Data Encryption/Overwrite
OPERATION GUIDE

KYOCERA
Document Solutions

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.

NOTE: If you install the security functions, *Running security function...* appears when the machine starts up and it may take a while.

Overwriting

Multi-functional products (MFPs) temporarily store the data of scanned originals and print jobs, as well as other data stored by users, on the hard disk or in FAX memory, and the job is output from that data. As the data storage areas used for such data remain unchanged on the hard disk or in FAX memory until they are overwritten by other data, the data stored in these areas is potentially restorable using special tools.

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 was stored on the hard disk/SSD or in FAX memory.

Overwrite Methods

Changing the data overwrite method is available, when a hard disk is installed. There are two overwrite methods, which can be switched at any time.

Once Overwrite Method

This function overwrites unneeded data areas (in the case of overwriting) or all areas (in the case of system initialization) with zeroes to prevent data restoration.

3-time Overwrite (DoD) Method (default)

This overwrite method complies with U.S. Department of Defense (DoD) standards, and overwrites unneeded data areas of the hard disk and FAX memory (in the case of overwriting) or all areas (in the case of system initialization) with specific characters, their complements, and random characters to prevent data restoration. Data restoration is not possible even when sophisticated restoration techniques are used, and a higher level of security than Once Overwrite is obtained.

This method may take more time than Once Overwrite method to process a larger amount of data.

NOTE: For SSD and FAX memory, the method used is Once Overwrite.

Encryption

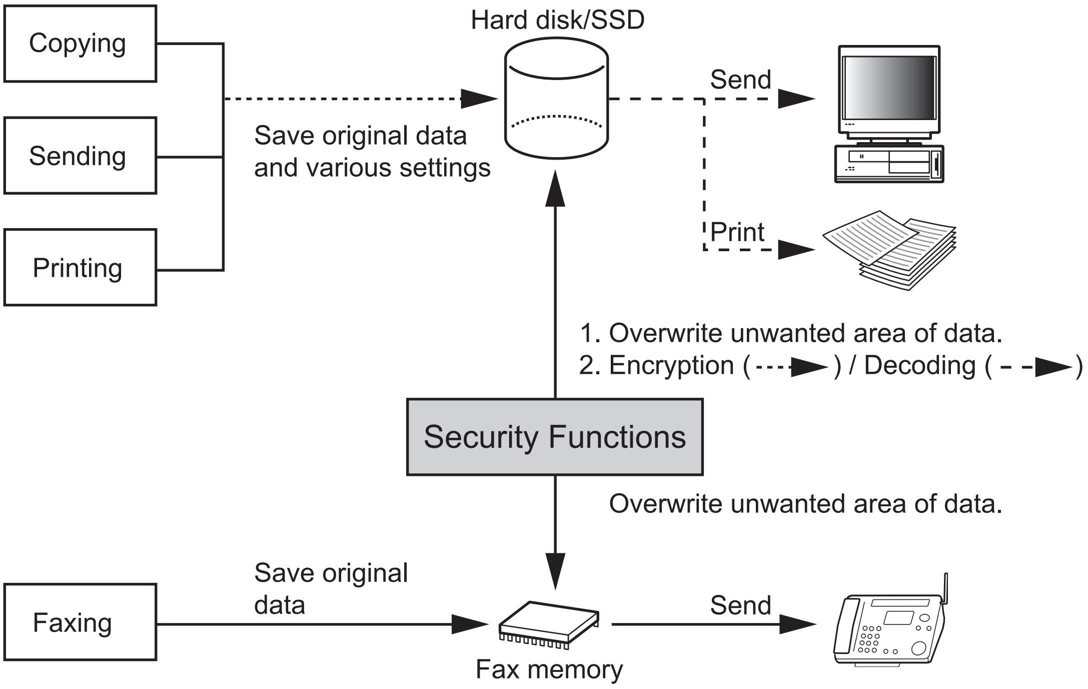
MFPs store the data of scanned originals and other data stored by users in the hard disk/SSD. It means the data could be possibly leaked or tampered with if the hard disk/SSD is stolen.

