



**MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS**

# **High Security Mode Management Guide**

---

**ES9466 MFP/ES9476 MFP**



# Preface

---

Thank you for purchasing Oki Multifunctional Digital Systems or Multifunctional Digital Color Systems. This manual explains about the conditions and settings for using the Multifunctional Digital Systems which complies with IEEE Std 2600.1™-2009. Read this manual carefully before using your Multifunctional Digital Systems under the high security mode. For the security precautions on operating the equipment complying with IEEE Std 2600.1™-2009, refer to “Security Precautions” in the “Safety Information”. Keep this manual within easy reach and use it to maintain the equipment complying with IEEE Std 2600.1™-2009.






## Note

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

## ■ How to read this manual

### □ Symbols in this manual

In this manual, some important items are 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, may 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.
-  **Index** Pages describing items related to what you are currently doing. See these pages 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.

### □ Optional equipment

For the available options, refer to the **Quick Start Guide**.

### □ Trademarks

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



# CONTENTS

---

<b>Preface</b> .....	<b>3</b>
How to read this manual .....	3

## **Chapter 1 The High Security Mode**

---

<b>Precautions on Using the High Security Mode</b> .....	<b>8</b>
Confirmation of the mode .....	9
Operational conditions.....	10

## **Chapter 2 UNIQUE FUNCTIONS**

---

<b>Temporary Password</b> .....	<b>14</b>
Conditions when a temporary password is used .....	14
Operation by a user when a temporary password is used.....	14
<b>Hold (Fax)</b> .....	<b>15</b>

## **Chapter 3 THE INITIAL VALUES**

---

<b>Precautions on the Initial Values</b> .....	<b>18</b>
Logging in .....	18
Initial value list.....	19



## The High Security Mode

<b>Precautions on Using the High Security Mode .....</b>	<b>8</b>
Confirmation of the mode .....	9
Operational conditions.....	10

## Precautions on Using the High Security Mode

---

This operation mode protects customers' important information against unauthorized access to the equipment and leakage.

The following are the security functions when you operate the equipment complying with IEEE Std 2600.1™-2009.

- User Authentication Setting function
- Role Management function
- Log collecting and browsing function
- Overwriting function of the specified data in HDD when jobs are completed or the power is turned ON
- Communication function with TLS
- Integrity Check function
- Management functions such as:
  - Log, Passwords, User, Password Policy, Date & Time, Auto Clear, Session Timer, Enable/disable of TLS

We have applied for ISO/IEC 15408 certification for the environment where the following equipment is operating in Japanese or English mode and connected to a PC running Windows 7 with Internet Explorer version 9.0.

MFP: ES9466 MFP/ES9476 MFP\*

\* Certification pending (as of April, 2016)

To operate the equipment complying with IEEE Std 2600.1™-2009 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 IEEE Std 2600.1™-2009.

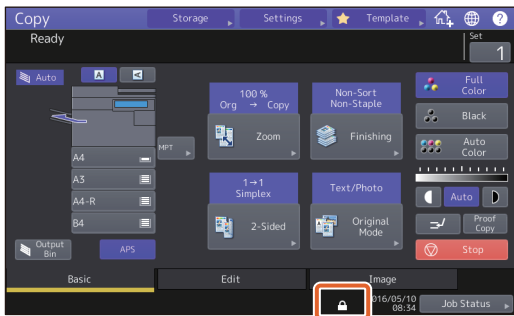
### Tip

For details of each security function and how to set the related items, refer to the **TopAccess Guide**.





## Confirmation of the mode

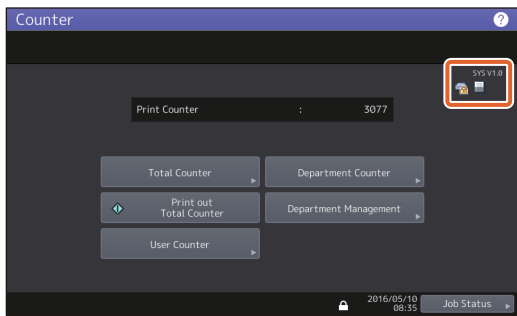
When this equipment is operated under the high security mode,  is displayed on the touch panel of the equipment.



### Tips

- The HDD inside the equipment which is operated under the high security mode is encrypted. Moreover, the Data Overwrite Option (GP-1070) is installed in such equipment. To confirm that each function is operating, check the display at the top right of the [Counter] screen on the touch panel of the equipment.

<p>The HDD is encrypted.</p>	<p> The icon is displayed. The HDD has been encrypted if this equipment is operated under the high security mode.</p>
<p>The Data Overwrite Enabler is operating properly.</p>	<p> The icon showing that the Data Overwrite Enabler is correctly operating is displayed. The version of the system which is running is displayed. (SYS V1.0)</p>



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

---

## ■ Operational conditions

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

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

**Manually select [FULL] and perform the integrity check at the time of installation and during use periodically.**

\* For details of the integrity check, refer to the *MFP Management Guide*.

