

TOSHIBA

**MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS**

TopAccess

e-STUDIO2020AC/2520AC

e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC

e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A

e-STUDIO6526AC/6527AC/7527AC

e-STUDIO6529A/7529A/9029A

Preface




Thank you for purchasing our product. This manual describes remote setup and remote management which operated from the web based management utility TopAccess. Read this manual before using the functions.

Operations on some items are restricted depending on the privileges assigned to the TopAccess user. Also, some items may not be displayed or may not function on some models.

■ 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, could 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.
	References describing items related to what you are currently doing. See these references as required.

□ Target audience for this manual

This is a manual that is aimed at general users and administrators.

□ Model and series names in this manual

In this manual, each model name is replaced with a series name as shown below.

Model name	Series name
e-STUDIO2020AC/2520AC	e-STUDIO6525AC Series
e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC	
e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A	e-STUDIO6528A Series
e-STUDIO6526AC/6527AC/7527AC	e-STUDIO7527AC Series
e-STUDIO6529A/7529A/9029A	e-STUDIO9029A Series

□ Optional equipment

For available options, see the reference below:

Information About Equipment - Information About Equipment - Options

□ Screens in this manual

In this manual, Windows 10 is taken for explanation purposes to describe the screens and operation procedures in Windows.

The details on the screens may differ depending on your model and how the equipment is used, such as the status of the installed options, the OS version and the applications.

❑ Abbreviations in this manual

In this manual, “Dual Scan Document Feeder” (DSDF) and “Reversing Automatic Document Feeder” (RADF) are collectively referred to as “Automatic Document Feeder” (ADF).

❑ About the defaults shown in this manual

- The defaults shown in this manual are the values in the standard operating environment. The values may have been changed from these defaults. The defaults for your model may differ from the defaults shown.
- The default for the list item is shown underlined.

❑ Trademarks

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

❑ Security Precautions

- To prevent the configuration settings from being changed illegally or similar, change the initial administrator password at the time of shipping before you use this product.
- Be sure to log out when leaving your computer while changing TopAccess settings for security purposes.
- For security purposes, do not access any other site while you are logged in to TopAccess.

CONTENTS

Preface.....	3
How to read this manual	3

Chapter 1 Overview

TopAccess Overview	10
TopAccess Conditions	11
Accessing TopAccess.....	12
Accessing TopAccess by entering URL.....	12
TopAccess Screen Descriptions.....	13
Access Policy Mode	14

Chapter 2 [Device]

[Device] Item List	18
Displayed Icons	20

Chapter 3 [Job Status]

[Job Status] Overview	24
[Print Job] Item list	24
[Fax/InternetFax Job] Item list.....	26
[Scan Job] Item list	27
[Multi Station] Item list	28

Chapter 4 [Logs]

[Logs] Overview	30
[View Logs] Item list	30
[Export Logs] Item list <access policy mode>.....	38
[Log Settings] Item list <access policy mode>.....	40

Chapter 5 [Registration]

[Registration] Overview.....	42
Public Home	42
Public Theme Settings.....	42
Public Home Settings	42
[Address Book] Item list.....	42
[Inbound FAX routing] Item list	53

Chapter 6 [Counter]

[Counter] Overview	60
[Counter] Item list.....	60

Chapter 7 [User Management]

[User Management] Overview	74
[User Accounts] Item list <access policy mode>	74
[Group Management] Item list <access policy mode>	82

[Role Management] Item list <access policy mode>	84
[Department Management] Item list <access policy mode>	90
[Project Management] Item list <access policy mode>	94
[Export/Import] Item list <access policy mode>	95
[Shared Settings] Item list <access policy mode>	97

Chapter 8 [Administration]

[Setup] Item List	101
General settings	101
Network settings	117
Copier settings	169
Fax settings	173
Save as file settings	182
Email settings	192
InternetFax settings	199
Printer/e-Filing settings	204
Printer settings	205
Print Service settings	212
ICC Profile settings	220
Print Data Converter settings	222
MFP Collaboration	223
Embedded Web Browser settings	233
Off Device Customization Architecture settings	236
Version	237
[Security] Item List	238
Authentication settings	238
Certificate Management settings	257
Password Policy settings	262
Security Stamp setting	265
Configuration settings	266
[Maintenance] Item List	267
Upload Software settings	267
Remove Software settings	269
Create Clone File settings	270
Install Clone File settings	272
Import settings	275
Export settings	277
Panel View	279
Idle Screen	280
Delete Files settings	286
Notification settings	287
Languages settings	290
Remote Command	293
Data Backup	295
User Paper Type	297
System Updates settings	298
Reboot settings	299
[Registration] ([Administration]) Item List	300
Public Home	300
Template settings	306
Public Theme Settings	334
Public Home Settings	335
Default Home	336
Default Home Settings	336
Simple Screen Settings	337
Image/Icon Management	338
Home Data List	340

Fax Received Forward and InternetFAX Received Forward settings	340
Meta Scan	355
XML Format File.....	359
[Application] Item List	360
Application List	360
Application Settings.....	363
User Extended Information	366
Resource Management.....	367
[License] Item List	368
License List.....	368
Activate.....	368

Chapter 9 [My Account]

[My Account] Overview	370
[My Account] Item list	370

Chapter 10 Functional Setups

Setting up Meta Scan Function	378
Procedure for using Meta Scan	378
Checking Meta Scan Enabler	379
Editing XML format file	379
Registering XML format file	383
Registering Extended Field Definition	383
Registering templates for Meta Scan	386
Meta Scan	389
Checking logs of Meta Scan	389
Setting Multi Station Print	390
Procedure for Multi Station Print	390
Procedure for Multi Station Print (Only in One Equipment Unit)	391
Checking the Multi Station Print Enabler	391
Setting Home Data Synchronization	392
Procedure for Home Data Synchronization	392
Using the Attribute of the External Authentication as a Role of the MFP	393
Exporting the role information setting file	393
Defining the role information setting file	393
Importing the role information setting file.....	394
Enabling the role base access setting.....	394
Setting up Email.....	395
Procedure for Email Setting	395
Installing Certificates	396
Installing a device certificate	396
Creating/Exporting a client certificate.....	403
Installing CA certificate.....	405
INDEX	407

Overview

TopAccess Overview	10
TopAccess Conditions	11
Accessing TopAccess.....	12
Accessing TopAccess by entering URL.....	12
TopAccess Screen Descriptions.....	13
Access Policy Mode	14


TopAccess Overview

TopAccess is a management utility that allows you to check device information of this equipment and job status, and to carry out device setting and maintenance through a web browser. TopAccess has an “end-user mode” and a “access policy mode”.

End-user mode


End users can:

- Display general device information, including status, drawer/accessory configuration, and paper supply information.
- Display and manage the status of print jobs, fax/Internet Fax transmission jobs, and scan jobs submitted by the user. (The Fax Unit is required to display and manage the fax transmission jobs)
- Display the job logs for print, fax/Internet Fax transmission, fax/Internet Fax reception, and scan. (The Fax Unit is required to display the fax transmission and fax reception job logs.)
- Register and modify templates.
- Add or modify contacts and groups in the address book.
- Register and modify mailboxes. (The Fax Unit is required.)
- Display counter logs.
- Download client software.

 P.12 “Accessing TopAccess”

Access policy mode

Operation privileges and displayed items vary depending on the user account you used to log in to TopAccess. Details of operations and displays vary depending on the management on roles and departments to where the user account is assigned.

 P.14 “Access Policy Mode”

Your equipment should be connected to the network and TCP/IP is correctly configured to operate TopAccess. When TCP/IP is correctly configured, you can access TopAccess via a web browser.

Supported browsers

- Windows
 - Microsoft Edge 89 or later
 - Firefox 86 or later
 - Chrome 89 or later
- macOS
 - Safari 14.0 or later
- UNIX
 - Firefox 86 or later

Note

- Because TopAccess uses cookies to store information on the user's system, these must be enabled in the browser.
- If TopAccess does not display the correct information in any page, delete the cookies and try again.
- If a proxy server is used, set the IP address of the equipment in use in "Exceptions" of the proxy server.
- Make sure you disable your web browser's pop-up blocker or allow pop-ups from TopAccess.

Tip

- TopAccess supports special letters of European languages. A note is described in each article if there are any restrictions in which letters can be entered.
- This equipment uses TLS 1.2 and TLS 1.3 as communication protocols.

Accessing TopAccess

You can access TopAccess by entering its URL in the address box of the web browser.

■ Accessing TopAccess by entering URL

1 Launch a web browser and enter the following URL in the address box.

http://<IP Address> or http://<Device Name>

 http://10.10.70.120/

For example

When the IP address of your equipment “10.10.70.120” (when IPv4 used):

http://10.10.70.120

When the IP address of your equipment is “3ffe:1:1:10:280:91ff:fe4c:4f54” (when IPv6 used):

3ffe-1-1-10-280-91ff-fe4c-4f54.ipv6-literal.net

or

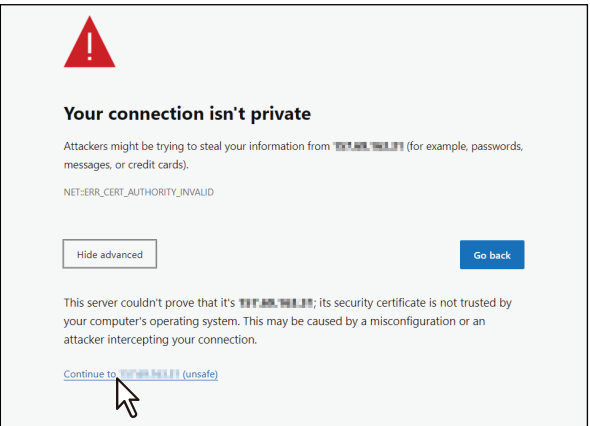
http://[3ffe:1:1:10:280:91ff:fe4c:4f54]

When your device name is “mfp-04998820”:

http://mfp-04998820

Note

When SSL/TLS for the HTTP network service is enabled, an alert message may appear when you enter the URL in the address box. In that case, click [Advanced], and then click [Continue to ~ (unsafe)] to proceed.



2 The TopAccess website appears.

The screen shows information, depending on the model and options you use.

Device


Job Status

Logs

Registration

Counter

Device



Options

Finisher	Saddle Stitch Finisher
Hole Punch Unit	2 Holes
Fax	Installed

Toner

Yellow(Y)	Good
Magenta(M)	Good
Cyan(C)	Good
Black(K)	Good

Device Information

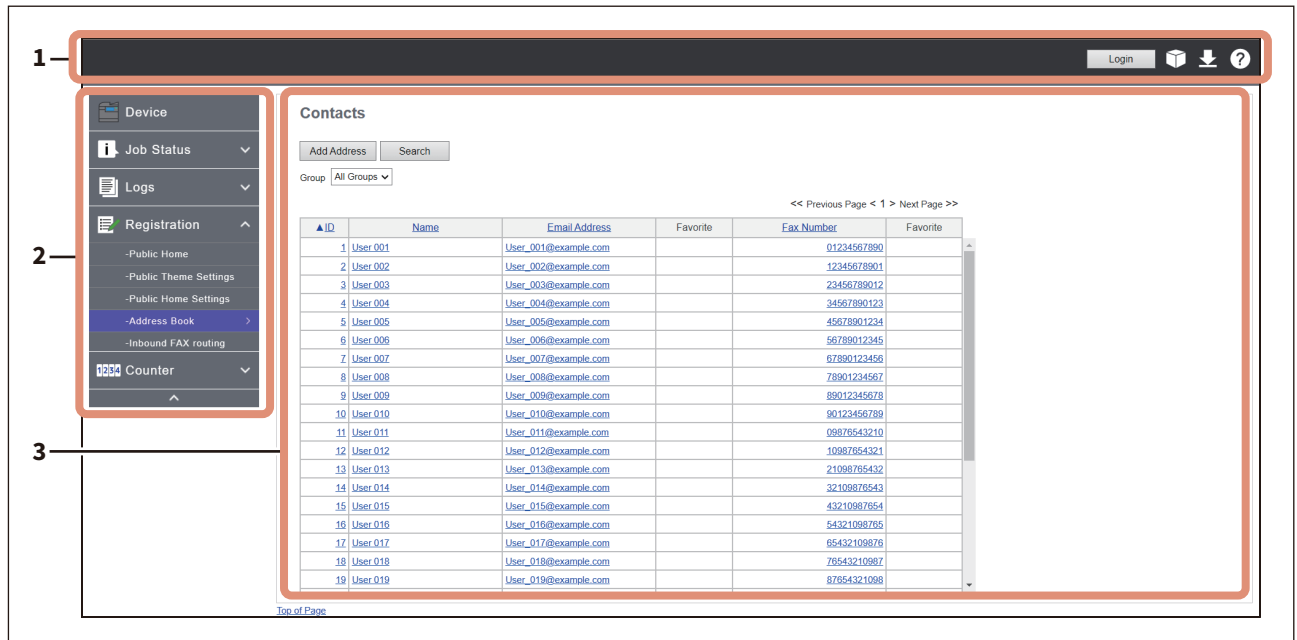
Status	Ready
Name	AFICIO
Location	
Copier Model	7000A-e-STD/DCSAC
Serial Number	0000000000000000
MAC Address	9C:40:00:00:00:00
Main Memory Size	6144 MB
Page Memory Size	940 MB
Save as File & e-Filing Space Available	29097 MB
Fax Space Available	930 MB
Contact Information	
Phone Number	
Message	
Alerts	*




Paper

Drawer	Size	Thickness	Attribute	Capacity	Level
Drawer 1	A4	Plain	None	600	<div></div>
Drawer 2	A3	Plain	None	600	<div></div>
Drawer 3	A4	Plain	None	600	<div></div>
Drawer 4	A4	Plain	None	600	<div></div>
External Large Capacity Feeder	A4	Plain	None	2300	<div></div>

Tip

You can also access TopAccess using the TopAccessDocMon link. For instructions on accessing TopAccess from TopAccessDocMon, refer to the **Help for TopAccessDocMon**.



	Item name	Description
1	Header area	<p>This area includes the operation buttons and icons.</p> <ul style="list-style-type: none"> • [Login] button — When you click this button, you can log in to TopAccess via the user authentication: after log-in, the button changes to [Logout] for you to log out. After you log in, the log-in username appears. When you are in the log-out status or the user authentication is disabled, the username does not appear. •  — Click this [e-Filing] icon to start up e-Filing. •  — Click this [Install Client Software] icon to open the page where you can download the installer file for the client software from TopAccess. •  — Click this [Help] icon to show help.
2	Menu area	<p>This area shows the layered menu of categorized functions. An arrowhead indicates the lower menu items. When you click an arrowhead, the lower menu opens or closes. When you click an item on the first layered menu, the second layered menu appears under the selected item. When you click or move your mouse pointer over an item on the second layered menu, the third layered menu pops up. The fourth menu, if any, appears in the setting display area, so that you can click an item to move to the setting concerned.</p>
3	Setting display area	<p>This area shows the functions and information according to the selection in the menu area. Click [Top of Page] to move back to the top of this area.</p>

Note

When the sub or pop-up window appears, do not click [X] of the browser to close it. Be sure to click the operation button of TopAccess.

Access Policy Mode

The access policy mode enables different operation privileges and displayed items to be applied depending on the user account you used to log in to TopAccess.

In the access policy mode, the details of operations and displays differ depending on the roles and department assigned to the given user account.

1 Access TopAccess.

 P.12 “Accessing TopAccess by entering URL”

2 Click [Login].




The Login page is displayed.

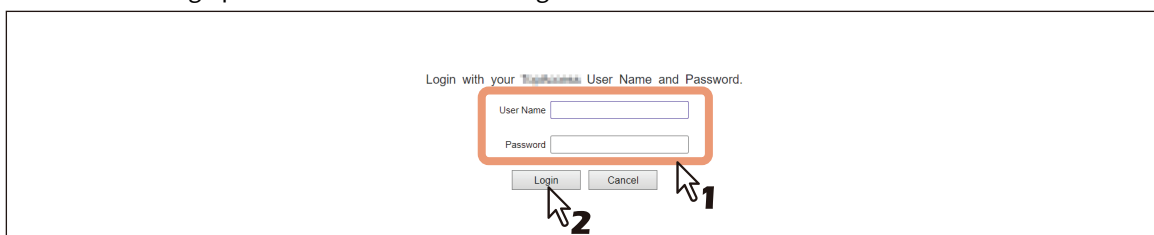
3 Enter the user name and password and click [Login].

If [User authentication] is enabled, you need to log in according to the [Authentication Type] setting.

- **[MFP Local Authentication]** – Enter your user name and password that are registered in the equipment.
- **[Windows Domain Authentication]** – Select [Domain Name] that manages users and enter your user name and password that are registered in the domain.
- **[LDAP Authentication]** – Select [LDAP Server] that manages users and enter your user name and password that are registered in that the server.

For details, see the reference below:

 P.240 “Setting up User Authentication Setting”




- Enter the user name and password that comply with TopAccess access policies.
- The Setup page is displayed.

Note

- The default log-in settings are “admin” for User Name and “123456” for Password. Depending on the model and destination, you are required to change the default administrator password for the first login. Follow the instructions on the screen.
- Failing to enter the correct password for a number of times at login will be considered unauthorized access and you may not be able to log in for a certain period of time. Contact the administrator if you see a message to inform you that your account is locked, or your user name or password is incorrect, and you are unable to continue the login operation.
- The input password is hidden with symbols.
- After login, you will be automatically logged out when the time specified in the [Session Timer] elapses.

Tip

- Lockout setting for user accounts can be set with [Administration] > [Security] > [Password Policy].
 P.262 “Password Policy settings”
- The [Session Timer] can be set with [Administration] > [Setup] > [General] > [WEB General Setting].

4

User Name: admin
Logout

Device

Job Status

Logs

Registration

Counter

User Management

Administration

-Setup

-Security

-Maintenance

-Registration

-Application

-License

^

Device

General

Network

Copier

Fax

Save as file

Email

Internet/Fax

Printer/e-Filing

Printer

Print Service

ICC Profile

Print Data Converter

MFP Collaboration

EWB

ODCA

Version

C Finisher

Device Information

Status	Ready
Name	MFP Collaboration
Location	
Copier Model	7700MFP e-STUDIO200AC
Serial Number	0000000000000000
MAC Address	00-11-11-11-11-11
Main Memory Size	6144 MB
Page Memory Size	940 MB
Save as File & e-Filing Space Available	29097 MB
Fax Space Available	930 MB
Contact Information	
Phone Number	
Message	
Alerts	

Paper

Drawer	Size	Thickness	Attribute	Capacity	Level
Drawer 1	A4	Plain	None	600	<div style="display: flex; gap: 2px;"><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div></div>
Drawer 2	A3	Plain	None	600	<div style="display: flex; gap: 2px;"><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div></div>
Drawer 3	A4	Plain	None	600	<div style="display: flex; gap: 2px;"><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div></div>
Drawer 4	A4	Plain	None	600	<div style="display: flex; gap: 2px;"><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div></div>
External Large Capacity Feeder	A4	Plain	None	2300	<div style="display: flex; gap: 2px;"><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div><div style="width: 15px; height: 15px; background-color: #2e7d32;"></div></div>

Tip

You can log out by clicking the [Logout] link at the top right of the page.

[Device]

[Device] Item List	18
Displayed Icons	20

[Device] Item List

TopAccess opens the [Device] page which includes a picture indicating the device status. At any time, the end user may click [REFRESH] to update the TopAccess status information. This page shows the following information about the device. The screen shows information, depending on the model and options you use.





The screenshot shows the TopAccess [Device] page. It features a navigation menu on the left with options like Device, Job Status, Logs, Registration, Counter, User Management, and Administration. The main content area displays device information, including a device image, a 'Device Information' table, an 'Options' table, a 'Toner' status table, and a 'Paper' table. A 'REFRESH' button is located in the top right corner. Numbered callouts 1 through 5 highlight specific features: 1 points to the 'Device Information' table, 2 points to the 'Options' table, 3 points to the 'Toner' status table, 4 points to the 'Paper' table, and 5 points to the 'REFRESH' button.







	Item name	Description
1	Device Information	<p>The following information is displayed.</p> <ul style="list-style-type: none"> • Status — Displays the device status. • Name — Displays the name of this equipment. • Location — Displays the equipment's location. • Copier Model — Displays the model name of this equipment. • Serial Number — Displays the serial number of this equipment. • MAC Address — Displays the MAC address of this equipment. • Main Memory Size (for some models only) — Displays the main memory size. • Page Memory Size (for some models only) — Displays the page memory size. • Save as File & e-Filing Space Available (for some models only) — Displays the total available space in the local folder and e-Filing on your equipment. • Fax Space Available — Displays the available space for sending and receive fax data. • Contact Information — Displays the contact name of the person responsible for managing this device. • Phone Number — Displays the phone number of the person responsible for managing this device. • Message — Displays administrative messages. • Alerts — Displays alert messages.

	Item name	Description
2	Options	<p>The following information is displayed.</p> <ul style="list-style-type: none"> • Finisher (for some models only)— Displays whether the Finisher is installed. • Hole Punch Unit (for some models only) — Displays whether the Hole Punch Unit is installed. • Fax — Displays whether the Fax Unit is installed. • Optional Function kit (for some models only) — Displays whether the optional function kit is installed.
3	Paper	<p>The following information is displayed.</p> <ul style="list-style-type: none"> • Drawer — Displays a list of the installed drawers. • Size — Displays the paper size set for each drawer. • Thickness — Displays the thickness of the paper set in each drawer. • Attribute — Displays the purpose of the paper set in each drawer. • Capacity — Displays the maximum paper capacity that can be set for each drawer. • Level — Displays the remaining amount of paper for each drawer. <p>Note</p> <p>The paper size for each drawer cannot be set from TopAccess. Set it from the touch panel of the equipment. For instructions on how to set the paper size for each drawer, see the reference below:</p> <p>Preparation of Paper (e-STUDIO6525AC Series/e-STUDIO6528A Series)-LOADING PAPER - Loading Paper in Drawers Preparation of Paper (e-STUDIO7527AC Series/e-STUDIO9029A Series) -LOADING PAPER - Loading Paper in Drawers</p>
4	Toner	Displays the estimated amount of toner remaining in the toner cartridges in the equipment.
5	REFRESH	Click this to update information.

Displayed Icons

When the equipment requires maintenance or when an error occurs with the equipment, icons indicating the status information appear near the graphic image of the equipment on the TopAccess [Device] page. The following are the icons displayed and their descriptions.

	Printer Error 1	<p>This icon indicates that a non-recommended toner cartridge is being used, and that the equipment has stopped printing. For information on resolving the error, see the reference below:</p> <p>Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge</p> <p>Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge</p>
	Printer Error 2	<p>This icon indicates one of the following:</p> <ul style="list-style-type: none"> You need to remove paper from the receiving tray. You need to remove paper from the Finisher tray. You need to remove the staples jammed in the Finisher. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Clearing a Staple Jam - Finisher Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Clearing a Staple Jam - Finisher You need to remove the staples jammed in the Saddle Stitch Unit. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series)- TROUBLESHOOTING FOR THE HARDWARE - Clearing a Staple Jam - Saddle Stitch unit Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Clearing a Staple Jam - Saddle Stitch unit You need to clear chads from the Hole Punch Unit. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Cleaning the Hole Punch Dust Bin Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Cleaning the Hole Punch Dust Bin A non-recommended toner cartridge is being used. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge You performed saddle stitch printing with the paper of the different sizes. The equipment cannot load paper from the Large Capacity Feeder. The equipment cannot eject the paper to the output tray. Data in the internal storage device of this equipment is required to be backed up. Replacing of the internal storage device of this equipment is required.
	Cover Open	<p>This icon indicates a cover such as the front cover or Automatic Duplexing Unit Cover is open.</p>
	Drawer Open	<p>This icon indicates the drawer is open.</p>

	Toner Empty	This icon indicates no toner is left. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing a Toner Cartridge
	Waste Toner Full	This icon indicates the waste toner box is full and requires replacing. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing the Waste Toner Box Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Replacing the Waste Toner Box
	Paper Empty	This icon indicates no paper is left in a drawer. For information on resolving the error, see the reference below: Preparation of Paper (e-STUDIO6525AC Series/e-STUDIO6528A Series)- LOADING PAPER - Loading Paper in Drawers Preparation of Paper (e-STUDIO7527AC Series/e-STUDIO9029A Series) - LOADING PAPER - Loading Paper in Drawers
	Paper Misfeed	This icon indicates a paper misfeed occurred. It also indicates the location of the paper misfeed. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Clearing a Paper Misfeed Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Clearing a Paper Misfeed
	Staples Empty	This icon indicates no staples are left in the Finisher. For information on resolving the error, see the reference below: Troubleshooting (e-STUDIO6525AC Series/e-STUDIO6528A Series) - TROUBLESHOOTING FOR THE HARDWARE - Refilling With Staples Troubleshooting (e-STUDIO7527AC Series/e-STUDIO9029A Series) - TROUBLESHOOTING FOR THE HARDWARE - Refilling With Staples
	Call for Service	Contact your service representative to have the equipment inspected.

[Job Status]

[Job Status] Overview	24
[Print Job] Item list	24
[Fax/InternetFax Job] Item list.....	26
[Scan Job] Item list	27
[Multi Station] Item list	28

[Job Status] Overview

You can display and delete print jobs, Fax/InternetFax jobs, and scan jobs. You can also print print jobs immediately.

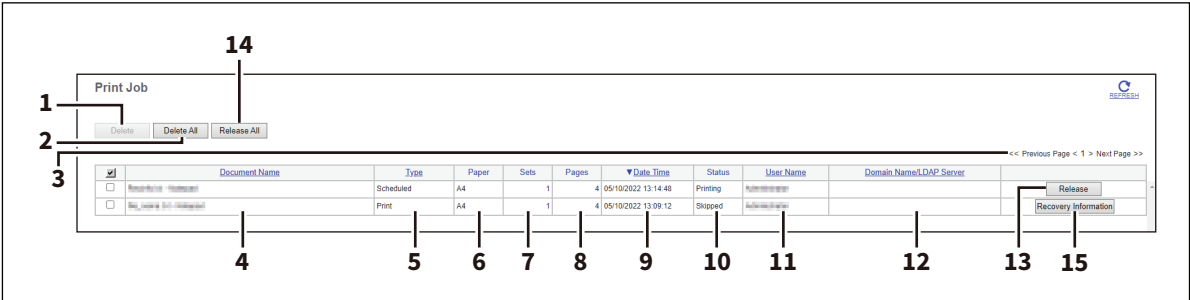
Tip

- When user authentication is enabled, you can operate on jobs associated with the user account you used to log in. However, a user account with administrator privileges can operate on all jobs.
- Click [REFRESH] at the upper part of the page to update information.

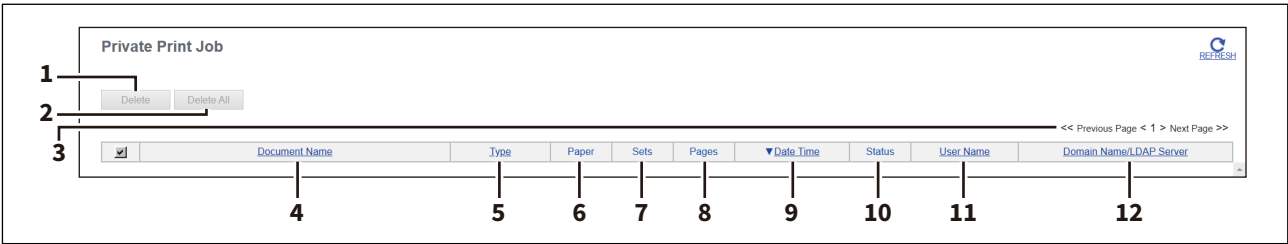
■ [Print Job] Item list

The Print Job page is divided into Print Job, Private Print Job, and Hold Print Job. You can select Private Print Job and Hold Print Job only when you are logged in with a user account with administrator privileges in the access policy mode.

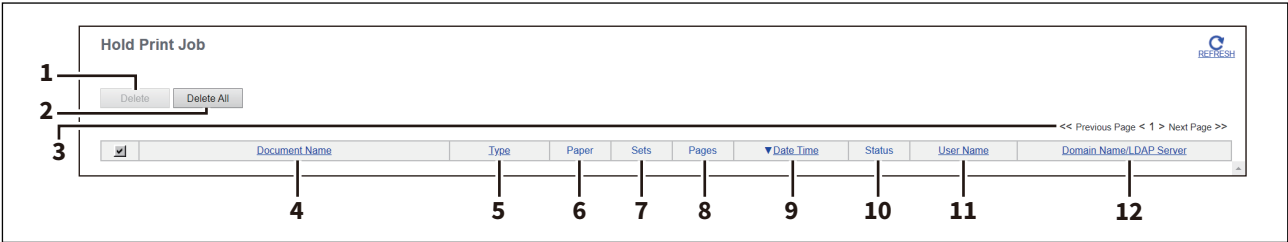
[Print Job] screen



[Private Print Job] screen



[Hold Print Job] screen



	Item name	Description
1	[Delete] button	The selected print job is deleted.
2	[Delete All] button	All print jobs are deleted.
3	Select Page	Allows you to select a page when there are 101 items or more.
4	Document Name	Displays the document name of the print job. Document names are displayed using 10 asterisks (*) when the Confidentiality Setting is enabled. P.106 “Setting up Confidentiality Setting”
5	Type	Displays the print job set in the printer driver. Possible values of print job are: [Normal], [Scheduled], [Private], [Proof], [Hold], and [MultiStation].
6	Paper	Displays the paper size of the print jobs.

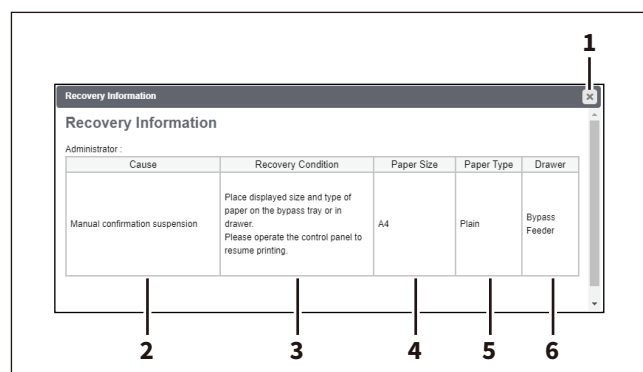
	Item name	Description
7	Sets	Displays the number of copies set for the print jobs.
8	Pages	Displays the number of pages of the print job.
9	Date Time	Displays the date and time when the print job was released from the client computers. They are displayed using “year, month, day, hour, minute, and second”. For example: 2016/12/24 12:34:56
10	Status	Displays the status of the print job. Possible values of status are: [Paused], [Wait], [Suspend], [Skipped], [Process], [Printing], and [Scheduled].
11	User Name	Displays the user account name of the owner of the print job.
12	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who is the owner of the print job.
13	[Release] button	If the selected print job is in the print queue, the job is printed.
14	[Release All] button	All print jobs on all pages are printed.
15	[Recovery Information] button	If the selected print job was skipped while the job skip feature was enabled, the recovery information screen is displayed. <div> <div></div> <div>P.25 “[Recovery Information] screen”</div> </div> <div> <div></div> <div>P.104 “Setting up Job Control”</div> </div>

Tip

- Print jobs that have finished being printed are displayed on the [Logs] page.
- Click a table heading item to refresh the page and reorder the print job list in the specified order.
- You cannot use the Print Job page to delete fax/Internet Fax jobs and E-mail reception print jobs.
- Private print jobs and hold print jobs cannot be released from TopAccess.

❏ [Recovery Information] screen

The Recovery Information screen displays the conditions for resuming printing.



	Item name	Description
1	[Close] button	Closes the [Recovery Information] screen.
2	Cause	Displays the cause of the print interruption.
3	Recovery Condition	Displays the procedure for resuming printing.
4	Paper Size	Displays the paper size set for the interrupted print job.
5	Paper Type	Displays the paper type set for the interrupted print job.
6	Drawer	Displays the paper source set for the interrupted print job.

■ [Fax/InternetFax Job] Item list

The Fax/InternetFax Job page displays the following information for each fax transmission job.

Fax / InternetFax Job

1: Title bar
 2: Toolbar with 'Delete' and 'Delete All' buttons
 3: Table header row
 4: File No. column
 5: TO(Name) column
 6: TO(Fax No./Email) column
 7: Delay Time column
 8: Pages column
 9: Date Time column (with dropdown arrow)
 10: Status column
 11: User Name column
 12: Domain Name/LDAP Server column

<input checked="" type="checkbox"/>	File No.	TO(Name)	TO(Fax No./Email)	Delay Time	Pages	Date Time	Status	User Name	Domain Name/LDAP Server

<< Previous Page < 1 > Next Page >>

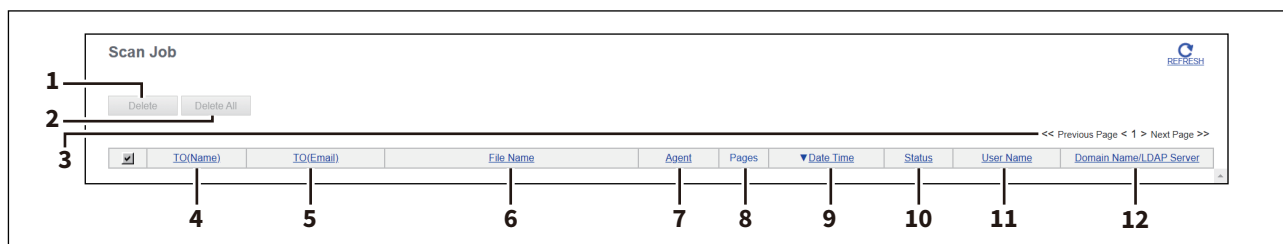
	Item name	Description
1	[Delete] button	The selected fax job is deleted.
2	[Delete All] button	All fax jobs are deleted.
3	Select Page	Allows you to select a page when there are 101 items or more.
4	File No.	Displays the file number (001 to 100) to identify the fax transmission job.
5	TO(Name)	Displays the destination name set for the fax transmission job.
6	TO(Fax No./Email)	Displays the fax number or E-mail address of the destination.
7	Delay Time	Displays the delayed time set for the fax transmission job.
8	Pages	Displays the number of pages of the fax transmission job.
9	Date Time	Displays the date and time when the fax transmission job is released from the touch panel or client computer using the N/W-Fax driver. They are displayed using “year, month, day, hour, minute, and second”. For example: 2016/12/24 12:34:56
10	Status	Displays the status of the fax transmission job. Possible values of status are: [Delayed], [Wait], [Line1], [Line2], and [Network].
11	User Name	Displays the user account name of the owner of the fax transmission job.
12	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who is the owner of the fax transmission job.

Tip

- Transmission jobs that have finished their transmission are displayed on the [Logs] page.
- Click a table heading item to refresh the page and reorder the print job list in the specified order.

■ [Scan Job] Item list

The Scan Job page displays the following information for each scan job.



	Item name	Description
1	[Delete] button	The selected scan job is deleted.
2	[Delete All] button	All scan jobs are deleted.
3	Select Page	Allows you to select a page when there are 101 items or more.
4	TO(Name)	Displays the destination (name) to where the scanned document is sent via an E-mail.
5	TO(Email)	Displays the destination (E-mail address) to where the scanned document is sent via an E-mail.
6	File Name	When the job performs the Scan to File or USB or Scan to e-Filing, it displays the document name to be stored. File names are displayed using 10 asterisks (*) when the Confidentiality Setting is enabled. P.106 “Setting up Confidentiality Setting”
7	Agent	Displays the agent of the scan job. Possible values of agent are: [Email], [Save as file], [Store to e-Filing], and [Store to USB Media].
8	Pages	Displays the number of pages of the scan job.
9	Date Time	Displays the date and time when the scan job is released from the touch panel. They are displayed using “year, month, day, hour, minute, and second”. For example: 2016/12/24 12:34:56
10	Status	Displays the status of the scan job. Possible values of status are: [Wait], [Suspended], [Processing], and [Scanning]
11	User Name	Displays the user account name who is the owner of the scan job.
12	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who is the owner of the scan job.

Tip

- Scan jobs that have finished being scanned are displayed on the [Logs] page.
- Click a table heading item to refresh the page and reorder the print job list in the specified order.

■ [Multi Station] Item list

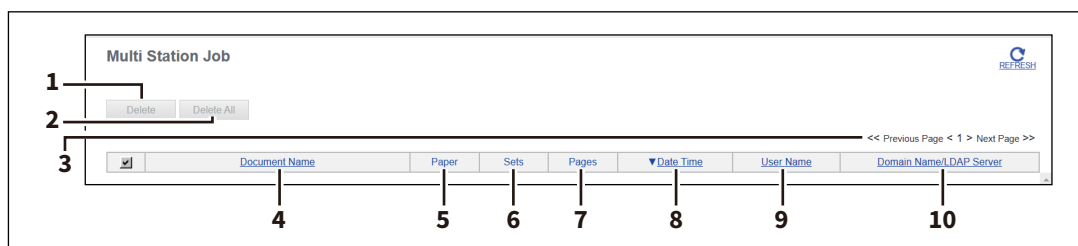
The following two pages show information about print jobs that you process with the Multi Station Print function.

- **Multi Station Job** – Displays information about the jobs that are in the print queue.
- **Multi Station Printed Job** – Displays information about the printed jobs.

You can select these pages only when you are logged in with a user account with administrator privileges in the access policy mode.

Note

You need the Multi Station Print Enabler option to use the [Multi Station Print] function. Contact your service technician for details.



	Item name	Description
1	[Delete] button	The selected print job is deleted.
2	[Delete All] button	All print jobs are deleted.
3	Select Page	Allows you to select a page when there are 101 items or more.
4	Document Name	Displays the document name of the print job.
5	Paper	Displays the paper size specified on the print job.
6	Sets	Displays the number of copies specified on the print job.
7	Pages	Displays the total number of pages in the print job.
8	Date Time	Displays the date and time when the print job was received from the client computer. The date and time are displayed in “YYYY/MM/DD HH:MM:SS” format. Example: 2016/12/24 12:34:56
9	User Name	Displays the owner user account name of the print job.
10	Domain Name/LDAP Server	Displays the domain name or LDAP server of the owner user account of the print job.

[Logs]

[Logs] Overview	30
[View Logs] Item list	30
[Export Logs] Item list <access policy mode>	38
[Log Settings] Item list <access policy mode>	40

[Logs] Overview

You can check the job history.

Note

Check the logs periodically to ensure that there is no unauthorized access to the equipment as a result of spoofing.

Tip

- Logs are recorded from the moment the equipment is turned on until it is shut down. Log recording continues also after entering the Super Sleep mode.
- Up to 100 logs are displayed in chronological order with the most recent first. When the number of logs exceeds 101, select the page you want to view. You can check up to 5,000 logs in Print Job Log Export, Fax Transmission Journal Export, Fax Reception Journal Export, and Scan Log Export, and up to 10,000 logs in Messages Log Export by exporting them. The oldest logs are deleted when the number of logs exceeds the maximum limit.
- The default Administrator and Auditor roles can check all logs. For more information on default roles and privileges, see the following:
 📖 P.85 “Default roles and privileges”
- When user authentication is enabled, you can check the logs associated with the user account you used to log in. Furthermore, a user account to which the default Administrator or Auditor role have been assigned can check all logs.
- Click [REFRESH] at the upper part of the page to update information.

■ [View Logs] Item list

□ Print Log

The Print Log page displays the following information for each print job log.

1	Print Log										REFRESH
	Document Name	Type	Paper	Sets	Pages	▼ Date Time	Status	User Name	Domain Name/LDAP Server	Project Code	<< Previous Page < 1 2 3 4 5 6 7 8 > Next Page >>
	2	3	4	5	6	7	8	9	10	11	

	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more.
2	Document Name	Displays the document name of the print job.
3	Type	Displays the print job type.
4	Paper	Displays the paper size of the print jobs.
5	Sets	Displays the number of copies set for print jobs.
6	Pages	Displays the number of pages of the print job.
7	Date Time	Displays the date and time that the print job was released from the client computers.
8	Status	Displays the status of the print log.
9	User Name	Displays the user account name of the owner of the print job.
10	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who was the owner of the print job.
11	Project Code	Displays the Project Code of the print job.

Tip

Click a table heading item to refresh the page and reorder the print log list in the specified order.

❑ Transmission Journal

The Transmission Journal page displays the following information for each transmission journal.

Transmission Journal													
1	No.	File No.	Duration	TO(Name)	TO(Fax No./Email)	Dept	Line	Mode	Pages	▼ Date Time	Status	User Name	Domain Name/LDAP Server
	2	3	4	5	6	7	8	9	10	11	12	13	14

	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more.
2	No.	Displays the serial number of the journals.
3	File No.	Displays the file number to identify the received job.
4	Duration	Displays the time length taken for the transmissions. If it takes more than 1 hour, "59:59" is indicated.
5	TO (Name)	Displays the destination name set for the transmission job.
6	TO (Fax No./Email)	Displays the fax number or E-mail address of the destination for the transmission job.
7	Dept	Displays the department code if department management is enabled.
8	Line	Displays the line used.
9	Mode	Displays the transmission mode*.
10	Pages	Displays the number of pages of the transmission job.
11	Date Time	Displays the date and time the transmission job was performed.
12	Status	Displays the result of the transmission.
13	User Name	Displays the user account name of the owner of the transmission job.
14	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who was the owner of the transmission job.

* The transmission mode is displayed by a combination of a 2-digit letter code, a 3-digit numeric code, and up to a 4-digit supplemental code. For example: EC 603

2-digit letter code (Communication Mode)	1st numeric code (bps)	2nd numeric code (Resolution)	3rd numeric code (Mode)	Up to 4 digit supplemental code
EC: ECM G3: G3 ML: E-mail	0: 2400 1: 4800 2: 7200 3: 9600 4: 12000 5: 14400 6: V.34	0: 8x3.85 1: 8x7.7 2: 8x15.4 4: 16x15.4 8: 300 dpi B: 600 dpi D: 150 dpi	0: MH 1: MR 2: MMR 3: JBIG	P: Polling SB: Mailbox SR/R: Relay mailbox SF/F: Forward mailbox ML: Internet Fax I: N/W-Fax O: Offramp Gateway

Tip

Click a table heading item to refresh the page and reorder the transmission journal list in the specified order.

❑ Reception Journal

The Reception Journal page displays the following information for each reception journal.

Reception Journal													
1	No.	File No.	Duration	From(Name)	From(Fax No./Email)	Dept	Line	Mode	Pages	▼ Date Time	Status	User Name	Domain Name/LDAP Server
	2	3	4	5	6	7	8	9	10	11	12	13	14

	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more.
2	No.	Displays the serial number of the journals.
3	File No.	Displays the file number to identify the received job.
4	Duration	Displays the time taken for the receptions. If it takes more than 1 hour, "59:59" is indicated.
5	From (Name)	Displays the sender's name of the received job.
6	From (Fax No./Email)	Displays the fax number or E-mail address of the sender for the received job.
7	Dept	Displays the department code if the department management is enabled.
8	Line	Displays the line used.
9	Mode	Displays the reception mode*.
10	Pages	Displays the number of pages of the received job.
11	Date Time	Displays the date and time of receiving the job.
12	Status	Displays the result of the reception.
13	User Name	Displays the user account name of the owner of the received job.
14	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who was the owner of the received job.

* The reception mode is displayed by a combination of a 2-digit letter code, a 3-digit numeric code, and up to a 4-digit supplemental code. For example: EC 603

2-digit letter code (Communication Mode)	1st numeric code (bps)	2nd numeric code (Resolution)	3rd numeric code (Mode)	Up to 4 digit supplemental code
EC: ECM G3: G3 ML: E-mail	0: 2400 1: 4800 2: 7200 3: 9600 4: 12000 5: 14400 6: V.34	0: 8x3.85 1: 8x7.7 2: 8x15.4 4: 16x15.4 8: 300 dpi B: 600 dpi D: 150 dpi	0: MH 1: MR 2: MMR 3: JBIG	P: Polling SB: Mailbox SR/R: Relay mailbox SF/F: Forward mailbox ML: Internet Fax I: N/W-Fax O: Onramp Gateway

Tip

Click a table heading item to refresh the page and reorder the reception journal list in the specified order.

□ Scan Log

The Scan Log page displays the following information for each scan job log.

Scan Log										
1	TO(Name)	TO(Email)	File Name	Agent	Mode	Pages	▼ Date Time	Status	User Name	Domain Name/LDAP Server
	2	3	4	5	6	7	8	9	10	11

	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more.
2	TO (Name)	Displays the destination (name) to where the scanned document was sent via an E-mail.
3	TO (Email)	Displays the destination (E-mail address) to where the scanned document was sent via an E-mail.
4	File Name	Displays the file name stored in a shared folder or e-Filing. This item may not be displayed depending on the access policies.
5	Agent	Displays the agent of the scan job.
6	Mode	Displays the transmission mode using 6-letter codes*.
7	Pages	Displays the number of pages of the scan job.
8	Date Time	Displays the date and time when the scan job was released from the touch panel.
9	Status	Displays the detailed result status of the scan job.
10	User Name	Displays the user account name of the owner of the scan job.
11	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account who was the owner of the scan job.

* Codes are displayed in the following format.

Code format: AA B C D E

<u>AA</u>: This describes the job type.	
CA	Copy and File Copy and Store to e-Filing
CT	Copy to e-Filing (without printing)
FS	Relay Mailbox Transmission
FF	Fax Received Forward
FE	Internet Fax Received Forward
ST	Scan to File or USB Scan to e-Filing Scan to Email
FA	Fax and Save as File
PA	Print and e-Filing
PT	Print to e-Filing
IA	N/W-Fax and Save as File
BE	e-Filing to Email
RS	Remote Scan or Web Services Scan
MS	Meta Scan
EN	E-mail notification
WS	WS Scan
RI	Save Result Report as File Email Result Report
AT	Save in Storage for Applications

<u>B</u>: This describes the transmission type.	
0	e-Filing
1	Email (SMTP)
2	FTP
3	SMB
4	Save in a local folder
5	NetWare IPX/SPX
6	USB
7	NetWare TCP/IP
8	FTPS
9	Remote Scan or Web Services Scan

<u>C</u>: This describes the resolution.	
0	100 dpi
1	150 dpi
2	200 dpi
3	300 dpi
4	400 dpi

5	600 dpi
A	8 x 3.85 (line/mm) (203 x 98)
B	8 x 7.7 (line/mm) (203 x 196)
C	8 x 15.4 (line/mm) (203 x 391)
D	16 x 15.4 (line/mm) (400 x 391)

D: This describes the file format.	
0	e-Filing
1	TIFF (Multi)
2	TIFF (Single)
3	PDF (Multi) or Encrypted PDF (Multi)
4	JPEG
5	PDF (Single) or Encrypted PDF (Single)
6	Slim PDF (Multi)
7	Slim PDF (Single)
8	XPS (Multi)
9	XPS (Single)
A	DIB
B	PDF/A (Multi)
C	PDF/A (Single)
D	Searchable PDF(Multi) or Searchable Encrypted PDF (Multi)
E	Searchable PDF(Single) or Searchable Encrypted PDF (Single)
F	Searchable Slim PDF (Multi)
G	Searchable Slim PDF (Single)
H	Searchable PDF/A (Multi)
I	Searchable PDF/A (Single)
J	DOCX (Multi)
K	DOCX (Single)
L	XLSX (Multi)
M	XLSX (Single)
N	PPTX (Multi)
O	PPTX (Single)
P	Slim PDF/A (Multi)
Q	Slim PDF/A (Single)
R	Searchable Slim PDF/A (Multi)
S	Searchable Slim PDF/A (Single)

E: This describes the file color mode.

B	Black
G	Gray Scale
C	Color
M	Mix

Note

The file format is recorded as DIB in the scan log if the data are scanned in BMP, JPEG, TIFF, or PNG format using the WIA (Windows Image Acquisition) driver.

Tip

Click a table heading item to refresh the page and reorder the scan log list in the specified order.

Application Log

The Application Log page displays the following information for each application log item.

Application Log					
Application Name	Error Level	Message	▼ Date Time	User Name	Domain Name/LDAP Server
1	2	3	4	5	6

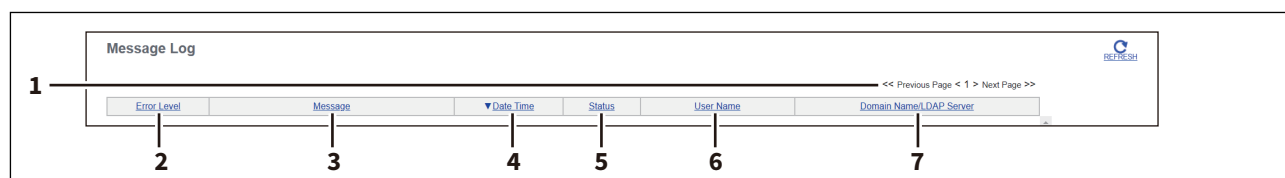
	Item name	Description
1	Application Name	Displays the application name where the error occurred.
2	Error Level	Displays the error level. Error — Errors that may not be cleared by some users. Warning — Errors that may be cleared by the administrator. Information — Errors that may be cleared by general users, or not errors.
3	Message	Displays the message if there is any.
4	Date Time	Displays the date and time of the error.
5	User Name	Displays the user account name that is related to the message.
6	Domain Name / LDAP Server	Displays the domain name or LDAP server of the user account that is related to the message.

❑ Message Log <access policy mode>

The Message Log page displays errors which have occurred on your model.

Tip

- Displays only when you are logged in with a user account which is granted administrator privileges or display privilege in the access policy mode.
- The default Administrator and Auditor roles can check all message logs. For more information on default roles and privileges, see the reference below:
📖 P.85 “Default roles and privileges”



	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more.
2	Error Level	Displays the error level. Error — Error that user and administrator may not be recoverable. Warning — Error that administrator is recoverable. Information — Error that end user is recoverable or that event is not error.
3	Message	Displays the message if available.
4	Date Time	Displays the date and time of the error.
5	Status	Displays the error code.
6	User Name	Displays the user account name related to the message.
7	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account related to the message.

Tip

For details on error codes and error messages, see the references below:

Frequently Asked Questions - QUESTIONS FOR ERROR MESSAGES

Frequently Asked Questions - QUESTIONS FOR ERROR CODES

■ [Export Logs] Item list <access policy mode>

You can erase logs or export them in a file.

Tip

- Displays only when you are logged in with a user account which is granted administrator or display privileges in the access policy mode.
- The exported data file can be either CSV format or XML format. [CSV] is set as the default.
- You can export up to 5,000 logs in Print Job Log Export, Fax Transmission Journal Export, Fax Reception Journal Export, and Scan Log Export, and up to 10,000 logs in Messages Log Export. The oldest logs are deleted when the number of logs exceeds the maximum limit.

The screenshot shows the 'Export Logs' window with a list of six exportable log types. Each log type has a status 'Not Created' and a 'File Name' field. Below these are 'File Size' and 'Date Created' fields. The 'Export Data Format' is set to 'CSV' (selected) or 'XML'. At the bottom of each section are three buttons: 'Create New File & Clear Log', 'Clear Log', and 'Create New File'. A note at the top states: 'It may take more than 10 minutes if there are a lot of entries.'

	Item name	Description
1	Print Job Log Export	<p>You can erase print logs or export (download) them in a file.</p> <p>Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file.</p> <p>Clear Log — Erases logs.</p> <p>Create New File — Creates a file according to the file format of the export data.</p> <p>You can display or download by clicking the created file.</p>
2	Fax Transmission Journal Export	<p>You can erase the transmission journal or export (download) it to a file.</p> <p>Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file.</p> <p>Clear Log — Erases logs.</p> <p>Create New File — Creates a file according to the file format of the export data.</p> <p>You can display or download by clicking the created file.</p>

	Item name	Description
3	Fax Reception Journal Export	You can erase the reception journal or export (download) it to a file. Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file. Clear Log — Erases logs. Create New File — Creates a file according to the file format of the export data. You can display or download by clicking the created file.
4	Scan Log Export	You can erase scan logs or export (download) them in a file. Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file. Clear Log — Erases logs. Create New File — Creates a file according to the file format of the export data. You can display or download by clicking the created file.
5	Application Log Export	You can erase application logs or export (download) them in a file. Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file. Clear Log — Erases logs. Create New File — Creates a file according to the file format of the export data. You can display or download by clicking the created file.
6	Messages Log Export	You can erase message logs or export (download) them in a file. Create New File & Clear Log — Creates a file according to the file format of the export data. Erases logs after a file has been created. You can display or download by clicking the created file. Clear Log — Erases logs. Create New File — Creates a file according to the file format of the export data. You can display or download by clicking the created file.

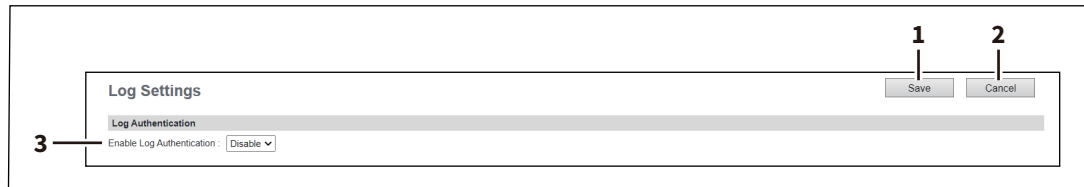
■ [Log Settings] Item list <access policy mode>

Tip

Displays only when you are logged in with a user account which is granted administrator or display privileges in the access policy mode.

□ Log Authentication

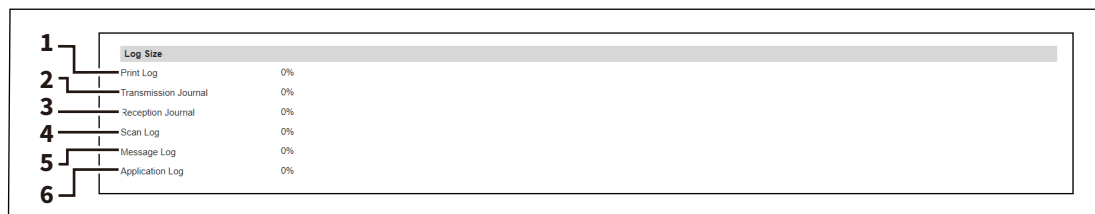
You can specify whether or not to use log authentication.



	Item name	Description
1	[Save] button	Saves log authentication settings.
2	[Cancel] button	Cancels the settings.
3	Enable Log Authentication	Enables log authentication. When log authentication is enabled, the log display for users will be restricted according to access policies. <ul style="list-style-type: none">• Enable — Enables log authentication. Display will be restricted according to access policies.• Disable — Disables log authentication. Logs for all users will be displayed.

□ Log size

Log size displays the log size.



	Item name	Description
1	Print Log	Displays the log size of print jobs.
2	Transmission Journal	Displays the log size of transmission journals.
3	Reception Journal	Displays the log size of reception journals.
4	Scan Log	Displays the log size of scan jobs.
5	Message Log	Displays the log size of message logs.
6	Application Log	Displays the log size of Application Logs.

[Registration]

[Registration] Overview.....	42
Public Home.....	42
Public Theme Settings.....	42
Public Home Settings	42
[Address Book] Item list.....	42
[Inbound FAX routing] Item list	53

[Registration] Overview

You can register templates, the address book, and inbound fax routing.

■ Public Home

General users can set [Public Home] under [Registration] only if they are allowed at [Home Setting].

📖 P.113 “Home Setting”

For [Public Home], see the reference below:

📖 P.300 “Public Home”

■ Public Theme Settings

General users can set [Public Theme Settings] under [Registration] only if they are allowed at [Home Setting].

📖 P.113 “Home Setting”

For [Public Theme Settings], see the reference below:

📖 P.334 “Public Theme Settings”

■ Public Home Settings

General users can set [Public Home Settings] under [Registration] only if they are allowed at [Home Setting].

📖 P.113 “Home Setting”

For [Public Home Settings], see the reference below:

📖 P.335 “Public Home Settings”

■ [Address Book] Item list

❏ [Address Book] screen

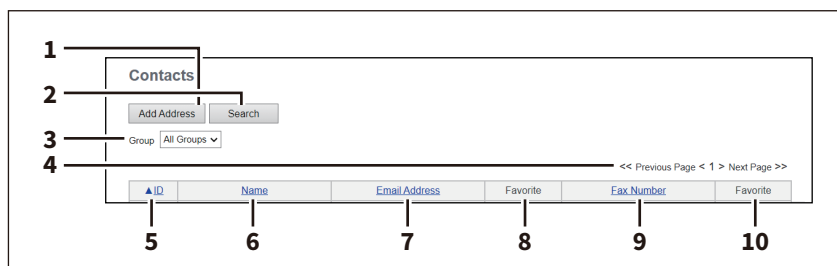
You can manage a contact list to be used in E-mail, Internet Fax, and fax transmissions.

Tip

- Click [Contacts], [Favorite Contact], [Groups], or [Favorite Groups] to switch the display between the list of addresses and the list of groups where contacts are assigned.
- Address Book can be also managed using the touch panel. For details, see the reference below:

User Functions - SETTING ITEMS (User) - Address - Managing contacts in address book

Contacts



	Item name	Description
1	[Add Address] button	Allows you to add a new contact in the address book. 📖 P.48 “[Create Destination information]/[Edit Destination information] screen”
2	[Search] button	Allows you to search a contact from the address book. 📖 P.50 “[Search Contact] screen”
3	Group	Select a group to display in the following options or from the group name. <ul style="list-style-type: none">• All Groups — Displays all the groups.• Local — Displays the local address book.• Shared — Displays the shared address book.
4	Select Page	Allows you to select a page when there are 101 items or more.

	Item name	Description
5	ID	Displays the registered ID of the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
6	Name	Displays the name registered to the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
7	Email Address	Displays the E-mail address registered to the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
8	Favorite	This check box is selected when Email Address is set as Favorite.
9	Fax Number	Displays the fax number registered to the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
10	Favorite	This check box is selected when Fax Number is set as Favorite.

Favorite Contact

	Item name	Description
1	[Save] button	Saves the specified information.
2	[Reset] button	Erases the specified information.
3	[Move Up]/[Move Down] button	Changes the priority order in the list.
4	ID	Displays the registered ID of the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
5	Name	Displays the name registered to the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
6	Email Address	Displays the E-mail address registered to the contact. P.48 “[Create Destination information]/[Edit Destination information] screen”
7	Favorite	This check box is selected when Email Address is set as Favorite.
8	Fax Number	Displays the fax number registered to the contact.
9	Favorite	This check box is selected when Fax Number is set as Favorite.

Group

The screenshot shows the 'Groups' screen. A 'New' button is at the top left, labeled with a '1'. Below it is a list of group entries. The first entry is labeled with a '2' pointing to its 'ID' field. The 'Group Name' field of the first entry is labeled with a '3'. The 'Contacts' field of the first entry is labeled with a '4'. The 'Favorite' checkbox of the first entry is labeled with a '5'.

	Item name	Description
1	[New] button	Allows you to add a new group. P.52 “[Create Group information]/[Edit Group information] screen”
2	ID	Displays the registered ID of the group. P.52 “[Create Group information]/[Edit Group information] screen”
3	Group Name	Displays the registered name of the group. P.52 “[Create Group information]/[Edit Group information] screen”
4	Contacts	Displays how many address books are registered in the group.
5	Favorite	This check box is selected when Group is set as Favorite.

Favorite Groups

The screenshot shows the 'Favorite Group' screen. A 'Save' button is at the top right, labeled with a '1'. Below it are 'Reset', 'Move Up', and 'Move Down' buttons. 'Reset' is labeled with a '2'. 'Move Up' and 'Move Down' are both labeled with a '3'. Below these buttons is a list of favorite groups. The first entry is labeled with a '4' pointing to its 'ID' field. The 'Group Name' field of the first entry is labeled with a '5'. The 'Contacts' field of the first entry is labeled with a '6'. The 'Favorite' checkbox of the first entry is labeled with a '7'.

	Item name	Description
1	[Save] button	Saves the specified information.
2	[Reset] button	Erases the specified information.
3	[Move Up]/[Move Down] button	Changes the priority order in the list.
4	ID	Displays the registered ID of the group. P.52 “[Create Group information]/[Edit Group information] screen”
5	Group Name	Displays the registered name of the group. P.52 “[Create Group information]/[Edit Group information] screen”
6	Contacts	Displays how many address books are registered in the group.
7	Favorite	This check box is selected when Group is set as Favorite.

Shared Setting

The screenshot shows the 'Shared Setting' interface. At the top right are 'Save' (1) and 'Cancel' (2) buttons. Below them is the 'Shared Setting' section with a dropdown menu (3) set to 'Enable (Primary)'. Underneath is the 'Connection Timeout (Primary MFP - Secondary MFP)(1-180)' field (4) with a value of '30' and the unit 'Seconds'. The 'Primary MFP Setting' section (5) includes 'Add' (6), 'Delete' (7), and 'Sync All' (8) buttons. Below these is an input box (9) for the 'Server Address'. At the bottom is a table with columns: 'Server Address' (9), 'TopAccess' (10), 'Sync' (11), and 'Last Update' (12). The table contains one row with a checkbox, an input field, and two buttons.

Note

If you have selected [Use Common Settings] on the [MFP Collaboration] > [Shared Address Book] screen, you cannot add and delete the secondary MFPs on this screen.

📖 P.224 “Shared Address Book”

5

[Registration]

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Shared Address Book	<p>Select whether this equipment should act as a primary or secondary MFP when managing the Shared Address Book in sync with other MFPs.</p> <ul style="list-style-type: none"> • Disable — Does not synchronize. • Enable (Primary) — Synchronizes as a primary MFP. • Enable (Secondary) — Synchronizes as a secondary MFP. <p>Note</p> <p>Select one MFP from among MFPs and select [Enable (Primary)] on it. Be sure to select [Enable (Secondary)] on other MFPs. As a result, the Address Book of the primary MFP can be shared on the secondary MFPs.</p>
4	Connection Timeout	Enter the timeout time to stop communicating if you cannot connect to the primary or secondary MFP. You can set 1 to 180 seconds.
5	[Add] button	<p>Adds a new secondary MFP.</p> <p>Enter the IP address or host name for the target secondary MFP in the input box below, and then click the [Add] button to register. You can register up to 10 MFPs.</p>
6	[Delete] button	Deletes the selected MFP from the list of secondary MFPs.
7	[Sync All] button	Synchronizes all the secondary MFPs with the primary MFP to share the Address Book.
8	Input box	Enter the IP address or host name when registering a secondary MFP.
9	Server Address	Shows the IP address of the added secondary MFP.
10	[TopAccess] button	Starts TopAccess.
11	[Sync] button	Synchronizes the secondary MFP with the primary MFP to share the Address Book.
12	Last Update	Displays the previous update time.

Import

You can import address information exported from an address book on another equipment or a different address book program in the CSV or XML format.

The importing method of address book data is either adding imported data to the address book already registered in this equipment or deleting all the address book data already registered and replacing them with the imported data. It is recommended that you export an address book in the CSV or XML format and edit it when creating address book data.

Note

You cannot import an address book when it exceeds the number of characters specified for each item or it includes invalid characters.

- Last Name: 32 characters
- First Name: 32 characters
- Index: 64 characters
- Email Address: 192 alphanumerical characters
- Phone Number: 128 numbers
- Tel Number 2: 128 numbers
- Company: 128 characters
- Department: 128 characters
- Keyword: 256 characters
- SUB: 20 characters
- SID: 20 characters
- SEP: 20 characters
- PWD: 20 characters

Tip

The group data may not be included depending on the imported address book data.

The screenshot shows the 'Import' dialog box for an 'Address Book'. It contains the following fields and controls:

- 1** points to the 'Import Method' section, which has two radio buttons: 'Addition' (selected) and 'Overwrite'.
- 2** points to the 'Address Book Type' section, which has two radio buttons: 'Local' (selected) and 'Shared'.
- 3** points to the 'Favorite' section, which has a dropdown menu currently set to 'Enable'.
- 4** points to the 'File Name' section, which includes a 'Choose File' button, the text 'No file chosen', and an 'Import' button.

	Item name	Description
1	Import Method	Specify the import method of the address book. Addition — Select this to append the imported information to the existing data. Overwrite — Select this to replace the existing data with the imported information.
2	Address Book Type	Specify “Local” or “Shared” as the import target when using the Shared Address Book function.
3	Favorite	Specify whether or not to enable Favorite information. The default is [Enable].
4	File Name	Select the address book file to be imported. [Choose File] button — Allows you to select the address book file. [Import] button — Imports the selected address book file.

Export

Tip

The group data may not be included depending on the exported address book data.

The screenshot shows the 'Export' dialog box with the following elements and numbered callouts:

- 1**: Points to the 'Address Book' header.
- 2**: Points to the 'File Name' field, which displays 'ADDR_220824.csv'.
- 3**: Points to the 'File Size' field, which displays '4628'.
- 4**: Points to the 'Date Created' field, which displays 'TUE AUG 24 15:31:53 2022'.
- 5**: Points to the 'Export Data Format' section, which has radio buttons for 'CSV' (selected) and 'XML'.
- 6**: Points to the 'Address Book Type' section, which has radio buttons for 'Local' (selected) and 'Shared'.
- 7**: Points to the 'Favorite' section, which has a dropdown menu currently set to 'Enable'.

A 'Create New File' button is located at the bottom right of the dialog box.

	Item name	Description
1	File Name	Displays the file name of the created export files. Click a file name to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the created date of the export files.
4	Export Data Format	Select the file format of the export file. <ul style="list-style-type: none">• CSV — Select this to create the file in the CSV format.• XML — Select this to create the file in the XML format.
5	Address Book Type	Specify “Local” or “Shared” as the export source when using the Shared Address Book function.
6	Favorite	Specify whether or not to enable Favorite information. The default is [Enable].
7	[Create New File] button	Creates the export file. <div>Tip If you previously exported address book data, the exported file link and information are displayed in the Address Book area. You can click the link to save the previously exported file.</div>

❑ [Create Destination information]/[Edit Destination information] screen

The screenshot shows the 'Create Destination information' screen. At the top right are buttons 1 (Save) and 2 (Cancel). Below them is a blue bar with 'Address Book' and a right arrow (3). Under this bar are buttons 4 (Reset), 5 (Delete), and 6 (Fax Setting). Below these is a 'Destination' dropdown menu (6) currently set to 'Local'. A note indicates that either '*' or '**' is required. Below the note are input fields for: 7 (First Name), 8 (Last Name), 9 (Index), 10 (Email Address), 11 (Fax Number), 12 (2nd Fax Number), 13 (Company), 14 (Department), and 15 (Keyword). Each field has a 'Favorite' checkbox to its right.

	Item name	Description
1	[Save] button	Saves the entered information.
2	[Cancel] button	Cancels adding or editing a contract.
3	[Reset] button	Erases information entered in the given box.
4	[Delete] button	Deletes the displayed contact.
5	[Fax Setting] button	Registers the contact for fax transmission. P.49 "[Fax Setting] screen"
6	Destination	Select Local Address Book or Shared Address Book as the registration target for contact information. Note This is only available when [Shared Setting] > [Shared Address Book] is set to [Enable (Primary)] or [Enable (Secondary)].
7	First Name	Enter the first name of the contact. You can enter up to 32 characters. Invalid characters are replaced with "!".
8	Last Name	Enter the last name of the contact. You can enter up to 32 characters. Invalid characters are replaced with "!".
9	Index	Enter the characters to be used as the index. You can enter up to 64 characters.
10	Email Address	Enter the E-mail address of the contact. You can enter up to 192 characters. Select [Favorite] to specify the contact as Favorite.
11	Fax Number	Enter the fax number of the contact. You can enter up to 128 characters. Select [Favorite] to specify the contact as Favorite.
12	2nd Fax Number	Enter the second fax number of the contact. You can enter up to 128 characters.
13	Company	Enter the company name of the contact. You can enter up to 64 characters. Invalid characters are replaced with "!".
14	Department	Enter the department name of the contact. You can enter up to 64 characters. Invalid characters are replaced with "!".
15	Keyword	Enter the comments on the contact. You can enter up to 256 characters. Invalid characters are replaced with "!".

Note

- You must specify either the [First Name] or [Last Name] box and either the [Email Address] or [Fax Number] box to register the contact.
- If you enter “-” in the [Fax Number] and [2nd Fax Number], a three-second pause is added for dialing the fax number.
- To perform fax transmission, the Fax Unit is required. If the Fax Unit is not installed, you cannot perform the fax transmission even if you specify the fax number.

❑ [Fax Setting] screen

The screenshot shows the 'Fax Setting' screen. At the top right are 'Save' (1) and 'Cancel' (2) buttons. Below them is a navigation bar with 'Address Book' and 'Create Destination information'. A 'Reset' button (3) is on the left. The main area contains a table with the following fields and callouts: SUB (4), SID (5), SEP (6), PWD (7), ECM (8), Line Select (9), Quality Transmit (10), and Transmission Type (11). The ECM, Line Select, and Quality Transmit fields have dropdown arrows.

	Item name	Description
1	[Save] button	Saves the entered information.
2	[Cancel] button	Cancels the fax settings.
3	[Reset] button	Restores fax settings set for the contact to the default status.
4	SUB	Enter the mailbox number if you want to send a fax to the contact's fax mailbox. You can enter up to 20 characters using numbers, #, and *.
5	SID	Enter the password to send a fax to the contact's fax mailbox. You can enter up to 20 characters using numbers, #, and *.
6	SEP	Enter the mailbox number if you want to retrieve a document from the contact's fax mailbox. You can enter up to 20 characters using numbers, #, and *.
7	PWD	Enter the password to retrieve a document from the contact's fax mailbox. You can enter up to 20 characters using numbers, #, and *.
8	ECM	Select whether to enable or disable ECM (Error Correction Mode). If [ON] is selected, it facilitates error free communications by automatically resending any portion of the document affected by phone line noise or distortion.
9	Line Select	Select whether specifying the line to be used. If this is set to [Auto], this equipment automatically selects the line to be used. However, [Line 2] can be applicable only when the 2nd Line for Fax Unit is installed.
10	Quality Transmit	Select whether to send a document in the Quality TX mode. If [ON] is selected, this equipment sends documents at a slower speed than normal so that the transmission will be less affected by line condition.
11	Transmission Type	Select whether the document will be sent in [Memory Transmit] mode or [Direct Transmit] mode.

❑ [Search Contact] screen

You can search for contacts in the LDAP server and add them to the address book.

Tip

In order to use the LDAP search, the directory service must be set up by a user who has been granted administrator privileges in the access policy mode. Before operating the LDAP search, ask your administrator if the Directory Service has been configured.

The screenshot shows a 'Search Contact' dialog box. It has a title bar 'Contacts' and a close button. Inside, there's a 'Search Contact' section with a 'Search' button (callout 1) and a 'Cancel' button (callout 2). Below these is a text input field (callout 3) with the placeholder 'Enter a partial name or Email address to search for a contact.'. Then, there's a 'Directory Service Name' dropdown menu (callout 4) currently showing 'MFP LOCAL'. Below that are seven text input fields for search criteria: 'First Name' (callout 5), 'Last Name' (callout 6), 'Email Address' (callout 7), 'Fax Number' (callout 8), 'Company' (callout 9), and 'Department'.

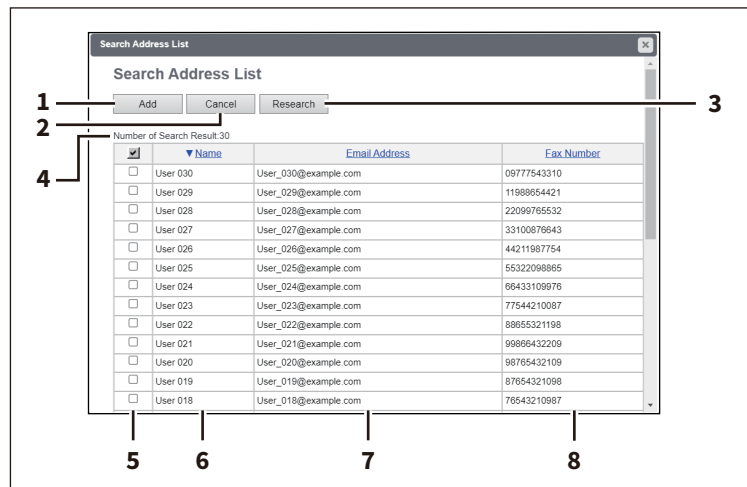
	Item name	Description
1	[Search] button	Searches contacts with the entered conditions. P.51 “[Search Address List] screen”
2	[Cancel] button	Cancels the contact search.
3	Directory Service Name	Select the LDAP server for the search.
4	First Name	Enter the search condition.
5	Last Name	
6	Email Address	
7	Fax Number	
8	Company	
9	Department	

Tip

- If you select [MFP LOCAL] at the [Directory Service Name] box, you can search for destinations in the address book of this equipment.
- TopAccess will search for destinations that contain the text entered in each item.
- Leaving the box blank allows wild-card searching. However, you must specify at least one.

❑ [Search Address List] screen

Select from the search address list and add to the address book.



	Item name	Description
1	[Add] button	Adds the contact selected in the search address list into the address book.
2	[Cancel] button	Cancels the search address list display.
3	[Research] button	Returns to the [Search Contact] screen to change the search criteria and execute the search again.
4	Number of Search Result	Displays the number of found contacts.
5	Check box	Select contacts to be registered to the address book.
6	Name	Displays the search result.
7	Email Address	
8	Fax Number	

❑ [Create Group information]/[Edit Group information] screen

You can create groups that contain multiple recipients.

This enables you to specify a group as the destination when sending an E-mail, Internet Fax, or fax to multiple recipients.

The screenshot shows the 'Create Group Information' dialog box. It includes an 'Address Book' dropdown, 'Reset' and 'Delete' buttons, a 'Required' checkbox, a 'Group Name' text field, a 'Favorite' checkbox, and a 'Destination' dropdown set to 'Local'. Below these is a table of contacts with columns for ID, Email, Fax, Name, Email Address, and Fax Number. The table lists users 026 through 030. Callouts 1-13 point to specific UI elements: 1 (OK button), 2 (Cancel button), 3 (Reset button), 4 (Delete button), 5 (Group Name field), 6 (Destination dropdown), 7 (ID column), 8 (Email column), 9 (Fax column), 10 (Name column), 11 (Email Address column), 12 (Fax Number column), and 13 (Favorite checkbox).

	Item name	Description
1	[OK] button	Registers the selected contacts as a group.
2	[Cancel] button	Cancels the group registration.
3	[Reset] button	Resets the contents.
4	[Delete] button	Deletes the displayed group.
5	Group Name	Enter the group name. You can enter up to 20 characters.
6	Destination	Select Local Address Book or Shared Address Book as the registration target for Group information. Note This is only available when [Shared Setting] > [Shared Address Book] is set to [Enable (Primary)] or [Enable (Secondary)].
7	ID	Displays the registered ID of the contact.
8	Email	Select the check box to register E-mail address into the group when the contact has E-mail information.
9	Fax	Select the check box to register fax number into the group when the contact has fax number information.
10	Name	Displays the last name and first name registered to the contact.
11	Email Address	Displays the E-mail address registered to the contact.
12	Fax Number	Displays the fax number registered to the contact.
13	Favorite	Select to set the group as your favorite.

■ [Inbound FAX routing] Item list

ITU-T communications function between fax devices with ITU-T support and enable fax transmission to and retrieval from mailboxes.

The type of mailboxes for ITU-T communications must be set in advance to either confidential, bulletin board, or forward. You can specify a password on any mailbox to secure confidentiality.

Note

- Mailboxes can be managed only when the Fax Unit is installed.
- The Internet/Fax (Relay) agent cannot be used to forward an inbound fax routed via Inbound FAX Routing.

Tip

Mailboxes can be managed using the touch panel. For details, see the reference below:

Fax - USING THE FAX UNIT (USEFUL FUNCTIONS) - Using the Mailbox Function - Creating, modifying, and deleting a mailbox (mailbox transmission)

□ [Inbound FAX routing] screen

You can manage mailboxes used for ITU-T communications.

To carry out ITU-T communications, you must first set up an Open Mailbox in the mailbox hub. You can set up a maximum of 300 mailboxes.

You can also delete mailboxes.

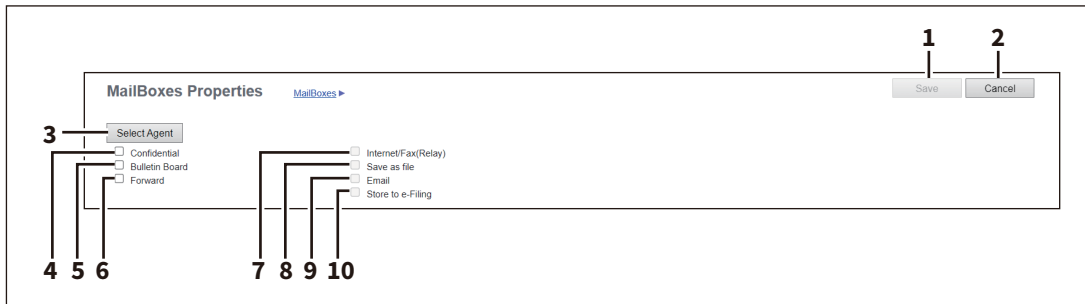
Note

If you want to delete an Open Mailbox, the document must first be retrieved, printed, or canceled from the Open Mailbox.

	Item name	Description
1	[New] button	Creates a mailbox for F-code communications. P.54 "[MailBoxes Properties] screen"
2	Box Number	Displays the registered mailbox number.
3	User Name	Displays the user name of the registered mailbox.
4	Agent	Displays the agent assigned to the mailbox.
5	Comment	Displays the registered comment.

❏ [MailBoxes Properties] screen

You can set a mailbox.



	Item name	Description
1	[Save] button	Saves the mailbox.
2	[Cancel] button	Cancels the mailbox settings.
3	[Select Agent] button	Set the agent to apply to the forward mailbox.
4	Confidential	Creates a confident mailbox. The Confidential Box allows a one-time document retrieval from the mailbox. Once a document is retrieved, it is cleared. If a new document is sent to the same box number where another document is stored, it is added to the existing box. P.55 “MailBox Setting (Mailbox)”
5	Bulletin Board	Creates a bulletin board mailbox. The Bulletin Board Box allows multiple document retrievals from the same mailbox. Once a document is retrieved, it is not cleared. If a new document is sent to the same Box, it replaces the existing one. P.55 “MailBox Setting (Mailbox)”
6	Forward	Creates a multiple transmission relay mailbox. When you select this, select the agent from [Internet/Fax(Relay)], [Save as file], [Email], or [Store to e-Filing]. Use the forward mailbox when you want to forward a fax document to specified destinations automatically.
7	Internet/Fax(Relay)	Creates a multiple transmission relay mailbox for the Internet Fax or fax. This agent can be combined with the Save as file agent or Store to e-Filing agent. P.55 “MailBox Setting (Mailbox)” P.57 “Destination Setting (Mailbox)” P.57 “InternetFax Setting (Mailbox)” P.57 “Relay End Terminal Report (Mailbox)” <div>Note</div> The Internet/Fax (Relay) agent cannot be used to forward an inbound fax routed via Inbound FAX Routing.
8	Save as file	Creates a shared folder forwarding mailbox. This agent can be combined with the Internet/Fax(Relay), Email, or Store to e-Filing agent. P.55 “MailBox Setting (Mailbox)” P.58 “Save as file Setting (Mailbox)”
9	Email	Creates an E-mail forwarding mailbox. This agent can be combined with the Save as file agent or Store to e-Filing agent. P.55 “MailBox Setting (Mailbox)” P.58 “Email Setting (Mailbox)”

	Item name	Description
10	Store to e-Filing	Creates an e-Filing forwarding mailbox. This agent can be combined with the Internet/Fax(Relay) agent, Save as file agent, or Email agent. P.55 "MailBox Setting (Mailbox)" P.58 "Box Setting (Mailbox)"

❑ MailBox Setting (Mailbox)

When you create a new mailbox, the setting page appears after you have set the agent. Click [MailBox Setting] to open the setting window and continue the operation.

Tip


- You can edit or delete the mailbox later.
- You need to enter the password for the operation if you have set it for the mailbox.

In the MailBox Setting page, specify the general information of the mailbox such as the box number, password, owner, comment, and notification.

Note

- The [Notification] and [Document Print] options are not available when creating the Confidential mailbox or Bulletin Board mailbox.
- Mailbox communication is disabled if the settings on this equipment and information registered for the destination do not match. Check how the box number and the fax number of the destination are registered on the journal before entering the box number.

	Item name	Description
1	[Save] button	Saves the settings for the mailbox.
2	[Cancel] button	Cancels the setting operation.

	Item name	Description
3	Box Number	<p>Enter the box number of the mailbox. You can enter up to 20 characters including numbers, sharp marks (#), and asterisks (*). You can also specify the sender's fax number to enable the Inbound Fax routing when registering a Forward mailbox. If you specify the sender's fax number here, the faxes that are received from the specified fax number will be routed according to the mailbox settings.</p> <p>Note</p> <ul style="list-style-type: none"> • The Inbound Fax routing is available only for a Forward mailbox. If you select [Confidential] or [Bulletin Board] as an agent, you cannot specify the fax number. • When a fax is sent from the specified fax number with a box number (or sub address), the Inbound Fax routing will not apply to the transmission and it is processed according to the specified box number (or sub address) settings. <p>Tip</p> <p>If you create a forward mailbox whose number is the fax number of the sender, you can use the TSI function. Using this function, this equipment forwards the original sent from the sender whose fax number is set to the mailbox number, based on the pre-set agent (Save as File / Email / Store to e-Filing).</p>
4	Password	Enter the box password if you want to protect the mailbox by the password. You can enter up to 20 characters including numbers, sharp marks (#), and asterisks (*).
5	User Name	Enter the user name of this mailbox. You can enter up to 30 characters.
6	Comment	Enter the comment. You can enter up to 30 characters.
7	Notification	<p>This specifies how the notification message will be sent if an error occurs.</p> <p>Send Email when an error occurs — Transmits a notification message to the specified E-mail address when an error occurs.</p> <p>Send Email when job is completed — Transmits a notification message to the specified E-mail address when a job is completed.</p> <p>Email Address — Enter the E-mail address for the notification messages. You can enter up to 192 alphanumerical characters.</p> <p>Note</p> <p>When you enable the Notification setting, make sure to set up the E-mail settings in the [Email] submenu of the [Setup] menu in the TopAccess access policy mode.</p> <p> P.192 "Email settings"</p>
8	Document Print	<p>Select whether to print a document sent to this mailbox.</p> <ul style="list-style-type: none"> • Always — Always prints documents sent to this mailbox. • ON ERROR — Prints the document if all specified forwarding has failed.

❑ Destination Setting (Mailbox)

In the Recipient List page, you can specify the destinations of the Internet/Fax (Relay), or Email agent.

When you are setting up the destinations for the Email agent, you can only specify the E-mail addresses for the destinations.

When you are setting up the destinations for the Internet/Fax (Relay) agent, you can specify both fax numbers and E-mail addresses for the destinations.

You can specify the destinations by entering their E-mail addresses or fax numbers manually, selecting recipients from the address book, selecting destination groups from the address book, or searching for destinations in the LDAP server.

Note

The methods of entering the destinations manually and searching for the destinations in the LDAP server are not available if you are setting the destination for the Internet/Fax (Relay) agent.

Operations are the same as the following procedure.

📖 P.307 “Destination Setting”

❑ InternetFax Setting (Mailbox)

In the InternetFax Setting page, you can specify the content of the Internet Fax to be sent.

Operations are the same as the following procedure.

📖 P.312 “InternetFax Setting”

❑ Relay End Terminal Report (Mailbox)

On the Relay End Terminal Report page, you can specify a destination to which the transmission result list will be sent.

The screenshot shows the 'Relay End Terminal Report' page. It includes a title bar, a 'Relay End Terminal Report' header, and two buttons: 'Add' (labeled 1) and 'Cancel' (labeled 2). Below these are links for 'Address Book' and 'Favorite Address Book'. A 'Reset' button is labeled 3. A 'Destination' input field is labeled 4. A 'Fax Type' dropdown menu is labeled 5 and currently shows 'G3 Fax'. At the bottom, a table of recipients is labeled 6. The table has columns for Email, Fax, ID, Name, Email Address, Favorite, Fax Number, and another Favorite column. It lists 16 users with their respective IDs, names, email addresses, and fax numbers.

Email	Fax	ID	Name	Email Address	Favorite	Fax Number	Favorite
<input type="radio"/>	<input type="radio"/>	0030	User 030	User_030@example.com		09777543310	
<input type="radio"/>	<input type="radio"/>	0029	User 029	User_029@example.com		11988654421	
<input type="radio"/>	<input type="radio"/>	0028	User 028	User_028@example.com		22099765532	
<input type="radio"/>	<input type="radio"/>	0027	User 027	User_027@example.com		33100876643	
<input type="radio"/>	<input type="radio"/>	0026	User 026	User_026@example.com		44211987754	
<input type="radio"/>	<input type="radio"/>	0025	User 025	User_025@example.com		55322088865	
<input type="radio"/>	<input type="radio"/>	0024	User 024	User_024@example.com		66433109976	
<input type="radio"/>	<input type="radio"/>	0023	User 023	User_023@example.com		77544210087	
<input type="radio"/>	<input type="radio"/>	0022	User 022	User_022@example.com		88655321198	
<input type="radio"/>	<input type="radio"/>	0021	User 021	User_021@example.com		99886432209	
<input type="radio"/>	<input type="radio"/>	0020	User 020	User_020@example.com		98765432109	

	Item name	Description
1	[Add] button	Adds settings to transmit the relay end terminal report.
2	[Cancel] button	Cancels the settings.
3	[Reset] button	Resets the settings.
4	Destination	Enter the E-mail address or fax number of the recipient.
5	Fax Type	When the fax number is entered, select [G3 Fax] in the [Fax Type] box. When the E-mail address is entered, select [InternetFax] in the [Fax Type] box.
6	Recipient list	Displays the registered destinations. Select the E-mail address or fax number of the destination.

Note


You cannot specify more than 1 destination for the destination of the Relay End Terminal Report.

Save as file Setting (Mailbox)

In the Save as file Setting page, you can specify how and where a received fax will be stored.

Instructions on how to do the Save as file setting for the mailbox are the same as for the Save as file setting for a template.

Operations are the same as the following procedure.

 P.319 “Save as file Setting”

Note


You cannot specify USB media as the storage in the Save as file Setting Page.

Email Setting (Mailbox)

In the Email Settings page, you can specify the content of E-mail document to be sent.

Instructions on how to do the E-mail setting for the mailbox are the same as for the E-mail setting for a template.


Operations are the same as the following procedure.

 P.316 “Email Setting”

Box Setting (Mailbox)

In the Box Setting page, you can specify how a received fax will be stored in the Box.

Operations are the same as the following procedure.

 P.324 “Box Setting”

[Counter]

[Counter] Overview	60
[Counter] Item list	60

[Counter] Overview

You can check the number of pages printed, copied, and scanned on the [Counter] page.

■ [Counter] Item list

□ [Total Counter] screen

You can display total counters of the print counter and scan counter, and total counters for small size and large size paper.

Note

- Neither an end user nor an administrator can reset counters from TopAccess. However, users who are granted administrator privileges in the access policy mode can reset the counter from the touch panel. For details, see the reference below:
User Functions - MANAGING COUNTERS (COUNTER MENU) - Department Management
- Because of paper jam and job cancellation, the total counter value might not be equal to the total number of pages in the print log.
- The total counter value might not be equal to the total number of pages in the print log, depending on the operating system you use.
- The total counter value might not be equal to the total values of other counters, depending on the counter settings.

Color models

Print Counter				
Total Counter				
	Full Color	Twin/ Mono Color	Black	Total
Copy	9	0	54	63
Fax	0	0	0	0
Printer	1436	0	785	2221
List	0	0	50	50
Total	1445	0	889	2334

2 → Detail

Total Counter				
	Full Color	Twin/ Mono Color	Black	Total
Copy	9	0	54	63
Fax	0	0	2	2
Network	138	0	123	261
Total	147	0	179	326

4 → Detail

	Small	Large	Total
Copy	59	2	61
Fax	0	0	0
Printer	959	621	1580
List	50	0	50
Total	1068	623	1691

6 OCR Counter

Total
48

Monochromatic models

The diagram illustrates the layout of the Monochromatic models counter interface. It features six numbered callouts pointing to specific components:

- 1** Print Counter: Points to the 'Print Counter' section, which includes a 'Total Counter' table.
- 2** Detail: Points to a blue right-pointing triangle icon used to expand details.
- 3** Scan Counter: Points to the 'Scan Counter' section, which includes a 'Total Counter' table.
- 4** Detail: Points to a blue right-pointing triangle icon used to expand details.
- 5** Sheet Counter: Points to the 'Sheet Counter' section, which includes a table showing counts for Small and Large paper sizes.
- 6** OCR Counter: Points to the 'OCR Counter' section, which includes a 'Total' display showing the value 0.

Print Counter Total Counter

	Black	Total
Copy	53	53
Fax	6	6
Printer	50	50
List	8	8
Total	117	117

Scan Counter Total Counter



	Full Color	Black	Total
Copy	0	8	8
Fax	0	28	28
Network	16	14	30
Total	16	50	66

Sheet Counter

	Small	Large	Total
Copy	53	0	53
Fax	6	0	6
Printer	49	0	49
List	8	0	8
Total	0	0	0

OCR Counter

Total
0

	Counter type	Description
1	Print Counter	Displays the total output count value.
2	Detail	Displays details of the total output count value when you click  .
3	Scan Counter	Displays the total scanned count value.
4	Detail	Displays details of the total count value of scanned documents when you click  .
5	Sheet Counter	Displays the number of printed sheets according to the function being used. Values are displayed according to the paper size set on your equipment. This counter increments by 1 for either single or dual-sided copying.
6	OCR Counter	Displays the number of images to which an OCR process has been performed.

Print Counter/Print Counter (Detail)

1	▼ Detail				
	Copy Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	9	0	52	61
	Large	0	0	2	2
2	Fax Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	0	0	0	0
	Large	0	0	0	0
	Total	0	0	0	0
3	Printer Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	623	0	553	1176
	Large	813	0	232	1045
	Total	1436	0	785	2221
4	List Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	0	0	50	50
	Large	0	0	0	0
	Total	0	0	50	50

	Counter	Description
1	Copy Counter	Displays the number of pages printed by copy operations for paper sizes set on your equipment.
2	Fax Counter	Displays the number of pages printed by fax reception for paper sizes set on your equipment.
3	Printer Counter	Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment.
4	List Counter	Displays the number of pages printed by system page print operations for paper sizes set on your equipment.

