



**KONICA MINOLTA**

# **IWS Scan to SFTP**

**User's Guide  
Version 1.0.0**

**KONICA MINOLTA, INC.**

## Index

<b>1. Overview .....</b>	<b>- 3 -</b>
<b>2. System Requirements .....</b>	<b>- 3 -</b>
2.1 Network environments .....	- 3 -
2.2 Device .....	- 3 -
<b>3. Application Install .....</b>	<b>- 5 -</b>
<b>4. Scan to SFTP Application Operating Procedures .....</b>	<b>- 6 -</b>
4.1. Starting the application.....	- 6 -
4.2. Creating a profile .....	- 7 -
4.2.1 Admin Settings screen (Profile Management).....	- 10 -
4.3. Creating a keypair.....	- 13 -
4.3.1. Admin Settings screen (Keypair Management).....	- 16 -
4.4. Scanning.....	- 18 -
4.4.1. Main screen (Password Authentication) .....	- 20 -
4.4.2. Main Screen (Public Key Authentication) .....	- 24 -
4.5. Checking Job History.....	- 25 -
4.5.1. Job History screen .....	- 26 -
4.6. Checking Application Information .....	- 28 -
4.6.1. Application Information screen.....	- 28 -
4.7. Application log management.....	- 29 -
4.7.1. Log Management screen .....	- 31 -
4.8. Language specification.....	- 32 -
<b>5. Application Uninstall.....</b>	<b>- 33 -</b>
<b>6. Troubleshoot.....</b>	<b>- 34 -</b>
6.1. Error Message Details .....	- 34 -
<b>7. Appendix .....</b>	<b>- 38 -</b>
7.1. Restrictions .....	- 38 -

## 1. Overview

This document describes the functional specifications of the IWS application (Scan to SFTP).

## 2. System Requirements

The system requirements for this application are as follows.

### 2.1 Network environments

A device (MFP) must be installed in a network environment that can be connected to the destination SSH server to which scan data is sent.

### 2.2 Device

The following settings should be configured on the device:

#### Network setting

- TCP/IP protocol (IPv4) settings are configured.
- The network is configured to allow connection to the destination SSH server to which scan data is sent.

#### IWS setting

- The IWS function is enabled. (Information on the setting procedures is omitted in this document. Refer to the IWS manual for details.)
- Connection to external networks is allowed.

\*Select the following panels to configure the settings.

[Administrator]->[Network]->IWS Setting]->[IWS Setting]->[Connect IWS Apps to Network]: ON

#### Function Permission setting

- Scan function is allowed due to function permission.

\*Select the following panels to configure the settings.

[Administrator]->[User Auth/Account Track]->[User Authentication Setting]->  
[User Registration]->[Edit]->[Function Permission]->  
[Scan]: Full Color/Black or Black Only

[Administrator]->[User Auth/Account Track]->[Account Track Setting]->  
[Account Track Registration]->[Edit]->[Function Permission]->  
[Scan]: Full Color/Black or Black Only

### **USB flash drive function setting**

- To use public key authentication, the public key should be exported to a USB flash drive.

Set [Save Document] to "ON" in the [USB flash drive function settings].

\*Select the following panels to configure the settings.

[Administrator]->[System Settings]->[User Box Setting]->[USB flash drive function settings]->[ Save Document] : ON

### **3. Application Install**

This application is installed using the IWS Install Tool.

Please refer to the IWS Install Tool manual for the installation procedure.

A Token Number (Token Number) may be required to install on a MFP.

Contact your MFP administrator for details.

Do not turn off the main power of the MFP while installing the application.

If you accidentally turn off the main power of the multifunction copier while installing an application, install the corresponding application again.

## 4. Scan to SFTP Application Operating Procedures

This section explains the operation procedure for Scan to SFTP and items displayed on each screen.

### 4.1. Starting the application

After Installing the application, tap the Scan to SFTP icon in the APP folder on the MFP panel to launch the application and display the Main screen as shown below.

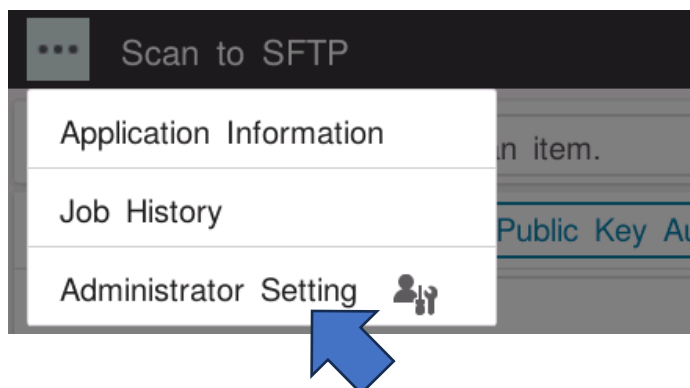
The screenshot displays the 'Scan to SFTP' application interface. At the top, a dark header bar contains a menu icon and the title 'Scan to SFTP'. Below this, the interface is divided into several sections. On the left, there is a 'Profiles' section showing '1 Profiles' and a dropdown menu 'Select an item.'. Below this are two tabs: 'Password Authentication' (selected) and 'Public Key Authentication'. Under the 'Password Authentication' tab, there are input fields for 'Host Name', 'Port No.', 'File Path', 'User Name', and 'Password'. To the right of these fields is a large, empty light purple rectangular area. On the far right, there is a settings panel with several options: 'Color' (Auto Color), 'Scan Size' (Auto Detect), 'Resolution' (300x300dpi), 'File Type' (Compact PDF), 'Duplex Settings' (1-Sided), and 'Document name'. At the bottom of the screen, there is a navigation bar with a home icon, a 'Reset' button, a 'Stop' button (with a red circle and slash icon), and a 'Start' button (with a blue diamond icon).

## 4.2. Creating a profile

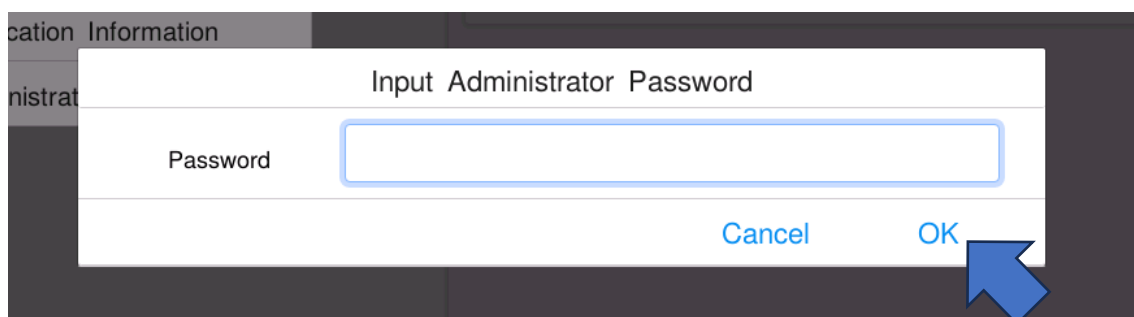
This application stores information about connection to the scan data destination SSH server and authentication in the application as profiles, reads a profile during scanning, connects to the SSH server according to the configured settings in the profile read and transfers the scan data to the SSH server.