The security functions encrypt data before storing it in the hard disk/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.

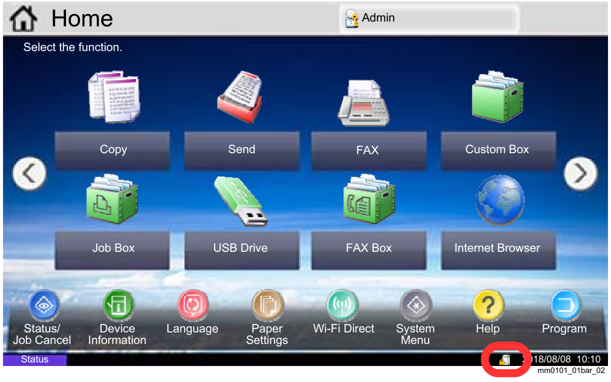
Security Functions



- If the security functions are introduced while the hard disk and SSD are installed in the machine, the destination where data received by FAX is to be saved is changed from SSD to hard disk. If you want to change the destination to SSD, contact your dealer or service technician.

Touch Panel Display after the Security Functions are Installed

Hard Disk Icon Display



In Security Mode, the security functions have been properly installed and is running. The hard disk icon appears on the lower right side of the touch panel in Security Mode.

NOTE: If the hard disk icon does not appear on the normal screen, it is possible that the Security Mode is not ON. Call service.

The hard disk icon display changes as follows during overwriting

The table below shows the icons displayed and their descriptions.

Icon displayed	Description
🟧	There is unneeded data on the hard disk/SSD or in FAX memory.
🟩	Overwriting the unwanted data
⬜	The unwanted data is overwritten.

CAUTION: Do not turn the power switch off while 🟩 is displayed. Risk of damage to the hard disk/SSD or FAX memory.

NOTE: If you turn the machine off at the power switch during overwriting, data may not be overwritten completely from the hard disk. Turn the machine back on at the power switch. Overwriting automatically resumes. If you accidentally turn the main power switch off during overwriting or initialization, the hard disk icon might not switch to the second icon shown above. This would be caused by a possible crash or failed overwriting of the data to be overwritten. This will not affect subsequent overwriting processes. However, hard disk initialization is recommended so as to return to normal stable operations. (Initialization should be performed by the administrator following the steps in *System Initialization on page 15*.)

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

The Security Functions Contents

The security functions package includes:

- License Certificate
- Installation Guide (for service personnel)
- Notice

In case of the standard specification, there will be no bundled items included.

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 hard disk/SSD will be initialized during installation of the security functions. This means that the data stored in the hard disk 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.
- The Repeat Copy function will be unavailable after the installation.
- [Adjustment/Maintenance] -> [System Initialization] will not be displayed in the *System Menu* after the installation.
- 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.

- If the security functions are introduced while the hard disk and SSD are installed in the machine, the destination where data received by FAX is to be saved is changed from SSD to hard disk. If you want to change the destination to SSD, contact your dealer or service technician.

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 and securely manage 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 hard disk/SDD 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 [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.

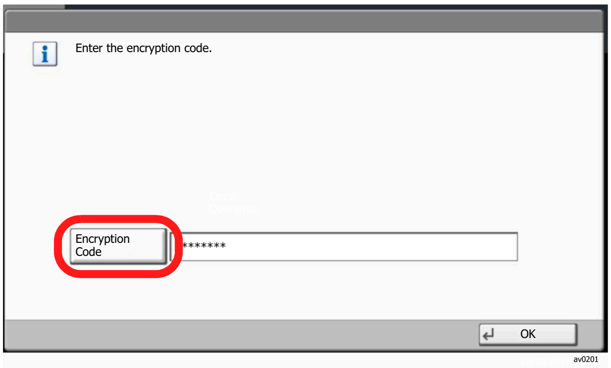
3 Press [Next] of *Optional Function*.

4 The optional function screen is displayed. Select *Data Encryption/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.

7 The screen for entering the encryption code is displayed. If you want to change the encryption code, change it by the following procedure. If the encryption code is not changed, go to the procedure 10.



Enter the encryption code.