Scan Counter/Scan Counter (Detail)

1	▼ Detail				
	Copy Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	9	0	52	61
	Large	0	0	2	2
2	Fax Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	0	0	0	0
	Large	0	0	2	2
	Total	0	0	2	2
3	Network Counter				
		Full Color	Twin/ Mono Color	Black	Total
	Small	131	0	55	186
	Large	7	0	68	75
	Total	138	0	123	261

	Counter	Description
1	Copy Counter	Displays the number of pages printed by copy operations for paper sizes set on your equipment.
2	Fax Counter	Displays the number of pages printed by fax reception for paper sizes set on your equipment.
3	Network Counter	Displays the number of pages scanned by scan operations for paper sizes set on your equipment.

❑ [Department Counter] screen

Displays 20 items of total counter information for each department per page.

1

Department Counter

Enter a department code to access department counters

Department Code Enter

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	123456	0	0	0	0

2 3 4 5 6 7 8

	Item name	Description
1	Department Code	Enter the department code which you want to check and click the [Enter] button.
2	Number	Displays the registered department number.
3	Department Name	Displays the department name. Click a department name link to check the information. P.64 "[Department Information] screen"
4	Dept Code	Displays the department code.
5	Total Printing	Displays the total output count value of the department.
6	Total Scanning	Displays the total scanned count value of the department.
7	Fax Transmission	Displays the total number of transmitted fax pages of the department.
8	Fax Reception	Displays the total number of received fax pages of the department.

❑ [Department Counter] screen <access policy mode>

1

Department Counter

<< Previous Page < 1 > Next Page >> All

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	123456	0	0	0	0
2	Dept02	123	0	0	0	0
1001	Undefined	00000	2321	324	0	0

2 3 4 5 6 7 8

	Item name	Description
1	Select Page	Allows you to select a page when there are 101 items or more. Click [All] to show all department counters on a page.
2	Number	Displays the registered department number.
3	Department Name	Displays the department name. Click a department name link to check the information. P.64 "[Department Information] screen"
4	Dept Code	Displays the department code.
5	Total Printing	Displays the total output count value of the department.
6	Total Scanning	Displays the total scanned count value of the department.
7	Fax Transmission	Displays the number of pages transmitted via fax.
8	Fax Reception	Displays the number of pages received via fax.

❑ [Department Information] screen

Color models

The screenshot shows the 'Department Information' window. Callout 1 points to the window title bar. Callout 2 points to the 'Department Number' field. Callout 3 points to the 'Department Name' field. Callout 4 points to the 'Department Code' field. Callout 5 points to the 'Color Quota Setting' field. Callout 6 points to the 'Print Counter' section. Callout 7 points to the 'Detail' link for the Print Counter. Callout 8 points to the 'Scan Counter' section. Callout 9 points to the 'Detail' link for the Scan Counter. Callout 10 points to the 'Fax Communication Counter' section. Callout 11 points to the 'Sheet Counter' section. Callout 12 points to the 'OCR Counter' section.

Department Information

Close

2 Department Number 1

3 Department Name Dept01

4 Department Code 123456

5 Color Quota Setting ON

Color Quota 10000

Default Color Quota 0

5 Black Quota Setting ON

Black Quota 50000

Default Black Quota 0

6 **Print Counter**

Total Counter

	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Printer	0	0	0	0
List	0	0	0	0
Total	0	0	0	0

7 [Detail](#)

8 **Scan Counter**

Total Counter

	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Network	0	0	0	0
Total	0	0	0	0

9 [Detail](#)

10 **Fax Communication Counter**

	Small	Large	Total
Transmit	0	0	0
Received	0	0	0
Total	0	0	0

11 **Sheet Counter**

	Small	Large	Total
Copy	0	0	0
Fax	0	0	0
Printer	0	0	0
List	0	0	0
Total	0	0	0

12 **OCR Counter**

Total
0

Monochromatic models



The screenshot shows a 'Department Information' window. On the left, a vertical list of numbered callouts (1-12) points to specific UI elements. The window itself has a title bar with a 'Close' button (callout 1). The main content area displays the following information:

- Department Information** (Section Header)
- Department Number: 1 (callout 2)
- Department Name: DepName001 (callout 3)
- Department Code: 12345 (callout 4)
- Quota Setting: ON (callout 5)
- Quota: 10000
- Default Quota: 0
- Print Counter** (callout 6): A table showing counts for Copy, Fax, Printer, List, and Total across Black and Total columns.
- Detail** (callout 7): A link to view details.
- Scan Counter** (callout 8): A table showing counts for Copy, Fax, Network, and Total across Full Color, Black, and Total columns.
- Detail** (callout 9): A link to view details.
- Fax Communication Counter** (callout 10): A table showing counts for Transmit, Received, and Total across Small, Large, and Total columns.
- Sheet Counter** (callout 11): A table showing counts for Copy, Fax, Printer, List, and Total across Small, Large, and Total columns.
- OCR Counter** (callout 12): A table showing a Total count of 0.

6

[Counter]

	Item name	Description
1	[Close] button	Closes the [Department Information] screen.
2	Department Number	Displays the registered department number.
3	Department Name	Displays the department name.
4	Department Code	Displays the department code.
5	Quota Setting	<ul style="list-style-type: none"> • OFF — No output restriction. • ON — Restricts output.
	Quota	Displays the remaining number for output.
	Default Quota	Displays the default number assigned for the user.
6	Print Counter	Displays the output total count value.

	Item name	Description
7	Detail	<p>Displays details of the total output count value when you click .</p> <p>Copy Counter: Displays the number of pages printed by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages printed by fax reception for paper sizes set on your equipment.</p> <p>Printer Counter: Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment.</p> <p>List Counter: Displays the number of pages printed by system page print operations for paper sizes set on your equipment.</p>
8	Scan Counter	Displays the total count value of scanned documents.
9	Detail	<p>Displays details of the total count value of scanned documents when you click .</p> <p>Copy Counter: Displays the number of pages scanned by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages scanned by fax reception for paper sizes set on your equipment.</p> <p>Network Counter: Displays the number of pages scanned by scan operations for paper sizes set on your equipment.</p>
10	Fax Communication Counter	Displays the communication record.
11	Sheet Counter	Displays the number of printed sheets according to the function being used. Values are displayed according to the paper size set on your equipment. This counter increments by 1 for either single or dual-sided copying.
12	OCR Counter	Displays the number of images to which an OCR process has been performed.

❑ [User Counter] screen <access policy mode>

This screen displays total counter information for each user who is logged in to TopAccess.

Tip

Total counters for all users are displayed when you are logged in as the Administrator.

The screenshot shows the 'User Counter' screen. A callout '1' points to the 'Number 28/28' text at the top left. Below the title bar is a table with columns: Number, User Name, Domain Name/LDAP Server, Total Printing, Total Scanning, Fax Transmission, and Fax Reception. The table contains three rows of data. Callouts 2 through 8 point to the following table elements: 2 points to the 'Number' column header, 3 points to the 'User Name' column header, 4 points to the 'Domain Name/LDAP Server' column header, 5 points to the 'Total Printing' column header, 6 points to the 'Total Scanning' column header, 7 points to the 'Fax Transmission' column header, and 8 points to the 'Fax Reception' column header.

Number	User Name	Domain Name/LDAP Server	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1			126	74	0	0
2			308	65	0	0
3			2	4	0	0

	Item name	Description
1	Select Page	Allows you to select a page when there are 20 items or more.
2	Number	Displays the registered user number.
3	User Name	Displays the user name. Click a user name to check the information. 📖 P.68 “[User Information] screen <access policy mode>”
4	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account.
5	Total Printing	Displays the total output count value.
6	Total Scanning	Displays the total scanned count value.
7	Fax Transmission	Displays the number of pages transmitted via fax.
8	Fax Reception	Displays the number of pages received via fax.

❑ [User Information] screen <access policy mode>

Color models

1

User Information
REFRESH
Close

2 User Name

3 Domain Name/LDAP Server

4 Authentication Method

5 Password :

6 Role Assignment

7 Group Assignment

8 Department Number

9 PanelUI Language

10 PanelUI Keyboard Layout

11 Color Quota Setting

11 Black Quota Setting

User001

MFP Local Authentication

User

English(US)

QWERTY

ON

100

100

ON

500

500

12 Print Counter

Total Counter	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Printer	0	0	0	0
List	0	0	0	0
Total	0	0	0	0

13 ▶ Detail

14 Scan Counter

Total Counter	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Network	0	0	0	0
Total	0	0	0	0

15 ▶ Detail

16 Fax Communication Counter

	Small	Large	Total
Transmit	0	0	0
Received	0	0	0
Total	0	0	0

17 Sheet Counter

	Small	Large	Total
Copy	0	0	0
Fax	0	0	0
Printer	0	0	0
List	0	0	0
Total	0	0	0

18 OCR Counter

Total	0
-------	---

Monochromatic models

12

Print Counter

Total Counter

	Black	Total
Copy	0	0
Fax	0	0
Printer	0	0
List	0	0
Total	0	0

13

Detail

14

Scan Counter

Total Counter

	Full Color	Black	Total
Copy	0	0	0
Fax	0	0	0
Network	0	0	0
Total	0	0	0

15

Detail

16

Fax Communication Counter

	Small	Large	Total
Transmit	0	0	0
Received	0	0	0
Total	0	0	0

17

Sheet Counter



	Small	Large	Total
Copy	0	0	0
Fax	0	0	0
Printer	0	0	0
List	0	0	0
Total	0	0	0

18

OCR Counter

Total	0
-------	---

	Item name	Description
1	[Close] button	Closes the [User Information] screen.
2	User Name	Displays the user name.
3	Domain Name/LDAP Server	Displays the registered domain name or LDAP server.
4	Authentication Method	Displays the user authentication method.
5	Password	You cannot display the password. Reset the password in the [User Accounts] item when changing the password. P.77 "[Enter Password] screen"
6	Role Assignment	Displays the registered roles.
7	Group Assignment	Displays the registered groups.
8	Department Number	Displays the registered departments.
9	PanelUI Language	Displays the registered display languages of the touch panel.
10	PanelUI Keyboard Layout	Displays the registered keyboard patterns for the touch panel.
11	Quota Setting	<ul style="list-style-type: none"> OFF — No output restriction. ON — Restricts output.
	Quota	Displays the remaining number for output.
	Default Quota	Displays the default number assigned for the user.
12	Print Counter	Displays the output total count value.

	Item name	Description
13	Detail	<p>Displays details of the total output count value when you click .</p> <p>Copy Counter: Displays the number of pages printed by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages printed by fax reception for paper sizes set on your equipment.</p> <p>Printer Counter: Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment.</p> <p>List Counter: Displays the number of pages printed by system page print operations for paper sizes set on your equipment.</p>
14	Scan Counter	Displays the total count value of scanned documents.
15	Detail	<p>Displays details of the total count value of scanned documents when you click .</p> <p>Copy Counter: Displays the number of pages scanned by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages scanned by fax reception for paper sizes set on your equipment.</p> <p>Network Counter: Displays the number of pages scanned by scan operations for paper sizes set on your equipment.</p>
16	Fax Communication Counter	Displays the communication record.
17	Sheet Counter	Displays the number of printed sheets according to the function being used. Values are displayed according to the paper size set on your equipment. This counter increments by 1 for either single or dual-sided copying.
18	OCR Counter	Displays the number of images to which an OCR process has been performed.

❑ [Quota Setting] screen <access policy mode>

You can make the quota management settings based on either a print count or a job. In job-based quota management, different weights can be assigned to each job when the number of outputs is counted.

	Item name	Description
1	[Save] button	Saves the quota settings.
2	[Cancel] button	Cancels the settings.
3	Black/Color Quota	Performs quota management based on the number of black and color outputs.
	<div>Tip</div> [Black Quota] is displayed in monochrome models, which performs quota management with the number of black outputs.	
4	Job Quota	Assigns weights to each job and calculates the sum total quotas of the print jobs and scan jobs for quota management. Different weights can be assigned to each of the jobs listed below. <ul style="list-style-type: none"> • Print <ul style="list-style-type: none"> - Small Full Color - Large Full Color - Small Twin/Mono Color - Large Twin/Mono Color - Small Black - Large Black • Scan <ul style="list-style-type: none"> - Color - Black • Quota Near Empty Limitation <ul style="list-style-type: none"> Sets the threshold to give notice of nearly reaching the quota. <div>Tip</div> <ul style="list-style-type: none"> • In monochrome models, only the weight assigned to Small Black or Large Black can be changed. • When assigning the weight to a job, you can enter a value in the range from 0.00 to 99.99. The default value of the print is “1.00” and that of the scan is “0.00”. For example, assuming that the weight assigned to Small Black in print is 0.50, if the user makes 2 outputs in Small Black, the quota value assigned to the user is decremented by 1.00.

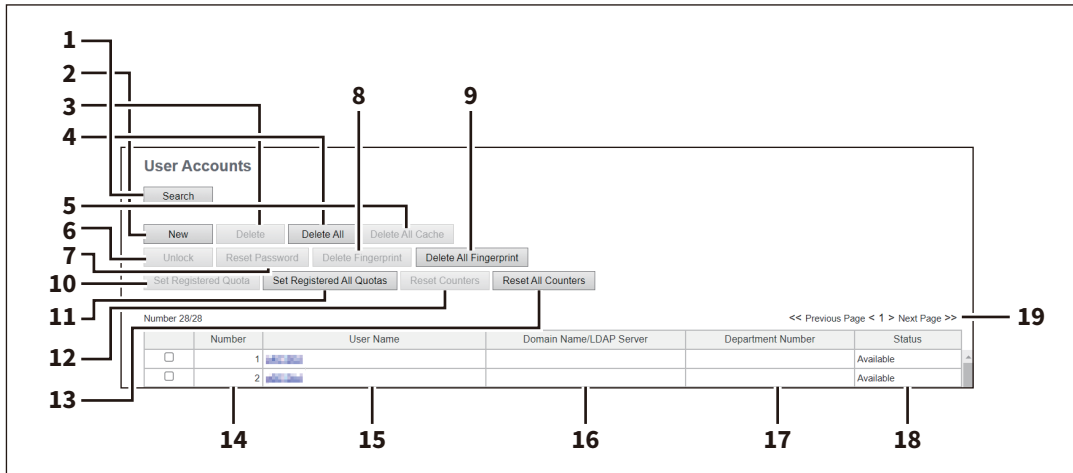
[User Management]

[User Management] Overview	74
[User Accounts] Item list <access policy mode>	74
[Group Management] Item list <access policy mode>	82
[Role Management] Item list <access policy mode>	84
[Department Management] Item list <access policy mode>	90
[Project Management] Item list <access policy mode>	94
[Export/Import] Item list <access policy mode>	95
[Shared Settings] Item list <access policy mode>	97

[User Management] Overview

■ [User Accounts] Item list <access policy mode>

You can search and set user accounts if you are logged in to the access policy mode.



	Item name	Description
1	[Search] button	Searches registered users. 📖 P.75 “[Search User Account] screen”
2	[New] button	Registers new users. 📖 P.75 “[Create User Information] screen”
3	[Delete] button	Deletes the user selected in the user account list. However, you cannot delete the default users.
4	[Delete All] button	Deletes all registered users. (Except default users)
5	[Delete All Cache] button	Select this to delete all the authentication information to be used when an authentication server failure occurs.
6	[Unlock] button	Unlocks a locked user selected in the user account list.
7	[Reset Password] button	Resets the password of the user selected in the user account list. 📖 P.77 “[Enter Password] screen”
8	[Delete Fingerprint] button	Contact your service technician for details.
9	[Delete All Fingerprint] button	Contact your service technician for details.
10	[Set Registered Quota] button	Initializes the registered quota for the user selected in the user account list.
11	[Set Registered All Quotas] button	Initializes quotas for all users.
12	[Reset Counters] button	Resets counters for the user selected in the user account list.
13	[Reset All Counters] button	Resets counters for all departments.
14	Number	Displays the registration number of the user. 10001 to 10009 are assigned to default users.
15	User Name	Displays the user name. Undefined, Admin, Service, Auditor, Faxope, Guest, Printope, Remote-access-service, and IdleScreenPrint are default users. You can check the user information by clicking the user name. 📖 P.78 “[Edit User Information] screen”
16	Domain Name/LDAP Server	Displays the domain name or LDAP server registered in the user information.
17	Department Number	Displays the department number registered in the user information.
18	Status	Displays the user status.
19	Select Page	Allows you to select a page when there are 101 items or more.

[Search User Account] screen

You can search registered users.
Select items to be searched and enter or select the search conditions.

Search User Account

1

☐ Number

StartEnd

2

☐ Department Number

0001 Dept01

3

☐ User Name

4

☐ Domain Name/LDAP Server

5

Search

	Item name	Description
1	Number	Enter the user number you want to search. The search condition should be in the range from 1 to 10000.
2	Department Number	Select the department number you want to search.
3	User Name	Enter the user name you want to search. A prefix search is performed with the entered character string.
4	Domain Name/LDAP Server	Enter the domain name or LDAP server you want to search.
5	[Search] button	Searches contacts with the entered and selected conditions.

[Create User Information] screen

You can register new user information.

1

2

Create User Information

3

*Required

4

User Name

5

☐ Local User which is available in Windows Domain Authentication/LDAP Authentication

Domain Name/LDAP Server

6

Authentication Method

MFP Local Authentication

7

Password

8

PIN Code

9

Card Information

10

Role Assignment

Edit

11

Group Assignment

Edit

12

Email Address

Address Book

13

Home Directory

14

Department Number

15

Panel/UI Language

English(GB)

16

Panel/UI Keyboard Display

ON

17

Panel/UI Keyboard Layout

QWERTY

18

Color Quota Setting

OFF

Color Quota

Default Color Quota

18

Black Quota Setting

OFF

Black Quota

Default Black Quota

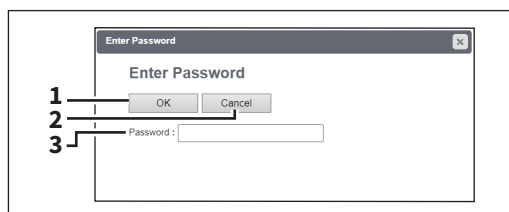
	Item name	Description
1	[Save] button	Saves the entered user information.

	Item name	Description
2	[Cancel] button	Cancels creating user information.
3	User Name	Enter the user name. You can enter up to 128 alphanumerical characters and symbols (except the following: " * + , / : ; < = > ? [\] space).
4	Local User which is available in Windows Domain Authentication/LDAP Authentication	Select this to register as a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication. Tip The above setting is available only when the [Local User which is available in Windows Domain Authentication/LDAP Authentication] checkbox is selected. P.248 "Windows Domain Authentication" P.251 "LDAP Authentication"
5	Domain Name/LDAP Server	Select the domain name or LDAP server.
6	Authentication Method	Select the user authentication method. <ul style="list-style-type: none"> • MFP Local Authentication — Use MFP local authentication on your equipment. • Windows Domain Authentication — Use network authentication managed by the Windows domain. • LDAP Authentication — Use network authentication managed by LDAP.
7	Password	Enter the password. You can enter up to 64 alphanumerical characters and symbols (! # () * + , - . / : ; = ? @ \$ ^ _ ` { } ~ \ space).
8	PIN Code	Enter the PIN code for the user authentication. Note <ul style="list-style-type: none"> • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. P.240 "Setting up User Authentication Setting" • If you change any settings, the changes will be reflected from the next time you log in. • When you use the PIN code for the Windows domain authentication or LDAP authentication, the unique PIN code should be assigned for all users.
9	Card Information	Enter the information necessary for card authentication.
10	Role Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Select from the registered roles. Click the [Edit] button and select roles from the displayed screen. P.81 "[Role Assignment] screen"
11	Group Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Select from the registered groups. Click the [Edit] button and select groups from the displayed screen. P.82 "[Group Assignment] screen"
12	Email Address	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the Email address of the user or select it from the address book. You can enter up to 192 half-width alphanumerical characters and symbols.

	Item name	Description
13	Home Directory	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the network path to the home directory. You can enter up to 128 half-width alphanumerical characters and symbols. For example, enter “\\192.168.1.1\\users\\name” to specify the folder called “users\\name” on the computer whose server address is “192.168.1.1”.
14	Department Number	Select from the registered departments. P.90 “[Department Management] Item list <access policy mode>”
15	PanelUI Language	Select the display language for the touch panel.
16	PanelUI Keyboard Display	Select whether to display the soft-keyboard when entering characters with the touch panel.
17	PanelUI Keyboard Layout	Select the keyboard pattern displayed on the touch panel.
18	Quota Setting	Select this to perform the quota setting of the department according to the setting specified at [Quota Setting] on the [Counter] page. <ul style="list-style-type: none"> • OFF — Not performed • ON — Performed P.71 “[Quota Setting] screen <access policy mode>”
	Quota	Displays the quota amount. This value decreases according to the weight set at [Quota Setting] on the [Counter] page, and output is restricted when the value becomes 0.00. The quota can be manually modified to any amount.
	Default Quota	Enter the default amount to assign to the department. When [Black/Color Quota] or [Black Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999. When [Job Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999.99.

❑ [Enter Password] screen

You can display the [Enter Password] screen by selecting the check box of the user whose password you want to change in the [User Accounts] item list and clicking the [Reset Password] button.



	Item name	Description
1	[OK] button	Saves the entered password.
2	[Cancel] button	Cancels the password change.
3	Password	Enter the new password.

❑ [Edit User Information] screen

You can update registered user information.

Edit User Information

1 Save 2 Cancel

3 Reset Counters 4 Delete

*Required
*User Name User001

☐ Local User which is available in Windows Domain Authentication/LDAP Authentication

Domain Name/LDAP Server

Authentication Method MFP Local Authentication

9 Password

10 PIN Code

11 Card Information

12 Role Assignment User Edit

13 Group Assignment Edit

14 Email Address Address Book

15 Home Directory

16 Department Number

17 PanelUI Language English(US)

18 PanelUI Keyboard Display ON

19 PanelUI Keyboard Layout QWERTY

20 Color Quota Setting
Color Quota 100
Default Color Quota 100

20 Black Quota Setting
Black Quota 500
Default Black Quota 500

21 Print Counter
Total Counter

	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Printer	0	0	0	0
List	0	0	0	0
Total	0	0	0	0

22 Detail

23 Scan Counter
Total Counter

	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Network	0	0	0	0
Total	0	0	0	0

24 Detail

25 Fax Communication Counter

	Small	Large	Total
Transmit	0	0	0
Received	0	0	0
Total	0	0	0





26 Sheet Counter

	Small	Large	Total
Copy	0	0	0
Fax	0	0	0
Printer	0	0	0
List	0	0	0
Total	0	0	0

27 OCR Counter
Total 0

	Item name	Description
1	[Save] button	Saves the entered user information.
2	[Cancel] button	Cancels changing user information.
3	[Reset Counters] button	Resets counters.
4	[Delete] button	Deletes the displayed user from the user account.

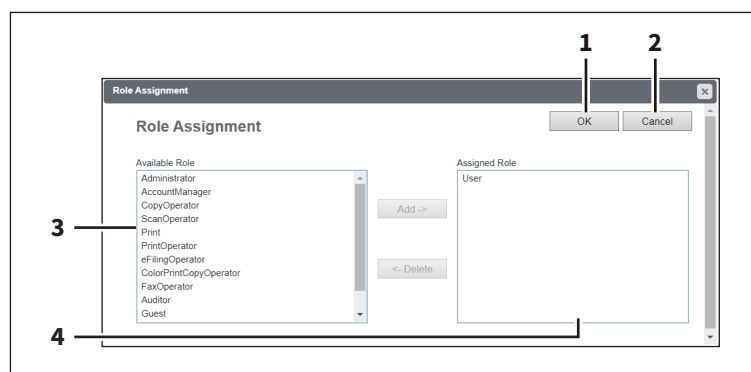
	Item name	Description
5	User Name	<p>Displays the user name.</p> <p>Note</p> <p>If you change any settings, the changes will be reflected from the next time you log in.</p>
6	Local User which is available in Windows Domain Authentication/LDAP Authentication	<p>Select this to register as a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.</p> <p>Note</p> <p>The above setting is available only when the [Local User which is available in Windows Domain Authentication/LDAP Authentication] checkbox is selected.</p> <p>📖 P.248 “Windows Domain Authentication”</p> <p>📖 P.251 “LDAP Authentication”</p>
7	Domain Name/LDAP Server	<p>Displays the registered domain name or LDAP server. Select this item if you want to change.</p> <p>You can select this item only when the authentication method is [Windows Domain Authentication] or [LDAP Authentication].</p>
8	Authentication Method	<p>Displays the user authentication method.</p> <ul style="list-style-type: none"> • MFP Local Authentication — Use MFP local authentication on your equipment. • Windows Domain Authentication — Use network authentication managed by the Windows domain. • LDAP Authentication — Use network authentication managed by LDAP.
9	Password	<p>You can change the password only when the authentication method is [MFP Local Authentication].</p> <p>Note</p> <p>If you change any settings, the changes will be reflected from the next time you log in.</p>
10	PIN Code	<p>Displays the PIN code for the user authentication. You can set this item only when the authentication method is [MFP Local Authentication].</p> <p>Note</p> <ul style="list-style-type: none"> • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. • If you change any settings, the changes will be reflected from the next time you log in. • When you use the PIN code for the Windows domain authentication or LDAP authentication, the unique PIN code should be assigned for all users. <p>📖 P.240 “Setting up User Authentication Setting”</p>
11	Card Information	<p>Enter the information necessary for card authentication.</p>
12	Role Assignment	<p>This can be configured when [MFP Local Authentication] is selected in [Authentication Method].</p> <p>Displays the registered roles. Click the [Edit] button and select roles from the displayed screen.</p> <p>📖 P.81 “[Role Assignment] screen”</p> <p>Note</p> <p>If you change any settings, the changes will be reflected from the next time you log in.</p>

	Item name	Description
13	Group Assignment	<p>This can be configured when [MFP Local Authentication] is selected in [Authentication Method].</p> <p>Displays the registered groups. Click the [Edit] button and select groups from the displayed screen.</p> <p> P.82 “[Group Assignment] screen”</p> <p>Note</p> <p>If you change any settings, the changes will be reflected from the next time you log in.</p>
14	Email Address	<p>This can be configured when [MFP Local Authentication] is selected in [Authentication Method].</p> <p>Enter the Email address of the user or select it from the address book. You can enter up to 192 half-width alphanumerical characters and symbols.</p>
15	Home Directory	<p>This can be configured when [MFP Local Authentication] is selected in [Authentication Method].</p> <p>Enter the network path to the home directory. You can enter up to 128 half-width alphanumerical characters and symbols.</p> <p>For example, enter “\192.168.1.1\users\name” to specify the folder called “users\name” on the computer whose server address is “192.168.1.1”.</p>
16	Department Number	<p>Displays the registered departments. Select this item if you want to change.</p> <p> P.90 “[Department Management] Item list <access policy mode>”</p>
17	PanelUI Language	Displays the registered display languages of the touch panel. Select this item if you want to change.
18	PanelUI Keyboard Display	Select whether to display the soft-keyboard when entering characters with the touch panel.
19	PanelUI Keyboard Layout	Displays the registered keyboard patterns for the touch panel. Select this item if you want to change.
20	Quota Setting	<p>Select this to perform the quota setting of the department according to the setting specified at [Quota Setting] on the [Counter] page.</p> <ul style="list-style-type: none"> • OFF — Not performed • ON — Performed <p> P.71 “[Quota Setting] screen <access policy mode>”</p>
	Quota	Displays the quota amount. This value decreases according to the weight set at [Quota Setting] on the [Counter] page, and output is restricted when the value becomes 0.00. The quota can be manually modified to any amount.
	Default Quota	<p>Enter the default amount to assign to the department.</p> <p>When [Black/Color Quota] or [Black Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999. When [Job Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999.99.</p>
21	Print Counter	Displays the output total count value.
22	Detail	<p>Displays details of the total output count value when you click .</p> <p>Copy Counter: Displays the number of pages printed by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages printed by fax reception for paper sizes set on your equipment.</p> <p>Printer Counter: Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment.</p> <p>List Counter: Displays the number of pages printed by system page print operations for paper sizes set on your equipment.</p>
23	Scan Counter	Displays the total count value of scanned documents.

	Item name	Description
24	Detail	Displays details of the total count value of scanned documents when you click [▶]. Copy Counter: Displays the number of pages scanned by copy operations for paper sizes set on your equipment. Fax Counter: Displays the number of pages scanned by fax reception for paper sizes set on your equipment. Network Counter: Displays the number of pages scanned by scan operations for paper sizes set on your equipment.
25	Fax Communication Counter	Displays the communication record.
26	Sheet Counter	Displays the number of printed sheets according to the function being used. Values for the small size and large size are displayed according to the paper size specified on your equipment. This counter increments by 1 for either single or dual-sided copying.
27	OCR Counter	Displays the number of images to which an OCR process has been performed.

❑ [Role Assignment] screen

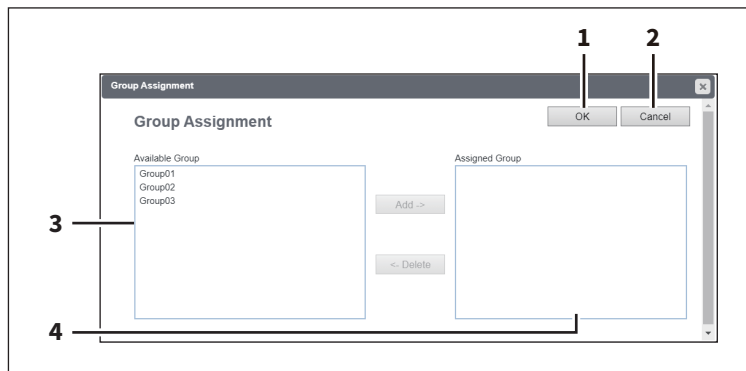
You can select roles to be assigned.



	Item name	Description
1	[OK] button	Saves the assigned roles.
2	[Cancel] button	Cancels assigning roles.
3	Available Role	Displays a list of registered roles. Select the role to be assigned and click the [Add] button.
4	Assigned Role	Displays a list of the assigned roles. Select the role to be removed from the assignment and click the [Delete] button.

❑ [Group Assignment] screen

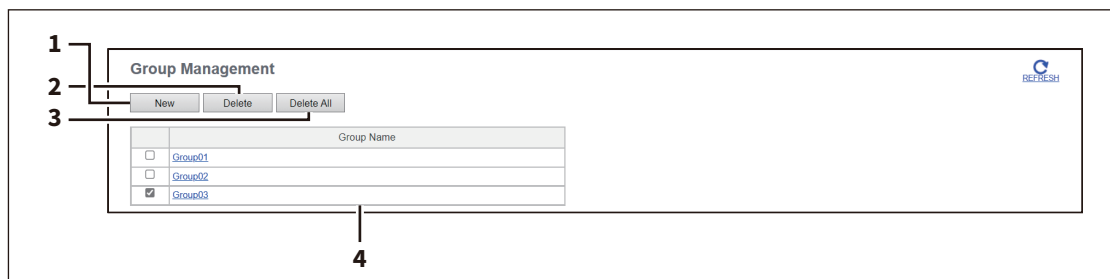
You can select groups to be assigned.



	Item name	Description
1	[OK] button	Saves the assigned groups.
2	[Cancel] button	Cancels assigning groups.
3	Available Group	Displays a list of registered groups. Select the group to be assigned and click the [Add] button.
4	Assigned Group	Displays a list of the assigned groups. Select the group to be removed from the assignment and click the [Delete] button.

■ [Group Management] Item list <access policy mode>

You can manage the registered roles as groups if you are logged in to the access policy mode.



	Item name	Description
1	[New] button	Allows you to add a new group. 📖 P.83 “[Create Group Information] screen”
2	[Delete] button	Deletes the group selected in the group list.
3	[Delete All] button	Deletes all groups.
4	Group Name	Displays the group name. You check group information by clicking the group name. 📖 P.83 “[Edit Group Information] screen”

[Create Group Information] screen

You can register new groups.

The screenshot shows the 'Create Group Information' screen. At the top, there's a title bar 'Group Information' with a close button. Below it are 'Save' and 'Cancel' buttons. The main content area has a form with two input fields: 'Group Name' (with a '*'Required label) and 'Role Assignment'. An 'Edit' button is located to the right of the 'Role Assignment' field. Numbered callouts are present: 1 points to the 'Save' button, 2 points to the 'Cancel' button, 3 points to the 'Group Name' field, and 4 points to the 'Role Assignment' field.

	Item name	Description
1	[Save] button	Saves the entered group information.
2	[Cancel] button	Cancels creating group information.
3	Group Name	Enter the group name. You can enter up to 128 alphanumeric characters and symbols other than “, ‘ (back quote), (,), *, +, /, :, ; (semicolon), <, =, >, ?, [, \,], ’ (apostrophe), {, , }, ~, and , (comma).
4	Role Assignment	You can select roles to be assigned to the group. Click the [Edit] button and select roles from the displayed screen. 📖 P.81 “[Role Assignment] screen”

[Edit Group Information] screen

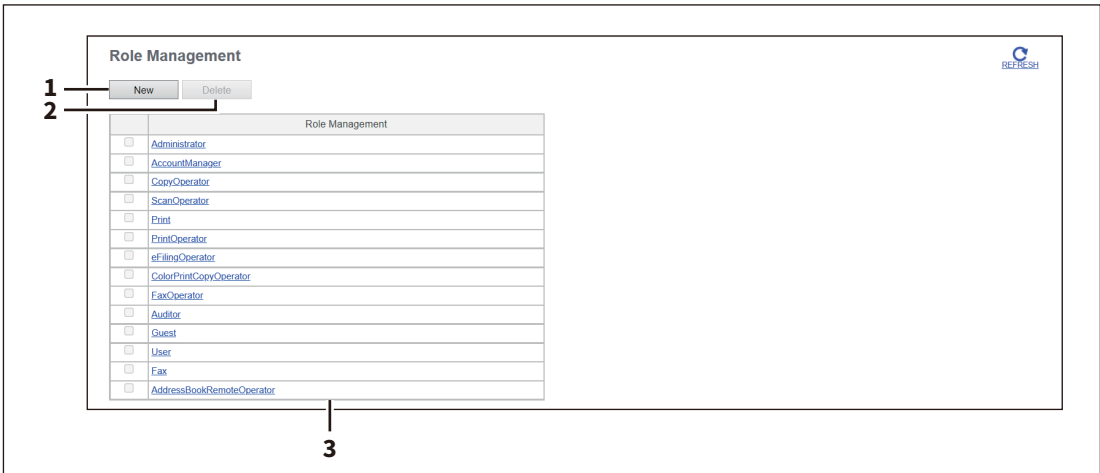
You can check roles registered to the group.

The screenshot shows the 'Edit Group Information' screen. At the top, there's a title bar 'Group Information' with a close button. Below it are 'Save' and 'Cancel' buttons. The main content area has a form with two input fields: 'Group Name' (with a '*'Required label) and 'Role Assignment'. The 'Group Name' field contains the text 'Group01'. The 'Role Assignment' field contains the text 'User'. An 'Edit' button is located to the right of the 'Role Assignment' field. Numbered callouts are present: 1 points to the 'Save' button, 2 points to the 'Cancel' button, 3 points to the 'Group Name' field, and 4 points to the 'Role Assignment' field.

	Item name	Description
1	[Save] button	Saves the entered group information.
2	[Cancel] button	Cancels changing group information.
3	Group Name	Displays the group name.
4	Role Assignment	Displays the roles assigned to the group. Click the [Edit] button and select roles from the displayed screen. 📖 P.81 “[Role Assignment] screen”

■ [Role Management] Item list <access policy mode>

You can manage and register roles if you are logged in to the access policy mode.



	Item name	Description
1	[New] button	Allows you to add a new role. P.87 “[Create New Role] screen”
2	[Delete] button	Deletes the role selected in the role list. However, you cannot delete the default roles.
3	Role Management	Displays the role name. For more information on default roles, see the following: P.85 “Default roles and privileges” You can check role information by clicking the role name. P.89 “[Edit Role] screen”

❑ Default roles and privileges

The following table describes privileges granted to default roles.

The functions listed in “Privileges” and “Permitted operations (functions)” below are displayed in “6 Function list” on the [Create Role Information] screen.

📖 P.87 “[Create New Role] screen”

Default role names	Privileges	Permitted operations (functions)
Administrator	EWB Function	EWB Access
	Scan Function ^{*1}	Store to e-Filing
	Output Setting ^{*2}	Color Print
	e-Filing	e-Filing Access e-Filing Deletion
	Device Setting	Device Setting
	User/Department Management	Create, read, edit, or delete information for user/department management
	Log Management	Read Export
	Job Management	Job Operation
	Addressbook Management	Export/Import Address Book Create a clone file/install an address book
AccountManager	EWB Function	EWB Access
	User/Department Management	Create, read, edit, or delete information for user/department management
CopyOperator	Copy Function	Copy Job
	EWB Function	EWB Access
ScanOperator	EWB Function	EWB Access
	Scan Function	Store to Local File Share Store to Remote Server Send Email RemoteScan/WSScan(Pull)
	Local File Share	Store to Local Storage Store to USB Device
	Remote	Send Email Store to Remote Server WS Scan(Push)
Print	Print Function ^{*1}	Print Job
	EWB Function	EWB Access
PrintOperator	Print Function ^{*1}	Print Management
	EWB Function	EWB Access
	Output Setting ^{*2}	Color Print
eFilingOperator	EWB Function	EWB Access
	Scan Function ^{*1}	Store to e-Filing
	e-Filing	e-Filing Access

Default role names	Privileges	Permitted operations (functions)
ColorPrintCopyOperator	Copy Function	Copy Job Color Copy
	Print Function ^{*1}	Print Job Color Print
	EWB Function	EWB Access
	Output Setting	Color Print
FaxOperator	EWB Function	EWB Access
	Fax/iFax Function	Internet Fax Transmission Fax Transmission Fax Received Print ^{*3}
Auditor	EWB Function	EWB Access
	Log Management ^{*1}	Read
Guest	(No privilege settings)	(No settings)
User	Copy Function	Copy Job Color Copy ^{*2} Store to Local File Share Store to Remote Server Store to e-Filing
	Print Function ^{*1}	Print Job Color Print ^{*2} Store to e-Filing
	EWB Function	EWB Access
	Scan Function	Store to Local File Share Store to Remote Server Send Email Store to e-Filing RemoteScan/WSScan(Pull)
	Fax/iFax Function ^{*1}	Internet Fax Transmission Fax Transmission Store to Local File Share Store to Remote Server
	Output Setting ^{*2}	Color Print
	Local File Share	Store to Local Storage Store to USB Device
	Remote	Send Email Store to Remote Server WS Scan(Push)
	e-Filing	e-Filing Access
Fax	EWB Function	EWB Access
	Fax/iFax Function ^{*1}	Internet Fax Transmission Fax Transmission
AddressBookRemoteOperator	Addressbook Management	Export/Import Address Book Create a clone file/install an address book

^{*1} Part of operations (functions) is permitted.

^{*2} Available only for models that support color printing.

^{*3} For the details of the fax received print function, contact your service technician.

❑ [Create New Role] screen

You can register a new role.

The screenshot shows the 'Create New Role' dialog box. It has a title bar with 'Create New Role' and a close button. Below the title bar are 'Save' and 'Cancel' buttons. The main area contains a form with the following elements:

- 1**: Points to the 'Save' button.
- 2**: Points to the 'Cancel' button.
- 3**: Points to the '*Required' label above the 'Role Name' field.
- 4**: Points to the 'Role Name' text input field.
- 5**: Points to the 'Base Role' dropdown menu.
- 6**: Points to the 'Copy Function' and 'Print Function' tables.

The 'Copy Function' table is highlighted with a red border. It contains the following data:

Function	Status
Copy Job	Disable
Color Copy	Disable
Store to Local File Share	Disable
Store to Remote Server	Disable
Store to e-Filing	Disable

The 'Print Function' table contains the following data:

Function	Status
Print Job	Disable
USB Direct Print	Disable
Color Print	Disable
Store to e-Filing	Disable
Print Management	Disable

	Item name	Description
1	[Save] button	Saves the entered role information.
2	[Cancel] button	Cancels creating the role.
3	Role Name	Enter the role name. You can enter up to 128 characters.
4	Base Role	Select a role which is used as a base of the new role. You can select any registered roles or default roles (CopyOperator, ScanOperator, Print, PrintOperator, eFilingOperator, ColorPrintCopyOperator, FaxOperator, Guest, User, Fax) as the base role.

	Item name	Description
5	MFP Function	Allows you to select the privileges to be assigned to the role.
	Copy Function	Assigns all copy functions.
	Copy Job	Assigns the copy job function.
	Print Function	Assigns all print functions.
	Print Job	Assigns the print job function.
	USB Direct Print	Assigns the USB direct print function.
	Print Management	Assigns the print management function.
	EWB Function ^{*1}	Assigns all EWB functions.
	EWB Access	Assigns the EWB access function.
	Scan Function	Assigns all scan functions.
	Remote Scan/ WSScan(Pull)	Assigns the Remote Scan or Web Services Scan function.
	FAX/iFAX Function	Assigns all fax/ifax functions.
	Internet Fax Transmission	Assigns all Internet Fax transmission functions.
	Fax Transmission	Assigns the fax transmission function.
	Fax Received Print	Assigns the fax/Internet Fax received print function.
	Output Setting ^{*2}	Assigns all output setting functions.
	Color Print	Assigns the color print function.
	Local File Share	Assigns all local file share functions.
	Store to Local Storage	Assigns all local file storage functions.
	Store to USB Device	Assigns all storage to USB device functions.
	Remote	Assigns all remote functions.
	Send Email	Assigns scan to function.
	Store to Remote Server	Assigns all storage to remote server functions.
	WS Scan(Push)	Assigns the WS scan (push) function.
	e-Filing	Assigns all e-Filing functions.
	e-Filing Access	Assigns the e-Filing access functions.
6	Function list	Displays operations (functions) enabled/disabled by privileges assigned to the role selected from “MFP Function”. Even if one item is selected from “MFP Function”, more than one function may be enabled. Example: If you select the [Send Email] check box in [Remote] from “MFP Function”, [Send Email] in [Remote] and that in [Scan Function] on the “Function list” will be enabled.

^{*1} The External Interface Enabler is required to use the EWB (Embedded Web Browser) function. This setting is available only for some models.

^{*2} Available only for models that support color printing.

❑ [Edit Role] screen

You can confirm and edit roles.

However, you cannot edit the default roles.

The screenshot shows the [Edit Role] screen with the following elements:

- 1**: [Save] button
- 2**: [Cancel] button
- 3**: *Required Role Name field (containing 'Role01')
- 4**: MFP Function section (containing checkboxes for Copy Function, Print Function, EWB Function, Scan Function, etc.)
- 5**: Device Management section (containing checkboxes for Device Setting, User/Department Management, Log Management, etc.)
- 6**: Function list table (highlighted with a red box, containing tables for Copy Function, Print Function, EWB Function, and Scan Function)

Function	Status
Copy Job	Enable
Color Copy	Enable
Store to Local File Share	Enable
Store to Remote Server	Enable
Store to e-Filing	Enable

Function	Status
Print Job	Enable
USB Direct Print	Enable
Color Print	Enable
Store to e-Filing	Enable
Print Management	Disable

Function	Status
EWB Access	Enable

Function	Status
Print Job	Enable
USB Direct Print	Enable
Color Print	Enable
Store to e-Filing	Enable
Print Management	Disable

Function	Status
EWB Access	Enable

Function	Status
Print Job	Enable
USB Direct Print	Enable
Color Print	Enable
Store to e-Filing	Enable
Print Management	Disable

Function	Status
EWB Access	Enable

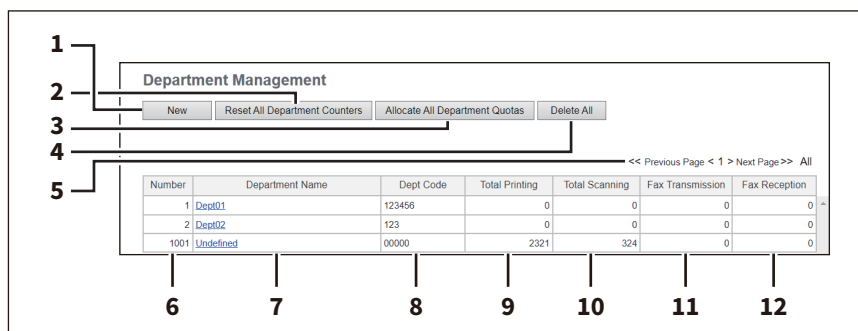
Function	Status
Print Job	Enable
USB Direct Print	Enable
Color Print	Enable
Store to e-Filing	Enable
Print Management	Disable

Function	Status
EWB Access	Enable

	Item name	Description
1	[Save] button	Saves the edited role information.
2	[Cancel] button	Cancels editing the role.
3	Role Name	Enter if changing the role name. You can enter up to 128 alphanumeric characters and symbols other than “, ‘ (backquote), (,), *, +, /, :, ; (semicolon), <, =, >, ?, [, \,], ' (apostrophe), {, , }, ~, and , (comma).
4	MFP Function	Allows you to select the MFP function to be assigned to the group. Select from the following functions. See the following for details: 📖 P.87 “[Create New Role] screen”
5	Device Management	Displays device management privileges assigned to default roles. (Default roles only) 📖 P.85 “Default roles and privileges”
6	Function list	Displays functions assigned to the role. See the following for details: 📖 P.87 “[Create New Role] screen”

■ [Department Management] Item list <access policy mode>

You can manage departments if you are logged in to the access policy mode.



	Item name	Description
1	[New] button	Allows you to add a new department. P.91 “[Department Information] screen”
2	[Reset All Department Counters] button	Resets counters for all departments.
3	[Allocate All Department Quotas] button	Initializes quotas for all departments.
4	[Delete All] button	Deletes the registered department.
5	Select Page	Allows you to select a page when there are 101 items or more.
6	Number	Displays the registration number of the department.
7	Department Name	Displays the department name. Click a department name link to check the department management information. P.92 “[Edit Department Information] screen”
8	Dept Code	Displays the department code.
9	Total Printing	Displays the total number of printed pages of the department.
10	Total Scanning	Displays the total number of scanned pages of the department.
11	Fax Transmission	Displays the total number of transmitted fax pages of the department.
12	Fax Reception	Displays the total number of received fax pages of the department.

❑ [Department Information] screen

You can register a new department.

The screenshot shows the 'Department Information' screen. At the top right, there are 'Save' and 'Cancel' buttons, with callout 1 pointing to 'Save' and callout 2 pointing to 'Cancel'. Below the title bar, there are two text input fields: 'Department Name' (callout 3) and 'Department Code' (callout 4). Below these are two sections for quota settings. The first section, 'Color Quota Setting' (callout 5), includes a dropdown menu set to 'OFF', and two text input fields for 'Color Quota' and 'Default Color Quota'. The second section, 'Black Quota Setting' (callout 5), includes a dropdown menu set to 'OFF', and two text input fields for 'Black Quota' and 'Default Black Quota'.

	Item name	Description
1	[Save] button	Saves the entered department information.
2	[Cancel] button	Cancels creating the department information.
3	Department Name	Enter the department name. You can enter up to 20 characters.
4	Department Code	Enter the department code. You can enter up to 63 characters (except the following: ! " # \$ % & ' () * + , / : ; < = > ? @ [\] ^ ` { } ~ space).
5	Quota Setting	Select this to perform the quota setting of the department according to the setting specified at [Quota Setting] on the [Counter] page. <ul style="list-style-type: none"> • OFF — Not performed • ON — Performed P.71 “[Quota Setting] screen <access policy mode>”
	Quota	Displays the quota amount. This value decreases according to the weight set at [Quota Setting] on the [Counter] page, and output is restricted when the value becomes 0.00. The quota can be manually modified to any amount.
	Default Quota	Enter the default amount to assign to the department. When [Black/Color Quota] or [Black Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999. When [Job Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999.99.

❑ [Edit Department Information] screen

You can confirm and edit department information.

The screenshot shows the 'Edit Department Information' screen. It includes a title bar with 'Save' and 'Cancel' buttons (1 and 2). Below the title bar are 'Reset Counters' (3) and 'Delete' (4) buttons. The form contains several input fields: 'Department Number' (5) with value '1', 'Department Name' (6) with value 'Dep01', and 'Department Code' (7) with value '*****'. There are also dropdown menus for 'Color Quota Setting' (8) and 'Black Quota Setting' (8), both set to 'ON'. Below these are input fields for 'Color Quota' (10000), 'Default Color Quota' (0), 'Black Quota' (50000), and 'Default Black Quota' (0). The screen features three tables: 'Print Counter' (9), 'Scan Counter' (11), and 'Fax Communication Counter' (13). Each table has a 'Total Counter' row and a 'Detail' link. The 'Print Counter' table has columns for Full Color, Twin/ Mono Color, Black, and Total. The 'Scan Counter' table has columns for Full Color, Twin/ Mono Color, Black, and Total. The 'Fax Communication Counter' table has columns for Small, Large, and Total. The 'Sheet Counter' (14) table has columns for Small, Large, and Total. The 'OCR Counter' (15) table has a 'Total' row. The 'Total' row for the OCR Counter shows a value of 0.

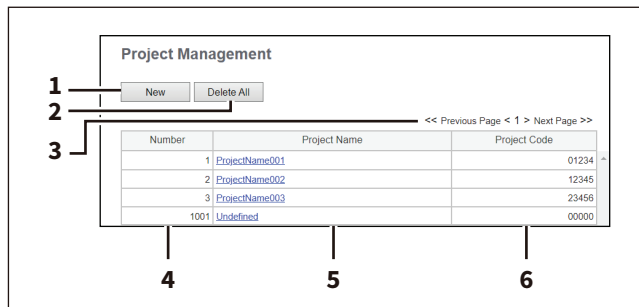
	Item name	Description
1	[Save] button	Saves the entered department information.
2	[Cancel] button	Cancels changing the department information.
3	[Reset Counters] button	Resets counters.
4	[Delete] button	Deletes the displayed department.
5	Department Number	Displays the registration number of the department.
6	Department Name	Enter if changing the department name. You can enter up to 20 characters.
7	Department Code	Enter if changing the department code. You can enter up to 63 characters (except the following: ! " # \$ % & ' () * + , / : ; < = > ? @ [\] ^ ` { } ~ space).

	Item name	Description
8	Quota Setting	<p>Select this to perform the quota setting of the department according to the setting specified at [Quota Setting] on the [Counter] page.</p> <ul style="list-style-type: none"> • OFF — Not performed • ON — Performed <p> P.71 “[Quota Setting] screen <access policy mode>”</p>
	Quota	Displays the quota amount. This value decreases according to the weight set at [Quota Setting] on the [Counter] page, and output is restricted when the value becomes 0.00. The quota can be manually modified to any amount.
	Default Quota	Enter the default amount to assign to the department. When [Black/Color Quota] or [Black Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999. When [Job Quota] is set at [Quota Setting] on the [Counter] page, you can enter up to 99,999,999.99.
9	Print Counter	Displays the output total count value.
10	Detail	<p>Displays details of the total output count value when you click .</p> <p>Copy Counter: Displays the number of pages printed by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages printed by fax reception for paper sizes set on your equipment.</p> <p>Printer Counter: Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment.</p> <p>List Counter: Displays the number of pages printed by system page print operations for paper sizes set on your equipment.</p>
11	Scan Counter	Displays the total count value of scanned documents.
12	Detail	<p>Displays details of the total count value of scanned documents when you click .</p> <p>Copy Counter: Displays the number of pages scanned by copy operations for paper sizes set on your equipment.</p> <p>Fax Counter: Displays the number of pages scanned by fax reception for paper sizes set on your equipment.</p> <p>Network Counter: Displays the number of pages scanned by scan operations for paper sizes set on your equipment.</p>
13	Fax Communication Counter	Displays the communication record.
14	Sheet Counter	Displays the number of printed sheets according to the function being used. Values for the small size and large size are displayed according to the paper size specified on your equipment. This counter increments by 1 for either single or dual-sided copying.
15	OCR Counter	Displays the number of images to which an OCR process has been performed.

■ [Project Management] Item list <access policy mode>

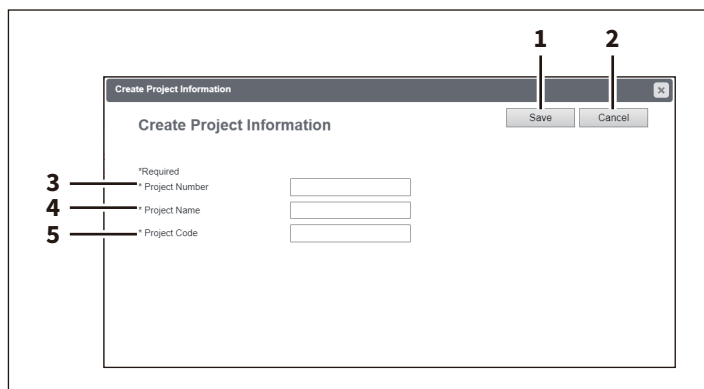
You can register project codes that can be assigned to jobs when you are logged in access policy mode.

□ [Project Management] screen



	Item name	Description
1	[New] button	Allows you to register a new project code. P.94 “[Create Project Information]/[Edit Project Information] screen”
2	[Delete All] button	Deletes all of the registered project codes.
3	Select Page	Allows you to select a page when there are 20 items or more.
4	Number	Displays the project code number.
5	Project Name	Displays the project name.
6	Project Code	Displays the project code.

□ [Create Project Information]/[Edit Project Information] screen



	Item name	Description
1	[Save] button	Registers the information of the new project code.
2	[Cancel] button	Cancels project code creation.
3	Project Number	Enter the project code number.
4	Project Name	Enter the project name.
5	Project Code	Enter the project code.

■ [Export/Import] Item list <access policy mode>

You can export and import your device settings if you are logged in to the access policy mode.

❏ Export

Note

The exported user information must be controlled appropriately to prevent illegal access or tampering.

Export

"It may take more than 10 minutes if there are a lot of entries."

1

User Information (Small/Large Counter)

File NameNot Created

File Size

Date Created

2

Create New File

User Information

File NameNot Created

File Size

Date Created

Create New File

User Information(All Counter)

File NameNot Created

File Size

Date Created

Create New File

Combined(User Information + Role + Group)

File NameNot Created

File Size

Date Created

Create New File

Combined(User Information(All Counter) + Role + Group)

File NameNot Created

File Size

Date Created

Create New File

LDAP Role

File NameNot Created

File Size

Date Created

Create New File

Department Information(Small/Large Counter)

File NameNot Created

File Size

Date Created

Create New File

Department Information

File NameNot Created

File Size

Date Created

Create New File

Department Information(All Counters)

File NameNot Created

File Size

Date Created

Create New File

Project Code

File NameNot Created

File Size

Date Created

Create New File

	Item name	Description
1	Select Export Information Type	<div>Select the information type to be exported from the following.</div> <div><div><div></div>User Information (Small/Large Counter)</div><div><div></div>User Information</div><div><div></div>User Information(All Counter)</div><div><div></div>Combined(User Information + Role + Group)</div><div><div></div>Combined(User Information(All Counter) + Role + Group)</div><div><div></div>LDAP Role</div><div><div></div>Department Information(Small/Large Counter)</div><div><div></div>Department Information</div><div><div></div>Department Information(All Counters)</div><div><div></div>Project Code</div></div>

	Item name	Description
2	[Create New File] button	Creates the export file of the selected information type.

❏ Import

The screenshot shows the 'Import' dialog box with the following components and numbered callouts:

- 1**: Points to the 'User Information' section header.
- 2**: Points to the 'Import Method' radio buttons (Overwrite, Addition, Addition and Clear Counter) under the 'Department Code' section.
- 3**: Points to the 'File Name' input field under the 'Project Code' section.
- 4**: Points to the 'Choose File' button under the 'Project Code' section.
- 5**: Points to the 'Import' button under the 'Project Code' section.

The dialog box contains the following sections and controls:

- User Information**: File Name (Choose File, No file chosen), Import button.
- Combined(User Information + Role + Group)**: File Name (Choose File, No file chosen), Import button.
- LDAP Role**: File Name (Choose File, No file chosen), Import button.
- Department Code**: Import Method (radio buttons: Overwrite, Addition, Addition and Clear Counter), File Name (Choose File, No file chosen), Import button.
- Project Code**: Import Method (radio buttons: Overwrite, Addition), File Name (Choose File, No file chosen), Import button.

Notes:

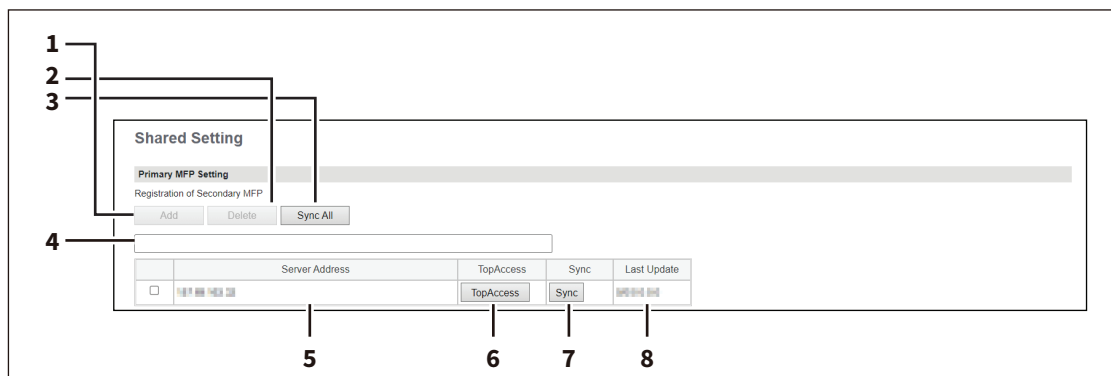
- *It may take more than 10 minutes if there are a lot of entries.
- *Counters of all departments will be cleared if you select "Addition and ClearCounter" and import.

	Item name	Description
1	Select Import Information Type	Select the information type to be imported from the following. <ul style="list-style-type: none"> • User Information • Combined(User Information + Role + Group) • LDAP Role • Department Code • Project Code
2	Import method	Specify this item when you have selected Department Code or Project Code.
3	File name	Displays the name of the import file.
4	[Choose File] button	Allows you to find and select the import file.
5	[Import] button	Imports the displayed file.

■ [Shared Settings] Item list <access policy mode>

When this printer is set as the primary MFP in [Shared Setting] from [Setting up User Authentication Setting], you can synchronize the user information on the printer with other secondary MFPs.

📖 P.240 “Setting up User Authentication Setting”



Note

If you have selected [Use Common Settings] on the [MFP Collaboration] > [Shared User Management] screen, you cannot add and delete the secondary MFPs on this screen.

📖 P.225 “Shared User Management”

	Item name	Description
1	[Add] button	Adds a new secondary MFP. Enter the IP address or host name for the secondary MFP for the distribution destination in the input box below, and then click the [Add] button to register. You can register up to 10 MFPs.
2	[Delete] button	Deletes the selected MFP from the list of secondary MFPs.
3	[Sync All] button	Synchronizes all the secondary MFPs with the primary MFP to share the user information. <div>Note</div> <ul style="list-style-type: none"> The synchronized information is the user information (User Name, Password, PIN Code, Card Information, Role Assignment, Group Assignment, PanelUI Language, PanelUI Keyboard Layout, Email Address, Home Directory, PanelUI Keyboard Display). Settings for Department Management and Project Management are not synchronized. Only user information updated since the last sync is synchronized. When a user has been deleted, the user of the secondary MFP is also deleted during the synchronization. During the initial synchronization, if there is user information in a secondary MFP that is not registered to the printer when the printer is a primary MFP, the user information for the secondary MFP is deleted. The Port Number does not synchronize with the primary MFP or different secondary MFPs. <p>📖 P.236 “Off Device Customization Architecture settings”</p>
4	Input box	Enter the IP address or host name when registering a secondary MFP.
5	Server Address	Shows the IP address of the added secondary MFP.
6	[TopAccess] button	Starts TopAccess.
7	[Sync] button	Synchronizes the secondary MFP with the primary MFP to share the user information.
8	Last Update	Displays the previous update time.

[Administration]

[Setup] Item List	101
General settings	101
Network settings	117
Copier settings	169
Fax settings	173
Save as file settings	182
Email settings	192
InternetFax settings	199
Printer/e-Filing settings	204
Printer settings	205
Print Service settings	212
ICC Profile settings	220
Print Data Converter settings	222
MFP Collaboration	223
Embedded Web Browser settings	233
Off Device Customization Architecture settings	236
Version	237
[Security] Item List	238
Authentication settings	238
Certificate Management settings	257
Password Policy settings	262
Security Stamp setting	265
Configuration settings	266
[Maintenance] Item List	267
Upload Software settings	267
Remove Software settings	269
Create Clone File settings	270
Install Clone File settings	272
Import settings	275
Export settings	277
Panel View	279
Idle Screen	280
Delete Files settings	286
Notification settings	287
Languages settings	290
Remote Command	293
Data Backup	295
User Paper Type	297
System Updates settings	298
Reboot settings	299
[Registration] ([Administration]) Item List	300

Public Home	300
Template settings	306
Public Theme Settings.....	334
Public Home Settings	335
Default Home	336
Default Home Settings.....	336
Simple Screen Settings.....	337
Image/Icon Management	338
Home Data List.....	340
Fax Received Forward and InternetFAX Received Forward settings.....	340
Meta Scan	355
XML Format File.....	359
[Application] Item List	360
Application List	360
Application Settings.....	363
User Extended Information	366
Resource Management.....	367
[License] Item List	368
License List.....	368
Activate.....	368

Note

The paper size for each drawer cannot be set from TopAccess. Set from the touch panel of the equipment. For instructions on how to set the paper size for each drawer, see the reference below:

Preparation of Paper (e-STUDIO6525AC Series/e-STUDIO6528A Series) - LOADING PAPER - Loading Paper in Drawers

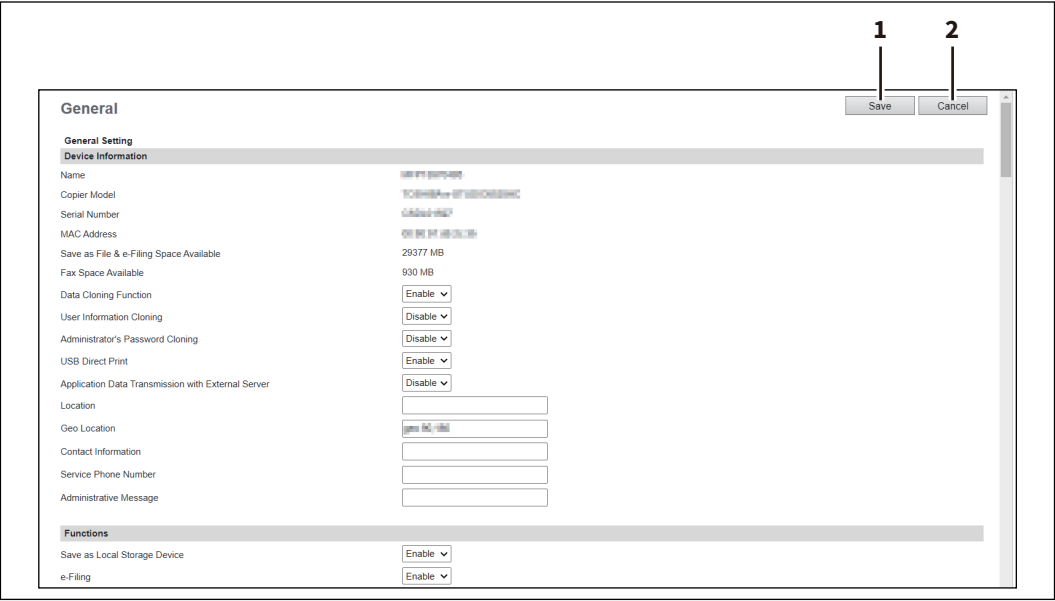
Preparation of Paper (e-STUDIO7527AC Series/e-STUDIO9029A Series) - LOADING PAPER - Loading Paper in Drawers

Tip

Users who are granted administrator privileges in access policy mode can access the [Setup] menu from the [Administration] page.

For how to access it, see the reference below:

P.14 “Access Policy Mode”



	Item name	Description
1	[Save] button	Saves the settings that you have made at [Setup].
2	[Cancel] button	Cancels the settings.

General settings

You can configure the general settings such as device information, energy save, date and time, and web general setting.

Note

Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Tip

The [General] submenu can be accessed from the [Setup] menu on the [Administration] page.

For how to access it and information on the [Setup] menu, see the references below:

P.14 “Access Policy Mode”

P.101 “[Setup] Item List”

❑ Setting up Device Information

You can set the device information displayed on the [Device] page.

	Item name	Description
1	Name	Displays the device name of your equipment.
2	Copier Model	Displays the model name of your equipment.
3	Serial Number	Displays the serial number of your equipment.
4	MAC Address	Displays the MAC address of your equipment.
5	Save as File & e-Filing Space Available	Displays the available space for save as file and e-Filing on your equipment.
6	Fax Space Available	Displays the available space for fax transmission and reception for your equipment.
7	Data Cloning Function	Enable this item when migrating settings on your equipment to another device.
8	User Information Cloning	Enable this item when migrating the user information to another device. This item is available only when [Data Cloning Function] is enabled.
9	Administrator's Password Cloning	Enable this item when migrating the password of the default administrator to another device. This item is available only when [Data Cloning Function] is enabled.
10	USB Direct Print	Select whether the USB Direct Print function is enabled or disabled. USB Direct Print is available only for some models.
11	Application Data Transmission with External Server	Select whether the data collection from the external server is enabled or disabled.
12	Location	Enter the installed location of your equipment. This is displayed on the [Device] page that appears first when accessing the TopAccess website for users.
13	Geo Location	Enter the latitude and longitude in that order with a comma between them. Enter the precise values if required. Up to 64 characters can be entered including ! \$ % & ' () * : + ; [, - =] . ~ . (e.g. geo:00.00,90.00)
14	Contact Information	Enter the name of the person who is responsible for this equipment. This is displayed on the [Device] page that appears first when accessing the TopAccess website for users.
15	Service Phone Number	Enter the telephone number of the person who is responsible for servicing this equipment. This is displayed on the [Device] page that appears first when accessing the TopAccess website for users.

	Item name	Description
16	Administrative Message	Enter the message to the users about this equipment. This is displayed on the [Device] page that appears first when accessing the TopAccess website for users.

□ Setting up Functions

Tip

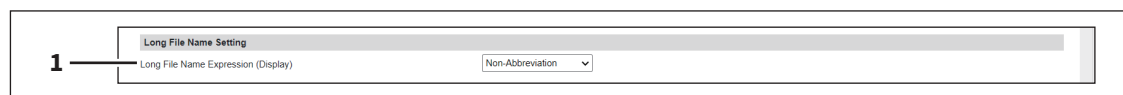
Some items may not be changeable depending on the installed options and their settings. For details, contact your service technician.

Number	Function Name	Setting
1	Save as Local Storage Device	Enable
2	e-Filing	Enable
3	Email Send	Enable
4	Save as FTP	Enable
5	Save as FTPS	Enable
6	Save to USB Media	Enable
7	Save as SMB	Enable
8	Save as Netware	Enable
9	iFax Send	Enable
10	Fax Send	Enable
11	Network iFax	Enable
12	Network Fax	Enable
13	Web Services Scan	Enable
14	Twain Scanning	Enable
15	Scan to External Controller	Enable
16	Background Copy	Disable
17	Background Scan	Disable

	Item name	Description
1	Save as Local Storage Device	Select whether to enable or disable the function to save on the internal storage device.
2	e-Filing	Select whether to enable or disable the e-Filing function.
3	Email Send	Select whether to enable or disable the function to transmit E-mails.
4	Save as FTP	Select whether to enable or disable the function to save using FTP.
5	Save as FTPS	Select whether to enable or disable the function to save using FTPS.
6	Save to USB Media	Select whether to enable or disable the use of USB media.
7	Save as SMB	Select whether to enable or disable the function to save using SMB.
8	Save as Netware	Select whether to enable or disable the function to save using NetWare.
9	iFax Send	Select whether to enable or disable the function to send Internet Faxes.
10	Fax Send	Select whether to enable or disable the function to send faxes.
11	Network iFax	Select whether to enable or disable the network iFax function.
12	Network Fax	Select whether to enable or disable the network fax function.
13	Web Services Scan	Select whether to enable or disable the web scanning service function.
14	Twain Scanning	Select whether to enable or disable the TWAIN scanning function.
15	Scan to External Controller	Select whether to enable or disable the function to scan to an external controller.
16	Background Copy	Select whether to enable or disable the copy function via a smart speaker that the embedded application supports.
17	Background Scan	Select whether to enable or disable the scan function via a smart speaker that the embedded application supports.

❑ Long File Name Setting

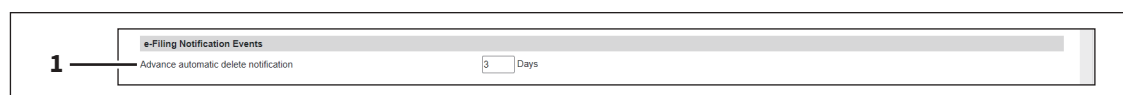
The touch panel of this equipment may not be able to fully display a file name when the name is long, for example, in private print jobs due to its restriction. You can specify how to display file names in Long File Name Setting.



	Item name	Description
1	Long File Name Expression (Display)	Select how to display file names. <ul style="list-style-type: none">• First Portion — The file name is displayed from the beginning and “...” is used to indicate that part of the name is not displayed.• Last Portion — The file name is displayed in the way where the end of the name can be seen.• First and Last Portions — The file name is displayed in the way where the beginning and the end of the file name can be seen.• Non-Abbreviation — The file name is displayed from the beginning up to the number of displayable characters.

❑ Setting up e-Filing Notification Events

You can set E-mail conditions for notifying you that the expiration date of data in e-Filing boxes is approaching.



	Item name	Description
1	Advance automatic delete notification	Select when an E-mail notifying you of the approaching of the expiration date of data in e-Filing boxes is to be sent. You can select how many days before the expiration date from 0 (not notified) to 99 days.

❑ Setting up Job Control



	Item name	Description
1	Job Skip Control	You can select whether to enable or disable the function to skip jobs which do not match the printing conditions. If you enable this function, you can set [Job Skip immediately], [Behavior after recovering suspended cause], [Restart only when owner logs in], and [Auto Delete Timer].
2	Job Skip immediately	Select whether to skip jobs immediately.
3	Behavior after recovering suspended cause	Select the operation after clearing the cause that has suspended jobs. <ul style="list-style-type: none">• Resume — Resumes the suspended jobs automatically.• Skipped — Leaves the jobs skipped to cope with them manually.• Auto — Restarts only undefined user's jobs, for example fax received print and others.

	Item name	Description
4	Restart only when owner logs in	<p>Select whether to allow only the log-in job owner to restart the skipped jobs when the user authentication is enabled.</p> <p>Note</p> <p>When the user authentication is disabled, any user can restart skipped jobs regardless of this setting.</p>
5	Auto Delete Timer	Set the time to delete the skipped jobs. [No Limit] does not delete skipped jobs.
6	Job Interrupt Control	You can select whether to turn on or off the function to interrupt print jobs. When it is turned on, another print job can interrupt and suspend the current job in printing. After the interrupting job is printed, printing the suspended job restarts.

❑ Setting up Restriction on Address Book Operation by administrator / AddressbookRemoteOperator

	Item name	Description
1	No Restriction	Allows all users to perform operations on the Address Book.
2	Can be operated by Administrator / AddressbookRemoteOperator only	Only users with Administrator access or an AddressbookRemoteOperator can perform operations on the Address Book.

❑ Restriction of Destination Selection Method

	Item name	Description
1	Prohibit Direct Entry	Prohibits direct entry of the destination.
2	Prohibit Use Of Local Address Book	Prohibits selection of the destination from the address book.

❑ Setting up Confidentiality Setting

You can specify whether or not to hide the document name, user name, and destination with asterisks (*) that are displayed on jobs.

Item name	Setting
1 Target of Restriction	None
2 Document Name	Disable
3 User Name	Disable
4 TO	Disable
5 FROM	Disable
6 Agent	Disable
7 Log Data Privacy Setting	Store
8 SNMP Data Restriction	Disable

	Item name	Description
1	Target of Restriction	<p>Specify whether or not to apply the confidentiality setting on the job.</p> <ul style="list-style-type: none"> • None — Does not apply the confidentiality setting. • Only JobStatus — Applies the confidentiality setting only to the job status. • Only Log — Applies the confidentiality setting only to the job log. • JobStatus and Log — Applies the confidentiality setting to both the job status and job log.
2	Document Name	<ul style="list-style-type: none"> • Enable — Displays 10 asterisks (*) instead of the document name. • Disable — Displays the document name.
3	User Name	<ul style="list-style-type: none"> • Enable — Displays 10 asterisks (*) instead of the user name. • Disable — Displays the user name.
4	TO	<ul style="list-style-type: none"> • Enable — Displays 10 asterisks (*) instead of the destination. • Disable — Displays the destination.
5	FROM	<ul style="list-style-type: none"> • Enable — Displays 10 asterisks (*) instead of the sender. • Disable — Displays the sender.
6	Agent	<ul style="list-style-type: none"> • Enable — Displays 10 asterisks (*) instead of the agent. • Disable — Displays the agent.
7	Log Data Privacy Setting	<p>Specify whether to hide user-related information for the protection of privacy which is recorded in all job logs, message logs, application logs, and fax transmission/reception journals.</p> <ul style="list-style-type: none"> • Store — Store user-related information as it is. • Not to Store — Hide user-related information with ten asterisks irrespective of user authentication and log authentication. <p>Note</p> <p>The default setting varies from shipment to shipment. This function is set to “Not to Store” as a default setting for some districts.</p>
8	SNMP Data Restriction	<p>Specify whether to restrict the MIB data reception of SNMP for the protection of privacy.</p> <ul style="list-style-type: none"> • Enable — Restricts the reception of the MIB data that contains user-related information. • Disable — Allows the reception of the MIB data that contains user-related information. <p>Note</p> <p>The default setting varies from shipment to shipment. This function is enabled as a default setting for some districts.</p>

❑ Setting up Energy Save

You can set Energy Save mode for your equipment.

For information on types of Energy Save mode and how to enter the mode, see the reference below:

Information About Equipment - Information About Equipment - Turning On/Off - Saving energy when not in use – energy saving modes –

The screenshot shows the 'Energy Save' settings menu. On the left, a vertical list of numbered callouts (1-11) points to specific settings. The main menu area contains the following settings:

- 1** Auto Clear: 45 Seconds
- 2** Auto Power Save: 1 Minute
- 3** Sleep Timer: 1 Minute
- 4** Sleep Mode: Auto
- 5** Super Sleep: Enable
- 6** Expected recovery print setting during Super Sleep: Enable
- 7** Recovery Setting:
 - Press Button: Disable
 - Document Detection: Disable
- 8** Wake Up Setting:

Please set the protocol for Wake up from Super Sleep mode.
Select up to 7 items
*This setting is valid only for broadcast and multicast.

Wired	Wireless	Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ARP
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SNMP for IPv4
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SNMP for IPv6
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SMB
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Bonjour for IPv4
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Bonjour for IPv6
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Neighbor Discovery (Link Local Address)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Neighbor Discovery (Manual/Stateful Address)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LLMNR
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	SLP
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Web Services for IPv4
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Web Services for IPv6
- 9** Motion Sensor: Disable
- 10** Card Reader Response Mode: Eco
- 11** Standby Margin: 60 Seconds

	Item name	Description
1	Auto Clear	<p>Select how long your equipment can remain inactive before the touch panel automatically returns to the default display.</p> <p>Tip</p> <p>The changed value is applied to Auto Clear if its setting is altered. The history of Auto Clear is registered in the log.</p>
2	Auto Power Save	Select how long your equipment can remain inactive before entering Automatic Energy Save mode.
3	Sleep Timer	Select how long your equipment can remain inactive before being entering Sleep mode.
4	Sleep Mode ^{*1}	<p>Select the sleep mode that is activated when a specified period of time has passed.</p> <ul style="list-style-type: none"> • Power Off — The equipment enters the Power Off mode. • Auto — The equipment enters the Sleep mode or the Power Off mode according to the LAN and Fax connections. If the connections are active, it enters the Sleep mode. If they are not active, it enters the Power Off mode. • Sleep — The equipment enters the Sleep mode. <p>Note</p> <p>After you do cloning between the color and monochrome models, the sleep mode action might be changed. If the equipment is turned off unexpectedly or the sleep mode does not work as you like, check the Sleep Mode setting.</p>

	Item name	Description
5	Super Sleep ^{*1}	<p>Select whether this equipment enters the Super Sleep mode when the specified period has elapsed in the Automatic Energy Save mode or when the [ENERGY SAVER] button on the control panel is pressed.</p> <p>Note</p> <ul style="list-style-type: none"> • When the IPsec feature is enabled, you cannot change the Super Sleep Mode from [Disable]. • If this equipment cannot be found on the network or cannot be connected via network while in Super Sleep, try searching again. • The equipment may not enter this mode at the set timing depending on its operational status. • If [Press Button] or [Document Detection] is enabled under [Recovery Setting], you cannot set [Super Sleep].
6	Expected recovery print setting during Super Sleep	<p>Select whether to recover the wired equipment from the Super Sleep mode quickly after it receives a print job. The recovery time can be shorter than the normal one.</p> <ul style="list-style-type: none"> • Enable — Enables this expected recovery print function. • Disable — Disables this expected recovery print function. <p>Note</p> <ul style="list-style-type: none"> • This setting is effective only for the equipment that is wired to the network and in the Super Sleep mode. • If this expected recovery occurs frequently but needlessly for some reason or other, you can disable this function. • This function does not work for private print jobs and hold print jobs. • This function works only for printing with Windows Universal Printer 2 and Universal PS3 printer drivers.
7	Recovery Setting	<p>Set the recovery operation from the sleep mode.</p> <ul style="list-style-type: none"> • Press Button — Select whether to enable or disable the recovery by pressing the buttons of the equipment. • Document Detection — Select whether to enable or disable the recovery by detecting documents on the Automatic Document Feeder.

	Item name	Description
8	Wake Up Setting	<p>Select the protocol to wake up your equipment from the Super Sleep mode (or the Sleep mode for the models with no Super Sleep mode function) by a network search. The number of available protocols varies depending on the model.</p> <p>Note</p> <ul style="list-style-type: none"> • The [Wake Up Setting] setting is enabled when sending an unspecified number of MFP data through “broadcasting” and sending multiple data with MFP specified through “multicasting”. The [Wake Up Setting] setting is disabled when using “unicast” which specifies an address and sends. • The wake up setting is enabled when the super sleep mode is enabled in the energy save setting. • The protocol selecting list of the Wake Up setting is made to select the desired protocols regardless of whether the selected protocol is enabled or disabled on each protocol setting. If the selected protocol is disabled in its protocol setting, however, the Wake Up setting is disabled too and therefore this equipment will not be recovered from the Super Sleep mode or the Sleep mode (for models in which no Super Sleep mode is installed). • When no response is returned from this equipment after you access the network even if a protocol selected on this setting is used, retry the access. <p>Tip</p> <p>For “unicast” communication which carries out transmission by specifying a certain address in the following protocols, the equipment can return from the Super Sleep mode (or the Sleep mode for the models with no Super Sleep mode function) even if the Wake Up setting is not applied. IPP, FTP, HTTP, SMB, SMTP, SNMP, RAW9100, LPD, WebService</p>
9	Motion Sensor ^{*2}	<p>Select whether the motion sensor is enabled or disabled.</p> <ul style="list-style-type: none"> • Disable — Disables the motion sensor. • Enable (Screen On) — Enables the motion sensor and turns on the screen. • Enable (Screen Off) — Enables the motion sensor and turns off the screen.
10	Card Reader Response Mode ^{*2}	<ul style="list-style-type: none"> • Normal — Click this button when the response of the card reader is slow. • Eco — Click this button to cut down the power consumption although the response of the card reader might become slow.
11	Standby Margin ^{*2}	Set the time (seconds) to accept the operation of the touch panel.

^{*1} This function is not available for some models.

^{*2} These functions are available only for some models with the motion sensor.

The following network settings are required for this equipment to enter the Super Sleep mode.

- Select other than [Use Stateless Address] in the IPv6 setting.
P.123 “IPv6/ IPv6 (Secondary)”
- Select [Disable] for [Enable IPX/SPX] in the IPX/SPX setting.
P.167 “Setting up IPX/SPX”
- Specify one of the following in [POP3 Network Service].
 - [Disable] for [Enable POP3 Client].
 - No entry for [POP3 Server Address].
 - No entry for [Account Name].
 - 0 for [Scan Rate].P.158 “Setting up POP3 Client”
- Disable IEEE 802.1X authentication.
For the IEEE 802.1X authentication method under the wired LAN environment, see the reference below:
User Functions - SETTING ITEMS (Admin) - 802.1X Settings

See the following for the network access setting in super sleep mode for your equipment.

- **ARP**
Select this to enable address resolution when this equipment is used under IPv4 environment.
- **SNMP for IPv4**
Select this to search for this equipment over the network with SNMP protocol when Client Utilities is used under IPv4 environment.
- **SNMP for IPv6**
Select this to search for this equipment over the network with SNMP protocol when Client Utilities is used under IPv6 environment.
- **SMB**
Select this to enable domain name resolution when NetBIOS name is used under IPv4 environment.
- **Bonjour for IPv4**
Select this to search for this equipment over the network with the Bonjour protocol when it is used under IPv4 environment.
- **Bonjour for IPv6**
Select this to search for this equipment over the network with the Bonjour protocol when it is used under IPv6 environment.
- **Neighbor Discovery (Link Local Address)**
Select this to enable address resolution when this equipment is used under IPv6 environment.
- **Neighbor Discovery (Manual/Stateful Address)**
Select this to enable address resolution when this equipment is used under IPv6 environment.
- **LLMNR**
Select this to enable domain name resolution when NetBIOS name is used.
- **SLP**
Select this to enable service discovery when SLP is used.
- **Web Services for IPv4**
Select this to search for this equipment over the network with WSDiscovery under IPv4 environment.
- **Web Services for IPv6**
Select this to search for this equipment over the network with WSDiscovery under IPv6 environment.

❑ Shutdown Setting

Specify whether to display a confirmation screen when shutting down the equipment.



	Item name	Description
1	Display the shutdown select screen when choices are one.	Specify whether or not to display the confirmation screen.

□ Setting up Date & Time

You can set the date, time, time zone, and date format.

Tip

- [Date & Time] settings are not available if the SNTP function is enabled.
- If the date and time is not set correctly, the SSL/TLS communications and Kerberos authentication with the server might fail.

	Item name	Description
1	Year/Month/Date/Time	Select the year and month in designated boxes. Also, enter the date and time in designated boxes.
2	Time Zone	Select the time zone where this equipment is located.
3	Date Format	Select the date format.

□ Setting up SNTP Service

In SNTP Service, you can specify the SNTP server to refresh the time settings of this equipment using SNTP service.

	Item name	Description
1	Enable SNTP	Select whether to enable or disable SNTP (Simple Network Time Protocol). When this is enabled, the time settings of this equipment can be adjusted using the SNTP service. Tip [Date & Time] settings are not available if enabled.
2	Primary SNTP Address	Enter the IP address or FQDN (Fully Qualified Domain Name) of the Primary SNTP Server Address when [Enable SNTP] is enabled.
3	Secondary SNTP Address	Enter the IP address or FQDN (Fully Qualified Domain Name) of the Secondary SNTP Server Address when [Enable SNTP] is enabled as required. Tip When the [Obtain a SNTP Server Address automatically] option is enabled in the TCP/IP settings, the SNTP server address can be obtained using the DHCP server. 📖 P.118 “Basic Setting”
4	Scan Rate	Enter how often this equipment should access the SNTP server to check the time.
5	Port Number	Enter the port number for the SNTP service. Generally “123” is used.
6	NTP Authentication	Select whether to enable or disable NTP authentication.

❑ Setting up Daylight Savings Time Setting

Make the required settings for daylight savings time.

	Item name	Description
1	Daylight Savings Time	Select [Enable] to shift the clock to the daylight savings time. [Disable] is set as the default.
2	Offset	Select the desired offset (time difference) from the local standard time. You can select from between -2 and +2 hours, excluding 0 hour, in 30-minute increments. [+1:00] is set as the default.
3	Dates	Select the applicable period for the daylight savings time. <ul style="list-style-type: none">• Start — Select or enter the start date and time of daylight savings time.• End — Select or enter the end date and time of daylight savings time.

Tip

- If you change the settings during the daylight saving time period, the changes will be reflected to the equipment's clock. If you select [Disable] during the applicable period, be sure to confirm that the correct time is displayed since the equipment's clock will shift to the current time. When the SNTP Service setting is enabled and if the SNTP server is synchronized, the correct time will be displayed.
📖 P.111 "Setting up Date & Time"
- If the equipment is turned off at the start or end date and time, the equipment will shift the clock the next time it is turned on.
- After the clock shifts, the daylight saving time will also apply to the weekly timers.

Note

Select the Start and the End dates and times based on the time set for the equipment.

📖 P.111 "Setting up Date & Time"

❑ Setting up WEB General Setting

You can set the session timer for TopAccess.

	Item name	Description
1	Session Timer	Enter how long you want this equipment to preserve the session data of TopAccess. You can enter any integer between 5 to 999. This setting also applies to the session data of the e-Filing web utility. "10" is set as the default.

Tip

- When logged in the access policy mode, you will be automatically logged out if the session timer elapses without any operation being performed.
- Once a logging-in user operates TopAccess, the changed value is applied to Session Timer if its setting is altered.

❑ Home Setting

You can set the default screen displayed by pressing the [Home] button on the control panel when user authentication is enabled. The settings vary, depending on the [Sync Setting] setting.

Tip

For the procedure for home data synchronization, see the reference below:

📖 P.392 “Setting Home Data Synchronization”

When [Disable] is selected from [Sync Setting]

1

2

3

14

Home Setting

Public Home

Default Home Screen Setting

Sync Setting

Public Home change from User

Disable

User

Disable

Enable

When [Use Network Server for Sync] is selected from [Sync Setting]

1

2

3

4

5

6

7

8

13

14

Home Setting

Public Home

Default Home Screen Setting

Sync Setting

Use Network Server for Sync

Server Name

Port Number

User Name

Password

Enable SSL/TLS

Delete All Shared Data

Public Home change from User

Disable

User

Use Network Server for Sync

21

Disable

Enable

When [Use MFP for Sync] is selected from [Sync Setting]

1

2

3

9

10

11

12

13

14

Home Setting

Public Home

Default Home Screen Setting

Sync Setting

Use MFP for Sync

☐

Assume this MFP is the Primary Server

Server Name

Port Number

Enable SSL/TLS

Delete All Shared Data

Public Home change from User

Disable

User

Use MFP for Sync

21

Disable

Enable

Note

If you have selected [Select from Common Settings] on the [MFP Collaboration] > [Shared Home] screen, you cannot enter the server name on this screen.

📖 P.228 “Shared Home”

	Item name	Description
1	Public Home	Select whether to enable or disable Public Home.
2	Default Home Screen Setting	Select the Home to be displayed as the default screen when you press the [Home] button. User: Select this to the User Home screen. Public: Select this to display the Public Home screen.

	Item name	Description
3	Sync Setting	Specify whether or not to synchronize the HOME screen with the network server or other MFPs. <ul style="list-style-type: none"> • Disable: Disable the Home sync function. • Use Network Server for Sync: Select this to use the network server for synchronization. • Use MFP for Sync: Select this to use MFP for synchronization.
4	Server Name	Enter the name of the network server.
5	Port Number	Enter the port number of the network server.
6	User Name	Enter the name of the user who accesses the network server.
7	Password	Enter the password of the user who accesses the network server.
8	Enable SSL/TLS	Select whether SSL/TLS is enabled or disabled.
9	Assume this MFP is the Primary Server	Select this check box to synchronize this MFP as the primary server. When you clear this check box, another MFP can synchronize as the primary server. <div> Note </div> If the FTP server is disabled, you cannot set this MFP as the primary server. 📖 P.150 “Setting up FTP Server”
10	Server Name	Enter the name of the primary server when you set another MFP other than this MFP as the primary server.
11	Port Number	Enter the port number of the primary server when you set another MFP other than this MFP as the primary server.
12	Enable SSL/TLS	Select whether SSL/TLS is enabled or disabled when you set another MFP other than this MFP as the primary server.
13	Delete All Shared Data	Delete all the shared data stored in the FTP server.
14	Public Home change from User	Select whether general users can change the Public Home screen. <ul style="list-style-type: none"> • Enable — Allows general users to change the Public Home screen. • Disable — Forbids general users to change the Public Home screen.

❑ Assignment for Programmable Button

You can assign functions to Programmable Button 1 and Programmable Button 2.

1

Assignment for Programmable Button

Programmable Button1
None

Programmable Button2
None

	Item name	Description
1	Programmable Button 1/ Programmable Button 2	Select the function to assign.

❑ Panel Setting

You can set the default screen on the control panel and the appearance order in the job lists.

The screenshot shows the 'Panel Setting' menu with the following items and their corresponding dropdowns:

- 1 Default Screen: Home Screen
- 2 Sort Order: Descending Order
- 3 Default Document List Setting: Document Name

Below these items, there are three more dropdowns: Document Name, Document Name, and Document Name.

	Item name	Description
1	Default Screen	Specify the functions to be displayed on the default screen after this equipment starts up. Select [Embedded Application] and then press [Assignment] to specify the applications to be set on the default screen.
2	Sort Order	Specify the appearance order of hold (fax) and secure Rx jobs in the job list. <ul style="list-style-type: none"> • Ascending Order — Shows the jobs in the ascending order by day. • Descending Order — Shows the jobs in the descending order by day.
3	Default Document List Setting	Specify the default appearance of the document list on the control panel respectively for [Hold(Fax) & Secure Rx], [USB Direct Print], and [Private, Hold, Proof, Multi Station Print]. <ul style="list-style-type: none"> • Document Name — Shows document names in the list. • Thumbnail Image — Shows thumbnail images in the list for PDF and JPEG files. The fixed icon appears for files of other formats. <div> Note <ul style="list-style-type: none"> • A thumbnail just represents the image of a file. The image may differ from the original, having parts of it cut or blank spaces added. • You need the Multi Station Print Enabler option to use the [Multi Station Print] function. </div>

❑ OCR Setting

You can specify the OCR function.