Therefore, you need to create profiles and register them with the application in advance.

To create a profile, select " Administrator Setting" from the Main screen menu first.

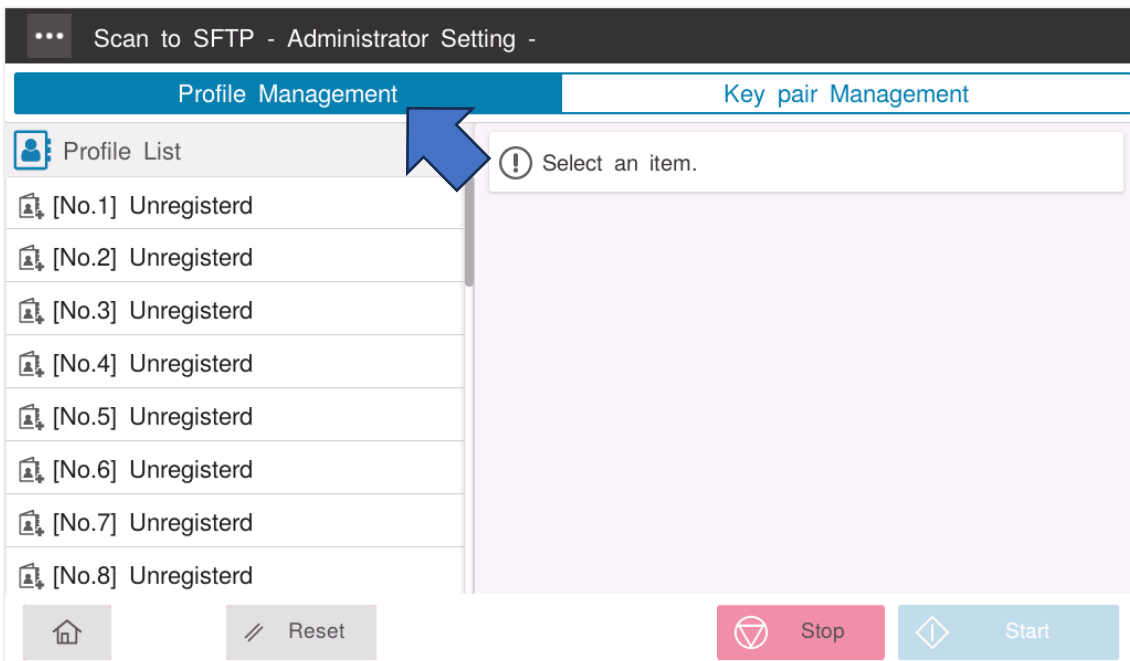


Enter MFP administrator password on textbox and press the OK button when "Input Administrator Password" dialog appears,



If wrong password will be entered, "Error occurred." dialog appears. Press the OK button to clear the dialog and select "Administrator Setting" again from the menu.

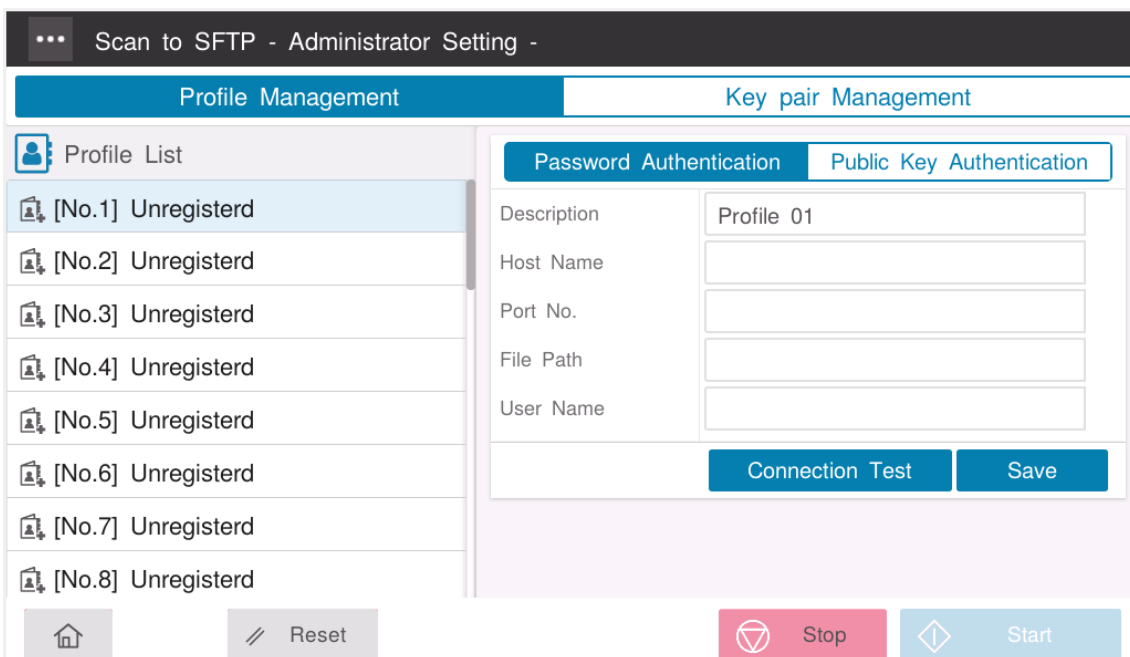
If the password entered is correct, the Administrator Setting screen appears.



Profile Management screen appears by selecting "Profile Management" from the menu at the top of the Administrator Setting screen.

- In the left pane of the Profile Management screen, "Profile List" displays a list of profiles registered in the List.

To create a new profile, select "Unregistered" from the Profile List.



This brings up the profile editing menu in the right pane of the screen.



Select either " Password Authentication" or " Public Key Authentication" for authentication of the SSH server.

"Password Authentication" and "Public Key Authentication" have different settings. See 4.2.1 for Admin Settings screen (Profile Management).

- In "Connection Test", check if connection to the SSH server can be established with the profile you registered.
- Tap the "Connection Test" button and a password entry dialog appears.
- Enter the password corresponding to the registered user or the passphrase corresponding to the selected keypair and tap the "OK" button to bring up a dialog that shows the connection test result.
- Enter the required items and tap the Save button to save them as a profile.

If there is a problem with the entry, an error dialog with details of the error will appear and the profile will not be saved. Review your entry and tap the Save button again to save.