**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.**

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

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

- Interrupt copy
- Network Fax
- AddressBook Viewer
- File Downloader
- TWAIN Driver
- e-Filing BackUp/Restore Utility
- Scheduled printing
- Storing to e-Filing from a printer driver\*
  - \* The function can be selected; however, an error occurs and the job is deleted. As a result, printing is not performed. When a job is deleted, it is recorded in the error log. Confirm it in the [Logs] tab on TopAccess or [Job Status] - [Log] - [Print] in the equipment.
- Disabling log authentication

**The automatic log-in function in the client software which comes with this equipment is not available. Be sure to enter the user name and password when using client software.**

**Any data sent to this equipment, such as a Fax and Internet Fax printed or received from a printer driver\*, can be outputted only when a user with the printing privilege is logged in.**

\* Use IPP SSL to communicate with this equipment.

---

**When IPP printing is performed, use the port created by entering “https://[IP address]:[SSL port number]/Print” into the URL field.**

(e.g.: https://192.168.1.2:443/Print)

\* For details, refer to [IPP printing] under [Installing Printer Drivers for Windows] - [Other Installations] in the *Software Installation Guide*.

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

**Do not use any applications which need a setting change of the [ODCA] sub menu in the [Setup] menu on the [Administration] tab under TopAccess.**

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

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

**Note**

Perform the setting correctly referring to Initial value list (📖 P.19).

- Use the encrypted PDF format when saving or sending a file and the encryption level shall be 128 bit AES.
- Specify a reliable remote PC for the saving destination of the scan data.
- Do not use PUBLIC BOX in e-Filing since no password can be set.
- Do not use MFP LOCAL since no password can be set.
- Administrators must regularly export and store the logs.

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

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

**When disposing of an MFP, be sure to contact your service technicians to erase the data in the HDD completely.**



## UNIQUE FUNCTIONS

<b>Temporary Password</b> .....	<b>14</b>
Conditions when a temporary password is used .....	14
Operation by a user when a temporary password is used.....	14
<b>Hold (Fax)</b> .....	<b>15</b>

## Temporary Password

---

In the high security mode, a password, tentatively assigned by an administrator to allow a user access, is treated as a temporary one. To use the equipment, you need to register your password after accessing it with the temporary one.

### Note

The security level is insufficient if you continue to use the temporary password. Register your password as soon as possible.

### ■ Conditions when a temporary password is used

A user temporary password is used in the following cases:

- For the first time to log in to the equipment after being registered by an administrator.
- When an administrator resets the user's password.
- When the user information password imported by an administrator is plain text.

### Note

When an administrator resets users' passwords, they must be so notified and prompted to change them to ones of their own choosing.

### Tip

To prevent user information exported from an equipment from being altered, it is hashed. If you change the password for the exported user information, plain text is used for the password.

### ■ Operation by a user when a temporary password is used

#### **If your password can be registered when accessing.**

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

#### **If you cannot register a new password when accessing the equipment.**

In the following utilities, an error occurs when you try to log in to the equipment with a temporary password. Therefore a new password cannot be registered either. Before using these utilities, register a new password on the control panel or in TopAccess.

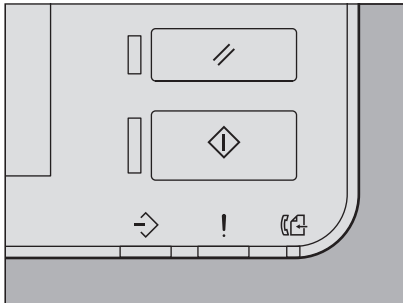
- Remote Scan driver
- e-Filing Web Utility

## Hold (Fax)

In the high security mode, when an email to which a Fax, Internet Fax or image is received, it is not automatically output. These jobs are stored in the [Hold (Fax)] queue and only a user having the [Fax Received Print] privilege can print the job.

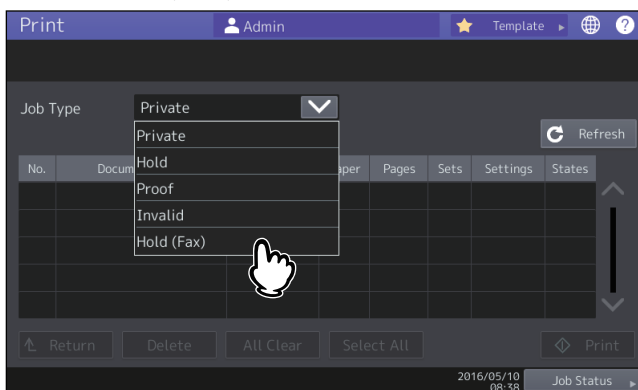
**Tip**

If a job is in the [Hold (Fax)] queue, the DATA IN MEMORY lamp blinks.