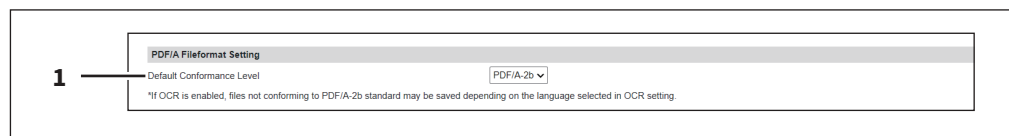
The screenshot shows the 'OCR Setting' menu with the following items and their corresponding settings:

- 1 Language: 1st English, 2nd None
- 2 Auto Rotation: Enable
- 3 XLSX Sheet Composition: 1 Page Becomes 1 Sheet (selected), Multi Pages Become 1 Sheet

	Item name	Description
1	Language	Select the prioritized primary and secondary languages.
2	Auto Rotation	Specify whether or not to automatically rotate.
3	XLSX Sheet Composition	Specify how to create the XLSX sheet. <ul style="list-style-type: none"> • 1 Page Becomes 1 Sheet — Makes 1 page 1 sheet. • Multi Pages Become 1 Sheet — Combines multiple pages into 1 sheet.

PDF/A Fileformat Setting

You can set the default level of the PDF/A file format.



	Item name	Description
1	Default Conformance Level	Select the default conformance level of PDF/A. <ul style="list-style-type: none">• PDF/A-1b — Selects PDF/A-1b as a default setting.• PDF/A-2b — Selects PDF/A-2b as a default setting.

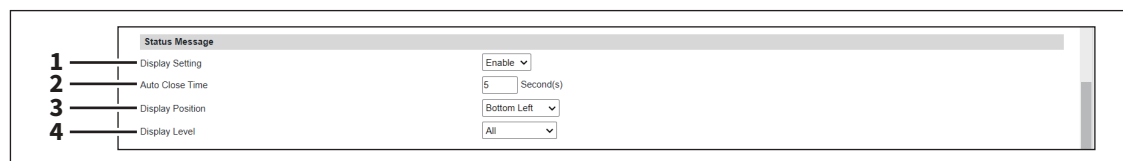
Note

- When you save searchable PDF/A-2b files with the enabled OCR function, they might not conform to the PDF/A-2b standard, depending on several OCR languages that you select. It is recommended that you select PDF/A-1b to save searchable PDF/A files with the OCR function.
- PDF with the digital signature might not be created in the PDF/A-1b file format, depending on the certificate settings.

P.261 “Setting up Certificate Setting”

Status Message

You can set the common message of the status message and icon that appears commonly on every screen of the control panel.



	Item name	Description
1	Display Setting	Select whether to enable or disable the appearance of the common message. The [Display Setting] setting on the [Application Details] window of the application takes priority over this one. P.360 “Application List”
2	Auto Close Time	Specify the time from 1 to 30 seconds (default 5 seconds) to close the common message automatically. The time specified for each status message takes priority over this one.
3	Display Position	Select where the common message appears on the screen: the default position is “Bottom Left”. The [Display Position] setting on the [Application Details] screen of the application takes priority over this one. P.360 “Application List”
4	Display Level	Select the display level of the common message from “All” (default), “Warning/Error”, or “Error”. Messages out of these levels do not appear on the screen.

■ Network settings

You can configure the network settings such as TCP/IP, Filtering, IPX/SPX, Bonjour, LDAP Session, SMB Session, NetWare Session, HTTP Network Service, SMTP Client, SMTP Server, POP3 Network Service, SNTP Service, FTP Client, FTP Server, SNMP Network Service, and Security Service.

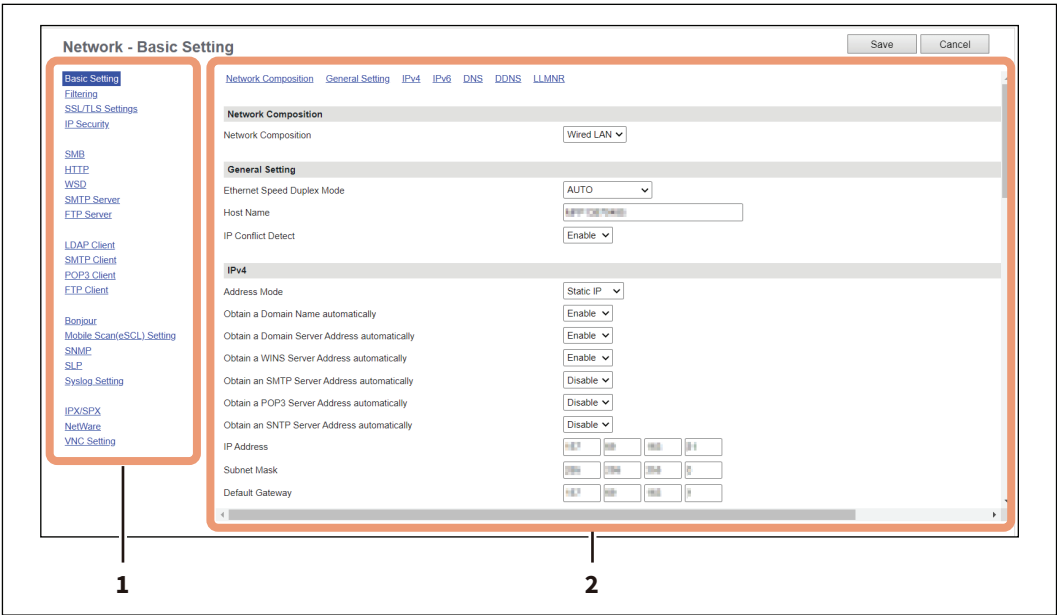
Note

During the initialization of the network, the network will not be available. A message is displayed to inform you that it will reconnect to TopAccess after a while. Also, the touch panel on this equipment displays a message to inform you that the network is not ready. When this message disappears, TopAccess will once again be available.

Tip

The [Network] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

- P.14 “Access Policy Mode”
- P.101 “[Setup] Item List”

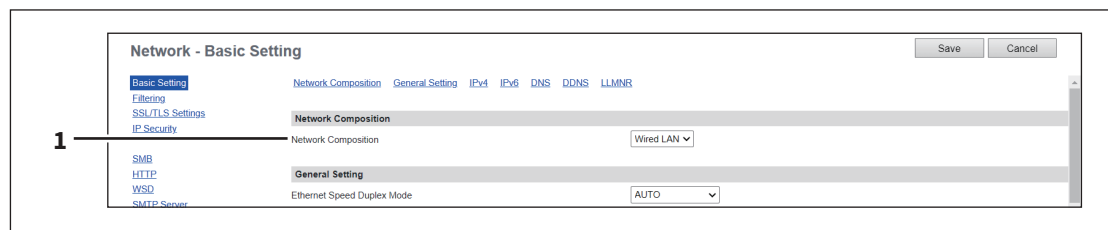


	Item name	Description
1	Menu area	This area shows the functions that you can set for [Network]. When you click a function name, the settings for the selected function appear in the setting display area on the right.
2	Setting display area	This area shows the settings for the function selected in the menu area. When you click an item at the link menu located on the top, you can move directly to the item. After you change the settings, be sure to click [Save]. To cancel the setting operation, click [Cancel].

Basic Setting

You can set TCP/IP, DNS, and DDNS in the Basic Setting. The TCP/IP must be configured to enable TopAccess, SMB printing, Raw TCP or LPR printing, IPP printing, Scan to Email, and Internet Fax.

Network Composition



	Item name	Description
1	Network Composition	<p>Select the network composition of this equipment.</p> <ul style="list-style-type: none">• Wired LAN — Select this to use the standard wired LAN as the primary network.• Wireless LAN — Select this to use the wireless LAN as the primary network. This setting appears if the wireless LAN module is attached to this equipment and the wireless LAN communication is configured properly.• Wired LAN + Wired LAN2 — Select this to use two channels at the same time with the wired LAN as the primary network and the wired LAN2 as the secondary network. This setting appears if the network adapter dedicated for the wired LAN2 is connected to this equipment.• Wireless LAN + Wired LAN — Select this to use two channels at the same time with the wireless LAN as the primary network and the standard wired LAN as the secondary network. This setting appears if the wireless LAN module is attached to this equipment and the wireless LAN communication is configured properly.

Note

The secondary network can support the following communications:

- Network printing
- Remote scan (by the use of the remote scan driver)
- Client applications
- TopAccess
- SNMP (without trap)
- Bonjour
- VNC
- IP Security

Tip

For information about the network adapter for Wired LAN2, ask your service representative.

General Setting / General Setting (Secondary)





You need to set [General Setting (Secondary)] for the secondary network when you use the two-channel networks.


	Item name	Description
1	Ethernet Speed Duplex Mode	<p>Select the ethernet speed. [AUTO] is set as the default.</p> <div> Note <ul style="list-style-type: none"> When you select a specific ethernet speed, you must select the same one as set in the connected network. If you do not know the ethernet speed that must be used, select [AUTO]. If the network is not stable, power OFF the equipment then ON. </div>
2	Host Name	<p>Enter the host name of your equipment. You can enter up to 63 alphanumerical characters including “-” (hyphens). You cannot use a “-” (hyphen) as the first and last character. The MFP name is set as the default.</p>
3	IP Conflict Detect	<p>Specify whether or not to detect IP address conflicts. Select [Enable] to display a message on the touch panel when an IP address conflict is detected. [Enable] is set as the default.</p>

IPv4 / IPv4 (Secondary)

You need to set [IPv4 (Secondary)] for the secondary network when you use the two-channel networks.

	Item name	Description
1	Address Mode	<p>Select how to set the IP address.</p> <ul style="list-style-type: none"> • Static IP — Select this to assign the static IP address manually. When this is selected, enter the static IP address in the [IP Address] box. • Dynamic — Select this to assign the IP address using the DHCP with Auto-IP addressing enabled. The IP address, subnet mask, gateway address, primary WINS server address, secondary WINS server address, POP3 server address, and SMTP server address can be automatically acquired from the DHCP server if the network supports DHCP. However, if the network does not support DHCP, use the AutoIP function to assign an IP address. • No AutoIP — Select this to assign the IP address using the DHCP with Auto-IP addressing disabled. The IP address, subnet mask, gateway address, primary WINS server address, secondary WINS server address, POP3 server address, and SMTP server address can be automatically acquired from the DHCP server if the network supports DHCP. If the communication with the DHCP cannot be established, the previous IP address is used.
2	Obtain a Domain Name automatically	<p>Select [Enable] when you want to obtain a domain name automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Enable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a domain name, the data are left blank in the domain name even if you set the correct domain name manually in the DDNS Session. In that case, select [Disable] here and set the correct domain name in the DDNS Session.</p> <p> P.126 “DDNS”</p>

	Item name	Description
3	Obtain a Domain Server Address automatically	<p>Select [Enable] when you want to obtain a domain server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Enable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a primary and secondary DNS server addresses, the data are left blank in the primary and secondary DNS server addresses, even if you set the correct primary and secondary DNS server addresses manually in the DNS Session. In that case, select [Disable] here and set the correct primary and secondary DNS server address in the DNS Session.  P.125 “DNS / DNS (Secondary)”</p>
4	Obtain a WINS Server Address automatically	<p>Select [Enable] when you want to obtain a primary or secondary WINS server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Enable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a primary and secondary WINS server addresses, the data are left blank in the primary and secondary WINS server addresses, even if you set the correct primary and secondary WINS server addresses manually in the SMB Session. In that case, select [Disable] here and set the correct primary and secondary WINS server address in the SMB Session.  P.142 “Setting up SMB”</p>
5	Obtain an SMTP Server Address automatically	<p>Select [Enable] when you want to obtain a SMTP server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Disable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a SMTP server address, the data are left blank in the SMTP server address even if you set the correct SMTP server address manually in the SMTP Client. In that case, select [Disable] here and set the correct SMTP server address in the SMTP Client.  P.155 “Setting up SMTP Client”</p>
6	Obtain a POP3 Server Address automatically	<p>Select [Enable] when you want to obtain a POP3 server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Disable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a POP3 server address, the data are left blank in the POP3 server address even if you set the correct POP3 server address manually in the POP3 Network Service. In that case, select [Disable] here and set the correct POP3 server address in the POP3 Network Service.  P.158 “Setting up POP3 Client”</p>

	Item name	Description
7	Obtain an SNTP Server Address automatically	<p>Select [Enable] when you want to obtain a SNTP server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option. [Disable] is set as the default.</p> <p>Note</p> <p>When the DHCP server does not have a SNTP server address, the data are left blank in the SNTP server address even if you set the correct SNTP server address manually in the SNTP Network Service. In that case, select [Disable] here and set the correct SNTP server address in the SNTP Network Service.</p> <p> P.111 “Setting up SNTP Service”</p>
8	IP Address	Enter the static IP address for your equipment when [Static IP] is selected in the [Address Mode] box. Specify within the range from 1 to 126 and 128 to 223 for the 1st octet, 0 to 255 for the 2nd to 4th octet.
9	Subnet Mask	Enter the subnet mask if required when [Static IP] is selected in the [Address Mode] box. Specify within the range from 0 0 0 0 to 255 255 255 255. However, you cannot set 0.0.0.0 and 255.255.255.255.
10	Default Gateway	Enter the gateway address if required when [Static IP] is selected in the [Address Mode] box. Specify within the range from 0 0 0 0 to 255 255 255 255.

IPv6/ IPv6 (Secondary)

You need to set [IPv6 (Secondary)] for the secondary network when you use the two-channel networks.

The screenshot shows the 'Network - Basic Setting' window for IPv6. On the left, a sidebar lists various settings: Basic Setting, Filtering, Link Local Address, Manual, and Stateless Address. The 'Manual' option is selected. The main area contains fields for IP Address, Prefix Length, and Gateway. There are also checkboxes for 'Use DHCPv6 Server for options' and 'Use Stateless Address'. A table shows the 'No. IP Address' and 'Prefix Length' for 1 to 7 addresses. A 'Gateway' field is also present. The 'Save' and 'Cancel' buttons are at the top right.

	Item name	Description
1	Enable IPv6	Select whether the IPv6 protocol is enabled or disabled. [Enable] is set as the default.
2	Link Local Address	The automatically generated unique IP Address used for the IPv6 is displayed.
3	Manual	<p>You assign the IPv6 address, prefix and default gateway manually. In this mode, you can assign one IPv6 address to this equipment.</p> <p>IP Address — Assign the IPv6 address for this equipment. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>Prefix Length — Assign the prefix length for the IPv6 address. Specify within the range from 0 to 128. “0” is set as the default.</p> <p>Gateway — Assign the default gateway address. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>Use DHCPv6 Server for options — Select this check box to use the optional information (IPv6 address for the DNS server, etc.) which is issued from the DHCPv6 server.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Tip</p> <ul style="list-style-type: none"> When [Manual] is selected, a stateful address cannot be set. If the selected IPv6 address is already assigned, DAD (Duplicate Address Detection) detects it and notifies you on the touch panel of this equipment. </div>


	Item name	Description
4	Use Stateless Address	<p>Use the IPv6 addresses (Stateless addresses) issued from routers.</p> <ul style="list-style-type: none"> • Use DHCPv6 Server for IP Address(M flag) — Use the IPv6 address issued from the DHCPv6 server in the stateless network environment. • Use DHCPv6 Server for options(O flag) — Use the optional information (IPv6 address for the DNS server, etc.) issued from the DHCPv6 server in the stateless network environment. • FQDN Option — The FQDN option is available if Use DHCPv6 Server for IP Address is selected. Select [Server] or [Client] for [Update Method] if using the FQDN option. [Server] is set as the default. • IP Address — Stateless Addresses obtained from routers are displayed. Up to 7 IPv6 addresses can be retained. <p>Tip</p> <p>When this equipment receives a router advertisement (RA) from a router, of which M flag configuration is “0”, the DHCPv6 function is disabled. If you change a router advertisement (RA) M flag configuration from “0” to “1”, it is necessary to reboot this equipment to enable the DHCPv6 function.</p>
5	Use Stateful Address	<p>Use the Stateful address issued from DHCPv6 server.</p> <ul style="list-style-type: none"> • Use DHCPv6 Server for IP Address — Select whether or not the IPv6 address which is issued from the DHCPv6 server is used for this equipment. • Use DHCPv6 Server for options — Select whether or not the optional information (IPv6 address for the DNS server, etc.) except the IPv6 address for this equipment, which is issued from the DHCPv6 server is used on this equipment. • FQDN Option — The FQDN option is available if Use DHCPv6 Server for IP Address is selected. Select [Server] or [Client] for [Update Method] if using the FQDN option. [Server] is set as the default. • IP Address — A stateful address, Prefix Length and Gateway obtained from DHCPv6 Server are displayed.

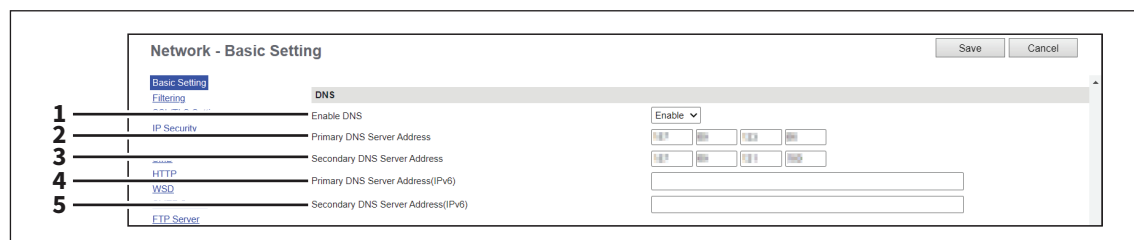
DNS / DNS (Secondary)

In DNS Session, you can specify the DNS server to enable the FQDN (Fully Qualified Domain Name) rather than the IP address on specifying each server address such as SMTP server, POP3 server, and LDAP server. You need to set [DNS (Secondary)] for the secondary network when you use the two-channel networks.

Tip

When the DNS service is enabled and the DNS server supports the dynamic DNS service, Set the DDNS Session as well.


 P.126 “DDNS”



	Item name	Description
1	Enable DNS	Select whether the DNS server is enabled or not. [Enable] is set as the default.
2	Primary DNS Server Address	Specify the IP address of the primary DNS server when the DNS service is enabled. Specify within the range from 0 0 0 0 to 255 255 255 255.
3	Secondary DNS Server Address	Specify the IP address of the secondary DNS server when the DNS service is enabled, as you require. Specify within the range from 0 0 0 0 to 255 255 255 255.
4	Primary DNS Server Address(IPv6)	Specify the IP address of the primary DNS server when the DNS service is enabled in IPv6. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
5	Secondary DNS Server Address(IPv6)	Specify the IP address of the secondary DNS server when the DNS service is enabled in IPv6, as required. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Tip

When the [Obtain a Domain Server Address automatically] option is enabled in the TCP/IP settings, the server address of the primary and secondary DNS server addresses can be obtained using the DHCP server.

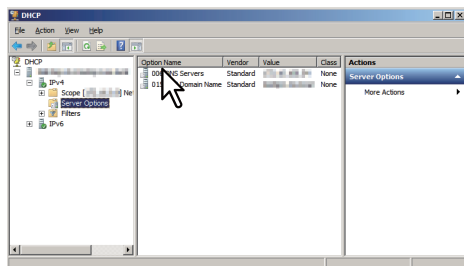
 P.118 “Basic Setting”

DDNS

In DDNS Session, you can enable the Dynamic DNS service if the DNS server supports the dynamic DNS.

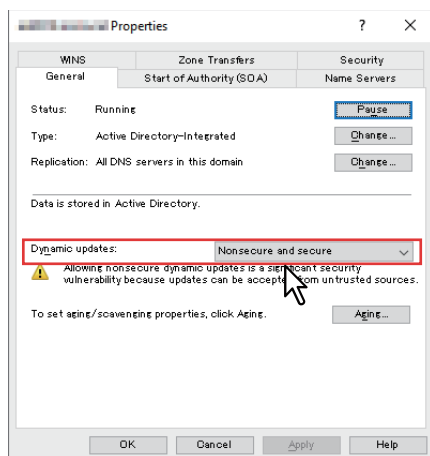
Note

- When using the security in DDNS, if the difference between the time set in the server, in which Windows DNS record is to be updated, and the one set in the equipment exceeds the time stated in the account policy of the server, the DNS update using the security will fail. Check the time set for the DNS server and match it with the one set for the equipment.
- When using DDNS and the IP address is assigned using DHCP, enable “006 DNS Servers” and “015 DNS Domain Name” in the DHCP Server’s Scope Options or Server Options.

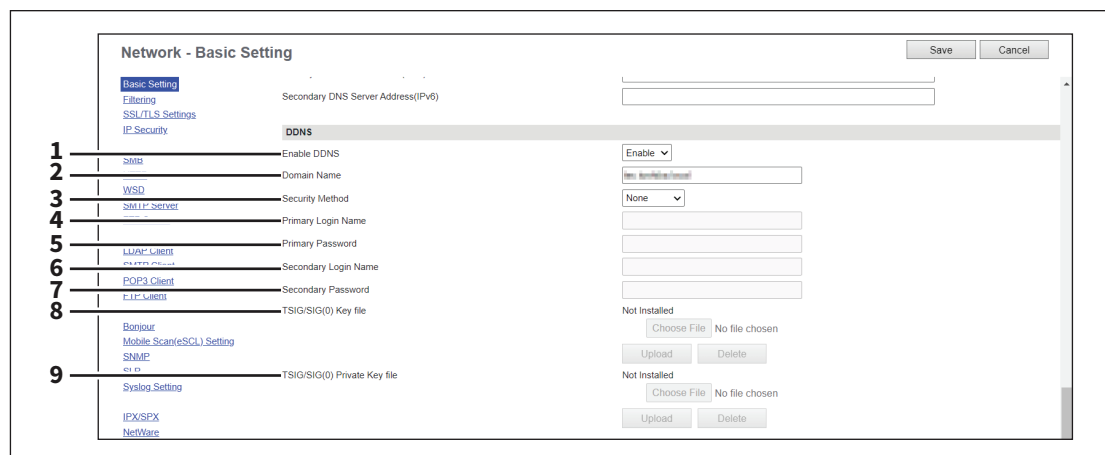
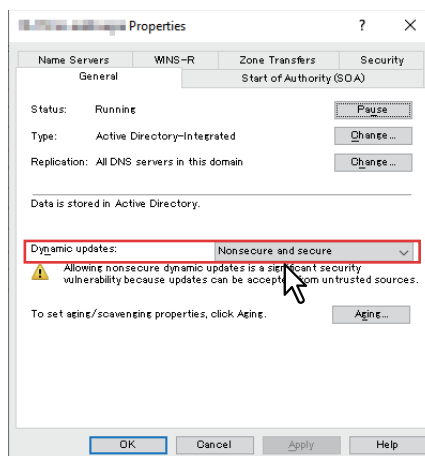



- When using DDNS, make sure the “Dynamic updates” option is set to “Nonsecure and secure” or “Secure only” for the Forward Lookup Zones and Reversed Lookup Zones in the DNS server (in Windows Server).
- If the DNS server has been set up with “Secure only”, be sure to set the security at the DDNS settings for the equipment.

Forward Lookup Zones
(Windows Server 2019)



Reversed Lookup Zones
(Windows Server 2019)



	Item name	Description
1	Enable DDNS	Select whether the dynamic DNS service is enabled or disabled. [Enable] is set as the default.
2	Domain Name	<p>Enter the domain name that will be added to the DNS server using DDNS. You can enter up to 96 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</p> <p>Tip</p> <p>When the [Obtain a Domain Name automatically] option is enabled in the TCP/IP settings, the domain name can be obtained using the DHCP server.  P.118 “Basic Setting”</p>
3	Security Method	<p>Enter the security method.</p> <ul style="list-style-type: none"> • None Select this to perform a non-secure DDNS update. • GSS-TSIG Select this to perform a secure DDNS session using GSS-TSIG. You must set a log-in name and a password. If both are not set, the secure DDNS session will not be available. • TSIG Select this to perform a secure DDNS session using TSIG. To select this, you must upload a key file and a private key file. If any of them is not uploaded, the security setting will be disabled. • SIG(0) Select this to perform a secure DDNS session using SIG(0). To select this, you must upload a key file and a private key file. If any of them is not uploaded, the security setting will be disabled.
4	Primary Login Name	Enter the primary login name if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
5	Primary Password	Enter the primary password if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
6	Secondary Login Name	Enter the secondary login name if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
7	Secondary Password	Enter the secondary password if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
8	TSIG/SIG(0) Key file	Use this setting to upload or delete a key file to be used for TSIG and SIG(0). To upload it, click [Choose File] and specify a private key file to be uploaded, and then click [Upload]. To delete it, click [Delete].
9	TSIG/SIG(0) Private Key file	Use this setting to upload or delete a private key file to be used for TSIG and SIG(0). To upload it, click [Choose File] and specify a private key file to be uploaded, and then click [Upload]. To delete it, click [Delete].

LLMNR / LLMNR (Secondary)

You need to set [LLMNR (Secondary)] for the secondary network when you use the two-channel networks.

The screenshot shows the 'Network - Basic Setting' window. On the left is a sidebar with various settings categories. The main area is divided into sections: 'Secondary DNS Server Address(Pv6)', 'DDNS', and 'LLMNR'. The 'LLMNR' section at the bottom has a dropdown menu currently set to 'Enable'. A red box and arrow labeled '1' point to this dropdown.

	Item name	Description
1	LLMNR	Select whether LLMNR is enabled or disabled. [Enable] is set as the default.

❑ Setting up Filtering

You can set filtering in order to restrict access from client computers to this equipment. Filtering can be specified with an IP address or a MAC address. You need to set [Secondary] for the secondary network when you use the two-channel network.

Note

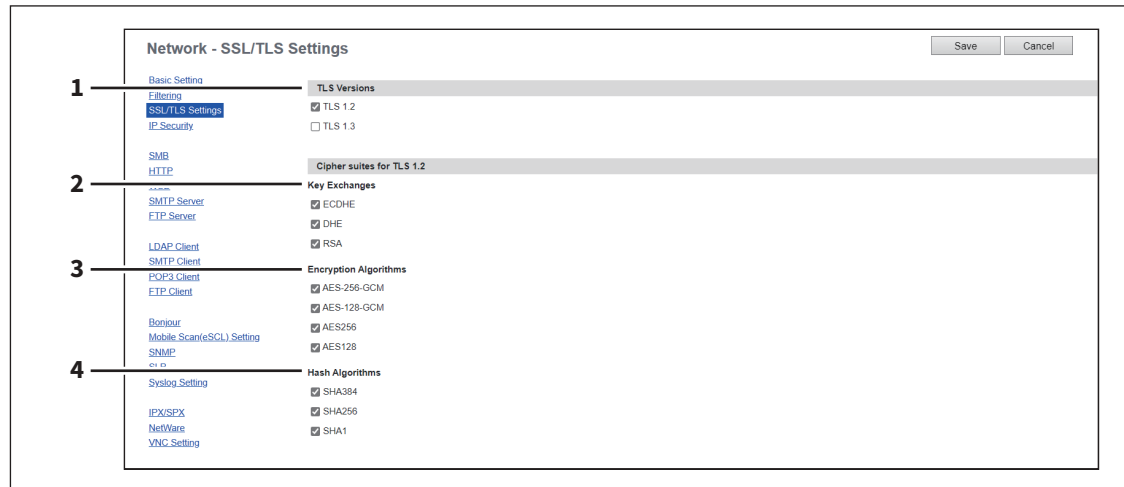
MAC address filtering is given priority over IP address filtering.

The screenshot shows the 'Network - Filtering' window. It has a sidebar on the left and a main area with two main sections: 'IP Filtering' and 'MAC Address Filtering'.
1. 'Enable IP Filtering' is set to 'Disable'.
2. 'IP Filtering Rule' is set to 'Permit'.
3. The 'IP Filtering' table has 10 filters. Each filter has columns for 'Start Address' (0, 0, 0, 0), 'End Address' (0, 0, 0, 0), and 'Port Number' (empty).
4. 'Apply the ICMP Filter' is set to 'Disable'.
5. 'Enable MAC Address Filtering' is set to 'Disable'.
6. 'MAC Address Filtering Rule' is set to 'Permit'.
7. The 'MAC Address Filtering' table has 10 filters. Each filter has a column for 'MAC Address' (empty).

	Item name	Description
1	Enable IP Filtering	<p>Select [Enable] for IP address filtering. When [Enable] is selected, access from devices on a network to which the IP address (specified in [IP Filtering]) is set is restricted under conditions set in [IP Filtering Rule]. [Disable] is set as the default.</p> <p>Note</p> <p>IP filtering is valid only in a network environment implemented with IPv4. It is not available in an IPv6 network environment. If you need to use IP address filtering under IPv6 environment, select MAC address filtering.</p>
2	IP Filtering Rule	<p>Select IP address filtering rules.</p> <ul style="list-style-type: none"> • Permit — Select this to permit access from devices on a network to which the IP address (specified in [IP Filtering]) is set. • Deny — Select this to deny access from devices to which the specified IP address is set.
3	IP Filtering	<p>Enter the start IP address, end IP address, and port number of the clients to apply IP filtering. Up to 10 addresses can be specified.</p> <p>Note</p> <p>Only IPv4 addresses are available. An IPv6 address cannot be specified.</p>
4	Apply the ICMP Filter	Specify [Enable] if you want to filter the Internet Control Message Protocol. The default is [Disable].
5	Enable MAC Address Filtering	Select [Enable] for MAC address filtering. When [Enable] is selected, access from devices on a network to which the MAC address (specified in [MAC Address Filtering]) is set is restricted under conditions set in [MAC Address Filtering Rule]. [Disable] is set as the default.
6	MAC Address Filtering Rule	<p>Select MAC address filtering rules.</p> <ul style="list-style-type: none"> • Permit — Select this to permit access from devices on a network to which the MAC address (specified in [MAC Address Filtering]) is set. • Deny — Select this to deny access from devices to which the specified MAC address is set.
7	MAC Address Filtering	Enter the MAC address of a target client computer for MAC address filtering. Up to 10 addresses can be specified.

❑ SSL/TLS Settings

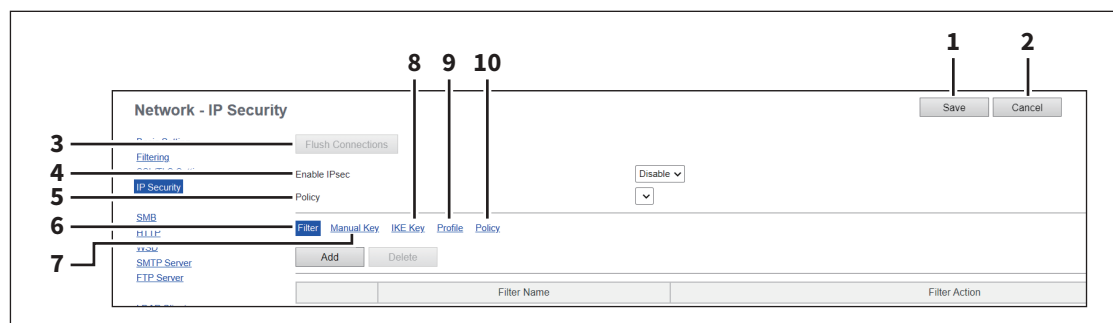
You can set the TLS version and the cipher suites for TLS 1.2 for SSL/TLS communications with the network servers



	Item name	Description
1	TLS Versions	Select the versions of TLS 1.2 and 1.3. Note <ul style="list-style-type: none"> You cannot deselect both versions at the same time, which causes impossible communications. If the different TLS versions are set for devices, it is impossible to communicate with each other.
2	Key Exchanges	Select the key exchange method for the TLS 1.2 cipher suite.
3	Encryption Algorithms	Select the encryption algorithm for the TLS 1.2 cipher suite.
4	Hash Algorithms	Select the hash algorithm for the TLS 1.2 cipher suite.

❑ Setting up IP Security

With the IP security function, you can enable data encryption communication using IPsec (IP Security Protocol).



	Item name	Description
1	[Save] button	Saves the IP Security setting.
2	[Cancel] button	Cancels the IP Security setting.
3	[Flush Connections] button	With the [Flush Connections] button, if the keys for IPsec communication are leaked or a security violation occurs, you can manually delete (flush) the current session with the flush connection function and start a new session. If you want to delete the information of SAD (Security Association Database) for any reason, you can delete it in the same way.

	Item name	Description
4	Enable IPsec	Specify whether or not to enable IPsec. <ul style="list-style-type: none"> • Enable — Enables IPsec. • Disable — Disables IPsec.
5	Policy	Select a policy to use in IPsec. To enable data encryption communication using IPsec, you must first create IPsec policies according to your system environment. P.141 “[Add Policy] / [Modify Policy] screen”
6	Filter	Creates a filter for the IPsec environment. [Add] button — You can add a filter on the [Add Filter] screen. P.132 “[Add Filter] / [Modify Filter] screen” [Delete] button — Select filters to delete and click the [Delete] button to delete them. Filter Name — Click a registered filter name to modify its content. P.132 “[Add Filter] / [Modify Filter] screen” Filter Action — Displays the action of the registered filter.
7	Manual Key	Set the IPsec manual key. [Add] button — You can add a manual key on the [Add Manual Key] screen. P.134 “[Add Manual Key] / [Modify Manual Key] screen” [Delete] button — Select manual keys to delete and click the [Delete] button to delete them. Manual Key Name — Click a registered manual key name to modify its content. P.134 “[Add Manual Key] / [Modify Manual Key] screen” Encryption Algorithm — Displays the registered encryption algorithms.
8	IKE Key	Set the IPsec IKE key. [Add] button — You can add an IKE key on the [Add IKE] screen. P.135 “[Add IKE] / [Modify IKE] screen” [Delete] button — Select keys to delete and click the [Delete] button to delete them. Key Name — Click a registered key name to modify its content. P.135 “[Add IKE] / [Modify IKE] screen” IKE Type — Displays the registered IKE types.
9	Profile	First create a filter and a manual key or IKE key according to your IPsec environment, and then create profiles by combining them. [Add] button — You can add a profile on the [Add Profile] screen. P.139 “[Add Profile] / [Modify Profile] screen” [Delete] button — Select profiles to delete and click the [Delete] button to delete them. Profile Name — Click a registered profile name to modify its content. P.139 “[Add Profile] / [Modify Profile] screen” Profile Mode — Displays the registered profile mode.
10	Policy	Create a policy to use in IPsec by combining the registered profiles. [Add] button — You can add a policy on the [Add Policy] screen. P.141 “[Add Policy] / [Modify Policy] screen” [Delete] button — Select policies to delete and click the [Delete] button to delete them. Policy Name — Click a registered policy name to modify its content. P.141 “[Add Policy] / [Modify Policy] screen”

[Add Filter] / [Modify Filter] screen

You can display this screen by clicking the [Add] button for Filter or a registered filter name.
You can create a filter to use in IPsec.

	Item name	Description
1	[OK] button	Saves the folder setting.
2	[Cancel] button	Cancels registration of the folder.
3	[Reset] button	Returns the settings to the defaults.
4	Filter Name	Enter a filter name. You can enter up to 63 alphanumeric characters and symbols other than #, %, &, +, \ (backslash), ' (apostrophe), ; (semicolon), , (comma), ", and =.
5	Internet Protocol Version	Select the IP version for IPsec. <ul style="list-style-type: none"> • IPv4 — Select this to use IPsec under the IPv4 environment. • IPv6 — Select this to use IPsec under the IPv6 environment.
6	Source Address	The IP address of this equipment is set as the source address to which the filter is applied. [My IP Address] is displayed in this box. This item cannot be changed.

	Item name	Description
7	Destination Address	<p>Specify the destination address for the communication to which the filter is applied.</p> <ul style="list-style-type: none"> • Specific IP Address — Set a specific IP address. Enter the IP address in the address input box. • Subnet / Prefix — Set the destination with its IP address and subnet mask. Enter the IP address and the prefix of the subnet mask directly in the address input box. • FQDN — Sets FQDN for the destination. Enter FQDN in the address input box. You can enter up to 255 alphanumerical characters including hyphen (-) and period (.). However, neither hyphen (-) nor period (.) can be used as first or last character. • Any IP Address — Set any IP address.
8	Protocol Type	<p>Select a protocol for the filter.</p> <ul style="list-style-type: none"> • Any — Set any protocol. • TCP — Select this to use TCP only. • UDP — Select this to use UDP only. • ICMP — Select this to use ICMP only.
9	Source Port	<p>Specify the source port number. This setting is available only if you selected TCP or UDP in the protocol type setting.</p> <ul style="list-style-type: none"> • Any — Set any source port. • Port Number — Set the port number of the sender. Enter the port number in the port number input box.
10	Destination Port	<p>Set the destination port number. This setting is available only if you selected TCP or UDP in the protocol type setting.</p> <ul style="list-style-type: none"> • Any — Set any destination port. • Port Number — Set the port number of the destination. Enter the port number in the port number input box.
11	Filter Action	<p>Set the operation of the filter.</p> <ul style="list-style-type: none"> • Permit — Select this to permit access from the specified destination. • Block — Select this to block access from the specified destination. • Negotiate Security — IPsec communication is performed with the specified destination. When this item is set, you must select the security protocol type to be used in IPsec communication from the following: <ul style="list-style-type: none"> - ESP — Select this to use ESP (Encapsulating Security Payload). - AH — Select this to use AH (Authentication Header).

[Add Manual Key] / [Modify Manual Key] screen

You can display this screen by clicking the [Add] button for Manual Key or a registered manual key name.
You can set a manual key to use in IPsec.

	Item name	Description
1	[OK] button	Saves the key setting.
2	[Cancel] button	Cancels registration of the key.
3	[Reset] button	Returns the settings to the defaults.
4	Manual Key Name	Enter the name of the manual key. You can enter up to 63 alphanumerical characters and symbols other than #, %, &, +, \ (backslash), ' (apostrophe), ; (semicolon), , (comma), ", and =.
5	Encryption Algorithm	Select an encryption algorithm. <ul style="list-style-type: none"> • None — Select this not to perform data encryption. • AES-256-CBC — Select this to use AES-CBC (256 bits). • AES-192-CBC — Select this to use AES-CBC (192 bits). • AES-128-CBC — Select this to use AES-CBC (128 bits). • 3DES-CBC — Select this to use 3DES-CBC. • DES-CBC — Select this to use DES-CBC.
6	Hash Algorithm	Select a hash algorithm. <ul style="list-style-type: none"> • SHA1 — Select this to use SHA1. • MD5 — Select this to use MD5. • AES-XCBC-MAC — Select this to use AES-XCBC-MAC.

	Item name	Description
7	Inbound Key	Select a key for the receiving side.
	Security Parameter Index	Specify a security parameter index (SPI) for identification. You can enter a value in the range from 256 to 4095.
	ESP Encryption Key	Enter an ESP (Encapsulating Security Payload) encryption key.
	ESP Authentication Key	Enter an ESP (Encapsulating Security Payload) authentication key.
	AH Authentication Key	Enter an AH (Authentication Header) authentication key.
8	Outbound Key	Select a key for the destination.
	Security Parameter Index	Specify a security parameter index (SPI) for identification. You can enter a value in the range from 256 to 4095.
	ESP Encryption Key	Enter an ESP (Encapsulating Security Payload) encryption key.
	ESP Authentication Key	Enter an ESP (Encapsulating Security Payload) authentication key.
	AH Authentication Key	Enter an AH (Authentication Header) authentication key.

[Add IKE] / [Modify IKE] screen

You can display this screen by clicking the [Add] button for IKE Key or a registered key name.

You can set an IKE key to use in IPsec.

The screenshot shows the 'Add IKE' configuration window. It has a title bar 'Add IKE' with 'OK' and 'Cancel' buttons (labeled 1 and 2). Below the title bar is a 'Reset' button (labeled 3) and a message: 'Selecting 'Save' in the Main Window is required to Save the new settings.' Below this is the 'IKE Key Name' text field (labeled 4). The 'General Setting' section (labeled 5) includes 'IKE Version' with radio buttons for 'IKEv1 (Main Mode)' (selected) and 'IKEv2'. Under 'IKEv1', there are radio buttons for 'Authentication Method' with 'Certificate' (selected) and 'Preshared Key'. A note states: '[Note: This selection will be applicable for all IKEv1 settings]'. Under 'IKEv2', there are radio buttons for 'Authentication Method' with 'Certificate' (selected) and 'Preshared Key'. The 'Preshared Key' section includes 'Local ID' and 'Remote ID' dropdown menus, each with an 'IP Address' text field. The 'Session Key Settings' section (labeled 6) includes 'Generate a new key after' with a text field '28800' and a unit '/Seconds', and a checkbox 'Enable PFS'. The 'FilterIKE Transforms' section (labeled 7) includes 'Integrity' with checkboxes for 'SHA1' (checked), 'SHA256', 'SHA384', and 'AES-XCBC-MAC'; 'Encryption' with checkboxes for 'AES-256-CBC', 'AES-192-CBC', 'AES-128-CBC' (checked), 'AES-CTR', and '3DES-CBC' (checked); and a 'Diffie-Hellman algorithm' dropdown menu set to 'MODP 1024 (Group 2)'.

The screenshot shows the 'Modify IKE' dialog box. At the top right, there are 'OK' and 'Cancel' buttons, with callout 1 pointing to 'OK' and callout 2 pointing to 'Cancel'. On the left side, there is a 'Reset' button with callout 3. Below it is the 'IKE Key Name' text field with callout 4, containing the text 'IKEKeyName001'. The main area is divided into sections: 'General Setting' (callout 5) with 'IKE Version' set to 'IKEv1 (Main Mode)', 'Authentication Method' set to 'Preshared Key', and a password field; 'Session Key Settings' (callout 6) with 'Generate a new key after' set to '28800 /Seconds' and 'Enable PFS' unchecked; and 'FilterIKE Transforms' (callout 7) with 'Integrity' set to 'SHA1', 'Encryption' set to 'AES-128-CBC' and '3DES-CBC', and 'Diffie-Hellman algorithm' set to 'MODP 1024 (Group 2)'. There are also 'Local ID' and 'Remote ID' dropdown menus.

	Item name	Description
1	[OK] button	Saves the key setting.
2	[Cancel] button	Cancels registration of the key.
3	[Reset] button	Returns the settings to the defaults.
4	IKE Key Name	<p>Enter the name of the IKE key. You can enter up to 63 alphanumerical characters and symbols other than #, %, &, +, \ (backslash), ' (apostrophe), ; (semicolon), , (comma), ", and =.</p> <div>Tip</div> <p>Up to 30 IKE keys can be created.</p>

	Item name	Description
5	General Setting	
	IKEv1 (Main Mode)	<p>Select this to use IKEv1.</p> <p>Certificate — Select this to use an electronic certificate. To select this, IPsec certificate must be installed in this equipment in advance.</p> <p>Preshared Key — Select this to perform authentication by sharing key information with the recipient of the communication in advance. Enter key information to be shared in the entry box. You can enter up to 128 alphanumerical characters and symbols other than &, <, and “.</p> <p>Note</p> <p>If you register more than one Preshared Key for IKEv1, only the one that you registered last will be valid.</p>
	IKEv2	<p>Select this to use IKEv2.</p> <p>Certificate — Select this to use an electronic certificate. To select this, IPsec certificate must be installed in this equipment in advance.</p> <p>Preshared Key — Select this to perform authentication by sharing key information with the recipient of the communication in advance. Enter key information to be shared in the entry box. You can enter up to 128 alphanumerical characters and symbols other than &, <, and “.</p> <ul style="list-style-type: none"> • Local ID — Select among IP Address, FQDN, Email and Key-ID. When you have selected the Key-ID, enter the value to the corresponding item. You can enter up to 128 alphanumerical characters and symbols other than &, <, and “. • Remote ID — Select among IP Address, FQDN, Email and Key-ID. When you selected FQDN, Email or Key-ID, enter a value corresponding to the item you selected. When you selected Key-ID, enter the corresponding value. You can enter up to 128 alphanumerical characters and symbols except the following: & < “. When you selected Email, you can enter up to 192 alphanumerical characters. When you selected FQDN, you can enter up to 255 alphanumerical characters including hyphen (-) and period (.). However, neither hyphen (-) nor period (.) can be used as first or last character.
6	Session Key Settings	
	Generate a new key after	<p>Enter the interval between generating key information for IPsec communications in seconds. Set the interval period for regenerating key information for IPsec communication from 60 seconds to 604,800 seconds (7 days).</p> <p>Enable PFS — Select the check box when using the PFS (Perfect Forward Secrecy) function in IKE.</p>

	Item name	Description
7	FilterIKE Transforms	
	Integrity	Select the authentication algorithm to be used in IKE. <ul style="list-style-type: none"> • SHA1 — Select this to use SHA1. • SHA256 — Select this to use SHA256. • SHA384 — Select this to use SHA384. • AES-XCBC-MAC — Select this to use AES-XCBC-MAC.
	Encryption	Select the encryption algorithm to be used in IKE. <ul style="list-style-type: none"> • AES-256-CBC — Select this to use AES-CBC (256 bits). • AES-192-CBC — Select this to use AES-CBC (192 bits). • AES-128-CBC — Select this to use AES-CBC (128 bits). • AES-CTR — Select this to use AES-CTR. • 3DES-CBC — Select this to use 3DES-CBC.
	Diffie-Hellman algorithm	Select the Diffie-Hellman group to be used in IKE. <ul style="list-style-type: none"> • MODP 768 (Group 1) — Select this to use the MODP group in 768 bits. • MODP 1024 (Group 2) — Select this to use the MODP group in 1024 bits. • MODP 2048 (Group 14) — Select this to use the MODP group 14 in 2048 bits. • MODP 2048 (Group 24) — Select this to use the MODP group 24 in 2048 bits. • Elliptic Curve P-256 (Group 19) — Select this to use Elliptic Curve P-256. • Elliptic Curve P-384 (Group 20) — Select this to use Elliptic Curve P-384. • Elliptic Curve P-521 (Group 21) — Select this to use Elliptic Curve P-521.

[Add Profile] / [Modify Profile] screen

You can display this screen by clicking the [Add] button for Profile or a registered profile name.

You can create a profile for an IPsec environment by combining the registered filter and either a manual key or an IKE key.

The 'Add Profile' dialog box contains the following elements:

- 1**: OK button
- 2**: Cancel button
- 3**: Reset button
- 4**: IKE Profile Name text field
- 5**: Tunnel Settings section, including Tunnel mode (No) and IPv4/IPv6 Address text field.
- 6**: Key Selection section, including Key dropdown menu (IKEKeyName001(IKEv1)).
- 7**: Proposals section, including ESP Transforms (Integrity: SHA1, AES-XCBC, AES-128-GCM, AES-192-GCM, AES-256-GCM; Encryption: AES-256-CBC, AES-192-CBC, AES-128-CBC, AES-128-GCM, AES-192-GCM, AES-256-GCM, AES-CTR, 3DES-CBC, None), AH Transforms (Integrity: SHA1, SHA256, AES-XCBC), and Session Key Settings (Generate a new key after: 3600 /Seconds, 100000 /KBytes).
- 8**: IP Filter section, including Move Up and Move Down buttons, and a table with columns: Move, Filter Name, Filter Action, Destination Address.

Move		Filter Name	Filter Action	Destination Address
<input type="radio"/>	<input type="checkbox"/>	FilterName001	Negotiate Security	Any IP Address
<input type="radio"/>	<input type="checkbox"/>	FilterName002	Negotiate Security	Any IP Address

The 'Modify Profile' dialog box contains the following elements:

- 1**: OK button
- 2**: Cancel button
- 3**: Reset button
- 4**: IKE Profile Name text field (ProfileName001)
- 5**: Tunnel Settings section, including Tunnel mode (No) and IPv4/IPv6 Address text field.
- 6**: Key Selection section, including Key dropdown menu (IKEKeyName001(IKEv1)).
- 7**: Proposals section, including ESP Transforms (Integrity: SHA1, AES-XCBC, AES-128-GCM, AES-192-GCM, AES-256-GCM; Encryption: AES-256-CBC, AES-192-CBC, AES-128-CBC, AES-128-GCM, AES-192-GCM, AES-256-GCM, AES-CTR, 3DES-CBC, None), AH Transforms (Integrity: SHA1, SHA256, AES-XCBC), and Session Key Settings (Generate a new key after: 3600 /Seconds, 100000 /KBytes).
- 8**: IP Filter section, including Move Up and Move Down buttons, and a table with columns: Move, Filter Name, Filter Action, Destination Address.

Move		Filter Name	Filter Action	Destination Address
<input type="radio"/>	<input checked="" type="checkbox"/>	FilterName001	Negotiate Security	Any IP Address
<input type="radio"/>	<input type="checkbox"/>	FilterName002	Negotiate Security	Any IP Address

	Item name	Description
1	[OK] button	Saves the profile setting.
2	[Cancel] button	Cancels registration of the profile.
3	[Reset] button	Returns the settings to the defaults.

	Item name	Description
4	IKE Profile Name	<p>Enter the profile name. You can enter up to 63 alphanumerical characters, including hyphen (-) and underscore (_).</p> <p>Tip Up to 30 profiles can be created.</p>
5	Tunnel Settings	
	Tunnel mode	<p>Select whether or not to use tunnel mode for IPsec communications.</p> <ul style="list-style-type: none"> • Yes — Select this to use the tunnel mode. • No — Select this not to use the tunnel mode. (The transport mode will be used instead.)
	IPv4/IPv6 Address	Enter the IP address for the gateway which encrypts and decrypts data in tunnel mode.
6	Key Selection	
	Key	Displays the IKE key settings registered in the equipment. IKE keys already registered in this equipment are displayed.
7	Proposals	
	ESP Transforms	<p>Specify the transform for ESP.</p> <ul style="list-style-type: none"> • Integrity — Selects the authentication algorithm to be used in ESP. <ul style="list-style-type: none"> - SHA1 — Select this to use SHA1. - AES-XCBC — Select this to use AES-XCBC. - AES-128-GCM — Select this to use AES-128-GCM. - AES-192-GCM — Select this to use AES-192-GCM. - AES-256-GCM — Select this to use AES-256-GCM. • Encryption — Selects the encryption algorithm to be used in ESP. <ul style="list-style-type: none"> - AES-256-CBC — Select this to use AES-CBC (256 bits). - AES-192-CBC — Select this to use AES-CBC (192 bits). - AES-128-CBC — Select this to use AES-CBC (128 bits). - AES-128-GCM — Select this to use AES-GCM (128 bits). - AES-192-GCM — Select this to use AES-192-GCM. - AES-256-GCM — Select this to use AES-256-GCM. - AES-CTR — Select this to use AES-CTR. - 3DES-CBC — Select this to use 3DES-CBC. - None — Select this not to perform data encryption.
	AH Transforms	<p>Specify the transform for AH.</p> <ul style="list-style-type: none"> • Integrity — Selects the authentication algorithm to be used in AH. <ul style="list-style-type: none"> - SHA1 — Select this to use SHA1. - AES-XCBC — Select this to use AES-XCBC.
	Session Key Settings	<p>Specify the session key for IPsec communications.</p> <ul style="list-style-type: none"> • Session Key Settings — Sets an interval for regenerating the session key. The interval can be set in time or the amount of data. Select the desired check box and then key in the value in the entry box. <ul style="list-style-type: none"> - Generate a new key after []/Seconds — Specify the interval between key generations in seconds. Specify within the range from 180 to 86,400 seconds (24 hours). - Generate a new key after []/KBytes — Specify the data volume between key generations in Kbytes. Specify within the range from 20,480 to 214,783,647 Kbytes.
	IPCOMP Transform	Select if using the IPCOMP transform.

	Item name	Description
8	IP Filter	You can display a list of filter settings registered in this equipment. Select the check box for the filter to be applied to the profile. If more than one filter is registered, you can change their order in the list. Click [Move] for the desired filter, and then click [Move Up] or [Move Down] to move the filter.

[Add Policy] / [Modify Policy] screen

You can display this screen by clicking the [Add] button for Policy or a registered policy name.

You can create a policy to use in IPsec by combining the registered profiles.

	Item name	Description
1	[OK] button	Saves the profile setting.
2	[Cancel] button	Cancels registration of the profile.
3	Policy Name	Enter the policy name. You can enter up to 63 alphanumerical characters and symbols other than #, %, &, +, \ (backslash), ' (single quotation), ; (semicolon), , (comma), " (double quotation) and =. <div style="border: 1px solid gray; padding: 2px; width: fit-content;">Tip</div> Up to 10 policies can be created.
4	Profile Name	Select profiles to apply to the policy. You can select multiple profiles.


❑ Setting up SMB


In SMB, you can specify the SMB network properties to access this equipment through a Microsoft Windows Network and enable SMB printing. When you enable the SMB, users can also browse the local folder in the equipment. You can also specify the WINS server when the WINS server is used to enable the Windows print sharing and Windows file sharing services between the different subnets.

The screenshot shows the 'Network - SMB' configuration window. On the left, a sidebar lists various network settings, with 'SMB' highlighted. The main area is divided into several sections:

- SMB**: Contains settings for SMB Server Protocol (Enable), SMB 1.0 Support for Server (Enable), SMB 1.0 Support for Client (Enable), Restriction (None), NetBIOS Name (Workgroup), and Logon (Workgroup).
- Authentication of SMB Server**: Contains Guest Logon (Enable), User Name, and Password.
- Authentication of SMB Client**: Contains SMB Client Authentication (Kerberos/NTLMv2).
- SMB Signing of SMB Server**: Contains radio button options for digital signature.
- SMB Signing of SMB Client**: Contains radio button options for digital signature.

	Item name	Description
1	SMB Server Protocol	Select whether the SMB protocol is enabled or disabled. <ul style="list-style-type: none"> • Enable — Select this to enable SMB. • Disable — Select this to disable SMB.
2	SMB 1.0 Support for Server	Select whether to support SMB 1.0 for the server. <ul style="list-style-type: none"> • Enable — Select this to enable SMB 1.0 for the server. • Disable — Select this to disable SMB 1.0 for the server.
3	SMB 1.0 Support for Client	Select whether to support SMB 1.0 for the client. <ul style="list-style-type: none"> • Enable — Select this to enable SMB 1.0 for the client. • Disable — Select this to disable SMB 1.0 for the client.
4	Restriction	Specify restrictions on SMB. <ul style="list-style-type: none"> • None — Select this to not specify restrictions on SMB. • Print Share — Select this to enable the file sharing service using SMB, but disable SMB printing. • File Share — Select this to enable SMB printing, but disable the file sharing service using SMB.

	Item name	Description
5	NetBIOS Name	<p>Enter the NetBIOS name of this equipment. The equipment uses “MFP<NIC Serial Number>” as the default NetBIOS name.</p> <p>Note</p> <p>You can enter only alphanumerical characters and “-” (a hyphen) for NetBIOS names. If you use any other characters, a warning message will be displayed.</p>
6	Logon	<p>Enter the workgroup or domain that this equipment joins.</p> <ul style="list-style-type: none"> • Workgroup — To include the equipment in the workgroup, enter the workgroup name. All client computers can access this equipment without a user name and password. • Domain — Select this and enter the domain name when the equipment will log on in the domain. Any client computers which are not members of the domain will need a valid user name and password to access this equipment. Use this to enhance access security to this equipment. <p>Note</p> <p>For workgroup and domain names, you can use only alphanumerical characters and symbols other than the following: ; : " < > + = \ ? , * # If you use any other characters, a warning message will be displayed.</p>
7	Primary Domain Controller	<p>Specify the server name or IP address of the primary domain controller when this equipment will log on the domain network. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</p>
8	Backup Domain Controller	<p>Specify the server name or IP address of the backup domain controller when this equipment will log on the domain network, if required. If the Primary Domain Controller is unavailable, the Backup Domain Controller will be used to log on. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</p> <p>Note</p> <p>If the wrong primary or backup domain controller is specified, the NETWORK INITIALIZING message will be displayed for up to 4 minutes while the equipment searches for the primary or backup domain controller. In that case, correct the primary or backup domain controller setting after the NETWORK INITIALIZING message disappears.</p>
9	Logon User Name	<p>Enter a valid user name to log on to the specified domain. You can enter up to 128 alphanumerical characters and symbols other than " / \ [] : ; = , + * ? < > .</p>
10	Password	<p>Enter the password for the specified log on user name to log on the domain network. You can enter up to 128 alphanumerical characters.</p>
11	Primary WINS Server	<p>Specify the IP address of the primary WINS server when the WINS server is used to provide the NetBIOS name in your local area network. This option would be more useful to access this equipment using the NetBIOS Name from a different subnet.</p> <p>Tip</p> <p>When the [Obtain a WINS Server Address automatically] option is enabled in the TCP/IP settings, the primary and secondary WINS server address can be obtained using the DHCP server.</p> <p> P.118 “Basic Setting”</p>

	Item name	Description
12	Secondary WINS Server	<p>Specify the IP address of the secondary WINS server as you require when the WINS server is used to provide NetBIOS name in your local area network. If the Primary WINS Server is unavailable, the Secondary WINS Server will be used.</p> <p>Tip</p> <p>When the [Obtain a WINS Server Address automatically] option is enabled in the TCP/IP settings, the primary and secondary WINS server address can be obtained using the DHCP server.</p> <p> P.118 “Basic Setting”</p> <p>Note</p> <p>If “0.0.0.0” is entered for the Primary WINS Server and Secondary WINS Server, this equipment will not use the WINS server.</p>
13	Host announcement sending of super sleep mode	<p>Specify this to display this equipment’s icon in the “Network” folder on the Windows computer even in super sleep mode.</p> <ul style="list-style-type: none"> • Disable: Disables host announcement sending in super sleep mode. • Enable: Even in super sleep mode, the icon for this printer is displayed in the “Network” folder on Windows computers. <p>Note</p> <p>When the printer’s super sleep mode is set to [Disable], the icon for this printer is displayed in the “Network” folder on Windows computers regardless of this setting.</p>
14	Guest Logon	<p>Select whether a guest user can log on to the SMB server. [Enable] is set as the default.</p>
15	User Name	<p>Enter a name of the user who logs on to the SMB server if [Guest Logon] is set to [Disable]. You can enter up to 32 alphanumerical characters and symbols except " / \ [] : ; = , + * ? < > .</p> <p>Note</p> <p>If you connect to the SMB server for this equipment before changing the user name, qualification information on the user name and the password is cached in your Windows computer. Restart your Windows computer to clear qualification information.</p>
16	Password	<p>Enter a password of the specified user if [Guest Logon] is set to [Disable]. You can enter up to 128 alphanumerical characters and symbols.</p> <p>Note</p> <p>If you connect to the SMB server for this equipment before changing the password, qualification information on the user name and the password is cached in your Windows computer. Restart your Windows computer to clear qualification information.</p>

	Item name	Description
17	SMB Client Authentication	<p>Specify the authentication method for the SMB clients.</p> <ul style="list-style-type: none"> • Kerberos/NTLMv2 — Specify this when connecting to an SMB server using Kerberos/NTLMv2 authentication. NTLMv2 authentication is used if Kerberos authentication has failed. • Kerberos/NTLMv1 — Specify this when connecting to an SMB server using Kerberos/NTLMv1 authentication. NTLMv1 authentication is used if Kerberos authentication has failed. • Kerberos — Specify this when connecting to an SMB server using Kerberos authentication. • NTLMv2 — Specify this when connecting to an SMB server using NTLMv2 authentication. • NTLMv1 — Specify this when connecting to an SMB server using NTLMv1 authentication. <p>Note</p> <p>SMB servers running macOS 10.12 or later do not support NTLMv1 authentication.</p>
18	SMB Signing of SMB Server	<p>Select whether SMB Signing is enabled or disabled when a client accesses this equipment using SMB, such as when a client accesses the shared folder in this equipment.</p> <ul style="list-style-type: none"> • If client agrees, digital signature is done for the communication. — Select this to use the digital signature to secure communication only when a client accesses this equipment with a digital signature. Even if a client accesses this equipment without a digital signature, the communication is allowed without the digital signature. • Digital signature is always done for the communication on the server side. — Select this to allow the communication only when a client accesses this equipment with a digital signature. When a client accesses this equipment without a digital signature, the communication is not allowed. • Digital signature isn't done for the communication for the server. — Select this to allow the communication only when a client accesses this equipment without a digital signature. When a client is set to always access an SMB server with a digital signature, the communication is not allowed. <p>Note</p> <p>If you do not know whether the SMB Signing of SMB Client is enabled or disabled in the client computers, it is recommended to select [If client agrees, digital signature is done for the communication.]. If this is set incorrectly, the SMB communication may become unavailable.</p>

	Item name	Description
19	SMB Signing of SMB Client	<p>Select whether SMB Signing is enabled or disabled when this equipment accesses the clients using SMB, such as when this equipment stores the scanned data in the network folder using SMB.</p> <ul style="list-style-type: none"> • If server agrees, digital signature is done for the communication. — Select this to use the digital signature to secure the communication to an SMB server only when the SMB Signing of SMB Server that this equipment accesses is enabled. If the SMB Signing of SMB Server is disabled in an SMB server, the communication is performed without the digital signature. • Digital signature is always done for the communication on the client side. — Select this to make this equipment always access an SMB server with a digital signature. When the SMB Signing of SMB Server is disabled in an SMB server, the communication is not allowed. • Digital signature isn't done for the communication for the client. — Select this to communicate to an SMB server without the digital signature. If the SMB Signing of SMB Server is always enabled in an SMB server, the communication is not allowed. <p>Note</p> <ul style="list-style-type: none"> • If you do not know whether the SMB Signing of SMB Server is enabled or disabled in the SMB servers, it is recommended to select [If server agrees, digital signature is done for the communication.]. If this is set incorrectly, the SMB communication may become unavailable. • The digital signature is always done for the communication on the server side as the default on Windows Server 2012 or later. Therefore specify “If server agrees, digital signature is done for the communication.” or “Digital signature is always done for the communication on the client side.” for SMB communications with Windows Server 2012 or later.

□ Setting up HTTP

In HTTP, you can enable or disable Web-based services such as TopAccess and e-Filing web utility.

	Item name	Description
1	Enable HTTP Server	Select whether the Web-based services such as TopAccess and e-Filing web utility are enabled or disabled. [Enable] is set as the default.
2	Enable SSL/TLS	<p>Select whether the SSL (Secure Socket Layer)/TLS (Transport Layer Security) is enabled or disabled. When this is enabled, the data transferred between the equipment and client computers will be encrypted using a private key when operating TopAccess and e-Filing web utility. [Disable] is set as the default.</p> <p>Note</p> <p>Not all operating systems support SSL/TLS for all protocols.</p>

	Item name	Description
3	Primary Port Number	<p>Enter the port number for the NIC HTTP server. You can enter a value in the range from 1 to 65535. Generally the default value “80” is used.</p> <p>Note</p> <p>The same port numbers as the ones for the following settings are not usable. Change the applicable port number before that for the Primary Port Number is set.</p> <ul style="list-style-type: none"> • HTTP Network Service / Secondary Port Number • HTTP Network Service / SSL/TLS Port Number • IPP Print / Port Number • IPP Print / SSL/TLS Port Number
4	Secondary Port Number	<p>Enter the port number for TopAccess and the e-Filing web utility. You can enter a value in the range from 1 to 65535. Generally the default value “8080” is used.</p> <p>Note</p> <p>The same port numbers as the ones for the following settings are not usable. Change the applicable port number before that for the Secondary Port Number is set.</p> <ul style="list-style-type: none"> • HTTP Network Service / Primary Port Number • HTTP Network Service / SSL/TLS Port Number • IPP Print / Port Number • IPP Print / SSL/TLS Port Number
5	SSL/TLS Port Number	<p>Enter the port number for the SSL/TLS. You can enter a value in the range from 1 to 65535. Generally the default value “10443” is used.</p> <p>Note</p> <p>The same port numbers as the ones for the following settings are not usable. Change the applicable port number before that for the SSL/TLS Port Number is set.</p> <ul style="list-style-type: none"> • HTTP Network Service / Primary Port Number • HTTP Network Service / Secondary Port Number • IPP Print / Port Number • IPP Print / SSL/TLS Port Number

❑ Setting up WSD

In WSD, you can set the Web Services Setting. The Web Services Print operations and Web Services Scan operations are performed on client computers with Windows through a network.

	Item name	Description
1	Enable SSL/TLS	Specify whether or not to use SSL/TLS in Web Service. <ul style="list-style-type: none"> • Enable — Select this to use SSL/TLS. • Disable — Select this no to use SSL/TLS.
2	Friendly Name	Assign the friendly name for this equipment. You can enter up to 127 characters and symbols other than =, ; (semicolon), #, /, \ (backslash), :, *, ?, “, >, <, , !, and , (comma).
3	Web Services Print	Select whether the Web Services Print is enabled or disabled. <ul style="list-style-type: none"> • Enable — Select this to enable the Web Services Print. • Disable — Select this to disable the Web Services Print. <div style="background-color: #333; color: white; padding: 2px; margin-top: 10px;">Note</div> <p>To enable Web Services Print using SSL/TLS, a certificate must be installed in this equipment or a client computer. For the details, see the reference below: 📖 P.396 “Installing Certificates”</p>
4	Printer Name	Assign the printer name for this equipment. You can enter up to 127 characters and symbols other than =, ; (semicolon), #, /, \ (backslash), :, *, ?, “, >, <, and . “MFP model name-Serial number” is set as the default.
5	Printer Information	Assign the printer information for this equipment. You can enter up to 127 characters other than =, ; (semicolon), #, and \ (backslash).
6	Web Services Scan	Select whether the Web Services Scan is enabled or disabled. <ul style="list-style-type: none"> • Enable — Select this to enable the Web Services Scan. • Disable — Select this to disable the Web Services Scan.
7	Scanner Name	Assign the scanner name for this equipment. You can enter up to 127 characters and symbols other than =, ; (semicolon), #, /, \ (backslash), :, *, ?, “, >, <, and . “MFP model name-Serial number” is set as the default.
8	Scanner Information	Assign the scanner information for this equipment. You can enter up to 127 characters other than =, ; (semicolon), #, and \ (backslash).

	Item name	Description
9	Authentication for PC Initiated Scan	<p>Specify whether to enable user authentication before accepting a scan from a client computer.</p> <ul style="list-style-type: none"> • Do not accept any job — Select this not to accept any jobs regardless of the result of user authentication. • Accept the job if user name is valid — Select this to accept jobs only after successful user authentication. • Accept any job — Select this to accept any jobs regardless of the result of user authentication.

❑ Setting up SMTP Server

In SMTP Server, you can enable or disable SMTP transmission for receiving the Internet Fax and E-mails. This function is usually set when you want to enable the Offramp Gateway feature.

	Item name	Description
1	Enable SMTP Server	Select whether this equipment works as an SMTP server or not. This must be enabled when you use the Offramp Gateway feature. When this is enabled, this equipment can receive Internet Faxes or E-mails that are forwarded through the SMTP to the domain of this equipment. [Enable] is set as the default.
2	Port Number	<p>Enter the port number to transmit an Internet Faxes or E-mails. Generally "25" is used.</p> <p>Note</p> <p>When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you make a mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.</p>
3	Email Address	Enter the E-mail address of this equipment. When this equipment works as an SMTP server, it can receive all Internet Faxes and E-mails that contain its domain name. If the E-mail address of the received document matches the address you set here, this equipment prints it. You can enter up to 192 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
4	Enable OffRamp Gateway	Select whether the OffRamp Gateway transmission is enabled or disabled. [Disable] is set as the default.
5	OffRamp Security	Select whether the Offramp Security is enabled or disabled. When this is enabled, this equipment cancels the offramp gateway transmissions that are forwarding to the fax numbers not registered in the Address Book of this equipment. This can prevent the unauthorized offramp gateway transmission. [Enable] is set as the default.

	Item name	Description
6	OffRamp Print	Select whether this equipment should print documents sent using the offramp gateway transmission. When this is enabled, this equipment automatically prints documents sent using offramp gateway transmission, so that they can be confirmed. [Enable] is set as the default.

❏ Setting up FTP Server

In FTP Server, you can enable or disable the FTP server functions.

The screenshot shows the 'Network - FTP Server' configuration window. On the left, a list of settings is shown with numbered arrows: 1 points to 'Basic Setting', 2 to 'Enable FTP Server', 3 to 'Enable SSL/TLS', and 4 to 'Default Port Number'. The 'Basic Setting' is selected. On the right, there are two dropdown menus: 'Enable' and 'Disable'. Below them are two input fields: '21' and '990'. At the top right, there are 'Save' and 'Cancel' buttons.

	Item name	Description
1	Enable FTP Server	<p>Select whether the FTP server is enabled or disabled. Select [Enable] to enable the following functions.</p> <ul style="list-style-type: none"> • FTP printing • Reading/writing the address book data using the AddressBook Viewer • Backing up/Restoring the e-Filing data using the e-Filing Backup/Restore Utility <p>[Enable] is set as the default.</p>
2	Enable SSL/TLS	<p>Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for the FTP server. [Disable] is set as the default.</p> <p>Note</p> <p>Not all operating systems support SSL/TLS for all protocols.</p>
3	Default Port Number	<p>Enter the port number for the FTP server. You can enter a value in the range from 1 to 65535. Generally the default value “21” is used.</p> <p>Note</p> <p>When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you set it by mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.</p>
4	SSL/TLS Port Number	<p>Enter the port number that is used to access this equipment using FTP with SSL/TLS. The port number depends on the port setting in the FTP server. You can enter a value in the range from 1 to 65535. Generally the default value “990” is used.</p> <p>Note</p> <p>When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you set it by mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.</p>

LDAP Client settings

You can register the directory service properties of the LDAP (Lightweight Directory Access Protocol) server. When a new directory service is added, the users can search destinations using the LDAP server.

	Item name	Description
1	[New] button	Registers the LDAP server that provides a directory service. P.152 “[Create LDAP Information]/[Edit LDAP Information] screen”
2	Directory Service List	Displays a list of registered LDAP servers. You can edit the registered details by clicking a directory service name. P.152 “[Create LDAP Information]/[Edit LDAP Information] screen”
3	Search Method	Select search conditions for LDAP searching. <ul style="list-style-type: none"> Partial match — Select this to search information partially matching the search conditions. Prefix match — Select this to search information that starts with contents matching the search conditions. Suffix match — Select this to search information that ends with contents matching the search conditions. Full match — Select this to search information fully matching the search conditions.
4	[Server Assignment] button	Registers the search target server. P.154 “[Server Assignment] screen”
5	[Move Up]/[Move Down] button	Moves up and down in the search list.

[Create LDAP Information]/[Edit LDAP Information] screen

You can display this screen by clicking a directory service name in the directly service list or the [New] button.

Directory Service Properties

Create LDAP Information

Reset Delete Save Cancel

*Required

Directory Service Basic Properties

1 Connection Test Execute

2 *Directory Service Name

3 *Server IP Address

4 *Port Number 389

5 Server Type Windows Server

6 Authentication Auto

7 Search Base

8 User Name

9 Password

10 Search Timeout 1

11 Enable SSL/TLS Disable

12 SSL/TLS Port Number 636

13 Attribute type for Search Contact

*First Name givenName

*Last Name sn

*Email Address mail

*Fax Number facsimileTelephoneNumber

*Company company

*Department department

14 Attribute type for Authentication

User Authentication

Attribute type of 'User Name' displayName Default Value

Attribute type of 'Server Name' eBMServerName

*The value registered in this attribute is used for the server name of login user when logging in with Card or PIN.

PIN Code Authentication Setting

Attribute type of "PIN" eBMUserPIN

Card Authentication


Attribute type of 'Card information' eBMUserCard

15 Attribute type for Email Address Setting

Attribute type of 'Email Address' mail

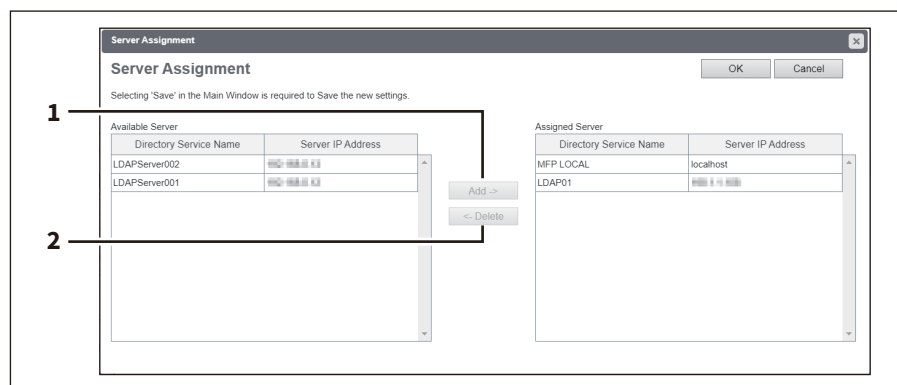
Attribute type of 'From Name' uid

	Item name	Description
1	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.
2	Directory Service Name	Enter the directory service name to identify the directory service. You can enter up to 64 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
3	Server IP Address	Enter the IP address or FQDN of the LDAP server. You can enter up to 128 alphanumerical characters and symbols.
4	Port Number	Enter the port number to access the LDAP server. You can enter a value in the range from 1 to 65535. Generally the default value “389” is used to access the LDAP server without SSL/TLS. When the SSL/TLS is required, generally the “636” port is used to access the LDAP server.
5	Server Type	Select the LDAP server you want to use for LDAP authentication. <ul style="list-style-type: none">• Windows Server — Select this when LDAP is running on a Windows server.• LDAP Server (Other than Windows Server) — Select this when the LDAP is running on a server other than a Windows one.

	Item name	Description
6	Authentication	<p>Select the SASL authentication protocol. If you do not know the authentication type, select [Auto].</p> <ul style="list-style-type: none"> • Auto — Select this to access the LDAP server using the appropriate authentication that this equipment detects. • Kerberos — Select this to access the LDAP server using the Kerberos authentication. • Digest-MD5 — Select this to access the LDAP server using the Digest-MD5 authentication. • CRAM-MD5 — Select this to access the LDAP server using the CRAM-MD5 authentication. • Login — Select this to access the LDAP server using the login authentication. • Plain — Select this to access the LDAP server using the plain authentication. • Simple Bind — Select this to access the LDAP server using the Simple Bind authentication.
7	Search Base	Enter the search base. When you configure the Active Directory in Windows server, make sure to enter this option. You can enter up to 256 alphanumerical characters and symbols other than ; (semicolon), #, and \ (backslash).
8	User Name	Enter the log-in user name if a user name is required to access the directory service. You can enter up to 256 alphanumerical characters and symbols.
9	Password	Enter the password if required to access the directory service. You can enter up to 32 alphanumerical characters and symbols.
10	Search Timeout	Select the timeout period for quitting communication when no response is received from the LDAP server. Specify within the range from 1 to 5. "1" is set as the default.
11	Enable SSL/TLS	<p>Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for communicating the LDAP directory service.</p> <ul style="list-style-type: none"> • Disable — Select this to disable the SSL/TLS for communicating the LDAP directory service. • Verify with imported CA certification(s) — Select this to enable the SSL/TLS using the imported CA certificate. • Accept all certificates without CA — Select this to enable the SSL/TLS without using imported CA certificate. <p>Note</p> <ul style="list-style-type: none"> • When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment.  P.405 "Installing CA certificate" • If at least one of the registered LDAP directory services requires the SSL/TLS, you must enable the [Enable SSL/TLS] option. When the [Enable SSL/TLS] option is enabled, this equipment will connect the registered LDAP directory services using SSL/TLS first. Then if the connection fails using SSL/TLS, this will connect to the registered LDAP directory service without using SSL/TLS. Therefore, even if you enable the [Enable SSL/TLS] option, this equipment can also connect to an LDAP directory service that does not require the SSL/TLS. • Not all operating systems support SSL/TLS for all protocols.

	Item name	Description
12	SSL/TLS Port Number	Enter the port number to access the LDAP server using SSL/TLS. You can enter a value in the range from 1 to 65535. Generally the default value “636” is used.
13	Attribute type for Search Contact	Enter the attribute type to be used for searching contacts using the external LDAP server. You can enter up to 32 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
14	Attribute type for Authentication	Specify the attribute name for authentication. Enter [Attribute type of 'User Name'], [Attribute type of 'Server Name'], and either [Attribute type of 'PIN'] or [Attribute type of 'Card information'] for authentication. You can enter up to 32 half-width alphanumerical characters and symbols (excluding = ; # \). Click the [Default Value] button to display the predetermined value.
15	Attribute type for Email Address Setting	Specify [Attribute type of 'Email Address'] and [Attribute type of 'From Name'] for authentication. You can enter up to 32 half-width alphanumerical characters and symbols (excluding = ; # \).

[Server Assignment] screen



	Item name	Description
1	[Add] button	Adds the server from the server list to the assigned servers.
2	[Delete] button	Deletes the server from the assigned servers.

❑ Setting up SMTP Client

In SMTP Client, you can enable or disable SMTP transmission for sending the Internet Fax and E-mails.

Note

A From Address setting is also required to send Internet Fax and E-mails. For information about the From Address setting, see the references below:

📖 P.192 “Email settings”

📖 P.199 “InternetFax settings”

The From Address can be also determined automatically when the User Management Setting is enabled. For more information about User Management Setting, see the reference below:

📖 P.73 “[User Management]”

Network - SMTP Client

1 Basic Setting
2 Filtering
3 SSL/TLS Settings
4 SMTP
5 WSO
6 SMTP Server
7 LDAP Client
8 SMTP Client
9 CUPS
10 Mobile Gateway
11 SNMP
12 Syslog Setting



Connection Test Execute

Enable SMTP Client: Enable
Enable SSL/TLS: Disable
STARTTLS: STARTTLS
POP Before SMTP: Disable
Authentication: Disable
Login Name:
Password:
Maximum Email / InternetFax Size(2-100): 30 MB
Port Number: 25
SMTP Client Connection Timeout(1-180): 30 Seconds

Save Cancel

	Item name	Description
1	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.
2	Enable SMTP Client	When this is enabled, this equipment sends an Internet Fax and an E-mail to the specified SMTP server for transmission over the Internet. [Enable] is set as the default.
3	Enable SSL/TLS	Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for SMTP transmission. <ul style="list-style-type: none">• Disable — Select this to disable the SSL/TLS for SMTP transmission.• Verify with imported CA certification(s) — Select this to enable the SSL/TLS using the imported CA certificate.• Accept all certificates without CA — Select this to enable the SSL/TLS without using imported CA certificate. <div>Note</div> <ul style="list-style-type: none">• When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment. 📖 P.405 “Installing CA certificate”• Not all operating systems support SSL/TLS for all protocols.


	Item name	Description
4	SSL/TLS	<p>Select the protocol for the SSL/TLS when the [Enable SSL/TLS] option is enabled.</p> <ul style="list-style-type: none"> • STARTTLS — Select this to send a message in TLS (Transport Layer Security) using STARTTLS that is the extension command for SMTP transmission. • Over SSL/TLS — Select this to send a message in SSL (Secure Socket Layer)/TLS (Transport Layer Security). <p>Note</p> <p>When you select [Over SSL/TLS], make sure to change the port number correctly. Generally, “465” port is used for the Over SSL/TLS instead of “25” port.</p>
5	SMTP Server Address	<p>Enter the IP address or FQDN (Fully Qualified Domain Name) of the SMTP server when [Enable SMTP Client] is enabled. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</p> <p>Note</p> <p>If you use FQDN to specify the SMTP server, you must configure the DNS server and enable the DNS in the DNS Session.</p> <p>Tip</p> <p>When the [Obtain a SMTP Server Address automatically] option is enabled in the TCP/IP settings, the SMTP server address can be obtained using the DHCP server.</p> <p> P.118 “Basic Setting”</p>
6	POP Before SMTP	<p>Select whether the POP Before SMTP authentication is enabled or disabled. [Disable] is set as the default.</p> <p>Note</p> <p>If [Application] has been selected for [Authentication] under [POP3 Client], this [POP Before SMTP] setting does not work.</p>
7	Authentication	<p>Select the type of authentication to access the SMTP server.</p> <ul style="list-style-type: none"> • Disable — Select this to access the SMTP server using no authentication. • Plain — Select this to access the SMTP server using plain authentication. • Login — Select this to access the SMTP server using the log-in authentication. • CRAM-MD5 — Select this to access the SMTP server using CRAM-MD5 authentication. • Digest-MD5 — Select this to access the SMTP server using Digest-MD5 authentication. • Kerberos — Select this to access the SMTP server using Kerberos authentication. • NTLM(IWA) — Select this to access the SMTP server using NTLM (IWA) authentication. • AUTO — Select this to access the SMTP server using the appropriate authentication that this equipment detects.

	Item name	Description
8	Login Name	<p>Enter the log-in name to access the SMTP server if the SMTP authentication is enabled. You can enter up to 64 alphanumerical characters and symbols.</p> <p>Note</p> <p>Enter the account name for accessing a POP3 server when the POP Before SMTP authentication is enabled.</p> <p> P.158 “Setting up POP3 Client”</p>
9	Password	<p>Enter the password to access the SMTP server if the SMTP authentication is enabled. You can enter up to 64 alphanumerical characters and symbols.</p> <p>Note</p> <p>Enter the password for accessing a POP3 server when the POP Before SMTP authentication is enabled.</p> <p> P.158 “Setting up POP3 Client”</p>
10	Maximum Email / InternetFax Size (2-100)	<p>Select the maximum size that this equipment is allowed to send using the SMTP. Specify within the range from 2 to 100 MB.</p> <p>Note</p> <p>The available maximum size includes that for attached files. Approx. 70 MB is the available maximum size for attached files when 100 MB is set in this option.</p>
11	Port Number	<p>Enter the port number for accessing the SMTP server when [Enable SMTP Client] is enabled. The port number depends on the port setting in the SMTP server. You can enter a value in the range from 1 to 65535. Generally the default value “25” is used.</p> <p>Note</p> <p>When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you set it by mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.</p>
12	SMTP Client Connection Timeout(1-180)	<p>Enter a timeout period for quitting communication when no response is received from the SMTP server. Specify within the range from 1 to 180 seconds. “30” is set as the default.</p>

❑ Setting up POP3 Client

In POP3 Client, you can specify the POP3 server to receive an Internet Fax and E-mails.

	Item name	Description
1	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.
2	Enable POP3 Client	Select whether retrieving an Internet Fax and an E-mail from the POP3 server is enabled or disabled. [Enable] is set as the default.
3	Enable SSL/TLS	<p>Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for POP3 transmission.</p> <ul style="list-style-type: none"> • Disable — Select this to disable the SSL/TLS for POP3 transmission. • Verify with imported CA certification(s) — Select this to enable the SSL/TLS using the imported CA certificate. • Accept all certificates without CA — Select this to enable the SSL/TLS without using imported CA certificate. <p>Note</p> <ul style="list-style-type: none"> • When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment. P.405 “Installing CA certificate” • Not all operating systems support SSL/TLS for all protocols.
4	POP3 Server Address	<p>Enter the IP address or FQDN (Fully Qualified Domain Name) of the POP3 server when [Enable POP3 Client] is enabled. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).</p> <p>Note</p> <p>If you use FQDN to specify the POP3 server, you must configure the DNS server and enable the DNS in the DNS Session.</p> <p>Tip</p> <p>When the [Obtain a POP3 Server Address automatically] option is enabled in the TCP/IP settings, you can obtain the POP3 server address from the DHCP server. P.118 “Basic Setting”</p>

	Item name	Description
5	Authentication	<p>Enable or disable the authentication for accessing the POP3 server.</p> <ul style="list-style-type: none"> • Disable — Select this to disable the authentication. • NTLM/SPA — Select this to access the POP3 server using the NTLM/SPA authentication. • Kerberos — Select this to access the POP3 server using the Kerberos authentication. • Application — Select this to access the POP3 server using the application that supports the authentication for the email cloud service. Click [Assignment] to show the list of the applications with which you can use the email cloud service. Select an application you want to use from the list and click [OK] to close the list screen. You can usually select the standard system application “Cloud Authentication for Email”. When the application name has appeared on the right side of the [Assignment] button, click [Save] that is located at the top of the screen. When the message prompts you to set up the application, click [OK] to close the message screen and then click the application name to open the setting screen. Select an email cloud service you want to use from the list, enter the account name for the email cloud service, and then click [Account Registration] to sign in the service. <p>Note</p> <p>If you select [Application], take note of the followings:</p> <ul style="list-style-type: none"> • The [POP Before SMTP] setting under [SMTP Client] does not work. • The credentials are used between the application and the email cloud service for the authentication. If they expire, the application cannot log in to the POP3 server. Install or update the application with the renewed credentials. Contact your service technician for details. <p>Tip</p> <ul style="list-style-type: none"> • If you change or reregister the current account name, click [Delete] to delete it and then redo the entry and registration. • You can also open the setting screen for [Cloud Authentication for Email] from [Administration] > [Application] > [Application List] > [System Application]. <p> P.360 “Application List”</p>
6	Type POP3 Login	<p>Select the POP3 login type.</p> <ul style="list-style-type: none"> • AUTO — Select this to automatically designate the POP3 log-in type of the POP3 server. • POP3 — Select this to use the general POP3 log-in type. • APOP — Select this to use the APOP log-in type. APOP allows users to access the POP3 server by encrypting the user name and password. <p>Note</p> <ul style="list-style-type: none"> • If it is not possible to log in to the mail server using [Auto], manually set the type of POP3 log in to either [POP3] or [APOP]. • Select [AUTO] when [Application] is selected in the [Authentication] option.

	Item name	Description
7	Account Name	<p>Enter the account name for this equipment to access the POP3 server. You can enter up to 96 alphanumerical characters and symbols.</p> <p>Note</p> <ul style="list-style-type: none"> • Enter the account name without the domain name when [NTLM/SPA] or [Kerberos] is selected in the [Authentication] option. • Enter the same account name you have registered on the setting screen of the application when [Application] is selected in the [Authentication] option.
8	Password	<p>Enter the password for this equipment to access the POP3 server. You can enter up to 96 alphanumerical characters and symbols.</p> <p>Tip</p> <p>You cannot enter any passwords, which are not required, when [Application] is selected in the [Authentication] option.</p>
9	Scan Rate	Enter how often this equipment should access the POP3 server for new messages. You can enter a value in the range from 0 to 4096. "5" is set as the default.
10	Port Number	Enter the port number to access the POP3 server. The port number depends on the port setting in the POP3 server. You can enter a value in the range from 1 to 65535. Generally the default value "110" is used.
11	SSL/TLS Port Number	Enter the port number to access the POP3 server using SSL/TLS. The SSL/TLS port number depends on the port setting in the POP3 server. Generally "995" is used.
12	POP3 Client Connection Timeout(1-180)	Enter a timeout period for quitting communication when no response is received from the POP3 server. Specify within the range from 1 to 180 seconds. "30" is set as the default.

❑ Setting up FTP Client

In FTP Client, you can specify the default port number used for the Save as file using the FTP protocol.

	Item name	Description
1	SSL/TLS Setting	<p>Specify the certificate used in the SSL/TLS.</p> <ul style="list-style-type: none"> • Verify with imported CA certification(s) — Select this to use the registered certificate(s). • Accept all certificates without CA — Select this to use all certificates.
2	Default Port Number	Enter the port number to access the FTP site. The port number depends on the port setting in the FTP site. You can enter a value in the range from 1 to 65535. Generally the default value "21" is used.

❑ Setting up Bonjour

In Bonjour, you can enable or disable Bonjour (mDNS) that is available for macOS or Windows OS. You need to set [Secondary] for the secondary network when you use the two-channel networks.

	Item name	Description
1	Enable Bonjour	Select whether Bonjour is enabled or disabled. [Enable] is set as the default.
2	Link-Local Host Name	Enter the DNS host name of this equipment. You can enter up to 127 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
3	Service Name	Enter the device name of this equipment that will be displayed in the Bonjour network. You can enter up to 63 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
4	Chrome OS Print	Select whether to enable the Chrome OS print service. It is enabled as a default.

❑ Setting up Mobile Scan(eSCL)

In Mobile Scan(eSCL), you can enable or disable the Mobile Scan settings.

Tip

The Mobile Scan(eSCL) settings are linked to the scan settings of the AirPrint function.

	Item name	Description
1	Enable Mobile Scan	Select whether Mobile Scan is enabled or disabled.
2	Secure Scan (SSL/TLS)	Select whether Secure Scan is enabled or disabled.
3	Authentication	Set whether or not to perform Basic Authentication when Secure Scan is enabled. [Disable] is the default setting.
4	User Name	Set a user name which is used for Basic Authentication. You can enter up to 127 alphanumeric characters and symbols (excluding = ; # \).
5	Password	Set a password which is used for Basic Authentication. You can enter up to 127 alphanumeric characters and symbols (excluding = ; # \).

❑ Setting up SNMP

In SNMP Network Service, you can enable or disable the SNMP to monitor the device status using a network monitoring utility. If an administrator wants to monitor the device status with a monitoring utility, programmed to match the MIB, you must enable the SNMP and SNMP Traps.

Note

The export operation may be unstable if administrators are accessing this equipment from multiple computers simultaneously in the access policy mode to export information. Be sure that the administrator accesses this equipment from only one computer when exporting.

	Item name	Description
1	Enable SNMP V1/V2	Select whether SNMP V1/V2 monitoring with MIB is enabled or disabled. This must be enabled to allow users to connect using TopAccessDocMon, TWAIN driver, File Downloader, or the AddressBook Viewer. [Enable] is set as the default.

	Item name	Description
2	Read Community	<p>Enter the SNMP read community name for the SNMP access. You can enter up to 31 alphanumeric characters and symbols other than =, ; (semicolon), #, and \ (backslash). “public” is set as the default.</p> <p>Note</p> <ul style="list-style-type: none"> • It is recommended to change the default Read Community name for security reasons. • If changing the Read Community name, match the setting with the applications in use. Otherwise, applications that use MIB (TopAccess, TWAIN driver, File Downloader, and AddressBook Viewer) will become unavailable. The SNMP communication of the printer driver also will be unavailable, so that obtaining the configurations, confirming the department code, and obtaining the available boxes in e-Filing will be disabled. • When you leave the [Read Write Community] option blank, the SNMP communication between the SNMP Browser of the Client computer and this equipment will be disabled.
3	Read Write Community	<p>Enter the SNMP Read Write community name for the SNMP access. You can enter up to 31 alphanumeric characters and symbols other than =, ; (semicolon), #, and \ (backslash). “private” is set as the default.</p> <p>Note</p> <ul style="list-style-type: none"> • It is recommended to change the default Read Write Community name for security reasons. • If changing the Read Write Community name, match the setting with the applications in use. Otherwise, applications that use MIB (TopAccess, TWAIN driver, File Downloader, and AddressBook Viewer) will become unavailable. The SNMP communication of the printer driver also will be unavailable, so that obtaining the configurations, confirming the department code, and obtaining the available boxes in e-Filing will be disabled.
4	Enable SNMP V3	Select whether SNMP V3 monitoring with MIB is enabled or disabled. This must be enabled to allow users to connect using TopAccessDocMon, TWAIN driver, File Downloader and the AddressBook Viewer.
5	SNMP V3 User Information	SNMP V3 user information registered into this equipment is displayed in a list. SNMP V3 user information can be registered, edited, deleted or exported.
6	Enable SNMP V3 Trap	Select whether SNMP V3 Trap is sent or not. [Disable] is set as the default.
7	SNMP V3 Trap User Name	Enter an SNMP V3 Trap User Name. You can enter up to 31 alphanumeric characters and symbols.
8	SNMP V3 Trap Authentication Protocol	<p>Select an authentication protocol.</p> <ul style="list-style-type: none"> • HMAC-MD5 — Select this to use HMAC-MD5. • HMAC-SHA — Select this to use HMAC-SHA.
9	SNMP V3 Trap Authentication Password	Enter an authentication password. You can enter up to 31 alphanumeric characters and symbols.
10	SNMP V3 Trap Privacy Protocol	<p>Select a protocol for data encryption.</p> <ul style="list-style-type: none"> • None — Select this not to encrypt data. • CBC-DES — Select this to use CBC-DES. • CFB-AES-128 — Select this to use AES-128 (CFB mode).
11	SNMP V3 Trap Privacy Password	Enter a privacy password. You can enter up to 31 alphanumeric characters and symbols.

