kyoceradocumentsolutions.com

Data Encryption/Overwrite Operation Guide

ECOSYS PA4000cx ECOSYS PA3500cx

2023.2
3MS2Z1KDEN0

Introduction

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)

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

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

Security Functions

The security functions enable overwriting and encryption.

Overwriting

Printers store print jobs as data in the SSD, and print 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 delete and overwrite (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

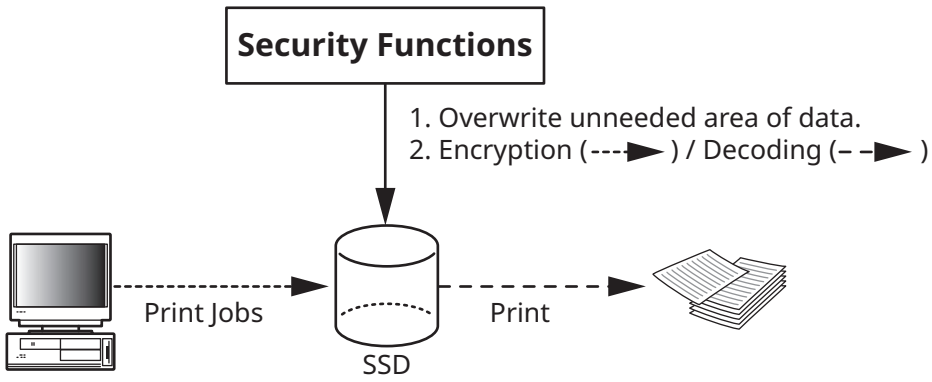
Printers store Custom Box and Job Box data in the SSD. It means the data could be possibly leaked or tampered with if the SSD is stolen.

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

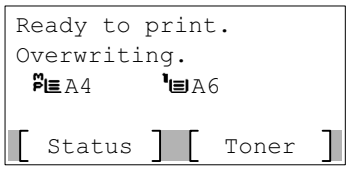
Encryption is automatically performed and no special procedure is required.

CAUTION: Encryption helps enhance security. However, data stored in a Custom Box or Job Box can be decoded by the normal printing operation. Never store confidential data in a Custom Box or Job Box.

Security Functions



Message Display after the Security Functions are Installed



When the security functions have been installed and is running properly, *Overwriting.* appears in the message display 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 Printer currently used.
- The network to which the machine is hooked up must be protected by a firewall to prevent extraneous attacks.

Installation

Installation of the security functions should be performed by the service personnel.

The administrator should log in the menu to enter the encryption code under the supervision of the service representative.

Encryption Code

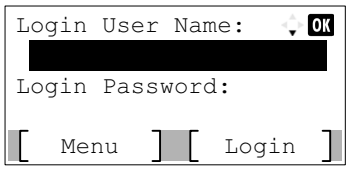
An encryption code of 8 alphanumeric characters (0 to 9, A to Z, a to z) to encrypt data needs to be entered. By default, the code is set *00000000*.

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.



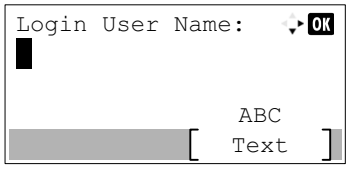
1 Press the [**Menu**] key.

2 Press the ▲ or ▼ key to select [Op Functions], and then press the [**OK**] key.

3 The Login screen appears.

NOTE: When user login administration is set:

- When logged in as an administrator, the log in screen is not displayed and the System/Network menu screen is displayed.
- The setting is not possible when logged in as anyone other than an administrator. Log in again as an administrator.

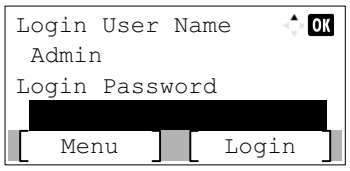


4 With the "Login User Name" entry field selected, press the [**OK**] key. The "Login User Name" entry screen is displayed.

