authentication	Settings	Authentication Settings	General	Authentication	Local Authentication
				Local Authorization Settings	Local Authorization	On
				Guest Authorization Settings	Guest Authorization	Off
				Simple Login Settings	Simple Login	Off
	History Settings	History Settings		Job Log History	Recipient E-mail Address	E-mail Address for the administrator of the machine
					Auto Sending	On

Items changed on the machine

Item			Value
System Menu	System/Network	Security Level	Very High
	Internet	Internet Browser	Off

For the procedures for changing the settings, refer to the machine OPERATION GUIDE and Command Center RX User Guide.

After installing the security functions, you can change the security password.

Refer to *page 8* for the procedures.

The administrator of the machine should periodically store the histories, and check each history to make sure there was no unauthorized access or abnormal operation.

Grant regular users permission based on your company rules, and promptly delete any user accounts that stop being used due to retirement or other reasons.

Changing Security Functions

Changing Security Password

You can customize the security password so that only the administrator can use the security functions.

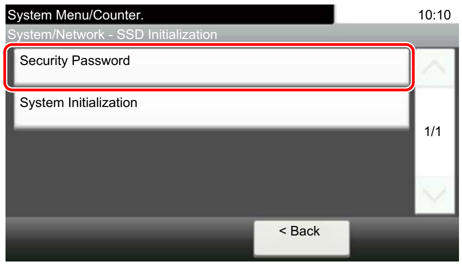
1 Press the [**System Menu/Counter**] key.

2 Press [∨] and [System/Network].

3 If user login is disabled, the user authentication screen appears. Enter your login user name and password and then press [Login]. For this, you need to log in with administrator privileges. Refer to the *machine's Operation Guide* for the default login user name and password.

4 Press [∨], [Data Security] and [SSD Initialization].

5 Enter the security password, and press [OK]. The initial setting for the Security Password is "000000".



6 Press [Security Password].

7 Enter a new security password 6 alphanumeric characters and symbols, and press [Next].

CAUTION: Avoid any easy-to-guess numbers for the security password (e.g. 111111 or 123456).

8 Enter the same password again.

9 Press [OK].

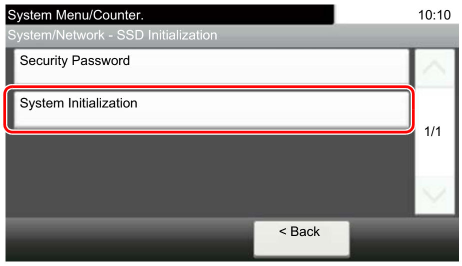
System Initialization

Overwrite all the data stored in the SSD when disposing of the machine.

CAUTION: If you accidentally turn the power switch off during initialization, the SSD might possibly crash or initialization might fail

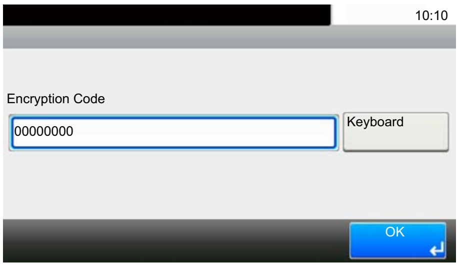
NOTE: If you accidentally turn the power switch off during initialization, turn the power switch on again. Initialization automatically restarts.

1. Press the [**System Menu/Counter**] key.
2. Press [∨] and [System/Network].
3. If user login is disabled, the user authentication screen appears. Enter your login user name and password and then press [Login]. For this, you need to log in with administrator privileges. Refer to the *machine's Operation Guide* for the default login user name and password.
4. Press [∨], [Data Security] and [SSD Initialization].
5. Enter the security password, and press [OK]. The initial setting for the Security Password is "000000".
6. Press [System Initialization].
7. Press [Start] on the screen to confirm the initialization. Initialization starts.
8. When the screen appears to show initialization is completed, check that the memory indicator is OFF, and turn the power switch off and then on.



Warning Message

If the encryption code information of the machine has been lost for some reason, the screen shown here appears when the power is turned on.



10:10

Encryption Code

00000000

Follow the steps below.

1. Enter the encryption code that was entered during the installation of the security functions.

CAUTION: Even though entering a different encryption code can also enable continuation of a job, this will overwrite all the data stored in the SSD. Exercise extreme caution when entering an encryption code.

The encryption code is not the same as the security password.

2. Press [OK].
3. Confirm that the memory indicator is off. After that, turn the power switch off and on.

Disposal

If the machine is unused and demolished, initialize the system of this product to erase the SSD data.

If the machine is unused and demolished, obtain directions for disposal from the dealer (from which you purchased the machine) or your service representative.

Appendix

List of factory default settings

The default settings for security mode are shown below.

Items changed in Command Center RX

Item						Value
Device Settings	Energy Saver/Timer	Energy Saver/Timer Settings		Timer Settings	Auto Panel Reset	On
					Panel Reset Timer	90 seconds
Function Settings	Printer	Printer Settings	Google Cloud Print Settings (Select [Settings])	Privet(Cloud Device Local Discovery Protocol and API)	Local Discovery	On
					Local Print	Setting any value
	Forwarding	Forward Settings			Forward	On
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	On
				IPSec Settings	IPSec	Off

Item						Value
Network Settings	Protocol	Protocol Settings		Print Protocols	NetBEUI	On
					LPD	On
					FTP Server (Reception)	On
					IPP	Off
					IPP over SSL	On
					IPP Authentication	Off
					Raw	On
					WSD Print	On
					POP3 (E-mail RX)	Off
				Send Protocols	SMTP (E-mail TX)	Off
					FTP Client (Transmission)	On
					SMB	On
					WSD Scan	Off
					eSCL	On
					eSCL over SSL	On
				Other Protocols	SNMPv1/v2c	On
					SNMPv3	Off
					HTTP	On
					HTTPS	On
					Enhanced WSD	On
					Enhanced WSD over SSL	On
					LDAP	Off
					IEEE802.1X	Off
					LLTD	On
					REST	On
					REST over SSL	On
Security Settings	Device Security	Device Security Settings	Edit Restriction		Address Book	Off
					One Touch Key	Off
			Authentication Security Settings	User Account Lockout Settings	Lockout Policy	Off

Item						Value
Security Settings	Network Security	Network Security Settings	Secure Protocol Settings	SSL		On
				Serverside Settings	TLS Version	SSL3.0/TLS1.0: Enable TLS1.1: Enable TLS1.2: Enable
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
				Clientside Settings	TLS Version	SSL3.0/TLS1.0: Enable TLS1.1: Disable TLS1.2: Disable
					Certificate Verification	On
Management Settings	Authentication	Settings	Authentication Settings	General	Authentication	Off
				Local Authorization Settings	Local Authorization	Off
				Guest Authorization Settings	Guest Authorization	Off
				Simple Login Settings	Simple Login	Off
	History Settings	History Settings		Job Log History	Recipient E-mail Address	No setting
					Auto Sending	Off

Items changed on the machine

Item			Value
System Menu	System/Network	Security Level	High
	Internet	Internet Browser	Off

2019.3
3MS2WLKDEN0