	Item name	Description
12	Enable Authentication Trap	Select whether to send SNMP Traps when this equipment is accessed using SNMP V1/V2 from a different read community. [Enable] is set as the default.
13	Enable Alerts Trap	Select whether to send SNMP V1/V2 Traps when an alert condition occurs. [Enable] is set as the default.
14	IP Trap Address 1 to 10	Enter the IP address where the SNMP Traps will be sent. You can specify up to 10 addresses. Specify within the range from 0 0 0 0 to 255 255 255 255.
15	IP Trap Community	Enter the trap community name for the IP Traps. You can enter up to 31 alphanumeric characters and symbols. "public" is set as the default.
16	IPX Trap Address	<p>Enter the IPX address where the SNMP Traps will be sent. You can enter up to 20 alphanumeric characters and symbols.</p> <p>Note</p> <p>When you want to use a user name registered in the SNMP V3 User Information list as an SNMP V3 Trap User Name, you must enter the same protocols and passwords registered for the authentication protocol, authentication password (not displayed on the list), privacy protocol and password (not displayed on the list) into the fields such as [SNMP V3 Trap Authentication Protocol], [SNMP V3 Trap Authentication Password], [SNMP V3 Trap Privacy Protocol] and [SNMP V3 Trap Privacy Password]. If they do not match, information registered in the list will be adopted.</p>
17	Enable SNMP	The same settings as ones for the primary network are applied to the secondary network when you use the two-channel networks. But the traps are not sent.

[Create SNMP V3 User Information] screen

You can display this screen by clicking the [New] button in the Create SNMP V3 User Information page.

Tip

Clicking [Save] on the [Create SNMP V3 User Information] screen instantly registers the SNMP V3 user information, enabling the registered user to access this equipment via SNMP over a network.

	Item name	Description
1	Context Name	Displays the context name.
2	User Name	Enter the user name. You can enter up to 31 alphanumeric characters and symbols.
3	Authentication Protocol	<p>Select an authentication protocol.</p> <ul style="list-style-type: none"> • HMAC-MD5 — Select this to use HMAC-MD5. • HMAC-SHA — Select this to use HMAC-SHA.
4	Authentication Password	Enter the password when the Authentication option is enabled. You can enter up to 31 characters.

	Item name	Description
5	Privacy Protocol	Select a protocol for data encryption. <ul style="list-style-type: none"> • None — Select this not to encrypt data. • CBC-DES — Select this to use CBC-DES. • CFB-AES-128 — Select this to use AES-128 (CFB mode).
6	Privacy Password	Enter the password for the user information. You can enter up to 31 alphanumeric characters and symbols.
7	Permissions Level	Select the access permission level of the SNMP V3 user. <ul style="list-style-type: none"> • General User — Select this to permit only the reading of data. • Administrator — Select this to permit both the reading and writing of data.

❑ Setting up SLP

When SLP is enabled, this equipment becomes a Service Agent that responds to requests from a User Agent for searching particular services and registers services to a Directory Agent.

Tip

The SLP setting only supports the print services shown below.
Raw TCP print, LPD print, IPP print, WSD print, SMB print, FTP print

Note

About the “printer-location” attribute of SLP

SLP has an attribute called “printer-location” as one of the services provided. The information of “printer-location” is the device setting information on the [General] submenu of the [Setup] menu on the [Administration] page, and that of the [Location] field of [Device Information] on the [Device] page. Turn the equipment off and on if you have changed [Location] from TopAccess. The change is reflected in “printer-location” of SLP after the equipment is restarted.

	Item name	Description
1	Enable SLP	Select whether SLP service is enabled or disabled. [Enable] is set as the default.
2	TTL	Set TTL (Time To Live, a scope in the network that provides SLP service). This is to enable the communication among User Agents and Directory Agents located on different networks.
3	Scope	Set this for specifying the scope of groups that provide SLP services. The default value is “DEFAULT”. <div> <div>Tip</div> <ul style="list-style-type: none"> • More than one group can be entered for [Scope] by separating them with a comma. • Characters () \ ! < = > ~ ; * + cannot be entered in the scope. • Do not leave this field blank or the SLP setting will be disabled. • You can search a particular service using Konqueror (SUSE Linux) or SLPSNOOP utility (Novell client) which is a User Agent (UA). </div>

❏ Syslog Setting

Specify these items when sending message logs to a syslog server using syslog.

Note

Be sure to confirm that message logs are sent to a Syslog server regularly.

	Item name	Description
1	Enable Syslog	Specify whether or not to enable Syslog transmission.
2	Server IP Address/Host Name	Specify the IP address or host name of the Syslog server. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
3	Port Number	Specify the port number to communicate with the Syslog server. You can enter a value in the range from 1 to 65535. Generally the default value “514” is used.
4	Protocol	Specify the communications protocol. <ul style="list-style-type: none"> • TCP — Select this to use TCP only. • UDP — Select this to use UDP only.
5	Enable SSL/TLS	Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for the Syslog server. <ul style="list-style-type: none"> • Disable — Select this to disable the SSL/TLS for POP3 transmission. • Verify with imported CA certification(s) — Select this to enable the SSL/TLS using the imported CA certificate. • Accept all certificates without CA — Select this to enable the SSL/TLS without using imported CA certificate. • When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment. P.405 “Installing CA certificate” • Not all operating systems support SSL/TLS for all protocols.
6	Severity	Specify the log type to be notified. <ul style="list-style-type: none"> • Error — Notifies when an error occurs. • Warning — Notifies when a warning occurs. • Information — Notifies information.
7	Facility	Specify the log content to be notified. <ul style="list-style-type: none"> • Security/Authorization — Security/Authorization log. • Local Use0 — Log that is other than the above. • Local Use1 (Job Log) — Job log <div>Tip</div> Specify both if you want to specify “Severity” and “Facility”.

❑ Setting up IPX/SPX

You can set the IPX/SPX protocol to enable the communication over IPX/SPX. The IPX/SPX must be configured to enable Novell printing as well as the IPX/SPX “Save as File” function with NetWare server over IPX/SPX.

	Item name	Description
1	Enable IPX/SPX	Select whether the IPX/SPX protocol is enabled or disabled. Enable this when configuring Novell printing over the IPX/SPX network. [Disable] is set as the default.
2	Frame Type	Select the desired frame type for IPX/SPX. <ul style="list-style-type: none"> • Auto Sense — Select this to use an appropriate frame type that the equipment found first. • IEEE 802.3/Ethernet II/IEEE 802.3 Snap/IEEE 802.2 — Instead of [Auto Sense], select the frame types to be used from these options.
3	Actual Frame	Displays the actual frame type of the equipment.

❑ Setting up NetWare

In NetWare Session, you can set the NetWare Bindery or NDS service. This must be set when configuring a Novell printing environment.

	Item name	Description
1	Enable NetWare	Select whether NetWare is enabled or disabled. <ul style="list-style-type: none"> • Enable — Enables NetWare. • Disable — Disables NetWare.
2	Enable Bindery	Select whether the NetWare Bindery mode for Novell printing is enabled or disabled. When you configure a Novell printing environment with the NetWare server in the bindery mode, you must enable this.
3	Enable NDS	Select whether the NetWare NDS mode for Novell printing is enabled or disabled. When you configure a Novell printing environment with the NetWare server in NDS mode, you must enable this. When this is enabled, you should also specify the context and tree for the NDS.
4	Context	Enter the NDS context where the NetWare print server for this equipment is located.
5	Tree	Enter the NDS tree.
6	Preferred File Server	Enter the NetWare server name in which this equipment preferentially searches for the queues.

VNC Setting

You can use a computer or a mobile terminal such as a tablet and a smartphone to check and operate the control panel.

Note

- The default password for this VNC function is “d9kvgn”. Be sure to change it before using this function. Specify a password with six or more and eight or less alphanumeric letters.
- You can use only one computer or mobile terminal for the VNC function.

Tip

- It is recommended that you use UltraVNC (client software) on Windows 10 or later for the VNC function.
- When this VNC function is enabled, the equipment does not enter the Super Sleep mode.
- “Your Screen is currently being monitored.” is displayed on the bottom left of the touch panel of an MFP in which a remote operation is being performed.



Network - VNC Setting

Save Cancel

1 Basic Setting Enable VNC Function Enable

2 Old Password

3 New Password

4 Retype Password

5 Enable SSL/TLS Disable

6 Enable Remote Panel Operation Disable

7 Open Range Admin

8 Intermediate Server Address https://ip address:port

	Item name	Description
1	Enable VNC Function	Select whether the VNC function is enabled or disabled. <ul style="list-style-type: none"> • Enable — Enables the VNC function. • Disable — Disables the VNC function.
2	Old Password	Enter the old password for the VNC function.
3	New Password	Enter a new password for the VNC function.
4	Retype Password	Retype the new password for the VNC function.
5	Enable SSL/TLS	Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for the VNC function. <ul style="list-style-type: none"> • Enable — Enables the VNC function. • Disable — Disables the VNC function.
6	Enable Remote Panel Operation	Select whether the remote panel operation function is enabled or disabled. <ul style="list-style-type: none"> • Enable — Select this to enable the remote panel operation function. • Disable — Select this to disable the remote panel operation function. <div> Note For the details about [Enable Remote Panel Operation], contact your service technician or representative. </div>
7	Open Range	Select the disclosure range of the remote panel operation function. <ul style="list-style-type: none"> • Admin — Permits the administrator. • User — Permits general users.
8	Intermediate Server Address	Enter an IP address and port number of the relay server used for the remote panel operation.

Copier settings

You can specify copier settings.

Tip

The [Copier] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

P.14 “Access Policy Mode”

P.101 “[Setup] Item List”

Setting up Default setting

In Default setting, you can set the default copier settings that apply for copy operation from the touch panel.

	Item name	Description
1	Color Mode ^{*1}	<p>Select the default color mode for copying.</p> <ul style="list-style-type: none"> • Auto Color — The equipment automatically judges the type of each color on originals. Colored originals are copied in full color and black and white originals are copied in black and white. • Full Color — All originals are copied in full color. • Black — All originals are copied in black and white. <p>Note</p> <p>Only [Black] can be selected when the No Limit Black function is enabled. For the details of the No Limit Black function, see the reference below: User Functions - MANAGING COUNTERS (COUNTER MENU) - Department Management - Setting the No Limit Black function</p>

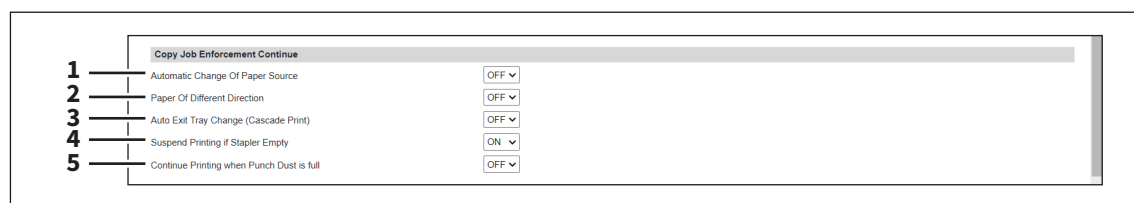
	Item name	Description
2	Original Mode for Color ^{*1}	<p>Select the default original mode for color originals.</p> <ul style="list-style-type: none"> • Text/Photo — Originals with text and photographs mixed. • Text — Originals with text (or text and line art) only. • Photo — Originals with general photographs on photographic printing paper. • Printed Image — Originals with photogravure (e.g. magazine, brochure). • Map — Originals with fine illustrations or text.
3	Original Mode for Black ^{*1} / Original Mode	<p>Select the default original mode for black and white originals.</p> <ul style="list-style-type: none"> • Text/Photo — Originals with text and photographs mixed. • Text — Originals with text (or text and line art) only. • Photo — Originals with photographs. • Image Smoothing ^{*2} — Originals with text and photographs mixed (especially originals requiring higher reproducibility on photos).
4	Exposure for Color ^{*1}	<p>Select the type of image density for color copies.</p> <ul style="list-style-type: none"> • Auto — Select this to set the Auto mode as the default exposure for color copy. The Auto mode automatically detects the density of the original to make copies at the optimum exposure. • Manual — Select this to set the Manual mode as the default exposure for color copy. The manual mode allows you to manually specify the density of the original.
5	Exposure for Black ^{*1} / Exposure	<p>Select the type of image density for black and white copies.</p> <ul style="list-style-type: none"> • Auto — Select this to set the Auto mode as the default exposure for black and white copies. The Auto mode automatically detects the density of the original to make copies at the optimum exposure. • Manual — Select this to set the Manual mode as the default exposure for black and white copies. The manual mode allows you to manually specify the density of the original.
6	Bypass feed	Select the default paper type for the Bypass Tray.
7	BOOK > 2 ^{*2}	<p>Select the default page arrangement of the book-type originals for Book to 2-sided copies. Available only when the Automatic Duplexing Unit is installed.</p> <ul style="list-style-type: none"> • Open from left — Select this to copy the booklet originals that can be read from the left page. • Open from right — Select this to copy the booklet originals that can be read from the right page.
8	Magazine Sort ^{*2}	<p>Select the default page arrangement for magazine sort copies. Available only when the Automatic Duplexing Unit is installed.</p> <ul style="list-style-type: none"> • Open from left — Select this to create a booklet that can be read from the left page. • Open from right — Select this to create a booklet that can be read from the right page.

	Item name	Description
9	2in1 / 4in1	<p>Select the default page arrangement for 2in1/4in1 copies.</p> <ul style="list-style-type: none"> • Write Laterally — Select this to copy two pages or four pages from left to right or from top to bottom. When the portrait originals are copied using 2in1 or 4in1, this equipment copies them from left to right. When the landscape originals are copied using 2in1 or 4in1, this equipment copies them from top to bottom. • Write Vertically — Select this to copy each two pages or four pages from right to left or from top to bottom. When the portrait originals are copied using 2in1 or 4in1, this equipment copies them from right to left. When the landscape originals are copied using 2in1 or 4in1, this equipment copies them from top to bottom.
10	Maximum Copies	Select the maximum numbers of pages that users can specify for copying. You can select from [9999]*2, [999], [99] or [9].
11	Auto 2-sided Mode	<p>Select how the 2-sided mode initially applies to copy settings when originals are set in the Reversing Automatic Document Feeder. Available only when the Reversing Automatic Document Feeder and the Automatic Duplexing Unit are installed.</p> <ul style="list-style-type: none"> • OFF — Select this to initially apply [1->1 SIMPLEX] when originals are set in the Reversing Automatic Document Feeder. • One-sided/Double-sided — Select this to initially apply [1->2 DUPLEX] when originals are set in the Reversing Automatic Document Feeder. • Double-sided/Double-sided — Select this to initially apply [2->2 DUPLEX] when originals are set in the Reversing Automatic Document Feeder. • User Selection — Select this to initially display the screen to select the 2-sided mode when originals are set in the Reversing Automatic Document Feeder.
12	Sort Mode Priority	<p>Select the default sort mode for copying.</p> <ul style="list-style-type: none"> • Non-Sort — Copies exit without sorting. • Staple *2 — Copies exit with their corner stapled. • Sort — Copies exit in the same page order as the originals one set after another. • Group — Copies grouped by page exit.

*1 Available only for models that support color printing.

*2 This function is not available for some models.

❑ Setting up Copy Job Enforcement Continue



Item	Setting
1	Automatic Change Of Paper Source: OFF
2	Paper Of Different Direction: OFF
3	Auto Exit Tray Change (Cascade Print): OFF
4	Suspend Printing if Stapler Empty: ON
5	Continue Printing when Punch Dust is full: OFF

	Item name	Description
1	Automatic Change Of Paper Source	Specify whether or not to change the paper source automatically when the size of the original and the paper in the paper source do not match. <ul style="list-style-type: none"> • ON — Select this to change the paper source and continue processing the job. • OFF — Select this to stop the job.
2	Paper Of Different Direction ^{*1}	Specify whether or not to copy on paper which is loaded in the paper source in a different orientation from the original. <ul style="list-style-type: none"> • ON — Select this to continue processing the job by copying on paper in a different orientation. • OFF — Select this to stop the job.
3	Auto Exit Tray Change (Cascade Print) ^{*1}	Specify whether or not to switch the receiving tray automatically. <ul style="list-style-type: none"> • ON — Select this to continue processing the job by switching the receiving tray. • OFF — Select this to stop the job.
4	Suspend Printing if Stapler Empty ^{*1}	Specify whether to stop printing when staples run out. <ul style="list-style-type: none"> • ON — Select this to stop printing when staples run out. • OFF — Select this not to stop printing when staples run out.
5	Continue Printing when Punch Dust is full ^{*1}	Specify whether to continue printing when the punch dust bin is full. <ul style="list-style-type: none"> • ON — Select this to continue printing even when the punch dust bin is full. • OFF — Select this to stop printing when the punch dust bin is full.

^{*1} This function is not available for some models.

Fax settings

You can specify fax settings.

Note

The [Fax] submenu in the [Setup] menu is available only when the Fax Unit is installed.

Tip

The [Fax] submenu can be accessed from the [Setup] menu on the [Administration] page.

For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

Setting up Fax Setting

In Fax Setting, you can set the default fax settings that apply to fax operations from the touch panel.

Tip

Some items may not be displayed or may not function on some models.

The screenshot displays the 'Fax' settings interface. On the left, a vertical list of 30 numbered items is shown, each corresponding to a specific fax setting. On the right, the configuration options for these settings are displayed. The settings include fields for Terminal ID, Fax Number, Line2 Number, Monitor Volume, Completion Tone Volume, Reception Mode, Dial Type, Dial Type(Line 2), Line-2 Mode, Resolution, Original Mode, Exposure, TTI, RTI, ECM, Discard, Reduction, Duplex Print, Rotate Sort, Recovery Transmit, Journal Auto Print, Memory Transmission Report, Multi Transmission Report, Polling Report, Relay Originator, RX End Tone, TX End Tone, Line Monitor, and Secure Receive. Each setting has a corresponding input field or dropdown menu. At the bottom, there are fields for Line1 and Line2 passwords, each with a 'Retype Password' field. The interface also includes 'Save' and 'Cancel' buttons at the top right.

	Item name	Description
1	Terminal ID	Enter the terminal ID name (company name) with up to 20 characters to identify this equipment. The name will be printed at the leading edge of all documents transmitted.

	Item name	Description
2	Terminal ID (Line2) * ¹	Enter the terminal ID name (company name) to identify this equipment on Line 2, if installed. The name will be printed at the leading edge of all documents transmitted via Line 2 of this equipment.
3	Fax Number	Enter the fax number of this equipment. This fax number will be printed at the leading edge of all documents transmitted from Line 1.
4	Line2 Number * ¹	Enter the fax number for Line 2 of this equipment, if installed. This fax number will be printed at the leading edge of all documents transmitted from Line 2.
5	Monitor Volume	Select the volume of the line monitor during transmission.
6	Completion Tone Volume	Select the volume of the line monitor when completing the printing of a received fax.
7	Reception Mode	<p>Select how this equipment activates when a fax is received.</p> <ul style="list-style-type: none"> • Auto — Select this to automatically receive incoming originals when the bell rings. Select this when the line is being used exclusively by the fax transmission. • Manual — Select this to manually receive incoming originals after pressing the [Start] button on the control panel.
8	Dial Type	<p>Select the dial type for Line 1.</p> <ul style="list-style-type: none"> • DP — Select this to use the Dial Pulse type for Line 1. • MF — Select this to use Multi-frequency type for Line 1. <p>Tip</p> <p>The following items are displayed for some models.</p> <ul style="list-style-type: none"> • 10 PPS — Select this to use the Dial Pulse type for 10 PPS. • 20 PPS — Select this to use the Dial Pulse type for 20 PPS. • PB — Select this to use a tone type push phone line.
9	Dial Type(Line 2) * ¹	<p>Select the dial type for Line 2, if installed.</p> <ul style="list-style-type: none"> • DP — Select this to use the Dial Pulse type for Line 2. • MF — Select this to use Multi-frequency type for Line 2. <p>Tip</p> <p>The following items are displayed for some models.</p> <ul style="list-style-type: none"> • 10 PPS — Select this to use the Dial Pulse type for 10 PPS. • 20 PPS — Select this to use the Dial Pulse type for 20 PPS. • PB — Select this to use a tone type push phone line.
10	Line-2 Mode * ¹	<p>Select how Line 2 is used, if installed.</p> <ul style="list-style-type: none"> • Tx / Rx — Select this to use Line 2 for sending and receiving a fax. • Rx Only (24 Hour) — Select this to use Line 2 only for receiving a fax. • Rx Only (Timer) — Select this to use Line 2 only for receiving a fax during specified time. When this is selected, enter the start time and end time that Line 2 is used for only receiving a fax.

	Item name	Description
11	Resolution	<p>Select the default resolution for sending faxes.</p> <ul style="list-style-type: none"> • Standard — Select this to use the standard mode as the default resolution. This mode is suitable when you are frequently transmitting text documents with normal size characters. • Fine — Select this to use the fine mode as the default resolution. This mode is suitable when you are transmitting documents with small size characters or fine drawings. • Ultra Fine — Select this to use the ultra fine mode as the default resolution. This mode is suitable when you are transmitting documents with very small size characters or detailed drawings.
12	Original Mode	<p>Select the default image quality mode for sending faxes.</p> <ul style="list-style-type: none"> • Text — Select this to set the Text mode as the default image quality mode appropriate for sending text originals. • Text/Photo — Select this to set the Text/Photo mode as the default image quality mode appropriate for sending originals containing both text and photos. • Photo — Select this to set the Photo mode as the default image quality mode appropriate for sending photo originals.
13	Exposure	<p>Select the default exposure for sending faxes. Select [Auto] to automatically apply the ideal contrast according to the original or select the contrast manually in 11 stages.</p>
14	TTI	<p>Select whether to print a transmission header (TTI) on received faxes to identify the sender of received faxes.</p> <p>Note</p> <p>The printed time is the transmission time of each page.</p>
15	RTI	<p>Select whether to print a reception header (RTI) on received faxes to clearly identify the time, date, and page count of received faxes.</p>
16	ECM	<p>Select whether to enable or disable the ECM (Error Correction Mode) to automatically re-send any portion of the document affected by phone line noise or distortion.</p>
17	Discard	<p>Select whether to discard the lower portion of the received fax image if it is larger than the recording paper.</p>
18	Reduction	<p>Select whether to reduce the received fax image if it is larger than the effective printing area of the recording paper.</p>
19	Duplex Print	<p>Select whether to print the received fax images on both sides of the recording paper. Available only when the Automatic Duplexing Unit is installed.</p>
20	Rotate Sort ^{*1}	<p>Select whether to rotate the output direction in the tray for each reception.</p>
21	Recovery Transmit	<p>Select whether to re-transmit a fax after failing the initially specified number of redial attempts. When this is enabled, select the stored time length from 1 to 24 hours.</p>
22	Journal Auto Print	<p>Select whether to automatically print a transmission and reception journal after every transmission completed.</p>

	Item name	Description
23	Memory Transmission Report	<p>Select how to print a result report after a memory transmission.</p> <ul style="list-style-type: none"> • OFF — Select this to not print a memory transmission report. • Always — Select this to print a memory transmission report with all page images for each memory transmission completed. • ON ERROR — Select this to print a memory transmission report with all page images only when the memory transmission is not successfully completed. • Always (Print 1st Page Image) — Select this to print a memory transmission report with the 1st page image for each memory transmission completed. • ON ERROR (Print 1st Page Image) — Select this to print a memory transmission report with the 1st page image only when the memory transmission is not successful.
24	Multi Transmission Report	<p>Select how to print a result report after a multi-address transmission.</p> <ul style="list-style-type: none"> • OFF — Select this to not print a multi-address transmission report. • Always — Select this to print a multi-address transmission report with all page images for each multi-address transmission completed. • ON ERROR — Select this to print a multi-address transmission report with all page images only when the multi-address transmission is not successfully completed. • Always (Print 1st Page Image) — Select this to print a multi-address transmission report with the 1st page image for each multi-address transmission completed. • ON ERROR (Print 1st Page Image) — Select this to print a multi-address transmission report with the 1st page image only when the multi-address transmission is not successful.
25	Polling Report	<p>Select how to print a result report after a multi-polling reception.</p> <ul style="list-style-type: none"> • OFF — Select this to not print a multi-polling report. • Always — Select this to print a multi-polling report for each multi-polling reception. • ON ERROR — Select this to print a multi-polling report only when the multi-polling reception is not successful.
26	Relay Originator	<p>Select how to print a result report after a relay transmission.</p> <ul style="list-style-type: none"> • OFF — Select this to not print a relay station report. • Always — Select this to print a relay station report with all page images for each relay transmission completed. • ON ERROR — Select this to print a relay station report with all page images only when the relay transmission is not successful. • Always (Print 1st Page Image) — Select this to print a relay station report with the 1st page image for each relay transmission completed. • ON ERROR (Print 1st Page Image) — Select this to print a relay station report with the 1st page image only when the relay transmission is not successful.

	Item name	Description
27	RX End Tone	<p>Select how to sound the RX end tone after the completion of reception.</p> <ul style="list-style-type: none"> • OFF — The RX end tone does not sound. • Print End — The RX end tone sounds at the completion of printing. • Receive End — The RX end tone sounds at the completion of reception.
28	TX End Tone	<p>Select how to sound the TX end tone after the completion of transmission.</p> <ul style="list-style-type: none"> • OFF — The TX end tone does not sound. • Always — The TX end tone sounds at the completion of transmission. • ON ERROR — Sounds in the case of a transmission failure. • Normal End — Sounds at the normal completion of transmission.
29	Line Monitor	<p>Select this to check the connection with the remote fax by confirming Line Monitor.</p> <ul style="list-style-type: none"> • OFF — Line Monitor not confirmed • ON — Line Monitor confirmed
30	Secure Receive	<p>You can set the Secure Receive function to store received fax jobs in the equipment without printing them.</p> <p>With this function, you can prevent the leaking of confidential information in a fax received when no people are present in your office, such as nighttime or holidays, or when an unspecified number of people visit your office.</p> <ul style="list-style-type: none"> • Enable — Enables the Secure Receive function. <p>To print the fax jobs the Secure Receive function received, you must set [Line1 : Password] and [Retype Password] or [Line2 : Password] ^{*1} and [Retype Password] ^{*1}. For the password, you can enter up to 20 alphanumerical characters and symbols (! # () * + , - . / : ; = ? @ \$ ^ _ ` { } ~ \ space).</p> <ul style="list-style-type: none"> • Disable — Disables the Secure Receive function. • Weekly Schedule — Sets whether the Secure Receive function is enabled or disabled for each day of the week. You can set the time to enable and disable the Secure Receive function (24-hour display). <ul style="list-style-type: none"> - For a day on which you want to enable the Secure Receive function all day, specify “00:00” for “Disable” and “00:00” for Enable. - For a day on which you want to disable the Secure Receive function all day, specify “00:00” for “Disable” and “24:00” for Enable. <p>To print the fax jobs the Secure Receive function received, you must set [Line1 : Password] and [Retype Password] or [Line2 : Password] ^{*1} and [Retype Password] ^{*1}. For the password, you can enter up to 20 alphanumerical characters and symbols (! # () * + , - . / : ; = ? @ \$ ^ _ ` { } ~ \ space).</p>

*1 This function is not available for some models.

❑ From Name Registration

You can register up to 20 names of the fax senders. The registered sender name can be selected when saving the InternetFax and Fax settings for the templates.

📖 P.312 “InternetFax Setting”

📖 P.313 “Fax Setting”



	Item name	Description
1	[Add] button	Adds a new name of the fax sender. When the entry window appears, you can enter up to 20 characters for a name. Click [Save] to register the name. To stop the setting operation, click the [Cancel] button to close the window.
2	[Delete] button	Deletes the name selected in the list.
3	[Move Up] button	Moves up the name selected in the list.
4	[Move Down] button	Moves down the name selected in the list.
5	From Name	Shows the registered names of the fax senders. You can scroll up or down the list to see up to 20 names.

□ Report Setting

You can select how to report fax results.

The screenshot shows the 'Report Setting' window. Callout 1 points to the 'Select Agent' button. Callout 2 points to the 'Use login user address (User Authentication)' section, which includes radio buttons for 'Use Email Address which was registered Local User' and 'Use Email Address which was LDAP registered'. Callout 3 points to the '1st Destination' and '2nd Destination' buttons. Callout 4 points to the 'Email Setting' section, which includes fields for Subject, From Address, From Name, Body, and File Name. Callout 5 points to the 'Save as file Setting' section, which includes fields for Destination and File Name. Callout 6 points to the 'Common Setting' section, which includes fields for File Format, Encryption, and Digital Signature.

	Item name	Description
1	[Select Agent] button	You can make detailed settings by selecting one of the following items, and then clicking [Select Agent]. Print — Select this to print. There are no settings available in [Select Agent]. Save as file — Select this to save as a file. Click [Select Agent] to make settings for [Save as file Setting] and [Common Setting]. Email — Select this to send an email. Click [Select Agent] to make address settings, and settings for [Email Setting] and [Common Setting].
2	Use login user address (User authentication)	Set whether or not to use the E-mail address for a login user as the destination for E-mail transmission during user authentication. You can set the following items when you select this check box. Use Email Address which was registered Local User: The E-mail address for a user set in MFP Local Authentication is used as the destination for E-mail transmission. Use Email Address which was LDAP registered: The E-mail address for a server registered in LDAP Client is used as the destination for E-mail transmission. Click [Server Assignment]. Up to 4 LDAP servers can be assigned. 📖 P.151 “LDAP Client settings”
3	[1st Destination] /[2nd Destination] button	This is enabled when you select [Email] from Report Settings, and then click the [Select Agent] button. Click to display the address list where you can set addresses. 📖 P.307 “Destination Setting”

	Item name	Description
4	[Email Setting] button	<p>This is enabled when you select [Email] from Report Settings, and then click the [Select Agent] button.</p> <p>Click to set the following items on the agent settings page for the Email settings.</p> <ul style="list-style-type: none"> • Subject • From Address • From Name • Body • File Name <p> P.316 “Email Setting”</p>
5	[Save as file Setting] button	<p>This is enabled when you select [Save as file] from Report Settings, and then click the [Select Agent] button.</p> <p>Click to set the following items on the agent settings page for the Save as file settings.</p> <ul style="list-style-type: none"> • Destination • File Name <p> P.319 “Save as file Setting”</p>
6	[Common Setting] button	<p>This is enabled when you select [Email] or [Save as file] from Report Settings, and then click the [Select Agent] button.</p> <p>You can set the following items on the agent settings page.</p> <ul style="list-style-type: none"> • File Format • Encryption • Digital Signature <p> P.316 “Email Setting”</p> <p> P.319 “Save as file Setting”</p>

Received Forward Setting for Application

You can set whether or not to save received data (meta data) which can be used for the activation of the received document (image file received by fax) and an application in its storage area. For details about the application, contact your service technician or representative.

Note

This cannot be used if an application which uses the received document is not installed in the equipment or the execution permission of the application is disabled.

	Item name	Description
1	Enable Received Forward	<p>Select [Enable] to save the received document in the storage area of the application. [Disable] is the default setting.</p> <p>Note</p> <p>When [Enable] is selected for [Enable Received Forward], the Received Forward to Applications setting is taken as the top priority even if other forward settings are also enabled.</p>

	Item name	Description
2	Backup Setting	<p>Select [Enable] to save the received document in the specified box as a backup file. [Enable] is the default setting.</p> <p>Tip This will be displayed when [Enable] is selected for [Enable Received Forward].</p>
3	[Box Setting] button	<p>Click this to change the box for saving the received document or to modify the folder name. When you click this button, the [Box Setting] screen will appear.</p> <p>Tip You can change the settings when [Enable] is selected for [Backup Setting].</p>

❑ Box Setting (Received Forward Setting for Application)

You can set the destination to back up the received document.

Note

Up to 400 documents can be stored in a box or folder, and up to 200 pages can be contained in a document. If an attempt is made to store documents exceeding the available numbers, storing to e-Filing will fail. Delete unnecessary documents in a box or e-Filing periodically. Alternatively, specify the document storage period after which unnecessary documents are automatically deleted.

	Item name	Description
1	Destination	<p>Set the box to save the received document.</p> <ul style="list-style-type: none"> • Box Number — Select the box number to save the received document. “000: Public Box” is set as the default. • Password — Enter the password if it is set for the specified box. • Retype Password — Enter the same password again for a confirmation.
2	Folder Name	<p>Enter the folder name in the box where the received document is saved. You can enter up to 64 characters.</p>
3	Document Name	<p>A job ID applied automatically by means of the equipment is displayed. This cannot be changed.</p>

■ Save as file settings

You can configure the Save as file settings that apply to the Save as file operations.

Tip

The [Save as file] submenu can be accessed from the [Setup] menu on the [Administration] page.

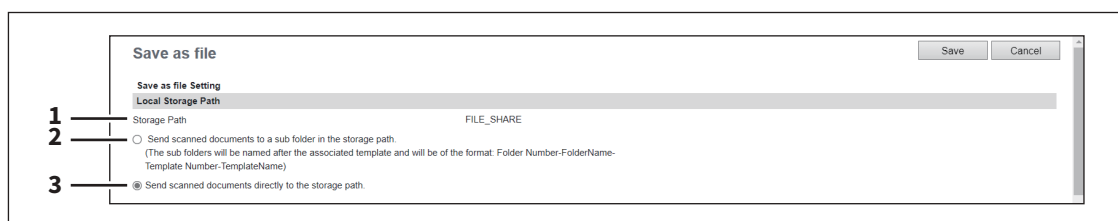
For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

□ Setting up Local Storage Path

You can see the folder path where files are stored by the Save as file to local folder. You can open the local folder by browsing this equipment from a Windows network.



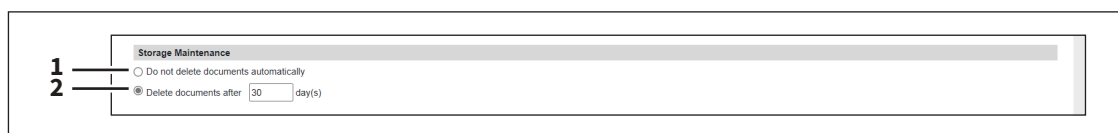
	Item name	Description
1	Storage Path	Displays the local storage path where files are stored when files are saved to the local folder by the Save as file functions.
2	Send scanned documents to a sub folder in the storage path.	Select this to save the files in the sub folder that is named as “Folder Number-Folder Name-Template Number-Template Name”. <div>Tip When you recall the template button registered outside the folder, the sub folder is named as “Template Number-Template Name”.</div>
3	Send scanned documents directly to the storage path.	Select this to save the files directly in the storage path.

□ Setting up Storage Maintenance

In Storage Maintenance, you can select how to delete files stored in the local folder.

Note

The folder created when storing the files in the local folder will be deleted automatically when all files in the folder are deleted.



	Item name	Description
1	Do not delete documents automatically	Select this to delete files stored in the local folder manually. If you select this option, files saved in the shared folder will not be deleted automatically.
2	Delete documents after [] day(s)	Select this to automatically delete files stored in the local folder after a specified number of days. When this is selected, enter the number of days that the files are to remain. [30days] is set as the default.

❑ Setting up Destination

You can specify whether a network folder can be used for Save as file.

1 — Do not allow any network folder to be used as a destination

2 — Use Network Folder Destination

3 — Default file path: Use local folder ▼

	Item name	Description
1	Do not allow any network folder to be used as a destination	You can specify that a network folder cannot be used for Save as file. When this is selected, users can only save a file in the local folder or USB media.
2	Use Network Folder Destination	You can specify that a network folder can be used for Save as file. When this is selected, set the Remote 1 and Remote 2 Settings to specify how users can select the network folders for Save as file destinations.
3	Default file path	Select the destination that will be set as the default destination when performing Save as file from the touch panel. <ul style="list-style-type: none"> • Use local folder — Select this to save in a local folder. • Remote 1 — Select this to save in the folder set in Remote 1. • Remote 2 — Select this to save in the folder set in Remote 2.

❑ Setting up Folder Name

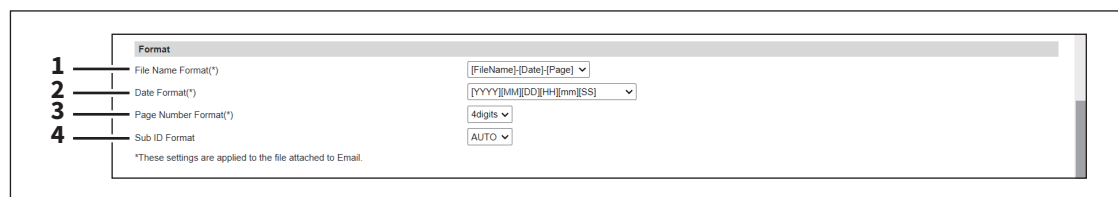
You can select whether to add information related to this equipment or users to the name of a folder created automatically when you save files.

1 — Folder Name Setting: Disable ▼

	Item name	Description
1	Folder Name Setting	Select additional information of the name of a folder created when you save files. <ul style="list-style-type: none"> • Disable — Select this not to add any information. • Add MachineName — Select this to add the NetBIOS name of this equipment. • Add UserName — Select this to add a user name set in user authentication.

❏ Setting up Format

You can set how to name files of the scanned images when you save them into the “FILE_SHARE” folder of this equipment or USB.



	Item name	Description
1	File Name Format	<p>Select the format of the file name. Information such as file name, date and time or page number is added according to the selected format. The added information will also be applied to file names attached to E-mails.</p> <ul style="list-style-type: none"> • [FileName]-[Date]-[Page] • [FileName]-[Page]-[Date] • [Date]-[FileName]-[Page] • [Date]-[Page]-[Filename] • [Page]-[FileName]-[Date] • [Page]-[Date]-[FileName] • [FileName]_[Date]-[Page]
2	Date Format	<p>Select how you add “date and time” of the file name selected in [File Name Format]. The added information will also be applied to file names attached to E-mails.</p> <ul style="list-style-type: none"> • [YYYY][MM][DD][HH][mm][SS] — Year (4 digits), month, day, hour, minute and second are added. • [YY][MM][DD][HH][mm][SS] — Year (2 digits), month, day, hour, minute and second are added. • [YYYY][MM][DD] — Year (4 digits), month, and day are added. • [YY][MM][DD] — Year (2 digits), month, and day are added. • [HH][mm][SS] — Hour, minute and second are added. • [YYYY][MM][DD][HH][mm][SS][mm0] — Year (4 digits), month, day, hour, minute, second and random number (2 digits and “0”) are added.
3	Page Number Format	<p>Select the number of digits of a page number applied to “Page” of the file name selected in [File Name Format] from 3 to 6. The added information will also be applied to file names attached to E-mails. [4digits] is set as the default.</p>
4	Sub ID Format	<p>This equipment automatically adds a sub ID (identification number) to the name of a file that you are saving the same file name exists. You can select the number of digits of this sub ID from 4 to 6 or [AUTO]. [AUTO] is selected by default. If [AUTO] is selected, a sub ID (4 to 6 digits, selected randomly) is added according to the status of the file name.</p>

❑ Setting up Single Page Data Saving Directory

If [SINGLE] is selected in [MULTI/SINGLE PAGE] on the scan menu of this equipment, the scanned data are saved as a single-page file. This setting is to select whether a subfolder is created or not when you are saving a single-page file.

	Item name	Description
1	Save under a subfolder	A subfolder is created in a specified directory and you can save the file into it.
2	Save without creating a subfolder	A subfolder is not created and the file is saved in a specified directory.

❑ Setting up File Composition

If [SINGLE] is selected in [MULTI/SINGLE PAGE] on the scan menu of this equipment, the scanned data are saved as a single-page file. This setting is to select a page configuration of a single-page file to be saved. The added information will also be applied to file names attached to E-mails.

	Item name	Description
1	Scanning 1 page makes 1 file. (2-sided originals become 2 files.)	When 1 page of an original is scanned, the scanned data are saved as 1 file. When you scan 1 sheet of a 2-sided original, for example, the data of its front side are saved as 1 file and those of its back side are also saved as 1 file.
2	Make to the file like a scanned manuscript. (2-sided originals become 1 files.)	When 1 page of an original is scanned, the scanned data are saved as 1 file. When you scan 1 sheet of a 2-sided original, for example, the data of both the front and back sides (= 2 pages) are saved as 1 file.

❑ Setting up User Name and Password at User Authentication for Save as File

If user authentication is enabled, you can select whether a user name and a password used for user authentication are automatically applied to [LOGIN USER NAME] and [PASSWORD] to be used for saving files into a network folder (specified in REMOTE 1/2) or not. This setting is applied only when [Use Network Folder Destination] of the Destination setting for the Remote 1 or the Remote 2 is checked.

	Item name	Description
1	User name and password of the device	User names and passwords being logged in will not be applied. Enter [LOGIN USER NAME] and [PASSWORD] as required when scanning originals.
2	Login User Name and Password (Template registration User Name and Password is prioritized to expand template)	A user name and a password being logged in will be automatically applied. When a template is used, a user name and a password registered there will be automatically applied.

	Item name	Description
3	Login User Name and Password (Login User Name and Password is prioritized to expand template)	A user name and a password being logged in will be automatically applied. When a template is used, the user name and password being logged in will be applied.

❑ Setting up Searching Interval

Select the interval for searching expired files in the “FILE_SHARE” folder. The content of this setting will also be applied to files in e-Filing boxes.

	Item name	Description
1	Deleting Expired File	<p>This equipment searches expired files every time a specified period of time has passed. The period can be selected from 1 to 24 hours. 12 hours is set by default.</p> <p>Tip</p> <p>You can set the expiration date of each file in the “FILE_SHARE” folder or whether to delete expired files or not using the items below.</p> <p> P.182 “Setting up Storage Maintenance”</p>


❑ Setting up Remote 1 and Remote 2 Settings

In Remote 1 and Remote 2, you can specify how users can select the network folders for Save as file destination when you select [Use Network Folder Destination] in the Destination setting. You can specify two network folders; Remote 1 and Remote 2. The setting items are the same for both Remote 1 and Remote 2.

Note

The network folder as a destination must be set to be shared by all users.

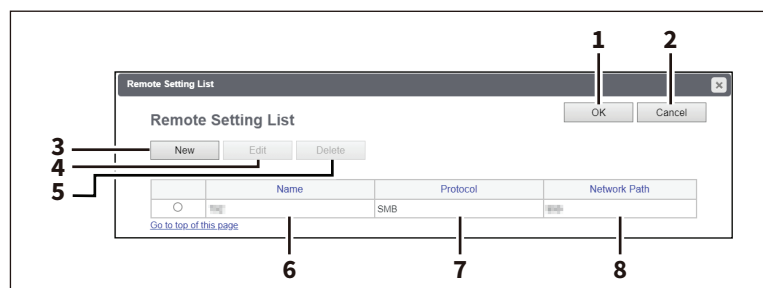
	Item name	Description
1	Allow user to register remote server details from panel	Select whether to allow users to register the remote servers from the control panel.

	Item name	Description
2	[Remote 1]/[Remote 2]	Select the remote network folder you want to use.
3	Allow the following network folder to be used as a destination	<p>Select this to restrict users to select only the network folder that you have specified. Otherwise, select [Allow user to select network folder to be used as a destination].</p> <p>[Remote Setting List] button — Sets a list of network folders for Save as file destination, which can be selected from Remote 1 and Remote 2. To select the specified setting list from the touch panel, you must select [Allow user to select network folder to be used as a destination].</p> <p> P.188 “[Remote Setting List] screen”</p>
4	Allow user to select network folder to be used as a destination	<p>Select this to allow users to specify a network folder as a destination. When the list of Save as file destinations has been set in [Remote Setting List], you can select a network folder from the list. Otherwise, select [Allow the following network folder to be used as a destination].</p> <div style="background-color: #d3d3d3; padding: 2px; margin: 5px 0;">Tip</div> <p>If you want to allow users to specify either Remote 1 or Remote 2, select the one that is not set for the network folder as a destination and select [Allow user to select network folder to be used as a destination] of the selected folder.</p>
5	Protocol	<p>Select the protocol to be used for uploading a file to the network folder.</p> <ul style="list-style-type: none"> • SMB — Select this to send a file to the network folder using the SMB protocol. • FTP — Select this to send a file to the FTP server. • FTPS — Select this to send a file to the FTP server using FTP over SSL/TLS. • NetWare IPX/SPX — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol. • NetWare TCP/IP — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol.
6	Server Name	<p>When you select [FTP] as the protocol, enter the FTP server name or IP address where a scanned file will be sent. For example, to send a scanned file to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box.</p> <p>When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).</p> <p>When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.</p> <p>You can enter up to 64 alphanumeric characters and symbols.</p>
7	Port Number(Command)	<p>Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number. You can enter a value in the range from 0 to 65535 using numbers and hyphens (-). “-” is set as the default.</p>

	Item name	Description
8	Network Path	When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”. When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”. When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”. You can enter up to 128 alphanumerical characters and symbols.
9	Login User Name	Enter the log-in user name to access an SMB server, an FTP server, or a NetWare file server, if required. When you select [FTP] as the protocol, an anonymous log-in is assumed if you leave this box blank. You can enter up to 32 alphanumerical characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.
10	Password	Enter the password to access an SMB server, an FTP server, or a NetWare file server, if required. You can enter up to 32 alphanumerical characters, symbols, and spaces. A single space only can also be entered.
11	Retype Password	Enter the same password again for a confirmation.
12	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.

[Remote Setting List] screen

In this screen, you can set a list of network folders for Save as file destination, which can be selected from Remote 1 and Remote 2. You can register up to 30 items in the Remote Setting List.



	Item name	Description
1	[OK] button	Registers the remote setting list.
2	[Cancel] button	Cancels the registration of the remote setting list.
3	[New] button	Sets a new remote setting. P.189 “[Remote Setting] screen”
4	[Edit] button	Edits the item selected in the remote setting list. P.189 “[Remote Setting] screen”
5	[Delete] button	Deletes the item selected in the remote setting list.
6	Name	Displays the name of the remote setting.
7	Protocol	Displays the protocol of the remote setting.
8	Network Path	Displays the network path of the remote setting.

[Remote Setting] screen

In this screen, you can set the network folders for Save as file destination that are to be registered in the list.

The screenshot shows the [Remote Setting] dialog box. It has a title bar with 'Remote Setting' and a close button. Below the title bar are 'Save' and 'Cancel' buttons. The main area contains the following fields and controls:

- 1**: [Save] button
- 2**: [Cancel] button
- 3**: [Execute] button
- 4**: *Required *Name (text input)
- 5**: Protocol (radio buttons: ☒ SMB, ☐ FTP, ☐ FTPS, ☐ NetWare IPX/SPX, ☐ NetWare TCP/IP)
- 6**: Server Name (text input)
- 7**: Port Number(Command) (text input)
- 8**: Network Path (text input)
- 9**: Login User Name (text input)
- 10**: Password (text input)
- 11**: Retype Password (text input)

	Item name	Description
1	[Save] button	Saves the specified network folder for Save as file destination.
2	[Cancel] button	Cancels the settings.
3	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.
4	Name	Enter the name of the network folder for Save as file destination.
5	Protocol	<p>Select the protocol to be used for uploading a file to the network folder.</p> <ul style="list-style-type: none"> • SMB — Select this to send a file to the network folder using the SMB protocol. • FTP — Select this to send a file to the FTP server. • FTPS — Select this to send a file to the FTP server using FTP over SSL/TLS. • NetWare IPX/SPX — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol. • NetWare TCP/IP — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol.
6	Server Name	<p>When you select [FTP] as the protocol, enter the FTP server name or IP address where a scanned file will be sent. For example, to send a scanned file to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box.</p> <p>When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).</p> <p>When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.</p> <p>You can enter up to 64 alphanumeric characters and symbols.</p>
7	Port Number(Command)	<p>Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number. You can enter a value in the range from 0 to 65535 using numbers and hyphens (-). “-” is set as the default.</p>

	Item name	Description
8	Network Path	When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”. When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”. When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”. You can enter up to 128 alphanumerical characters and symbols.
9	Login User Name	Enter the log-in user name to access an SMB server, an FTP server, or a NetWare file server, if required. When you select [FTP] as the protocol, an anonymous log-in is assumed if you leave this box blank. You can enter up to 32 alphanumerical characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.
10	Password	Enter the password to access an SMB server, an FTP server, or a NetWare file server, if required. You can enter up to 32 alphanumerical characters, symbols, and spaces. A single space only can also be entered.
11	Retype Password	Enter the same password again for a confirmation.

❑ Setting up N/W-Fax Destination

You can configure a network folder to store documents that are sent using the N/W-Fax driver with the Save as file option enabled.

1 N/W-Fax Destination

2 ☐ Do not allow any network folder to be used as a destination

☒ Use Network Folder Destination

	Item name	Description
1	Do not allow any network folder to be used as a destination	Select this to not allow any network folders to be used as Save as file destinations for N/W-Faxes documents. When selected, users can only save an N/W-Fax document with the Save as file option enabled to local storage.
2	Use Network Folder Destination	Select this to allow network folders to be used as Save as file destinations for N/W-Fax documents. When selected, set the N/W-Fax Folder settings to specify which network folder to use.

❑ Setting up N/W-Fax Folder

In the N/W-Fax Folder, you can specify in which network folder N/W-Fax documents are saved.

1 N/W-Fax Folder

2 Protocol ☒ SMB ☐ FTP ☐ FTPS ☐ NetWare IPX/SPX ☐ NetWare TCP/IP

3 Server Name

4 Port Number(Command)

5 Network Path

6 Login User Name

7 Password Retype Password

8 Connection Test Execute

9

	Item name	Description
1	Check box	Select the check box so that the popup prompts you to enter the network path or the server name if you try to save the settings without it.
2	Protocol	<p>Select the protocol for uploading an N/W-Fax document to a network folder.</p> <ul style="list-style-type: none"> • SMB — Select this to send an N/W-Fax document to the network folder using the SMB protocol. • FTP — Select this to send a file to the FTP server. • FTPS — Select this to send a file to the FTP server using FTP over SSL/TLS. • NetWare IPX/SPX — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol. • NetWare TCP/IP — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol.
3	Server Name	<p>When you select [FTP] as the protocol, enter the FTP server name or IP address where an N/W-Fax document will be sent. For example, to send an N/W-Fax document to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box.</p> <p>When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).</p> <p>When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.</p>
4	Port Number(Command)	Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number.
5	Network Path	<p>When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”.</p> <p>When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”.</p> <p>When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”.</p>
6	Login User Name	Enter the login user name to access an SMB server, an FTP server, or a NetWare file server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank. You can enter up to 32 alphanumeric characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.
7	Password	Enter the password to access an SMB server, an FTP server, or a NetWare file server, if required. The space can be entered.
8	Retype Password	Enter the same password again for a confirmation.
9	[Execute] button	Tests the connection using the specified network settings to check if the communications can be established.

Email settings

You can configure the E-mail settings that are needed for Scan to Email operations. This section describes necessary settings for E-mail transmissions.

Tip

The [Email Setting] submenu can be accessed from the [Setup] menu on the [Administration] page. For how to access it and information on the [Setup] menu, see the references below:

- P.14 “Access Policy Mode”
- P.101 “[Setup] Item List”

Note

Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting up Email Setting

You can specify the file format, fragment message size, and default body strings that apply to the Scan to Email documents.

Email

Save

Cancel

Email Setting

Network Setting

1

SMTP Client

Settings

2

POP3 Client

Settings

General Setting

3

From Address

mtfp01@example.com

4

From Name

5

Message Header (Inbound FAX Routing)

Received from: (Sender's TSI)

Received by: (Receiver's CSI)

6

Recipient Domain Name

Disable

7

File Format(Black)

PDF(Multi)

8

File Format(Colour)

PDF(Multi)

9

Number of Retry

3

10

Retry interval

1 Minutes

11

Mail Fragmentation

No Fragmentation

12

Default Subject

Factory Default

13

Add the date and time to the Subject

Enable

14

Editing of Subject

Enable

15

Default Body Strings

16

Body String Transmission

Enable

17



BCC Address Display on Job Log, Job Status

OFF


18

From Address cannot be edited in Scan to Email.

	Item name	Description
1	SMTP Client	<div>Specify SMTP transmission for e-mails.</div> <div>Tip</div> <div>For how to set SMTP Client, see the reference below:</div> <div>P.155 “Setting up SMTP Client”</div>

	Item name	Description
2	POP3 Client	<p>Specify the POP3 server that receives e-mail print jobs.</p> <p>Tip</p> <p>For how to set POP3 Client, see the reference below:  P.158 “Setting up POP3 Client”</p>
3	From Address	<p>Enter the E-mail address of this equipment.</p> <p>Tip</p> <ul style="list-style-type: none"> • Email addresses are displayed on the transmission/reception history (log). • The operation using easy-to-understand addresses is recommended. <p>Note</p> <p>The [From Address] must be entered to enable E-mail transmission. However, the E-mail address of the user who is logged in to this equipment will be automatically set if any user management settings apart from MFP local authentication are enabled. For more information about User Management Setting, see the reference below:  P.73 “[User Management]”</p>
4	From Name	Enter the name of this equipment.
5	Message Header (Inbound FAX Routing)	Select TTI to be used as a subject when the received Internet Fax is forwarded.
6	Recipient Domain Name	<p>Enable or disable automatic addition of a domain name while a destination is being entered.</p> <ul style="list-style-type: none"> • Enable — Select this to add a domain name. • Disable — Select this not to add a domain name. <p>Enter the domain name to be added in the text box. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), # and \ (backslash).</p>

	Item name	Description
7	File Format(Black)	<p>Select the file format of files to be sent when scanning in black mode.</p> <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • XPS(Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS(Single) — Select this to save scanned images separately as Single-page XPS files. • PDF/A(Multi) — Select this to save scanned images as a Multi-page PDF/A file. • PDF/A(Single) — Select this to save scanned images separately as Single-page PDF/A files. • DOCX(Multi) — Select this to save scanned images as a Multi-page Word file (DOCX) after OCR processing. • DOCX(Single) — Select this to save scanned images as a Single-page Word file (DOCX) after OCR processing. • XLSX(Multi) — Select this to save scanned images as a Multi-page Excel file (XLSX) after OCR processing. • XLSX(Single) — Select this to save scanned images as a Single-page Excel file (XLSX) after OCR processing. • PPTX(Multi) — Select this to save scanned images as a Multi-page PowerPoint file (PPTX) after OCR processing. • PPTX(Single) — Select this to save scanned images as a Single-page PowerPoint file (PPTX) after OCR processing. <p>You can select whether to enable OCR by [Enable OCR].</p>

	Item name	Description
8	File Format(Color)	<p>Select the file format of files to be sent when scanning in color mode.</p> <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • Slim PDF(Multi) — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over quality of image. • Slim PDF(Single) — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over quality of image. • XPS(Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS(Single) — Select this to save scanned images separately as Single-page XPS files. • JPEG — Select this to save scanned images as JPEG files. • PDF/A(Multi) — Select this to save scanned images as a Multi-page PDF/A file. • PDF/A(Single) — Select this to save scanned images separately as Single-page PDF/A files. • DOCX(Multi) — Select this to save scanned images as a Multi-page Word file (DOCX) after OCR processing. • DOCX(Single) — Select this to save scanned images as a Single-page Word file (DOCX) after OCR processing. • XLSX(Multi) — Select this to save scanned images as a Multi-page Excel file (XLSX) after OCR processing. • XLSX(Single) — Select this to save scanned images as a Single-page Excel file (XLSX) after OCR processing. • PPTX(Multi) — Select this to save scanned images as a Multi-page PowerPoint file (PPTX) after OCR processing. • PPTX(Single) — Select this to save scanned images as a Single-page PowerPoint file (PPTX) after OCR processing. <p>You can select whether to enable OCR by [Enable OCR].</p>
9	Number of Retry	Enter the number of times to try sending scanned images when it fails. “3” is set as the default.
10	Retry interval	<p>Enter the interval to try sending scanned images when it fails. [1minutes] is set as the default.</p> <p>Note</p> <p>When the [Number of Retry] and [Retry interval] options are changed, the [Number of Retry] and [Retry interval] options in the Internet Fax settings are also changed.</p> <p> P.199 “Setting up InternetFax Setting”</p>

	Item name	Description
11	Mail Fragmentation	<p>Select whether to fragment E-mail for transmission and select how to fragment it when sending E-mail with attached scanned files.</p> <ul style="list-style-type: none"> • No Fragmentation — Select this to send E-mail without fragmentation. • Size Split — Select this to send an E-mail as splitting it by the size selected from [Split Size]. The fragmented E-mails are combined as one at reception. • Page Split — Select this to send an E-mail as splitting the attached files by the page according to the limit size specified in [Split Size]. The receiver receives the fragmented E-mails with the attached files split. The fragment number/the total number of the E-mails is added to the end of the subject of each E-mail and the fragment number is added to the end of the name of each attached file. All the fragmented E-mails contain the same body text. <p>Note</p> <p>E-mails with the XPS, DOCX, XLSX, and PPTX format files cannot be fragmented.</p>
12	Default Subject	<p>Select whether to set the E-mail subject to the factory default or a desired string.</p> <ul style="list-style-type: none"> • Factory Default — Select this to display the BCC address entry column. • <Entry box> — Enter the desired subject.
13	Add the date and time to the Subject	<p>Select whether to append or not date and time to the E-mail subject. This is set as a default.</p> <ul style="list-style-type: none"> • Enable — Select this to append date and time to the subject. • Disable — Select this to not append date and time to the subject.
14	Editing of Subject	<p>Select whether to allow or not editing of the E-mail subject.</p> <ul style="list-style-type: none"> • Enable — Select this to allow the user to edit the E-mail subject. • Disable — Select this to not allow the user to edit the E-mail subject.
15	Default Body Strings	<p>Enter the body text that will be automatically entered in the [Body] box when users operate Scan to Email from the touch panel. This sets only the default body text, so that it can be changed on each operation by users.</p>
16	Body Strings Transmission	<p>Select whether the body strings will be sent or not.</p>
17	BCC Address Display on Job Log, Job Status	<p>Select the display form of the destination of the BCC address displayed in the scan log and the scan job.</p> <ul style="list-style-type: none"> • ON — Select this to display [Bcc Address], instead of the destination of the BCC address. • OFF — Select this to display the destination of the BCC address.
18	From Address cannot be edited in Scan to Email.	<p>Select this item to prohibit modification of the From Address.</p>

❑ Setting up URL Transmission Settings

You can set to provide a URL (link) to the saving directory of the file instead of attaching it before sending a scanned image by email.

1 — URL Transmission



2 — Threshold to Send Attached File(1-100)

3 — Preservation Period for Download File

4 — Search Interval to delete the Expired Download File

5 — Host Name Format in URL

	Item name	Description
1	URL Transmission	<p>Select whether to enable or disable the function to provide a URL to the saving directory of the scanned data.</p> <ul style="list-style-type: none">• Enable — Provides a URL to the saving directory.• Disable — Sends the data as attachments. <p>Tip</p> <ul style="list-style-type: none">• The scanned data is stored in MFP Local.• If a URL to the saving directory is provided, its link and the preservation period are stated in the email.
2	Threshold to Send Attached File (1-100)	<p>Select the maximum size of an attached file. The allowable range is between 1 MB and 100 MB. Select [Send Email with URL at any time] if you want to provide a URL to the saving directory of the file, regardless of the file size. If a maximum size is specified, any file whose size is smaller than the specified one is attached to an email message. On the other hand, if a file exceeds the specified maximum size, a URL to the saving directory is provided.</p>
3	Preservation Period for Download File	<p>Select the preservation period of the file if a URL to the saving directory is provided. If you do not want to impose any limits on the preservation period, select [Unlimited]. If you prefer to automatically delete download files regularly, select a period until the data is deleted.</p> <p>Tip</p> <p>If the data cannot be stored in MFP Local because it is full, this results in an error. Delete the stored files regularly. If you want to delete them manually, all scanned data in the shared folder is deleted.</p>
4	Search Interval to delete the Expired Download File	<p>Selects the interval of monitoring the expiration of the specified preservation period.</p>

	Item name	Description
5	Host Name Format in URL	<p>Selects the host name of the format.</p> <ul style="list-style-type: none"> • IP Address: Select this to use the IP address set in the equipment. • Host Name (FQDN): Select this to use the FQDN configured with the combination of the host and domain names set in the equipment. • NetBIOS Name: Select this to use the NetBIOS name set in the equipment. <p>Note</p> <ul style="list-style-type: none"> • Be sure to set the domain name of DDNS when [Host Name (FQDN)] is selected. If it has not been set, the IP Address is used for the format of the host name. Perform the name resolution for FQDN in the DNS server so that connection to a URL from a client computer becomes possible.  P.126 “DDNS” • [NetBIOS Name] means “[NetBIOS Name] of SMB” set in this equipment. If [Disable] is selected for [SMB Server Protocol] of SMB, the IP Address is used for the format of the host name.  P.142 “Setting up SMB”

■ InternetFax settings

You can specify Internet Fax settings. This section describes necessary settings for Internet Fax transmissions.

Tip

The [InternetFax] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

Note

Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

□ Setting up InternetFax Setting

You can specify the fragment page size and default body strings that apply to the Internet Faxes.

InternetFax

SaveCancel

InternetFax Setting

Network Setting

1SMTP ClientSettings

2POP3 ClientSettings

3SMTP ServerSettings

General Setting

4From Address

5From Name

6Message Header (Inbound FAX Routing)
☐ Received from: (Sender's TSI)
☒ Received by: (Receiver's CSI)

7Recipient Domain Name
Disable

8Number of Retry
3

9Retry interval
1 Minutes

10Fragment Page Size
No Fragmentation

11Default Body Strings



12Body String Transmission
Enable

13TTI
OFF

14RTI
OFF

15To/Bcc Destination
To

	Item name	Description
1	SMTP Client	Specify SMTP transmission for InternetFax. <div>Tip For how to set SMTP Client, see the reference below: 📖 P.155 “Setting up SMTP Client”</div>
2	POP3 Client	Specify the POP3 server that receives InternetFax print jobs. <div>Tip For how to set POP3 Client, see the reference below: 📖 P.158 “Setting up POP3 Client”</div>
3	SMTP Server	Specify SMTP reception for InternetFax. <div>Tip For how to set SMTP Server, see the reference below: 📖 P.149 “Setting up SMTP Server”</div>

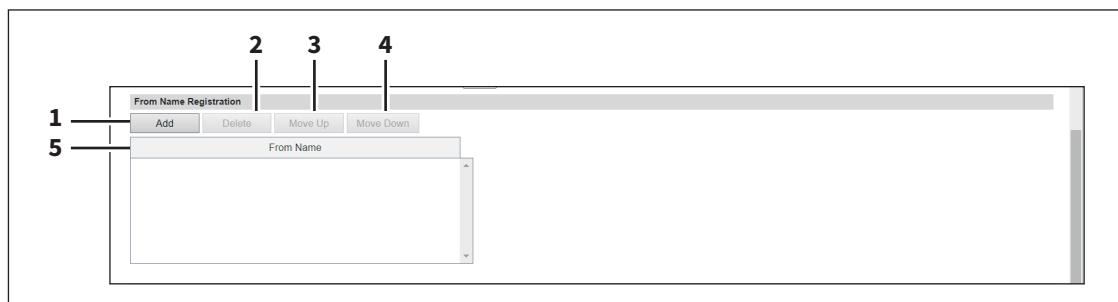
	Item name	Description
4	From Address	<p>Enter the E-mail address of this equipment.</p> <p>Note</p> <p>The [From Address] must be entered to enable Internet Fax transmission. However, the E-mail address of the user who is logged in to this equipment will be automatically set if any user management settings apart from MFP local authentication are enabled. For more information about User Management Setting, see the reference below:  P.73 “[User Management]”</p>
5	From Name	Enter the name of this equipment.
6	Message Header (Inbound FAX Routing)	Select TTI to be used as a subject when the received Internet Fax is forwarded.
7	Recipient Domain Name	<p>Enable or disable automatic addition of a domain name while a destination is being entered.</p> <p>Enable: Select this to add a domain name.</p> <p>Disable: Select this not to add a domain name.</p> <p>Enter the domain name to be added in the text box. You can enter up to 128 alphanumerical characters and symbols other than =, ; (semicolon), # and \ (backslash).</p>
8	Number of Retry	Enter the number of times to try sending the Internet Faxes when it fails. “3” is set as the default.
9	Retry interval	<p>Enter the interval to try sending the Internet Faxes when it fails. [1minutes] is set as the default.</p> <p>Note</p> <p>When the [Number of Retry] and [Retry interval] options are changed, the [Number of Retry] and [Retry interval] options in the E-mail settings are also changed.</p> <p> P.192 “Email settings”</p>
10	Fragment Page Size	Select the size of the message fragmentation.
11	Default Body Strings	Enter the body text that will be automatically entered in the [Body] box when users operate Scan to Internet Fax from the touch panel. This sets only the default body text, so that it can be changed on each operation by users.
12	Body String Transmission	Select whether the body strings will be sent or not.
13	TTI	Specify whether or not to add the sender information in the header.
14	RTI	Specify whether or not to add the sender information in the footer.
15	To/Bcc Destination	<p>You can set the destination of the internet fax to be sent only to To or Bcc.</p> <p>Note</p> <p>When Bcc is set as the destination, To becomes blank and the transmitted internet fax may be treated as spam depending on the settings of the mail server, mailer or security software. Check the settings for spam.</p>

❑ From Name Registration

You can register up to 20 names of the fax senders. The registered sender name can be selected when saving the InternetFax and Fax settings for the templates.

📖 P.312 “InternetFax Setting”

📖 P.313 “Fax Setting”



	Item name	Description
1	[Add] button	Adds a new name of the fax sender. When the entry window appears, you can enter up to 20 characters for a name. Click [Save] to register the name. To stop the setting operation, click the [Cancel] button to close the window.
2	[Delete] button	Deletes the name selected in the list.
3	[Move Up] button	Moves up the name selected in the list.
4	[Move Down] button	Moves down the name selected in the list.
5	From Name	Shows the registered names of the fax senders. You can scroll up or down the list to see up to 20 names.

❑ Report Setting





You can select how to report internet fax results.

The screenshot shows the 'Report Setting' window. It has a title bar and a main content area. On the left side, there are numbered callouts 1 through 6 pointing to specific elements:

- 1** points to the 'Select Agent' button at the top left.
- 2** points to the 'Use login user address (User Authentication)' section, which includes a checked checkbox and two radio button options: 'Use Email Address which was registered Local User' and 'Use Email Address which was LDAP registered' (which is selected).
- 3** points to the '1st Destination' and '2nd Destination' input fields.
- 4** points to the 'Email Setting' section, which includes fields for Subject, From Address, From Name, Body, and File Name.
- 5** points to the 'Save as file Setting' section, which includes fields for Destination and File Name.
- 6** points to the 'Common Setting' section, which includes fields for File Format, Encryption, and Digital Signature.

The 'Server Assignment' section is also visible, showing a table with columns: LDAP Server, Server IP Address, Attribute type of 'User Name', and Attribute type of 'Email Address'. Below this table, it says 'The priority is from the top.'

	Item name	Description
1	[Select Agent] button	<p>You can make detailed settings by selecting one of the following items, and then clicking [Select Agent].</p> <p>Print — Select this to print. There are no settings available in [Select Agent].</p> <p>Save as file — Select this to save as a file. Click [Select Agent] to make settings for [Save as file Setting] and [Common Setting].</p> <p>Email — Select this to send an email. Click [Select Agent] to make address settings, and settings for [Email Setting] and [Common Setting].</p>
2	Use login user address (User Authentication)	<p>Set whether or not to use the E-mail address for a login user as the destination for E-mail transmission during user authentication. You can set the following items when you select this check box.</p> <p>Use Email Address which was registered Local User: The E-mail address for a user set in MFP Local Authentication is used as the destination for E-mail transmission.</p> <p>Use Email Address which was LDAP registered: The E-mail address for a server registered in LDAP Client is used as the destination for E-mail transmission. Click [Server Assignment]. Up to 4 LDAP servers can be assigned. 📖 P.151 “LDAP Client settings”</p>
3	[1st: Destination] / [2nd: Destination] button	<p>This is enabled when you select [Email] from Report Settings, and then click the [Select Agent] button.</p> <p>Click to display the address list where you can set addresses. 📖 P.307 “Destination Setting”</p>

	Item name	Description
4	[Email Setting] button	<p>This is enabled when you select [Email] from Report Settings, and then click the [Select Agent] button.</p> <p>Click to set the following items on the agent settings page for the Email settings.</p> <ul style="list-style-type: none"> • Subject • From Address • From Name • Body • File Name <p> P.316 “Email Setting”</p>
5	[Save as file Setting] button	<p>This is enabled when you select [Save as file] from Report Settings, and then click the [Select Agent] button.</p> <p>Click to set the following items on the agent settings page for the Save as file settings.</p> <ul style="list-style-type: none"> • Destination • File Name <p> P.319 “Save as file Setting”</p>
6	[Common Setting] button	<p>This is enabled when you select [Email] or [Save as file] from Report Settings, and then click the [Select Agent] button.</p> <p>You can set the following items on the agent settings page.</p> <ul style="list-style-type: none"> • File Format • Encryption • Digital Signature <p> P.316 “Email Setting”</p> <p> P.319 “Save as file Setting”</p>

■ Printer/e-Filing settings

Tip

The [Printer/e-Filing] submenu can be accessed from the [Setup] menu on the [Administration] page. For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

❑ Setting up Printer/e-Filing Job Enforcement Continue

	Item name	Description
1	Automatic Change Of Paper Source	Specify whether or not to change the paper source automatically when the size of the original and the paper in the paper source do not match. <ul style="list-style-type: none">• ON — Select this to change the paper source and continue processing the job.• OFF — Select this to stop the job.
2	Paper Of Different Direction ^{*1}	Specify whether or not to copy on paper which is loaded in the paper source in a different orientation from the original. <ul style="list-style-type: none">• ON — Select this to continue processing the job by copying on paper in a different orientation.• OFF — Select this to stop the job.
3	Enforcement Continue (Illegal Paper) ^{*1}	Specify whether or not to continue processing the job forcibly when the specified output tray is incorrect. <ul style="list-style-type: none">• ON — Select this to print to the specified output tray.• OFF — Select this to stop the job.
4	Auto Exit Tray Change (Cascade Print) ^{*1}	Specify whether or not to switch the receiving tray automatically. <ul style="list-style-type: none">• ON — Select this to continue processing the job by switching the receiving tray.• OFF — Select this to stop the job.
5	Suspend Printing if Stapler Empty ^{*1}	Specify whether to stop printing when staples run out. <ul style="list-style-type: none">• ON — Select this to stop printing when staples run out.• OFF — Select this not to stop printing when staples run out.
6	Continue Printing when Punch Dust is full ^{*1}	Specify whether to continue printing when the punch dust bin is full. <ul style="list-style-type: none">• ON — Select this to continue printing even when the punch dust bin is full.• OFF — Select this to stop printing when the punch dust bin is full.

^{*1} This function is not available for some models.

■ Printer settings

You can configure how the printer works and the printer options needed for the raw print jobs.

Tip

The [Printer] submenu can be accessed from the [Setup] menu on the [Administration] page.

For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

□ Setting up General Setting

In General Setting, you can specify the printer related options.

	Item name	Description
1	Period of time to save Private, Hold, Proof and invalid Jobs	Select how long the private, hold, and test print jobs are kept. You can select in the range from 1 to 12 hours, or from 1 to 30 days. Select [Indefinite] to retain all jobs in the queues until a user manually deletes them. [14 Days] is set as the default.
2	LT<-->A4 / LD <-->A3 ^{*1}	Select whether to print a document intended for one paper size can be printed on paper of a different size. For example, you can print a document set up for Letter size on A4 paper. When disabled, this equipment will prompt users for the correct paper size. [Enable] is set as the default.
3	Wide A4 Mode (for PCL)	Select whether the width of the printable area of copy paper is widened or not when you are printing a PCL print job on A4 paper. Select [Enable] to widen it for approx. 3.5 mm / 0.14 inch (when in a portrait direction) and approx. 1.5 mm / 0.06 inch (when in a landscape direction). Thus more data can be printed for each line. [Disable] is set as the default. Note This item is available only for some models.
4	Restriction for Print Job	Select whether or not to restrict printing certain print jobs. <ul style="list-style-type: none"> • None — Select this to print all data. • Only Private — Select this to print private print jobs only. • Only Hold — Select this to print hold print jobs only. • Only Private/Hold — Select this to print private and hold print jobs only.

^{*1} The [LD <--> A3] function is not available for some models.

❑ Setting up Default Direct Print Setting

You can set the default settings for USB Direct Print and E-mail Direct Print.

Note

Some print settings do not work on printouts according to file formats.

- The [PDF Overprint], [PDF Prioritize Original Size], and [PDF Size Options] settings can work only on PDF printouts.
- The [Enable Print Header] and [Enable Print Message Body] settings can work only on the E-mail Direct Print function.
- E-mails with encrypted PDF (secure PDF) files attached cannot be printed by the E-mail Direct Print function.

Color models

The screenshot shows the 'Default Direct Print Setting' dialog box. On the left, there is a list of settings numbered 1 through 10. On the right, the corresponding settings are displayed in a form. The settings are: 1. Color Mode (Auto Color), 2. 2-Sided (1Side), 3. Size (A4), 4. Finishing (NON-Staple), 5. PDF Overprint (ON(PDF/X only)), 6. PDF Prioritize Original Size (ON), 7. PDF Size Options (Fit), 8. Email Direct Print (Disable), 9. Enable Print Header (Disable), and 10. Enable Print Message Body (Enable).

Monochromatic models

The screenshot shows the 'Default Direct Print Setting' dialog box for monochromatic models. The settings are: 2. 2-Sided (1Side), 3. Size (A4), 4. Finishing (NON-Staple), 6. PDF Prioritize Original Size (ON), 7. PDF Size Options (Fit), 8. Email Direct Print (Disable), 9. Enable Print Header (Disable), and 10. Enable Print Message Body (Enable). Note that item 1 (Color Mode) is not visible in this view.

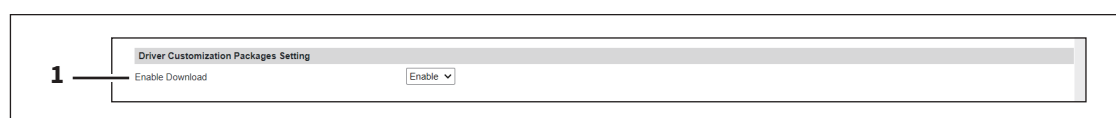
	Item name	Description
1	Color Mode	Select the default color mode setting for direct print. This item is available only for color models. <ul style="list-style-type: none"> • Auto Color — Select this to enable auto color print. • Full Color — Select this to enable full color print. • Black — Select this to enable monochrome print.
2	2-Sided	Select the default setting to print one side or both sides of paper for direct print. This item is available only when Automatic Document Feeder has been installed. <ul style="list-style-type: none"> • 1Side — Select this to enable one-side print. • Book — Select this to enable duplex book print. • Tablet — Select this to enable duplex tablet print.
3	Size	Select the default paper size for direct print.
4	Finishing ^{*1}	Select the default setting as to whether to staple paper or not. <ul style="list-style-type: none"> • NON-Staple — Select this to disable stapling paper. • Upper Left — Select this to staple paper on the upper left corner. • Upper Right — Select this to staple paper on the upper right corner.

	Item name	Description
5	PDF Overprint	Select the default setting as to whether to overprint colors in PDF files or not. <ul style="list-style-type: none"> • OFF — Select this to disable overprint. • ON — Select this to enable overprint. • ON (PDF/X only) — Select this to enable overprint only for PDF/X files.
6	PDF Prioritize Original Size	Select the default setting as to whether to prioritize the PDF original size or not. <ul style="list-style-type: none"> • OFF — Select this to prioritize the selected paper size over the original size. • ON — Select this to prioritize the original size over the selected paper size, which prints PDF files without enlargement or reduction.
7	PDF Size Options	Select the default setting as to how to print PDF files when [PDF Prioritize Original Size] is set to [OFF]. <ul style="list-style-type: none"> • Fit — Select this to enlarge or reduce pages by fitting the original size to the paper size. • Shrink Oversized Pages — Select this to reduce pages if the original size is larger than the paper size. Pages are printed without enlargement if the original size is equal to or smaller than the paper size.
8	Email Direct Print	Select the default setting as to whether to print E-mails with PDF, JPEG, and XPS files attached by the Email Direct Print function. <ul style="list-style-type: none"> • Disable — Select this to disable Email Direct Print. • Auto — Select this to process Email Direct Print automatically.
9	Enable Print Header	Select whether to print the E-mail header when receiving E-mail print jobs. [Disable] is set as the default.
10	Enable Print Message Body	Select whether to print the body message when receiving E-mail print jobs. [Enable] is set as the default.

*1 This function is not available for some models.

❑ Setting up Driver Customization Packages Setting

You can set the function to download the customization packages for the printer driver.



	Item name	Description
1	Enable Download	Select whether the function is enabled or disabled to download customization packages for the printer driver. <ul style="list-style-type: none"> • Enable — Select this to enable this download function. • Disable — Select this to disable this download function.

❑ Setting up Default Raw Job Setting

In Default Raw Job Setting, you can specify the default raw job setting, which applies to a raw job for which no queue name is specified or for which a specified queue name does not exist.

Note

This setting is available only for some models.

Tip

You can also add LPR queue names and specify the raw job setting for each queue.

📖 P.209 “Setting up Raw Job Setting”

Item	Setting	Value
1	Raw Jobs - Duplex Printing	Disable
2	Raw Jobs - Default Paper Size	A4
3	Raw Jobs - Default Paper Type	Plain
4	Raw Jobs - Default Orientation	Portrait
5	Raw Jobs - Default Stapling	OFF
6	Raw Jobs - Default Output Tray	Inner Tray
7	PCL Form Line	12.0
8	PCL Font Pitch	10.0
9	PCL Font Point Size	12.0
10	PCL Font Number	0
11	PCL Line Termination	Auto
12	Symbol set	Roman-8
13	Paper Source	Auto
14	Do not Print Blank Pages	OFF
15	Letterhead Print Mode	OFF

	Item name	Description
1	Raw Jobs - Duplex Printing	Select whether a raw job will be printed on both sides of the paper.
2	Raw Jobs - Default Paper Size	Select the default paper size that applies to a raw job.
3	Raw Jobs - Default Paper Type	Select the default paper type that applies to a raw job.
4	Raw Jobs - Default Orientation	Select the default orientation that applies to a raw job.
5	Raw Jobs - Default Stapling ^{*1}	Select whether a raw job will be stapled.
6	Raw Jobs - Default Output Tray ^{*1}	Select the default output tray that applies to a raw job. A banner page that is created by NetWare, UNIX, and Windows operating systems also will be outputted to the tray set here.
7	PCL Form Line	Enter the point size of line spacing. (12.00 makes 6 lines/inch)
8	PCL Font Pitch	Enter the font pitch when the selected font number represents a fixed pitch scalable font. The font pitch indicates the number of ANK characters per inch. 10 pitch prints 10 ANK characters within an inch.
9	PCL Font Point Size	Enter the font size when the selected font number represents a proportionally spaced scalable font. The Font Size option allows you to determine the point size (height) of the default font.
10	PCL Font Number	Enter the font number of the internal PCL font to be used as the default font for printing. You can check the font numbers and internal PCL fonts in the Internal PCL Font List. For the internal PCL fonts, see the reference below: Specifications - SPECIFICATIONS OF EQUIPMENT - List of Internal Fonts - Internal PCL fonts list
11	PCL Line Termination	Select the type of the line termination.
12	Symbol set	Select the symbol set that applies to a raw job.
13	Paper Source	Select the paper source that applies to a raw job.

	Item name	Description
14	Do not Print Blank Pages	<p>Select whether blank pages are printed or not.</p> <p>Note</p> <p>When printing is performed using the UNIX filters or CUPS, this setting is not reflected. If you do not want to print blank pages in these printings, enable [Do not Print Blank Pages] in the UNIX filter command or CUPS setting. For the setting instructions, see the references below: Installation - INSTALLING PRINTER DRIVERS FOR UNIX/Linux - Setting Up the CUPS - Configuring UNIX/Linux printing using CUPS Print - OTHER PRINTING METHODS - Printing From UNIX/Linux - General options</p>
15	Letterhead Print Mode	<p>Select whether the last page (odd page number) is printed on the same side as the other odd-number pages when printing both sides of a Raw print job whose total page number is odd. Select [ON] to print the last page on the same side (back) as the other odd-number pages. Select [OFF] to print it on the same side (front) as even-number pages.</p> <p>Note</p> <p>This item is available only for some models.</p>

*1 This function is not available for some models.

❑ Setting up Raw Job Setting

In Raw Job Setting, you can add up to 16 LPR queue names and specify the raw job setting for each queue. These queue names can be used when printing without a printer driver, such as printing from UNIX workstation.

Note

This setting is available only for some models.

Queue Name	Duplex Printing	Paper Size	Paper Type	Orientation	Stapling	Output Tray	PCL Form Line	PCL Font Pitch	PCL Font Point Size	PCL Font Number	PCL Line Termination	Symbol set	Paper Source	Do not Print Blank Pages	Letterhead Print Mode
QueueName001	Disable	A4	Plain	Portrait	OFF	Inner Tray	12.0	10.0	12.0	0	Auto	Roman-8	Auto	OFF	OFF

	Item name	Description
1	[Add] button	Select this to add a LPR queue. 📖 P.210 “[Add New LPR Queue] screen”
2	[Edit] button	Select this to edit the LPR queue selected in the LPR queue list. 📖 P.210 “[Add New LPR Queue] screen”
3	[Delete] button	Select this to delete the LPR queue selected in the LPR queue list.
4	LPR queue list	Select this to display the list of registered LPR queues.

[Add New LPR Queue] screen

	Item name	Description
1	Queue Name	Enter the queue name with up to 31 alphanumerical characters. The queue name is case sensitive so that “Queue1” and “queue1” will be added as different queues.
2	Duplex Printing	Select whether a raw job will be printed on both sides of the paper.
3	Paper Size	Select the default paper size that applies to a raw job.
4	Paper Type	Select the default paper type that applies to a raw job.
5	Orientation	Select the default orientation that applies to a raw job.
6	Stapling ^{*1}	Select whether a raw job will be stapled.
7	Output Tray ^{*1}	Select the default output tray that applies to a raw job. A banner page that is created by NetWare, UNIX, and Windows operating systems also will be outputted to the tray set here.
8	PCL Form Line	Enter the number of lines printed per page.
9	PCL Font Pitch	Enter the font pitch when the selected font number represents a fixed pitch scalable font. The font pitch indicates the number of ANK characters per inch. 10 pitch prints 10 ANK characters within an inch.
10	PCL Font Point Size	Enter the font size when the selected font number represents a proportionally spaced scalable font. The Font Size option allows you to determine the point size (height) of the default font.
11	PCL Font Number	Enter the font number of the internal PCL font to be used as the default font for printing. You can check the font numbers and internal PCL fonts in the Internal PCL Font List. For the internal PCL fonts, see the reference below: Specifications - SPECIFICATIONS OF EQUIPMENT - List of Internal Fonts - Internal PCL fonts list
12	PCL Line Termination	Select the type of the line termination.
13	Symbol set	Select the symbol set that applies to a raw job.
14	Paper Source	Select the paper source that applies to a raw job.

	Item name	Description
15	Do not Print Blank Pages	<p>Select whether blank pages are printed or not.</p> <p>Note</p> <p>When printing is performed using the UNIX filters or CUPS, this setting is not reflected. If you do not want to print blank pages in these printings, enable [Do not Print Blank Pages] in the UNIX filter command or CUPS setting. For the setting instructions, see the references below:</p> <p>Installation - INSTALLING PRINTER DRIVERS FOR UNIX/Linux - Setting Up the CUPS - Configuring UNIX/Linux printing using CUPS</p> <p>Print - OTHER PRINTING METHODS - Printing From UNIX/Linux - General options</p>
16	Letterhead Print Mode	<p>Select whether the last page (odd page number) is printed on the same side as the other odd-number pages when printing both sides of a Raw print job whose total page number is odd. Select [ON] to print the last page on the same side (back) as the other odd-number pages. Select [OFF] to print it on the same side (front) as even-number pages.</p> <p>Note</p> <p>This item is available only for some models.</p>

*1 This function is not available for some models.

■ Print Service settings

You can configure such print services as Raw TCP Print, LPD Print, IPP Print, FTP Print, NetWare Print, Email Print, and Multi Station Print.

Tip

The [Print Service] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

- 📖 P.14 “Access Policy Mode”
- 📖 P.101 “[Setup] Item List”

Note

Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

□ Setting up Raw TCP Print

In Raw TCP Print, you can enable or disable the Raw TCP print service.

Print Service

Print Service Setting

Raw TCP Print

- 1 Enable Raw TCP (Enable)
- 2 Port Number (9100)
- 3 Enable Raw bi-directional (Disable)

Save Cancel

	Item name	Description
1	Enable Raw TCP	Enable or disable Raw TCP print service. [Enable] is set as the default.
2	Port Number	If enabling the Raw TCP, enter the Raw TCP port number for the Raw TCP print. You can enter a value in the range from 1024 to 32767. Generally the default value “9100” is used. Note When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you set it by mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.
3	Enable Raw bi-directional	Enable or disable Raw bi-directional communication. [Disable] is set as the default. Note This item is available only for some models.

□ Setting up LPD Print

In LPD Print, you can set the LPD print options to enable the LPD/LPR print service.

LPD Print

- 1 Enable LPD (Enable)
- 2 Port Number (515)
- 3 Banners (OFF)

	Item name	Description
1	Enable LPD	Enable or disable LPD print service. [Enable] is set as the default.

	Item name	Description
2	Port Number	<p>Enter the port number for LPR printing. You can enter a value in the range from 1 to 65535. Generally the default value “515” is used.</p> <p>Note</p> <p>When the same port number as the secondary one in the HTTP setting (SSL/TLS port number when SSL/TLS in the HTTP setting is enabled) is selected, you cannot access TopAccess or the e-Filing web utility. If you set it by mistake, use the touch panel of the equipment to change the HTTP setting and enter the correct port number.</p>
3	Banners	<p>Select whether to print a banner page for each print job using LPR printing. [OFF] is set as the default.</p> <p>Note</p> <p>This item is available only for some models.</p>

□ Setting up IPP Print

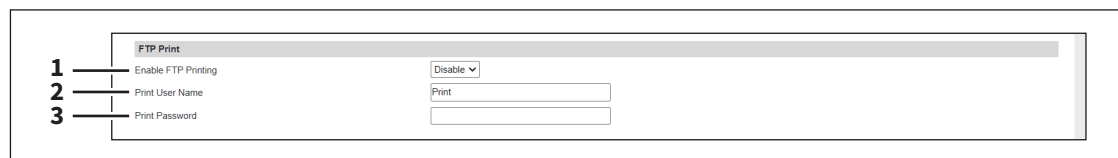
In IPP Print, you can set the IPP Print options to enable the IPP print service.

	Item name	Description
1	Enable IPP	Enable or disable the IPP print service. [Enable] is set as the default.
2	Port80 Enable	<p>Enable or disable Port80 for IPP printing. Port631 is usually used for IPP access so users must specify the IPP port to the URL, i.e. “http://<IP address or DNS name>:631/Print”, for the IPP port. When this is enabled, this equipment allows IPP access through the Port80, which is the default port for the HTTP access so users do not have to specify the port number in the IPP port, i.e. “http://<IP address or DNS name>/Print”. [Disable] is set as the default.</p>
3	Port Number	<p>If enabling the IPP, enter the IPP port number. You can enter a value in the range from 1 to 65535. Generally the default value “631” is used.</p> <p>Note</p> <p>The same port numbers as the ones for the following settings are not usable. Change the applicable port number before that for the Port Number is set.</p> <ul style="list-style-type: none"> • HTTP Network Service / Primary Port Number • HTTP Network Service / Secondary Port Number • HTTP Network Service / SSL/TLS Port Number
4	URL	Display the URL for IPP printing. You cannot change the URL for IPP printing. This URL should be set as the print port when users set up the printer driver for IPP printing.

	Item name	Description
5	Enable SSL/TLS	<p>Enable or disable SSL/TLS for IPP printing. [Enable] is set as the default.</p> <p>Tip</p> <ul style="list-style-type: none"> When the SSL/TLS is enabled, users can print to the IPP print port using the SSL/TLS. To print to the IPP print port using the SSL/TLS, specify the following URL for the IPP print port. https://<IP Address>:<SSL/TLS Port Number>/Print Example: https://192.168.53.204:631/Print Not all operating systems support SSL/TLS for all protocols.
6	SSL/TLS Port Number	<p>Enter the port number for SSL/TLS. You can enter a value in the range from 1 to 65535. Generally the default value “631” is used.</p> <p>Note</p> <p>The same port numbers as the ones for the following settings are not usable. Change the applicable port number before that for the SSL/TLS Port Number is set.</p> <ul style="list-style-type: none"> HTTP Network Service / Primary Port Number HTTP Network Service / Secondary Port Number HTTP Network Service / SSL/TLS Port Number
7	SSL/TLS URL	<p>Display the SSL/TLS URL for IPP printing. You cannot change the SSL/TLS URL for IPP printing. This SSL/TLS URL should be set as the print port when users set up the printer driver for IPP printing if the SSL/TLS for IPP printing is enabled.</p>
8	Printer Name	<p>Enter the printer name for IPP printing. You can enter up to 127 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash). The MFP name is set as the default.</p>
9	Authentication	<p>Enable or disable the authentication for creating the IPP queue on the client computers. When this is enabled, the dialog box to enter a user name and password will be displayed when a user creates the IPP print port.</p> <ul style="list-style-type: none"> Disable — Select this to disable the authentication. Basic — Select this to enable the authentication. <p>Note</p> <p>When IPP printing is used for printing from the macOS printer driver (PPD), do not enable the authentication. The macOS printer driver (PPD) does not support the authentication for IPP printing.</p>
10	User Name	<p>Enter the user name when the Authentication option is enabled. Users must enter this user name to create an IPP queue on the client computers. You can enter up to 127 alphanumerical characters and symbols other than =, ; (semicolon), #, @, and \ (backslash).</p>
11	Password	<p>Enter the password when the Authentication option is enabled. Users must enter this password to create an IPP queue on the client computers. You can enter up to 127 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash). “password” is set as the default.</p>

□ Setting up FTP Print

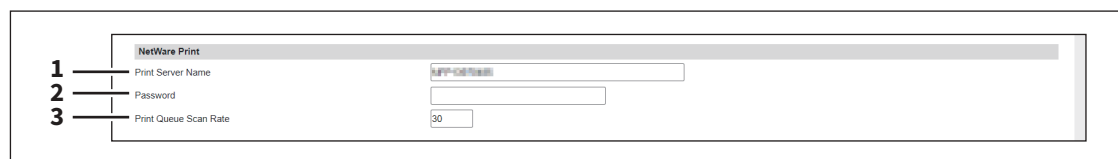
In FTP Print, you can set the FTP Print options to enable the FTP print service.