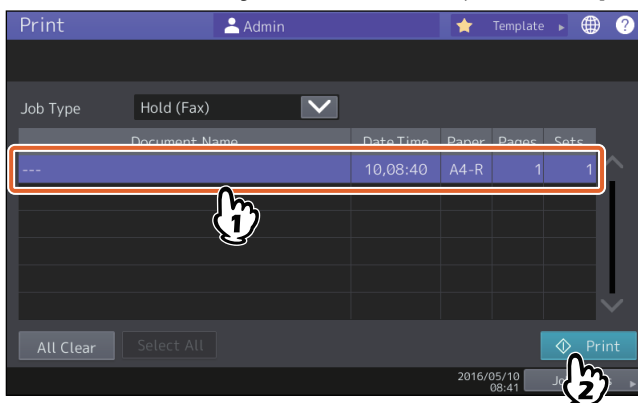
### Printing a job in the Hold (Fax) queue

- 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.





## THE INITIAL VALUES

<b>Precautions on the Initial Values.....</b>	<b>18</b>
Logging in .....	18
Initial value list .....	19

## Precautions on the Initial Values

---

To securely operate the equipment, the initial and selectable values in the equipment under the high security mode may differ from those under the normal security mode. This manual only explains about the initial values and setting items which are different from those under the normal security mode.

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

### Notes

- For the initial and setting values in the normal security mode, refer to the **TopAccess Guide** and **MFP Management Guide**.
- To reset all settings by performing “Initialization” of this equipment, back up the setting of this equipment and customers’ data before initializing. For details, refer to the **TopAccess Guide** and **MFP Management Guide**.

## ■ Logging in

- The [User Management] and [Administration] tabs in TopAccess are displayed by logging in as a user with the administrator privilege. Open TopAccess, click “Login” on the top right, and then enter the user name and password to log in.



- Be sure to log in the [Admin] tab in the [Setting] mode of the equipment as a user with the Administrator privilege.

## ■ Initial value list

### Home screen:

[Setting -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] Tab

[Setup] Menu

[General] Sub Menu

Item	Initial value for the high security mode	Remarks
Device Information		
USB Direct Print	Disable	
Functions		
Save as FTP	Disable	
Save to USB Media	Disable	
Save as SMB	Disable	
Save as Netware	Disable	
Network iFax	Disable	
Network Fax	Disable	
Web Services Scan	Disable	
Twain Scanning	Disable	
Restriction on Address Book Operation by administrator / AddressbookRemoteOperator		
Can be operated by Administrator / AddressbookRemoteOperator only		
Power Save		
Auto Clear *	45 Seconds	The initial value is the same as in the Normal Security Mode; however, OFF cannot be selected.

\* The value can be changed in the [ADMIN] tab in the [Setting -User-] mode in the touch panel of the equipment.

[Network] Sub Menu

Item	Initial value for the high security mode	Remarks
SMB		
SMB Server Protocol	Disable	
HTTP		
Enable SSL *	Enable	
WSD		
Enable SSL	Enable	
Web Services Print	Disable	
Web Services Scan	Disable	
SMTP Server		
Enable SMTP Server	Disable	
FTP Server		
Enable FTP Server	Disable	
Enable SSL	Enable	
SMTP Client		
Enable SSL	Verify with imported CA certification(s)	The secure setting is “Verify with imported CA certification(s)” or “Accept all certificates without CA”.
Authentication	AUTO	Be sure to confirm that one of “CRAM-MD5”, “Digest-MD5”, “Kerberos” or “NTLM (IWA)” is applied to your use environment.
POP3 Client		
Enable SSL	Verify with imported CA certification(s)	
FTP Client		
SSL 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		
Enable SSL	Verify with imported CA certification(s)	

\* The value can be changed in the [ADMIN] tab in the [Setting-User-] mode in the touch panel of the equipment.

## [Printer] Sub Menu

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

## [Print Service] Sub Menu

Item	Initial value for the high security mode	Remarks
Raw TCP Print		
Enable Raw TCP	Disable	
LPD Print		
Enable LPD	Disable	
IPP Print		
Enable SSL	Enable	
FTP Print		
Enable FTP Printing	Disable	

## [ODCA] Sub Menu

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

## [Security] Menu

## [Authentication] Sub Menu

Item	Initial value for the high security mode	Remarks
User Authentication Setting		
User Authentication	Enable	You cannot change the setting to "Disable".
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".

[Password Policy] Sub Menu

Item	Initial value for the high security mode	Remarks
Policy for Users		
Minimum Password Length	8 (digits)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	
Available Period	Disable	(Same as in the Normal Security Mode)
Expiration day(s)	90 (days)	
Policy for Administrator, Auditor		
Minimum Password Length	8 (digits)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	
Available Period	Disable	(Same as in the Normal Security Mode)
Expiration day(s)	90 (days)	
Policy for e-Filing Boxes, Template Groups, Templates, SecurePDF, SNMPv3, Cloning, Secure Receive		
Minimum Password Length	8 (digits)	
Requirements to Apply	Enable	
Lockout Setting	Enable	(Same as in the Normal Security Mode)
Number of Retry	3 (times)	
Lockout Time	2 (minutes)	



**Oki Data Corporation**  
4-11-22 Shibaura, Minato-ku, Tokyo  
108-8551, Japan

[www.oki.com/printing/](http://www.oki.com/printing/)