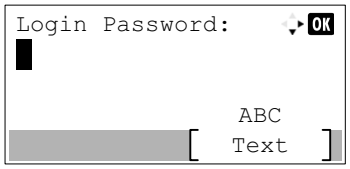
5 Enter the Login User Name using the numeric keys then press the [**OK**] key. The log in screen reappears.

NOTE: The initial setting for the administrator's Login User Name is "Admin".

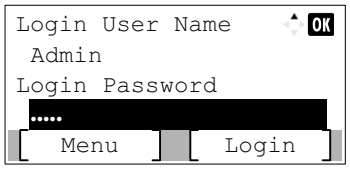
- For details on entering characters, refer to the machine's *Operation Guide*.



6 Press the ▲ or ▼ key to select the "Login Password" entry field.



7 Press the [**OK**] key. The "Login Password" entry screen is displayed.



8 Enter the Login Password using the numeric keys then press the [**OK**] key. The log in screen reappears.

NOTE: The initial setting for the administrator's Login Password is "Admin".

9 Pressing [Login]. If the entered Login User Name and Login Password are correct, the Op Functions menu screen appears.

10 Press the ▲ or ▼ key to select the [DATA SECURITY].

11 Press the [**OK**] key. The DATA SECURITY menu screen appears.

12 Press the ▲ or ▼ key to select the [License On].

13 Press the [**OK**] key. The License On menu screen appears.

14 Press the ▲ or ▼ key to select the [Official].

15 Press the [**OK**] key. The entering License key screen appears.

16 Enter the license key using the numeric keypad, and then press the [**OK**] key. A confirmation screen will appear.

17 Pressing [Yes].

18 Turn the power switch on again following to the indication in the panel 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
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	Off
				IPSec Settings	IPSec	On
					Restriction	Allowed
		Allowed IPSec Rules* ("Settings" selection of any of Rule No.)	Policy		Rule	On
					Key Management Type	IKEv1
					Encapsulation Mode	Transport
			IP Address		IP Version	IPv4
					IP Address (IPv4)	IP Address of the destination terminal
					Subnet Mask	Setting any value
			Authentication	Local Side	Authentication Type	Pre-shared Key
					Pre-shared Key	Setting any value

Item					Value
Network Settings	TCP/IP	Allowed IPSec Rules* ("Settings" selection of any of Rule No.)	Key Exchange (IKE phase1)	Mode	Main mode
				Hash	MD5:Disable, SHA1:Disable, SHA-256:Enable, SHA-384:Enable, SHA-512:Enable AES-XCBC:Disable
				Diffie-Hellman Group	Select one from following option. modp2048(14), modp4096(16), modp6144(17), modp8192(18), ecp256(19), ecp384(20), ecp521(21), modp1024s160 (22), modp2048s224 (23), modp2048s256 (24)
			Data Protection (IKE phase2)	Protocol	ESP
				Hash	MD5:Disable, SHA1:Disable, SHA-256:Enable, SHA-384:Enable, SHA-512:Enable, AES-XCBC: Setting any value, AES-GCM-128:Enable, AES-GCM-192:Enable, AES-GCM-256:Enable, AES-GMAC128: Setting any value, AES-GMAC-192: Setting any value, AES-GMAC-256: Setting any value

Item					Value
Network Settings	Protocol	Protocol Settings	Print Protocols	NetBEUI	Off
				LPD	Off
				FTP Server (Reception)	Off
				IPP	Off
				IPP over TLS	On
				IPP Authentication	Off
				Raw	Off
				WSD Print	Off
				POP3 (E-mail RX)	Off
Network Settings	Protocol	Protocol Settings	Send Protocols	SMTP (E-mail TX)	On
				SMTP (E-mail TX) - Certificate Auto Verification	Validity Period: Enable
			Other Protocols	SNMPv1/v2c	Off
				SNMPv3	Off
				HTTP	Off
				HTTPS	On
				HTTP(Client side) - Certificate Auto Verification	Validity Period : Enable
				Enhanced WSD	Off
				Enhanced WSD(TLS)	On
				LDAP	Off
				IEEE802.1X	Off
				LLTD	Off
				REST	Off
				REST over TLS	Off
				VNC(RFB)	Off
				VNC(RFB) over TLS	Off
				Enhanced VNC(RFB) over TLS	Off
Security Settings	Device Security	Device Security Settings	Job Status/Job Log Settings	Display Jobs Detail Status	My Jobs Only
				Display Jobs Log	My Jobs Only