	Item name	Description
1	Enable FTP Printing	Enable or disable FTP print service. [Disable] is set as the default.
2	Print User Name	Enter the user name if you want to request the log-in user name from someone who attempts FTP printing. You can enter up to 31 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash). If you leave this box blank, the default user name "Print" is used.
3	Print Password	Enter the password if you want to request the log-in password of users who attempt FTP printing. You can enter up to 31 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).

□ Setting up NetWare Print

In NetWare Print, you can set the NetWare print options to enable the Novell print service.



	Item name	Description
1	Print Server Name	Enter the print server name that is created in the NetWare file server. You can enter up to 47 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash). The MFP name is set as the default.
2	Password	Enter the password that is set to the print server, if required. You can enter up to 31 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash).
3	Print Queue Scan Rate	Enter how frequently to scan the print queues for print jobs. This should be entered in seconds. You can enter between 1 to 255. "30" is set as the default.

❑ Setting up Email Print

In Email Print, you can set how the E-mail print jobs are printed.

	Item name	Description
1	Enable Print Header	Select whether to print the E-mail header when receiving E-mail print jobs. [Disable] is set as the default.
2	Enable Print Message Body	Select whether to print the body message when receiving E-mail print jobs. [Enable] is set as the default.
3	Maximum Email Body Print	Enter the maximum number of pages to print the body strings of the received E-mail print job. You can enter between 1 to 99. "5" is set as the default.
4	Enable Print Email Error	Select whether to print the report when an error occurs for E-mail printing. [Enable] is set as the default.
5	Enable Email Error Forward	Select whether to send an error message to an administrative E-mail address when E-mail printing cannot be completed. [Disable] is set as the default.
6	Email Error Transfer Address	If enabling the Email Error Forward, enter an administrative E-mail address where the error message is sent. You can enter up to 192 alphanumeric characters and symbols other than =, ; (semicolon) , #, and \ (backslash).
7	Enable Partial Email	Select whether to print E-mail jobs that are partially received. [Enable] is set as the default.
8	Partial Wait time	Enter how long this equipment should wait before printing a partial E-mail job. Specify within the range from 1 to 168 hours. "24" is set as the default.
9	MDN Reply	Select whether to send an MDN message reply or not when the equipment receives an E-mail print job with an MDN request. [Disable] is set as the default.

❑ Setting up USB Cable Print

	Item name	Description
1	USB Printing	Set whether to enable or disable USB cable printing.
2	USB Cable Print Mode	Select the mode used for printing via a USB connection. IPP Over USB — Normally use this mode. Legacy USB (Win) — Use this mode when you are already using our MFPs and want to grant priority to the compatibility with them.

❏ Setting up Multi Station Print

For the operation of the setting, see the reference below:

📖 P.390 “Setting Multi Station Print”

Note

- You need the Multi Station Print Enabler option to use the [Multi Station Print] function. Contact your service technician for details.
- If you have selected [Use Common Settings] on the [MFP Collaboration] > [Multi Station Print] screen, you cannot add and delete the MFPs on this screen.
📖 P.230 “Multi Station Print”

Tip

- Use this service in an environment where the number of PCs to connect to 1 MFP is 30 or less.
- You can connect up to 10 MFPs in a group and connect up to 5 groups including a group to which this MFP belongs: you can add 4 groups for the connection.

The screenshot shows the 'Multi Station Print' configuration interface. On the left, a vertical list of numbers 1 through 22 points to specific UI elements. The interface includes sections for general settings (Enable, Document Expired Time, Number of Display Job, Sort Order), a list of MFPs (with Add/Delete buttons), a table for MFP groups (with Group Name, Primary IP Address / Host Name, and Secondary IP Address / Host Name columns), and a 'Delete All' button at the bottom.

	Item name	Description
1	Enable Multi Station Print	Specify whether to enable or disable the Multi Station Print service.
2	Document Expired Time	Specify the retention period of the printed document.
3	Number of Display Job	Specify the number of jobs to be displayed.
4	Sort Order	Specify the display order.
5	Thumbnail List	Select whether to display thumbnail images of the multi station print files in the document list on the control panel. Thumbnail images appear for PDF and JPEG files and the fixed icon appears for files of other formats. <div style="background-color: black; color: white; padding: 2px; display: inline-block;">Note</div> A thumbnail just represents the image of a file. The image may differ from the original, having parts of it cut or blank spaces added.

	Item name	Description
6	Print Order	<p>Specify the print order.</p> <p>Tip</p> <p>When you select [Indication Order] from [Print Order], documents are printed according to the [Sort Order] setting at the item 4.</p>
7	Enable Printed Jobs	Specify whether to enable or disable reprinting.
8	Connection MFP	<p>Specify the following communication settings for the multi station print.</p> <ul style="list-style-type: none"> • Port Number — Enter the port number. • Enable SSL/TLS — Select the SSL/TLS setting for the multi station print. <ul style="list-style-type: none"> - Disable — Select this to disable SSL/TLS. - Verify with imported CA certification(s) — Select this to use CA certificates for connection. You need to export the certificate from each MFP and import it into all MFPs. - Accept all certificates without CA — Select this to accept all certificates without CA. There is no need to import the certificate of each MFP. • Authentication — Select [Disable] or [Basic] for authentication. [Disable] is set as the default. • User Name — Enter the user name. You can enter up to 127 alphanumeric characters and symbols except = ; # @ \. • Password — Enter the password of the user. You can enter up to 127 alphanumeric characters and symbols except = ; # \. <p>Note</p> <p>All MFPs should have the same settings for the connection.</p> <p>Tip</p> <p>Although the multi station print is available even if the user authentication is disabled, this MFP cannot be connected to other MFPs: the job list is not shared.</p>
9	[Add] button	Allows you to add the device to connect.
10	[Delete] button	Allows you to delete the selected device.
11	Connection MFP entry field	<p>Enter the IP address or host name of the MFP you want to register.</p> <p>Tip</p> <p>If the user authentication is disabled with more than one address registered in the [Connection MFP] list, the [Connection MFP] settings are not displayed.</p>
12	IP Address / Host Name	Shows the IP address or host name of the registered MFP.
13	[Connect] button	<p>Tests the connection with the specified MFP to check if the communications can be established.</p> <p>Note</p> <p>Be sure to save the Multi Station Print settings with the [Save] button before you test the MFP connection with the [Connect] button.</p>
14	[TopAccess] button	Starts TopAccess.
15	Group Connection Enable	Select whether to connect the MFP groups. [Disable] is set as the default.

	Item name	Description
16	Own Group Name	<p>Enter a group name to which this MFP belongs. You can enter up to 12 characters.</p> <p>Note</p> <p>All groups should share the same name of each group for the connection.</p>
17	[Add] button	<p>Allows you to add a group. Click this button to show the [Add Connection Group Information] screen. Set the following information and click [Save] to save the settings. To edit the information, click the name of the group added in the list.</p> <ul style="list-style-type: none"> • Group Name — Enter the name of the connection group. You can enter up to 12 characters. • Primary IP Address / Host Name — Enter the IP address or host name of the primary device which represents the connection group. You can enter up to 256 characters. This device accesses the specified primary device first to retrieve the job list. • Secondary IP Address / Host Name — Enter the IP address or host name of the secondary device which represents the connection group. You can enter up to 256 characters. If the access to the primary device fails, this device accesses the specified secondary device next to retrieve the job list.
18	[Delete] button	Allows you to delete the selected group.
19	Group Name	Shows the name of the added connection group.
20	Primary IP Address / Host Name	Shows the IP address or host name of the primary device which represents the added connection group.
21	Secondary IP Address / Host Name	Shows the IP address or host name of the secondary device which represents the added connection group.
22	[Delete All] button	Deletes all of the multi station print jobs.

■ ICC Profile settings

You can set up profiles used in printing functions.

Note

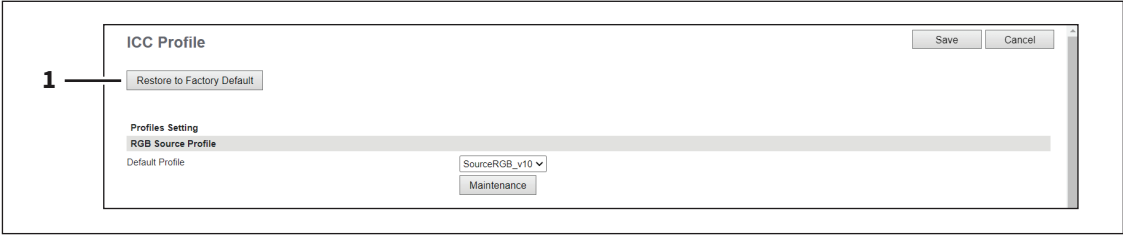
This setting is available only for some models.

Tip

The [ICC Profile] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

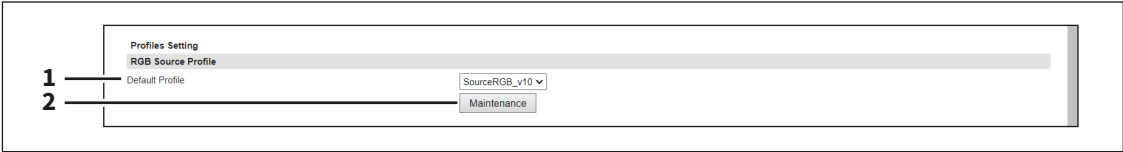
📖 P.101 “[Setup] Item List”



	Item name	Description
1	Restore to Factory Default	Click this to restore all the ICC profile settings to the factory defaults.

❑ Setting up RGB Source Profile

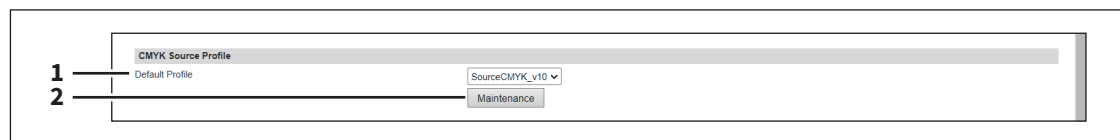
Select an input profile to be used for RGB color space conversion when you print RGB data.



	Item name	Description
1	Default Profile	Select an RGB source profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among the RGB source profiles already registered in this equipment.
2	[Maintenance] button	Click this to perform maintenance of RGB source profiles. The Maintenance RGB Source Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. <div>Note Profiles registered as a factory default cannot be deleted.</div>

❑ Setting up CMYK Source Profile

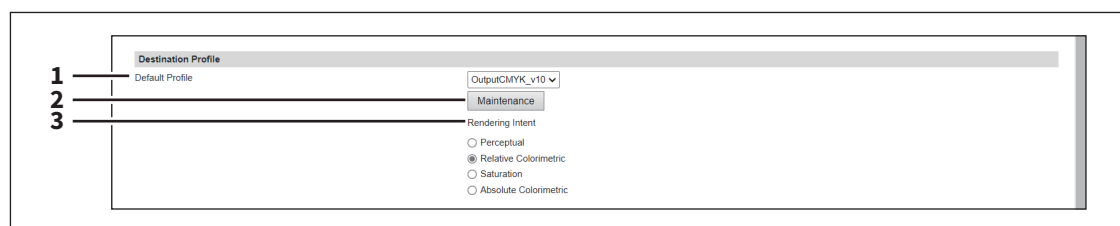
Select an input profile to be used for CMYK color space conversion when you print CMYK data.



	Item name	Description
1	Default Profile	Select an CMYK source profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among CMYK source profiles already registered in this equipment.
2	[Maintenance] button	Click this to perform maintenance of CMYK source profiles. The Maintenance CMYK Source Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. <div>Note</div> Profiles registered as a factory default cannot be deleted.

❑ Setting up Destination Profile

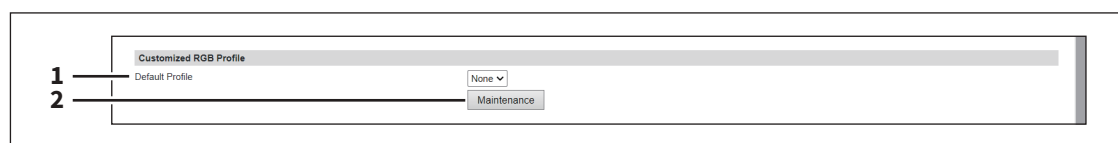
Select an output profile to be used for color space conversion when you print color data.



	Item name	Description
1	Default Profile	Select a destination profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among destination profiles already registered in this equipment.
2	[Maintenance] button	Click this to perform maintenance of destination profiles. The Maintenance Destination Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. <div>Note</div> Profiles registered as a factory default cannot be deleted.
3	Rendering Intent	Select from [Perceptual], [Relative Colorimetric], [Saturation], and [Absolute Colorimetric] for the Rendering Intent of the Destination Profile.

❑ Setting up Customized RGB Profile

Contact your service technician for details on Customized RGB Profile.



	Item name	Description
1	Default Profile	Specify the Customized RGB Profile to be displayed as the default for the color profile setting of the printer driver when printing. You can select from the Customized RGB Profiles registered in this equipment.
2	[Maintenance] button	Click this button when maintaining the Customized RGB Profile. When you click, the Customized RGB Profile maintenance page is displayed that allows you to import the profile into this equipment, or delete the registered profiles. <div>Note</div> Profiles registered as a factory default cannot be deleted.

■ Print Data Converter settings

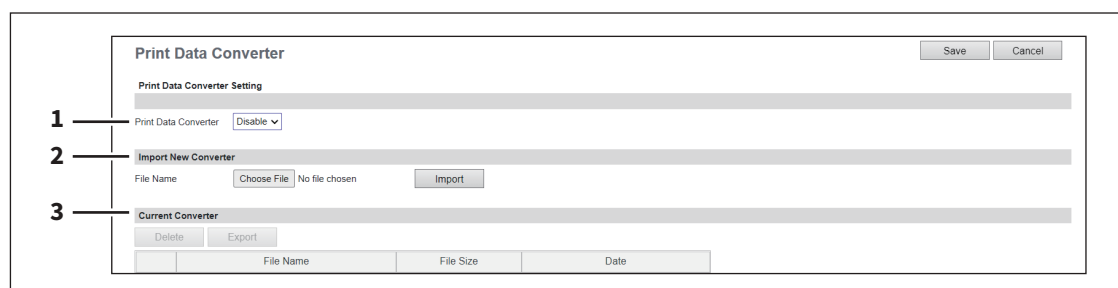
For the details of the print data converter, contact your service technician.

Tip

The [Print Data Converter] submenu can be accessed from the [Setup] menu on the [Administration] page. For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”



	Item name	Description
1	Print Data Converter	Select whether the print data converter function is enabled or disabled. You cannot enable the function if the converter setting file has not been imported.
2	Import New Converter	Import the converter setting file. <div>Tip</div> Click the [Choose File] button to select the file to import and click [Open]. Check the file name and click the [Import] button.
3	Current Converter	Display the imported converter setting file.

MFP Collaboration

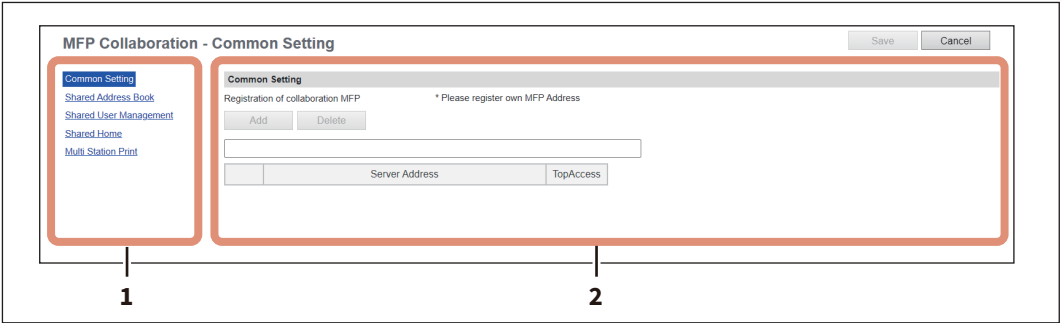
You can make the necessary settings all at one screen for registration and collaboration of MFPs.

Tip

The [General] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:

P.14 “Access Policy Mode”

P.101 “[Setup] Item List”



	Item name	Description
1	Menu area	Click a function name for the MFPs collaboration.
2	Setting area	Set the function that you have selected in the menu area. <div><div>Note</div><p>You need the Multi Station Print Enabler option to use the [Multi Station Print] function. Contact your service technician for details.</p></div>

Common Settings

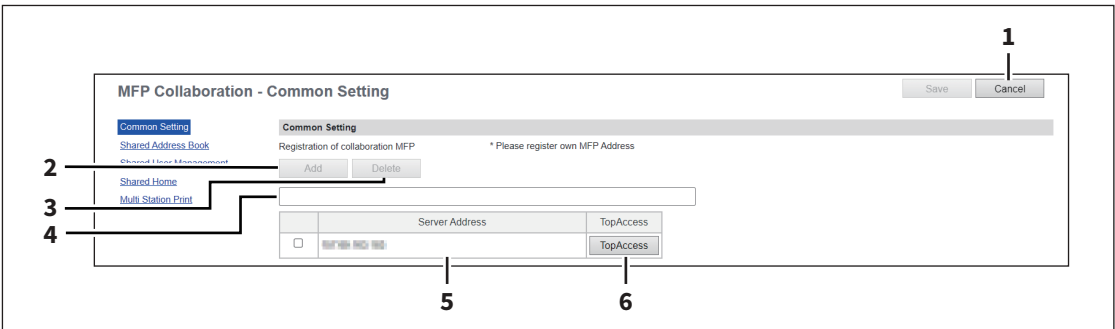
You can register MFPs all at once on this screen to set up them for collaboration.

Note

Be sure to register this equipment as a collaborating MFP.

Tip

You do not need to click the [Save] button on the [Common Settings] screen.



	Item name	Description
1	[Cancel] button	Cancel the settings.
2	[Add] button	Registers an MFP for collaboration. Enter the IP address or host name of the collaborating MFP in the input box below and then click the [Add] button to register it. You can register up to 10 MFPs.

	Item name	Description
3	[Delete] button	Deletes the MFP that you have selected in the list below.
4	Input box	Enter the IP address or host name of an MFP that you want to register.
5	Server Address	Shows the IP address of the registered MFP.
6	[TopAccess] button	Starts TopAccess of the MFP concerned.

❑ Shared Address Book

You can set the address book that is shared on the collaborating MFPs. The settings are applied to the MFPs registered in the list.

Note

Register MFPs on the [Common Settings] screen in advance to select the [Use Common Settings] setting.
 📖 P.223 “Common Settings”

Tip

The [Shared Address Book] settings are linked to the settings on the [Registration] > [Address Book] > [Shared Setting] screen.

📖 P.45 “Shared Setting”

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Shared Address Book	<p>Select whether this equipment should act as a primary or secondary MFP when managing the Shared Address Book in sync with other MFPs.</p> <ul style="list-style-type: none"> • Disable — Does not synchronize. • Enable (Primary) — Synchronizes as a primary MFP. • Enable (Secondary) — Synchronizes as a secondary MFP. <p>Note</p> <p>Select one MFP from among MFPs and select [Enable (Primary)] on it. Be sure to select [Enable (Secondary)] on other MFPs. As a result, the Address Book of the primary MFP can be shared on the secondary MFPs.</p>
4	Connection Timeout	Enter the timeout time to stop communicating if you cannot connect to the primary or secondary MFP. You can set 1 to 180 seconds.

	Item name	Description
5	Use Common Settings	Uses information of the MFPs registered on the [Common Settings] screen to update the following list automatically: you cannot change the list. The [TopAccess] and [Sync] buttons are not available for your own MFP.
6	Use Separate Settings	Uses information of the MFPs registered in the following list.
7	[Add] button	Adds a new secondary MFP. Enter the IP address or host name for the target secondary MFP in the input box below, and then click the [Add] button to register. You can register up to 10 MFPs.
8	[Delete] button	Deletes the selected MFP from the list of secondary MFPs.
9	[Sync All] button	Synchronizes all the secondary MFPs with the primary MFP to share the Address Book.
10	Input box	Enter the IP address or host name when registering a secondary MFP.
11	Server Address	Shows the IP address of the added secondary MFP.
12	[TopAccess] button	Starts TopAccess.
13	[Sync] button	Synchronizes the secondary MFP with the primary MFP to share the Address Book.
14	Last Update	Displays the previous update time.

❑ Shared User Management

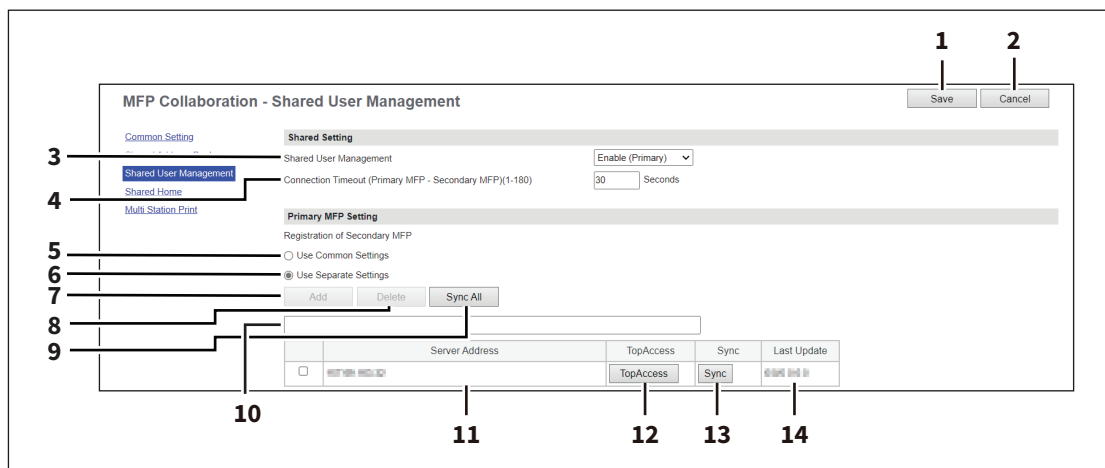
You can set the management of user information that is shared on the collaborating MFPs. The settings are applied to the MFPs registered in the list.

Note


- Register MFPs on the [Common Settings] screen in advance to select the [Use Common Settings] setting.
📖 P.223 “Common Settings”
- Although information can be synchronized and managed for up to 10,000 users, it is recommended that the maximum number of users should be 2,000 for the practical synchronized management.
- User information cannot be registered, updated, and deleted on the user management screen of the secondary MFPs.

Tip

- Information on the collaborating MFPs is linked to the MFP information on the [User Management] > [Shared Setting] screen.
📖 P.97 “[Shared Settings] Item list <access policy mode>”
- The [Shared User Management] and [Connection Timeout] settings are linked to the settings at [Administration] > [Security] > [Authentication] > [User Authentication Setting] > [Shared Setting].
📖 P.240 “Setting up User Authentication Setting”



	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Shared User Management	<p>Select whether this equipment should act as a primary or secondary MFP when managing user information in sync with other MFPs.</p> <ul style="list-style-type: none"> • Disable — Does not synchronize. • Enable(Primary) — Synchronizes as a primary MFP. • Enable(Secondary) — Synchronizes as a secondary MFP. <p>Note</p> <p>Select one MFP from among MFPs and select [Enable (Primary)] on it. Be sure to select [Enable (Secondary)] on other MFPs. As a result, the user information of the primary MFP can be shared on the secondary MFPs.</p>
4	Connection Timeout	Enter the timeout period before stopping communication if the primary MFP cannot connect to the secondary MFPs. You can set 1 to 180 seconds.
5	Use Common Settings	Uses information of the MFPs registered on the [Common Settings] screen to update the following list automatically: you cannot change the list. The [TopAccess] and [Sync] buttons are not available for your own MFP.
6	Use Separate Settings	Uses information of the MFPs registered in the following list.
7	[Add] button	<p>Adds a new secondary MFP.</p> <p>Enter the IP address or host name for the secondary MFP for the distribution destination in the input box below, and then click the [Add] button to register. You can register up to 10 MFPs.</p>
8	[Delete] button	Deletes the selected MFP from the list of secondary MFPs.

	Item name	Description
9	[Sync All] button	<p>Synchronizes all the secondary MFPs with the primary MFP to share the user information.</p> <p>Note</p> <ul style="list-style-type: none"> • The synchronized information is the user information (User Name, Password, PIN Code, Card Information, Role Assignment, Group Assignment, PanelUI Language, PanelUI Keyboard Layout, Email Address, Home Directory, PanelUI Keyboard Display). Settings for Department Management and Project Management are not synchronized. • Only user information updated since the last sync is synchronized. When a user has been deleted, the user of the secondary MFP is also deleted during the synchronization. • During the initial synchronization, if there is user information in a secondary MFP that is not registered to the printer when the printer is a primary MFP, the user information for the secondary MFP is deleted. • The Port Number does not synchronize with the primary MFP or different secondary MFPs. <p> P.236 “Off Device Customization Architecture settings”</p>
10	Input box	Enter the IP address or host name when registering a secondary MFP.
11	Server Address	Shows the IP address of the added secondary MFP.
12	[TopAccess] button	Starts TopAccess.
13	[Sync] button	Synchronizes the secondary MFP with the primary MFP to share the user information.
14	Last Update	Displays the previous update time.

❏ Shared Home

You can set the shared home for the collaborating MFPs. For the procedure for home data synchronization, see the reference below:

📖 P.392 “Setting Home Data Synchronization”

Note

Register MFPs on the [Common Settings] screen in advance to select the [Select from Common Settings] setting.

📖 P.223 “Common Settings”

Tip

The [Shared Home] settings are linked to the settings on the [Administration] > [Setup] > [General] > [Home Setting] screen.

📖 P.113 “Home Setting”

When [Disable] is selected from [Sync Setting]

The screenshot shows the 'MFP Collaboration - Shared Home' configuration screen. On the left, a sidebar contains links: 'Common Setting', 'Shared Address Book', 'Shared User Management', 'Shared Home' (highlighted), and 'Multi Station Print'. The main area has a 'Sync Setting' dropdown menu set to 'Disable'. At the top right, there are 'Save' and 'Cancel' buttons. Numbered callouts point to: 1. Save button, 2. Cancel button, and 3. Shared Home link in the sidebar.


When [Use Network Server for Sync] is selected from [Sync Setting]

The screenshot shows the 'MFP Collaboration - Shared Home' configuration screen with 'Sync Setting' set to 'Use Network Server for Sync'. The main area contains fields for 'Server Name', 'Port Number' (set to 21), 'User Name', 'Password', and 'Enable SSL/TLS' (set to Disable). There is also a 'Delete All Shared Data' button. At the top right are 'Save' and 'Cancel' buttons. Numbered callouts point to: 1. Save button, 2. Cancel button, 3. Shared Home link, 4. Shared User Management link, 5. Port Number field, 6. User Name field, 7. Password field, 8. Enable SSL/TLS dropdown, and 14. Delete All Shared Data button.

When [Use MFP for Sync] is selected from [Sync Setting]

The screenshot shows the 'MFP Collaboration - Shared Home' configuration screen with 'Sync Setting' set to 'Use MFP for Sync'. The main area contains a checkbox 'Assume this MFP is the Primary Server', a 'Server Name' field, a radio button 'Select from Common Settings' (selected), a radio button 'Use Separate Settings', a 'Port Number' field (set to 21), and an 'Enable SSL/TLS' dropdown (set to Disable). There is also a 'Delete All Shared Data' button. At the top right are 'Save' and 'Cancel' buttons. Numbered callouts point to: 1. Save button, 2. Cancel button, 3. Shared Home link, 9. Shared User Management link, 10. Select from Common Settings radio button, 11. Use Separate Settings radio button, 12. Port Number field, 13. Enable SSL/TLS dropdown, and 14. Delete All Shared Data button.

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.

	Item name	Description
3	Sync Setting	Specify whether or not to synchronize the HOME screen with the network server or other MFPs. <ul style="list-style-type: none"> • Disable: Disable the Home sync function. • Use Network Server for Sync: Select this to use the network server for synchronization. • Use MFP for Sync: Select this to use MFP for synchronization.
4	Server Name	Enter the name of the network server.
5	Port Number	Enter the port number of the network server.
6	User Name	Enter the name of the user who accesses the network server.
7	Password	Enter the password of the user who accesses the network server.
8	Enable SSL/TLS	Select whether SSL/TLS is enabled or disabled.
9	Assume this MFP is the Primary Server	Select this check box to synchronize this MFP as the primary server. When you clear this check box, another MFP can synchronize as the primary server. <div>Note</div> <p>If the FTP server is disabled, you cannot set this MFP as the primary server.  P.150 "Setting up FTP Server"</p>
10	Select from Common Settings	Select the primary MFP from among the MFPs registered on the [Common Settings] screen when you set another MFP other than this MFP as the primary server.
11	Use Separate Settings	Enter the IP address of the primary MFP when you set another MFP other than this MFP as the primary server.
12	Port Number	Enter the port number of the primary server when you set another MFP other than this MFP as the primary server.
13	Enable SSL/TLS	Select whether SSL/TLS is enabled or disabled when you set another MFP other than this MFP as the primary server.
14	Delete All Shared Data	Delete all the shared data stored in the FTP server.

❏ Multi Station Print

You can set the multi station print function that is used on the collaborating MFPs. The settings are applied to the MFPs registered in the list. For the operation of the setting, see the following.

📖 P.390 “Setting Multi Station Print”

Note

- You need the Multi Station Print Enabler option to use the [Multi Station Print] function. Contact your service technician for details.
- Register MFPs on the [Common Settings] screen in advance to select the [Select from Common Settings] setting.
📖 P.223 “Common Settings”

Tip

The [Multi Station Print] settings are linked to the settings on the [Administration] > [Setup] > [Print Service] > [Multi Station Print] screen.

📖 P.217 “Setting up Multi Station Print”

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Enable Multi Station Print	Specify whether to enable or disable the Multi Station Print service.
4	Document Expired Time	Specify the retention period of the printed document.
5	Number of Display Job	Specify the number of jobs to be displayed.
6	Sort Order	Specify the display order.

	Item name	Description
7	Thumbnail List	<p>Select whether to display thumbnail images of the multi station print files in the document list on the control panel. Thumbnail images appear for PDF and JPEG files and the fixed icon appears for files of other formats.</p> <p>Note</p> <p>A thumbnail just represents the image of a file. The image may differ from the original, having parts of it cut or blank spaces added.</p>
8	Print Order	<p>Specify the print order.</p> <p>Tip</p> <p>When you select [Indication Order] from [Print Order], documents are printed according to the [Sort Order] setting at the item 4.</p>
9	Enable Printed Jobs	Specify whether to enable or disable reprinting.
10	Connection MFP	<p>Specify the following communication settings for the multi station print.</p> <ul style="list-style-type: none"> • Port Number — Enter the port number. • Enable SSL/TLS — Select the SSL/TLS setting for the multi station print. <ul style="list-style-type: none"> - Disable — Select this to disable SSL/TLS. - Verify with imported CA certification(s) — Select this to use CA certificates for connection. You need to export the certificate from each MFP and import it into all MFPs. - Accept all certificates without CA — Select this to accept all certificates without CA. There is no need to import the certificate of each MFP. • Authentication — Select [Disable] or [Basic] for authentication. [Disable] is set as the default. • User Name — Enter the user name. You can enter up to 127 alphanumeric characters and symbols except = ; # @ \. • Password — Enter the password of the user. You can enter up to 127 alphanumeric characters and symbols except = ; # \. <p>Note</p> <p>All MFPs should have the same settings for the connection.</p> <p>Tip</p> <p>Although the multi station print is available even if the user authentication is disabled, this MFP cannot be connected to other MFPs: the job list is not shared.</p>
11	Use Common Settings	Uses information of the MFPs registered on the [Common Settings] screen to update the following list automatically: you cannot change the list. The [Connection] and [TopAccess] buttons are not available for your own MFP.
12	Use Separate Settings	Uses information of the MFPs registered in the following list.
13	[Add] button	Allows you to add the device to connect.
14	[Delete] button	Allows you to delete the selected device.
15	Connection MFP entry field	<p>Enter the IP address or host name of the MFP you want to register.</p> <p>Tip</p> <p>If the user authentication is disabled with more than one address registered in the [Connection MFP] list, the [Connection MFP] settings are not displayed.</p>
16	Server Address	Shows the IP address or host name of the registered MFP.

	Item name	Description
17	[Connect] button	<p>Tests the connection with the specified MFP to check if the communications can be established.</p> <p>Note</p> <p>Be sure to save the Multi Station Print settings with the [Save] button before you test the MFP connection with the [Connect] button.</p>
18	[TopAccess] button	Starts TopAccess.
19	Group Connection Enable	Select whether to connect the MFP groups. [Disable] is set as the default.
20	Own Group Name	<p>Enter a group name to which this MFP belongs. You can enter up to 12 characters.</p> <p>Note</p> <p>All groups should share the same name of each group for the connection.</p>
21	[Add] button	<p>Allows you to add a group. Click this button to show the [Add Connection Group Information] screen. Set the following information and click [Save] to save the settings. To edit the information, click the name of the group added in the list.</p> <ul style="list-style-type: none"> • Group Name — Enter the name of the connection group. You can enter up to 12 characters. • Primary IP Address / Host Name — Enter the IP address or host name of the primary device which represents the connection group. You can enter up to 256 characters. This device accesses the specified primary device first to retrieve the job list. • Secondary IP Address / Host Name — Enter the IP address or host name of the secondary device which represents the connection group. You can enter up to 256 characters. If the access to the primary device fails, this device accesses the specified secondary device next to retrieve the job list.
22	[Delete] button	Allows you to delete the selected group.
23	Group Name	Shows the name of the added connection group.
24	Primary IP Address / Host Name	Shows the IP address or host name of the primary device which represents the added connection group.
25	Secondary IP Address / Host Name	Shows the IP address or host name of the secondary device which represents the added connection group.
26	[Delete All] button	Deletes all of the multi station print jobs.

■ Embedded Web Browser settings

You can set the EWB (Embedded Web Browser) function to display a web page on the touch panel.

Tip

The [EWB] submenu can be accessed from the [Setup] menu on the [Administration] page.

For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

Note

- The External Interface Enabler is required to use the EWB (Embedded Web Browser) function.
- This setting is available only for some models.
- When an error page appears due to a network failure while being connected to the internet, this may continue to be displayed even after recovery has taken place. In that case, reboot the equipment.

□ Setting up Home Page Setting

You can specify the home page for the EWB function.

	Item name	Description
1	Home Page	Enter the URL of the home page.
2	Enforcement automatic screen change	Specify whether or not the screen is automatically changed to [JOB STATUS] when a job cannot be performed due to paper empty or toner empty, etc. while the EWB screen is displayed. <ul style="list-style-type: none"> • Enable — Select this to change the screen to [JOB STATUS]. • Disable — Select this not to change the screen.

□ Setting up Proxy Setting

You can set the proxy for the EWB function.

Tip

The proxy settings are basically common to the Embedded Web Browser, Idle Screen, and Application functions. If you change them for one function, they change accordingly for others.

📖 P.285 “Proxy Setting”

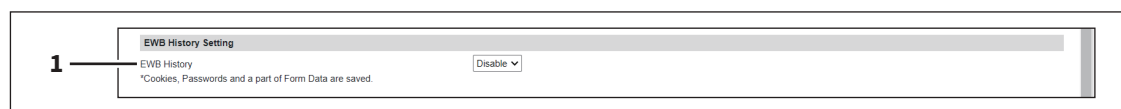
📖 P.364 “Proxy Setting”

	Item name	Description
1	Host Name	Enter the host name of the proxy server.
2	Port Number	Enter the port number of the proxy server.

	Item name	Description
3	Bypass proxy settings for these addresses	Enter URLs which do not use the proxy server delimited with a semicolon (;).
4	Account ID	Enter the account ID of the proxy server.
5	Password	Enter the password of the proxy server.
6	Use automatic configuration script	Enable or disable the automatic configuration script.
7	URL	<p>Specify the location of the PAC file by URL for the automatic configuration script.</p> <p>Note</p> <p>Note the following points for the PAC file.</p> <ul style="list-style-type: none"> • Be sure to enter the protocol. • Do not use functions.

❑ Setting up EWB History Setting

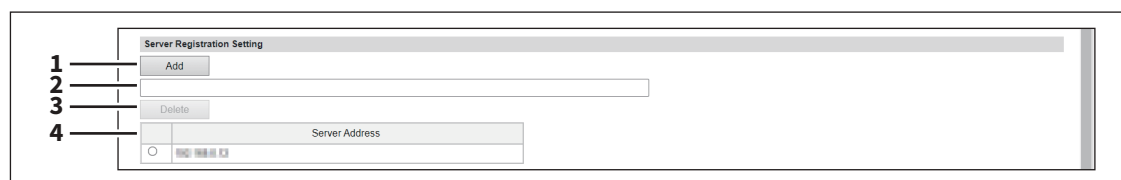
You can set the history conditions for the EWB function.



	Item name	Description
1	EWB History	Specify whether to restrict the size of the recorded history information. The size is restricted to 100MB if you restrict.

❑ Setting up Server Registration Setting

You can register the address of the server used for the EWB function.



	Item name	Description
1	[Add] button	Registers the server address entered in the entry column into the list.
2	Entry column	Enter the server address.
3	[Delete] button	Deletes the selected server address from the list.
4	Server Address list	Lists the registered server addresses.

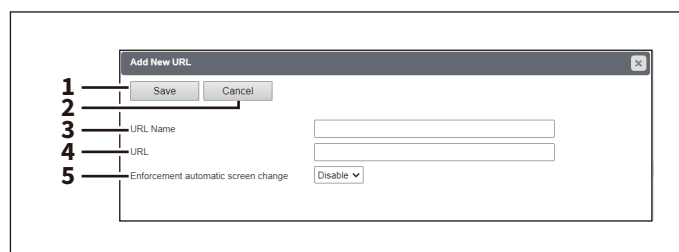
❑ Setting up URL List for Home screen

You can register URLs to be displayed in the Home screen on the touch panel.



	Item name	Description
1	[Add] button	Registers a URL to be displayed on the touch panel. P.235 “[Add New URL] screen”
2	[Delete] button	Deletes the URL that you have selected from the URL list for Home screen.
3	URL list	Lists URLs which are displayed on the touch panel.

❑ [Add New URL] screen



	Item name	Description
1	[Save] button	Registers the entered URL name and URL.
2	[Cancel] button	Cancels adding a URL.
3	URL Name	Enter the URL name to be registered.
4	URL	Enter the URL to be registered.
5	Enforcement automatic screen change	Specify whether or not the screen is automatically changed to [JOB STATUS] when a job cannot be performed due to paper empty or toner empty, etc. while the EWB screen is displayed.

■ Off Device Customization Architecture settings

Set ODCA (Off Device Customization Architecture) when you are linking external application software to services provided by this equipment.
For details, refer to the application software manual.

Tip

The [ODCA] submenu can be accessed from the [Setup] menu on the [Administration] page.
For how to access it and information on the [Setup] menu, see the references below:
📖 P.14 “Access Policy Mode”
📖 P.101 “[Setup] Item List”

□ Setting up Network

You can set up the network respectively for SOAP (Simple Object Access Protocol) and REST (REpresentational State Transfer).

	Item name	Description
1	Enable Port	Select whether the external connection is enabled or disabled.
2	Port Number	Specify the port number where the external connection is enabled.
3	Enable SSL/TLS Port	Select whether SSL/TLS is enabled or disabled for the external connection.
4	SSL/TLS Port Number	Specify the SSL/TLS port number where the external connection is enabled.

□ Setting up Configuration

	Item name	Description
1	Session Timeout(60-99999)	Specify the duration to maintain the connection.

□ Notification Events

	Item name	Description
1	[Delete All] button	Deletes all notification events registered with external application software.

Version

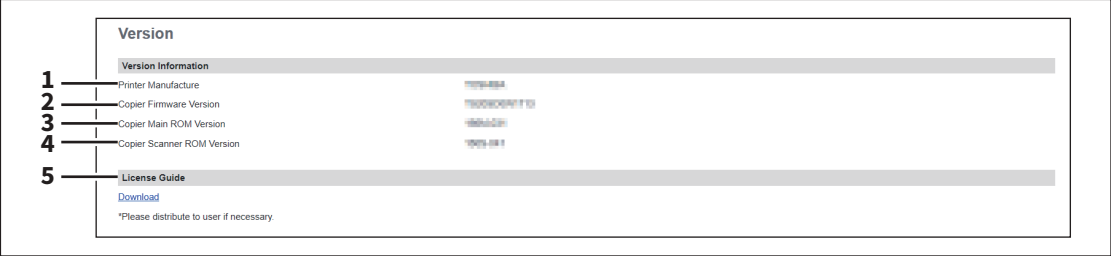
The screen displays version information, depending on the model.

Tip

The [Version] submenu can be accessed from the [Setup] menu on the [Administration] page. For how to access it and information on the [Setup] menu, see the references below:

P.14 “Access Policy Mode”

P.101 “[Setup] Item List”



	Item name	Description
1	Printer Manufacture	Displays the manufacturer name of your equipment.
2	Copier Firmware Version	Displays the firmware version of your equipment.
3	Copier Main ROM Version	Displays the main ROM version information of your equipment.
4	Copier Scanner ROM Version	Displays the copier scanner ROM version information of your equipment.
5	License Guide	The License Guide can be downloaded.

Tip

Users who are granted administrator privileges in access policy mode can access the [Security] menu from the [Administration] page.
For how to access it, see the reference below:
 P.14 “Access Policy Mode”



	Item name	Description
1	[Save] button	Saves the settings after you change the settings at [Security] menu.
2	[Cancel] button	Cancels the changed settings.

■ Authentication settings

You can restrict user operations using the authentication function of your equipment.

Tip

The [Authentication] submenu can be accessed from the [Security] menu on the [Administration] page.
For how to access it and information on the [Security] menu, see the references below:
 P.14 “Access Policy Mode”
 P.238 “[Security] Item List”

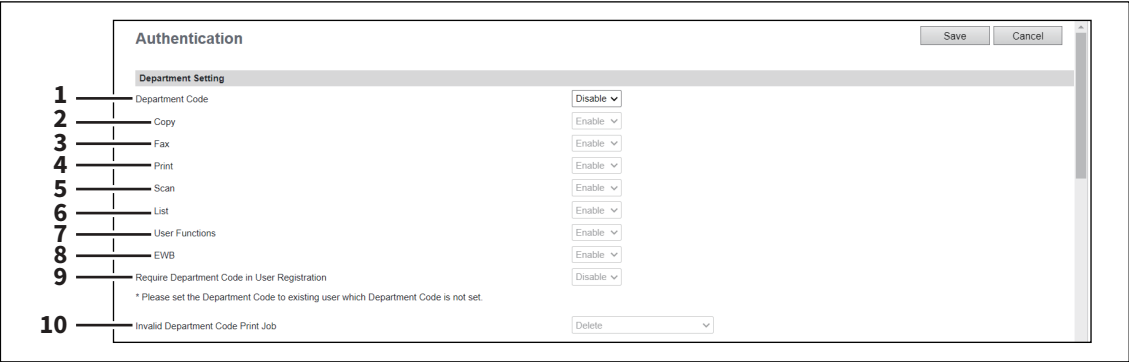
□ Setting up Department Setting

When you want to manage the counters for every department, enable department management. If this is done, the department code input screen will be displayed on the computer and the touch panel when copying, scanning, faxing, faxing via the Internet, and operating on e-Filing to enable you to manage operations by departments.

Note

The following applications can access your equipment regardless of the department setting.

- AddressBook Viewer
- Backup/Restore Utility
- TWAIN Driver
- File Downloader



	Item name	Description
1	Department Code	Select whether or not to enable department management. [Disable] is set as the default.

	Item name	Description
2	Copy	When this function is enabled, the following counters are managed in each department. <ul style="list-style-type: none"> • Number of copied sheets • Number of originals scanned while copying [Enable] is set as the default.
3	Fax	When this function is enabled, the following counters are managed in each department. <ul style="list-style-type: none"> • Number of transmitted fax pages • Number of original pages scanned while transmitting faxes • Number of received fax pages • Number of received fax pages which are printed* [Enable] is set as the default.
4	Print	When this function is enabled, the number of outputs in printing (for printing, received E-mail and Internet Fax) is managed in each department. [Enable] is set as the default.
5	Scan	When this function is enabled, the number of originals scanned such as when they are stored in the shared folder is managed in each department. [Enable] is set as the default.
6	List	When this function is enabled, the number of system page outputs is managed in each department. [Enable] is set as the default.
7	User Functions	When this function is enabled, operations in the USER FUNCTION menu are managed in each department. [Enable] is set as the default.
8	EWB	Specify whether or not to enable the EWB (Embedded Web Browser) function. You need the External Interface Enabler option to use EWB.
9	Require Department Code in User Registration	Select whether or not to register the department code when registering a user. [Disable] is set as the default.
10	Invalid Department Code Print Job	Select whether or not to print jobs without a department code or with an invalid department code when department management is enabled. <ul style="list-style-type: none"> • Force use of department code — Select this to force the entry of the department code when printing. • Print — Select this to print jobs with an invalid department code. • Delete — Select this to delete jobs with an invalid department code. <div>Tip</div> <p>While SNMP communication is disabled in the printer driver, if the Invalid Department Code Print Job is set to Force use of department code and an invalid department code is entered in the printer driver, a printing job will be registered in Invalid department code print job list.</p>


* The number of outputs are only counted for received faxes, in which the department code needs to be entered, such as manual reception, polling reception or the printing of originals stored in the confidential mailbox and the bulletin mailbox.




❑ Setting up User Authentication Setting

You can configure user authentication to access your equipment.

	Item name	Description
1	User Authentication	<p>Select whether or not to enable user authentication. [Disable] is set as the default.</p> <div> Note <ul style="list-style-type: none"> You cannot configure “E-mail authentication” if you enable user authentication. The No Limit Black function becomes unavailable if you enable user authentication. For the details of the No Limit Black function, see the reference below: User Functions - MANAGING COUNTERS (COUNTER MENU) - Department Management - Setting the No Limit Black function </div>
2	User Authentication According To Function	Specify whether or not to authenticate users for each function.
3	Copy	Enable or disable user authentication when the Copy function is used. [Enable] is set as the default.

	Item name	Description
4	Fax	<p>Enable or disable user authentication when the FAX function is used. [Enable] is set as the default.</p> <p>Note</p> <p>When you want to set [Disable] for this function, use the latest version of a N/W-Fax driver. For details, contact your service technician.</p>
5	Print	<p>Enable or disable user authentication when the Print function is used. [Enable] is set as the default.</p> <p>Note</p> <p>When you want to set [Disable] for this function, use the latest version of a printer driver. For details, contact your service technician.</p>
6	Scan	<p>Enable or disable user authentication when the Scan function is used. [Enable] is set as the default.</p>
7	List	<p>Enable or disable user authentication when the List function is used. [Enable] is set as the default.</p>
8	User Functions	<p>Enable or disable user authentication when the User Functions are used. [Enable] is set as the default.</p>
9	EWB	<p>Specify whether or not to enable the EWB (Embedded Web Browser) function. You need the External Interface Enabler option to use EWB.</p>
10	Authentication Method for Admin	<p>Select the administrator authentication method.</p> <ul style="list-style-type: none"> • User Name and Password — Select this to authenticate an administrator with a user name and a password. • Only Password — Select this to authenticate an administrator with a password.
11	Authentication failed print job/Raw Print Job	<p>Select whether or not to print jobs which have failed user authentication.</p> <ul style="list-style-type: none"> • Hold — Select this to register in the hold print job. • Print — Select this to print jobs which failed authentication. • Delete — Select this to delete jobs which failed authentication. <p>Note</p> <p>When the N/W-Fax driver is used, selecting [Hold] deletes the job.</p>
12	Auto Release on Login	<p>Specify whether to process private jobs and hold jobs at login.</p> <ul style="list-style-type: none"> • Disable — Select this not to print at login. • Enable — Select this to print at login.
13	Project Management	<p>Specify whether or not to enable project management.</p>
14	Print Job(Without Project Code)	<p>Specify whether or not to print the print jobs without project codes when Project Management is enabled.</p> <ul style="list-style-type: none"> • Hold — Registers print jobs to Hold. • Print — Prints print jobs that failed authentication. • Delete — Deletes print jobs that failed authentication.

	Item name	Description
15	Authentication Method for Print Jobs	<p>Select the user authentication method for print jobs. Although this equipment can be configured to use two network channels at the same time, it might not be possible to authenticate users via the secondary network depending on the authentication processes in the network environment. You can use this setting to set the user authentication to the network environment.</p> <ul style="list-style-type: none"> • Use User Name and Domain Name — Uses a user name and domain name for authentication. This is the usual authentication method for a single network channel. • Use Only User Name — Uses only a user name for authentication. If users can be authenticated only with their names, they can print with this equipment. • Use Only Domain Participation Information — Uses only information about the domain participation for authentication. If users can be authenticated only with the domain participation information, they can print with this equipment. <p>Tip</p> <p>The simultaneous use of the two-channel network can be set at [Administration] > [Setup] > [Network] > [Basic Setting] > [Network Composition]. For details, see the reference below:  P.118 “Basic Setting”</p>
16	Use Password Authentication for Print Job	Performs user authentication for each print job. The user name and password are required to execute printing.
17	Delete Own Account	<p>Specify whether to permit users to delete their own accounts.</p> <ul style="list-style-type: none"> • Disable — Prohibit user to delete their own accounts. • Enable — Permit users to delete their own accounts. <p>Note</p> <p>The default setting varies from shipment to shipment. This function is enabled as a default for some districts.</p>
18	Enable Guidance Screen	<p>Select the screen dedicated to the card authentication.</p> <p>Note</p> <p>For the details of the card authentication setting, contact your service technician.</p>
19	Enable Guest User	Enables operations by the guest user.

	Item name	Description
20	Authentication Type	<p>Select the authentication method.</p> <ul style="list-style-type: none">• <u>MFP Local Authentication</u> You can manage network users with the MFP local authentication of your equipment when you do not have a user authentication system in your environment. When MFP local authentication is enabled, users must enter the user name and password that is registered in the equipment to operate the touch panel.  P.244 “MFP Local Authentication”• <u>Windows Domain Authentication</u> You can manage network users with Windows domain authentication when you already manage your network using Windows domains. When Windows domain authentication is enabled, users must enter the user name and password that are registered in the Windows domain to operate the touch panel.  P.248 “Windows Domain Authentication”• <u>LDAP Authentication</u> You can manage network users with LDAP authentication when you already manage your network using LDAP. When LDAP authentication is enabled, users must enter the user name and password that are registered in the LDAP server to operate the touch panel.  P.251 “LDAP Authentication”

MFP Local Authentication

User Authentication Setting

User Authentication

Enable

User Authentication According to Function

Disable

Copy

Enable

Fax

Enable

Print

Enable

Scan

Enable

List

Enable

User Functions

Enable

EWB

Enable

Authentication Method for Admin

User Name and Password

Authentication failed print Job/Raw Print Job

Hold

Auto Release on Login

Disable

Project Management

Disable

Print Job(Without Project Code)

Hold

Authentication Method for Print Jobs

Use User Name and Domain Name

☐ Use Password Authentication for Print Job

*It is not able to print from other than Windows Client when this function is enabled.

Delete Own Account

Disable

Enable Guidance Screen

Card Authentication

☐ Enable Guest User

Authentication Type

MFP Local Authentication

☐ Automatic deletion of unlogged-in user

Validity Period of Local User

30

Days(1-180)

PIN Code Authentication Setting

PIN Code Authentication

Disable

Minimum PIN Code Length

1

(1-32)

Card Authentication Setting

Card Authentication

Enable

Auto Change Login User

Enable

☐ Card ID is used as User Name

☒ Create User Information Automatically

☒ User authentication is performed during automatic registration

Authentication Type

Windows Domain Authentication

☐ Use NT Domain Server

Add

Edit

Delete

Move Down

Move Up

Domain Name	PDC	BDC

The priority is from the top.

☐ Require PIN Code

Shared Setting

Shared User Management

Enable (Primary)

Connection Timeout (Primary MFP - Secondary MFP)(1-180)

30

Seconds

Card Authentication Setting

Card Authentication

Enable

Auto Change Login User

Enable

☐ Card ID is used as User Name

☒ Create User Information Automatically

☒ User authentication is performed during automatic registration

Authentication Type

LDAP Authentication

Server Assignment

Move Down

Move Up

LDAP Server	Server IP Address	Type	Attribute type of "User Name"

The priority is from the top.

☐ Require PIN Code

Server Assignment

Move Down


Move Up


LDAP Server	Server IP Address	Type	Attribute type of "User Name"

The priority is from the top.

244 [Security] Item List

	Item name	Description
1	Automatic deletion of unlogged-in user	Enables the function to delete unlogged-in local users automatically after the specified period. If the days set in [Validity Period of Local User] have passed after local users logged out last, they are automatically deleted every 24 hours or at the restart of the equipment.
2	PIN Code Authentication Setting	<p>PIN Code Authentication — Select the PIN code authentication method.</p> <ul style="list-style-type: none"> • Disable — Select this no to use the PIN code authentication. Use the user name and password for authentication. • Enable — Select this to use the PIN code authentication. Instead of the PIN code, it is possible to use the user name and password for authentication. <p>Minimum PIN Code Length — Enter a figure that specifies the minimum digits for the PIN code.</p>
3	Card Authentication	<p>Select whether or not to enable card authentication.</p> <p>Note</p> <p>For the details of the card authentication setting, contact your service technician.</p>
4	Auto Change Login User	Select whether or not to enable the function to change login users automatically when authenticating users with the card.
5	Card ID is used as User Name	Select whether or not to use the card ID as a user name.
6	Create User Information Automatically	Select whether or not to add unregistered user information to the equipment automatically when authenticating users with the card.
7	User authentication is performed during automatic registration	Select whether or not to perform user authentication with the external servers before registering the user information automatically when [Create User Information Automatically] is enabled. When this setting is enabled, only the information of users authenticated with the external servers is registered. You need to select the authentication type and set the external authentication servers in the list of servers.
8	Authentication Type	<p>Select the authentication method for the automatic user registration when [User authentication is performed during automatic registration] is enabled.</p> <ul style="list-style-type: none"> • Windows Domain Authentication — You can manage users with Windows domain authentication when you already manage your network using Windows domains. • LDAP Authentication — You can manage users with LDAP authentication when you already manage your network using LDAP.
9	Use NT Domain Server	Select whether or not to manage the domain with the NT domain controller when [Windows Domain Authentication] is selected from [Authentication Type].

	Item name	Description
10	Server List	<p>Displays up to 16 user authentication domains or servers in the list depending on the [Authentication Type] setting.</p> <ul style="list-style-type: none"> • Windows Domain Authentication — Displays a list of domains that are assigned for Windows Domain Authentication. Click [Add] and enter the following items in the displayed screen to register a domain. Select the domain and click [Edit] to edit a domain. Use [Move Up] and [Move Down] to change the priority order in the list. Delete the selected domain using [Delete] button. <ul style="list-style-type: none"> Domain Name — Enter the domain name. PDC — Enter the server name or IP address of the Primary Domain Controller (PDC). You can enter up to 128 alphanumerical characters and symbols. BDC — Enter the server name or IP address of the Backup Domain Controller (BDC) as required. You can enter up to 128 alphanumerical characters and symbols. <p>Note</p> <ul style="list-style-type: none"> • You can add the primary domain controllers and the backup domain controllers only when [Use NT Domain Server] is selected. • If the wrong primary or backup domain controller is specified, the [OK] in the user authentication screen on the touch panel is highlighted while this equipment searches for the primary or backup domain controller for 2 to 4 minutes. <ul style="list-style-type: none"> • LDAP Authentication — Displays a list of servers that are assigned for the card authentication. Click [Server Assignment] and add the server in the displayed screen to assign a server. Register the available server as [LDAP Client]. Use [Move Up] and [Move Down] to change the priority order in the list. <p> P.151 “LDAP Client settings”</p>
11	Require PIN Code	<p>Select whether or not to require PIN code when authenticating users with the card.</p> <p>Tip</p> <p>This function is available only on the equipment that supports the PIN code input.</p>

	Item name	Description
12	Shared Setting	<p>Shared User Management —Select whether this equipment should act as a primary or secondary MFP when managing user information in sync with other MFPs.</p> <ul style="list-style-type: none"> • Disable — Does not synchronize. • Enable(Primary) — Synchronizes as a primary MFP. • Enable(Secondary) — Synchronizes as a secondary MFP. <p>Connection Timeout —Enter the timeout period before stopping communication if the primary MFP cannot connect to the secondary MFPs. You can set 1 to 180 seconds.</p> <p>Note</p> <ul style="list-style-type: none"> • The [Shared User Management] and [Connection Timeout] settings are linked to the same settings on the [MFP Collaboration] > [Shared User Management] screen. •  P.225 “Shared User Management” • Although information can be synchronized and managed for up to 10,000 users, it is recommended that the maximum number of users should be 2,000 for the practical synchronized management. • User information cannot be registered, updated, and deleted on the user management screen of the secondary MFPs.

Windows Domain Authentication

User Authentication Setting

User Authentication

Enable ▾

User Authentication According to Function

Disable ▾

Copy

Enable ▾

Fax

Enable ▾

Print

Enable ▾

Scan

Enable ▾

List

Enable ▾

User Functions

Enable ▾

EWB

Enable ▾

Authentication Method for Admin

User Name and Password ▾

Authentication failed print job/Raw Print Job

Hold ▾

Auto Release on Login

Disable ▾

Project Management

Disable ▾

Print Job(Without Project Code)

Hold ▾

Authentication Method for Print Jobs

User User Name and Domain Name ▾

☐ Use Password Authentication for Print Job

*It is not able to print from other than Windows Client when this function is enabled.

Delete Own Account

Disable ▾

Enable Guidance Screen

Card Authentication ▾

☐ Enable Guest User

Authentication Type

Windows Domain Authentication ▾

☒ Create User Information Automatically

☐ Use cache information when user authentication failed

Validity Period of Cache

7 Days(1-14)

☐ Register Local User which is available in Windows Domain Authentication/LDAP Authentication

Validity Period of Local User

30 (0-180, Unlimited 0)

Windows Domain Authentication

☐ Use NT Domain Server

Add Edit Delete Move Down Move Up

Domain Name	PDC	BDC
Domain001		

The priority is from the top.

Connection Timeout

PDC(1 - 180)

30 Seconds

*Reboot is necessary to reflect Connection Timeout.

Role Based Access Setting

Role Based Access using LDAP server

Disable ▾

LDAP Server

LDAP01 ▾

PIN Code Authentication Setting

PIN Code Authentication

Disable ▾

Minimum PIN Code Length

1 (1-32)

Card Authentication Setting

Card Authentication

Enable ▾

Auto Change Login User

Enable ▾


☐ Require PIN Code


Server Assignment

Move Down Move Up

LDAP Server	Server IP Address	Type	Attribute type of "User Name"	Attribute type of "Card information"
-------------	-------------------	------	-------------------------------	--------------------------------------

The priority is from the top.

	Item name	Description
1	Create User Information Automatically	<p>Select whether or not to register user information automatically to this equipment. This item is selected as the default. By registering user accounts to the printer, you can manage counters and quotas for each user.</p> <p>Tip</p> <p>When automatically adding a user while printing from the printer driver, enable [Use Password Authentication for Print Job] on the [User Authentication Setting] screen.</p> <p> P.240 “Setting up User Authentication Setting”</p>
2	Use cache information when user authentication failed	<p>Either of the following data is saved according to the authentication method. Password, Card number, Domain name, PIN code, Home Directory information or RBAC information.</p> <p>Tip</p> <p>The cache information will be updated if user authentication succeeds with the authentication server. However, if a user is authenticated with the cache information, it is not updated.</p>
3	Validity Period of Cache	Enter the number of days to maintain the cache information. 1 to 14 days can be set from the latest update.
4	Register Local User which is available in Windows Domain Authentication/LDAP Authentication	Select this to register a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
5	Validity Period of Local User	Enter the number of valid days for local users. Up to 180 days can be set from the user creation day. If 0 is set, the number of valid days will be indefinite.
6	Use NT Domain Server	Select this check box if you are managing the domain using the NT domain controller.
7	Domain List	<p>Displays a list of domains that are assigned for Windows Domain Authentication.</p> <p>Click [Add] and enter the following items in the displayed screen to register a domain. Select the domain and click [Edit] to edit a domain.</p> <p>Use [Move Up] and [Move Down] to change the priority order in the list. Delete the selected domain using [Delete] button.</p> <p>Domain Name — Enter the domain name.</p> <p>PDC — Enter the server name or IP address of the Primary Domain Controller (PDC). You can enter up to 128 alphanumerical characters and symbols.</p> <p>BDC — Enter the server name or IP address of the Backup Domain Controller (BDC) as required. You can enter up to 128 alphanumerical characters and symbols.</p> <p>Note</p> <ul style="list-style-type: none"> • You can add the primary domain controllers and the backup domain controllers only when [Use NT Domain Server] is selected. • If the wrong primary or backup domain controller is specified, the [OK] in the user authentication screen on the touch panel is highlighted while this equipment searches for the primary or backup domain controller for 2 to 4 minutes.
8	Connection Timeout	Enter the timeout period for quitting communication when no response is received from the PDC or BDC server. Specify within the range from 1 to 180 seconds.

	Item name	Description
9	Role Based Access Setting	<p>Configure role based access using an LDAP server.</p> <p>Role Based Access using LDAP server — Select whether enable or disable role based access. [Disable] is set as the default.</p> <p>LDAP Server — Select the LDAP server that manages the Role Based Access Control.</p>
10	PIN Code Authentication Setting	<p>PIN Code Authentication — Select the PIN code authentication method.</p> <ul style="list-style-type: none"> • Disable — Select this no to use the PIN code authentication. Use the user name and password for authentication. • Enable — Select this to use the PIN code authentication. Instead of the PIN code, it is possible to use the user name and password for authentication. <p>Minimum PIN Code Length — Enter a figure that specifies the minimum digits for the PIN code.</p>
11	Card Authentication	<p>Select whether or not to enable card authentication.</p> <p>Note</p> <p>For the details of the card authentication setting, contact your service technician.</p>
12	Auto Change Login User	<p>Select whether or not to enable the function to change login users automatically when authenticating users with the card.</p>
13	Require PIN Code	<p>Select whether or not to require PIN code when authenticating users with the card.</p> <p>Tip</p> <p>This function is available only on the equipment that supports the PIN code input.</p>
14	LDAP Server List	<p>Displays a list of servers that are assigned for the PIN code or card authentication. Click [Server Assignment] and add the server in the displayed screen to assign a server. Register the available server as [LDAP Client]. Use [Move Up] and [Move Down] to change the priority order in the list.</p> <p> P.151 “LDAP Client settings”</p> <p>Tip</p> <p>If [Windows Server] is selected as an LDAP server for the PIN code or card authentication, the following attribute type of user name is employed for the one at the login and the one of the user which is automatically registered while [Create User Information Automatically] is enabled.</p> <ul style="list-style-type: none"> • If Kerberos is selected to access the LDAP server: sAMAccountName • If Digest-MD5, CRAM-MD5, Login, Plain or Simple Bind is selected to access the LDAP server: displayName

LDAP Authentication

User Authentication Setting

User Authentication: Enable

User Authentication According to Function: Disable

Copy: Enable

Fax: Enable

Print: Enable

Scan: Enable

List: Enable

User Functions: Enable

EWB: Enable

Authentication Method for Admin: User Name and Password

Authentication failed print job/Raw Print Job: Hold

Auto Release on Login: Disable

Project Management: Disable

Print Job(Without Project Code): Hold

Authentication Method for Print Jobs: Use User Name and Domain Name

☐ Use Password Authentication for Print Job
*It is not able to print from other than Windows Client when this function is enabled.

Delete Own Account: Disable

Enable Guidance Screen: Card Authentication

☐ Enable Guest User

Authentication Type: LDAP Authentication

1 ☒ Create User Information Automatically

2 ☐ Use cache information when user authentication failed

3 Validity Period of Cache: 7 Days(1-14)

4 ☐ Register Local User which is available in Windows Domain Authentication/LDAP Authentication

5 Validity Period of Local User: 30 (0-180, Unlimited 0)

6 **Server Assignment** Move Down Move Up

LDAP Server	Server IP Address	Type	Attribute type of "User Name"
LDAP01	192.168.1.1	Windows Server	displayName
LDAPServer001	192.168.1.2	Windows Server	displayName
LDAPServer002	192.168.1.3	Windows Server	displayName

The priority is from the top.

7 **Role Based Access Setting**

Role Based Access using LDAP server: Disable

LDAP Server: LDAP01

8 **PIN Code Authentication Setting**

PIN Code Authentication: Disable

Minimum PIN Code Length: 1 (1-32)

9 **Card Authentication Setting**

Card Authentication: Enable

10 Auto Change Login User: Enable

11 ☐ Require PIN Code

12 **Server Assignment** Move Down Move Up

LDAP Server	Server IP Address	Type	Attribute type of "User Name"	Attribute type of "Card Information"
-------------	-------------------	------	-------------------------------	--------------------------------------

The priority is from the top.

	Item name	Description
1	Create User Information Automatically	<p>Select whether or not to register user information automatically to this equipment. This item is selected as the default. By registering user accounts to the printer, you can manage counters and quotas for each user.</p> <p>Tip</p> <p>When automatically adding a user while printing from the printer driver, enable [Use Password Authentication for Print Job] on the [User Authentication Setting] screen.</p> <p> P.240 "Setting up User Authentication Setting"</p>

	Item name	Description
2	Use cache information when user authentication failed	<p>Either of the following data is saved according to the authentication method. Password, Card number, Domain name, PIN code, Home Directory information or RBAC information.</p> <p>Tip</p> <p>The cache information will be updated if user authentication succeeds with the authentication server. However, if a user is authenticated with the cache information, it is not updated.</p>
3	Validity Period of Cache	Enter the number of days to maintain the cache information. 1 to 14 days can be set from the latest update.
4	Register Local User which is available in Windows Domain Authentication/LDAP Authentication	Select this to register a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
5	Validity Period of Local User	Enter the number of valid days for local users. Up to 180 days can be set from the user creation day. If 0 is set, the number of valid days will be indefinite.
6	LDAP Server List	<p>Displays a list of servers that are assigned for LDAP Authentication. Click [Server Assignment] and add the server in the displayed screen to assign a server. Register the available server as [LDAP Client].</p> <p>Use [Move Up] and [Move Down] to change the priority order in the list.</p> <p> P.151 “LDAP Client settings”</p>
7	Role Based Access Setting	<p>Configure role based access using an LDAP server.</p> <p>Role Based Access using LDAP server — Select whether enable or disable role based access. [Disable] is set as the default.</p> <p>LDAP Server — Select the LDAP server that manages the Role Based Access Control.</p>
8	PIN Code Authentication Setting	<p>PIN Code Authentication — Select the PIN code authentication method.</p> <ul style="list-style-type: none"> • Disable — Select this no to use the PIN code authentication. Use the user name and password for authentication. • Enable — Select this to use the PIN code authentication. Instead of the PIN code, it is possible to use the user name and password for authentication. <p>Minimum PIN Code Length — Enter a figure that specifies the minimum digits for the PIN code.</p>
9	Card Authentication	<p>Select whether or not to enable card authentication.</p> <p>Note</p> <p>For the details of the card authentication setting, contact your service technician.</p>
10	Auto Change Login User	Select whether or not to enable the function to change login users automatically when authenticating users with the card.
11	Require PIN Code	<p>Select whether or not to require PIN code when authenticating users with the card.</p> <p>Tip</p> <p>This function is available only on the equipment that supports the PIN code input.</p>

	Item name	Description
12	LDAP Server List	<p>Displays a list of servers that are assigned for the PIN code or card authentication. Click [Server Assignment] and add the server in the displayed screen to assign a server. Register the available server as [LDAP Client]. Use [Move Up] and [Move Down] to change the priority order in the list.</p> <p> P.151 “LDAP Client settings”</p> <p>Tip</p> <p>If [Windows Server] is selected as an LDAP server for the PIN code or card authentication, the following attribute type of user name is employed for the one at the login and the one of the user which is automatically registered while [Create User Information Automatically] is enabled.</p> <ul style="list-style-type: none"> • If Kerberos is selected to access the LDAP server: sAMAccountName • If Digest-MD5, CRAM-MD5, Login, Plain or Simple Bind is selected to access the LDAP server: displayName

Setting up Email Authentication


When E-mail authentication is enabled, users must enter the user name and password before performing Scan to Email.

	Item name	Description
1	Email Authentication	Select whether or not to enable E-mail authentication.
	<p>Note</p> <p>You must carry out “E-mail address setting” to use E-mail authentication.</p> <p> P.254 “Setting up Email Address Setting”</p>	

❏ Setting up Email Address Setting

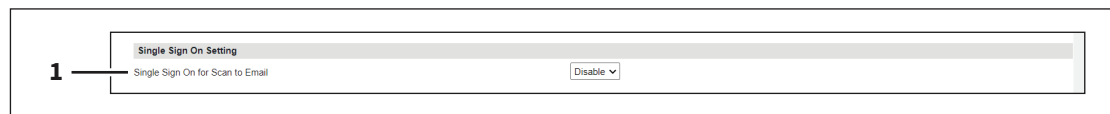
You can configure the E-mail address when E-mail authentication is enabled.

	Item name	Description
1	From Address	<p>Specify the From Address.</p> <p>'From Address' of Email Setting: Select this to set the From Address in E-mail settings.</p> <p>User Name + @ + Mail Domain Name: Select this to specify the From Address in the “User Name + @ + Mail Domain Name” format. The authenticated user name is employed as the “User Name”. The domain name specified in the [Domain Name] box is used as the “Mail Domain Name”. When this is selected, enter the domain name in the [Domain Name] box.</p> <p>'User Name' of LDAP: Select this to set the From Address with the one you have selected from LDAP addresses. When you select this function, a list of servers assigned for LDAP authentication is displayed to allow you to select one. Specify the mail domain name to be used in the case the LDAP server search fails in the [Domain Name] box. The equipment searches the authenticated user name in [Attribute type of “User Name”] of the LDAP server. If the registered user name has been found in the specified schema, the schema value set in [Attribute type of “Email Address”] becomes the sender address. If the registered user name has not been found in the specified schema, the format set in [User Name + @ + Mail Domain Name] becomes the sender address. You can assign up to 4 registered LDAP servers to search. Click the [Server Assignment] button and add the server in the displayed screen to change the assignment. Register the available server as [LDAP Client]. Use [Move Up] and [Move Down] to change the priority order in the list. P.151 “LDAP Client settings”</p> <p>Use Email Address which was registered Local User: Specify the Email Address that is registered to the user information.</p> <p>From Address cannot be edited in Scan to Email.: Select this check box if you do not want to allow users to edit the From Address.</p>
2	From Name	<p>Specify the From Name.</p> <p>Account Name of From Address + From Name of Email Setting: Select this to specify the From Name in the “Account Name of From Address + From Name of Email Setting” format.</p> <p>'From Name' of Email setting: Select this to set the From Name which has been specified in E-mail settings.</p> <p>'User Name' of LDAP: If the “From Address” is already set to “'User Name' of LDAP”, “From Name” is also automatically set to “'User Name' of LDAP” and used as the sender of the e-mail to the selected LDAP address.</p> <p>Login User Name: Specify the Login User Name that is registered to the user information.</p>

	Item name	Description
3	Restriction setting for Email Destination	<p>When User Authentication or Email Authentication is enabled, select whether to set the From Address of the authenticated user as a destination.</p> <ul style="list-style-type: none"> • None — Not used as a destination. • Fixed To — Only the From Address of the authenticated user is used for “To”. • To — The From Address of the authenticated user is added to “To”. • Cc — The From Address of the authenticated user is added to “Cc”. • Bcc — The From Address of the authenticated user is added to “Bcc”. <p>When you select any setting except None, the item list appears so that you can select one of the following items from the list to specify one's own address besides the sender's address.</p> <p>use From Address: Select this to use the E-mail address (log-in user's E-mail address) which has been set at the above-mentioned [From Address].</p> <p>'From Address' of Email Setting: Select this to set the From Address in E-mail settings.</p> <p>User Name + @ + Mail Domain Name: Select this to specify the From Address in the “User Name + @ + Mail Domain Name” format. The authenticated user name is employed as the “User Name”. The domain name specified in the [Domain Name] box is used as the “Mail Domain Name”. When this is selected, enter the domain name in the [Domain Name] box.</p> <p>'User Name' of LDAP: Select this to set the From Address with the one you have selected from LDAP addresses. When you select this function, a list of servers assigned for LDAP authentication is displayed to allow you to select one. Specify the mail domain name to be used in the case the LDAP server search fails in the [Domain Name] box. The equipment searches the authenticated user name in [Attribute type of “User Name”] of the LDAP server. If the registered user name has been found in the specified schema, the schema value set in [Attribute type of “Email Address”] becomes the sender address. If the registered user name has not been found in the specified schema, the format set in [User Name + @ + Mail Domain Name] becomes the sender address. You can assign up to 4 registered LDAP servers to search. Click the [Server Assignment] button and add the server in the displayed screen to change the assignment. Register the available server as [LDAP Client]. Use [Move Up] and [Move Down] to change the priority order in the list.  P.151 “LDAP Client settings”</p> <p>Use Email Address which was registered Local User: Specify the Email Address that is registered to the user information.</p>

❑ Setting up Single Sign On Setting

Normally users are required to enter the user name and password for E-mail authentication and Scan to Email; however, you can enable the single sign on setting to eliminate these operations.



	Item name	Description
1	Single Sign On for Scan to Email	Select whether or not to enable single sign on. [Disable] is set as the default.

❑ Setting up Home Directory Setting

You can configure the home directory when home directory is enabled.



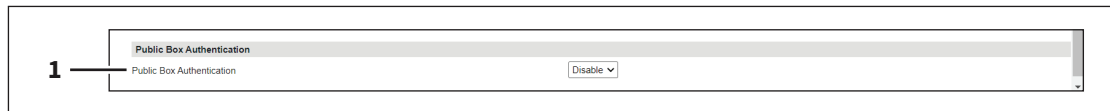
	Item name	Description
1	Home Directory	Select whether or not to enable home directory.
2	Home Directory Server	<p>Specify the home directory server.</p> <ul style="list-style-type: none">• Use Home Directory, Registered as Local User — Select this to use the home directory which was registered for a local user. This option is available only when [MFP Local Authentication] is selected for [Authentication Type].• Use User Authentication Server — Select this to use the user authentication server as the home directory server.• Use User Authentication Server(Use specific server for Card Authentication) — Select this to use the user authentication server as the home directory server. However, use the specified server as the home directory server in the case of Card Authentication.• User Specific Server — Select this to specify the home directory server. <p>If you select “Use User Authentication Server (Use specific server for Card Authentication)” or “User Specific Server”, the LDAP server list appears on the screen. You can set up to 3 servers. Click the “Primary” button to select the primary server.</p> <p>Click the LDAP server name on the list to open the Home Directory Server Setting screen. Select the home directory server for each server name. If you do not specify the server, select “Disable”.</p>

Public Box Authentication

You can set the password authentication for the public box.

Note

This setting can protect the public box with a password. Set the password at the properties window of the public box that you can open from inside the e-Filing box.



	Item name	Description
1	Public Box Authentication	Select whether to enable the password authentication for the public box. <ul style="list-style-type: none">• Disable — Disables the password authentication. The password entry is not required for the access to the public box.• Enable — Enables the password authentication. The password entry is required for the access to the public box.

Certificate Management settings

You can manage device certificates and client certificates.

Tip

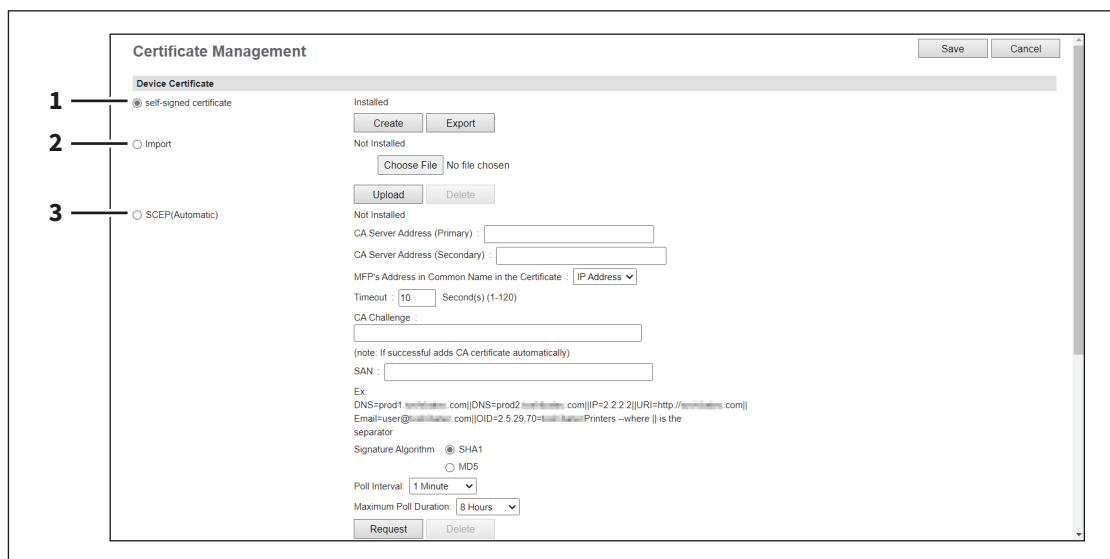
The [Certificate Management] submenu can be accessed from the [Security] menu on the [Administration] page. For how to access it and information on the [Security] menu, see the references below:


📖 P.14 “Access Policy Mode”

📖 P.238 “[Security] Item List”

Setting up Device Certificate

You can configure the device certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS.



	Item name	Description
1	self-signed certificate	<p>Creates a certificate for encrypted communications using SSL/TLS on your device.</p> <p>[Create] button — Displays the [Create self-signed certificate] screen. Specify items necessary for the certificate to create the self-signed certificate.</p> <p> P.259 “[Create self-signed certificate] screen”</p> <p>[Export] button — Exports the created self-signed certificate.</p>
2	Import	<p>Import the certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS.</p> <p>[Choose File] button — Allows you to select the certificate file.</p> <p>[Upload] button — Uploads the selected certificate file.</p> <p>[Delete] button — Deletes the registered certificate file.</p>
3	SCEP(Automatic)	<p>Automatically acquires the certificate for encrypted communications using IP sec or SSL/TLS.</p> <p>CA Server Address (Primary) — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols.</p> <p>CA Server Address (Secondary) — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols.</p> <p>MFP's Address in Common Name in the Certificate — Select whether you use the IP address or FQDN as the address of this equipment to be entered in the [Common Name] box of the certificate. [IP Address] is set as the default.</p> <p>Timeout — Enter a timeout period for quitting communication when no response is received from the CA server. Specify within the range from 1 to 120 seconds. “10” is set as the default.</p> <p>CA Challenge — Enter the password for the CA challenge. You can enter up to 32 alphanumerical characters. You need to enter a maximum of 32 alphanumerical characters for the first time when you extend the password length.</p> <p>SAN — Set the SAN attribute if necessary. Enter DNS, IP address, URI, e-mail address and OID by dividing them with . There are some restrictions as below.</p> <p>DNS: You can enter up to 253 letters with alphanumerical characters and symbols “.” and “-”.</p> <p>URI: You can use alphanumerical characters and symbols “- . _ ~ : / ? # ! @ \$ ' () * + ; =”.</p> <p>Email: You need to enter “@” and “.” in the address.</p> <p>Signature Algorithm — Select SHA1 or MD5 as the signature algorithm.</p> <p>Poll Interval — Specify the polling interval. [1 Minute] is set as the default.</p> <p>Maximum Poll Duration — Specify the polling duration. [8 Hours] is set as the default.</p> <p>[Request] button — Click this button to request the certificate.</p> <p>[Delete] button — Deletes the registered certificate.</p>

[Create self-signed certificate] screen

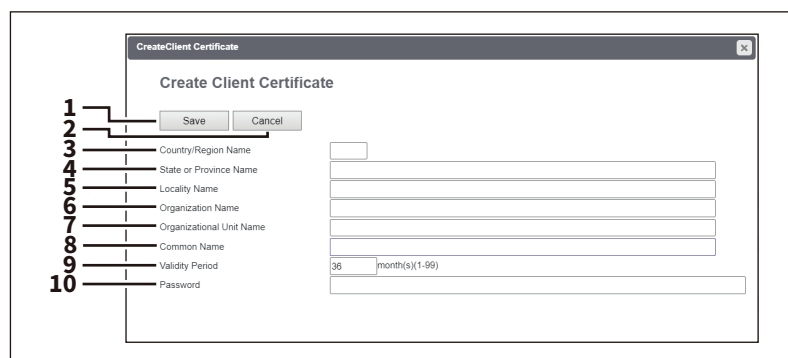
	Item name	Description
1	[Save] button	Saves the self-signed certificate.
2	[Cancel] button	Cancels creating the certificate.
3	Country/Region Name	Enter the country or region name using two alphanumerical characters and symbols. (Example: JP)
4	State or Province Name	Enter the state or province name with alphanumerical characters and symbols. You can enter up to 128 characters.
5	Locality Name	Enter the city or town name with alphanumerical characters and symbols. You can enter up to 128 characters.
6	Organization Name	Enter the organization name with alphanumerical characters and symbols. You can enter up to 64 characters.
7	Organizational Unit Name	Enter the organizational unit name with alphanumerical characters and symbols. You can enter up to 64 characters.
8	Common Name	Enter the FQDN or IP address of this equipment with alphanumerical characters and symbols. You can enter up to 64 characters.
9	Email Address	Enter the E-mail address with alphanumerical characters and symbols. You can enter up to 64 characters.
10	Validity Period	Enter the number of months in the validity period of the self-signed certificate.

❑ Setting up Client Certificate



	Item name	Description
1	Client Certificate	Creates the client certificate. [Create] button — Displays the [Create Client Certificate] screen. Specify items necessary for the certificate to create the client certificate. 📖 P.260 “[Create Client Certificate] screen”

[Create Client Certificate] screen



	Item name	Description
1	[Save] button	Saves the Client certificate.
2	[Cancel] button	Cancels creating the certificate.
3	Country/Region Name	Enter the country or region name using two alphanumerical characters and symbols. (Example: JP)
4	State or Province Name	Enter the state or province name with alphanumerical characters and symbols. You can enter up to 128 characters.
5	Locality Name	Enter the city or town name with alphanumerical characters and symbols. You can enter up to 128 characters.
6	Organization Name	Enter the organization name with alphanumerical characters and symbols. You can enter up to 64 characters.
7	Organizational Unit Name	Enter the organizational unit name with alphanumerical characters and symbols. You can enter up to 64 characters.
8	Common Name	Enter the FQDN or IP address of this equipment with alphanumerical characters and symbols. You can enter up to 64 characters.
9	Validity Period	Enter the number of months in the validity period of the self-signed certificate.
10	Password	Enter the password of the certificate with alphanumerical characters and symbols. You can enter up to 64 characters.

❑ Setting up Certificate Setting

The screenshot shows a 'Certificate Setting' window. Step 1 points to the 'Signature Algorithm' dropdown menu, which is set to 'SHA256'. Step 2 points to the 'Public Key' dropdown menu, which is set to 'RSA2048'.

Note

When you create PDF with the digital signature in the PDF/A-1b file format, you need to select the [SHA1] signature algorithm and the [RSA1024] public key.

📖 P.116 “PDF/A Fileformat Setting”

	Item name	Description
1	Signature Algorithm	<p>Select the signature algorithm to be used in Certificate.</p> <p>SHA1 — Select this to use SHA1.</p> <p>SHA256 — Select this to use SHA256.</p> <p>SHA384 — Select this to use SHA384.</p> <p>SHA512 — Select this to use SHA512.</p> <p>Tip</p> <p>Select a signature algorithm from SHA256, SHA384, and SHA512 to create a self-signed certificate.</p>
2	Public Key	<p>Select the public key to be used in Certificate.</p> <p>RSA1024 — Select this to use RSA1024.</p> <p>RSA2048 — Select this to use RSA2048.</p> <p>Tip</p> <p>Select “RSA2048” for the public key to create a self-signed certificate.</p>

❑ Setting up CA Certificate

When you want to enable SSL/TLS and verify with a CA certificate for the SMTP Client, POP3 Network Service, FTP Client, Directory Service, or Syslog Setting, you must install the CA certificate. You can install up to 10 CA certificates in this equipment.

The screenshot shows a 'CA certificate' window. Step 1 points to the 'CA Certificate(PEM)' radio button. Step 2 points to the 'CA certificate (DER)' radio button. Below the radio buttons are two 'Choose File' buttons, each with 'No file chosen' text. At the bottom are 'Upload' and 'Delete' buttons.

	Item name	Description
1	CA Certificate(PEM)	<p>Selects the certificate in the PEM format.</p> <p>[Upload] button — Uploads the certificate.</p> <p>[Delete] button — Deletes the registered certificate.</p>
2	CA certificate (DER)	<p>Selects the certificate in the DER format.</p> <p>[Upload] button — Uploads the certificate.</p> <p>[Delete] button — Deletes the registered certificate.</p>

❑ Setting up Certificate Files

You can display a list of registered certificate files.

■ Password Policy settings

You can configure policies for the password to register.

Tip

The [Password Policy] submenu can be accessed from the [Security] menu on the [Administration] page. For how to access it and information on the [Security] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.238 “[Security] Item List”

□ Setting up Policy for Users

You can configure policies for user registration.

Tip

If you change the settings, they become effective from the next login.

The screenshot shows a 'Password Policy' configuration window. It has a title bar with 'Save' and 'Cancel' buttons. The main area is titled 'Policy for Users' and contains four numbered items: 1. Minimum Password Length (0-64), 2. Requirements to Apply (Disable), 3. Lockout Setting (Enable), and 4. Available Period (Disable). The 'Requirements to Apply' section is expanded, showing a list of strings that cannot be used as passwords. The 'Lockout Setting' section is also expanded, showing 'Number of Retry' (10) and 'Lockout Time' (1 minute). The 'Available Period' section is expanded, showing 'Expiration day(s)' (1-999).

	Item name	Description
1	Minimum Password Length	Specify the minimum number of digits for the password. Specify within the range from 0 to 64. “0” is set as the default.
2	Requirements to Apply	Select [Enable] to set restrictions on the character strings that can be used in passwords. [Disable] is set as the default. Restrictions <ul style="list-style-type: none">• The user name and password cannot be the same.• The same password cannot be used again.• A password consisting of sequences of the same characters cannot be used.• A password containing the characters entered in the restricted character text box cannot be used.
3	Lockout Setting	Specify whether or not to enable the lockout setting when the user failed to supply the correct password. [Enable] is set as the default. Number of Retry — Specify the number of incorrect password entry times to lock out the user. Specify within the range from 1 to 30 times. “10” is set as the default. Lockout Time — Specify the duration to lock out the user. Specify within the range from 1 to 1440 minutes. “1” is set as the default. <p>Tip</p> Due to a change in the number of retry times, a user may lock out in the next login. The history of lockouts is registered in the log.

	Item name	Description
4	Available Period	<p>Select [Enable] to specify how long the password is valid before its expiry. [Disable] is set as the default.</p> <p>Expiration day(s) — Specify how long the password is valid before its expiry. Specify within the range from 1 to 999 days. “180” is set as the default.</p> <p>Tip</p> <p>When the number of days set in [Expiration day(s)] elapses, a screen that prompts the user to change the password will appear the next time the user logs in.</p>

❑ Setting up Policy for Administrator, Auditor

You can configure policies for administrator and auditor registration.

	Item name	Description
1	Minimum Password Length	Specify the minimum number of digits for the password. Specify within the range from 6 to 64. “6” is set as the default.
2	Requirements to Apply	<p>Select [Enable] to set restrictions on the character strings that can be used in passwords. [Disable] is set as the default.</p> <p>Restrictions</p> <ul style="list-style-type: none"> • The user name and password cannot be the same. • The same password cannot be used again. • A password consisting of sequences of the same characters cannot be used. • A password containing the characters entered in the restricted character text box cannot be used.
3	Lockout Setting	<p>Specify whether or not to enable the lockout setting when the user failed to supply the correct password. [Enable] is set as the default.</p> <p>Number of Retry — Specify the number of incorrect password entry times to lock out the user. Specify within the range from 1 to 30 times. “10” is set as the default.</p> <p>Lockout Time — Specify the duration to lock out the user. Specify within the range from 1 to 1440 minutes. “1” is set as the default.</p> <p>Tip</p> <p>Due to a change in the number of retry times, a user may lock out in the next login. The history of lockouts is registered in the log.</p>

	Item name	Description
4	Available Period	<p>Select [Enable] to specify how long the password is valid before its expiry. [Disable] is set as the default.</p> <p>Expiration day(s) — Specify how long the password is valid before its expiry. Specify within the range from 1 to 999 days. “180” is set as the default.</p> <p>Tip</p> <p>When the number of days set in [Expiration day(s)] elapses, a screen that prompts the user to change the password will appear the next time the user logs in.</p>

❑ Setting up Policy for e-Filing Boxes, SecurePDF, SNMPv3, Cloning, Secure Receive

You can configure policies for passwords for operations and applications on your equipment.