Scan to SFTP - Administrator Setting -

Profile Management      Key pair Management

Profile List

- [No.1] test-profile  
test@10.9.0.9:22/test
- [No.2] Suzuki's Profile  
user02@1.2.3.4:22/myfile
- [No.3] Kimura's Profile  
kimura@example.jp:22/kimura
- [No.4] Unregisterd
- [No.5] Unregisterd
- [No.6] Unregisterd

Key pair Management

Password Authentication      Public Key Authentication

Description: Suzuki's Profile

Host Name: 1.2.3.4

Port No.: 22

File Path: myfile

User Name: user02

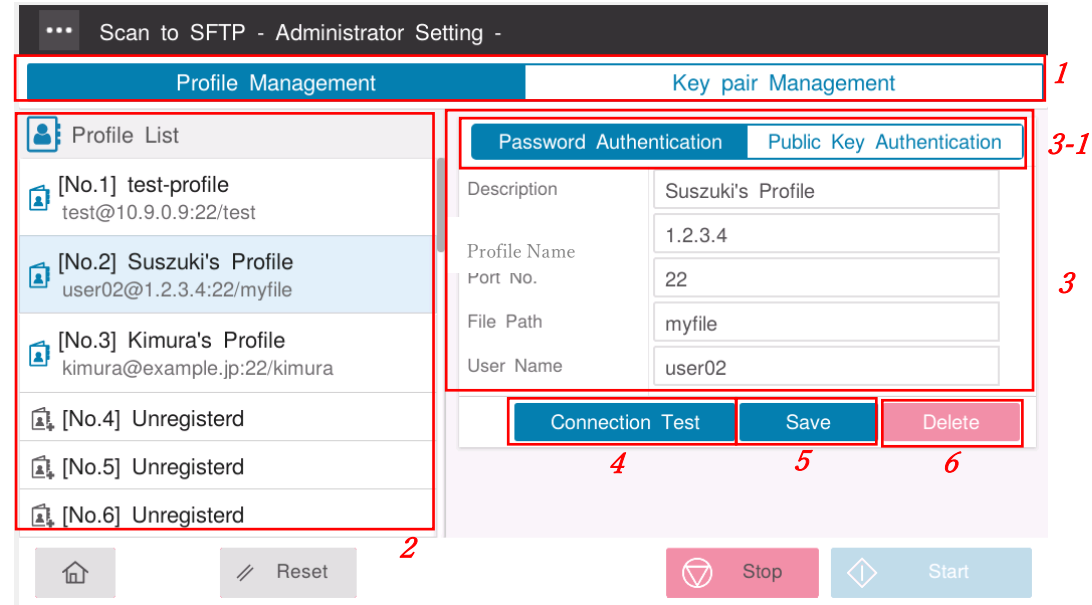
Connection Test      Save      Delete

Home      Reset      Stop      Start

For the profiles that have been registered, the settings for each profile are displayed in the right pane of the screen when you select a desired profile from the list. The profile settings can be changed. To overwrite the profile, change the settings and tap the Save button.

Tapping the Delete button enables you to delete the selected profile.

4.2.1 Admin Settings screen (Profile Management)



1 Button to select settings

Item	Default value	Purpose	Remarks
Button to select settings	Profile Management	This button is to change setting types. There are two setting type options to select. <ul style="list-style-type: none"><li>- Profile Management</li><li>- Keypair Management</li></ul>	When [Keypair Management] is selected, the screen display changes to the Keypair Settings page. See "4.3.1. Admin Settings screen (Keypair Management)" for details.

2 Profile List

The list of profiles created is displayed in descending order of creation date and time.  
The maximum number of profiles that can be registered is 30.  
Tapping a profile in this list displays the details of the profile specified in 3.

### 3 Profile information entry field

Item	Default value	Purpose	Remarks
Description	Profile X	Any profile name can be specified. X: Unique number	Single-byte/double-byte characters are allowed. Maximum of 64 characters. Empty string is allowed.
Host Name	Blank	Host Name of the SSH server	Single-byte alphanumeric characters + two types of single-byte symbols (- .) are allowed. Maximum of 253 characters.
Port No.	Blank	Port Number of the SSH server	1-65535
File Path	Blank	Destination where to save SSH server files	Single-byte/double-byte characters are allowed. Maximum of 256 characters.
User Name	Blank	User Name to connect to the SSH server	Single-byte/double-byte characters are allowed. Maximum of 64 characters.
Private key	Blank	Private key to use for Public Key Authentication	This item appears only when you select Public Key Authentication in 3-1. Select a private key from a keypair you created on the Admin Settings screen

			(Keypair Settings) in advance.
--	--	--	--------------------------------

#### 4 Test Connection button

Item	Behavior when clicked	Remarks
Connection test button	<p>Pressing this button displays a dialog for password entry. Enter the password corresponding to the specified user for password authentication and passphrase set for the keypair you selected for public authentication and press the OK button. This then performs SSH connection test based on the settings entered in 3 and displays either one of the following connection results in a dialog.</p> <ul style="list-style-type: none"> <li>- Connection was successful.</li> <li>- Failed to connect to server.</li> </ul>	

#### 5 Save button

Item	Behavior when clicked	Remarks
Save button	Saves the settings entered in 3.	

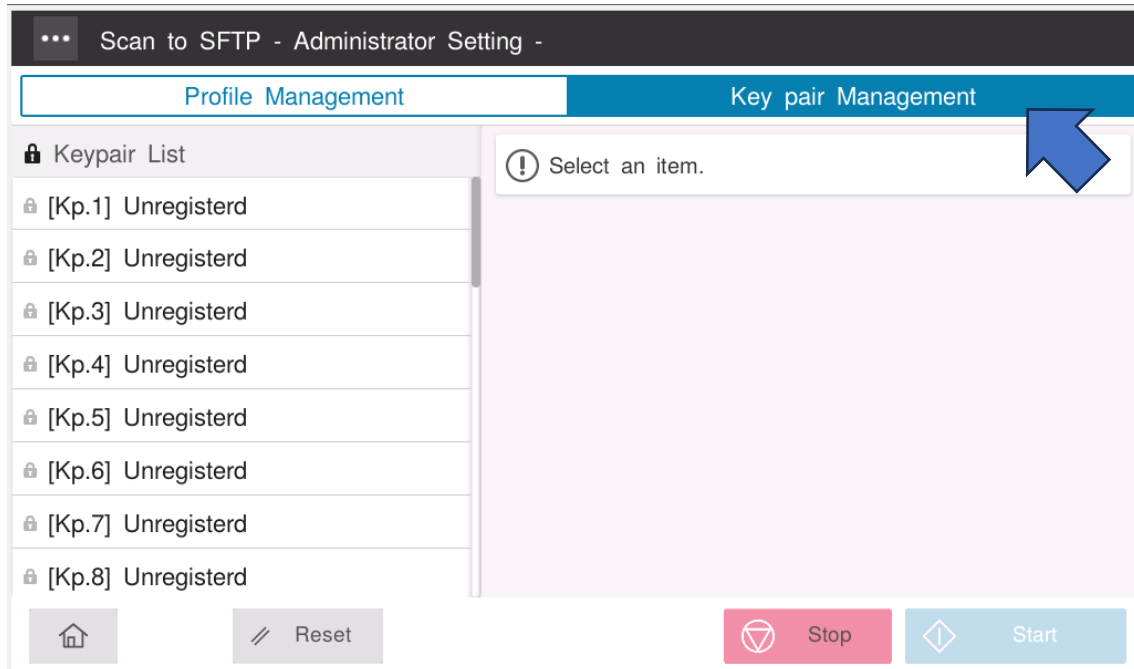
#### 6 Delete button

Item	Behavior when clicked	Remarks
Delete button	Deletes a specified profile.	Displayed only when a registered profile is selected.

### 4.3. Creating a keypair

If Public Key Authentication is selected as the method of authentication for the SSH server, it is necessary to create a keypair to be used for Public Key Authentication.