8 Press [Encryption Code].

9 Press [Backspace] and enter the 8-digit alphanumeric encryption code (0 to 9, A to Z, a to z) after erasing [00000000], and press [OK].

10 Press [OK]. Hard disk/SSD formatting begins.

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

12 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	General		Remote Printing	Prohibit
			Google Cloud Print Settings (Select [Settings])	Privet(Cloud Device Local Discovery Protocol and API)	Local Discovery	Off
					Local Print	Off
	FAX/i-FAX	FAX/i-FAX Settings	Fax Settings	Remote Settings	FAX Remote Diagnostics	Off
	RX/Forward Rules	Settings	RX/Forward Rules Settings		RX/Forward Rules	[Use Rule for Specific RX] or [Rule for All RX]
				Forward Settings	Forwarding	On
					Forward Destination	Any forwarding destination
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	Off
				IPSec Settings	IPSec	On
					Restriction	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
			Key Exchange (IKE phase1)			Setting any value(Always the Mode selects the Main mode)
			Data Protection (IKE phase2)			Setting any value(Always the Protocol selects the ESP)

Item					Value
Network Settings	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
				DSM Scan	Off
				eSCL	Off
				eSCL over SSL	Off
			Other Protocols	SNMPv1/v2c	Off
				SNMPv3	Off
				HTTP	Off
				HTTPS	On
				Enhanced WSD	Off
				Enhanced WSD(SSL)	On
				LDAP	Off
				IEEE802.1X	Off
				LLTD	Off
				REST	Off
				REST over SSL	Off
				VNC(RFB)	Off
				VNC(RFB) over SSL	Off
				Enhanced VNC(RFB) 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	Password Policy Settings	Password Policy	On
					Maximum password age	Setting any value
					Minimum password length	On 8 or more characters
					Password complexity	Setting any value
Security Settings	Device Security	Device Security Settings	Authentication Security Settings	User Account Lockout Settings	Lockout Policy	On
					Number of Retries until Locked	Setting any value
					Lockout Duration	Setting any value
					Lockout Target	All
	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
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Setting any value
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
					Enhanced WSD Security	Secure Only (Enhanced WSD over SSL)
				Clientside Settings	TLS Version	SSL3.0/TLS1.0: Disable TLS1.1: Disable TLS1.2: Enable
					Effective Encryption	ARCFOUR: Disable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Setting any value
					Certificate Verification	On

Item						Value
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
				Login History Settings	Login History	On
					Recipient E-mail Address	E-mail Address for the administrator of the machine
					Auto Sending	On
				Device Log History Settings	Device Log History	On
					Recipient E-mail Address	E-mail Address for the administrator of the machine
					Auto Sending	On
				Secure Communication Error Log History Settings	Secure Communication Error Log History	On
					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 changing the settings, run [Software verification] in the system 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 as well as the method for overwriting the entire hard disk.

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 or FTP server which is set on the main unit.
- In case the setting does not match, data sent by mail or FTP 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 Security Functions

Changing Security Password

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

Use the procedure below to change the security password.

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

2 Press [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.

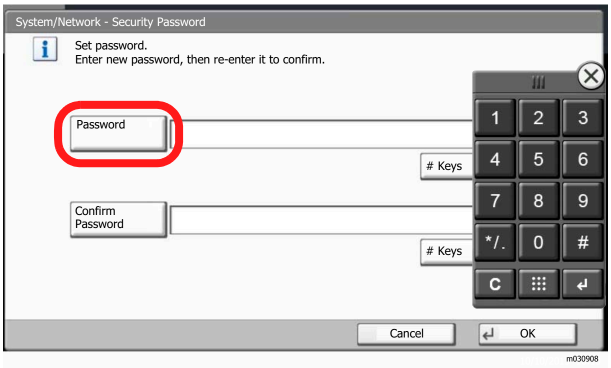
4 Press [Next] of *Data Security.*

5 Press [Next] of *SSD Initialization.*

NOTE: When a hard disk is installed, "Hard Disk Initialization" is displayed. When a hard disk and an SSD are installed, "Hard Disk/SSD Initialization" is displayed.