	Item name	Description
1	Minimum Password Length (e-Filing Boxes)	Specify the minimum number of digits for the password of e-Filing boxes. Specify within the range from 0 to 20. “1” is set as the default.
2	Minimum Password Length (SecurePDF, SNMPv3, Cloning, Secure Receive)	Specify the minimum number of digits for the password of Secure PDF, SNMPv3, Cloning, and Secure Receive. Specify within the range from 0 to 20. ^{*1} “0” is set as the default.
3	Requirements to Apply	<p>Select [Enable] to set restrictions on the character strings that can be used in passwords. [Disable] is set as the default.</p> <p>Restrictions</p> <ul style="list-style-type: none"> • The file name and password cannot be the same.^{*2} • The same password cannot be used again.
4	Lockout Setting ^{*3}	<p>Specify whether or not to enable the lockout setting when the user failed to supply the correct password. [Disable] is set as the default.</p> <p>Number of Retry — Specify the number of incorrect password entry times to lock out the user. “10” is set as the default.</p> <p>Lockout Time — Specify the duration to lock out the user. Specify within the range from 1 to 1440 minutes. “1” is set as the default.</p> <p>Tip</p> <p>Due to a change in the number of retry times, a user may lock out in the next login. The history of lockouts is registered in the log.</p>

^{*1} With SNMPv3 and encrypted PDF files, a password of at least one character is required.

^{*2} With Cloning, you can also register the same password as the file name.

^{*3} The Lockout Setting is enabled only when you are using e-Filing Boxes.

■ Security Stamp setting

You can add information such as the date, time and user name at the edge of the print output or transmission images.

	Item name	Description
1	Print	Copy — Specify whether or not to add information to copy jobs. [Disable] is set as the default. Printer — Specify whether or not to add information to print jobs. [Disable] is set as the default. e-Filing — Specify whether or not to add information to e-Filing jobs. [Disable] is set as the default.
2	Fax	Transmission — Specify whether or not to add information to fax transmission jobs. [Disable] is set as the default.
3	Job ID	Specify whether or not to include the job ID in the stamp.
4	Date & Time	Specify whether or not to include the date and time in the stamp. <ul style="list-style-type: none"> • Date: Prints the date. • Date & Time: Prints the date and time.
5	Card ID	Specify whether or not to include the card ID in the stamp.
6	User Name	Specify whether or not to include the user name in the stamp.
7	Serial Number	Specify whether or not to include the serial number in the stamp.
8	Department Name	Specify whether or not to include the department name in the stamp.
9	Optional text	Specify whether or not to include optional text in the stamp. You can enter up to 32 alphanumeric characters.

Note

If you add both the TTI and security stamp, the TTI is added as the first line and the security stamp is added as the second line.

Security stamps are added at the top 5mm of the fax image; therefore, the top 5mm of the image is not printed at the recipient.

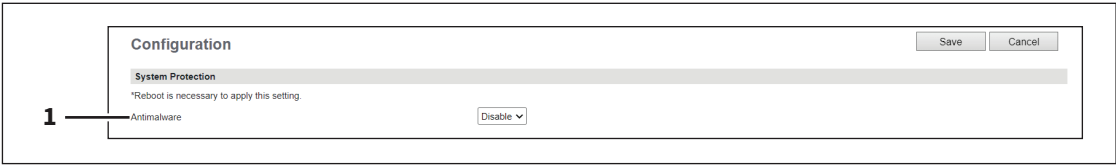
Tip

When including the date and time in the stamp, the transmission date and time of the first page is printed on all pages for security stamps. Whereas the transmission date and time of each page is printed for TTI.

■ Configuration settings

❑ System Protection

You can configure the equipment to protect the system from malware. The information about the applications that can run on the equipment is automatically updated so that the activity of malware can be monitored. If you run any unknown application with this function enabled, the equipment records the activity in the log and shows the service call message on the control panel. Do not run the application after the equipment restarts. For details, ask your service representative.



	Item name	Description
1	Antimalware	<p>Select whether to enable the antimalware function. Change and save the setting while no jobs are in execution, and reboot the equipment, so that this function becomes effective.</p> <ul style="list-style-type: none">• Enable — Enables the antimalware function. The antimalware icon appears on the counter screen on the control panel of the equipment to monitor the activity of malware.• Disable — Disables the antimalware function.

Tip

Users who are granted administrator privileges in access policy mode can access the [Maintenance] menu from the [Administration] page.
For how to access it, see the reference below:
 P.14 “Access Policy Mode”

■ Upload Software settings

You can update client software embedded in your equipment. Users can download client software on their computers using the TopAccess [Install Software] link.

- Installer (Setup files) for Client Utilities CD-ROM or Client Utilities/User Documentation DVD
- Mac PPD Files
- UNIX Filters

Note

Uploading new software overwrites the old version of software that had been uploaded.

Tip

The files for uploading are provided for each client software.

- **Driver Files**
 - Contact your dealer for information about obtaining driver files with the installer.
 - You can create a driver file for uploading by compressing folders under “Client\Drivers” in the Client Utilities/User Documentation DVD in zip format. P.268 “Preparing a driver file for uploading”
- **Mac PPD Files** — These files are stored in the “MacPPD” folders in the Client Utilities/User Documentation DVD. The PPD file for duplex printing is stored in the “2-sided_default” folder, whereas the PPD file for simplex printing is stored in the “normal” folder.
- **Unix Filters** — These filters are stored in the folder for each workstation in the “Admin\BW_Unix_Linux” folder (for black printing) or “Admin\Color_Unix_Linux” folder (for color printing) included in the Client Utilities/User Documentation DVD. The CUPS filter for duplex printing is stored in the “2-sided_default” folder whereas the one for simplex printing is in the “normal” folder.

The [Upload Software] submenu can be accessed from the [Maintenance] menu on the [Administration] page.
For how to access it and information on the [Maintenance] menu, see the references below:

- P.14 “Access Policy Mode”
- P.267 “[Maintenance] Item List”

When [Driver Customization Packages] is selected:

Upload Software

You can upload client software to the controller. This allows end-users to install the software into their system from the TopAccess "Install Software" icon, located at the top of the TopAccess page.

1 Upload Files Driver Customization Packages ▼

2 Upload

The following are the required files.

3 File Name Choose File No file chosen

4 **Installed Driver Customization Packages List**

Number	Version	Size	Description
--------	---------	------	-------------

	Item name	Description
1	Upload Files	<p>Select the software you want to upload to the equipment.</p> <ul style="list-style-type: none"> • Driver Files — Select this to upload the setup files. • Mac PPD Files — Select this to upload the PPD file which is used by macOS. • Unix Filters — Select this to upload the tar files that contain filters for each UNIX workstation. • Driver Customization Packages — Select this to upload the custom package file for the printer driver. <p>[OK] button — Confirms the selected software.</p>
2	[Upload] button	Uploads the browsed setting file.
3	[Choose File] button	<p>Browses the setting file to be uploaded. Select the corresponding setting file.</p> <p>Note</p> <p>At the left of each box, the file name will be displayed. Be sure to specify the same file for each box.</p>
4	Installed Driver Customization Packages List	Displays a list of installed custom package files.

❑ Preparing a driver file for uploading

- 1 **Insert the Client Utilities/User Documentation DVD into the computer's CD-ROM or DVD-ROM drive.**
- 2 **Open the folder where driver files and plug-in files are stored.**
They are stored in the "Client\Drivers" folder.
- 3 **Compress the folder in zip format to create the driver file for uploading.**

Folder name	Name of the ZIP file to be created	Remarks
UNI	univ.zip	Universal printer driver
PS	ps3.zip	PS3 printer driver (PostScript)

Tip

Match the name of the ZIP file to be created with the file name displayed on the TopAccess screen. The file name is case sensitive. If the file name is different, you will not be able to upload it.

■ Remove Software settings

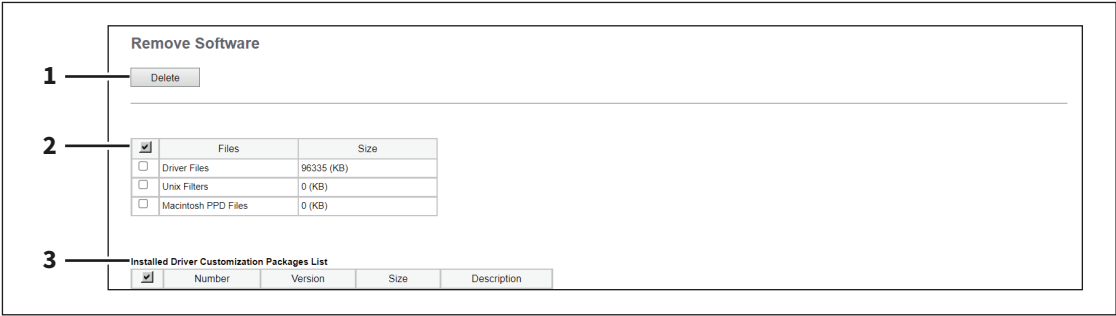
You can delete the software uploaded to the equipment.

Tip

The [Remove Software] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”



	Item name	Description
1	[Delete] button	Deletes the selected software. Select and click the software to be deleted from the software list.
2	Software list	Displays a list of software uploaded to your equipment. Select the software files you want to delete.
3	Installed Driver Customization Packages List	Displays a list of the installed custom package files. Select the files you want to delete.

Create Clone File settings

You can create a clone file of the environment on your equipment.
You can implement a cloned environment by installing the created clone file on another equipment.
For the details of the clone file and how to use it, contact your service technician.

Note

- The clone files are compatible with other equipment units. For details about the available models, contact your service representative.
- When an end-user (either an individual or an entity) intends to clone data (font, ICC profile, or any data downloaded or added by the end-user) stored in TTEC products (copier, MFP), the end-user shall investigate, review and confirm terms of use for such data and intellectual property rights thereof. The end-user shall perform such cloning at your own risk and responsibility.
TTEC AND ITS AFFILIATES HEREBY DISCLAIM ANY WARRANTY OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE WARRANTIES OF QUALITY AND PERFORMANCE OF TTEC PRODUCTS, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF THIRD PARTIES INTELLECTUAL PROPERTY RIGHTS, IN THE USE OF CLONING BY THE END-USER.
IN NO EVENT WILL TTEC BE LIABLE TO THE END-USER NOR ANY THIRD PARTY FOR ANY DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHERWISE, INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, LOST DATA OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF CLONING BY THE END-USER, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.
- When you clone the LDAP role, make sure of the consistent LDAP settings between the equipment units.
- If you have installed a clone file from other models, the equipment might not work properly. For recovery, be sure to create a clone file on the target equipment and keep it before installing the clone file.

Tip

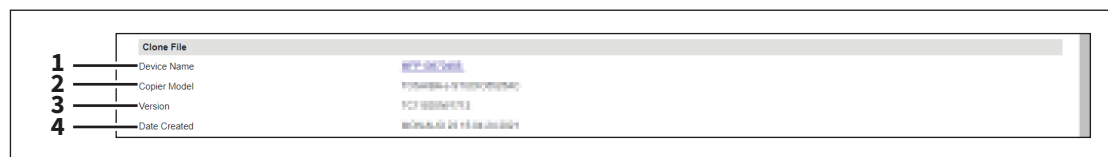
The [Create Clone File] submenu can be accessed from the [Maintenance] menu on the [Administration] page.
For how to access it and information on the [Maintenance] menu, see the references below:

- 📖 P.14 “Access Policy Mode”
- 📖 P.267 “[Maintenance] Item List”



	Item name	Description
1	[Create] button	Creates the clone file of the category selected in the category setting. When you click this button, a screen is displayed to set a password on the clone file.

❑ Setting up Clone File



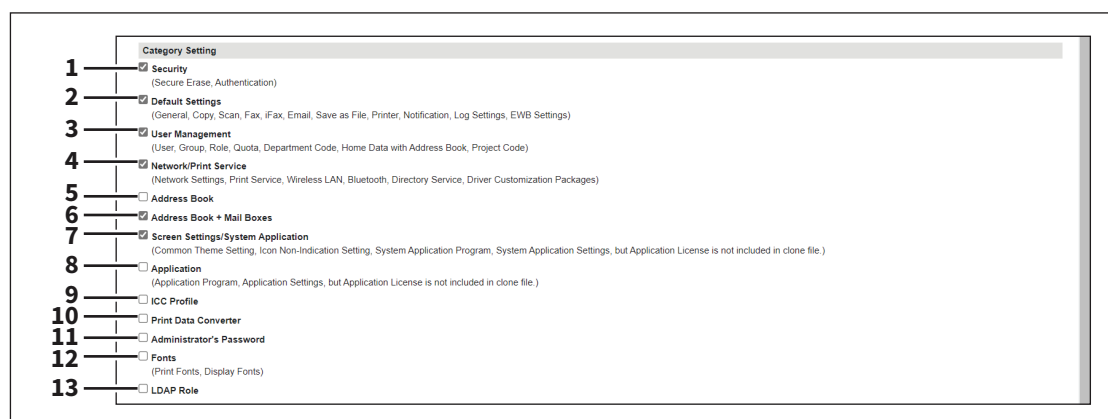
	Item name	Description
1	Device Name	Displays the device name of the created clone file. Click the device name to download the clone file.
2	Copier Model	Displays the copier model of the created clone file.
3	Version	Displays the system ROM version of the created clone file.
4	Date Created	Displays the created date of the clone file.

❑ Setting up Category Setting

Select the category for the clone file.

Tip

The clone file will include the settings listed in “Description” that make up the category you select.



	Item name	Description
1	Security	Includes secure erase and authentication settings in the clone file.
2	Default Settings	Includes the general, copy, scan, fax, ifax, E-mail, save as file, printer, notification, log settings, and EWB settings in the clone file.
3	User Management	Includes the user, group, role, quota, department code, home data with address book, and project code in the clone file.
4	Network/Print Service	Includes network, print service, wireless LAN, Bluetooth, directory service, and driver customization packages settings in the clone file.
5	Address Book	Includes the address book in the clone file.
6	Address Book + Mail Boxes	Includes the address book and mail boxes in the clone file.
7	Screen Settings/System Application	Includes the common theme setting, the icon non-indication setting, the system application program, and the system application settings (except licenses) in the clone file.
8	Application	Includes the application program and application setting (except licenses) in the clone file.

	Item name	Description
9	ICC Profile	Includes ICC profiles installed from TopAccess in the clone file. Note <ul style="list-style-type: none"> You can select ICC profiles only for color models. You are required to have the license to use some ICC profiles.
10	Print Data Converter	Includes print data converter settings in the clone file.
11	Administrator's Password	Includes the password of the default administrator in the clone file.
12	Fonts	Includes downloaded fonts for print and display in the clone file. Note You are required to have the license to use some fonts.
13	LDAP Role	Includes information about the LDAP role in the clone file.

■ Install Clone File settings

You can install the created clone file.

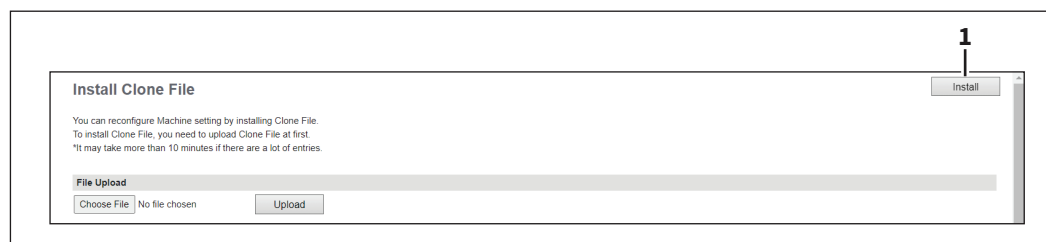
You can implement a cloned environment by installing the clone file created on another equipment.

Note

- Before the clone file is installed, confirm that no jobs in progress or under waiting remain by means of the [Job Status] page. If any jobs do remain, the installation of the clone files cannot be carried out.
[P.24 "\[Job Status\] Overview"](#)
- After the clone file has been installed, reboot this equipment in accordance with the guidance. Manually reboot this equipment if you did not do so by closing the installation execution screen.
- After you do cloning between the color and monochrome models, the sleep mode action might be changed. If the equipment is turned off unexpectedly or the sleep mode does not work as you like, check the Sleep Mode setting.
[P.107 "Setting up Energy Save"](#)

Tip

- The [Install Clone File] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:
[P.14 "Access Policy Mode"](#)
[P.267 "\[Maintenance\] Item List"](#)
- When the installation of the clone file is complete, the screen shows the reference link so that you can click it to download a file that records the result of the installation.



	Item name	Description
1	[Install] button	Installs the selected clone file. When you click this button, a dialog box is displayed to prompt you to enter the password you specified when creating the clone file.

❑ Setting up File Upload

1 — Choose File | No file chosen | Upload

2 — Clone file information

	Item name	Description
1	[Choose File] button	Select a clone file.
2	[Upload] button	Displays information on the selected clone file and what is included in the clone file.

❑ Setting up Clone File Information

1 — Device Name

2 — Copier Model

3 — Version

4 — Date Created

	Item name	Description
1	Device Name	Displays the device name of the created clone file.
2	Copier Model	Displays the copier model of the created clone file.
3	Version	Displays the system ROM version of the created clone file.
4	Date Created	Displays the created date of the clone file.

❑ Setting up Setting data included in Clone File

1 — Security

2 — Default Settings

3 — User Management

4 — Network/Print Service

5 — Address Book

6 — Address Book + Mail Boxes

7 — Screen Settings/System Application

8 — Application

9 — ICC Profile

10 — Print Data Converter

11 — Administrator's Password

12 — Fonts

13 — LDAP Role

	Item name	Description
1	Security	Displays if secure erase and authentication settings are included.
2	Default Settings	Displays if the general, copy, scan, fax, ifax, E-mail, save as file, printer, notification, log settings, and EWB settings are included.
3	User Management	Displays if the user, group, role, quota, department code, home data with address book, and project code are included. Tip Select whether or not to include the address book information when user management is included but the address book is not. When excluding the address book has been selected, it is necessary to input again the addresses registered from the address book.

	Item name	Description
4	Network/Print Service	Displays if network, print service, wireless LAN, Bluetooth, directory service, and driver customization packages settings are included.
5	Address Book	Displays if the address book is included.
6	Address Book + Mail Boxes	Displays if the address book and MailBox are included.
7	Screen Settings/System Application	Displays if the common theme setting, the icon non-indication setting, the system application program, and the system application settings (except licenses) are included.
8	Application	Displays if the application program and application setting (except licenses) are included.
9	ICC Profile	Displays if the ICC profiles installed from TopAccess are included. This item appears only for color models.
10	Print Data Converter	Displays if the print data converter settings are included.
11	Administrator's password	Displays if the password of the default administrator is included.
12	Fonts	Displays if downloaded fonts for print and display are included.
13	LDAP Role	Displays if the LDAP role is included.

■ Import settings

You can import address book data and department code information exported from another equipment.

Tip

The [Import] submenu can be accessed from the [Maintenance] menu on the [Administration] page.

For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”

Note

Before the data are imported, confirm that no jobs in progress or under waiting remain by means of the [Job Status] page. You cannot import data if there are these jobs.

If import is taking too long, try importing data after your equipment has entered sleep mode.

📖 P.24 “[Job Status] Overview”

□ Setting up Address Book

You can import address information exported from an address book on another equipment or a different address book program in the CSV or XML format.

The importing method of address book data is either adding imported data to the address book already registered in this equipment or deleting all the address book data already registered and replacing them with the imported data.

It is recommended that you export an address book in the CSV or XML format and edit it when creating address book data.

Note

You cannot import an address book when it exceeds the number of characters specified on each item. Invalid characters are replaced with “!”.

- Last Name: 32 characters
- First Name: 32 characters
- Index: 64 characters
- Email Address: 192 alphanumerical characters
- Phone Number: 128 numbers
- Tel Number 2: 128 numbers
- Company: 128 characters
- Department: 128 characters
- Keyword: 256 characters
- SUB: 20 characters
- SID: 20 characters
- SEP: 20 characters
- PWD: 20 characters


Tip

The group data are not included in the imported address book data.

	Item name	Description
1	Import Method	Specify the import method of the address book. Addition — Select this to append the imported information to the existing data. Overwrite — Select this to replace the existing data with the imported information.

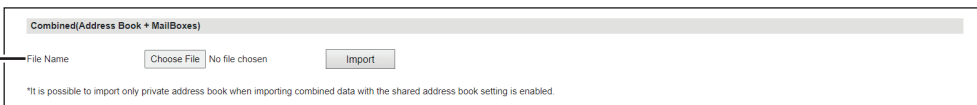
	Item name	Description
2	Address Book Type	Select “Local” or “Shared” as the import source when using the Shared Address Book function.
3	Favorite	Specify whether or not to enable Favorite information. The default is [Enable].
4	File Name	Select the address book file to be imported. [Choose File] button — Allows you to select the address book file. [Import] button — Imports the selected address book file.

❑ Setting up MailBoxes

1 The MailBoxes dialog box has a title bar 'MailBoxes'. It contains a 'File Name' label, a 'Choose File' button, the text 'No file chosen', and an 'Import' button.


	Item name	Description
1	File Name	Select the mailbox file to be imported. [Choose File] button — Allows you to select the mailbox file. [Import] button — Imports the selected mailbox file.

❑ Setting up Combined (Address Book + MailBoxes)

1 The Combined(Address Book + MailBoxes) dialog box has a title bar 'Combined(Address Book + MailBoxes)'. It contains a 'File Name' label, a 'Choose File' button, the text 'No file chosen', and an 'Import' button. Below the buttons, it says: '*It is possible to import only private address book when importing combined data with the shared address book setting is enabled.'

	Item name	Description
1	File Name	Select the combined (address book + mailboxes) file to be imported. [Choose File] button — Allows you to select the combined file. [Import] button — Imports the selected combined file.

❑ Template Data Conversion

1 The Template Data Conversion dialog box has a title bar 'Template Data Conversion'. It contains a 'File Name' label, a 'Choose File' button, the text 'No file chosen', and an 'Import' button. Below the buttons, it says: '*Convert Template data of old model and import to Home data.'

	Item name	Description
1	File Name	Import the template data file of the old models to convert it to the home data. [Choose File] button — Allows you to select the old template data file. [Import] button — Imports the selected old template data file. <div>Note> <ul style="list-style-type: none"> • Templates exceeding the registration limit cannot be converted. • Templates items protected with passwords cannot be converted. • My Menu is converted to Private Home according to the current user information: the user information should be cloned in advance. </div>

■ Export settings

You can export the address book, mailboxes and so on.

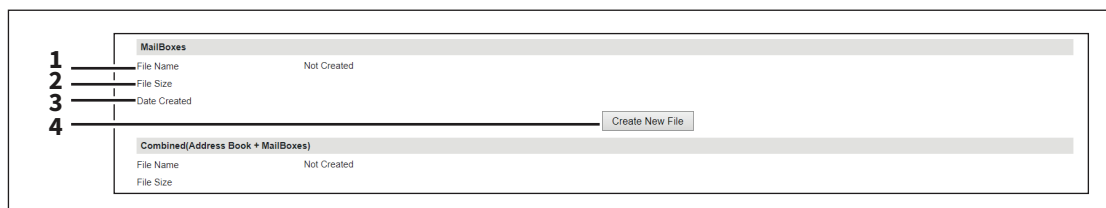
Tip

- The [Export] submenu can be accessed from the [Maintenance] menu on the [Administration] page.
For how to access it and information on the [Maintenance] menu, see the references below:
 - 📖 P.14 “Access Policy Mode”
 - 📖 P.267 “[Maintenance] Item List”
- The group data are not included in the exported address book data.

❑ Setting up Address Book

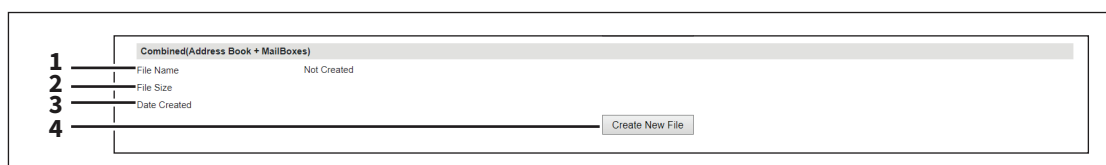
	Item name	Description
1	File Name	Displays the file name of the created export files. Click a file name to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the created date of the export files.
4	Export Data Format	Format Select the file format of the export file. <ul style="list-style-type: none"> • CSV — Select this to create the file in the CSV format. • XML — Select this to create the file in the XML format.
5	Address Book Type	Specify “Local” or “Shared” as the export source when using the Shared Address Book function.
6	Favorite	Specify whether or not to enable Favorite information. The default is [Enable].
7	[Create New File] button	Creates the export file. <div>Tip</div> If you previously exported address book data, the exported file link and information are displayed in the Address Book area. You can click the link to save the previously exported file.

❑ Setting up MailBoxes



	Item name	Description
1	File Name	Displays the file name of the created export files. Click a file name to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the created date of the export files.
4	[Create New File] button	Creates the export file. <div>Tip</div> <p>If you previously exported address book data, the exported file link and information are displayed in the Address Book area. You can click the link to save the previously exported file.</p>

❑ Setting up Combined (Address Book + MailBoxes)



	Item name	Description
1	File Name	Displays the file name of the created export files. Click a file name to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the created date of the export files.
4	[Create New File] button	Creates the export file. <div>Note</div> <p>If you previously exported address book data, the exported file link and information are displayed in the Address Book area. You can click the link to save the previously exported file.</p>

■ Panel View

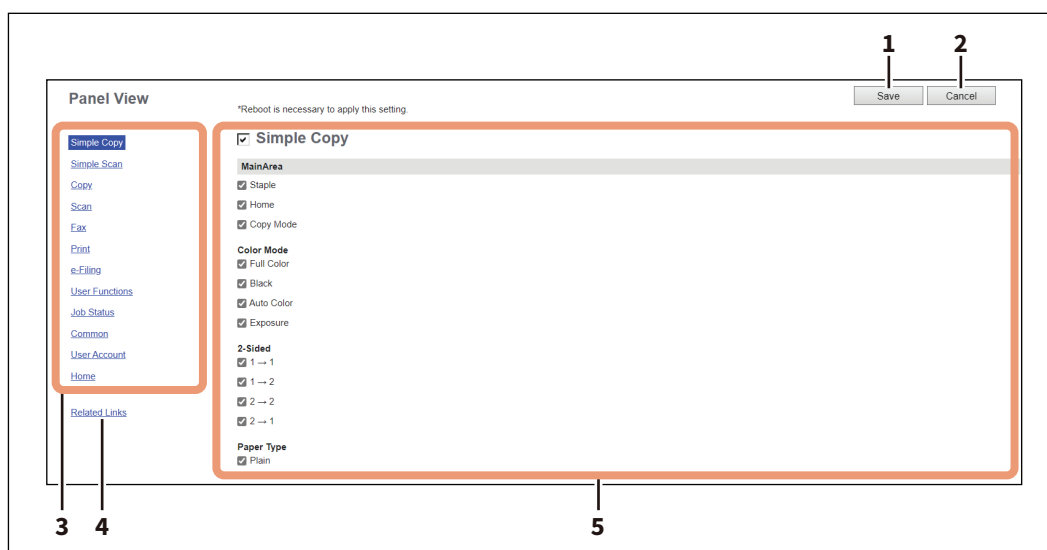
You can customize the appearance on the control panel by showing the necessary buttons and lists and hiding the forbidden buttons and lists.

Note

After you change the settings, you need to restart the equipment.

Tip

- The [Panel View] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:
 P.14 “Access Policy Mode”
 P.300 “[Registration] ([Administration]) Item List”
- Hidden functions does not appear but they are not disabled.



	Item name	Description
1	[Save] button	Saves the changed settings.
2	[Cancel] button	Cancels the changed settings.
3	Simple Copy Simple Scan Copy Scan Fax Print e-Filing User Functions Job Status Common User Account Home	Select the screen of the control panel that you want to customize.
4	Related Links	Displays the links related to the panel view.
5	Title Guidance MainArea	The target items are classified into categories. Select the check box for the item that you want to show on the selected screen of the control panel and clear the check box for the item that you want to hide.

■ Idle Screen

You can set the display of the specified contents on the control panel during idle hours.

Note

YOU SHALL ADHERE TO THE FOLLOWING POINTS WHEN USING CONTENTS DISPLAY FUNCTION ON THE STANDBY SCREEN, INCLUDING, WITHOUT LIMITATION, IMAGE CONTENTS, WEB CONTENTS, OR EXTERNAL URL CONTENTS; YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR INCORPORATING, DISPLAYING, AND TRANSMITTING ANY CONTENT, COPYRIGHTED MATERIAL, OR INFORMATION THROUGH THE USE ON THE STANDBY SCREEN.

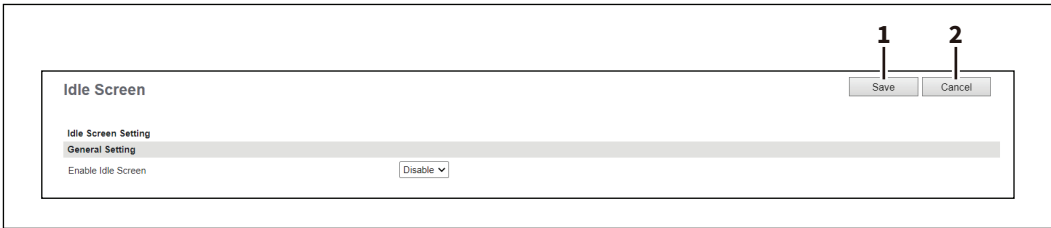
YOU FURTHER ACKNOWLEDGE AND AGREE THAT TOSHIBA TEC CORPORATION AND/OR TOSHIBA TEC AFFILIATED COMPANIES ARE NOT RESPONSIBLE TO YOU OR ANY THIRD PARTY IN CONNECTION WITH USE OF ANY CONTENTS, FOR ANY DAMAGES, LOSSES, COSTS OR EXPENSES ARISING OUT OF:

(I) INFRINGEMENT, VIOLATION, OR MISAPPROPRIATION OF ANY THIRD-PARTY RIGHT, INCLUDING ANY COPYRIGHT, TRADEMARK, PATENT, TRADE SECRET, MORAL RIGHT, OR ANY OTHER INTELLECTUAL PROPERTY OR PROPRIETARY RIGHT, PRIVACY RIGHT, RIGHT OF PUBLICITY, OR

(II) SLANDER, DEFAME, LIBEL, OR INVASION OF THE RIGHT OF PRIVACY, PUBLICITY OR OTHER PROPERTY RIGHTS OF ANY OTHER PERSON.

Tip

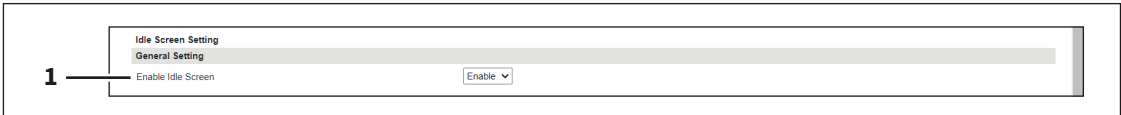
- You have to follow the security guidelines provided by government agencies and/or third-party organizations, such as OWASP, when creating web content.
- The [Panel View] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:
 - 📖 P.14 “Access Policy Mode”
 - 📖 P.300 “[Registration] ([Administration]) Item List”



	Item name	Description
1	[Save] button	Saves the [Idle Screen] settings.
2	[Cancel] button	Cancels the settings.

□ General Setting

You can turn on or off the idle screen function.



	Item name	Description
1	Enable Idle Screen	Enable or disable the idle screen function.

❑ Close Button Setting

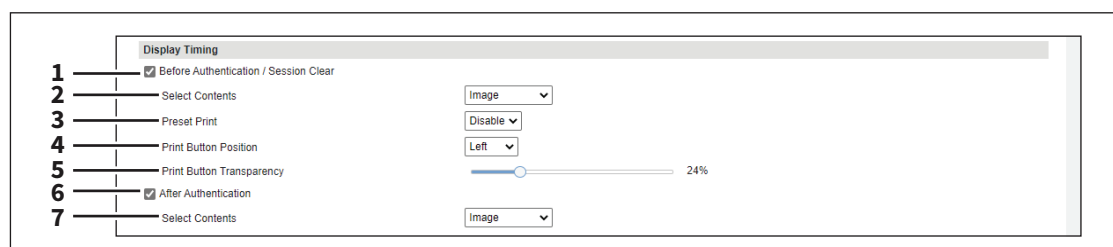
You can turn on or off the appearance of the button that closes the idle screen.



	Item name	Description
1	Display Button	Enable or disable the button to close the idle screen.
2	Transparency	Set the transparency of the button that closes the idle screen. You can set it when [Display Button] is enabled.

❑ Display Timing

You can set the display timing of the idle screen.



	Item name	Description
1	Before Authentication / Session Clear	<p>Select this check box to show the idle screen before authentication and after the session clear. Only when this setting is selected, you can set the following [Select Contents], [Preset Print], [Print Button Position], and [Print Button Transparency].</p> <ul style="list-style-type: none"> • Before Authentication — When the user authentication is enabled, the idle screen appears before user log-in, at the start-up of MFP, and at the recovery from the sleep/super sleep mode. When the user authentication is disabled, the idle screen appears at the start-up of MFP and at the recovery from the sleep/super sleep mode. • After Session Clear — After the auto clear, the idle screen appears after users press the [FUNCTION CLEAR] button twice or after they press the [ACCESS] button. <p>Tip After the session clear, the energy saver screen does not appear even if the sleep timer goes off.</p>
2	Select Contents	<p>Select the type of contents that appears as the idle screen before authentication and after clearing the session. You need to set the contents under [Contents Setting].</p> <ul style="list-style-type: none"> • Image — Shows up to ten imported images. • Web Contents — Shows the imported Web contents. • External URL — Shows the contents specified by the URL.

	Item name	Description
3	Preset Print	<p>Enable or disable the preset print function. When [Enable] is selected, users can print a PDF file on the idle screen that appears before authentication and after the session clear. You need to preset the PDF file under [Preset Print Setting].</p> <p>Note</p> <ul style="list-style-type: none"> You cannot select this setting in the following situations. <ul style="list-style-type: none"> - When the equipment is used in the High Security mode - When the print jobs are restricted - When the print data converter function is enabled - When the project management function is enabled The preset print function is not available on the idle screen that appears after the user authentication.
4	Print Button Position	Select the left, center, or right position of the print button for the preset print function.
5	Print Button Transparency	Set the transparency of the print button for the preset print function.
6	After Authentication	<p>Select this check box to show the idle screen after the authentication. If the authentication is enabled, the idle screen appears after users have logged in. Only when this setting is selected, you can set the following [Select Contents].</p> <p>Note</p> <p>You cannot select [After Authentication] when the user authentication is disabled.</p>
7	Select Contents	<p>Select the type of contents on the idle screen that appears after authentication. You need to set the contents under [Contents Setting].</p> <ul style="list-style-type: none"> Image — Shows up to ten images at regular intervals. Web Contents — Shows the imported Web contents. External URL — Shows the contents specified by the URL.

❑ Contents Setting

You can set three types of contents that can appear on the idle screen.

- **Image** — You can import and register up to ten JPEG, PNG, and GIF files. The recommended values per file are as follows: the file size is up to 1.5MB, the resolution is 1024 x 600 pixels, and the color depth is 32-bits. They are displayed as enlarged or reduced according to the touch panel size.
- **Web Contents** — You can import a ZIP file that contains HTML, CSS, JPEG, PNG, GIF, and JavaScript files. The recommended file size is up to 20MB. The display size depends on the created contents and the contents are not enlarged or reduced to the touch panel size.
- **External URL** — You can specify one URL for the contents. The display size depends on the specified URL and the contents are not enlarged or reduced to the touch panel size.

Note

Use one-byte characters for file names.

Tip

Contents of the 1,024 x 600-pixel resolution can be displayed without enlargement and reduction.

	Item name	Description
1	Import Image	<p>Import an image file to show on the idle screen.</p> <ul style="list-style-type: none"> • [Choose File] button — Click this button to select an image file. • [Import] button — Click this button to import the selected image file. The imported image file is registered in the list below. <p>Note</p> <p>You cannot register more than one file with the same file name.</p>
2	External URL	<p>Enter the external URL for the file that shows as an image content.</p> <ul style="list-style-type: none"> • [Registration] button — Click this button to register the specified image file in the list below. • [Preview] button — Click this button to show the preview of the image in another window. Click [X] to close the preview window. <p>Note</p> <ul style="list-style-type: none"> • You cannot register the same URLs many times. • If the proxy is not set correctly, the image might not show properly on the touch panel even if you see it properly in TopAccess.

	Item name	Description
3	Image File	<p>Register up to ten image files in the list. The idle screen shows the registered images in order from top to bottom at regular intervals.</p> <ul style="list-style-type: none"> • [Delete] button — Click this button to delete the image file from the list. • [Move Down] button — Select the image file in the list and click this button to move it down. • [Move Up] button — Select the image file in the list and click this button to move it up. <p>Note</p> <p>You cannot cancel the operation of the [Delete], [Move Down], and [Move Up] buttons even before you click the [Save] or [Cancel] button.</p>
4	Switch Time	<p>Specify an interval in seconds (1 to 60) for the appearance so that the idle screen shows the registered images sequentially at intervals of the specified time.</p>
5	Web Contents	<p>Import a ZIP file in which the Web contents are archived for the display on the idle screen.</p> <ul style="list-style-type: none"> • [Choose File] button — Click this button to select a ZIP file. • [Import] button — Click this button to import the selected ZIP file. • [Delete] button — Click this button to delete the imported ZIP file. <p>Note</p> <ul style="list-style-type: none"> • When you create a ZIP file for import, locate the file, which you want to display first, as “index.html” in the root directory. • If you want to change the Web contents after importing them, delete the imported contents first and then import new ones. • You cannot cancel the operation of the [Delete] button even before you click the [Save] or [Cancel] button.
6	External URL	<p>Enter one URL to show the contents on the idle screen. You can clear the URL for deletion.</p> <ul style="list-style-type: none"> • [Preview] button — Click this button to show the preview of the contents in another window. Click [X] to close the preview window. <p>Note</p> <p>If the proxy is not set correctly, the content image might not show properly on the touch panel even if you see it properly in TopAccess.</p>


❏ Preset Print Setting

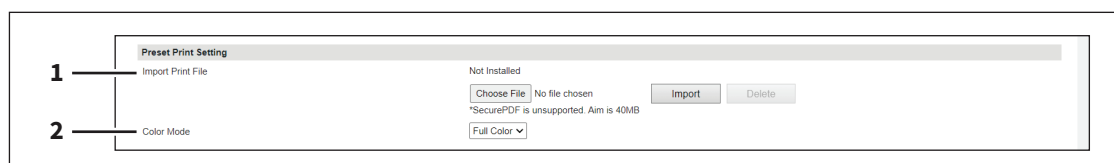
You can preset a PDF file that users can print on the idle screen. The recommended file size is up to 40MB.

Note

- Do not preset encrypted PDF files because they cannot be printed.
- When the EWB scan or print job is executed while the idle screen appears, the job execution screen appears over the idle screen.
- Preset print cannot be done if there are print jobs other than scheduled print jobs and print jobs waiting for user operation.

Tip

- Preset print is done in the color mode you have set on the equipment.
- Preset print is done with the paper size you have set for the PDF file.
- The print settings other than the color mode and the paper size depend on the default raw job settings.
 P.208 “Setting up Default Raw Job Setting”




	Item name	Description
1	Import Print File	<p>Import a PDF file as the preset file that users can print on the idle screen.</p> <ul style="list-style-type: none"> • [Choose File] button — Click this button to select a PDF file. • [Import] button — Click this button to import the selected PDF file. • [Delete] button — Click this button to delete the imported PDF file. <p>Note You cannot cancel the operation of the [Delete] button even before you click the [Save] or [Cancel] button.</p>
2	Color Mode	Select the color mode [Full Color] or [Black] for the preset print function.


❏ Proxy Setting

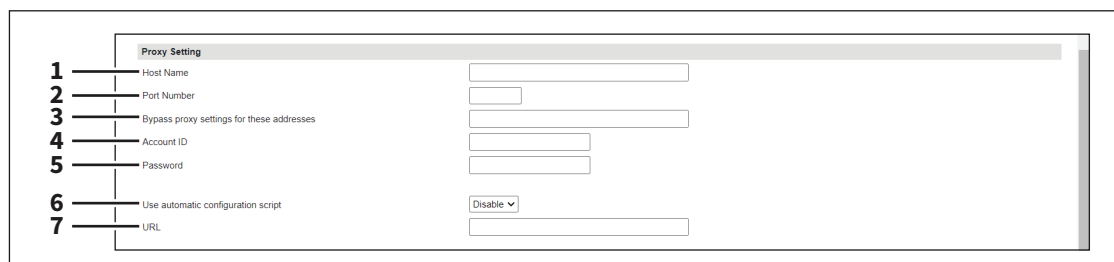
You can set up the proxy for the idle screen function.

Tip

The proxy settings are basically common to the Embedded Web Browser, Idle Screen, and Application functions. If you change them for one function, they change accordingly for others.

 P.233 “Setting up Proxy Setting”

 P.364 “Proxy Setting”



	Item name	Description
1	Host Name	Specify a host name of the proxy server.

	Item name	Description
2	Port Number	Specify a port number of the proxy server.
3	Bypass proxy settings for these addresses	Specify URLs that do not use the proxy server. When you specify more than one URL, delimit each with a semicolon (;).
4	Account ID	Enter the account ID of the proxy server.
5	Password	Enter the password of the proxy server.
6	Use automatic configuration script	Enable or disable the automatic configuration script for the proxy server.
7	URL	<p>Specify a URL for the PAC file when the automatic configuration script is enabled.</p> <p>Note</p> <p>Note the following points for the PAC file.</p> <ul style="list-style-type: none"> • Be sure to enter the protocol without omission. • Do not use functions.

■ Delete Files settings

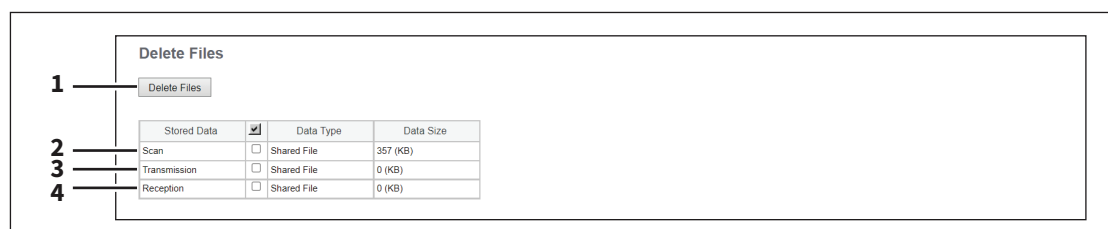
You can delete information such as scanned data, transmission data, and reception data that are stored in the local folder using the Save as file function. It is recommended to delete the stored data periodically to maintain the internal storage device.

Tip

The [Delete Files] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”



	Item name	Description
1	[Delete Files] button	Click this to delete the selected data files.
2	Scan	Deletes all scan data stored in the shared folder.
3	Transmission	Deletes all fax/ifax transmission data stored in the shared folder.
4	Reception	Deletes all fax/ifax reception data and mailbox/fax/ifax forwarding data in the shared folder.

■ Notification settings

An administrator can configure notification to receive E-mail (mobile terminal can also be used) notifications when an error occurred or a job is complete.

Note

To enable the E-mail notification, the E-mail settings in the [Setup] menu page must be configured correctly.

📖 P.192 “Email settings”

Tip

The [Notification] submenu can be accessed from the [Maintenance] menu on the [Administration] page.

For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”

	Item name	Description
1	[Save] button	Stores settings for transmitting the report to the registered E-mail address.
2	[Cancel] button	Cancels the changed settings.

□ Setting up Email Setting

	Item name	Description
1	Notify administrator at Email Address 1	Register E-mail addresses for administrators who receive the notification. The notification is sent to the selected administrators by E-mail.
2	Notify administrator at Email Address 2	
3	Notify administrator at Email Address 3	

❑ Setting up System Message Notification Events

System Message Notification Events

- Device**
 - ☐ Paper Misfeed
 - ☐ Drawer Out of Paper
 - ☐ Door/Drawer Open
 - ☐ Print Needs Attention
 - ☐ Toner Empty
 - ☐ Waste Toner Box is Full
 - ☐ Power Status
 - ☐ H/W Option Attachment History
- Maintenance**
 - ☐ Change Settings
 - ☐ Maintenance User Data
 - ☐ Export/Import
 - ☐ Cloning
 - ☐ System Updates
 - ☐ Log Full
 - ☐ Storage Device Alert/Data Backup
- Network**
 - ☐ Error
- Security**
 - ☐ Error
 - ☐ Warning
 - ☐ Information
- Received Fax/InternetFax**
 - ☐ Error
 - ☐ Warning
 - ☐ Information
- Scan**
 - ☐ Warning
 - ☐ Information
- e-Filing**
 - ☐ Warning
 - ☐ Information

You can select the events to be notified of.

	Item name	Description
1	Device	Paper Misfeed — Select this to be notified of paper misfeeds. Drawer Out of Paper — Select this to be notified when you are out of paper. Door/Drawer Open — Select this to be notified when a cover or drawer is open. Print Needs Attention — Select this to be notified when a job is printed. Toner Empty — Select this to be notified when a toner is empty. Waste Toner Box is Full — Select this to be notified when the waste toner box is full. Power Status — Select this to be notified when the power source status changes such as a power cut. H/W Option Attachment History — Select this to be notified when a hardware option is installed.
2	Maintenance	Change Settings — Select this to be notified of setting changes. Maintenance User Data — Select this to be notified when user information is edited. Export/Import — Select this to be notified of an export or import. Cloning — Select this to be notified when a clone is made. System Updates — Select this to be notified of system updates. Log Full — Select this to be notified when the log has reached the maximum size. Storage Device Alert/Data Backup — Select this to be notified when the backup or replacement of the internal storage device of this equipment is required due to its abnormality.
3	Network	Error — Select this to be notified of network errors.
4	Security	Error — Select this to be notified of security errors. Warning — Select this to be notified of security warnings. Information — Select this to be notified of security information.
5	Received Fax/InternetFax	Error — Select this to be notified of fax/Internet Fax reception errors. Warning — Select this to be notified of fax/Internet Fax reception warnings. Information — Select this to be notified of fax/Internet Fax reception information.

	Item name	Description
6	Scan	<p>Warning — Select this to be notified of the periodical deletion of scanned files or fax/Internet Fax transmission and reception data is successfully completed.</p> <p>Information — Select this to be notified of the deletion of scanned files or fax/Internet Fax transmission and reception data by the [Delete Files] function under the [Maintenance] menu is successfully completed.</p>
7	e-Filing	<p>Warning — Select this to be notified when the available space in the e-Filing box is low or the preservation period of documents in the e-Filing box is expiring soon.</p> <p>Information — Select this to be notified when the e-Filing box is initialized.</p> <p>Tip</p> <p>Use the e-Filing box web utility and specify in the property screen for each box if you want to notify whether e-Filing box operations are successfully completed. For information on how to set, see the reference below:</p> <p>e-Filing - OPERATING WITH A CLIENT COMPUTER - Managing User Boxes and Folders - Modifying and displaying user box and folder properties - Modifying box properties</p>

□ Setting up Job Notification Events

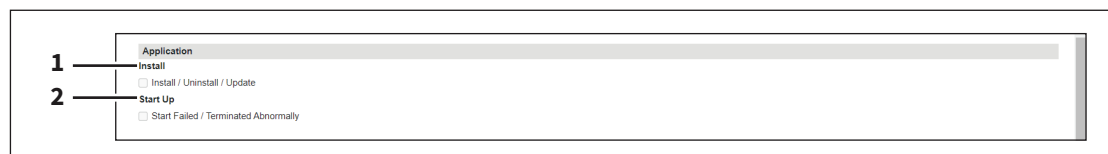
The screenshot shows a configuration window titled "Job Notification Events". It contains a list of five job types, each with two checkboxes: "Send Email when an error occurs" and "Send Email when job is completed". The jobs are numbered 1 through 5 on the left side of the window.

- 1. Scan
 - ☐ Send Email when an error occurs
 - ☐ Send Email when job is completed
- 2. Received Fax/InternetFax
 - ☐ Send Email when an error occurs
 - ☐ Send Email when job is completed
- 3. Fax Received Forward
 - ☐ Send Email when an error occurs
 - ☐ Send Email when job is completed
- 4. InternetFAX Received Forward
 - ☐ Send Email when an error occurs
 - ☐ Send Email when job is completed
- 5. Received Forward for Application
 - ☐ Send Email when an error occurs
 - ☐ Send Email when job is completed

You can select jobs to be notified.

	Item name	Description
1	Scan	<p>Send Email when an error occurs</p> <p>Send Email when job is completed</p>
2	Received Fax/InternetFax	<p>Send Email when an error occurs</p> <p>Send Email when job is completed</p>
3	Fax Received Forward	<p>Send Email when an error occurs</p> <p>Send Email when job is completed</p>
4	InternetFAX Received Forward	<p>Send Email when an error occurs</p> <p>Send Email when job is completed</p>
5	Received Forward for Application	<p>Send Email when an error occurs</p> <p>Send Email when job is completed</p>

❑ Setting up Application

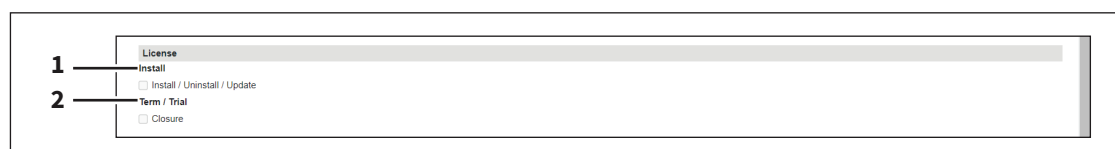


You can select jobs to be notified.

	Item name	Description
1	Install	Notifies when the added application has been installed, uninstalled, or updated.
2	Start Up	Notifies when the application has failed to start or has been terminated abnormally.

❑ Setting up License

You can select jobs to be notified.



	Item name	Description
1	Install	Notifies when the added license has been installed, uninstalled, or updated.
2	Term / Trial	Notifies when the trial term has been terminated.

■ Languages settings

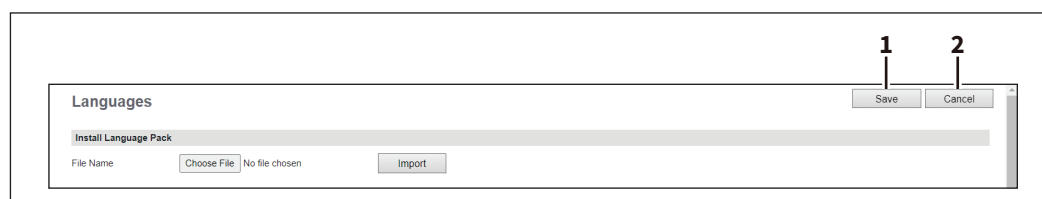
You can specify the language for the touch panel of your equipment.

Tip

The [Languages] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”

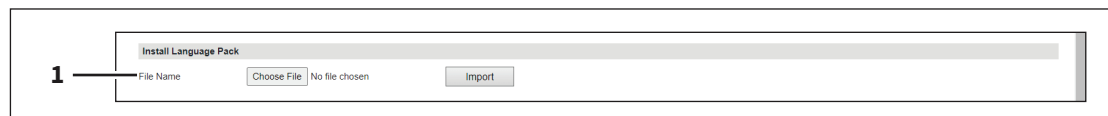


	Item name	Description
1	[Save] button	Saves the registered language.
2	[Cancel] button	Cancels the changed settings and operation.

❑ Setting up Install Language Pack

You can install additional language packs.

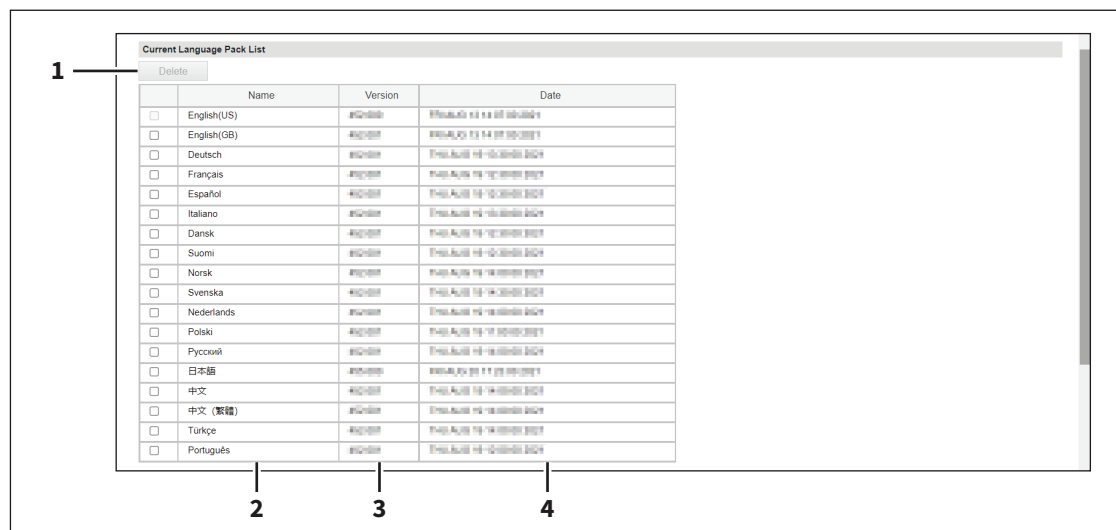
📖 P.291 “Setting up Current Language Pack List”



	Item name	Description
1	File Name	Select the language pack file to be installed. [Choose File] button — Allows you to select the language pack file. [Import] button — Imports the selected language pack file.

❑ Setting up Current Language Pack List

Displays a list of installed language packs. You can delete unnecessary language packs.



	Item name	Description
1	[Delete] button	Select unnecessary language packs and click the [Delete] button to delete them.
	<div>Tip</div> You cannot delete [English(US)] or the language selected in [PanelUI Language].	
2	Name	Displays the name of the language pack.
3	Version	Displays the version of the language pack.
4	Date	Displays the installed date of the language pack.

❑ Setting up Default Setting for PanelUI

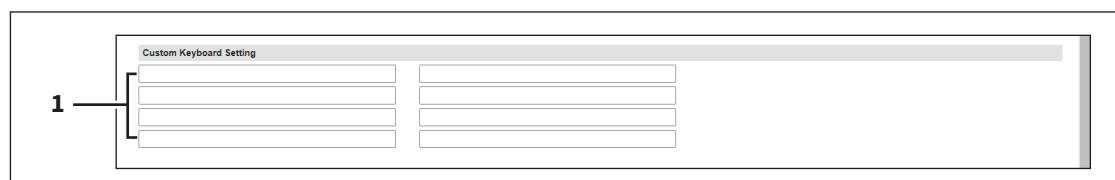
Select the display language for the touch panel.



	Item name	Description
1	PanelUI Language	Select the display language for the touch panel.
2	PanelUI Keyboard Display	Select whether to display the soft-keyboard when entering characters with the touch panel.
3	PanelUI Keyboard Layout	Select the panel keyboard layout displayed on the touch panel.

❑ Custom Keyboard Setting

When you use the English keyboard or you enter an E-mail address on the control panel, you can select [CUSTOM] to enter a specific string of characters easily. You can register up to eight patterns of strings as the custom keyboard.



	Item name	Description
1	(Registration areas)	<p>Register up to eight patterns of strings with up to 64 alphanumeric characters and symbols. The control panel shows them in the same order as the registration.</p> <div>Note</div> <p>The number of characters and the prohibited characters for entry vary from area to area on the control panel.</p> <ul style="list-style-type: none">• If you register too many characters for entry, the control panel does not show the exceeding characters and users cannot enter them.• If you register prohibited characters, users cannot select the patterns including them on the control panel.

Remote Command

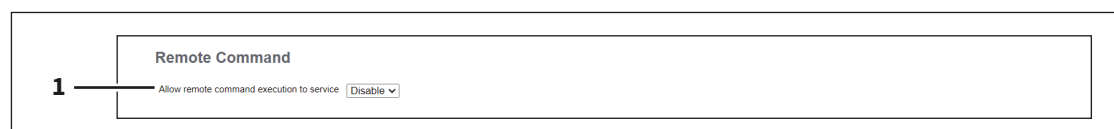
The remote command is used to maintain your equipment from a distance. It can get information about the settings and status of your equipment and change the settings. You can set how to execute the remote command and check the log of the execution.

Tip

The [Languages] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”



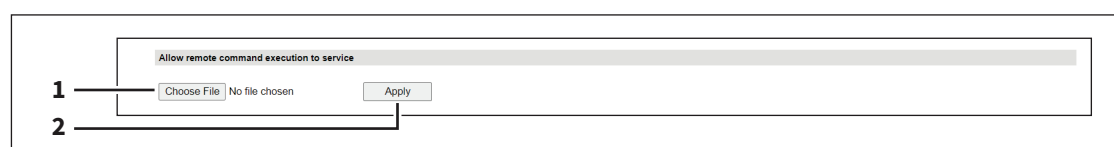
	Item name	Description
1	Allow remote command execution to service	Select whether to allow your service technician to do the remote maintenance. <ul style="list-style-type: none">• Enable — Allows your service technician to execute the remote command from a remote place.• Disable — Prohibits your service technician from executing the remote command from a remote place.

Apply Remote Command File

If the remote maintenance is not allowed, get the remote command file. You can execute the remote command from TopAccess.

Tip

For the remote command file, contact your service representative.



	Item name	Description
1	[Choose File] button	Select the obtained remote command file.
2	[Apply] button	Execute the selected remote command file and apply it to your equipment. After application, the screen shows the file name, the schema version, and the day of execution. <ul style="list-style-type: none">• If the execution has succeeded, the link appears for you to download the result file. Click the link to download the file. Click [OK] to make the message disappear.• If the settings of the equipment have been changed, the message appears and prompts you to reboot the equipment. Click [OK] to reboot it.• If the execution has failed, the message with the error code appears. Write it down and consult your service technician.

❑ Remote Command Execution History

You can check the log of the executed remote command up to three times.

Remote Command Execution History						
	Date	Command Type	Result	User	Schema version	Remote Command File
1	2023-09-20 10:10:10	Get Setting	Success	Admin	0.0.4	2023-09-20 10:10:10
2	2023-09-20 10:10:10	Set Setting	Success	Admin	0.0.4	2023-09-20 10:10:10
3	2023-09-20 10:10:10	Set Setting	Success	Admin	0.0.4	2023-09-20 10:10:10

1

2

3

4

5

6

7

	Item name	Description
1	Date	Shows the execution day and time of the remote command file.
2	Command Type	Shows the type of the remote command. <ul style="list-style-type: none">• Get Setting — Shows that the remote command has been executed to get information about the settings of the equipment.• Set Setting — Shows that the remote command has been executed to set the equipment.
3	Result	Shows the execution result of the remote command file. <ul style="list-style-type: none">• Success — Shows that the execution has succeeded.• Failed (error code) — Shows that an error has occurred. You can check the error code to tell your service technician.
4	User	Shows the executor of the remote command. <ul style="list-style-type: none">• Service — Shows that the service technician has executed the remote command from a remote place or on the control pane of the equipment.• Admin — Shows that the administrator has executed the remote command from TopAccess.
5	Schema version	Shows the schema version of the remote command file.
6	Remote Command File	Shows the name of the executed remote command file. You can click it to download the file.
7	Remote Command Execution History	Shows the name of the file that records the result of the executed remote command. You can click it to download the file.

■ Data Backup

You can back up the data of the internal storage device embedded in your equipment.

Tip

The [Data backup] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

P.14 “Access Policy Mode”

 P.267 “[Maintenance] Item List”

❏ Data Backup

Data Backup

Save Cancel

Data Backup

Data Backup : Enable

☐ Use External Server for Data Backup

Protocol ☒ SMB ☐ FTP ☐ FTPS ☐ Cloud

Server Name

Port Number(Command) 0

Network Path

Login User Name

Password Retype Password

Connection Test Execute

Schedule of Automatic Data Backup Disable

Day of Week Sun

Time 00 : 00

Target of Data Backup

☒ MFPP Setting

☒ User Management (User, Group, Role, Quota, Department Code, Address Book, Project Code, Home Setting)

☐ MailBox

☒ Application (Including License)

☐ e-Filing

	Item name	Description
1	[Save] button	Saves the settings for the data backup function.
2	[Cancel] button	Cancels the changed settings.
3	Data Backup	Select whether the Data backup function is enabled or disabled. [Enable] is set as the default.

	Item name	Description
4	Use External Server for Data Backup	<p>Select this check box to store backed-up data of the internal storage device in an external server.</p> <p>Enter the following items to configure the external server to store the backed-up data of the internal storage device.</p> <p>Protocol</p> <p>Select the protocol to be used for storing the backed-up data of the internal storage device in an external server.</p> <ul style="list-style-type: none"> • SMB — Select this to send the backed-up data of the internal storage device in an external server using the SMB protocol. • FTP — Select this to send the backed up data of the internal storage device in an FTP server. • FTPS — Select this to send the backed-up data of the internal storage device to an FTP server using FTP over SSL/TLS. • Cloud — Select this to send the backup data of the internal storage device to the cloud. <p>Server Name</p> <p>When you select [FTP] as the protocol, enter an FTP server name or an IP address.</p> <p>You can enter up to 64 alphanumeric characters and symbols.</p> <p>Port Number(Command)</p> <p>When you select [FTP] as the protocol, enter the port number to be used for the controls. Generally, “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number. You can enter a value in the range within from 0 to 65535 using numbers and hyphens (-). “-” is set as the default.</p> <p>Network Path</p> <p>When you select [SMB] as the protocol, enter the network path to the network folder.</p> <p>When you select [FTP] as the protocol, enter the directory in the specified FTP server.</p> <p>You can enter up to 128 alphanumeric characters and symbols.</p> <p>Login User Name</p> <p>Enter the log-in user name to access an SMB server or an FTP server, if required. When you select [FTP] as the protocol, an anonymous log-in is assumed if you leave this box blank. Enter the login user name to access an SMB server, an FTP server, or a NetWare server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank. You can enter up to 32 alphanumeric characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.</p> <p>You can enter up to 32 alphanumeric characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.</p> <p>Password</p> <p>Enter the password to access an SMB server or an FTP server, if required. You can enter up to 32 alphanumeric characters, symbols and spaces. A single space only can also be entered.</p> <p>Retype Password</p> <p>Enter the same password again for a confirmation.</p> <p>Connection Test</p> <p>By clicking [Execute], a connection test is performed by using the specified network settings to check if the communications can be established.</p>

	Item name	Description
	Use External Server for Data Backup (Continued)	Schedule of Automatic Data Backup Set the period of automatic backup. You can select the period from Disable, Weekly, Every 2 weeks and Monthly. <ul style="list-style-type: none"> • Day of Week: Select this to specify the day of week. • Time: Select this to specify the time. (24-hour display)
5	Target of Data Backup	Select the data to be backed up.

■ User Paper Type

You can set user paper types.

Note

After you set user paper types, you need to restart the equipment.

Tip

- The [User Paper Type] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:
 - 📖 P.14 “Access Policy Mode”
 - 📖 P.267 “[Maintenance] Item List”
- For details on the registration of user paper types, consult your service representative.

□ User Paper Type

User Paper Type

* Reboot is necessary to apply the imported file.

User Paper Type

Import File

1 File Name Choose File No file chosen Import

User Paper Type List

2 Delete Export

3

No	Name	File Name	Base Type	Status
01	UserType1		Plain	Not Available
02	UserType2		Plain	Not Available
03	UserType3		Plain	Not Available
04	UserType4		Plain	Not Available
05	UserType5		Plain	Not Available
06	UserType6		Plain	Not Available
07	UserType7		Plain	Not Available
08	UserType8		Plain	Not Available
09	UserType9		Plain	Not Available
10	UserType10		Plain	Not Available

4 5 6 7 8

	Item name	Description
1	File Name	Select a file to install a user paper type. <ul style="list-style-type: none"> • [Choose File] button — Select a file for the user paper type. • [Import] button — Click this button after you select a user type name in [User Paper Type List], so that the selected user paper type file is imported at the selected user type name.
2	[Delete] button	Click this button to delete the user paper type selected in [User Paper Type List].

	Item name	Description
3	[Export] button	Click this button to export the user paper type selected in [User Paper Type List]. Tip You can export the user paper types that have been imported with the [Import] button.
4	No	Indicates the number for the user paper type. You can import up to 10 files for user paper types.
5	Name	Shows the name of the user paper type. Click this to change the name.
6	File Name	Shows the file name for the user paper type.
7	Base Type	Shows the base paper type for the user paper type.
8	Status	Shows the status of the user paper type.

■ System Updates settings

You can update the system on your equipment.

You can also update the fax system when the FAX Unit is installed.

Note

If a message appears to tell the data is invalid, download the updating file again.

Tip

The [System Updates] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”

❑ Setting up Install Software Package

	Item name	Description
1	File Name	Select the software pack file to be installed. [Choose File] button — Allows you to select the software pack file. [Install] button — Installs the selected software pack file.

❑ Setting up Current Software List

The screen displays information about the installed firmware, depending on the model. Click [REFRESH] to update the information.

Current Software List			
Name	Version	Date Created	Date Installed
SYSTEM FIRMWARE	Firmware Ver. 1.0	2017-06-16	2017-06-16
SYSTEM SOFTWARE	Firmware Ver. 1.0		2017-06-16
SD SPECIFIC PACKAGE	Firmware Ver. 1.0		2017-06-16
SD PRODUCTION PACKAGE	Firmware Ver. 1.0		2017-06-16
ENGINE FIRMWARE	Firmware Ver. 1.0		2017-06-16
SCANNER FIRMWARE	Firmware Ver. 1.0		2017-06-16
RADF/DSDF FIRMWARE	Firmware Ver. 1.0		2017-06-16
PFC FIRMWARE	Firmware Ver. 1.0		2017-06-16
NIC FIRMWARE	Firmware Ver. 1.0		2017-06-16
FAX1 FIRMWARE	Firmware Ver. 1.0		2017-06-16
FAX2 FIRMWARE	Firmware Ver. 1.0		2017-06-16
PUNCH FIRMWARE	Firmware Ver. 1.0		2017-06-16
FINISHER FIRMWARE	Firmware Ver. 1.0		2017-06-16

1 2 3 4

	Item name	Description
1	Name	Displays the name of the System Firmware.
2	Version	Displays the version of the System Firmware.
3	Date Created	Displays the Created date of the System Firmware.
4	Date Installed	Displays the installed date of the System Firmware.

❑ Install Card Reader Firmware

Contact your service technician for details.

■ Reboot settings

You can reboot your equipment by clicking the [Reboot] button. If rebooting is performed, warming-up may take longer than normally.

Note

While the equipment is being restarted, the network will not be available. A message is displayed to inform you that it will reconnect to TopAccess after a while. Also, the touch panel on this equipment displays a message to inform you that the network is not ready. When this message disappears, TopAccess will once again be available.

Tip

The [Reboot] submenu can be accessed from the [Maintenance] menu on the [Administration] page. For how to access it and information on the [Maintenance] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.267 “[Maintenance] Item List”

[Registration] ([Administration]) Item List

Tip

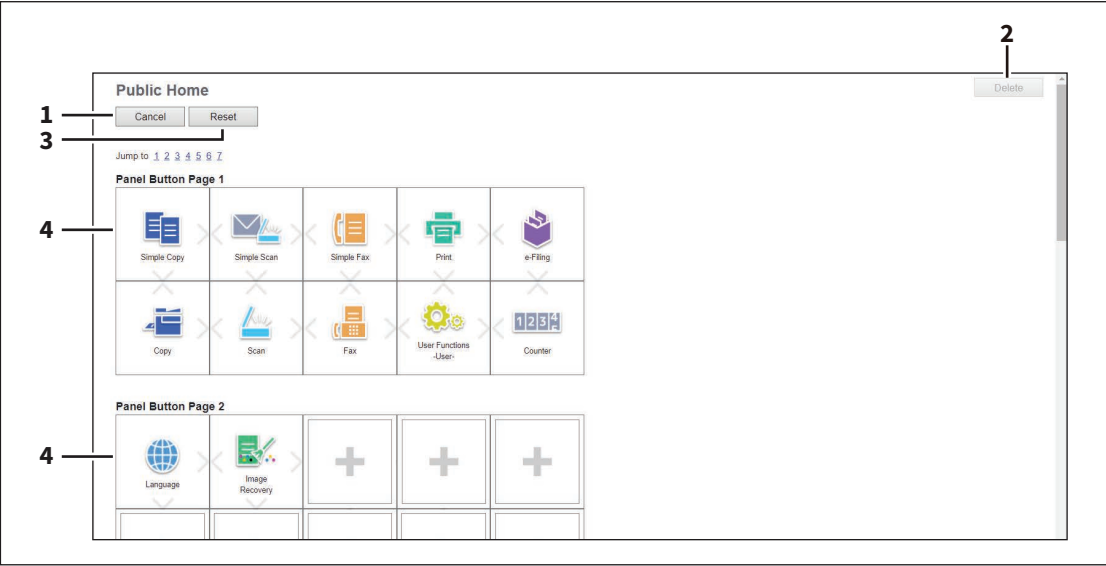
Users who are granted administrator privileges in access policy mode can access the [Registration] menu from the [Administration] page.
For how to access it, see the reference below:
P.14 “Access Policy Mode”

Public Home

In Public Home, you can set the Home screen that is displayed when you press the [Home] button.
You can register the functions used frequently as panel buttons.

Tip

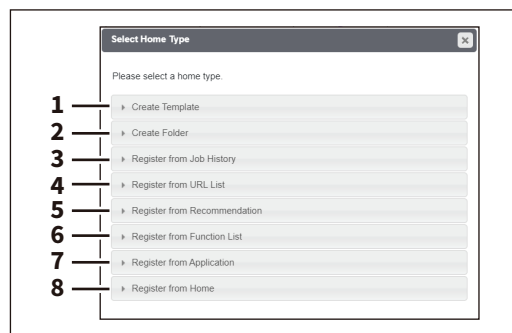
- General users can set [Public Home] under [Registration] only if they are allowed at [Home Setting].
P.113 “Home Setting”
- The administrator can set [Public Home] only under [Administration].
P.14 “Access Policy Mode”
P.300 “[Registration] ([Administration]) Item List”



	Item name	Description
1	[Cancel] button	Cancels the operation.
2	[Delete] button	Deletes the selected Panel Button. When you delete a folder, the confirmation message appears and all buttons inside the folder are deleted.
3	[Reset] button	Deletes the current settings.
4	Panel button list	<p>Displays a list of panel buttons you can select for the shared home. You can drag and drop the icon with your mouse or click the arrows to change the button position.</p> <p>Select the panel buttons you want to use.</p> <p>Click the link to edit the home type. When you open the [Edit Settings] screen, you can change the button icon and names, and delete or move the button: you cannot move the folder button. When you move your mouse pointer over an icon, the check box appears at the upper left. Select this check box to delete the selected button.</p> <p>Click the [+] icon that represents an empty position to register the button.</p> <p>P.301 “[Select Home Type] screen”</p> <div>Tip</div> <p>In Public Home, you can register 64 types.</p>

❑ [Select Home Type] screen

Select a home type to add to Public Home.

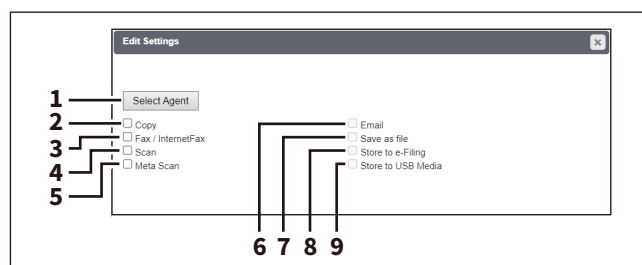


	Item name	Description
1	Create Template	Registers a template button. 📖 P.301 “[Edit Settings] screen for templates”
2	Create Folder	Registers a folder button. You can register up to 64 folders. 📖 P.302 “[Edit Settings] screen for folders”
3	Register from Job History	Registers a panel button from the job history. 📖 P.303 “[Register from Job History] screen”
4	Register from URL List	Registers a panel button from the URL list. 📖 P.304 “[Register from URL List] screen”
5	Register from Recommendation	Registers a panel button from the recommendation list. 📖 P.304 “[Register from Recommendation] screen”
6	Register from Function List	Registers a panel button from the function list. 📖 P.304 “[Register from Function List] screen”
7	Register from Application	Registers a panel button from the application. 📖 P.305 “[Register from Application] screen”
8	Register from Home	Registers a panel button from the home screen. 📖 P.305 “[Register from Home] screen”

[Edit Settings] screen for templates

You can set the template you are registering.

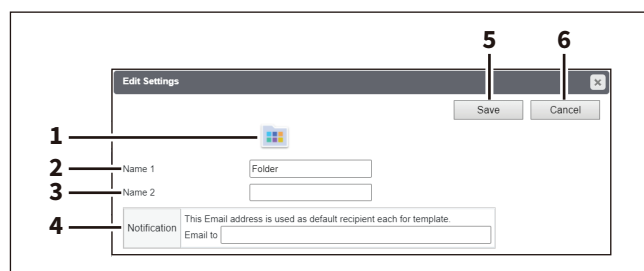
When you select agents, the setting status of the selected agents and the button to open the edit screen appear at the bottom of the screen.



	Item name	Description
1	[Select Agent] button	Allows you to set the selected agent. You can set the template details when creating a new agent. 📖 P.306 “Template settings”

	Item name	Description
2	Copy	You can create a template which copies the document. Select this agent if you want to print a copy when you are sending a document to another destination. You can also specify the [Save as file] agent or [Store to e-Filing] agent at the same time.
3	Fax / InternetFax	You can create a template for fax or Internet Fax transmission. You can also specify the [Save as file] agent at the same time.
4	Scan	You can create a template for a scan. You need to select either the [Email] agent, [Save as file] agent, [Store to e-Filing] agent, or [Save to USB Media] agent at the same time. You can specify up to two agents for a scan template.
5	Meta Scan	This agent is enabled when the meta scan option is installed. You can create a template for the meta scan option. Refer to the document provided by the vendor of the application which supports meta scan option for details.
6	Email	You can transmit the document as an E-mail attachment.
7	Save as file	You can save the document in a shared folder.
8	Store to e-Filing	You can store the document in the e-Filing.
9	Save to USB Media	You can save the document in USB media.

[Edit Settings] screen for folders

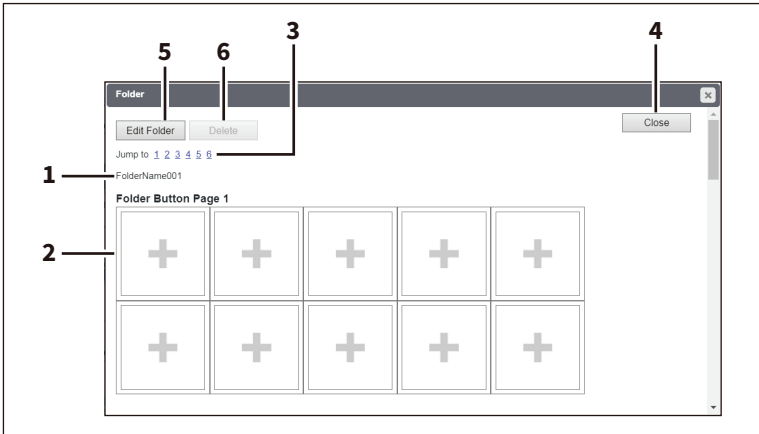


Note

You cannot change the position of the registered folder.

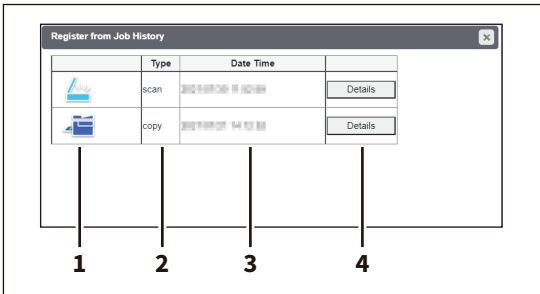
	Item name	Description
1	Icon	This folder icon appears on the touch panel. You cannot change this icon.
2	Name 1	Enter a name 1 (upper position) for the folder icon that appears on the touch panel. You can enter up to 20 characters including the following: " * + , / ; < = > ? [\]
3	Name 2	Enter a name 2 (lower position) for the folder icon that appears on the touch panel. You can enter up to 20 characters including the following: " * + , / ; < = > ? [\]
4	Notification	Enter a recipient E-mail address for the notification message. You can either select an option to send it to the E-mail address set in a private group or specify an E-mail address.
5	[Save] button	Saves the changed settings.
6	[Cancel] button	Cancels the operation.

You can register buttons in a folder.



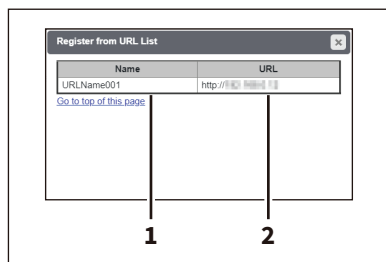
	Item name	Description
1	Folder name	Shows [Name 1] of the registered folder.
2	Folder Button Page	You can register up to 60 buttons in a folder.
3	Jump to	Click a number to jump directly to the registration page.
4	[Close] button	Closes the edit screen.
5	[Edit Folder] button	Opens the [Edit Settings] screen so that you can change [Name 1], [Name 2], and [Notification]. You can delete the folder itself.
6	[Delete] button	Deletes the registered template.

[Register from Job History] screen



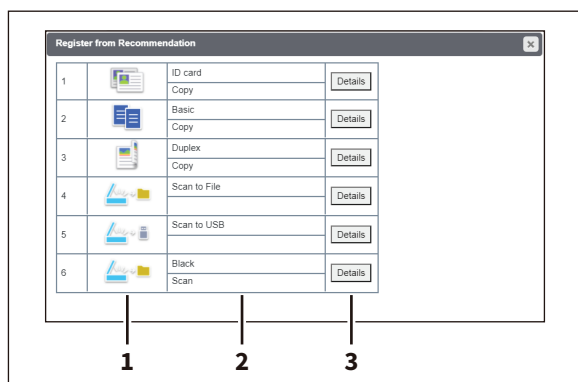
	Item name	Description
1	Button Icon	Displays the button icon.
2	Type	Displays the job type.
3	Date Time	Displays the date and time that a job was performed.
4	[Details] button	Displays the job details.

[Register from URL List] screen



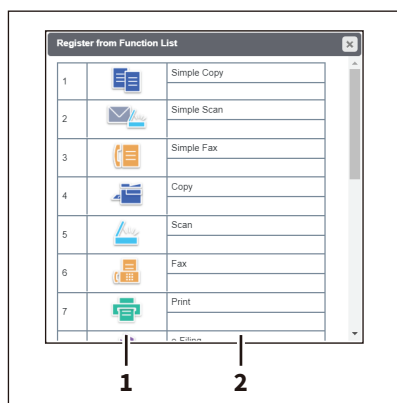
	Item name	Description
1	Name	Displays the name of the connection.
2	URL	Displays the URL.

[Register from Recommendation] screen



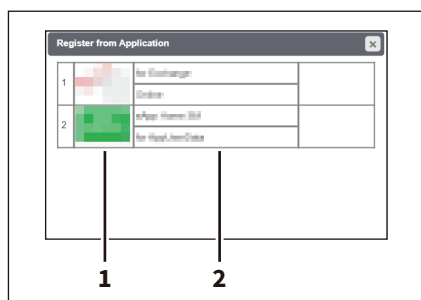
	Item name	Description
1	Button Icon	Displays the button icon.
2	Name	Displays the name of the function.
3	[Details] button	Displays the details for the function.

[Register from Function List] screen



	Item name	Description
1	Button Icon	Displays the button icon.
2	Name	Displays the name of the function.

[Register from Application] screen



	Item name	Description
1	Button Icon	Displays the button icon.
2	Name	Displays the name of the function.

Tip

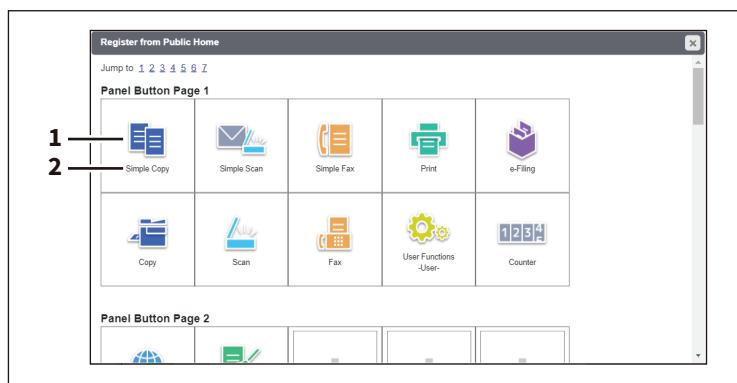
Some applications have the button templates and show the [Details] button on the [Register from Application] screen. When you click this button, you can select one of the buttons for which the button names and icon information are registered as templates. The selected button template appears on the [Edit Settings] screen.

[Register from Home] screen

You can register from the Public Home or the User Home screen. The content displayed is the same for both.

Tip

When you register buttons from Home, you can select and copy the buttons inside folders, but you cannot copy folders themselves.



	Item name	Description
1	Button Icon	Displays the button icon.
2	Name	Displays the name of the function.

■ Template settings

You can set the following functions according to the agents that you have selected on the [Edit Settings] screen for templates.


📖 P.301 “[Edit Settings] screen for templates”

Specify how the icon for the template is displayed in the touch panel, and the notification settings for the template.

Tip

You can open the [Edit Settings] screen of the registered template to change the settings but you cannot change the agents.

	Item name	Description
1	Choose icon from the Gallery	This indicates the icon that will be displayed in the touch panel. The icon is automatically designated according to the agent that you select. You can click the icon to choose it from the gallery.
2	Name 1	Enter a name 1 (upper position) for the icon that appears on the touch panel. You can enter up to 20 characters including the following: " * + , / : ; < = > ? [\]
3	Name 2	Enter a name 2 (lower position) for the icon that appears on the touch panel. You can enter up to 20 characters including the following: " * + , / : ; < = > ? [\]
4	Automatic Start	Select whether the automatic start function is enabled or disabled. When this check box is selected, pressing the template button registered on the Home screen of the touch panel starts the operation automatically without pressing the [START] button or [Scan]. Note If the user names or passwords of the User Authentication for Scan to E-mail and the User Management Setting are different, or only the User Authentication for Scan to E-mail is enabled, you need to enter the user name and password of the User Authentication for Scan to E-mail also when recalling the template with the automatic start function enabled.
5	Notification — Send Email when an error occurs	Select this to send a notification message to the specified E-mail address when an error occurs.
6	Notification — Send Email when job is completed	Select this to send a notification message to the specified E-mail address when a job is completed.

	Item name	Description
7	Notification — Email to	<p>Enter a recipient E-mail address for the notification message. You can either select an option to send it to the E-mail address set in a private group or specify an E-mail address.</p> <p>Note</p> <p>When you enable the Notification setting, make sure to set up the E-mail settings in the [Email] submenu of the [Setup] menu in the TopAccess access policy mode.</p> <p> P.192 “Email settings”</p>
8	[Save] button	Saves the settings.
9	[Cancel] button	Cancels the operation.


❑ Destination Setting

In the Recipient List page, you can specify the destinations to which the Fax, Internet Fax, or Scan to E-mail document will be sent.

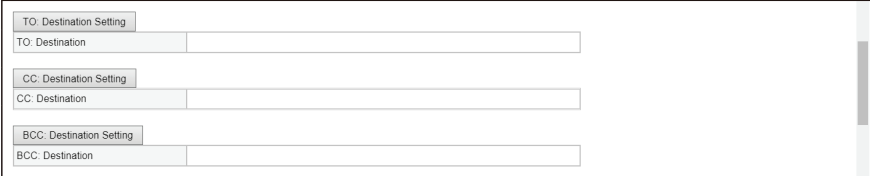
When you are setting up the destinations for the Scan to Email agent, you can only specify the E-mail addresses for the destinations.

When you are setting up the destinations for the Fax/InternetFax agent, you can specify both fax numbers and E-mail addresses for the destinations.

When Creating a Fax/Internet Fax agent:



When Creating an Email agent:



You can specify the destinations by entering their E-mail addresses or fax numbers manually, selecting destinations from the address book, selecting destination groups from the address book, or searching for destinations in the LDAP server.

Note

The Fax Unit must be installed in this equipment to specify the fax numbers of the destinations.

Entering the destinations manually

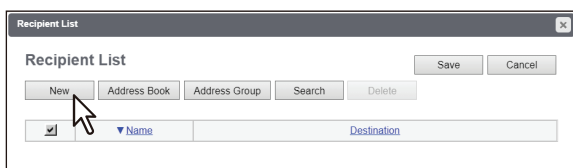
You can add a destination manually to the Recipient List.

Note

You cannot enter destinations if [Restriction of Destination Selection Method] > [Prohibit Direct Entry] is enabled.
P.105 “Restriction of Destination Selection Method”

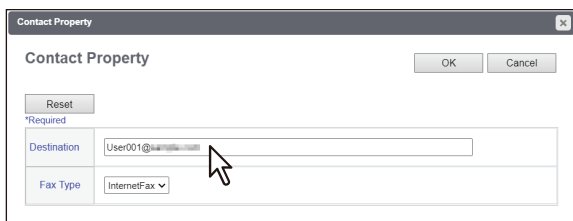
1 Click [Destination Setting] (when creating a Fax/Internet Fax agent) or [TO: Destination Setting] / [CC: Destination Setting] / [BCC: Destination Setting] (when creating an Email agent) to open the Recipient List page.

2 Click [New].



The Contact Property page is displayed.

3 Enter the E-mail address or fax number of the destination, in the [Destination] box.



Note

You can specify the fax number for the destination only when the Fax Unit is installed.

Tip

When the fax number is entered, select [G3 Fax] in the [Fax Type] box. When the E-mail address is entered, select [InternetFax] in the [Fax Type] box.

4 Click [OK].

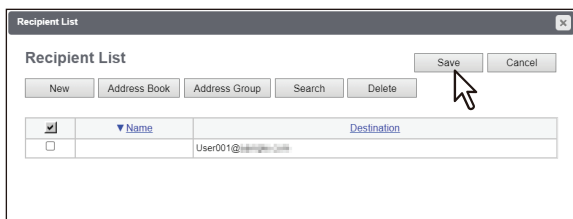
The destination is added to the Recipient List page.

5 Repeat steps 2 to 4 to add all additional destinations that you require.

Tip

You can remove the destinations you added to the Recipient List before saving the destination settings.
P.312 “Removing the contacts from the Recipient List”

6 Click [Save].



The contacts are added as destinations.

Selecting the destinations from the address book

You can select destinations from the address book in this equipment.

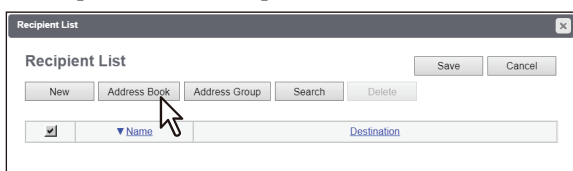
Note

You cannot select destinations from the address book if [Restriction of Destination Selection Method] > [Prohibit Use Of Local Address Book] is enabled.

📖 P.105 “Restriction of Destination Selection Method”

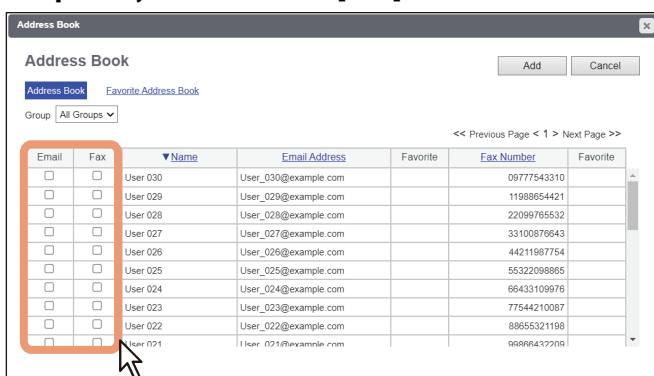
1 Click [Destination Setting] to open the Recipient List page.

2 Click [Address Book].



The Address Book page is displayed.

3 Select the [Email] check boxes of users you want to add as the E-mail recipients or Internet Fax recipients, and select the [Fax] check boxes of users you want to add as the Fax recipients.



Note

- When you are creating a Scan to E-mail template, only the [Email] check boxes are displayed in the Address Book page.
- You can specify the fax number for the destination only when the Fax Unit is installed.

Tip

If you want to sort the Recipient List by a specific group, select the desired group name in the [Group] box.

4 Click [Add].

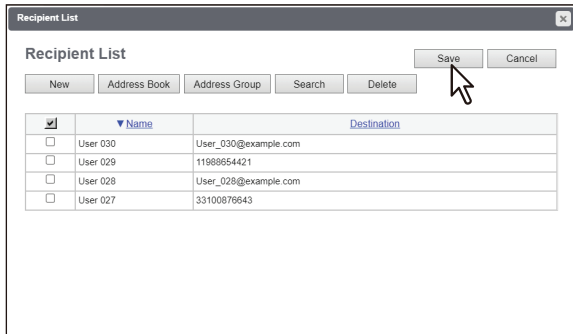
The selected destinations are added to the Recipient List page.

Tip

You can remove the destinations you added to the Recipient List before saving the destination settings.

📖 P.312 “Removing the contacts from the Recipient List”

5 Click [Save].



Recipient List

New Address Book Address Group Search Delete Save Cancel

<input checked="" type="checkbox"/>	▼ Name	Destination
<input type="checkbox"/>	User 030	User_030@example.com
<input type="checkbox"/>	User 029	11988654421
<input type="checkbox"/>	User 028	User_028@example.com
<input type="checkbox"/>	User 027	33100876643

The contacts are added as destinations.

Selecting the groups from the address book

You can select groups from the address book.

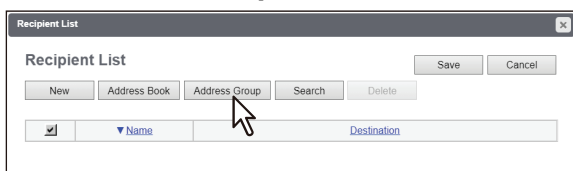
Note

You cannot select destinations from the address group if [Restriction of Destination Selection Method] > [Prohibit Use Of Local Address Book] is enabled.

📖 P.105 “Restriction of Destination Selection Method”

1 Click [Destination Setting] to open the Recipient List page.

2 Click [Address Group].



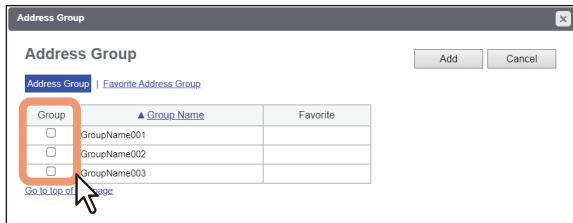
Recipient List

New Address Book Address Group Search Delete Save Cancel

▼ Name Destination

The Address Group page is displayed.