When "Key pair Management" is selected from the menu at the top of the Administrator Setting screen, the Key pair Management screen is displayed. The screen shows a list of registered keypairs in the left half and detailed settings for the selected keypair in the right half.



To create a new keypair, select "Unregistered" from the Keypair List.

Scan to SFTP - Administrator Setting -

Profile Management      Key pair Management

Keypair List

- [Kp.1] Unregisterd
- [Kp.2] Unregisterd
- [Kp.3] Unregisterd
- [Kp.4] Unregisterd
- [Kp.5] Unregisterd
- [Kp.6] Unregisterd
- [Kp.7] Unregisterd
- [Kp.8] Unregisterd

Description: Key pair 01

Passphrase:

Encryption Method: RSA-2048

Save

Home   Reset   Stop   Start

When the setting items are displayed in the right pane of the screen, enter the required items. See 4.3.1. Admin Settings screen (Keypair Settings) for each setting.

After entering the required items, tap the Save button to save the configured settings in the application. If there is a problem with the entry, an error dialog with details of the error will appear and the keypair will not be saved. Review your entries and tap the Save button again to save.

Scan to SFTP - Administrator Setting -

Profile Management      Key pair Management

Keypair List

- [Kp.1] example.com  
RSA-2048
- [Kp.2] key02  
RSA-2048
- [Kp.3] aaa-sever  
RSA-2048
- [Kp.4] Unregisterd
- [Kp.5] Unregisterd
- [Kp.6] Unregisterd

Description: example.com

Passphrase: .....

Encryption Method: RSA-2048

Save   Public Key Export   Delete

Home   Reset   Stop   Start

For the keypairs that have been registered, the settings for each keypair are displayed in the right pane of the screen when you select a desired keypair from the list.

The keypair settings can be changed. To overwrite the keypair, change the settings and tap the Save button.

- Tapping the Delete button enables you to delete the selected keypair.
- A public key can be exported to a USB flash drive using the created keypair.  
See “2. System Requirements” for prerequisites for using USB flash drive.

When you connect a USB flash drive to the MFP and tap “Public Key Export” button, a folder “ Keypair-XX\_YYYYMMDDhhmmss (XX: KeypairID、YYYYMMDDhhmmss: year, month, date, time, minute and second) ” is created in the USB flash drive, and in the folder, two public key folders in the PEM and OpenSSH formats shown below are created.

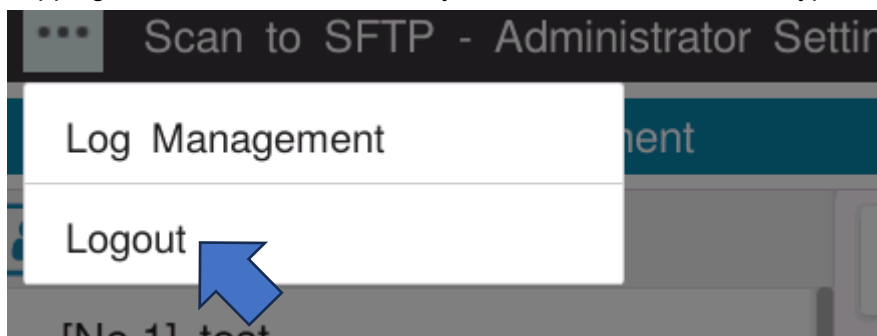
- PEM format : public-key(PEM)
- OpenSSH format : public-key(OpenSSH)

If keypair export fails, an error dialog with details of the error will appear. Check the error details and perform the keypair export again.

You can perform public key authentication from this application by registering either of the above public keys in the SSH server according to the specifications of the SSH server you are using.

For the profiles that have been registered, the settings for each profile are displayed in the right pane of the screen when you select a desired keypair from the list. The keypair settings can be changed. To overwrite the keypair, change the settings and tap the Save button.

Tapping the Delete button enables you to delete the selected keypair.



After creating the profile and keypair, tap “Logout” from the menu to return to the Main screen.

### 4.3.1. Admin Settings screen (Keypair Management)

The screenshot shows the 'Scan to SFTP - Administrator Setting' screen. It has two tabs: 'Profile Management' and 'Key pair Management'. The 'Key pair Management' tab is active. On the left, there is a 'Keypair List' with a lock icon. It contains a list of keypairs: [Kp.1] example.com RSA-2048, [Kp.2] key02 RSA-2048, [Kp.3] aaa-sever RSA-2048, [Kp.4] Unregisterd, [Kp.5] Unregisterd, and [Kp.6] Unregisterd. A red box labeled '1' highlights this list. On the right, there is a form for editing a keypair. It has fields for 'Description' (example.com), 'Passphrase' (masked with dots), and 'Encryption Method' (RSA-2048). A red box labeled '2' highlights this form. Below the form, there are three buttons: 'Save' (labeled '3'), 'Public Key Export' (labeled '4'), and 'Delete' (labeled '5'). At the bottom of the screen, there are buttons for 'Reset', 'Stop', and 'Start'.

#### 1 Keypair List

The list of keypairs created is displayed in descending order of creation date and time.

The maximum number of keypairs that can be registered is 30.

Tapping a keypair in this list displays the details of the keypair specified in 2.

#### 2 Keypair information entry field

Item	Default value	Description	Remarks
Description	KeypairX	Any keypair name can be specified. X: Unique number	Single-byte/double-byte characters are allowed. Maximum of 64 characters. Empty string is allowed.
Passphrase	Blank	A passphrase that must be entered during public key authentication to the SSH server.	Single-byte alphanumeric characters and symbols are allowed. Maximum of 32 characters.



Encryption Method	RSA-2048	Encryption method to create a keypair Select one of the following. - RSA-2048	
-------------------	----------	---	--

### 3 Save button

Item	Behavior when clicked	Remarks
Save button	Saves the settings entered in 2.	If there is a problem with the input content, pressing this button will display an error dialog.