Item						Value
Security Settings	Network Security	Network Security Settings	Secure Protocol Settings	TLS		On
				Serverside Settings	TLS Version	TLS1.0: Disable TLS1.1: Disable TLS1.2: Enable TLS1.3: Enable
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Setting any value CHACHA20/POLY1305: Setting any value
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
					Enhanced WSD Security	Secure Only (Enhanced WSD over TLS)
				Clientside Settings	TLS Version	TLS1.0: Disable TLS1.1: Disable TLS1.2: Enable TLS1.3: Enable
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Setting any value CHACHA20/POLY1305: Setting any value
Management Settings	Authentication	Settings	Authentication Settings	General	Authentication	Local Authentication
	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
Menu	Security	Security Level	Very High

For the procedures for changing the settings, refer to the machine Operation Guide and Command Center RX User Guide.
After changing the settings, run [Software verification] in the menu to verify that the machine operates correctly. Periodically perform [Software verification] after installation as well.
After installing the security functions, you can change the security password.
Refer to *page 13* 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.

IPsec setting

It is possible to protect data by enabling the IPsec function that encrypts the communication path.
Please note the following points when enabling the IPsec function.

- The value set by the IPsec rule has to be matched with the destination PC. Communication error occurs in case the setting does not match.
- IP address set by the IPsec rule has to be matched with the IP address of the SMTP server which is set on the main unit.
- In case the setting does not match, data sent by mail can’t be encrypted.
- Pre-shared key set by the IPsec rule has to be created by using the alphanumeric symbols of 8 digits or more which will not be easily guessed.

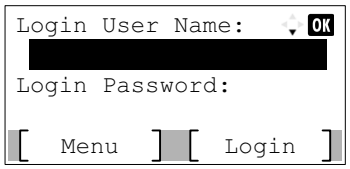
Changing Data Security Functions

Enter the security password to change data security functions.

1 Press the [**Menu**] key.

2 Press the ▲ or ▼ key to select [Security], and then press the [**OK**] key.

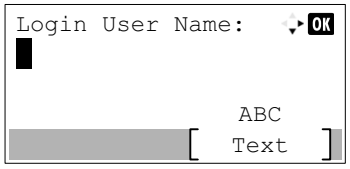
3 The Login screen appears.



NOTE: When user login administration is set:

- When logged in as an administrator, the log in screen is not displayed and the System/Network menu screen is displayed.
- The setting is not possible when logged in as anyone other than an administrator. Log in again as an administrator.

4 With the "Login User Name" entry field selected, press the [**OK**] key. The "Login User Name" entry screen is displayed.

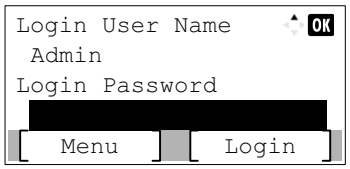


5 Enter the Login User Name using the numeric keys then press the [**OK**] key. The log in screen reappears.

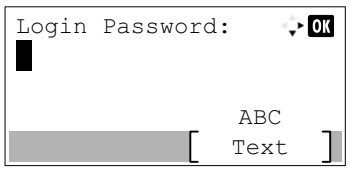
NOTE: The initial setting for the administrator's Login User Name is "Admin".

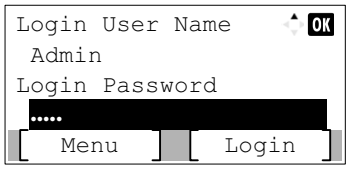
- For details on entering characters, refer to the machine's *Operation Guide*.

6 Press the ▲ or ▼ key to select the "Login Password" entry field.



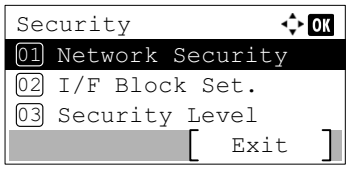
7 Press the [**OK**] key. The "Login Password" entry screen is displayed.