6 Enter the default security password, *000000*.

7 Press [Change] of *Security Password.*



System/Network - Security Password

Set password.
Enter new password, then re-enter it to confirm.

8 Press [Password] to enter a new security password 6 to 16 alphanumeric characters and symbols.

CAUTION: Avoid any easy-to-guess numbers for the security password (e.g. 11111111 or 12345678).

9 Press [Confirm Password] to enter the same password again.

10 Press [OK].

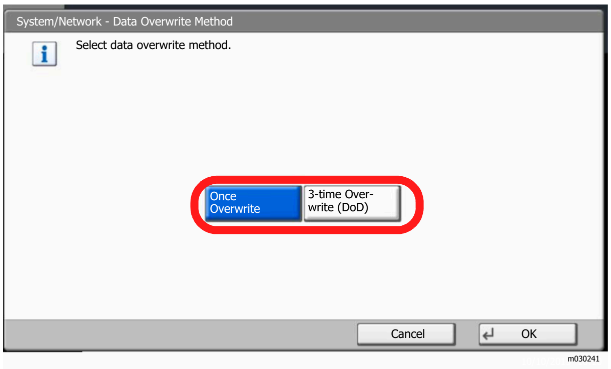
Changing the Data Overwrite Method

The method used to overwrite data can be changed. Refer to *Overwriting on page 2* for details. Changing the data overwrite method is not available, when a hard disk is not installed.

NOTE: The overwrite methods are used both for overwriting and hard disk initialization, and cannot therefore be set individually.

Use the procedure below to select the interface.

1. Press the [**System Menu/Counter**] key.
2. Press [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 [Next] of *Data Security.*
5. Press [Next] of *Hard Disk Initialization.*
6. Enter the security password. By default, the code is set *000000*.
7. Press [Change] of *Data Overwrite Method*.
8. Press [3-time Overwrite (DoD)] (default) or [Once Overwrite].
9. Press [OK].



System/Network - Data Overwrite Method

Select data overwrite method.

System Initialization

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

CAUTION: If you accidentally turn the power switch off during initialization, the system 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.

Use the procedure below to initialize the system.

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

2 Press [System/Network].

3 If the user authentication screen appears, enter the login user name and login password, and press [Login].

For this, you need to log in with administrator privileges. If the user authentication screen does not appear, go to Step 4.

4 Press [Next] of *Data Security.*

5 Press [Next] of *SSD Initialization.*

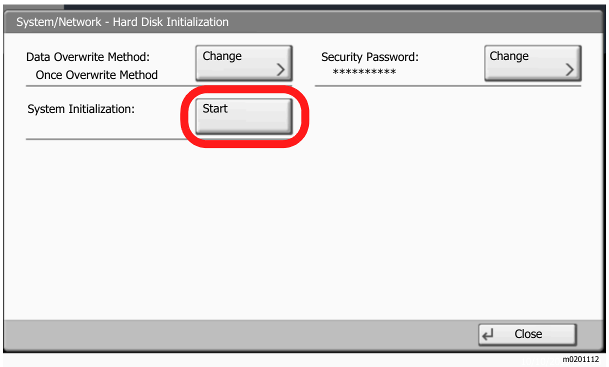
NOTE: When a hard disk is installed, "Hard Disk Initialization" is displayed. When a hard disk and an SSD are installed, "Hard Disk/SSD Initialization" is displayed.

6 Enter the default security password, *000000*.

7 Press [Execute] of *System Initialization*.

8 Press [Yes] on the screen to confirm the initialization. Initialization starts.

9 When the screen appears to show initialization is completed, turn the power switch off and then on.


System/Network - Hard Disk Initialization

Data Overwrite Method: Once Overwrite Method

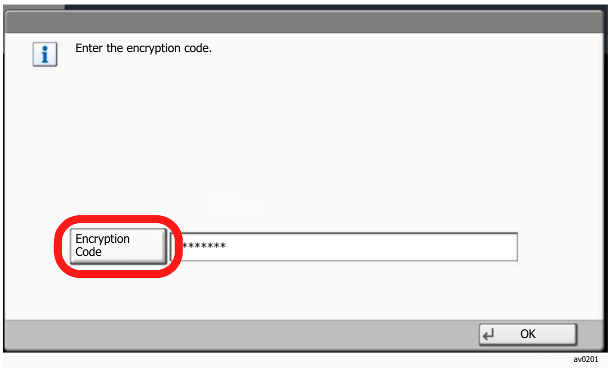
Security Password: **********

System Initialization:

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.