### 4 Public Key Export button

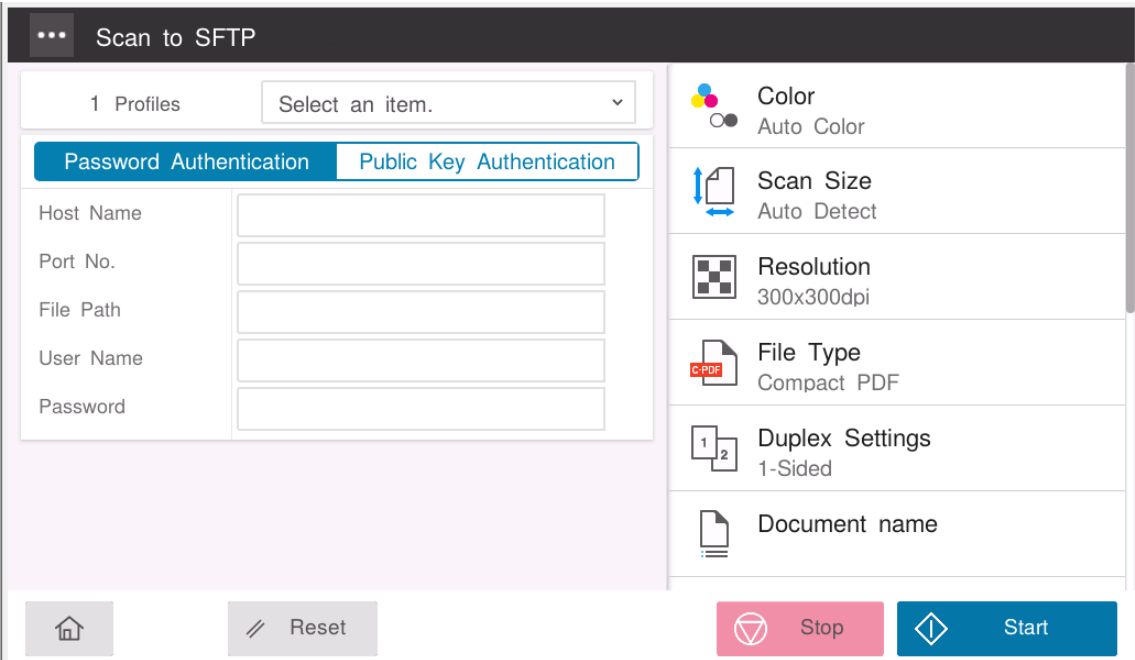
Item	Behavior when clicked	Remarks
Public Key Export button	Saves a public key of the specified keypair in the specific directory of a USB flash drive connected to the MFP. If export of the public key to the USB flash drive fails, one of the following message will appear in a dialog. "Public key export failed." "Please insert USB flash drive." "Access to the USB flash drive is restricted."	Displayed only when a registered keypair is selected. When using a USB flash drive, the MFP settings need to be changed. Refer to USB flash drive function setting in 2.System Requirements.

### 5 Delete button

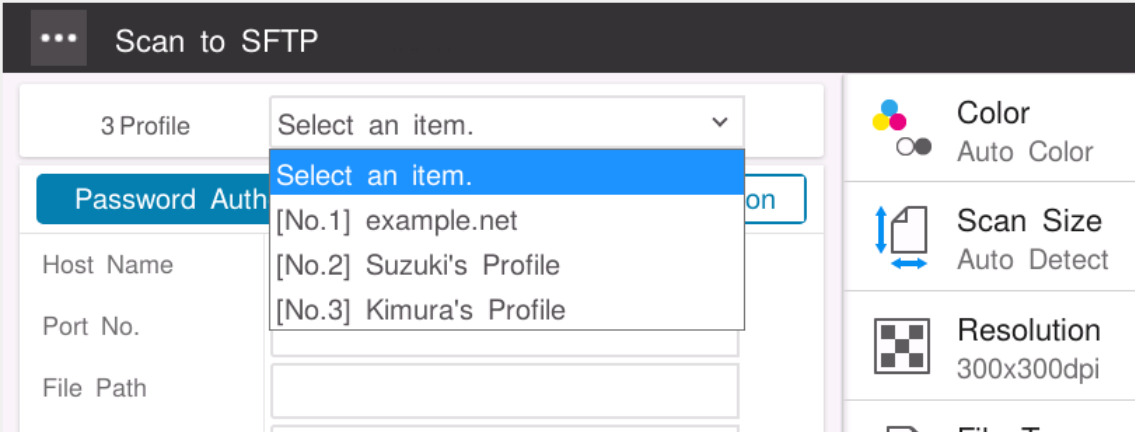
Item	Behavior when clicked	Remarks
Delete button	Deletes a specified keypair.	Displayed only when a registered keypair is selected.

4.4. Scanning

This section describes the steps from scanning to sending the scan data to the SSH server. The Main screen displays a pull-down menu and authentication settings in the left pane and scan settings in the right pane.



When “Profiles” is selected from the pull-down menu on the Main screen, a list of the registered profiles is displayed.



When you select a desired profile, the profile details specified in the authentication settings are displayed.

... Scan to SFTP

3 Profile [No.3] Kimura's Profile

Public Key Authentication

Host Name example.com

Port No. 22

File Path /kimura/scan

User Name kimura

Private key [Kp.1] example.com

Passphrase Select an item.

[Kp.1] example.com

[Kp.2] key02

[Kp.3] aaa-sever

Color Auto Color

Scan Size Auto Detect

Resolution 300x300dpi

File Type Compact PDF

Duplex Settings 1-Sided

File Name

Reset Stop Start

The authentication settings can be changed on the screen but be aware that your changes will not be saved to the profile.

See 4.4.1. Main screen (Password Auth) and 4.4.2. Main Screen (Public Key Auth) for details of the settings.

Each scan setting can be changed in the scan settings pane in the right of the screen.

There are setting items that cannot be combined. Items that are not allowed to be combined with the item you are currently setting are grayed out and cannot be selected to prevent forbidden combinations.

After configuring the scan settings, press the Start button at the lower right of the screen or the Start button of the MFP to perform scan according to the configured settings and transfer the scan data to the folder in the SSH server specified in the profile.

If there is a problem with the entry, an error dialog with details of the error will appear and scan will not be performed. Review your entry and press the start button again to perform scan.

#### 4.4.1. Main screen (Password Authentication)

##### 1 Profile selection field

Item	Default value	Purpose	Remarks
Profiles	Blank	This item is to select a profile you created in advance. The destination information saved in the selected profile is reflected in 3. For details on creating the profile, see “4.2.Creating a profile”.	

##### 2 Authentication method selection button

Item	Default value	Purpose	Remarks
Authentication method selection button	Password Authentication	This item is to select an authentication method to connect to the SSH server. Select the authentication method from the following two options. <ul style="list-style-type: none"> <li>- Password Authentication</li> <li>- Public Key Authentication</li> </ul>	When Public Key Authentication is selected, the contents displayed in 3 will be changed. For details, see “4.4.2. Main Screen (Public Key Authentication).”

### 3 Destination information entry field

Item	Default value	Purpose	Remarks
Host Name	Blank	Host Name or IP Address of the SSH server	Single-byte alphanumeric characters + two types of single-byte symbols (- .) are allowed. Maximum of 253 characters.
Port No.	Blank	Port Number of the SSH server	1-65535
File Path	Blank	Destination where to save SSH server files	Single-byte/double-byte characters are allowed. Maximum of 256 characters.
User Name	Blank	User Name to connect to the SSH server	Single-byte/double-byte characters are allowed. Maximum of 64 characters.
Password	Blank	Password to connect to the SSH server	Input characters are masked. Single-byte alphanumeric characters and symbols are allowed. Maximum of 64 characters.

#### 4 Scan setting entry field

The scan setting items are basically conform to the scan function of the Basic UI of each MFP. Details of the items therefore are omitted in this document. Items with different specifications are listed in the Remarks column.