3 Select the [Group] check boxes that contain the desired destinations.



Address Group

Add Cancel

Address Group Favorite Address Group

Group	▲ Group Name	Favorite
<input type="checkbox"/>	GroupName001	
<input type="checkbox"/>	GroupName002	
<input type="checkbox"/>	GroupName003	

[Go to top of page](#)

4 Click [Add].

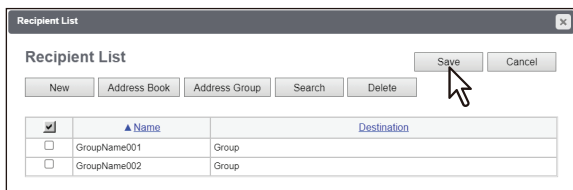
All recipients in the selected groups are added to the Recipient List page.

Tip

You can remove the destinations you added to the Recipient List before saving the destination settings.

📖 P.312 “Removing the contacts from the Recipient List”

5 Click [Save].



Recipient List

New Address Book Address Group Search Delete Save Cancel

<input checked="" type="checkbox"/>	▲ Name	Destination
<input type="checkbox"/>	GroupName001	Group
<input type="checkbox"/>	GroupName002	Group

The contacts are added as destinations.

Searching for destinations in the LDAP server

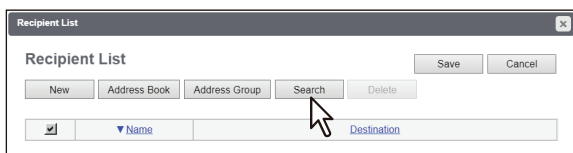
You can search for destinations in the registered LDAP server and in the address book.

Note

The LDAP server used for the search must be registered by a user who is granted administrator privileges in access policy mode.

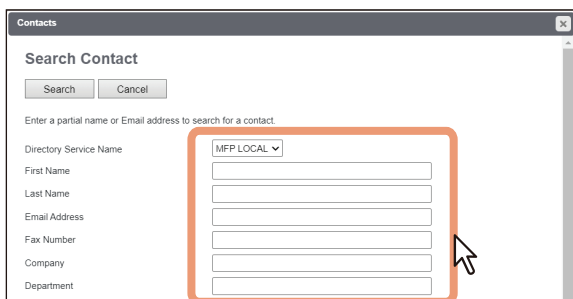
P.151 “LDAP Client settings”

- 1 Click [Destination Setting] to open the Recipient List page.
- 2 Click [Search].



The Search Contact page is displayed.

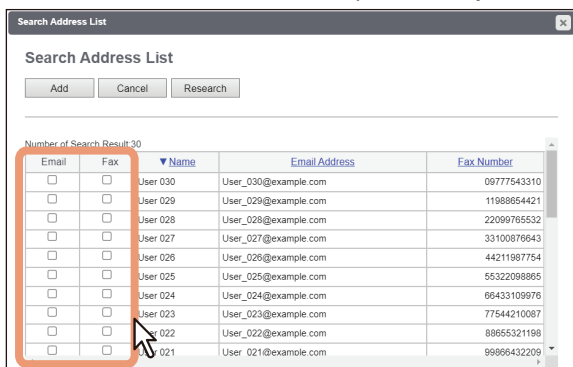
- 3 Select the directory service name that you want to search for in the [Directory Service Name] box, and enter the search terms in the boxes that you want to search.



Tip

- If you select the model name of this equipment at the [Directory Service Name] box, you can search for destinations in the address book of this equipment.
- TopAccess will search for destinations who match the entries.
- Leaving the box blank allows wild-card searching. However, you must specify at least one.

- 4 Click [Search].
TopAccess will start searching for destinations in the LDAP server and the Search Address List page will display the results.
- 5 Select the [Email] check boxes of users you want to add as the E-mail recipients or Internet Fax recipients, and select the [Fax] check boxes of users you want to add as Fax recipients.
Click [Research] to return to step 3 so that you can change the search criteria and execute the search again.



Note

- You can specify the fax number for the destination only when the Fax Unit is installed.
- The value of [company] and [department] will depend on the settings made by the user who is granted administrator privileges in the access policy mode.

6 Click [Add].

The selected destinations are added to the Recipient List page.

Tip

You can remove the destinations you added to the Recipient List before saving the destination settings.

P.312 “Removing the contacts from the Recipient List”

7 Click [Save].

<input checked="" type="checkbox"/>	Name	Destination
<input type="checkbox"/>	User 027	33100876643
<input type="checkbox"/>	User 028	22099765532
<input type="checkbox"/>	User 029	User_029@example.com

The contacts are added as destinations.

Removing the contacts from the Recipient List

1 Click [Destination Setting] to open the Recipient List page.

2 Select the check boxes of the destinations that you want to remove from the Recipient List, and click [Delete].

<input checked="" type="checkbox"/>	Name	Destination
<input checked="" type="checkbox"/>	User 027	33100876643
<input checked="" type="checkbox"/>	User 028	22099765532
<input type="checkbox"/>	User 029	User_029@example.com
<input type="checkbox"/>	User 030	User_030@example.com

The selected destinations are removed from the Recipient List.

InternetFax Setting

In the InternetFax Setting page, you can specify the content of the Internet Fax to be sent.

InternetFax Setting	
*Required	
1 Subject	<input type="radio"/> Scanned from (Device Name)[(Template Name)](Date)(Time) <input type="text"/> (Date)
2 *From Address	<input type="text"/>
3 From Name	From Name in Internet fax general setting
4 Body	<input type="text"/>
5 File Format	TIFF-S
6 Fragment Page Size	No Fragmentation

	Item name	Description
1	Subject	This sets the subject of the Internet Faxes. Select [Scanned from (Device Name) [(Template Name)] (Date) (Time)] to automatically apply the subject, or enter the desired subject in the box. If you enter manually, the subject will be [(Subject) (Date) (Time)].
2	From Address	Enter the E-mail address of the sender. When the recipient replies to a received document, the message will be sent to this E-mail address. You can enter up to 140 alphanumerical characters.



	Item name	Description
3	From Name	Select "From Name in Internet fax general setting" or one registered From Name from the list. P.178 "From Name Registration" P.199 "Setting up InternetFax Setting"
4	Body	Enter the body message of the Internet Fax. You can enter up to 1000 characters (including spaces).
5	File Format	Select the file format of the scanned image. Only [TIFF-S] (TIFF-FX (Profile S)) format can be selected.
6	Fragment Page Size	Select the size of the message fragmentation. [No Fragmentation] is set as the default.

Fax Setting

In the Fax Setting page, you can specify how the fax will be sent.

	Item name	Description
1	Preview	Select whether or not to preview before sending a fax. <ul style="list-style-type: none"> • ON — Select this to preview. • OFF — Select this not to preview.
2	Resolution	Select the resolution for sending faxes. <ul style="list-style-type: none"> • Standard — Select the Standard mode as the normal resolution. This mode is suitable when you are frequently transmitting text documents with normal size characters. • Fine — Select the Fine mode as the normal resolution. This mode is suitable when you are transmitting documents with small size characters or fine drawings. • Ultra Fine — Select the Ultra Fine mode as the normal resolution. This mode is suitable when you are transmitting documents with very small size characters or detailed drawings.

	Item name	Description
3	Original Mode	<p>Select the image quality mode for sending faxes.</p> <ul style="list-style-type: none"> • Text — Select the Text mode as the normal image quality mode. This mode is suitable when you are transmitting text documents. • Text/Photo — Select the Text/Photo mode as the normal image quality mode. This mode is suitable when you are transmitting documents which contain both texts and photos. • Photo — Select the Photo mode as the normal image quality mode. This mode is suitable when you are transmitting photo documents.
4	Exposure	<p>Select the exposure for sending faxes.</p> <p>Select [Auto] to automatically apply the ideal contrast, or adjust the contrast manually in 11 stages.</p>
5	Transmission Type	<p>Select the send mode.</p> <ul style="list-style-type: none"> • Memory Transmit — Select the Memory TX mode to automatically send the document after it has been temporarily stored to memory. This mode is useful if you want to return original files immediately. You can also send the same originals to two or more remote faxes. • Direct Transmit — Select the Direct TX mode to send the original as it is being scanned. This mode is useful if you want confirmation from the remote party. Originals are not stored to memory, and you can specify only one remote fax at a time. <p>Tip</p> <p>You can select [Direct Transmit] when you have created a template for Fax/InternetFax (not for Saved as file).</p> <p>When Fax/InternetFax and [Save as file setting] are combined, this item will be unselectable and will not be displayed.</p>
6	ECM	<p>Enable or disable the ECM (Error Correction Mode) to automatically resend any portion of the document affected by phone line noise or distortion.</p>
7	Line Select ^{*1}	<p>Select whether specifying the line to be used.</p> <ul style="list-style-type: none"> • Auto — Select not to specify the line to be used. • Line1 — Select to use Line 1 for this Fax agent. • Line2 — Select to use Line 2 for this Fax agent if installed.
8	Quality Transmit	<p>Select this to send a document in the Quality TX mode. This feature sends a document at a slower speed than normal so the transmission will be less affected by line conditions.</p>
9	SUB/SEP	<p>Enter the SUB number or SEP number if you want to set the mailbox transmission.</p>
10	SID/PWD	<p>Enter the password for SUB or SEP if required.</p>

	Item name	Description
11	Polling	<p>Select this to set Polling communications.</p> <ul style="list-style-type: none"> • (Blank) — Select the blank box when you do not want to perform polling. • Transmission — Select this to perform Polling Reservation that allows users to store the document in the memory. • Received — Select this to perform Turnaround Polling that allows users to poll another fax after transmitting documents to the remote fax on the same phone call. <p>Note</p> <p>You can select [Transmission] when you have created a template for Fax/InternetFax (not to be Saved as file).</p> <p>When Fax/InternetFax and [Save as file setting] are combined, this item will be unselectable and will not be displayed.</p>
12	Password	Enter the 4-digit security code for the document to be stored or received.
13	Fax Number(Security)	<p>When you select [Transmission] at the [Polling] box, enter the security fax number that allows polling of stored document.</p> <p>When you select [Received] at the [Polling] box, enter the security fax number to poll the documents from remote faxes.</p>
14	Delayed Transmit	If you enable the delayed communications for this agent, enter the day and time to send a document. Delayed transmission is disabled when the date is set to "0".
15	Priority Transmit	Select whether the document will be sent prior to other jobs.
16	Line Monitor	Select this to check the connection with the remote fax by confirming Line Monitor.
17	From Name	<p>Select "Terminal ID" or one registered From Name from the list.</p> <p> P.173 "Setting up Fax Setting"</p> <p> P.178 "From Name Registration"</p>

*1 This function is not available for some models.

❑ Email Setting

In the Email Setting page, you can specify the content of the Scan to Email document to be sent.

The screenshot shows the 'Email Setting' dialog box with the following fields and settings:

- 1 Subject:** Includes radio buttons for 'Use Email Setting in Administration Setting' (selected), 'Send data from (Device name) [(Template Name)]', and a checkbox for 'Add the date and time to the subject' (checked).
- 2 *From Address:** Includes radio buttons for 'Use From Address Setting set by Administrator' (selected) and a text input field.
- 3 From Name:** Includes radio buttons for 'Use From Name Setting set by Administrator' (selected) and a text input field.
- 4 Body:** A large text area for the email body.
- 5 File Format:** A dropdown menu set to 'PDF(Multi)' and a checkbox for 'Enable OCR'.
- 6 Encryption:** Includes a checked 'Encryption' checkbox, password fields for 'User Password' and 'Master Password' (each with a 'Retye Password' field), an 'Encryption Level' dropdown set to '128-bit AES', and checkboxes for 'Authority' (Printing, Change of Documents, Content Copying or Extraction, Content Extraction for accessibility).
- 7 Digital Signature:** A dropdown menu set to 'Disable'.
- 8 File Name:** Includes radio buttons for 'DOCMMDDYY(MMDDYY is a date)' (selected) and a text input field, and a checked checkbox for 'Add the date and time to a file name'.
- 9 Fragment Message Size:** A dropdown menu set to 'No Fragmentation'.

	Item name	Description
1	Subject	<p>This sets the subject of the E-mail.</p> <p>Use Email Setting in Administration Setting — Select this to set the subject specified in [Administration] > [Setup] > [Email] as subject.</p> <p>Send data from (Device Name)[(Template Name)] — Select this to set the [(Template Name)] data sent from (Device Name) as subject.</p> <p><Entry box> — Enter the text to set as subject.</p> <p>Add the date and time to the Subject — Select this to append date and time to the subject selected above.</p> <div> <p>Tip</p> <p>When [Meta Scan] is selected, you can use a variable as the subject. For more information on variables, see the reference below: 📖 P.379 “Variables of XML format files”</p> </div>
2	From Address	<p>This sets the E-mail address of the sender. When the recipient replies to a received document, the message will be sent to this E-mail address.</p> <p>Use From Address Setting set by Administrator — Select this to use the E-mail address specified in [Administration] > [Setup] > [Email]. When User Authentication or Email Authentication is enabled, select this to use the E-mail address specified in [Administration] > [Security] > [Authentication] > [Email Address Setting].</p> <p><Entry box> — Specify the sender address using up to 140 alphanumeric characters.</p>
3	From Name	<p>This sets the sender name of the E-mail document.</p> <p>Use From Name Setting set by Administrator — Select this to use the sender name specified in [Administration] > [Setup] > [Email]. When User Authentication or Email Authentication is enabled, select this to use the sender name specified in [Administration] > [Security] > [Authentication] > [Email Address Setting].</p> <p><Entry box> — Specify the sender name using up to 64 characters.</p>

	Item name	Description
4	Body	Enter the body message of the Scan to Email documents. You can enter up to 1000 characters (including spaces).
5	File Format	<p>Select the file format of the scanned image.</p> <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • Slim PDF(Multi) — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • Slim PDF(Single) — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • XPS(Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS(Single) — Select this to save scanned images separately as Single-page XPS files. • JPEG — Select this to save scanned images as JPEG files. • PDF/A(Multi) — Select this to save scanned images as a Multi-page PDF/A file. • PDF/A(Single) — Select this to save scanned images separately as Single-page PDF/A files. • DOCX(Multi) — Select this to save scanned images as a Multi-page Word file (DOCX) after OCR processing. • DOCX(Single) — Select this to save scanned images as a Single-page Word file (DOCX) after OCR processing. • XLSX(Multi) — Select this to save scanned images as a Multi-page Excel file (XLSX) after OCR processing. • XLSX(Single) — Select this to save scanned images as a Single-page Excel file (XLSX) after OCR processing. • PPTX(Multi) — Select this to save scanned images as a Multi-page PowerPoint file (PPTX) after OCR processing. • PPTX(Single) — Select this to save scanned images as a Single-page PowerPoint file (PPTX) after OCR processing. <p>You can select whether to enable OCR by [Enable OCR].</p> <div> <p>Tip</p> <p>If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> </div>

	Item name	Description
6	Encryption	<p>Set this for encrypting PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.</p> <p>Encryption — Select this if you want to encrypt PDF files.</p> <p>User Password — Enter a password for opening encrypted PDF files.</p> <p>Master Password — Enter a password for changing PDF encryption settings.</p> <p>Encryption Level — Select an encryption level.</p> <ul style="list-style-type: none"> • 40-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1. • 128-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4. • 128-bit AES — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6. • 256-bit AES — Select this to set an encryption level to the one compatible with Acrobat 9.0, PDF V1.7. <p>Authority — Select the desired authority items on encrypted PDF files.</p> <ul style="list-style-type: none"> • Printing — Select this to authorize users to print documents. • Change of Documents — Select this to authorize users to change documents. • Content Copying or Extraction — Select this to authorize users to copy and extract the contents of documents. • Content Extraction for accessibility — Select this to enable the accessibility feature. <p>Tip</p> <ul style="list-style-type: none"> • If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, see the reference below: <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> <ul style="list-style-type: none"> • The user password and the master password are not set at the factory shipment. • Passwords must be from 1 to 32 one-byte alphanumeric characters. • The user password must differ from the master password. <p>Note</p> <p>These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. The setting of the encryption will become available when either the user password or the master password is entered. For the details of the encryption setting, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> <p>Ask the administrator for resetting these passwords.</p>
7	Digital Signature	<p>Select whether the addition of the digital signature to PDF is enabled or disabled.</p> <p>Tip</p> <p>You cannot select this setting if you have selected a file format except PDF (Multi), PDF (Single), Slim PDF (Multi), Slim PDF (Single), PDF/A (Multi), and PDF/A (Single).</p>

	Item name	Description
8	File Name	<p>Select how the scanned file will be named. Select [DocYMMDD] to name it as described, or enter the desired file name in the box.</p> <p>When you want to add the date and time in the file name, select the [Add the date and time to a file name] check box.</p> <p>Tip</p> <p>When [Meta Scan] is selected, if you select [Add the date and time to a file name] in [File Name], it is also applied to the meta data file name.</p>
9	Fragment Message Size	Select the size of the message fragmentation. [No Fragmentation] is set as the default.

❑ Save as file Setting

In the Save as file Setting page, you can specify how and where a scanned file will be stored.

The screenshot shows the 'Save as file Setting' dialog box with the following components and callouts:

- 1** File Format: A dropdown menu set to 'TIFF(Multi)'.
- 2** Encryption: A section containing checkboxes for 'Encryption', 'Enable OCR', 'User Password', 'Master Password', 'Encryption Level' (set to '128-bit AES'), and 'Authority' (with sub-options: 'Printing', 'Change of Documents', 'Content Copying or Extraction', 'Content Extraction for accessibility').
- 3** Digital Signature: A dropdown menu set to 'Disable'.
- 4** Select following 2 items: A section with radio buttons for 'Use local folder' (selected), 'Remote 1', and 'Use Administrator Setting'.
- 5** Destination: A section for 'Remote 1' settings, including 'Storage Path' (VMFP13970485/FILE_SHARE), 'Protocol' (radio buttons for SMB, FTP, FTPS, NetWare IPX/SPX, NetWare TCP/IP), 'Network Path', 'Server Name', 'Port Number(Command)', 'Network Path', 'Login User Name', 'Password', 'Retype Password', and 'Connection Test' (with an 'Execute' button).
- 6** Destination: A section for 'Remote 2' settings, including 'Use Administrator Setting', 'Protocol', 'Network Path', 'Server Name', 'Port Number(Command)', 'Network Path', 'Login User Name', 'Password', 'Retype Password', and 'Connection Test' (with an 'Execute' button).
- 7** File Name: A section with radio buttons for 'DocMMDDYY(MMDDYY is a date)' (selected) and 'Add the date and time to a file name' (checked).

	Item name	Description
1	File Format	<p>Select the file format for the scanned file to be stored.</p> <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • Slim PDF(Multi) — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • Slim PDF(Single) — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • XPS(Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS(Single) — Select this to save scanned images separately as Single-page XPS files. • JPEG — Select this to save scanned images as JPEG files. • PDF/A(Multi) — Select this to save scanned images as a Multi-page PDF/A file. • PDF/A(Single) — Select this to save scanned images separately as Single-page PDF/A files. • DOCX(Multi) — Select this to save scanned images as a Multi-page Word file (DOCX) after OCR processing. • DOCX(Single) — Select this to save scanned images as a Single-page Word file (DOCX) after OCR processing. • XLSX(Multi) — Select this to save scanned images as a Multi-page Excel file (XLSX) after OCR processing. • XLSX(Single) — Select this to save scanned images as a Single-page Excel file (XLSX) after OCR processing. • PPTX(Multi) — Select this to save scanned images as a Multi-page PowerPoint file (PPTX) after OCR processing. • PPTX(Single) — Select this to save scanned images as a Single-page PowerPoint file (PPTX) after OCR processing. <p>You can select whether to enable OCR by [Enable OCR].</p> <div> <p>Tip</p> <p>If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> </div>

	Item name	Description
2	Encryption	<p>Set this for encrypting PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.</p> <p>Encryption — Select this if you want to encrypt PDF files.</p> <p>User Password — Enter a password for opening encrypted PDF files.</p> <p>Master Password — Enter a password for changing PDF encryption settings.</p> <p>Encryption Level — Select an encryption level.</p> <ul style="list-style-type: none"> • 40-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1. • 128-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4. • 128-bit AES — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6. • 256-bit AES — Select this to set an encryption level to the one compatible with Acrobat 9.0, PDF V1.7. <p>Authority — Select the desired authority items on encrypted PDF files.</p> <ul style="list-style-type: none"> • Printing — Select this to authorize users to print documents. • Change of Documents — Select this to authorize users to change documents. • Content Copying or Extraction — Select this to authorize users to copy and extract the contents of documents. • Content Extraction for accessibility — Select this to enable the accessibility feature. <p>Tip</p> <ul style="list-style-type: none"> • If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, see the reference below: <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> <ul style="list-style-type: none"> • The user password and the master password are not set at the factory shipment. • Passwords must be from 1 to 32 one-byte alphanumeric characters. • The user password must differ from the master password. <p>Note</p> <p>These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. The setting of the encryption will become available when either the user password or the master password is entered. For the details of the encryption setting, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> <p>Ask the administrator for resetting these passwords.</p>
3	Digital Signature	<p>Select whether the addition of the digital signature to PDF is enabled or disabled.</p> <p>Tip</p> <p>You cannot select this setting if you have selected a file format except PDF (Multi), PDF (Single), PDF/A (Multi), and PDF/A (Single).</p>

	Item name	Description
4	Destination — Use local folder	<p>Select this to save a scanned file to the “FILE_SHARE” folder.</p> <p>Tip When [Meta Scan] is selected, you can only specify one destination.</p>
5	Destination — Remote 1	<p>Select this check box to save the scanned file to a network folder. How you can set this item depends on how the user with administrator privileges configured Remote 1 in the [Save as file] submenu under the [Setup] menu. When you select [Allow the following network folder to be used as a destination], you can only select [Use Administrator Setting]. The protocol and the network path are displayed below this item.</p> <p>When you select [Allow user to select network folder to be used as a destination], you can select [Use User Setting] and enter the following items to specify where to save the file.</p> <p>If you are allowed to specify a network folder, select [Use User Setting] and enter the following items to specify where to save the file.</p> <p>Protocol Select the protocol to be used for uploading a scanned file to the network folder.</p> <ul style="list-style-type: none"> • SMB — Select this to send a scanned file to the network folder using the SMB protocol. • FTP — Select this to send a scanned file to the FTP server. • FTPS — Select this to send a scanned file to the FTP server using FTP over SSL/TLS. • NetWare IPX/SPX — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol. • NetWare TCP/IP — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol. <p>Server Name When you select [FTP] as the protocol, enter the FTP server name or IP address where a scanned file will be sent. For example, to send a scanned file to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box. When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available). When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server. You can enter up to 64 alphanumerical characters and symbols.</p> <p>Port Number(Command) Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number. You can enter a value in the range from 0 to 65535 using numbers and hyphens (-). Hyphen (-) is set as the default.</p>

	Item name	Description
	Destination — Remote 1 (Continued)	<p>Network Path When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned\”. When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”. When you select “NetWare IPX/SPX” or “NetWare TCP/IP” as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”. You can enter up to 128 alphanumerical characters and symbols.</p> <p>Login User Name Enter the login user name to access an SMB server, FTP server, or NetWare file server, if required. When you select [FTP] as the protocol, an anonymous log in is assumed if you leave this box blank. You can enter up to 32 alphanumerical characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.</p> <p>Password Enter the password to access an SMB server, FTP server, or NetWare file server, if required. You can enter up to 32 alphanumerical characters, symbols, and spaces. A single space only can also be entered.</p> <p>Retype Password Enter the same password again for a confirmation.</p> <p>[Execute] button Tests the connection using the specified network settings to check if the communications can be established.</p> <p>Tip When [Meta Scan] is selected, you can only specify one destination.</p>
6	Destination — Remote 2	<p>Select this check box to save the scanned file to a network folder. How you can set this item depends on how the user with administrator privileges configured Remote 2 in the [Save as file] submenu under the [Setup] menu. If the user with administrator privileges specified Remote 2 to use only the specified network folder, you can only select [Use Administrator Setting]. The protocol and the network path are displayed below this item. If the Remote 2 allows you to specify a network folder, you can specify the network folder settings. See the description of the Remote 1 option for each item.</p> <p>Tip When [Meta Scan] is selected, you can only specify one destination.</p>
7	File Name	<p>Select how the scanned file will be named. Select [DocYMMDD] to name it as described, or enter the desired file name in the box. When you want to add the date and time in the file name, select the [Add the date and time to a file name] check box.</p> <p>Tip When [Meta Scan] is selected, if you select [Add the date and time to a file name] in [File Name], it is also applied to the meta data file name.</p>

❑ Box Setting

In the Box Setting page, you can specify how scanned images will be stored in the Box.

Box Setting

1 Destination: Box Number (000 - Public Box), Password, Retype Password

2 Folder Name

3 Document Name: ☒ DocMMDDYY(MMDDYY is a date), ☐ [Empty field]

Buttons: Save, Cancel

	Item name	Description
1	Destination	Specify the destination box number for e-Filing. Box Number — Select the box number to store the scanned image. Password — Enter the password if the specified box is set with a password. Retype Password — Enter the same password again for a confirmation.
2	Folder Name	Enter the name of the folder where scanned images will be stored. If the specified named folder does not exit, the folder will be created automatically. You can enter up to 64 characters.
3	Document Name	Select how the scanned file will be named. Select [DocYMMDD] to name it as described, or enter the desired file name in the box.

❑ Store to USB Device Setting

On the Store to USB Device Setting page, you can set the method for saving templates in USB media.

Store to USB Setting

1 File Format: TIFF(Multi), Enable OCR ☐

2 Encryption: ☐ Encryption, User Password, Retype Password, Master Password, Retype Password, Encryption Level (128-bit AES)

3 Digital Signature: Disable

4 File Name: ☒ DocMMDDYY(MMDDYY is a date), ☐ [Empty field], ☒ Add the date and time to a file name.

Buttons: Save, Cancel

	Item name	Description
1	File Format	<p>Select the file format of the scanned image.</p> <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • Slim PDF(Multi) — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • Slim PDF(Single) — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. • XPS(Multi)— Select this to save scanned images as a Multi-page XPS file. • XPS(Single) — Select this to save scanned images separately as Single-page XPS files. • JPEG — Select this to save scanned images as JPEG files. • PDF/A(Multi) — Select this to save scanned images as a Multi-page PDF/A file. • PDF/A(Single) — Select this to save scanned images separately as Single-page PDF/A files. • DOCX(Multi) — Select this to save scanned images as a Multi-page Word file (DOCX) after OCR processing. • DOCX(Single) — Select this to save scanned images as a Single-page Word file (DOCX) after OCR processing. • XLSX(Multi) — Select this to save scanned images as a Multi-page Excel file (XLSX) after OCR processing. • XLSX(Single) — Select this to save scanned images as a Single-page Excel file (XLSX) after OCR processing. • PPTX(Multi) — Select this to save scanned images as a Multi-page PowerPoint file (PPTX) after OCR processing. • PPTX(Single) — Select this to save scanned images as a Single-page PowerPoint file (PPTX) after OCR processing. <p>You can select whether to enable OCR by [Enable OCR].</p> <p>Tip</p> <p>If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p>

	Item name	Description
2	Encryption	<p>Set this for encrypting PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.</p> <p>Encryption — Select this if you want to encrypt PDF files.</p> <p>User Password — Enter a password for opening encrypted PDF files.</p> <p>Master Password — Enter a password for changing PDF encryption settings.</p> <p>Encryption Level — Select an encryption level.</p> <ul style="list-style-type: none"> • 40-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1. • 128-bit RC4 — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4. • 128-bit AES — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6. • 256-bit AES — Select this to set an encryption level to the one compatible with Acrobat 9.0, PDF V1.7. <p>Authority — Select the desired authority items on encrypted PDF files.</p> <ul style="list-style-type: none"> • Printing — Select this to authorize users to print documents. • Change of Documents — Select this to authorize users to change documents. • Content Copying or Extraction — Select this to authorize users to copy and extract the contents of documents. • Content Extraction for accessibility — Select this to enable the accessibility feature. <p>Tip</p> <ul style="list-style-type: none"> • If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF • The user password and the master password are not set at the factory shipment. • Passwords must be from 1 to 32 one-byte alphanumeric characters. • The user password must differ from the master password. <p>Note</p> <p>These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. The setting of the encryption will become available when either the user password or the master password is entered. For the details of the encryption setting, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF Ask the administrator for resetting these passwords.</p>
3	Digital Signature	<p>Select whether the addition of the digital signature to PDF is enabled or disabled.</p> <p>Tip</p> <p>You cannot select this setting if you have selected a file format except PDF (Multi), PDF (Single), Slim PDF (Multi), Slim PDF (Single), PDF/A (Multi), and PDF/A (Single).</p>

	Item name	Description
4	File Name	<p>Select how the scanned file will be named. Select [DocYYMMDD] to name it as described, or enter the desired file name in the box.</p> <p>When you want to add the date and time in the file name, select the [Add the date and time to a file name] check box.</p> <p>Tip</p> <p>When [Meta Scan] is selected, if you select [Add the date and time to a file name] in [File Name], it is also applied to the meta data file name.</p>

□ Scan Setting

In the Scan Setting page, you can specify how originals are scanned for the Scan to File, Scan to Email, and Scan to e-Filing agent.

The screenshot shows the 'Scan Setting' dialog box with the following settings and callouts:

- 1: Preview (OFF)
- 2: Single-Sided Scan (Single)
- 3: Rotation (A → A, A ← A, V → A, V ← A)
- 4: Book Original Scan (Enable)
- 5: Color Mode (Black)
- 6: Resolution (200dpi)
- 7: Book Start Page (Right)
- 8: Book Layout (Open from right)
- 9: Book Image Shift (Disable)
- 10: Book Image Shift Margin (mm)
- 11: Compression (Middle)
- 12: Original Mode (Text)
- 13: Exposure (Auto)
- 14: Original Size (Custom)
- 15: Custom Size (Auto Cut of Print Area, Expand Size 2 mm, Skew Correction)
- 16: Background (Auto)
- 17: Contrast (Auto)
- 18: Sharpness (Auto)
- 19: Saturation (Auto)
- 20: RGB Adjustment (Red, Green, Blue)
- 21: Omit Blank Page (OFF)
- 22: Outside Erase (OFF)
- 23: Scanner Streaks Reduction (OFF)
- 24: OCR (Language: 1st Japanese, 2nd English, Auto Rotation: Enable)
- 25: Drop Out Color (OFF)
- 26: Multiple Annotation (Setting Items: String1, String2, Serial Number, Date, Page, Position, Start Page, End Page, Background, Stamp Direction, Font Size)

	Item name	Description
1	Preview	<p>Select whether to display the scanned image on the touch panel after the scanning an original.</p> <ul style="list-style-type: none"> • OFF — Select this not to display the scanned image. • ON — Select this to display the scanned image.

	Item name	Description
2	Single/2-Sided Scan	<p>Select whether to scan one side or both sides of an original. You cannot select this when [Book Original Scan] is enabled. Available only when the Reversing Automatic Document Feeder is installed.</p> <ul style="list-style-type: none"> • Single — Select this to scan one side of an original. • Duplex Book — Select this to scan both sides of originals when the pages are printed vertically in the same direction and bound along the vertical side of the paper. • Duplex Tablet — Select this to scan both sides of originals with a vertical reversal to be bound along the horizontal side of the paper.
3	Rotation	<p>Select how the scanned images will be rotated. You cannot select the 180-degree and 270-degree rotations (right two options) when [Book Original Scan] is enabled.</p>
4	Book Original Scan	<p>Specify whether to scan two facing pages of book-type originals separately. You cannot specify this when [Omit Blank Page] is set to [ON].</p> <ul style="list-style-type: none"> • Disable — Disables the Book Original Scan function. • Enable — Enables the Book Original Scan function. You can set [Book Start Page], [Book Layout], [Book Image Shift], and [Book Image Shift Margin].
5	Color Mode	<p>Select the color mode for scanning.</p> <ul style="list-style-type: none"> • Black — Select this to scan in the black mode. • Gray — Select this to scan in the gray scale mode. • Full Color — Select this to scan in the full color mode. • Auto Color — Select this to scan in the auto color mode. <p>Note</p> <ul style="list-style-type: none"> • The [Color Mode] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting. • When [Auto Color] is selected, you cannot select JPEG or TIFF (Multi) for the file format. Also when [Black] is selected, JPEG is not allowed.
6	Resolution	<p>Select the resolution for scanning.</p> <p>Note</p> <p>The [Resolution] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting.</p>
7	Book Start Page	<p>Select a starting page of the book-type originals. You can select this only when [Book Original Scan] is enabled.</p> <ul style="list-style-type: none"> • Right — Select this to scan two facing pages separately for the book-type originals which start from the right page. • Left — Select this to scan two facing pages separately for the book-type originals which start from the left page.
8	Book Layout	<p>Select how to open the book-type originals. You can select this only when [Book Original Scan] is enabled.</p> <ul style="list-style-type: none"> • Open from right — Select this to scan two facing pages separately for the book-type originals which you open from the right. • Open from left — Select this to scan two facing pages separately for the book-type originals which you open from the left.

	Item name	Description
9	Book Image Shift	<p>Select whether to shift the images of two facing pages that have been scanned separately, considering the margins for binding the book-type originals. You can select this only when [Book Original Scan] is enabled.</p> <ul style="list-style-type: none"> • Enable — Select this to scan two facing pages separately and shift the page images, considering the margins. • Disable — Select this to scan two facing pages separately as they are without considering the margins.
10	Book Image Shift Margin	<p>Set the margin of the book-type originals from 0 to 30 mm to shift the page images of two facing pages that have been scanned separately. You can set the margin only when [Book Original Scan] and [Book Image Shift] are enabled.</p>
11	Compression	<p>Select the compression for scanning.</p> <p>Note</p> <ul style="list-style-type: none"> • This cannot be set when [Black] is selected at the [Color Mode] box. • The [Compression] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting.
12	Original Mode	<p>Select the document type of the originals.</p> <ul style="list-style-type: none"> • Text — Select this to set the Text mode as the default original mode. • Text/Photo — Select this to set the Text/Photo mode as the default original mode. Depending on the model, this can be selected only when [Black] is selected in the [Color Mode] box.*¹ • Photo — Select this to set the Photo mode as the default original mode. <p>Note</p> <p>This cannot be set when [Gray] is selected in the [Color Mode] box.</p>
13	Exposure	<p>Select the exposure for scanning.</p> <p>Select [Auto] to automatically apply the best contrast for the document. You can also manually adjust the exposure in 11 stages. The farther to the right that you set the value, the darker the density of the scanned image will become.</p> <p>Note</p> <p>[Auto] is not available when [Gray], [Full Color], or [Auto Color] is selected at the [Color Mode] box. In that case, set the exposure manually.</p>
14	Original Size	<p>Select the original size.</p> <p>If this is set to [Auto], the size is automatically detected. Select [Mixed Original Sizes] to scan a document with mixed sizes. You can also specify the original size. If this is set to [Custom], you can specify the custom original size for scanning.</p>

	Item name	Description
15	Custom Size	<p>Select the custom original size for scanning. You can set [Skew Correction] for the following settings.</p> <ul style="list-style-type: none"> • Registered Size — Select this to select the custom original size that has been registered on the control panel. • Auto Cut of Print Area — Select this to set the custom size by cutting the print area of the original. You can enter a value in [Expand Size] to expand the area. • Auto Detected — Select this to set the custom size by detecting the original size automatically. This function is available only when the Dual Scan Document Feeder (DSDF) has been installed.
16	Background	Select the density level of the background of the scanned image. Density can be adjusted in 9 levels. The farther to the right that you set the value, the darker the density of the background will become.
17	Contrast	<p>Select the contrast level of the scanned image. Contrast can be adjusted in 9 levels. The farther to the right that you set the value, the higher the contrast level will become.</p> <p>Note</p> <p>This is not available when [Black] or [Gray] is selected at the [Color Mode] box.</p>
18	Sharpness	Select the sharpness level of the scanned image. Sharpness can be adjusted in 9 levels. The farther to the right that you set the value, the sharper the scanned image will become.
19	Saturation	<p>Select the saturation level of the scanned image. Saturation can be adjusted in 7 levels. The farther to the right you set the value, the more vivid the scanned image will become.</p> <p>Note</p> <p>This is not available when [Black] or [Gray] is selected at the [Color Mode] box.</p>
20	RGB Adjustment	<p>Select the RGB density level of the scanned image. RGB density can be adjusted in 9 levels for each color. The farther to the right you set the value, the darker the density of the selected color will become.</p> <p>Note</p> <p>This is not available when [Black] or [Gray] is selected at the [Color Mode] box.</p>
21	Omit Blank Page	<p>Select whether to automatically omit a blank page in the scanned image if it is included in originals. You cannot select this when [Book Original Scan] is enabled.</p> <ul style="list-style-type: none"> • OFF — The blank page is not omitted. • ON — The blank page is omitted.
22	Outside Erase	<p>Select whether to erase a shade that appears outside of the scanned image when an original is placed on the original glass while the Original Cover is left open. The erased shade will be whitened.</p> <p>If you want to erase it, you can select the criteria in 7 levels for judging if it is an area to be erased. The farther to the right you select, the larger the area that will be erased. [OFF] is selected by default.</p>

	Item name	Description
23	Scanner Streaks Reduction	<p>Use this setting if streaks are conspicuous on images when originals are scanned.</p> <ul style="list-style-type: none"> • OFF — Select this not to perform streak reduction. • ON — Select this to perform streak reduction. <p>Tip If this function is used, the scanning speed will be slower than usual.</p>
24	OCR	<p>You can specify the prioritized language and auto rotation for OCR processing.</p> <ul style="list-style-type: none"> • Language — Select the primary and secondary languages. • Auto Rotation — Specify whether or not to automatically rotate.
25	Drop Out Color	<p>Select the drop out level of colors eliminated from the scanned original. Drop out can be adjusted in 7 levels. Select [OFF] to disable this function.</p>

	Item name	Description
26	Multiple Annotation	<p>Set the multiple annotation function that allows you to add specified information as annotations when the scanned originals are saved as PDF files.</p> <ul style="list-style-type: none"> • ON/OFF — Turn on or off the multiple annotation function. When you select [ON], you can specify the following information to add it as annotations. • Setting Items — As you select [String1], [String2], [Serial Number], [Date], and [Page] arbitrarily, they appear in order of selection. They are added as annotations. • String1, Space — Select the check box so that you can enter up to 32 characters as a string 1. Select [Space] to add a space after the string 1. • String2, Space — Select the check box so that you can enter up to 32 characters as a string 2. Select [Space] to add a space after the string 2. • Serial Number, Digits, Space — Select the check box so that you can enter the first serial number and the number of digits (1 - 10). Select [Space] to add a space after the serial number. • Date, Space — Select the check box so that you can select the date format (YYYY-MM-DD, DD-MM-YYYY, or MM-DD-YYYY) and specify the date. When you select [User Setting], you can enter an arbitrary date. When you select [Auto], the date of the file creation is automatically set. Select [Space] to add a space after the date. • Page, Start Page, Space — Select the page format (page number only, page number enclosed with hyphens, or page number/total page number) and specify the starting page number (1 - 30,000). Select [Space] to add a space after the page number. • Position — Select the annotation position (Top Left, Top Center, Top Right, Middle Left, Middle Right, Bottom Left, Bottom Center, or Bottom Right). • Start Page — Enter the first page number (1 - 1,000) to start adding annotations. • End Page, Last — Because [Last] is selected as a default, annotations are added up to the last page: you cannot enter the end page number. To end adding annotations before the last page, clear the [Last] selection and enter the end page number (1 - 1,000). • Background — Select the background (None or White) of the annotation characters. • Stamp Direction — Select the direction (Horizontal or Vertical) of the annotation characters. • Font Size — Select the font size (8 - 16) of annotation characters.

	Item name	Description
	Multiple Annotation (Continued)	<div>Note</div> <ul style="list-style-type: none"> • The multiple annotation function is disabled when scanned originals are saved in the file formats other than PDF. • The appearance order of annotations in the [Annotation] box might change. Even if you have selected [String2] and [String1] in this order and saved them, the order changes to [String1] and [String2] and the specified strings are replaced with each other. • When you select [User Setting] at [Date], the entered date is added as it is for an annotation. Do not enter an impossible date. • If you select [Space] for the last selected annotation, the last space is ignored. • The annotation is not added if you enter the number at [Start Page] which is greater than the real number of scanned originals. You cannot enter the number which is greater than the one entered at [End Page]. • The annotation is added up to the last page if you enter the number at [End Page] which is greater than the real number of scanned originals. You cannot enter the number which is smaller than the one set entered at [Start Page]. • When you select [Vertical] at [Stamp Direction], the whole annotation is rotated by 90 degrees counterclockwise and characters are arranged upward. And you cannot select [Top Center] and [Bottom Center] at [Position].

*1 Available only for models that support color printing.

Extended Field settings

You can set extended fields for meta data.

Set the field you have registered in [Administration] > [Registration] > [Extended Field Definition].

	Item name	Description
1	Extended Field Definition No.	Allows you to select a registered extended field definition.

Extended Field Properties

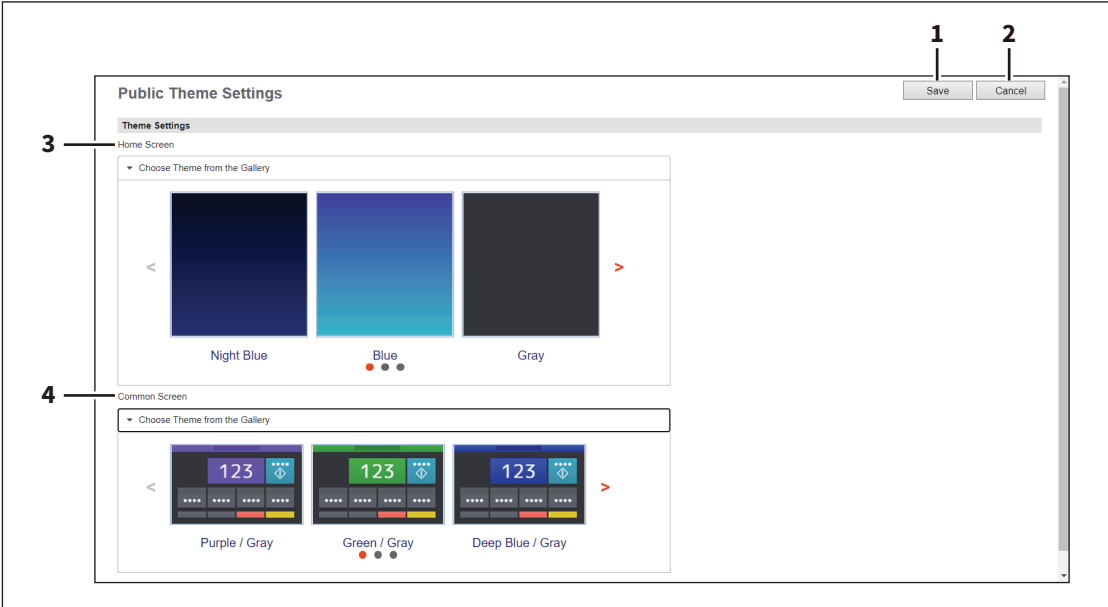
[Extended Field Properties] set under the selected extended field definition are displayed.

Values set in this screen are used as the default values for [Extended Field Properties] displayed on the touch panel when using Meta Scan.

Items with an asterisk (*) attached at the beginning of the [Extended Field Properties] name are mandatory entry fields.

Public Theme Settings

You can specify the theme of the shared home screen.



	Item name	Description
1	Save	Saves the changed settings.
2	Cancel	Cancels the operation.
3	Home Screen	Specify the theme for Home screen. You can select the theme from a list if you select [Choose Theme from the Gallery].
4	Common Screen	Specify the theme for common screens. You can select the theme from a list if you select [Choose Theme from the Gallery]. <div>Note</div> General users cannot change this setting.

Public Home Settings

You can specify the background, button size, and transparency of the shared home screen.

The screenshot shows the 'Public Home Settings' dialog box. It has a title bar with 'Save' (1) and 'Cancel' (2) buttons. The dialog is divided into five sections, each with a number 3 through 6. Section 3 is 'Background Settings' with 'Current Background' set to 'Gloaming Blue' and a 'Choose Background Image from Gallery' button. Section 4 is 'Button Size Settings' with 'Current Button Size' set to 'Medium' and a 'Choose Button Size from Gallery' button. Section 5 is 'Transparency Settings' with sliders for 'Title' and 'Panel Button' both set to 100%, and a 'Preview' image. Section 6 is 'Font Settings' with 'Font Size' set to 'Medium' and 'Font Color' set to 'White'.

	Item name	Description
1	Save	Saves the changed settings.
2	Cancel	Cancels the operation.
3	Background Settings	Specify the background of the home screen. You can select the background design from a list if you select [Choose Background Image from Gallery] at [Current Background]. Note General users cannot change this setting.
4	Button Size Settings	Specify the button size. You can select the button size from a list if you select [Choose Button Size from Gallery] at [Current Button Size].
5	Transparency Settings	Specify the transparency of the home screen. <ul style="list-style-type: none"> • Title — You can specify the transparency of the title bar. • Panel Button — You can specify the transparency of the buttons.
6	Font Settings	Specify the font used on the public home screen. <ul style="list-style-type: none"> • Font Size — You can specify the font size. • Font Color — You can specify the font color.

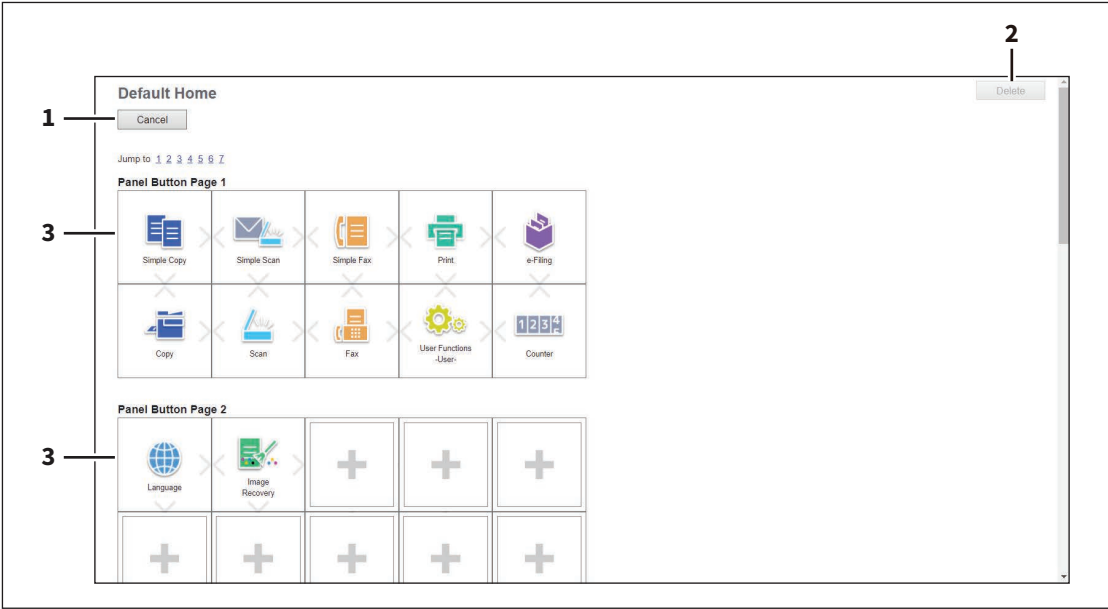
■ Default Home

You can use Default Home to specify the default status of the home screen that is displayed when you press the [Home] button on the control panel.

Tip

The [Default Home] submenu can be accessed from the [Registration] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:

- 📖 P.14 “Access Policy Mode”
- 📖 P.300 “[Registration] ([Administration]) Item List”



	Item name	Description
1	[Cancel] button	Cancels the operation.
2	[Delete] button	Deletes the selected panel button.
3	Panel button list	Displays a list of panel buttons you can select for the shared home. Select the panel buttons you want to use. Click the link to edit the home type. 📖 P.301 “[Select Home Type] screen”

■ Default Home Settings

You can specify the background, button size, and transparency of the initial home screen. Setting items are the same as [Public Home Settings].

- 📖 P.335 “Public Home Settings”

Simple Screen Settings

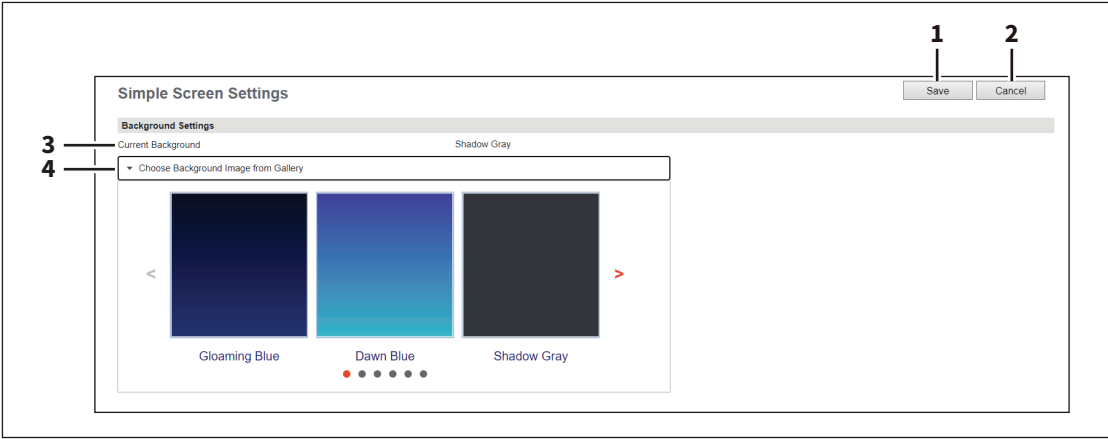
You can select the background of the simple screen.

Tip

The [Simple Screen Settings] submenu can be accessed from the [Registration] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:

P.14 “Access Policy Mode”

P.300 “[Registration] ([Administration]) Item List”

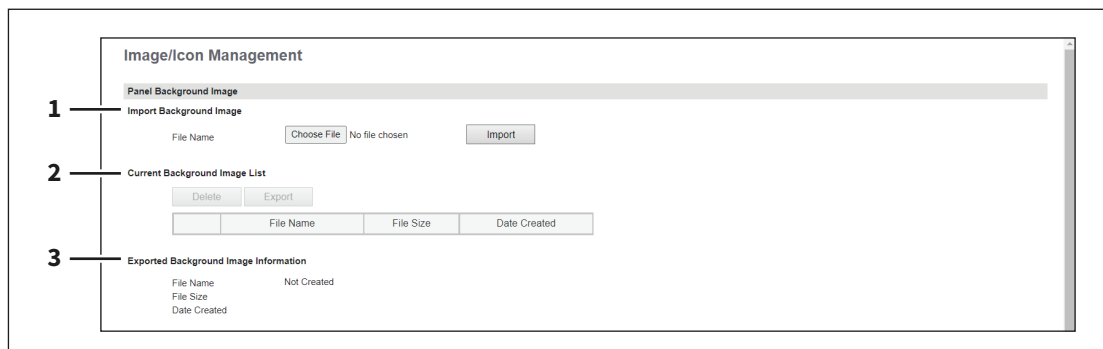


	Item name	Description
1	Save	Saves the changed settings.
2	Cancel	Cancels the operation.
3	Current Background	Shows the name of the current background.
4	Choose Theme from the Gallery	Click this to show the list, so that you can select the background.

■ Image/Icon Management

You can manage background and icon images.

□ Panel Background Image

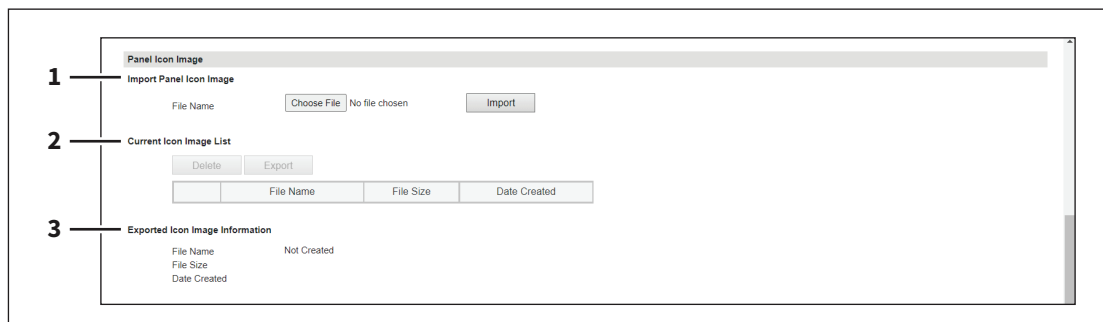


	Item name	Description
1	Import Background Image	Imports a background image. <ul style="list-style-type: none">• [Choose File] button — You can select an image file.• [Import] button — You can import the selected image file.
2	Current Background Image List	Displays the list of the registered images and allows you to manage them. <ul style="list-style-type: none">• [Delete] button — You can delete the selected image file.• [Export] button — You can export the selected image file.
3	Exported Background Image Information	Displays information on the selected image file.

You can import images in the following format.

- Image size: 1024 x 600 pixels (recommended size)
- Image format: png
- Color: 24 bits
- Maximum file size: 1.5MB

□ Panel Icon Image



	Item name	Description
1	Import Panel Icon Image	Imports an icon image. <ul style="list-style-type: none">• [Choose File] button — You can select an image file.• [Import] button — You can import the selected image file.

	Item name	Description
2	Current Icon Image List	Displays the list of the registered images and allows you to manage them. <ul style="list-style-type: none"> • [Delete] button — You can delete the selected image file. • [Export] button — You can export the selected image file.
3	Exported Icon Image Information	Displays information on the exported image file.

You can import images in the following format.

- Image size: 193 x 128 pixels
- Image format: png
- Color: 24 bits
- Maximum file size: 50KB

❑ Card Authentication Guidance Image

The screenshot displays the 'Card Authentication Guidance Image' management interface. It is divided into three main sections:

- Import Card Authentication Guidance Image:** This section includes a 'File Name' input field, a 'Choose File' button, a 'No file chosen' status indicator, and an 'Import' button.
- Card Authentication Guidance Image List:** This section contains 'Delete' and 'Export' buttons above a table. The table has columns for 'File Name', 'File Size', and 'Date Created'. A single row is visible with a checked checkbox, 'image01.png', '2.45 KB', and a date.
- Export Card Authentication Guidance Information:** This section shows fields for 'File Name', 'File Size', and 'Date Created', with a 'Not Created' status indicator.

	Item name	Description
1	Import Card Authentication Guidance Image	Imports a image for the card authentication guidance. <ul style="list-style-type: none"> • [Choose File] button — You can select an image file. • [Import] button — You can import the selected image file.
2	Card Authentication Guidance Image List	Displays the list of the registered images and allows you to manage them. <ul style="list-style-type: none"> • [Delete] button — You can delete the selected image file. • [Export] button — You can export the selected image file.
3	Export Card Authentication Guidance Information	Displays information on the exported image file.

You can import images in the following format.

- Image size: 500 x 320 pixels
- Image format: png, gif
- Maximum file size: 2MB

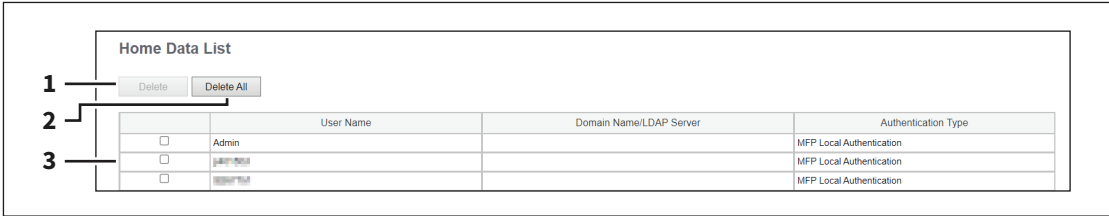
■ Home Data List

You can use Home Data List to display a list of all saved home screens and manage them.

Tip

The [Home Data List] submenu can be accessed from the [Registration] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:

- 📖 P.14 “Access Policy Mode”
- 📖 P.300 “[Registration] ([Administration]) Item List”



	Item name	Description
1	[Delete] button	Deletes the selected home screen.
2	[Delete All] button	Deletes all home screens.
3	Home screen list	Displays a list of registered home screens.

■ Fax Received Forward and InternetFAX Received Forward settings

You can forward received faxes and Internet Faxes to a specified address using fax received forward and Internet Fax received forward functions. You can check all faxes and Internet Faxes received by this equipment using these functions.

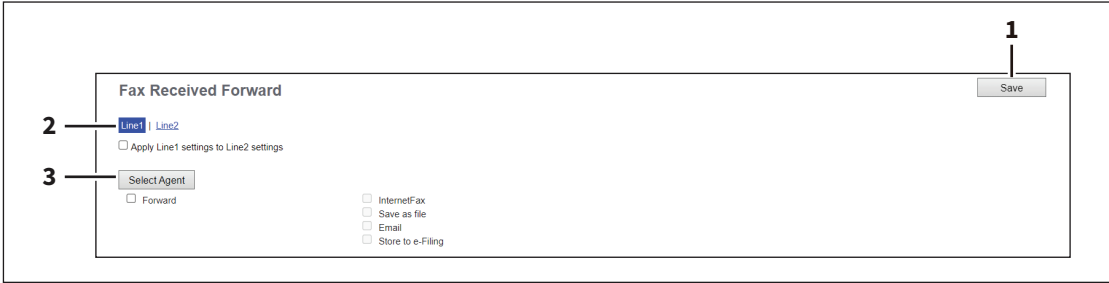
Tip

The [Fax Received Forward]/[InternetFAX Received Forward] submenu can be accessed from the [Registration] menu on the [Administration] page.

For how to access it and information on the [Registration] menu, see the references below:

- 📖 P.14 “Access Policy Mode”
- 📖 P.300 “[Registration] ([Administration]) Item List”

To forward received faxes, you need to set differently on two screens [Fax Received Forward] and [InternetFAX Received Forward] according to the reception method. The settings are common except the selection of fax lines via the telephone lines.



	Item name	Description
1	[Save] button	Click this button to save the settings after you have set them.
2	Line1/Line2	Select a fax line [Line1] or [Line2] because you can set up two lines differently for faxes via the telephone lines. If you have set up for the line 1 and want to apply the settings for the line 1 to the line 2, select [Apply Line1 settings to Line2 settings].
3	[Select Agent] button	<p>Select [Forward] and other agents from among the following options to forward received faxes. To stop forwarding faxes, clear the [Forward] check box.</p> <ul style="list-style-type: none"> • Internet/Fax(Relay) — Forwards received faxes to another Internet Fax device. This agent can be combined with the [Save as file] or [Store to e-Filing] agent. • Save as file — Forwards received faxes to a shared folder on the equipment or a network folder. This agent can be combined with another one. • Email — Forwards received faxes to E-mail addresses. This agent can be combined with the [Save as file] or [Store to e-Filing] agent. • Store to e-Filing — Forwards received faxes to e-Filing on the equipment. This agent can be combined with another one. <p>When you click the [Select Agent] button, the screen shows the necessary settings and the function lists for the selected agents. When you click the button located above each list, another window appears so that you can set the necessary functions.</p>

Note

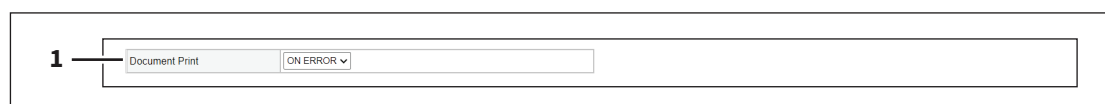
- You can also forward using the F-code communications function on this equipment when communicating with a fax which supports the F-code communications function. You need to create a mailbox in advance. Also, you can use the TSI (sender information) forwarding function by making the counterpart fax number as a box number and forwarding documents in the box (mailbox) to a specified saving location.
- [Fax Received Forward] is available only when the Fax Unit is installed on this equipment.
- Two lines become available in [Fax Received Forward] by installing the 2nd Line for FAX Unit in the FAX Unit. It is possible to set the reception setting in each line. The received faxes are forwarded to the specified destinations according to the settings regardless of whether the faxes are received through line 1 or line 2.
- The image quality of the file that is stored by Save as file, E-mail, and Store to e-Filing is different from the output of the received fax when it is printed.

The received fax and Internet Faxes can be transmitted to the following destinations:

- Other Internet Fax devices
- Local folder in this equipment or network folders
- E-mail addresses
- Box in this equipment

❑ Setting up Document Print (Fax/InternetFax Received Forward)

Select when to print received fax documents that are forwarded.



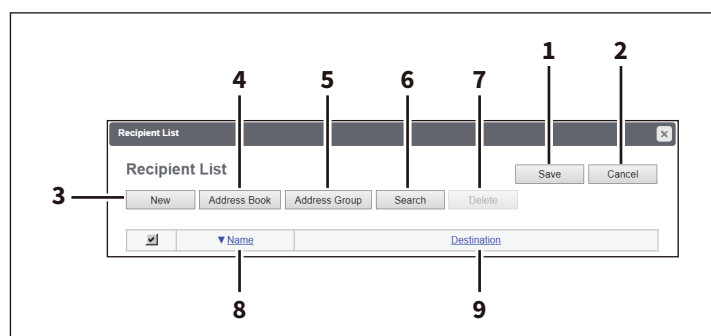
1 — Document Print ON ERROR ▼

	Item name	Description
1	Document Print	<ul style="list-style-type: none">• Always — Select this to always print forwarded document.• ON ERROR — Select this to print the received document when an error occurred on all forwarding destinations. (For example, the document is not printed when the E-mail transmission only failed in a combined setting of Save as File and E-mail.)



❑ Setting up Destination Setting (Fax/Internet Fax Received Forward)

When you have selected the [Internet/Fax(Relay)] or [Email] agent, you can specify the E-mail address to which received faxes are forwarded. Click the [Destination Setting], [TO: Destination Setting], [CC: Destination Setting], or [BCC: Destination Setting] button to open the following window for setup.

Recipient List



1 — Save button
2 — Cancel button
3 — New button
4 — Address Book button
5 — Address Group button
6 — Search button
7 — Delete button
8 — Name column header
9 — Destination column header

	Item name	Description
1	[Save] button	Saves recipient settings.
2	[Cancel] button	Cancels the settings.
3	[New] button	Displays a screen where you can register an E-mail address as the recipient.  P.48 “[Create Destination information]/[Edit Destination information] screen”
4	[Address Book] button	Allows you to select a recipient from the address book.
5	[Address Group] button	Allows you to select an address book group as a destination.
6	[Search] button	Allows you to search a recipient from the address book.  P.50 “[Search Contact] screen”
7	[Delete] button	Deletes the selected recipient.
8	Name	Displays the names registered to the address book. <div>Note</div> <p>You can remove destinations that you have added to the Recipient List before saving the destination settings.</p>
9	Destination	Displays the E-mail addresses.

[Contact Property] screen

You can specify an E-mail address as the recipient.

1

2

3

4

	Item name	Description
1	[OK] button	Saves the recipient.
2	[Cancel] button	Cancels the settings.
3	[Reset] button	Deletes the entered E-mail address.
4	Destination	Enter the E-mail address.

❑ Setting up InternetFax Setting (Fax/Internet Fax Received Forward)

When you have selected the [Internet/Fax(Relay)] agent, you can set how to forward received faxes. Click the [Internet/Fax(Relay)] button to open the following window for setup.

1

2

3

4

5

6

7

8

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Subject	This sets the subject of the Internet Faxes. Select [Scanned from (Device Name) [(Template Name)] (Date) (Time)] to automatically apply the subject, or enter the desired subject in the box. If you manually enter the subject, the subject will be “(Subject) (Date)” by automatically adding the date.
4	From Address	Enter the E-mail address of the sender. When the recipient replies to a received document, the message will be sent to this E-mail address.
5	From Name	Enter the sender name of the Internet Fax.
6	Body	Enter the body message of the Internet Fax. You can enter up to 1000 characters (including spaces).
7	File Format	Select the file format of the scanned image. Only [TIFF-S] (TIFF-FX (Profile S)) format can be selected.
8	Fragment Page Size	Select the size of the message fragmentation.

❑ Setting up Save as file Setting (Fax/InternetFAX Received Forward)

When you have selected the [Save as file] agent, you can set how and where to store received faxes. Click the [Save as file] button to open the following window for setup.

The screenshot shows the 'Save as file Setting' dialog box. It has a title bar with a close button (X) and two buttons: 'Save' (labeled 1) and 'Cancel' (labeled 2). The main area is divided into several sections:

- File Format** (labeled 3): A dropdown menu set to 'TIFF(Multi)' and an 'Enable OCR' checkbox.
- Encryption** (labeled 4): An 'Encryption' checkbox, fields for 'User Password' and 'Master Password' (each with a 'Retype Password' field), an 'Encryption Level' dropdown set to '128-bit AES', and an 'Authority' section with checkboxes for 'Printing', 'Change of Documents', 'Content Copying or Extraction', and 'Content Extraction for accessibility'.
- Digital Signature** (labeled 5): A 'Digital Signature' dropdown menu set to 'Disable'.
- Destination** (labeled 8): A section for selecting the storage location. It includes 'Select following 2 items', a checked 'Use local folder' option, a 'Storage Path' field showing '\\MFP13970495\\FILE_SHARE\\', and an unchecked 'Remote 1' option. Below this are fields for 'Protocol', 'Network Path', 'Server Name', 'Port Number(Command)', 'Login User Name', and 'Password' (with a 'Retype Password' field), and a 'Connection Test' button labeled 'Execute'.
- File Name** (labeled 9): A section for naming the file. It includes a 'Format' dropdown set to '[FileName]-[Date]-[Page]', a 'Comment' field, a 'Date' dropdown set to '[YYYY][MM][DD][H][mm][SS]', a 'Page' dropdown set to '4digits', a 'Sub ID' dropdown set to 'Auto', and a checked 'Add line information to File Name' checkbox.

Other callouts include 6 pointing to the 'Use local folder' checkbox and 7 pointing to the 'Storage Path' field.

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.

	Item name	Description
3	File Format	<p>Select the file format to which the received document will be saved.</p> <ul style="list-style-type: none"> • TIFF (Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF (Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF (Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF (Single) — Select this to save scanned images separately as Single-page PDF files. • XPS (Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS (Single) — Select this to save scanned images separately as Single-page XPS files. <p>You can select whether to enable OCR by [Enable OCR].</p> <p>Tip</p> <p>If the Forced Encryption setting is enabled, only PDF (Multi) and PDF (Single) are selectable for a file format. For the Forced Encryption function, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p>

	Item name	Description
4	Encryption	<p>Set this to encrypt PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.</p> <p>Encryption Select this if you want to encrypt PDF files.</p> <p>User Password Enter a password for opening encrypted PDF files.</p> <p>Master Password Enter a password for changing the Encrypt PDF setting.</p> <p>Encryption Level Select the desired encryption level.</p> <ul style="list-style-type: none"> • 40-bit RC4 — Select this to set an encryption level to one compatible with Acrobat 3.0, PDF V1.1. • 128-bit RC4 — Select this to set an encryption level to one compatible with Acrobat 5.0, PDF V1.4. • 128-bit AES — Select this to set an encryption level to one compatible with Acrobat 7.0, PDF V1.6. • 256-bit AES — Select this to set an encryption level to one compatible with Acrobat 9.0, PDF V1.7. <p>Authority Select the desired types of authority for Encrypt PDF.</p> <ul style="list-style-type: none"> • Printing — Select this to authorize users to print documents. • Change of Documents — Select this to authorize users to change documents. • Content Copying or Extraction — Select this to authorize users to copy and extract the contents of documents. • Content Extraction for accessibility — Select this to enable the accessibility feature. <p>Tip</p> <ul style="list-style-type: none"> • If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF • The user password and the master password are not set at the factory shipment. • Passwords must be from 1 to 32 one-byte alphanumeric characters. • The user password must differ from the master password. <p>Note</p> <p>These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box if they are not authorized to change the master password. The setting of the encryption will become available when either the user password or the master password is entered. For the details of the encryption setting, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p>

	Item name	Description
5	Digital Signature	<p>Select whether the addition of the digital signature to PDF is enabled or disabled.</p> <p>Tip</p> <p>You cannot select this setting if you have selected a file format except PDF (Multi) and PDF (Single).</p>
6	Destination — Use local folder	Select this to save a received document to the “FILE_SHARE” folder.
7	Destination — Remote 1	<p>Select this check box to save a received document to Remote 1. How you can set this item depends on how you have set Remote 1 up in the [Save as file] submenu under the [Setup] menu.</p> <p>If you have selected [Allow the following network folder to be used as a destination], you can only select [Use Administrator Setting]. The protocol and the network path are displayed below this item.</p> <p>If you have selected [Allow user to select network folder to be used as a destination], select [Use User Setting] and enter the following items to configure the destination to save files.</p> <p>Protocol</p> <p>Select the protocol to be used for uploading a received document to the network folder.</p> <ul style="list-style-type: none"> • SMB — Select this to send a received document to the network folder using the SMB protocol. • FTP — Select this to send a received document to the FTP server. • FTPS — Select this to send a scanned file to the FTP server using FTP over SSL/TLS. • NetWare IPX/SPX — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol. • NetWare TCP/IP — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol. <p>Server Name</p> <p>When you select [FTP] as the protocol, enter the FTP server name or IP address to which a received document will be sent. For example, to send a received document to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box.</p> <p>When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).</p> <p>When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.</p> <p>Port Number(Command)</p> <p>Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number.</p> <p>Network Path</p> <p>When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users/scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”.</p> <p>When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”.</p> <p>When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”.</p>

	Item name	Description
	Destination — Remote 1 (Continues)	<p>Login User Name Enter the login user name to access an SMB server, an FTP server, or a NetWare server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank. You can enter up to 32 alphanumerical characters and symbols other than <, >, “ (double quotation), : (colon) and ; (semicolon). A user name with only a single space is not possible.</p> <p>Password Enter the password to access an SMB server, an FTP server, or a NetWare server, if required.</p> <p>Retype Password Enter the same password again for a confirmation.</p> <p>[Execute] button Tests the connection using the specified network settings to check if the communications can be established.</p>
8	Destination — Remote 2	<p>Select this check box to save a received document to Remote 2. How you can set this item depends on how the 2nd Folder has been set up in the [Save as file] submenu in the [Setup] menu. If Remote 2 does not allow you to specify a network folder, you can only select [Use Administrator Setting]. The protocol and the network path are displayed below this item. If the Remote 2 allows you to specify a network folder, you can specify the network folder settings. See the description of the Remote 1 option for each item.</p>

	Item name	Description
9	File Name	<p>Format Select the format of the file name. Information such as file name, date and time or page number is added according to the selected format.</p> <ul style="list-style-type: none"> • [FileName]-[Date]-[Page] • [FileName]-[Page]-[Date] • [Date]-[FileName]-[Page] • [Date]-[Page]-[Filename] • [Page]-[FileName]-[Date] • [Page]-[Date]-[FileName] • [FileName]_[Date]-[Page] <p>Comment Enter the comment on the file.</p> <p>Date Select how you add “date and time” of the file name selected in [Format].</p> <ul style="list-style-type: none"> • [YYYY][MM][DD][HH][mm][SS] — Year (4 digits), month, day, hour, minute and second are added. • [YY][MM][DD][HH][mm][SS] — Year (2 digits), month, day, hour, minute and second are added. • [YYYY][MM][DD] — Year (4 digits), month, and day are added. • [YY][MM][DD] — Year (2 digits), month, and day are added. • [HH][mm][SS] — Hour, minute and second are added. • [YYYY][MM][DD][HH][mm][SS][mm0] — Year (4 digits), month, day, hour, minute, second and random number (2 digits and “0”) are added. • [None] — Date is not added. <p>Page Select the number of digits of a page number applied to “Page” of the file name selected in [Format] from 3 to 6. [4digits] is set as the default.</p> <p>Sub ID This equipment automatically adds a sub ID (identification number) to the name of a file that you are saving the same file name exists. You can select the number of digits of this sub ID from 4 to 6 or [Auto]. [Auto] is selected by default. If [Auto] is selected, a sub ID (4 to 6 digits, selected randomly) is added according to the status of the file name.</p> <p>Add line information to File Name Select this check box to add the incoming line information (Line 1, Line 2 ^{*1}, and Internet Fax) to the file name. The “Add line information to File Name” check box is [ON] as the default.</p>

^{*1} The 2nd line information is not available for the models without the 2nd line for FAX Unit.

Note

Up to 999 files that are sent from the same sender can be stored in the same destination. If 999 files that are sent from the same sender have already been stored in the specified destination, this equipment will print the received document from the same sender instead of storing them as files.

❑ Setting up Email Setting (Fax/InternetFAX Received Forward)

When you have selected the [Email] agent, you can set the contents of E-mail to be sent. Click the [Email] button to open the following window for setup.

The screenshot shows the 'Email Setting' dialog box. It has a title bar with 'Email Setting' and standard window controls. Below the title bar are 'Save' and 'Cancel' buttons. The main area contains several sections: 'Subject' with a radio button for 'Scanned from (Device Name)[(Template Name)](Date)(Time)' and a text box; 'From Address' with a text box containing 'mfp01@example.com'; 'From Name' with a text box; 'Body' with a large text area; 'File Format' with a dropdown set to 'PDF(Multi)' and an 'Enable OCR' checkbox; 'Encryption' with an 'Encryption' checkbox, password fields for 'User Password' and 'Master Password', an 'Encryption Level' dropdown set to '128-bit AES', and an 'Authority' section with checkboxes for 'Printing', 'Change of Documents', 'Content Copying or Extraction', and 'Content Extraction for accessibility'; 'Digital Signature' with a 'Disable' dropdown; 'File Name' with a 'Format' dropdown set to '[FileName]-[Date]-[Page]', a 'Comment' text box, a 'Date' dropdown set to '[YYYY][MM][DD][H][mm][SS]', a 'Page' dropdown set to '4digits', a 'Sub ID' dropdown set to 'Auto', and a checked 'Add line information to File Name' checkbox; and 'Fragment Message Size' with a 'No Fragmentation' dropdown. Numbered callouts 1 through 11 point to the 'Save' button, 'Cancel' button, 'Subject' section, 'From Address' text box, 'From Name' text box, 'Body' text area, 'File Format' dropdown, 'Encryption' section, 'Digital Signature' dropdown, 'File Name' section, and 'Fragment Message Size' dropdown respectively.

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Subject	This sets the subject of the E-mail documents. Select [Scanned from (Device Name) [(Template Name)](Date)(Time)] to automatically apply the subject, or enter the desired subject in the box. If you manually enter the subject, the subject will be “(Subject) (Date)” by automatically adding the date.
4	From Address	Enter the E-mail address of the sender. When the recipient replies, the message will be sent to this E-mail address.
5	From Name	Enter the sender name of the E-mail document.
6	Body	Enter the body message of the E-mail document. You can enter up to 1000 characters (including spaces).

	Item name	Description
7	File Format	<p>Select the file format to which the received document will be converted.</p> <ul style="list-style-type: none"> • TIFF (Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF (Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF (Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF (Single) — Select this to save scanned images separately as Single-page PDF files. • XPS (Multi) — Select this to save scanned images as a Multi-page XPS file. • XPS (Single) — Select this to save scanned images separately as Single-page XPS files. <p>You can select whether to enable OCR by [Enable OCR].</p> <div> <p>Tip</p> <p>If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, see the reference below:</p> <p>User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> </div>

	Item name	Description
8	Encryption	<p>Set this to encrypt PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.</p> <p>Encryption Select this if you want to encrypt PDF files.</p> <p>User Password Enter a password for opening encrypted PDF files.</p> <p>Master Password Enter a password for changing the Encrypt PDF setting.</p> <p>Encryption Level Select the desired encryption level.</p> <ul style="list-style-type: none"> • 40-bit RC4 — Select this to set an encryption level to one compatible with Acrobat 3.0, PDF V1.1. • 128-bit RC4 — Select this to set an encryption level to one compatible with Acrobat 5.0, PDF V1.4. • 128-bit AES — Select this to set an encryption level to one compatible with Acrobat 7.0, PDF V1.6. • 256-bit AES — Select this to set an encryption level to one compatible with Acrobat 9.0, PDF V1.7. <p>Authority Select the desired types of authority for Encrypt PDF.</p> <ul style="list-style-type: none"> • Printing — Select this to authorize users to print documents. • Change of Documents — Select this to authorize users to change documents. • Content Copying or Extraction — Select this to authorize users to copy and extract the contents of documents. • Content Extraction for accessibility — Select this to enable the accessibility feature. <p>Tip</p> <ul style="list-style-type: none"> • If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF • The user password and the master password are not set at the factory shipment. • Passwords must be from 1 to 32 one-byte alphanumeric characters. • The user password must differ from the master password. <p>Note</p> <p>These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box if they are not authorized to change the master password. The setting of the encryption will become available when either the user password or the master password is entered. For the details of the encryption setting, see the reference below: User Functions - SETTING ITEMS (Admin) - Security - Setting secure PDF</p> <p>Ask the administrator for resetting these passwords.</p>

	Item name	Description
9	Digital Signature	<p>Select whether the addition of the digital signature to PDF is enabled or disabled.</p> <p>Tip</p> <p>You cannot select this setting if you have selected a file format except PDF (Multi) and PDF (Single).</p>
10	File Name	<p>Format</p> <p>Select the format of the file name. Information such as file name, date and time or page number is added according to the selected format.</p> <ul style="list-style-type: none"> • [FileName]-[Date]-[Page] • [FileName]-[Page]-[Date] • [Date]-[FileName]-[Page] • [Date]-[Page]-[Filename] • [Page]-[FileName]-[Date] • [Page]-[Date]-[FileName] • [FileName]_[Date]-[Page] <p>Comment</p> <p>Enter the comment on the file.</p> <p>Date</p> <p>Select how you add “date and time” of the file name selected in [Format].</p> <ul style="list-style-type: none"> • [YYYY][MM][DD][HH][mm][SS] — Year (4 digits), month, day, hour, minute and second are added. • [YY][MM][DD][HH][mm][SS] — Year (2 digits), month, day, hour, minute and second are added. • [YYYY][MM][DD] — Year (4 digits), month, and day are added. • [YY][MM][DD] — Year (2 digits), month, and day are added. • [HH][mm][SS] — Hour, minute and second are added. • [YYYY][MM][DD][HH][mm][SS][mm0] — Year (4 digits), month, day, hour, minute, second and random number (2 digits and “0”) are added. • [None] — Date is not added. <p>Page</p> <p>Select the number of digits of a page number applied to “Page” of the file name selected in [Format] from 3 to 6. [4digits] is set as the default.</p> <p>Sub ID</p> <p>This equipment automatically adds a sub ID (identification number) to the name of a file that you are saving the same file name exists. You can select the number of digits of this sub ID from 4 to 6 or [Auto]. [Auto] is selected by default. If [Auto] is selected, a sub ID (4 to 6 digits, selected randomly) is added according to the status of the file name.</p> <p>Add line information to File Name</p> <p>Select this check box to add the incoming line information (Line 1, Line 2 ^{*1}, and Internet Fax) to the file name. The “Add line information to File Name” check box is [ON] as the default.</p>
11	Fragment Message Size	Select the size of the message fragmentation.

*1 The 2nd line information is not available for the models without the 2nd line for FAX Unit.

❑ Setting up Box Setting (Fax/InternetFAX Received Forward)

When you have selected the [Store to e-Filing] agent, you can set how to store received faxes in the e-Filing box. Click the [Store to e-Filing] button to open the following window for setup.

The screenshot shows a 'Box Setting' dialog box. It contains the following elements:

- 1**: Points to the 'Save' button.
- 2**: Points to the 'Cancel' button.
- 3**: Points to the 'Destination' field.
- 4**: Points to the 'Folder Name' field.
- 5**: Points to the 'Document Name' field.

The 'Box Number' is set to '000 - Public Box'. The 'Document Name' field has a hint: '(Sender)-NNN (NNN is a sequential number)'.

	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Destination	Specify the destination box number for e-Filing. Box Number Enter the Box number where a received document will be stored. Password Enter the password if the specified Box number requires a password. Retype Password Enter the same password again for a confirmation.
4	Folder Name	Enter the name of the folder where a received document will be stored.
5	Document Name	Display how the received document will be named. You cannot change the document name.

■ Meta Scan

The images scanned with the Meta Scan function can have meta data. You can define and register up to 100 extended fields for the meta data.

Tip

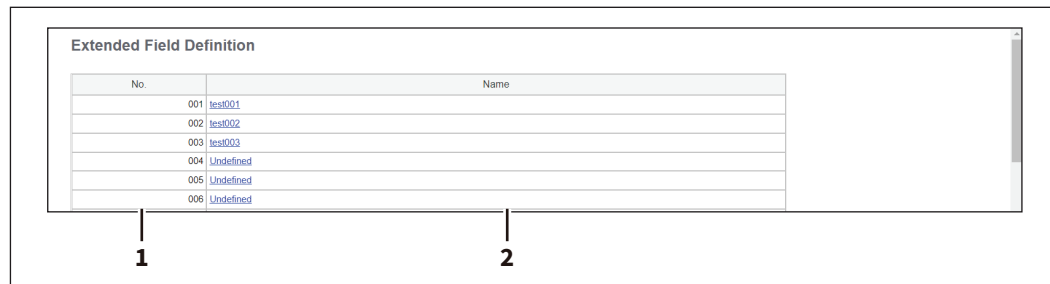
The [Extended Field Definition] submenu can be accessed from the [Registration] menu on the [Administration] page. For how to access it and information on the [Registration] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.300 “[Registration] ([Administration]) Item List”

Note

The Meta Scan Enabler is required to use the Meta Scan function. For the details, contact your distributor or service technician.



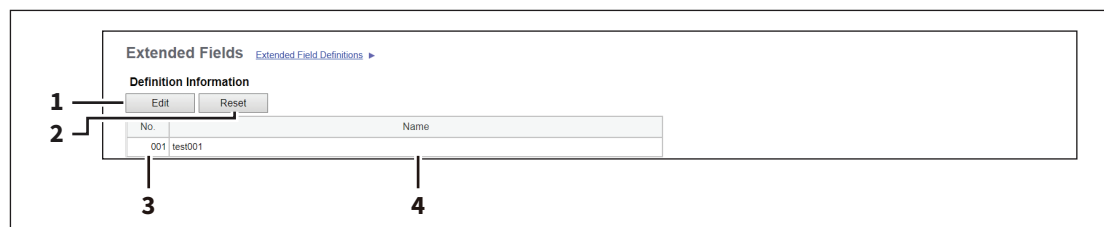
	Item name	Description
1	No.	Displays the extended field definition number.
2	Name	Displays the extended field definition name. Click a registered name to check and edit the existing extended field definition. 📖 P.355 “[Extended Fields] screen” Click [Undefined] to register a new extended field definition. 📖 P.359 “Definition Properties”

❑ [Extended Fields] screen

You can set the information entered from the touch panel when using meta scan.

📖 P.383 “Registering Extended Field Definition”

❑ Setting up Definition Information



	Item name	Description
1	[Edit] button	Allows you to edit the extended field definition. 📖 P.359 “Definition Properties”
2	[Reset] button	Allows you to delete the extended field definition.
3	No.	Displays the extended field definition number.
4	Name	Displays the extended field definition name.

❑ Setting up Extended Field settings

1 Extended Field settings

New									
Field Number	Field Name	Display Name	Mandatory Input	Hidden Attribute	Input Method	Minimum Value	Maximum Value	Default Value	Date
1	FieldName001	DisplayName001	No	No	Numerical	0	999	1	-
2	FieldName002	DisplayName002	No	No	Password	-	-	*****	-
3	FieldName003	DisplayName003	No	No	Date	-	-	-	📅

2 3 4 5 6 7 8 9 10 11

	Item name	Description
1	[New] button	Allows you to add a extended field property. 📖 P.357 “[Extended Fields Properties] screen”
2	Field Number	Displays the extended field property number.
3	Field Name	Displays the extended field property name.
4	Display Name	Displays the caption of the extended field property for the display on the touch panel.
5	Mandatory Input	Displays whether the extended field property is a mandatory entry or not.
6	Hidden Attribute	Displays whether the extended field property is a hidden item on the touch panel.
7	Input Method	Displays the type of the extended field property.
8	Minimum Value	Displays the minimum value for the extended field property.
9	Maximum Value	Displays the maximum value for the extended field property.
10	Default Value	Displays the default value for the extended field property.
11	Date	Displays the default date for the extended field property.

❑ [Extended Fields Properties] screen

You can register up to 25 extended field properties.

📖 P.386 “Registering templates for Meta Scan”

	Item name	Description
1	[Save] button	Creates an extended field property with the entered data.
2	[Cancel] button	Cancels the settings.
3	Field Name	Specify the extended field name.
4	Display	Specify how to display the extended field on the touch panel. Name Enter the caption of the extended field name for the display on the touch panel. You can enter up to 256 characters. Enter the Box number where a received document will be stored. Mandatory Input Select this check box if the extended field is a mandatory entry item. Hidden Attribute Select this check box if the extended field is a hidden item on the touch panel.
5	Input Method *	Select the type of an extended field. <ul style="list-style-type: none"> • Numerical — Select this to create an extended field as an integer value. • Decimal — Select this to create an extended field as a decimal value. • Text — Select this to create an extended field as a character string. • List — Select this to create an extended field as a list selection. • Address — Select this to create an extended field as an address. • Password — Select this to create an extended field as a password. • Date — Select this to create an extended field as a date.

	Item name	Description
6	List Items	<p>Specify list items to be selected for the extended field. The registered list items are listed in the List items. When you register a list item, enter [Name] and [Value], and then click [Add]. If you select an item and click [Move Up], the selected item moves up in the list. Click [Move Down] to move it down. Select an item and click [Delete] to delete an unnecessary item from the list.</p> <p>Name Enter the name of the item.</p> <p>Value Enter a value or text to be applied for the selected item.</p> <p>Note</p> <ul style="list-style-type: none"> • You cannot exceed the total number of characters displayable in the List Items (127). • You cannot use a semicolon in [Name] or [Value].
7	Minimum Length	Specify the minimum number of characters that can be entered in the extended field if the field is a character string.
8	Maximum Length	Specify the maximum number of characters that can be entered in the extended field if the field is a character string.
9	Minimum Value	Specify the minimum numerical value that can be entered in the extended field if the field is a numerical value.
10	Maximum Value	Specify the maximum numerical value that can be entered in the extended field if the field is a numerical value.
11	Default Value	Specify the default value for the extended field.
12	Password	Specify the default password for the extended field if the field is a password.
13	Date	Specify the default date for the extended field if the field is a date.

* The following shows the types and settable items of an extended field for each [Input Method]. (*) is displayed for mandatory setting items.

Input method (Extended field type)	Mandatory setting items	Optional setting items
Numerical value	[Maximum Value], [Minimum Value] Settable value: -999,999,999,999 to 999,999,999,999	[Default Value]
Decimal value	[Maximum Value], [Minimum Value] Settable value: -999,999,999,999.999999 to 999,999,999,999.999999 Contact your service technician if you want to input a value with more than two decimal places.	[Default Value]
Text	[Maximum Length], [Minimum Length] Settable value: 0 to 256	[Default Value]
List	[List Items] You can register up to 30 [List Items]. You can set from 1 to 126 characters in [Name]. You can set from 1 to 126 characters in [Value]. However, the total number of characters set in [Name] and [Value] must be from 2 to 127.	[Default Value] Select from the registered selection items.
Address	None	[Default Value]
Password	None Settable value: 0 to 256	[Default Value]
Date	None	[Default Value]

❑ Definition Properties

	Item name	Description
1	[Save] button	Creates an extended field definition with the entered data.
2	[Cancel] button	Cancels adding new.
3	Number	Displays the extended field definition number.
4	Name	Specify the extended field definition name.
5	XML Format File	Select the XML format file for meta data.

■ XML Format File


You can import and delete the XML format file.

	Item name	Description
1	Import XML Format File	Import the XML format file. <ul style="list-style-type: none"> • [Choose File] — Select the XML format file. • [Import] — Import the selected XML format file.
2	Delete XML Format File	The list shows the name, size, and date of the imported XML format file. <ul style="list-style-type: none"> • [Delete] — Delete the XML format file selected in the list.

[Application] Item List

Users who have been granted administrator authority in access policy mode can access the [Application] menu from the [Administration] page.

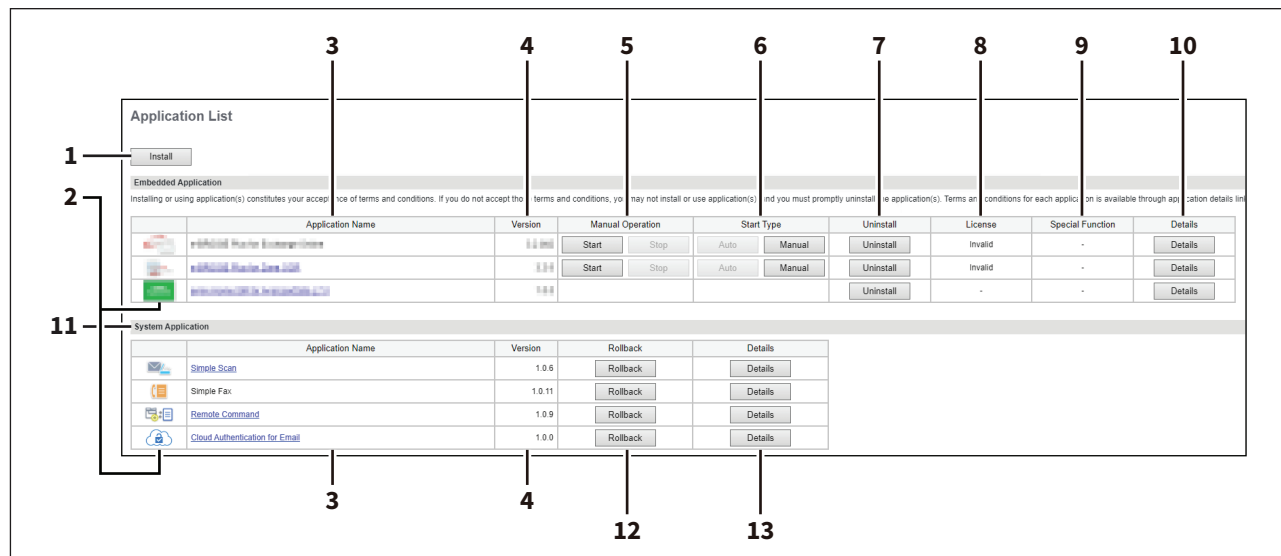
See the following for details on accessing.

 P.14 “Access Policy Mode”

■ Application List





Displays the list of installed applications.