8 Enter the Login Password using the numeric keys then press the [**OK**] key. The log in screen reappears.

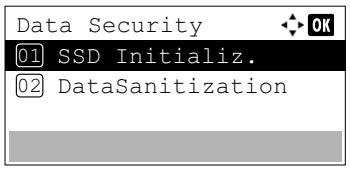
NOTE: The initial setting for the administrator's Login Password is "Admin".



9 Pressing [Login]. If the entered Login User Name and Login Password are correct, the Security menu screen appears.

10 Press the ▲ or ▼ key to select [Data Security].

11 Press the [**OK**] key. The Data Security screen appears.

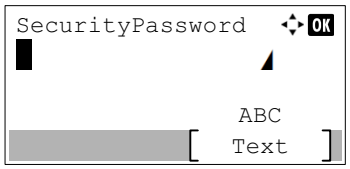


Changing Security Password

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

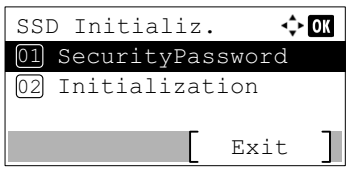
1 In the Data Security menu, press the [?] or [?] key to select [SSD Initializ.].

2 Press the [**OK**] key. The "SecurityPassword" entry screen appears.



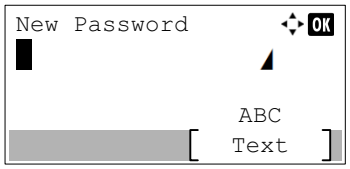
3 Enter the Security Password using the numeric keys.

NOTE: The initial setting for the Security Password is "000000".



4 Press the [**OK**] key. If the Security Password entered is correct, the "SSD Initializ." menu screen appears. If the Security Password entered was not correct, "Incorrect password." is displayed and the SecurityPassword screen reappears. Enter the correct Security Password.

5 In the SSD Initializ. menu, press the ▲ or ▼ key to select [Security Passwd].

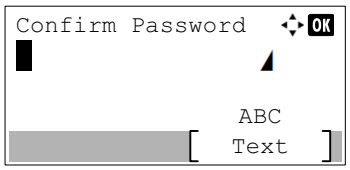


6 Press the [**OK**] key. The "New Password" entry screen appears.

7 Enter the new Security Password using the numeric keys.

The security password must be 6 alphanumeric characters.

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



8 Press the [**OK**] key. The "Confirm Password" entry screen appears.

9 To confirm, re-enter the security password to be registered. Enter the new Security Password using the numeric keys.

10 Press the [**OK**] key. If the Security Password entered matches then the password is changed to the new password and the SSD Initializ. menu reappears.

If the password does not match, "Incorrect password." is displayed and the "New Password" screen reappears. Enter again from the new Security Password.

System Initialization

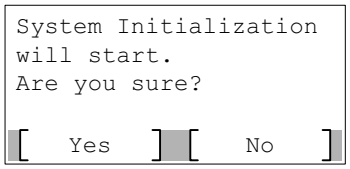
Overwrite all the data stored in the SSD when disposing of the machine.

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 In the SSD Initializ. menu, press the [?] or [?] key to select [Initialization].

2 Press the [**OK**] key. A confirmation message is displayed.



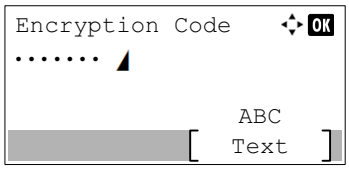
3 Press [Yes]. Initialization starts.

If you do not wish to initialize, press [No]. The SSD Initializ. menu reappears.

4 When the initialization is finished Task is completed. is displayed. 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.



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 the [**OK**] key.