Item	Default value	Remarks
Color	Auto Color	
Scan Size	Auto Detect	
Resolution	300 × 300dpi	
File Type	Compact PDF	
Duplex Setting	1-Sided	
File Name	Blank	
Mixed Original	OFF	
Thin Paper Orig.	OFF	
Z-Folded Orig.	OFF	
Blank Page Removal	OFF	
Original Direction	Vertical Direction	
Original Type	Text/Photo Photo Printed	
Density	Standard	
Bkgd.Removal	Bleed Removal/Standard	

## 5 Start button

Item	Behavior when clicked	Remarks
Start button	Performs a scan according to the configured scan settings and sends data to the configured destination via SFTP.  If the scan is paused, the scan job is resumed.	
Stop button	If pressed Stop button while a scan is in progress, the scan job in progress will be interrupted.	

Manual changes to destination settings on this screen will not be saved in the profile.

#### 4.4.2. Main Screen (Public Key Authentication)

Selecting [Public Key Authentication] on the Main screen will display the following screen.

For items common with the [Password Auth] screen, refer to "3.4.1. Main screen (Password Auth)".

Scan to SFTP

3 Profile [No.3] Kimura's Profile

Password Authentication Public Key Authentication

Host Name example.com

Port No. 22

File Path /kimura/scan

User Name kimura

Private key [Kp.1] example.com

Passphrase Select an item.

[Kp.1] example.com

[Kp.2] key02

[Kp.3] aaa-sever

Color Auto Color

Scan Size Auto Detect

Resolution 300x300dpi

File Type Compact PDF

Duplex Settings 1-Sided

File Name

Reset Stop Start

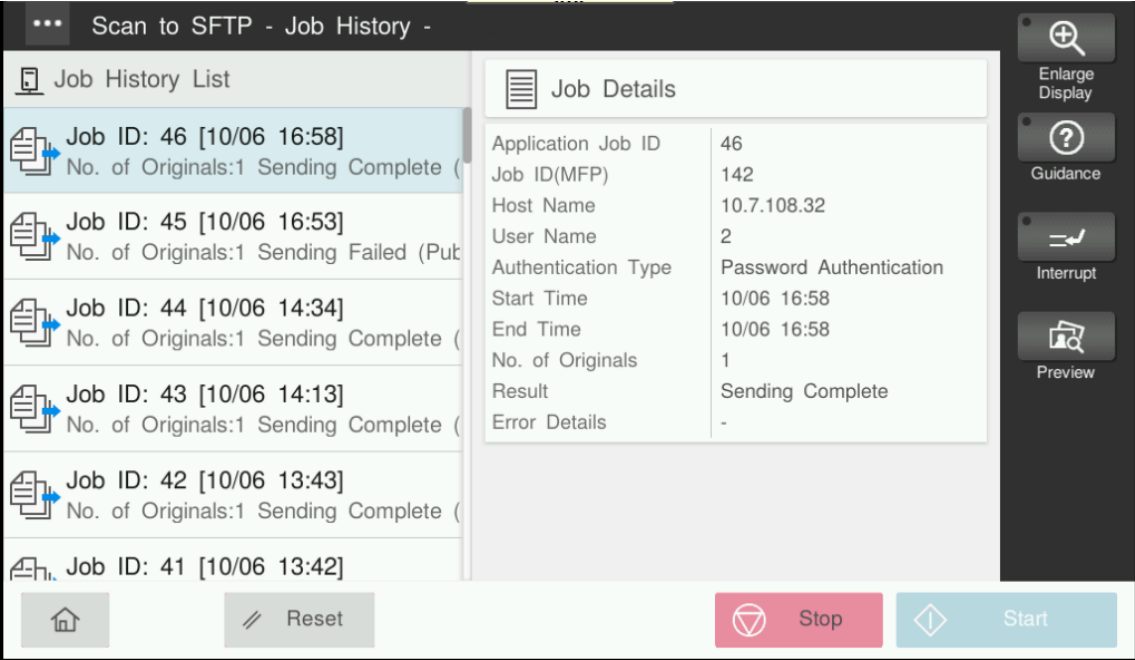
#### 1 Secret Key selection field

Item	Default value	Purpose	Remarks
Private Key	Blank	This item is to select a private key file from a keypair you created in advance. For details on creating the keypair, see "4.3.Creating a keypair".	
Passphrase	Blank	This item is to enter a passphrase that was set for a specified keypair.	Input characters are masked. Single-byte alphanumeric characters and symbols are allowed. Maximum of 32 characters.



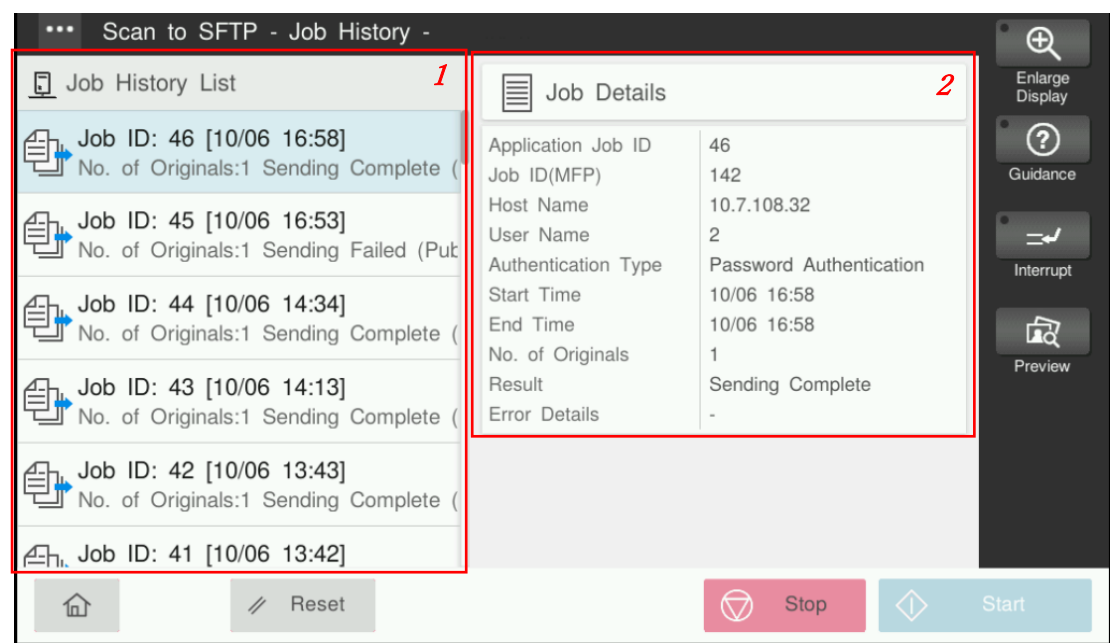
4.5. Checking Job History

If you select "Job History" from the Main screen menu, the Job History screen appears and displays a list of results of scan jobs executed by this application.



The Job History screen displays a list of jobs in the left pane and details of the job selected from the list in the right pane. See 4.5.1. Job History screen for details of each item.

4.5.1. Job History screen



1 Job History

A list of scan jobs executed in this application is displayed in descending order of job execution date and time.

The maximum number of jobs that can be stored in the Job History is 100.

When more than the maximum storage capacity of jobs is registered, they are deleted in order from the oldest execution date and time.

When a job in the List is tapped, the details of the specified job appears in the right pane of the screen (2).