Enter the encryption code.

1 Press [Encryption Code], and 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 hard disk/ SSD. Exercise extreme caution when entering an encryption code.

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

2 Turn the power switch off and on.

Disposal

If the machine is unused and demolished, initialize the system of this product to erase the hard disk/SSD data and FAX memory.

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	General		Remote Printing	Permit
			Google Cloud Print Settings (Select [Settings])	Privet(Cloud Device Local Discovery Protocol and API)	Local Discovery	On
					Local Print	On
	FAX/i-FAX	FAX/i-FAX Settings	Fax Settings	Remote Settings	FAX Remote Diagnostics	Off
	RX/Forward Rules	Settings	RX/Forward Rules Settings		RX/Forward Rules	Off
				Forward Settings	Forwarding	Off
					Forward Destination	No setting
Network Settings	TCP/IP	TCP/IP Settings		Bonjour Settings	Bonjour	On
				IPSec Settings	IPSec	Off
					Restriction	Allowed

Item						Value
Network Settings	TCP/IP	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
			Key Exchange (IKE phase1)		Mode	Main Mode
					Hash	SHA1
					Encryption	3DES, AES-CBC-128, AES-CBC-192, AES-CBC-256
					Diffie-Hellman Group	modp1024(2)
					Lifetime (Time)	28800 seconds
			Data Protection (IKE phase2)		Protocol	ESP
					Hash	SHA1
					Encryption	3DES, AES-CBC-128, AES-CBC-192, AES-CBC-256
					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 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	On
				DSM Scan	Off
				eSCL	On
				eSCL over SSL	On
			Other Protocols	SNMPv1/v2c	On
				SNMPv3	Off
				HTTP	On
				HTTPS	On
				Enhanced WSD	On
				Enhanced WSD(SSL)	On
				LDAP	Off
				IEEE802.1X	Off
				LLTD	On
				REST	On
				REST over SSL	On
				VNC(RFB)	Off
				VNC(RFB) over SSL	Off
				Enhanced VNC(RFB) over SSL	On

Item						Value
Security Settings	Device Security	Device Security Settings	Edit Restriction		Address Book	Off
					One Touch Key	Off
			Authentication Security Settings	Password Policy Settings	Password Policy	Off
					Maximum password age	Off
					Minimum password length	Off
					Password complexity	No more than two consecutive identical char
Security Settings	Device Security	Device Security Settings	Authentication Security Settings	User Account Lockout Settings	Lockout Policy	Off
					Number of Retries until Locked	3 times
					Lockout Duration	1 minute
					Lockout Target	Remote Login Only
	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
					Effective Encryption	ARCFOUR: Enable, DES: Disable, 3DES: Enable, AES: Enable, AES-GCM: Disable
					HTTP Security	Secure Only (HTTPS)
					IPP Security	Secure Only (IPPS)
					Enhanced WSD Security	Secure Only (Enhanced WSD over SSL)
				Clientside Settings	TLS Version	SSL3.0/TLS1.0: Enable TLS1.1: Disable TLS1.2: Disable
					Effective Encryption	ARCFOUR: Enable, DES: Enable, 3DES: Enable, AES: Enable, AES-GCM: Disable
					Certificate Verification	On

Item						Value
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
				Login History Settings	Login History	Off
					Recipient E-mail Address	No setting
					Auto Sending	Off
				Device Log History Settings	Device Log History	Off
					Recipient E-mail Address	No setting
					Auto Sending	Off
				Secure Communication Error Log History Settings	Secure Communication Error Log History	Off
					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

The initial value of the custom box

Item	Value
Box Owner	None
Box Permission	Private