3 When the Task is completed. screen appears, turn the power switch off and then 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
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	On
				IPSec Settings	IPSec	Off
					Restriction	Allowed
		IPSec Rules ("Settings" selection of any of Rule No.)	Policy		Rule	Off
					Key Management Type	IKEv1
					Encapsulation Mode	Transport
			IP Address		IP Version	IPv4
					IP Address (IPv4)	No setting
					Subnet Mask	No setting
			Authentication	Local Side	Authentication Type	Pre-shared Key
					Pre-shared Key	No setting
Network Settings	TCP/IP	IPSec Rules ("Settings" selection of any of Rule No.)	Key Exchange (IKE phase1)		Mode	Main Mode
					Hash	MD5: Disable, SHA1: Enable, SHA-256: Enable, SHA-384: Enable, SHA-512: Enable AES-XCBC: Disable
					Encryption	3DES: Enable, AES-CBC-128: Enable, AESCBC-192: Enable, AESCBC-256: Enable, AESCBC-128: Enable, AESCBC-192: Enable, AESCBC-256: Enable
					Diffie-Hellman Group	modp1024(2)
					Lifetime (Time)	28800 seconds

Item					Value
Network Settings	TCP/IP	IPSec Rules ("Settings" selection of any of Rule No.)	Data Protection (IKE phase2)	Protocol	ESP
				Hash	MD5: Disable, SHA1: Enable, SHA-256: Enable, SHA-384: Enable, SHA-512: Enable, AES-XCBC: Disable, AES-GCM-128: Enable, AES-GCM-192: Enable, AES-GCM-256: Enable, AES-GMAC-128: Disable, AES-GMAC-192: Disable, AES-GMAC-256: Disable
				Encryption	3DES: Enable, AES-CBC-128: Enable, AES-CBC-192: Enable, AES-CBC-256: Enable, AES-GCM-128: Enable, AES-GCM-192: Enable, AES-GCM-256: Enable, AES-CTR: Disable
				PFS	Off
				Lifetime Measurement	Time & Data Size
				Lifetime (Time)	3600 seconds
				Lifetime (Data Size)	100000KB
				Extended Sequence Number	Off

Item					Value
Network Settings	Protocol	Protocol Settings	Print Protocols	NetBEUI	On
				LPD	On
				FTP Server (Reception)	On
				IPP	Off
				IPP over TLS	On
				IPP Authentication	Off
				Raw	On
				WSD Print	On
				POP3 (E-mail RX)	Off
			Send Protocols	SMTP (E-mail TX)	Off
			Other Protocols	SNMPv1/v2c	On
				SNMPv3	Off
				HTTP	On
				HTTPS	On
				HTTP(Client side) - Certificate Auto Verification	Validity Period: Enable
				Enhanced WSD	On
				Enhanced WSD(TLS)	On
				LDAP	Off
				IEEE802.1X	Off
				LLTD	On
				REST	On
				REST over TLS	On
				VNC(RFB)	Off
				VNC(RFB) over TLS	Off
				Enhanced VNC(RFB) over TLS	On
Security Settings	Device Security	Device Security Settings	Job Status/Job Log Settings	Display Jobs Detail Status	Show All
				Display Jobs Log	Show All

Item						Value
Security Settings	Network Security	Network Security Settings	Secure Protocol Settings	TLS		On
				Serverside Settings	TLS Version	TLS1.0: Disable TLS1.1: Enable TLS1.2: Enable TLS1.3: Enable
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Disable, CHACHA20/POLY1305: Enable
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
					Enhanced WSD Security	Secure Only (Enhanced WSD over TLS)
				Clientside Settings	TLS Version	TLS1.0: Disable TLS1.1: Enable TLS1.2: Enable TLS1.3: Enable
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Enable, CHACHA20/POLY1305: Enable
Management Settings	Authentication	Settings	Authentication Settings	General	Authentication	Off
	History Settings	History Settings		Job Log History	Recipient E-mail Address	No setting
					Auto Sending	Off

Items changed on the machine

Item			Value
Menu	Security	Security Level	High

The initial value of the custom box

Item	Value
Owner	Local User
Permission	Private

Log information

The following settings and status regarding security are shown in the machine log.

- Event date and time
- Type of event
- Information of the log in user or the user who attempted to log in
- Event result (Success or fail)

Event to be displayed in the log

Log	Event
Job Logs	End job/Check job status/Change job/Cancel job