## 2 Job details pane

The pane displays the details of the job specified in 1

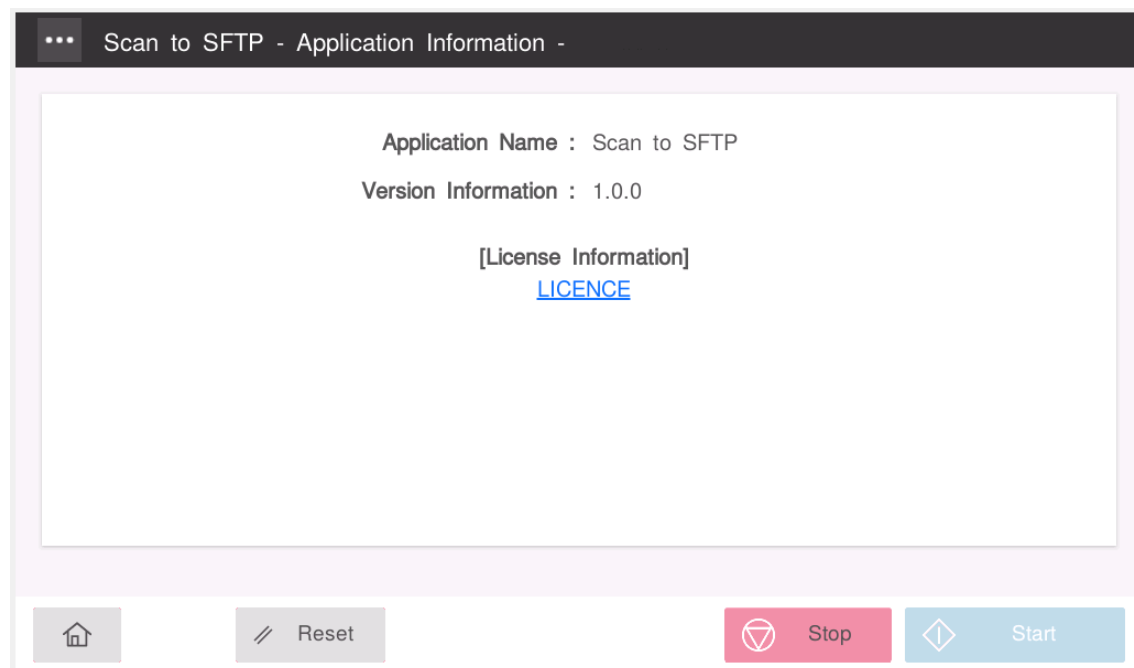
Item	Purpose	Remarks
Application Job ID	Job ID controlled by this application	
Job ID(MFP)	Job ID controlled by the MFP linked to the above Job ID	A job with the job ID (MFP) is saved as a WebDav Scan job in the Job History on the MFP side.
Host Name	Host name of the destination SSH server	
User Name	Authentication information of the destination SSH server	
Authentication Type	Authentication method for the destination SSH server	"Password Authentication" or "Public Key Authentication"
Start Time	Starting time of job execution in this application	
End Time	Ending time of job execution in this application	
No. of Originals	Number of sheets scanned	
Result	Execution result of a scan job in this application. Either of the following results is displayed. - Sending Complete - Sending Failed	
Error Details	This item displays error details when the result is "Sending Failed". Error details include: - Network Connection Error - Authentication Error - Scan Error (Refer to MFP Job List) - TX Error - Other errors - Cancel	

## 4.6. Checking Application Information

If you select "Application Information" from the Main screen menu, the Application Information screen appears.

On the screen, you can view information about version of this application and the license used for the application. See 4.6.1. Application Information screen for details of each item.

### 4.6.1. Application Information screen

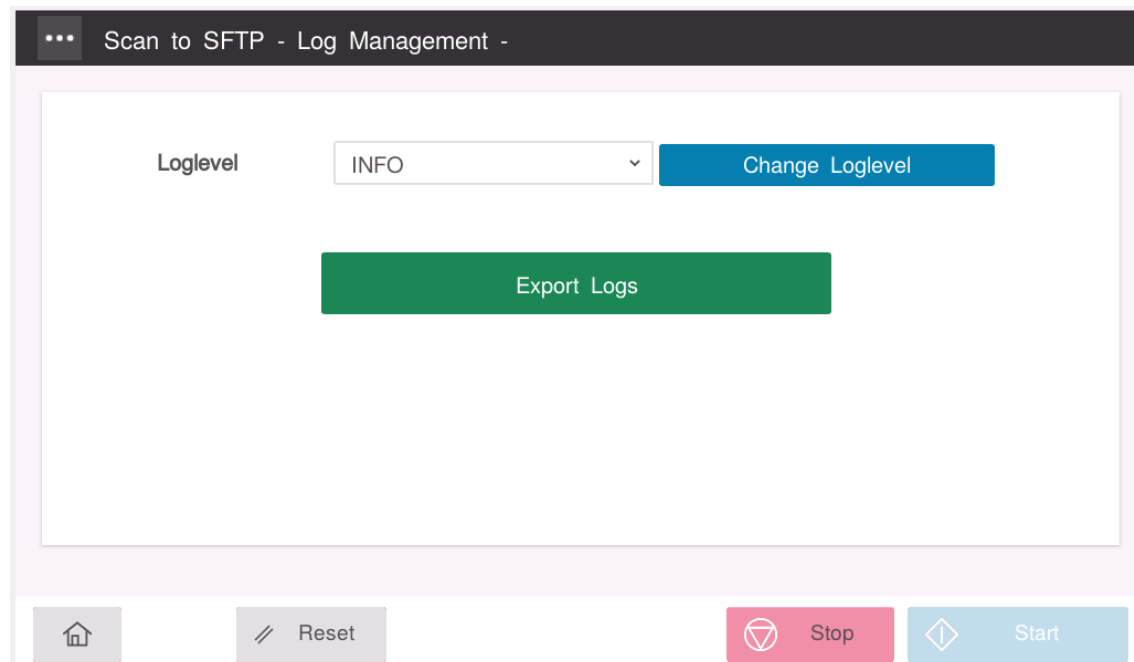


Item	Description	Remarks
Application Name	Name of this application	
Version Information	Version name of this application installed	
License Information	Name of the license used for this application	When the license name is tapped, the license text appears.

## 4.7. Application log management

If you select "Log Management" from the menu in the Administrator Setting screen, the Log management screen appears.

On the screen, you can configure settings for operation logs to be stored in this application. See 4.7.1. Log Management screen for details of the settings.



Operation logs can be exported to a USB flash drive from this screen.

Operation logs of this application are stored in the application according to the following specifications.

[Log file name]

yyyy-MM-dd\_nn.log

yyyy-MM-dd : Year-month-day of new log file creation

nn : Rotation sequence (00~99)

When a log file exceeds its maximum size (262,144 bytes), a new file is created separately, and new logs are written to the new destination file. The old logs are compressed and saved under the file name yyyy-MM-dd \_ nn.log.gz.

The maximum number of log files to keep is 14. When the maximum number is exceeded, the oldest log file will be deleted.

Connect a USB flash drive to the MFP and tap the "Export Logs" button to create a folder, "Log\_YYYYMMDDhhmmss (YYYYMMDDhhmmss: year, month, day, time, minute, second)". The folder stores up to 14 files including the latest log file and compressed old log files as described above.

If log export fails, an error dialog showing details of the error will appear. Check the error details and perform the log export again.

#### 4.7.1. Log Management screen

...

Scan to SFTP - Log Management -

Loglevel

INFO

Change Loglevel

Export Logs

Reset

Stop

Start

Item	Purpose	Remarks
Loglevel	<p>This item is to change log levels. Selecting a log level from the pull-down list and tapping the "Change Loglevel" button changes the level to the one you have specified. The configurable log levels are:</p> <ul style="list-style-type: none"> <li>- OFF</li> <li>- FATAL</li> <li>- ERROR</li> <li>- WARN</li> <li>- INFO</li> <li>- DEBUG</li> <li>- TRACE</li> <li>- ALL</li> </ul>	<p>TRACE is the lowest log level and FATAL is the highest.</p> <p>All logs below the specified log level will be saved.</p> <p>If OFF is specified, no log is kept.</p> <p>If ALL is specified, logs of all levels are saved.</p>
Export Logs	<p>This item is to save log files stored in the application to a specific directory of a USB flash drive.</p> <p>When exporting to the USB flash drive fails, one of the following message appears in a dialog.</p> <p>" Logs export failed."</p>	<p>When using a USB flash drive, the MFP settings need to be changed.</p> <p>Refer to USB flash drive function setting in</p>

	“Please insert USB flash drive.” “Access to the USB flash drive is restricted.”	2. System Requirements.
--	---	----------------------------

#### 4.8. Language specification

Display languages in the application change according to the MFP language setting.

When the language setting on the MFP is set to anything other than English, Korean, or Japanese, the display language in the application will be set to English.



## **5. Application Uninstall**

This application is uninstalled using the IWS Install Tool.

Please refer to the IWS Install Tool manual for the uninstallation procedure.

When the application is uninstalled, all information set by the application will be deleted.

When uninstalling an application, please do so while the application is not displayed on the operation panel.

(e.g., press the "menu key" on the main unit to display the top menu)

If uninstallation is performed while the application is displayed, the MFP may not operate properly. If this happens, turn the power back on and try uninstalling the application again.

In this case, turn the power back on and try uninstalling the application again.

Do not turn off the main power of the MFP while uninstalling an application. If you accidentally turn off the main power of the MFP while uninstalling an application, uninstall the corresponding application again.

## 6. Troubleshoot

### 6.1. Error Message Details

Error messages displayed on each screen and their causes/measures are described.

Screen Title	operation	Error message	cause	countermeasures
Main screen	Scan	Scan (SFTP transmission) Failed.	Failed to connect to SSH server.	Check that the profile settings are correct. and the password or passphrase is correct.
	Value input	Error occurred Enter Host Name.	Validity check error for screen input values.	Enter Host Name.
		Error occurred The Host name contains invalid characters.		See 4.4.1. Main screen (Password Authentication) and do not include invalid characters in the input value.
		Error occurred Specify the Port No between 1 and 65535.		Enter a value between 1 and 65535 in the port number.
		Error occurred Enter File Path.		Do not leave the File Path blank.
		Error occurred The File Path contains invalid characters.		See 4.4.1. Main screen (Password Authentication) and do not include invalid characters in the input value.
		Error occurred Enter User Name.		Do not leave the User Name blank.
		Error occurred		See 4.4.1. Main screen (Password Authentication)

		The User Name contains invalid characters.		and do not include invalid characters in the input value.
		Error occurred The Password contains invalid characters.		See 4.4.1. Main screen (Password Authentication) and do not include invalid characters in the input value.
		Error occurred The Passphrase contains invalid characters.		See 4.4.2. Main screen (Public Key Authentication) and do not include invalid characters in the input value.
Admin Settings screen	login	The Administrator Password is incorrect.	The Administrator Password is incorrect.	Please login again with the correct administrator password.
Admin Settings screen (Profile Settings)	Profile Management	Error occurred The Description contains invalid characters.	Validity check error for screen input values. Validity check error for screen input values.	See 4.2.1. Admin Settings screen (Profile Management) and do not include invalid characters in the input value.
		Error occurred Enter Host Name.		Enter Host Name.
		Error occurred The Host name contains invalid characters.		See 4.2.1. Admin Settings screen (Profile Management) and do not include invalid characters in the input value.

		Error occurred Specify the Port No between 1 and 65535.		Enter a value between 1 and 65535 in the port number.
		Error occurred Enter File Path.		Do not leave the File Path blank.
		Error occurred The File Path contains invalid characters.		See 4.2.1. Admin Settings screen (Profile Management) and do not include invalid characters in the input value.
		Error occurred Enter User Name.		Do not leave the User Name blank.
		Error occurred The User Name contains invalid characters.		See 4.2.1. Admin Settings screen (Profile Management) and do not include invalid characters in the input value.
	Keypair Management	Error occurred The Passphrase contains invalid characters.		See 4.3.1. Admin Settings screen (Keypair Management) and do not include invalid characters in the input value.
Admin Settings screen (Profile Settings)	Test Connection	Failed to connect to server.	Failed to connect to SSH server.	Check that the profile settings are correct. and the password or passphrase is correct.

Admin Settings screen (Keypair Settings)	Public key Export	Public key export failed.	Failure to write to USB flash drive.	Make sure the USB flash drive is properly connected to the MFP and run the export again.
		Please insert USB flash drive	USB flash drive is not connected.	Insert USB flash drive to MFP correctly and execute Public key export again.
		Access to the USB flash drive is restricted.	USB flash drive is write-protected.	Check the write permission setting of the USB flash drive.
Log Management screen	Log Export	Log export failed.	Failure to write to USB flash drive.	Make sure the USB flash drive is properly connected to the MFP and run the export again.
		Please insert USB flash drive	USB flash drive is not connected.	Insert USB flash drive to MFP correctly and execute Public key export again.
		Access to the USB flash drive is restricted.	USB flash drive is write-protected.	Check the write permission setting of the USB flash drive.

## 7. Appendix

### 7.1. Restrictions

- The below file types are not supported on Scan to SFTP application.
  - XPS
  - Compact XPS
  - DOCX
  - XLSX
- The following function is not supported.
  - PDF/A
  - PDF Document Properties
- The setting items displayed in the Scan setting entry field (refer to “4.4 Scanning”) may not conform to individual functions of each MFP model.  
(If a scan is performed with settings that cannot be used for the MFP model in question, the scan processing is handled as an error in the application.)
- Not support IPv6 transmission.
- After setting the Page Separation setting to "ON" in the File Type detail settings, the page separation setting will be changed to "OFF" if File Type detail settings is selected again.

#### [Reproduce Procedure]

The issue happens if user will do the following procedure.

1. Go to "Scan Setting -> File Type -> Detail setting -> Page Separation" and set as "ON".
2. Go back to Scan to SFTP Top screen.
3. Go to "Scan Setting -> File Type -> Detail setting -> Page Separation" again.
4. The setting will be changed to "OFF".

#### [Workaround]

Please set the setting as "ON" again.

The issue will happen once user will access "Scan Setting -> File Type -> Detail setting -> Page Separation" again.