You can manage operations for each embedded application such as opening/closing, setting the startup method, and uninstalling/installing. You can also install the system application so that you can check information about it and roll it back to the previous one.



	Item name	Description
1	[Install] button	<p>Installs the embedded application and the system application. Click this button to display the installation page for the application. You can specify the file name for the distribution package on this page, and then install.</p> <p>When you install the system application, follow instructions to select one that you want to install and agree to the end user license agreement.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> Tip <ul style="list-style-type: none"> Installing or using application(s) constitutes your acceptance of the terms and conditions. If you do not accept those terms and conditions, uninstall the application(s). Terms and conditions for each application is available through application details link. You need to acquire the application's distribution package in advance. When installing multiple application packages, install them one at a time. If a message appears to tell the framework version is old when you install an application, update the system of this equipment. For details, contact your service technician. </div>
2	Application Icon	Displays the application icon.
3	Application Name	<p>Displays the application name. You can click the name if the application allows you to change the settings. When you click it, the setting page opens.</p>
4	Version	Displays the application version.

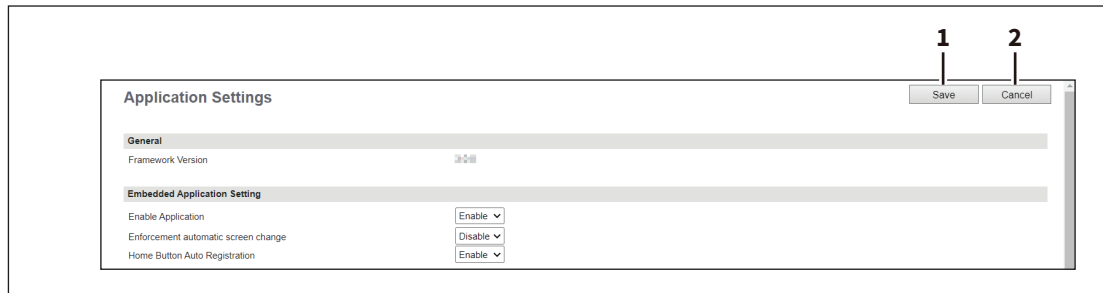
	Item name	Description
5	Manual Operation	<p>Allows you to start and stop the application manually. This is displayed only when the application package includes the background application.</p> <ul style="list-style-type: none"> • Start — Select this to start the application. • Stop — Select this to close the application.
6	Start Type	<p>Changes the applications startup method. This is displayed only when the application package includes the background application.</p> <ul style="list-style-type: none"> • Auto — Select this to start the application automatically after it has been installed or the MFP starts. • Manual — Select this to start the application manually.
7	Uninstall	<p>Uninstalls the application. Click this button to display the uninstallation page for the application.</p>
8	License	<p>Displays the installation status of license files to utilize applications.</p> <ul style="list-style-type: none"> • - — Installation of a license file is not necessary. • Invalid — An application cannot be used since its license file is not installed. Contact your service technician if you want to use an application with an invalid license. • Valid — An application can be used since its license file is installed.
9	Special Function	<p>Contact your service technician or representative for details on Special Function.</p>

	Item name	Description
10	Details	<p>Opens the screen that shows detailed information and settings of the application.</p> <ul style="list-style-type: none"> You can set the department or user authentication at the startup of each application. Click [Details] to open [Details] screen, select [Enable] at [Authentication], and click [Save], so that the authentication screen appears at the startup of the application. Select [Disable] and click [Save] not to show the authentication screen. Click [Cancel] to cancel the setting. This [Authentication] setting works at the next startup of the application. It does not appear for the background application. You can enable or disable the connection to the external devices for the embedded application that has the communication function. When [Enable] is selected at [External Device Connection], the embedded application is ready to connect to the external devices. When [Disable] is selected, it is not ready for connection. Click [Save] after changing the setting or [Cancel] to discard it. [Use of external USB Device] shows whether the embedded application can use external USB devices. At [Display Setting] under [Status Message] you can select whether to enable or disable the appearance of the status message and icon that the embedded application shows. At [Display Position] you can select the position where the status message and icon appear on the touch panel. These settings take priority over the settings common to the status messages that you set under [Administration] > [Setup] > [General]. When you select [Common] here, the common settings take over these ones you set here.  P.116 “Status Message” If the application can make use the received fax images, [Use Received Document] reads “Used”. If not possible, nothing appears for this function.  P.180 “Received Forward Setting for Application” <p>Tip</p> <ul style="list-style-type: none"> To authenticate users at the startup of the embedded application, enable “User Authentication According To Function”.  P.240 “Setting up User Authentication Setting” You cannot change [Authentication] for embedded applications that require the authentication and embedded applications that do not have the authentication setting. The contents of the license agreement are displayed by clicking “Display” in License Agreement. “Language” is displayed when the embedded application contains the language pack.
11	System Application	<p>Displays the system applications installed in the equipment.</p> <p>Tip</p> <p>You need to set up [Cloud Authentication for Email] at [Administration] > [Setup] > [Network] > [POP3 Client] > [Authentication] to use it. You can open the setting screen by clicking its name that appears at [Authentication] or the [System Application] list.  P.158 “Setting up POP3 Client”</p>

	Item name	Description
12	Rollback	Rolls back the installed system application to the previous one. When you click the button, the confirmation messages appear. Follow instructions and click the button.
13	Details	Opens the screen that shows detailed information and settings of the system application.

■ Application Settings

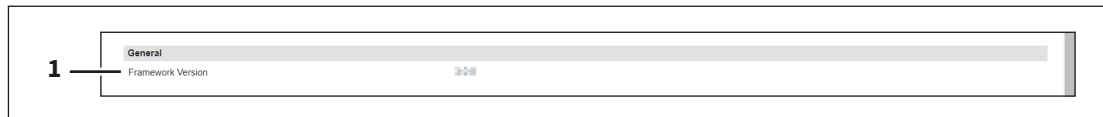
You can perform operations such as application settings, proxy settings, and debugging levels for all of the applications that are installed.



	Item name	Description
1	[Save] button	Saves changes made to the settings.
2	[Cancel] button	Cancels changes made to the settings.

□ General

You can check the framework version.



	Item name	Description
1	Framework Version	Displays the framework version.

❑ Embedded Application Setting

You can enable or disable embedded application functions.

	Item name	Description
1	Enable Application	Sets the application to enable/disable. <ul style="list-style-type: none">• Enable — Select this to enable application.• Disable — You cannot install, uninstall, start, or make settings for the application on the [Application List] screen. Also, you cannot start the application from the MFP's touch panel. <div>Tip</div> <p>You can always install, roll back and make settings of the system applications without being affected by this setting.</p>
2	Enforcement automatic screen change	When a warning occurs during the Home application, set whether or not to automatically switch to the [JOB STATUS] screen.
3	Home Button Auto Registration	Sets whether or not automatically to register a button of an application on the Home screen when it is installed.

❑ Proxy Setting

You can set a proxy for the application.

	Item name	Description
1	Host Name	Enter a host name for the proxy server.
2	Port Number	Enter a port number for the proxy server.
3	Bypass proxy settings for these addresses	Enter URLs that proxy server is not used by dividing them using semicolons (;).
4	Account ID	Enter the account ID of the proxy server.
5	Password	Enter the password of the proxy server.

Tip

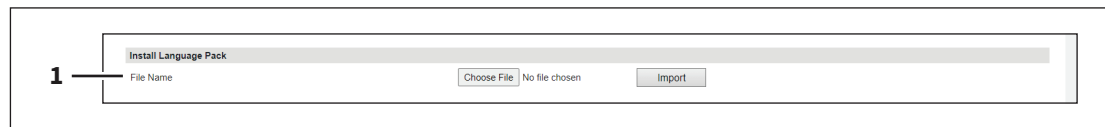
The proxy settings are basically common to the Embedded Web Browser, Idle Screen, and Application functions. If you change them for one function, they change accordingly for others.

📖 P.233 “Setting up Proxy Setting”

📖 P.285 “Proxy Setting”

❑ Install Language Pack

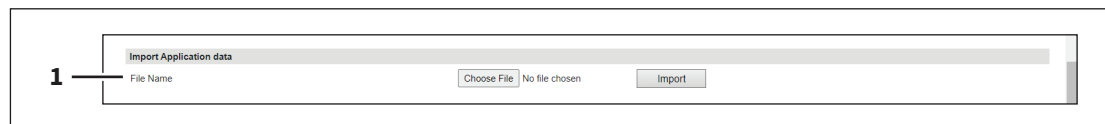
You can install the language packs for the applications.



	Item name	Description
1	File Name	Select the language pack file that you install. <ul style="list-style-type: none">• [Choose File] button — Allows you to select the language pack file.• [Import] button — Imports the selected language pack file.

❑ Import Application Data

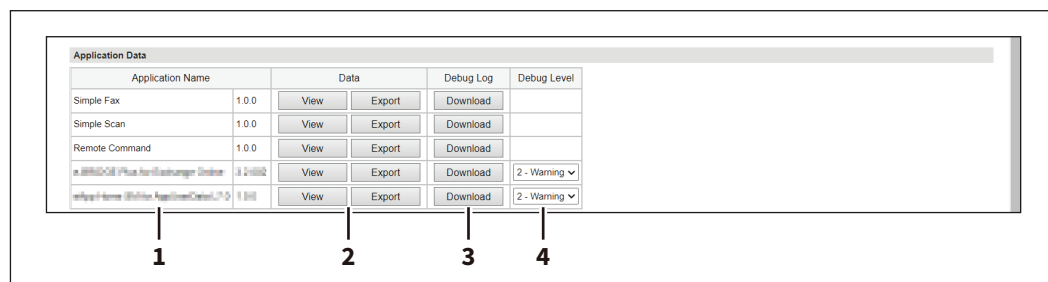
You can deliver the application data files.



	Item name	Description
1	File Name	Select the application data file that you deliver. <ul style="list-style-type: none">• [Choose File] button — Allows you to select the application data file.• [Import] button — Imports the selected application data file for delivery.

❑ Application Data

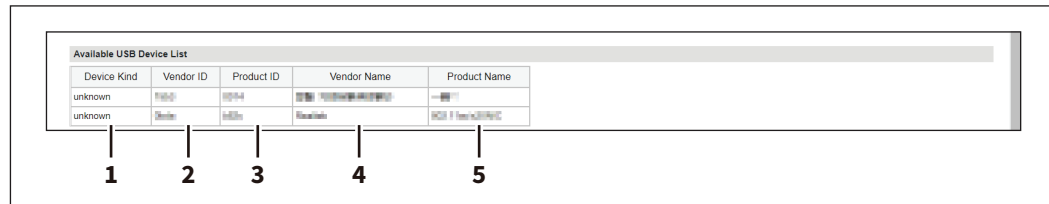
You can collect and check the data files of the applications, and collect the debug logs of the applications.



	Item name	Description
1	Application Name	Shows the application name.
2	Data	Collects the data files of the application so that you can check them. <ul style="list-style-type: none">• [View] button — Shows information of the application data files.• [Export] button — Exports the application data files.
3	Debug Log	Collects the debug log files of the applications. <ul style="list-style-type: none">• [Download] — Downloads the debug log files.
4	Debug Level	Select the debug level of the applications. When you click [Save], the confirmation message appears.

❑ Available USB Device List

You can check information about external USB devices that can work with applications.



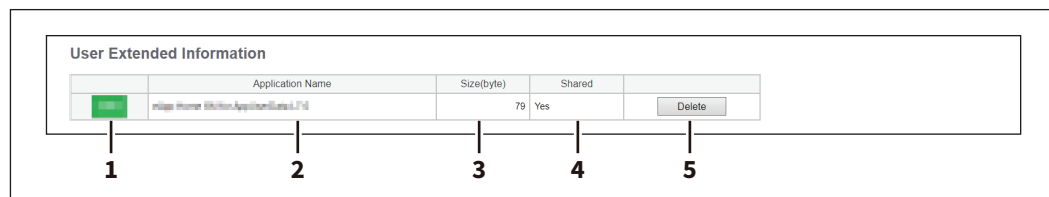
	Item name	Description
1	Device Kind	Displays the kind of the USB device.
2	Vendor ID	Displays the vendor ID of the USB device.
3	Product ID	Displays the product ID of the USB device.
4	Vendor Name	Displays the vendor name of the USB device.
5	Product Name	Displays the product name of the USB device.

Note

USB hubs do not work stably.

■ User Extended Information

You can check and delete the user extended information file of the application.

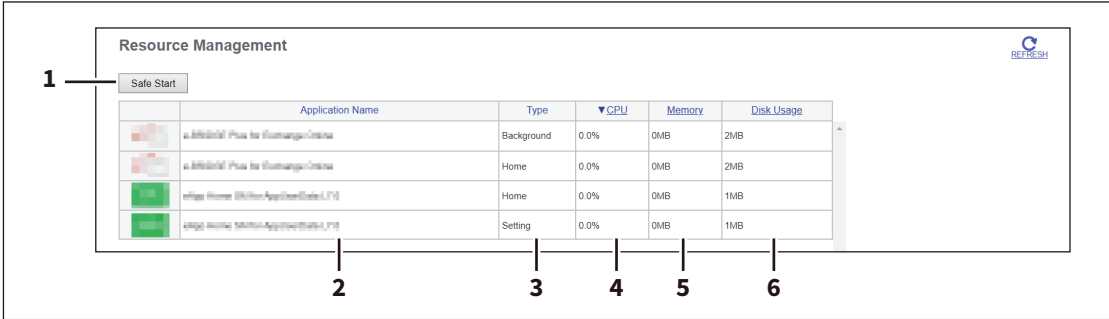


	Item name	Description
1	Application Icon	Shows the icon of the application.
2	Application Name	Shows the name of the application.
3	Size(byte)	Shows the size (byte) of the user extended information file.
4	Shared	Shows whether the user extended information includes the shared information. <ul style="list-style-type: none">• [Yes] — Shows the message when you delete the file that Includes the shared information.• [No] — Shows the message when you delete the file that Includes no shared information.
5	Delete	Deletes the user extended information file.

Resource Management

You can monitor the resources of the running applications. When you click a resource name [CPU], [Memory], or [Disk Usage], the clicked resource is sorted and displayed in ascending or descending order. When you click [REFRESH], the list shows the latest information.

If any applications use the resources extremely, you can restart the equipment with all applications disabled, so that you can cope with the extreme resource usage.




	Item name	Description
1	Safe Start	Restarts the equipment with all applications disabled. When you click [Safe Start], the confirmation message appears, so that you can click [OK] to execute the safe start operation. Click [Cancel] to stop the operation.
2	Application Name	Shows the icon and name of the application.
3	Type	Shows the type of the application.
4	CPU	Shows the CPU usage of the application.
5	Memory	Shows the memory usage of the application.
6	Disk Usage	Shows the disk usage of the application.

[License] Item List

Note

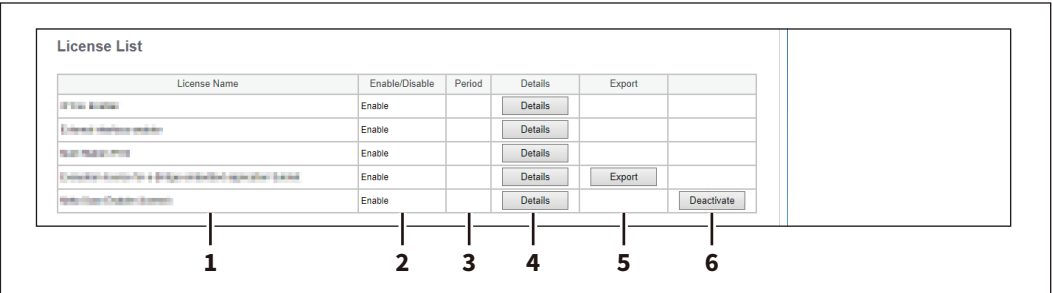
- Before you install licenses, make sure that the equipment is not in operation.
- If you have any unclear issues about licenses, contact your service technician or representative.

Tip

Users who are granted administrator privileges in access policy mode can access the [License] menu from the [Administration] page. For how to access it, see the reference below:
 P.14 “Access Policy Mode”

License List

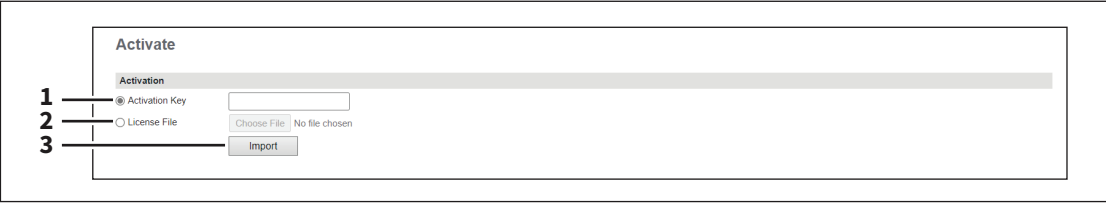
You can check the list of the installed licenses.



	Item name	Description
1	License Name	Displays the license name.
2	Enable/Disable	Displays the status (Enable or Disable) of the license.
3	Period	Displays the validation period of the license.
4	Details	Displays the details on the license.
5	Export	Exports the license file.
6	Deactivate	Deactivates the license.

Activate

You can activate the license with the activation key or the license file.



	Item name	Description
1	Activation Key	Enter the acquired activation key to activate the license.
2	License File	Click [Choose File] and select the license file to activate the license.
3	Import	Imports the selected license file.

[My Account]

[My Account] Overview	370
[My Account] Item list	370

[My Account] Overview

The [My Account] page is displayed if [User Authentication] is enabled on the [Administration] page under [Security] > [Authentication] > [User Authentication Setting].

It displays the account information of the user who is accessing TopAccess. Also, you can change the display language and keyboard layout on the touch panel.


■ [My Account] Item list

The screenshot shows the [My Account] page with the following elements labeled by callouts:

- 1**: Save button
- 2**: Cancel button
- 3**: Change Password button
- 4**: Home Screen button
- 5**: Delete Fingerprint button
- 6**: Sync button
- 7**: Delete Account button
- 8**: Delete EWB History button
- 9**: User Name (User001)
- 10**: Domain Name/LDAP Server
- 11**: Role Assignment (User)
- 12**: Group Assignment
- 13**: Email Address
- 14**: Home Directory
- 15**: Department Number
- 16**: PanelUI Language (English(US))
- 17**: PanelUI Keyboard Display (ON)
- 18**: PanelUI Keyboard Layout (QWERTY)
- 19**: Color Quota Setting (ON, 100)
- 19**: Black Quota Setting (ON, 500)
- 20**: Total Counter table

	Full Color	Twin/ Mono Color	Black	Total
Copy	0	0	0	0
Fax	0	0	0	0
Printer	0	0	0	0
List	0	0	0	0
Total	0	0	0	0

	Item name	Description
1	[Save] button	Saves the content of the account.
2	[Cancel] button	Cancels the operation.
3	[Change Password] button	Changes the password of the user who is accessing TopAccess. 📖 P.372 “[Change Password] screen”
4	[Home Screen] button	Click the [Home] button on the control panel and perform the settings on the Home screen. On the [My Account] page, set the Home screen of the user who is accessing TopAccess. 📖 P.372 “[Home Screen setting] screen”
5	[Delete Fingerprint] button	Contact your service technician for details.
6	[Sync] button	When this printer is set as the primary MFP in [Shared Setting] from [Setting up User Authentication Setting], you can synchronize the user information on the printer with other secondary MFPs. 📖 P.97 “[Shared Settings] Item list <access policy mode>” 📖 P.240 “Setting up User Authentication Setting”

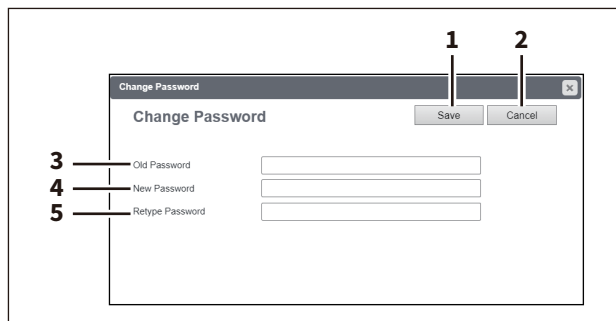
	Item name	Description
7	[Delete Account] button	Deletes user's own account if a user has logged in successfully. This button is not available in the following situations: <ul style="list-style-type: none"> • Built-in users • External users who are not registered locally • When users are prohibited from deleting their own account: [Delete Own Account] is set to [Disable] at [User Authentication Setting].  P.240 "Setting up User Authentication Setting" • When this equipment is configured as a secondary device for the shared user management: [Shared User Management] is set to [Enable(Secondary)] at [User Authentication Setting].  P.240 "Setting up User Authentication Setting"
8	[Delete EWB History] button	Deletes user's own EWB history if a user has logged in successfully. This function is not available for built-in users.
9	User Name	Displays the name of the user who is accessing TopAccess.
10	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user who is accessing TopAccess.
11	Role Assignment	Displays the role assigned to the user who is accessing TopAccess. Click the [Confirm Permission] button to display the [Confirm Permission] screen and check the detailed role information.  P.376 "[Confirm Permission] screen"
12	Group Assignment	Displays the group assigned to the user who is accessing TopAccess.
13	Email Address	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the Email address of the user or select it from the address book. You can enter up to 192 half-width alphanumerical characters and symbols.
14	Home Directory	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the network path to the home directory. You can enter up to 128 half-width alphanumerical characters and symbols. For example, enter "\\192.168.1.1\users\name" to specify the folder called "users\name" on the computer whose server address is "192.168.1.1".
15	Department Number	Displays the department number registered by the user who is accessing TopAccess.
16	PanelUI Language	Select the display language for the touch panel.
17	PanelUI Keyboard Display	Select whether to display the soft-keyboard when entering characters with the touch panel.
18	PanelUI Keyboard Layout	Select the keyboard layout on the touch panel.
19	Quota Setting	You can specify this item if you have selected "Job Quota" for "Quota Setting". <ul style="list-style-type: none"> • OFF — Not setting quota. • ON — Setting quota.  P.71 "[Quota Setting] screen <access policy mode>"
	Quota	Displays the quota amount. This value decreases according to the weight in [Quota Setting], and output is restricted when the value becomes 0.00. The quota can be manually modified to any amount.
	Default Quota	Enter the default amount to assign to users. You can enter a value up to 99,999,999.99.
20	Total Counter	Displays the total counter of the user who is accessing TopAccess.

❑ [Change Password] screen

Changes the password of the user who is accessing TopAccess. You can change the password only if [MFP Local Authentication] is selected for the authentication method.

Note

The changed password will be valid from the next log-in on.

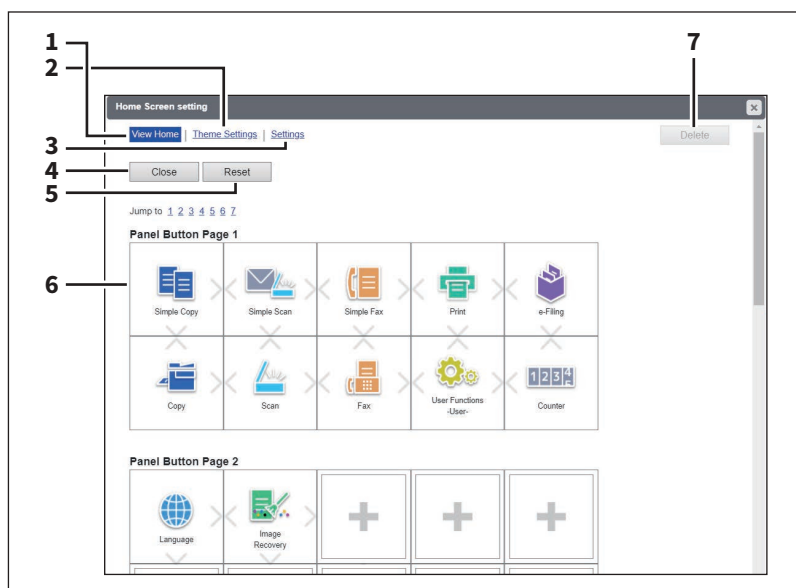


	Item name	Description
1	[Save] button	Saves the password changes.
2	[Cancel] button	Cancels the operation.
3	Old Password	Enter the current password.
4	New Password	Enter the new password.
5	Retype Password	Enter the same password again for a confirmation.

❑ [Home Screen setting] screen

You can set the Home screen of the user who is accessing TopAccess.

The Home screen is displayed by pressing the [Home] button on the control panel. You can register frequently used templates and folders, and External Interface Enabler shortcuts.

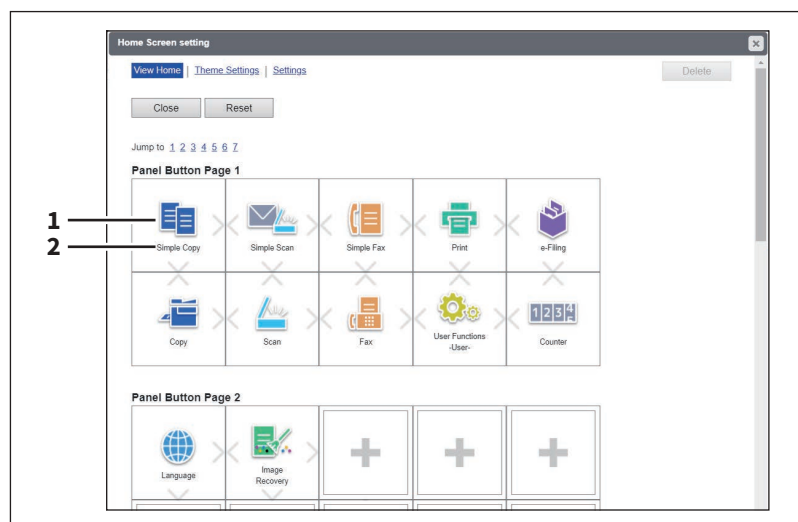


	Item name	Description
1	View Home	Displays the settings for the home screen. P.373 "[View Home] screen"

	Item name	Description
2	Theme Settings	Specify the theme of the home screen. P.374 “[Theme Settings] screen”
3	Settings	Specify the background, button size, and transparency of the home screen. P.375 “[Settings] screen”
4	[Close] button	Closes the [Menu Setting] screen.
5	[Reset] button	Deletes the current settings.
6	Panel button list	Displays a list of panel buttons you can select for the home. Select the panel buttons you want to use. Tip In the Home settings, you can register 64 types.
7	[Delete] button	Deletes the selected menu settings.

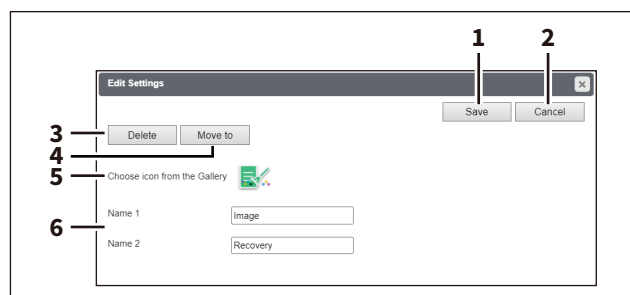
❏ [View Home] screen

You can edit the settings for the home screen.



	Item name	Description
1	Button Icon	Displays button icons. You can register new buttons when you click the Undefined icon.
2	Name	Displays the function names.

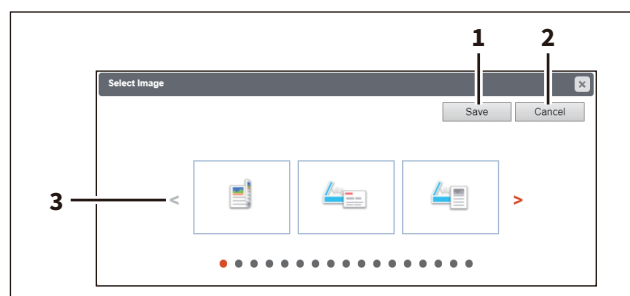
[Edit Settings] screen



	Item name	Description
1	[Save] button	Stores the icon settings.

	Item name	Description
2	[Cancel] button	Cancels the operation.
3	[Delete] button	Deletes the icon settings.
4	[Move to] button	Moves the icon to another position.
5	Choose icon from the Gallery	Select the icon for the image. P.374 “[Select Image] screen”
6	Name1/Name2	Enter the button name.

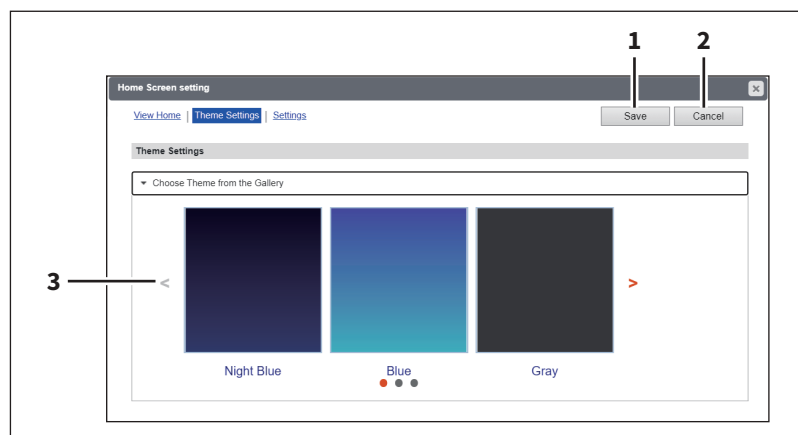
[Select Image] screen



	Item name	Description
1	[Save] button	Stores the icon settings.
2	[Cancel] button	Cancels the operation.
3	Select Image	Select the icon for the image.

[Theme Settings] screen

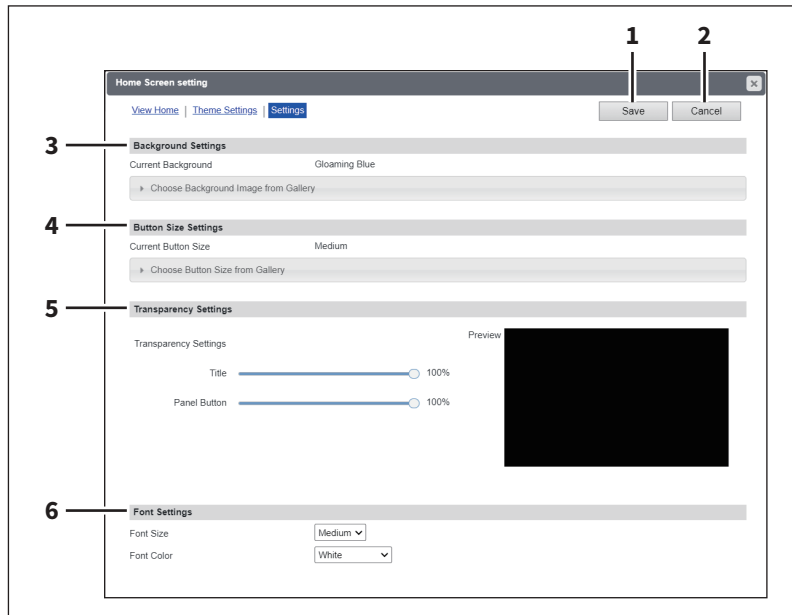
You can specify the theme of the home screen.



	Item name	Description
1	Save	Saves the theme settings.
2	Cancel	Cancels the operation.
3	Choose Theme from the Gallery	Specify the theme.

❏ [Settings] screen

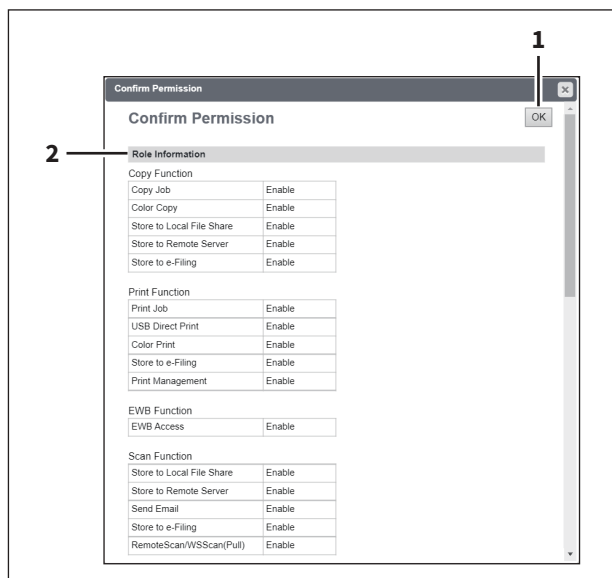
You can specify the background, button size, and transparency of the home screen.



	Item name	Description
1	Save	Saves the settings.
2	Cancel	Cancels the operation.
3	Background Settings	Specify the background of the home screen. You can select the background design from a list if you select [Edit Background Image from Gallery] at [Current Background].
4	Button Size Settings	Specify the button size. You can select the button size from a list if you select [Edit Button Size from Gallery] at [Current Button Size].
5	Transparency Settings	Specify the transparency of the home screen. <ul style="list-style-type: none">• Title — You can specify the transparency of the title bar.• Panel Button — You can specify the transparency of the buttons.
6	Font Settings	Specify the font used on the home screen. <ul style="list-style-type: none">• Font Size — You can specify the font size.• Font Color — You can specify the font color.

❑ [Confirm Permission] screen

You can display granted permissions of the user who is accessing TopAccess.



	Item name	Description
1	[OK] button	Closes the [Confirm Permission] screen.
2	Role Information	The role information assigned to the user who is accessing TopAccess is displayed.

Functional Setups

Setting up Meta Scan Function	378
Procedure for using Meta Scan	378
Checking Meta Scan Enabler	379
Editing XML format file	379
Registering XML format file	383
Registering Extended Field Definition	383
Registering templates for Meta Scan	386
Meta Scan	389
Checking logs of Meta Scan	389
Setting Multi Station Print	390
Procedure for Multi Station Print	390
Procedure for Multi Station Print (Only in One Equipment Unit)	391
Checking the Multi Station Print Enabler	391
Setting Home Data Synchronization	392
Procedure for Home Data Synchronization	392
Using the Attribute of the External Authentication as a Role of the MFP	393
Exporting the role information setting file	393
Defining the role information setting file	393
Importing the role information setting file.....	394
Enabling the role base access setting.....	394
Setting up Email.....	395
Procedure for Email Setting	395
Installing Certificates	396
Installing a device certificate	396
Creating/Exporting a client certificate.....	403
Installing CA certificate.....	405

Setting up Meta Scan Function

The Meta Scan is a function to attach information (meta data) generated within the device to scanned images. The attached meta data can be processed by workflow servers or other means to supplement the scanned image. To use Meta Scan, select [E-MAIL], [Save as file] and [Save to USB Media] agents of Meta Scan for templates and register them.

Meta data is managed by an XML file which defines the scheme to store the information.

This section describes the data structure using the XML file <defaultForm3.xml> registered as the default as an example.

The default XML file consists of two data areas; the “basic data area” and “extended data area”.

The “basic data area” records device information, scan parameters, and user information, while the “extended data area” records information entered by the user on the touch panel (maximum 25 items) when running Meta Scan.

The user can create fields in “extended data area” to store information entered from the touch panel under [Extended Field Definition] > [Extended Field Properties].

When using applications that interact with Meta Scan, follow the instructions of the application vendor to set the XML format file and the extended field.

■ Procedure for using Meta Scan

Setup

	Operation	Description	Reference
1	Checking the Meta Scan option	Check whether the Meta Scan option can be used with your equipment.	📖 P.379 “Checking Meta Scan Enabler”
2	Editing the XML format file	If necessary, edit the XML format file for meta data.	📖 P.379 “Editing XML format file”
3	Registering an XML format file	Register an XML format file for meta data.	📖 P.383 “Registering XML format file”
4	Registering an extended field definition	If necessary, register an extended field definition.	📖 P.383 “Registering Extended Field Definition”
5	Registering a template for Meta Scan	Register a template for Meta Scan.	📖 P.386 “Registering templates for Meta Scan”

Operation

	Operation	Description	Reference
1	Meta Scan	Perform a meta scan using a template for Meta Scan.	Template - USING TEMPLATE BUTTONS - Recalling Templates - Using templates
2	Checking Meta Scan logs	Check the scan log to confirm if meta data has been correctly created.	📖 P.389 “Checking logs of Meta Scan” Information About Equipment - Information About Equipment - Confirming Job Statuses of Printing/ Copying/Scanning/Faxing - Confirming job history

■ Checking Meta Scan Enabler

The Meta Scan Enabler is required to use the Meta Scan function. For the details, contact your distributor or service technician.

You can check whether the Meta Scan option is set on your equipment as follows.

Meta Scan function is available if [Meta scan enabler] is registered under [Admin] > [General] > [License Management].

Note

This function is available only for some models.

■ Editing XML format file

Edit XML format files in accordance with the applications that interact with Meta Scan. You can define variables in the XML format file and the variables are replaced with the corresponding information (meta scan) during the Meta Scan operation.

Tip

Enter variables in XML format files using the \${variable name} format.

□ Variables of XML format files

Variables that can be defined in XML format files are shown below.

Tip

You can use variables for the subject of E-mail, the file name of Meta Scan image files, and the file name of meta data.

Variable (\${variable name})	Data to be stored	Value
\${MANUFACT}	Manufacturer name	TOSHIBA
\${MODEL}	Model name	string
\${FWVER}	Firmware version	string
\${SERIAL}	Serial number for machine	string
\${LOCATION}	Location set from TopAccess	string
\${CONTACT}	Contact information set from TopAccess	string
\${CONTACTTEL}	Contact telephone number set from TopAccess	string
\${IP}	IP address	string
\${IPV6}	IPv6 address	string
\${NETBIOSNAME}	NetBIOS name	string
\${FQDN}	Fully Qualified Domain Name	string
\${RESOLUTION}	Scan resolution	HHHxVVdpi
\${FILEFORMAT}	File format	MultipleTIFF singleTIFF MultiplePDF singlePDF MultipleSLIMPDF singleSLIMPDF MultipleXPS singleXPS JPEG MultiplePDF/A singlePDF/A

Variable (\${variable name})	Data to be stored	Value
\${COLORMODE}	Color mode	BLACK GRAY SCALE FULLCOLOR AUTOCOLOR
\${NUMFILE}	Number of image files	string
\${PAGES}	Number of pages	string
\${PATH} *1 *2	Save path of the image file	string
\${FILE} *2	Image file name	string
\${MYEMAIL}	Sender email address	string
\${DATE}	Scanned date	YYYY-MM-DD
\${YEAR}	Scanned year	YYYY
\${MONTH}	Scanned month	MM
\${DAY}	Scanned day	DD
\${TIME}	Scanned time	HH:MM:DD.mmmTZ D *3
\${USER}	Login user name	string
\${DOMAIN}	Login user's domain name	string
\${DEPTCODE}	Login department code	string
\${DEPTNAME}	Login department name	string
\${TEMPGROUPNO}	Folder number where the template buttons are registered	string
\${TEMPGROUPNAME}	Folder name where the template buttons are registered	string
\${TEMPNO}	Template number	string
\${TEMPNAME}	Template name	string
\${FIELDNAME} *4	Extended field name	string
\${FIELDNAME} *4	Extended field name	string

*1 It cannot be used for the subject of E-mail.

*2 It cannot be used for the file name of image files or the file name of meta data.

*3 TZD is Time zone.

*4 A field number (from 1 to 25) comes at "n". For details, refer to the next chapter.

❑ Default XML file format

Contents of the default XML format file <defaultForm3.xml> registered in this equipment are shown below. XML format files must be in the UTF-8 XML format. During the Meta Scan operation, the equipment stores information corresponding to the variable in each field of the XML format file and attaches it as meta data in the XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- metadata version 3.1 -->
<mfp_metadata>
<metadata_version>
<major>3</major>
<minor>1</minor>
</metadata_version>
<device_info>
<ip_address>${IP}</ip_address>
<ipv6_address>${IPV6}</ipv6_address>
<fqdn>${FQDN}</fqdn>
```



```

<netbios_name>${NETBIOSNAME}</netbios_name>
<location>${LOCATION}</location>
<contact>${CONTACT}</contact>
<contact_tel>${CONTACTTEL}</contact_tel>
<FW_version>${FWVER}</FW_version>
<manufacture>${MANUFACT}</manufacture>
<model>${MODEL}</model>
<serial>${SERIAL}</serial>
<!-- deprecated tag start -->
<host_name>${NETBIOSNAME}</host_name>
<tempt_file_ver>1.0</tempt_file_ver>
<!-- deprecated tag end -->
</device_info>
<scan_info>
<template >
<template_group_no>${TEMPGROUPNO}</template_group_no>
<template_group_name>${TEMPGROUPNAME}</template_group_name>
<template_group_user></template_group_user>
<template_no>${TEMPNO}</template_no>
<template_name>${TEMPNAME}</template_name>
<template_user></template_user>
</template >
<scanned_date>${YEAR}-${MONTH}-${DAY}</scanned_date>
<scanned_time>${DATE}T${TIME}</scanned_time>
<color_mode>${COLORMODE}</color_mode>
<resolution>${RESOLUTION}</resolution>
<file_format>${FILEFORMAT}</file_format>
<no_of_files>${NUMFILE}</no_of_files>
<no_of_pages>${PAGES}</no_of_pages>
<file_path>${PATH}</file_path>
<file_name>${FILE}</file_name>
<sender_email>${MYEMAIL}</sender_email>
<!-- deprecated tag start -->
<workflow>${TEMPGROUPNAME} ${TEMPNAME}</workflow>
<!-- deprecated tag end -->
</scan_info>
<user_info>
<user_id>${USER}</user_id>
<user_domain>${DOMAIN}</user_domain>
<dept_code>${DEPTCODE}</dept_code>
<dept_name>${DEPTNAME}</dept_name>
<!-- deprecated tag start -->
<user_email>${MYEMAIL}</user_email>
<!-- deprecated tag end -->
</user_info>
<user_input>
<field1 name="${FIELDNAME1}">${VALUE1}</field1>
<field2 name="${FIELDNAME2}">${VALUE2}</field2>
<field3 name="${FIELDNAME3}">${VALUE3}</field3>
<field4 name="${FIELDNAME4}">${VALUE4}</field4>
<field5 name="${FIELDNAME5}">${VALUE5}</field5>
<field6 name="${FIELDNAME6}">${VALUE6}</field6>
<field7 name="${FIELDNAME7}">${VALUE7}</field7>
<field8 name="${FIELDNAME8}">${VALUE8}</field8>
<field9 name="${FIELDNAME9}">${VALUE9}</field9>
<field10 name="${FIELDNAME10}">${VALUE10}</field10>
<field11 name="${FIELDNAME11}">${VALUE11}</field11>
<field12 name="${FIELDNAME12}">${VALUE12}</field12>
<field13 name="${FIELDNAME13}">${VALUE13}</field13>
<field14 name="${FIELDNAME14}">${VALUE14}</field14>

```

```

<field15 name="{FIELDNAME15}">{VALUE15}</field15>
<field16 name="{FIELDNAME16}">{VALUE16}</field16>
<field17 name="{FIELDNAME17}">{VALUE17}</field17>
<field18 name="{FIELDNAME18}">{VALUE18}</field18>
<field19 name="{FIELDNAME19}">{VALUE19}</field19>
<field20 name="{FIELDNAME20}">{VALUE20}</field20>
<field21 name="{FIELDNAME21}">{VALUE21}</field21>
<field22 name="{FIELDNAME22}">{VALUE22}</field22>
<field23 name="{FIELDNAME23}">{VALUE23}</field23>
<field24 name="{FIELDNAME24}">{VALUE24}</field24>
<field25 name="{FIELDNAME25}">{VALUE25}</field25>
</user_input>
</mfp_metadata>

```

❏ Setting for saving meta data

You can specify the location to save meta data and the file name by adding the following elements to the XML file.

Specifying the location to save meta data

Protocol	Format
SMB	<metadata_file_path>file://server name/path/</metadata_file_path>
FTP	<metadata_file_path>ftp://server name/path/</metadata_file_path>
FTPS	<metadata_file_path>ftps://server name/path/</metadata_file_path>
NetWare (Binary mode)	<metadata_file_path>server name/path/</metadata_file_path>
NetWare (NDS mode)	<metadata_file_path>Tree/Context/file_share/</metadata_file_path>

Example:

Protocol: SMB

External server: 192.168.1.1

Save folder: metadata

Format: <metadata_file_path>file://192.168.1.1/metadata/</metadata_file_path>

Note

Ensure that the protocol is the same as the protocol for saving the Meta Scan image file.

You can check the protocol for saving the Meta Scan image file in [Destination] of Save as file Setting, which is set for the template.

Specifying a meta data file name

<metadata_file_name>file name.xml</metadata_file_name>

Example:

File name: Sample_MetaData.xml

Format: <metadata_file_name>Sample_MetaData.xml </metadata_file_name>

Tip

You can use an XML format file variable for the file name of the meta data.

Example using the date variables ({DATE}):

<metadata_file_name>Sample_MetaData_{DATE}.xml </metadata_file_name>

📖 P.383 “Registering Extended Field Definition”

For more information on variables, see the following:

📖 P.379 “Variables of XML format files”

■ Registering XML format file

You can select the XML format file when registering the definitions of extended fields.

📖 P.383 “Registering Extended Field Definition”

When using applications that interact with Meta Scan, follow the instructions of the application vendor to set the XML format file and the extended field.

Tip

You can register up to 99 XML format files.

■ Registering Extended Field Definition

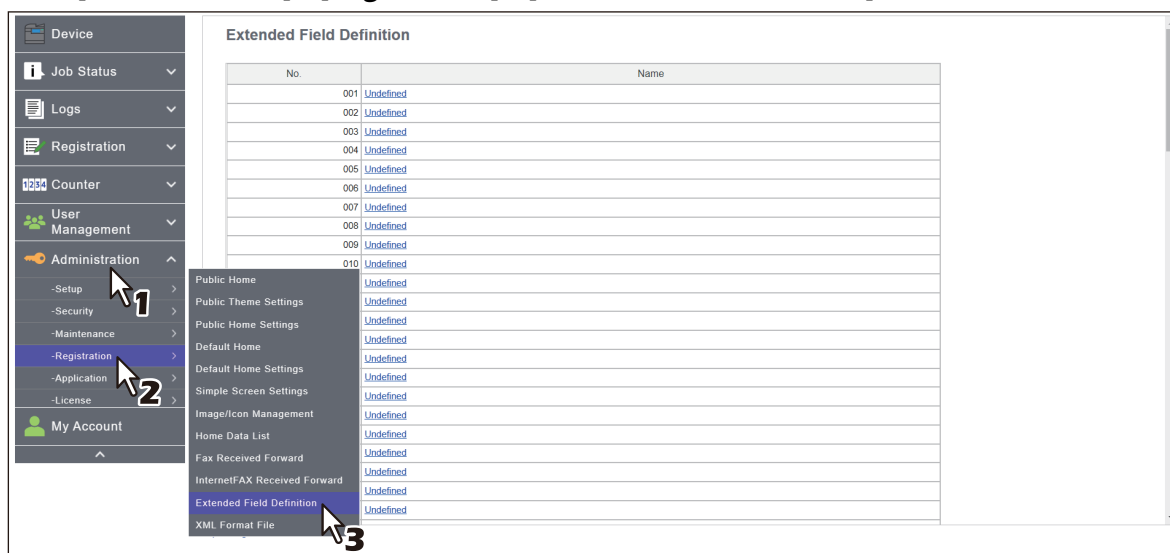
You can register up to 100 “extended field definitions”, select an “XML format file” for each of them, and set “extended field properties” as necessary.

When using applications that interact with Meta Scan, follow the instructions of the application vendor to set the XML format file and the extended field.

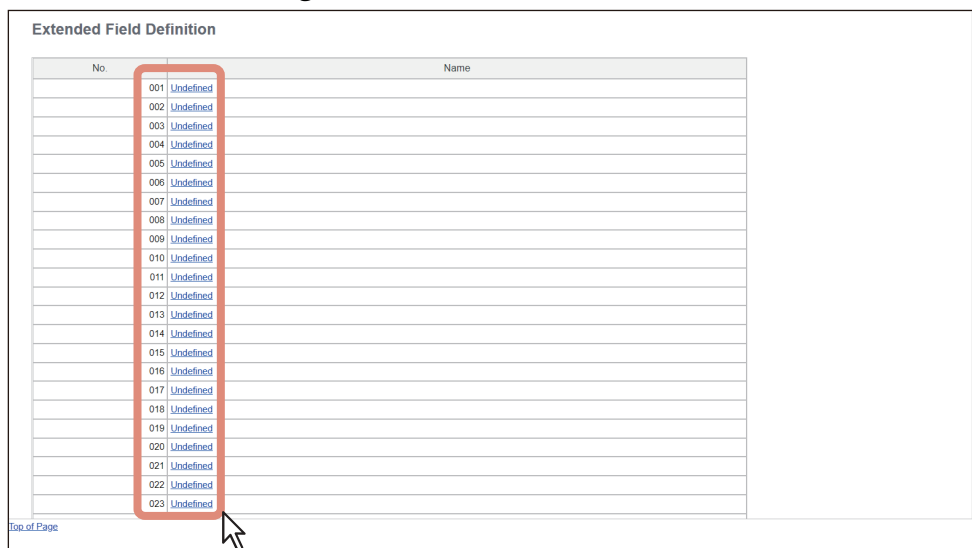
1 Start TopAccess access policy mode.

📖 P.14 “Access Policy Mode”

2 Click [Administration] > [Registration] > [Extended Field Definition].



3 Click [Undefined] to register an extended field definition.



Click a registered extended field name to display the edit screen for the extended field. Skip to step 6.

4 Enter the field name, select an XML format file, and click [Save].

Click [Edit] on the right of the XML format file to select it when you want to use a customized XML format file. Select “defaultForm3.xml” if you do not have any customized XML format file.

Definition Properties

Definition Information

No.	Name
003	

*Required

Number	003
*Name	test003
XML Format File	defaultForm3.xml

Save Cancel

5 Click [New] under Extended Field settings when setting extended field properties.

Click [Extended Field Definitions] in the upper part of the screen if you are not setting extended field properties.

Extended Fields

Definition Information

No.	Name
003	test003

Extended Field settings

New

Field Name Display Name Mandatory Input Hidden Attribute Input Method Minimum Value Maximum Value Default Value Date

6 Set the extended field properties.

Extended Field Properties

Field Name

Name

*Display

Mandatory Input Hidden Attribute

Input Method

Numerical Decimal Text List Address Password Date

List Items

Name	Value

Move Up Move Down Delete

Minimum Length

Maximum Length

*Minimum Value

*Maximum Value

Default Value

Password

Date

Year Month Date

*Required

Field Name	Specify the extended field name.
Display	<p>Specify how to display the extended field on the touch panel.</p> <p>Name</p> <p>Enter the caption of the extended field name for the display on the touch panel. You can enter up to 20 characters. Enter the Box number where a received document will be stored.</p> <p>Mandatory Input</p> <p>Select this check box if the extended field is a mandatory entry item.</p> <p>Hidden Attribute</p> <p>Select this check box if the extended field is a hidden item on the touch panel.</p>

Input Method *	<p>Select the type of an extended field.</p> <ul style="list-style-type: none"> • Numerical — Select this to create an extended field as an integer value. • Decimal — Select this to create an extended field as a decimal value. • Text — Select this to create an extended field as a character string. • List — Select this to create an extended field as a list selection. • Address — Select this to create an extended field as an address. • Password — Select this to create an extended field as a password. • Date — Select this to create an extended field as a date.
List Items	<p>Specify list items to be selected for the extended field. The registered list items are listed in the List Items. When you register a list item, enter [Name] and [Value], and then click [Add]. If you select an item and click [Move Up], the selected item moves up in the list. Click [Move Down] to move it down. Select an item and click [Delete] to delete an unnecessary item from the list.</p> <p>Name Enter the name of the item.</p> <p>Value Enter a value or text to be applied for the selected item.</p> <p>Note</p> <ul style="list-style-type: none"> • You cannot exceed the total number of characters displayable in the List Items (127). • You cannot use a semicolon in [Name] or [Value].
Minimum Length	Specify the minimum number of characters that can be entered in the extended field if the field is a character string.
Maximum Length	Specify the maximum number of characters that can be entered in the extended field if the field is a character string.
Minimum Value	Specify the minimum numerical value that can be entered in the extended field if the field is a numerical value.
Maximum Value	Specify the maximum numerical value that can be entered in the extended field if the field is a numerical value.
Default Value	Specify the default value for the extended field.
Password	Specify the default password for the extended field if the field is a password.
Date	Specify the default date for the extended field if the field is a date.

* The following shows the types and settable items of an extended field for each [Input Method]. (*) is displayed for mandatory setting items.

Input method (Extended field type)	Mandatory setting items	Optional setting items
Numerical value	[Maximum Value], [Minimum Value] Settable value: -999,999,999,999 to 999,999,999,999	[Default Value]
Decimal value	[Maximum Value], [Minimum Value] Settable value: -999,999,999,999.999999 to 999,999,999,999.999999 Contact your service technician if you want to input a value with more than two decimal places.	[Default Value]
Text	[Maximum Length], [Minimum Length] Settable value: 0 to 256	[Default Value]

Input method (Extended field type)	Mandatory setting items	Optional setting items
List	[List Items] You can register up to 30 [List Items]. You can set from 1 to 126 characters in [Name]. You can set from 1 to 126 characters in [Value]. However, the total number of characters set in [Name] and [Value] must be from 2 to 127.	[Default Value] Select from the registered selection items
Address	None	[Default Value]
Password	None Settable value: 0 to 256	[Default Value]
Date	None	[Default Value]

7 Click [Save] to register the extended field properties.

You can register up to 25 extended field properties.

The extended field properties are registered.

■ Registering templates for Meta Scan

You must register a template for Meta Scan before using the Meta Scan function.

Tip

Only if the administrator has enabled [Public Home change from User] at [Home Setting], general users can register templates at the [Registration] > [Public Home] submenu. The following procedure explains the steps with the screens for the administrator.

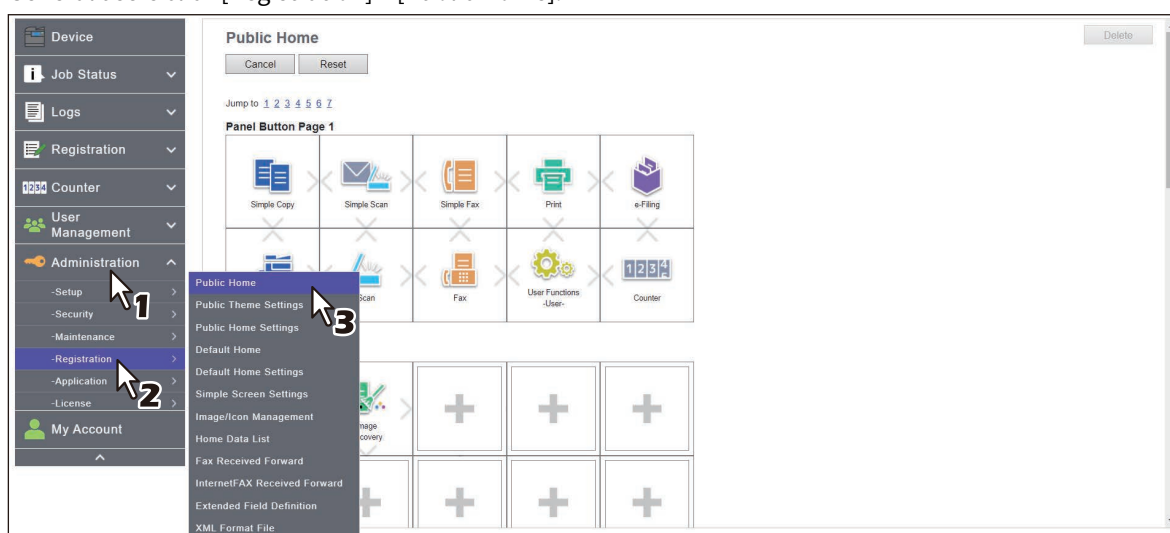
📖 P.113 “Home Setting”

1 Start TopAccess access policy mode.

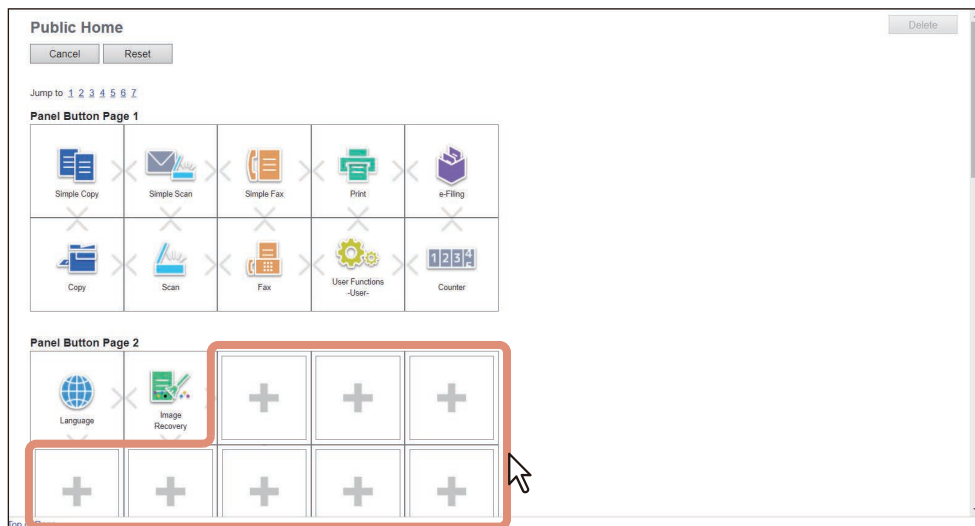
📖 P.14 “Access Policy Mode”

2 Click [Administration] > [Registration] > [Public Home].

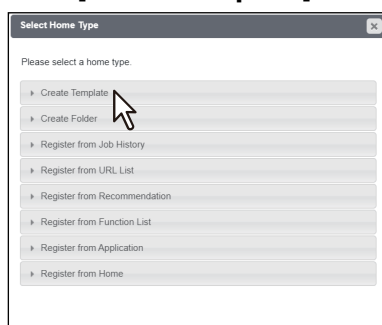
General users click [Registration] > [Public Home].



3 Click the [+] icon that represents an empty position at the Panel Button list.



4 Click [Create Template].



5 Select the check box for the [Meta Scan], and then select the agent and click [Select Agent].



Note

To select [Meta Scan], the Meta Scan Enabler must be set up for use.
If it is not set up, you cannot select [Meta Scan].

For [Meta Scan], [Email], [Save as file], and [Store to USB Media] are to be selected individually, except for [Email] and [Save as file], which can be selected simultaneously.

Email	<p>You can transmit the document as an Email attachment.</p> <p>Tip</p> <ul style="list-style-type: none"> • When [Meta Scan] is selected, you can use a variable as the subject • Addresses specified in [From Address] are included in the meta data. • When [Meta Scan] is selected, if you select [Add the date and time to a file name] in [File Name], it is also applied to the meta data file name. <p>📖 P.316 “Email Setting”</p>
--------------	--

Save as file	<p>You can save the document in a shared folder.</p> <p>Note</p> <ul style="list-style-type: none"> When [Meta Scan] is selected, you can only specify one destination. Protocols and network paths specified in the destination are included in the meta data. <p>Example: Protocol: SMB Network Path: \\192.168.1.1\ImageFolder</p> <p><file_path>file: //192.168.1.1/ImageFolder/</file_path></p> <ul style="list-style-type: none"> When [Meta Scan] is selected, if you select [Add the date and time to a file name] in [File Name], it is also applied to the meta data file name. <p> P.319 “Save as file Setting”</p>
Store to USB Media	You can save the document in USB media.

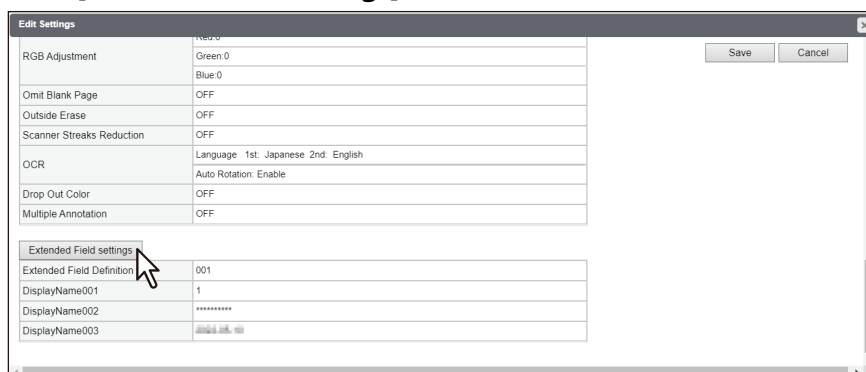
6 Set the agent.

Setting operations are the same as for normal templates.

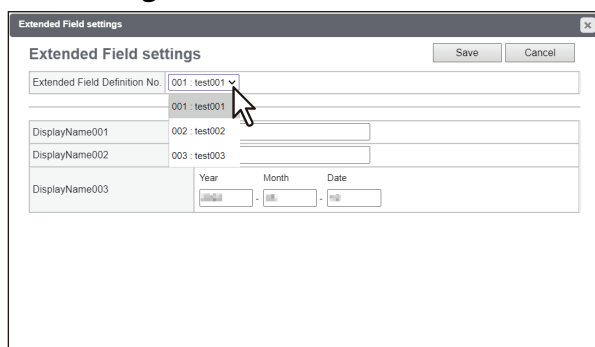
P.306 “Template settings”

The following describes how to set “Extended Field settings”. Be sure to set the settings for the Meta Scan templates.

7 Click [Extended Field settings] to set extended fields.



8 Select a registered extended field definition using [Extended Field Definition No.].



9 Enter the default value for the [Extended Field Properties].

This is displayed if [Extended Field Properties] are set for the selected extended field definition.

Values set in this screen are used as the default values for [Extended Field Properties] displayed on the touch panel when using Meta Scan.

Items with an asterisk (*) at the beginning of the [Extended Field Properties] name are mandatory entry fields.

10 Click [Save] to save the extended field settings.

11 Click [Save] to register the template.

The template for Meta Scan is registered.

Meta Scan

You can run Meta Scan using a Meta Scan template.

For the operational procedure, see the reference below:

Template - USING TEMPLATE BUTTONS - Recalling Templates - Using templates

Tip

If [Extended Field Definition] set in [Extended Field Settings] in the Meta Scan template is deleted, the default XML format file <defaultForm3.xml> is used.

Checking logs of Meta Scan

You can check the scan log to confirm if meta data has been correctly created.

Check the following items in the scan log.

Check Item	Description
Mode	Displays "MSxxxx" (xxxx is in the code format) to indicate Meta Scan.
Status	Meta data is correctly created if no errors are displayed.

See the following for details of the scan log:

📖 P.33 "Scan Log"

Setting Multi Station Print

Multi Station Print is the function to enable printing from any of the registered MFPs when a job is sent from a client computer, by adding multiple MFPs as a cooperative device in advance. Up to 10 MFPs can be registered. Operating with only one equipment unit is possible if the purpose is to use the output setting change function when printing. You can connect up to 10 MFPs in a group and connect up to 5 groups including a group to which this MFP belongs: you can add 4 groups for the connection.

■ Procedure for Multi Station Print

When the Multi Station Print function is used, it is necessary to set all MFPs to be connected. There are two methods to set the 2nd or later MFPs to be connected: by manual means and by copying the settings of the 1st MFP using a clone file.

Setup

	Operation	Description	Reference
1	Checking the Multi Station Print Enabler	Check whether the Multi Station Print Enabler can be used with your MFP.	P.391 “Checking the Multi Station Print Enabler”
2	Enabling user authentication	Enable user authentication.	P.240 “Setting up User Authentication Setting” P.225 “Shared User Management”
3	Enabling the Multi Station Print function	Enable the Multi Station Print function.	P.230 “Multi Station Print” P.217 “Setting up Multi Station Print”
4	Setting the connection MFP (1st device/no group connection)	Select and register the 1st MFP (no group connection) from among MFPs for collaboration.	P.230 “Multi Station Print” P.217 “Setting up Multi Station Print”
5	Setting the connection MFP (2nd or later devices/groups)	Register the 2nd or later MFPs by manual means.	P.230 “Multi Station Print” P.217 “Setting up Multi Station Print”
		When registering the 2nd or later MFPs by copying the settings for the 1st MFP, create a clone file and install it in them.	P.270 “Create Clone File settings” P.272 “Install Clone File settings”

Operation

	Operation	Description	Reference
1	Performing Multi Station Print	Print a job from the MFP connected by the network.	Print - PRINTING FROM WINDOWS APPLICATIONS - Outputting a Job Saved to the Equipment - Printing from Another MFP (Multi Station Print)

■ Procedure for Multi Station Print (Only in One Equipment Unit)

When an attempt is made to use the Multi Station Print function only in one equipment unit, register only the MFP to be used since no MFP connection is carried out.

Setup

	Operation	Description	Reference
1	Checking the Multi Station Print Enabler	Check whether the Multi Station Print Enabler can be used with your MFP.	P.391 "Checking the Multi Station Print Enabler"
2	Enabling the Multi Station Print function	Enable the Multi Station Print function.	P.230 "Multi Station Print" P.217 "Setting up Multi Station Print"
3	Setting the MFP	Register the MFP (this equipment) which is being connected with TopAccess.	P.230 "Multi Station Print" P.217 "Setting up Multi Station Print"

Operation

	Operation	Description	Reference
1	Performing Multi Station Print	Print a job from the registered MFP.	Print - PRINTING FROM WINDOWS APPLICATIONS - Outputting a Job Saved to the Equipment - Printing from Another MFP (Multi Station Print)

■ Checking the Multi Station Print Enabler

The Multi Station Printer Enabler is required for the use of the Multi Station Print function. For details, contact your service technician or representative.

The setting of the Multi Station Print Enabler in your MFP can be confirmed as below.

[User Functions -User-] > [Admin] > [General] > [License Management]

If [Multi Station Print] is registered in [License Management], the Multi Station Print function can be used.

Setting Home Data Synchronization

Once you have registered multiple MFPs for connection, you can use the common HOME screen when you log in to any one of the registered MFPs that are connected to the network. If MFP is used to synchronize the HOME screens, up to 10 MFPs can be connected.

Note

If you change the default settings on any of the connected MFPs after you start the home data synchronization, you need to set the same changes for all of the connected MFPs or you need to create a clone file except User Management and Address Book on the MFP where you have changed the settings and install it into all the other connected MFPs.

■ Procedure for Home Data Synchronization

The following table explains the procedure to synchronize the HOME screens by means of MFP.


	Operation	Description	Reference
1	Setting the first MFP for connection	Select one MFP as a primary server from among MFPs for collaboration. Make several settings such as user information, address book, default settings for jobs, installation of applications, EWB function settings, and others.	P.74 “[User Management] Overview” P.42 “[Address Book] Item list” P.360 “[Application] Item List” P.233 “Embedded Web Browser settings”
		Note Make sure that [Enable FTP Server] is enabled. P.150 “Setting up FTP Server”	
2	Creating a clone file	Create a clone file to copy the settings of the first MFP and install it into the second or later MFPs. Include the following categories in the clone file: <ul style="list-style-type: none">• Default Settings• User Management• Network/Print Service• Address Book• Application	P.270 “Create Clone File settings”
3	Setting the second or later MFPs for connection	Install the created clone file into the second or later MFPs.	P.272 “Install Clone File settings”
		Note Execute [Delete All Shared Data] before you install the clone file. P.228 “Shared Home” P.113 “Home Setting”	
4	Setting the primary server	Select one MFP as the primary server for connection and configure the shared user management and the shared address book.	P.225 “Shared User Management” P.240 “Setting up User Authentication Setting” P.45 “Shared Setting”
5	Setting the home data synchronization	Set the home data synchronization on all MFPs for connection.	P.228 “Shared Home” P.113 “Home Setting”
		Note <ul style="list-style-type: none">• To disconnect MFP, select [Disable] from [Public Home] or [Sync Setting] on the MFP concerned.• Select [Assume this MFP is the Primary Server] on the MFP that you use as the primary server.	

Using the Attribute of the External Authentication as a Role of the MFP

When the external authentication (Windows domain authentication and LDAP authentication) is enabled, associating the role defined in this equipment with the attribute of the external authentication server is required in order to log in the equipment from an external authentication server as an administrator. The role can be associated with the equipment by importing the role information setting file in this equipment. The role information setting file is a file in which the attributes of the external authentication server and corresponding MFP are defined in XML. You can edit the role information setting file exported from the equipment and import it back to the equipment.

■ Exporting the role information setting file

For how to export the role information setting file, see the reference below:

 P.95 “Export”

■ Defining the role information setting file

The role information setting file is written in XML format. The role of this equipment can be assigned to the attribute set in the external server by defining the role information setting file in accordance with the external authentication server setting. The three examples of the major definition method for this file are explained here. Alphanumeric characters can be used for the content of each element. An asterisk (*) can be used as a wildcard for the <attributeValue> element.

Tip

The role of the user that does not correspond to the <RoleSet> element is defined in the <AnyOtherUser> element. This element can only be used once.

❑ When setting one role to one attribute

Attribute name set in the external authentication server	Department
Attribute value set in the external authentication server	ITDept
Role name to be set	Administrator

```
<RoleSetting>
<RoleSet>
<Condition>
<AttributeName>department</AttributeName>
<AttributeValue>ITDept</AttributeValue>
</Condition>
<Role>Administrator</Role>
</RoleSet>
<AnyOtherUser>User</AnyOtherUser>
</RoleSetting>
```

❑ When setting multiple roles to one attribute

Attribute name set in the external authentication server	Department
Attribute value set in the external authentication server	ITDept
Role name to be set [1]	Administrator
Role name to be set [2]	PrintOperator

```

<RoleSetting>
<RoleSet>
<Condition>
<AttributeName>department</AttributeName>
<AttributeValue>ITDept</AttributeValue>
</Condition>
<Role>Administrator</Role>
</RoleSet>
<RoleSet>
<Condition>
<AttributeName>department</AttributeName>
<AttributeValue>ITDept</AttributeValue>
</Condition>
<Role>PrintOperator</Role>
</RoleSet>
<AnyOtherUser>User</AnyOtherUser>
</RoleSetting>

```

❑ When setting one role to multiple attributes

Attribute name set in the external authentication server [1]	Department
Attribute value set in the external authentication server [1]	Sales
Attribute name set in the external authentication server [2]	Title
Attribute value set in the external authentication server [2]	SeniorManager
Role name to be set	Print

```

<RoleSetting>
<RoleSet>
<Condition>
<AttributeName>department</AttributeName>
<AttributeValue>Sales</AttributeValue>
</Condition>
<Condition>
<AttributeName>title</AttributeName>
<AttributeValue>SeniorManager</AttributeValue>
</Condition>
<Role>Print</Role>
</RoleSet>
<AnyOtherUser>User</AnyOtherUser>
</RoleSetting>

```

■ Importing the role information setting file

For how to import the role information setting file, see the reference below:

📖 P.96 “Import”

Tip

To change the setting, import the role information setting file again.

■ Enabling the role base access setting

In order to use the imported role information setting file, enabling the role base access setting is required. For the procedure, see the reference below:

📖 P.240 “Setting up User Authentication Setting”

Setting up Email

Set the necessary settings for the email transmission, reception and operation from the [Administration] page displayed by logging in by means of the access policy mode.

Tip

When Email is used, setting up of the basic settings of the network is necessary. The [Network] submenu can be accessed from the [Setup] menu on the [Administration] page. For how to access it and information on the [Setup] menu, see the references below:

📖 P.14 “Access Policy Mode”

📖 P.101 “[Setup] Item List”

■ Procedure for Email Setting

	Operation	Description	Reference
1	Email transmission function confirmation	Check whether [Enable] is set for the Email transmission function from [Setup] > [General] > [Setting up Functions].	📖 P.101 “General settings” 📖 P.103 “Setting up Functions”
2	Setting up SMTP Client	Set [Enable] for SMTP transmission of Email.	📖 P.155 “Setting up SMTP Client”
3	Email Settings	Set the necessary settings for the Email transmission operation.	📖 P.192 “Email settings”
4	Setting up URL Transmission Settings	Set to apply to an Email the URL where scanned images are stored, instead of attaching themselves.	📖 P.197 “Setting up URL Transmission Settings”
5	Setting up Email Authentication	Set to require the entry of a user name and a password when Email transmission is attempted from the scanning screen.	📖 P.238 “Authentication settings” 📖 P.253 “Setting up Email Authentication”
6	Setting up Email Address Setting	Set to enable Email transmission to a sender’s e-mail address when [Enable] is set for Email authentication or user authentication.	📖 P.238 “Authentication settings” 📖 P.240 “Setting up User Authentication Setting” 📖 P.253 “Setting up Email Authentication” 📖 P.254 “Setting up Email Address Setting”
7	Setting up Single Sign On Setting	Set to apply the user name and the password, which are entered from the control panel, for logging into the equipment to the SMTP communication, when an authentication method for connecting an SMTP server is selected in [SMTP Client] and [Enable] is set for [User Authentication] or [Email Authentication].	📖 P.155 “Setting up SMTP Client” 📖 P.238 “Authentication settings” 📖 P.240 “Setting up User Authentication Setting” 📖 P.253 “Setting up Email Authentication” 📖 P.256 “Setting up Single Sign On Setting”

Installing Certificates

In the Security Service page, you can install a wireless LAN certificate for authentication with the RADIUS server, install and export a device certificate to enable SSL/TLS and set up its SCEP (automatic installation), install CA certificate, and install certificates for IEEE 802.1X authentication and set up its SCEP.

■ Installing a device certificate

To enable SSL/TLS for HTTP setting, FTP server setting, IPP Print Service, Web Services Print, or Off Device Customization Architecture settings, you must install a device certificate for each.


To install these device certificates, you need to create a self-signed certificate, install them from an authentication agency or the CA server. You can also install them automatically from the CA server using SCEP.

Tip

When you want to enable SSL/TLS for HTTP setting, FTP Server, IPP Print, Web Services Print, or Off Device Customization Architecture settings, the certificates required to install to the equipment and the client computer are as follows:

Use SSL/TLS for...	Required Certificate for this equipment			Required Certificate for Client computer		
	Device Certificate		CA Certificate	Self-signed Certificate	Client Certificate	CA Certificate
	Self-signed Certificate	Device certificates installed from authentication agency / CA server				
HTTP, FTP, IPP Print, Off Device Customization Architecture*	Required	-	-	(Required)	-	-
	-	Required	-	-	-	(Required)
Web Service Print	-	Required	Required	-	Required	Required
	Required	-	-	Required	-	-

* In the HTTP Network Service, FTP Server, IPP Print, and Off Device Customization Architecture settings, if you create a self-signed certificate for the equipment, you need to install the self-signed certificate to the client computer. If you select to install an imported device certificate to the equipment, also install the CA certificate to the client computer.


 P.405 “Installing CA certificate”

Note

When you install the User Certificate in this equipment, it is recommended to connect this equipment and a client computer using a crossing cable for ensuring security.

□ Creating/exporting a self-signed certificate

1 Start TopAccess access policy mode.

 P.14 “Access Policy Mode”

2

3

3

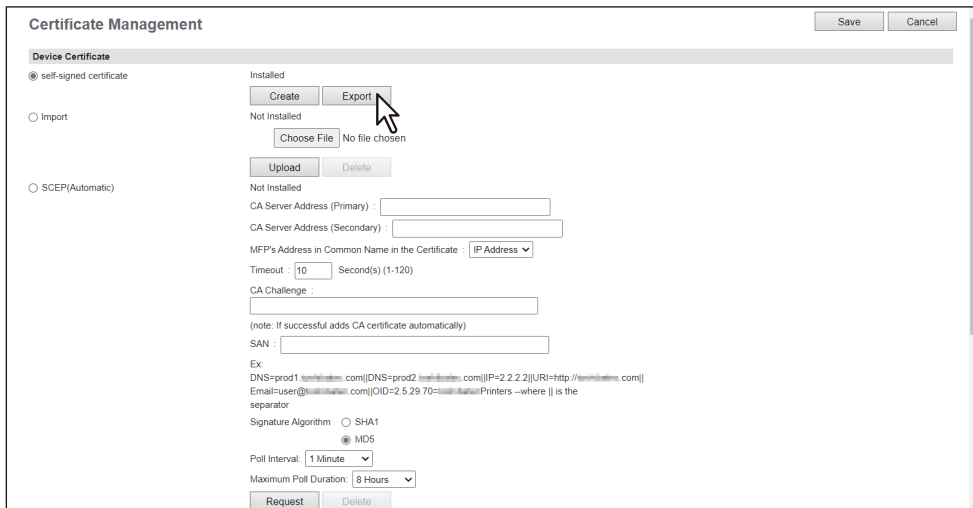
4

4

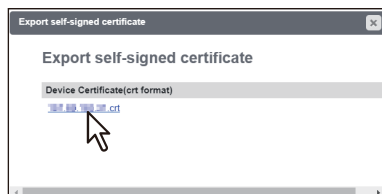
5

5

6 A self-signed certificate is created. Click [Export] if you are exporting.









The image shows a 'Certificate Management' dialog box. On the left, under 'Device Certificate', the 'self-signed certificate' option is selected. In the center, there are two tabs: 'Installed' and 'Not Installed'. The 'Installed' tab is active, showing a 'Create' button and an 'Export' button. A mouse cursor is pointing at the 'Export' button. Below the 'Not Installed' tab, there is a 'Choose File' button and the text 'No file chosen'. Further down, there are 'Upload' and 'Delete' buttons. The 'Not Installed' section contains several input fields: 'CA Server Address (Primary)', 'CA Server Address (Secondary)', 'MFP's Address in Common Name in the Certificate' (with a dropdown set to 'IP Address'), 'Timeout' (set to 10), 'Second(s) (1-120)', 'CA Challenge', and 'SAN'. A note states: '(note: If successful adds CA certificate automatically)'. Below the 'SAN' field, an example is provided: 'Ex: DNS-prod1.example.com[DNS-prod2.example.com][IP=2.2.2.2][URI=http://example.com]'. Below this, there is an 'Email' field and a 'separator' label. At the bottom, there are 'Signature Algorithm' options (SHA1 and MD5, with MD5 selected), 'Poll Interval' (set to 1 Minute), and 'Maximum Poll Duration' (set to 8 Hours). At the very bottom, there are 'Request' and 'Delete' buttons.

7 Click the link for the file name of the certificate to be exported.



The file is downloaded.

8 Then you can enable SSL/TLS for the following network settings.

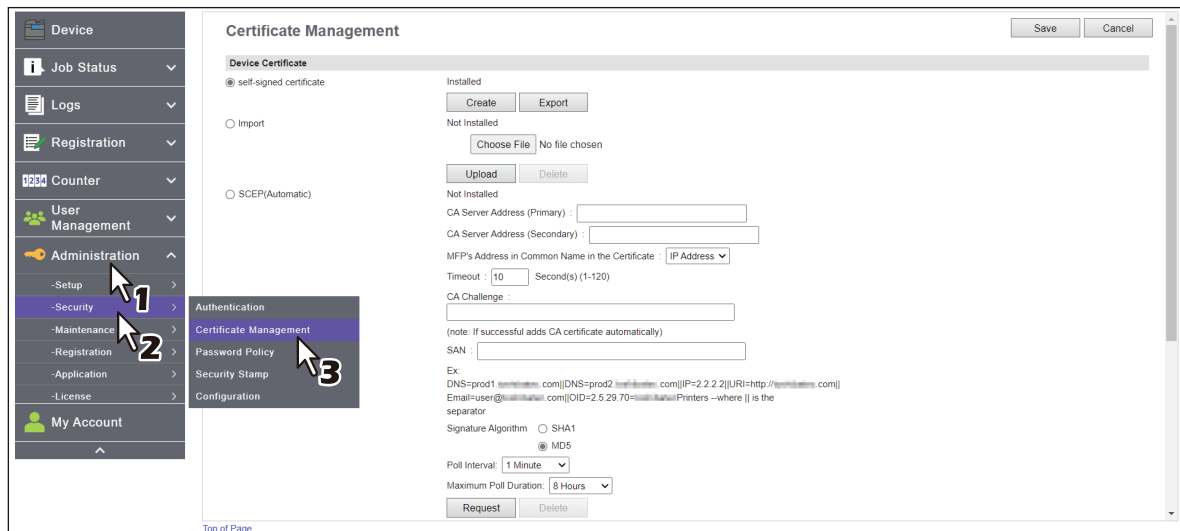
-  P.146 "Setting up HTTP"
-  P.148 "Setting up WSD"
-  P.150 "Setting up FTP Server"
-  P.151 "LDAP Client settings"
-  P.155 "Setting up SMTP Client"
-  P.158 "Setting up POP3 Client"
-  P.213 "Setting up IPP Print"
-  P.236 "Off Device Customization Architecture settings"

❑ Installing an imported device certificate

1 Start TopAccess access policy mode.

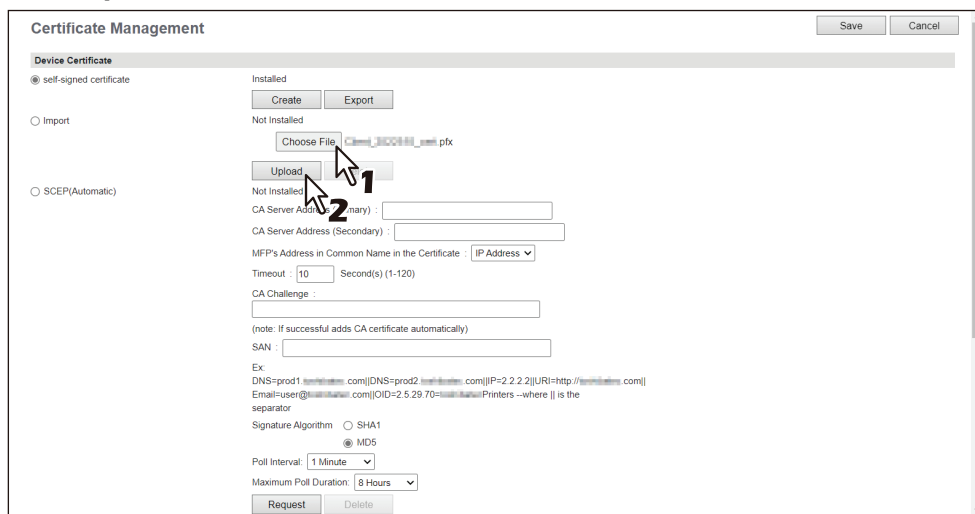
📖 P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].



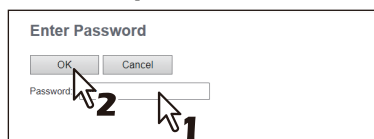
The Certificate Management page is displayed.

3 Click [Choose File] of [Import] in [Device Certificate] to select a device certificate file, and then click [Upload].



The alert message dialog box appears.

4 Enter the password for the device certificate, and then click [OK].



The device certificate is imported.

5 Click [Save] on the [Certificate Management] submenu.

6 Then you can enable SSL/TLS for the following network settings.

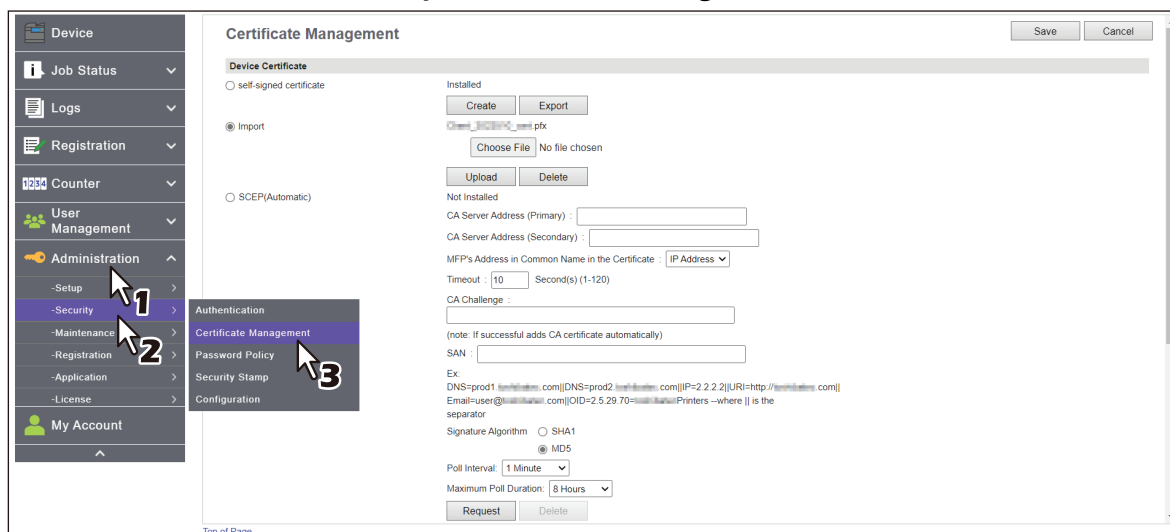
- P.146 “Setting up HTTP”
- P.148 “Setting up WSD”
- P.150 “Setting up FTP Server”
- P.151 “LDAP Client settings”
- P.155 “Setting up SMTP Client”
- P.158 “Setting up POP3 Client”
- P.213 “Setting up IPP Print”
- P.236 “Off Device Customization Architecture settings”

❑ Deleting an imported device certificate

1 Start TopAccess access policy mode.

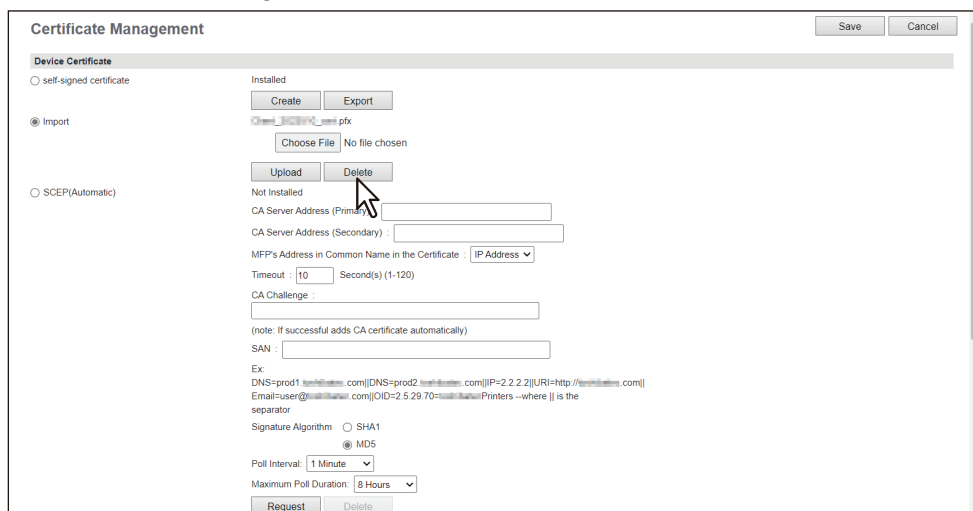
- P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].



The Certificate Management page is displayed.

3 Click [Delete] of [Import] in [Device Certificate].



The confirmation dialog box appears.

Note

If no device certificate has been imported, you cannot delete it.

4 Click [OK].

The device certificate is deleted.

5 Click [Save] on the [Certificate Management] submenu.

❑ Installing a device certificate automatically

1 Start TopAccess access policy mode.

P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].

The Certificate Management page is displayed.

3 Enter the following items in [SCEP(Automatic)] of [Device Certificate], and then click [Request].

CA Server Address (Primary)	Enter the IP address or FQDN of the CA server. You can enter up to 128 characters.
CA Server Address (Secondary)	Enter the IP address or FQDN of the CA server. You can enter up to 128 characters.
MFP's Address in Common Name in the Certificate	Select whether to use the IP address or FQDN as the address of this equipment to be entered in the [Common Name] box of the certificate.
Timeout	Enter a timeout period for quitting communication when no response is received from the CA server.
CA Challenge	Enter the CA challenge.
Signature Algorithm	Select SHA1 or MD5 as the signature algorithm.
Poll Interval	Specify the polling interval.
Maximum Poll Duration	Specify the polling duration.

Note

- If FQDN is used in [CA Server address], you need to configure a DNS server and enable DNS settings.
- If [FQDN] is selected in [MFP's Address in Common Name in the Certificate], the IP address of this equipment must be registered in the DNS server.

A device certificate is installed.

Note

A CA certificate is installed automatically as well as a device certificate. If a CA certificate is already installed, delete the existing one by clicking [DELETE] of SCEP in [Device Certificate]. Then click [Request] to install a new CA certificate.

4 Click [Save] on the [Certificate Management] submenu.

5 Then you can enable SSL/TLS for the following network settings.

- 📖 P.146 “Setting up HTTP”
- 📖 P.148 “Setting up WSD”
- 📖 P.150 “Setting up FTP Server”
- 📖 P.151 “LDAP Client settings”
- 📖 P.155 “Setting up SMTP Client”
- 📖 P.158 “Setting up POP3 Client”
- 📖 P.213 “Setting up IPP Print”
- 📖 P.236 “Off Device Customization Architecture settings”

❑ Deleting a device certificate installed automatically

1 Start TopAccess access policy mode.

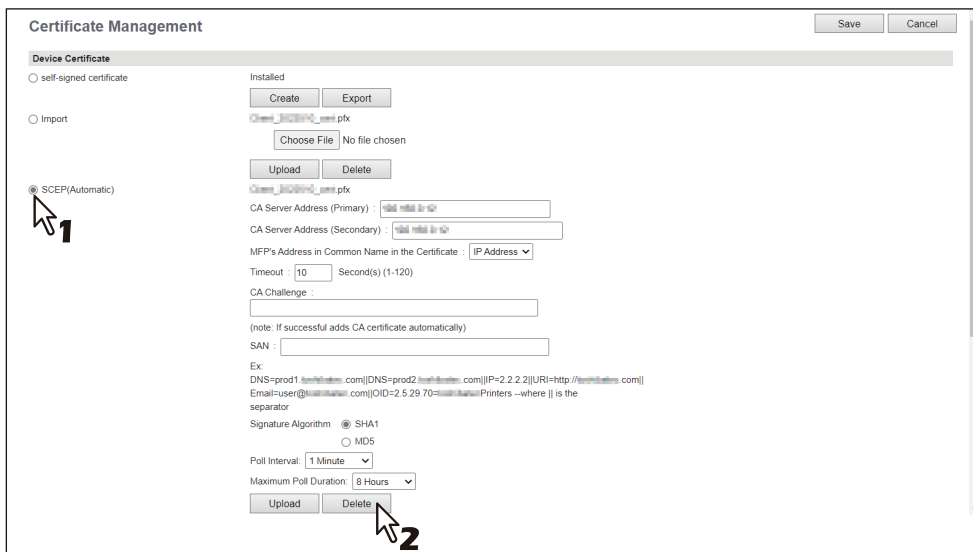
- 📖 P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].

The screenshot shows the 'Certificate Management' page. On the left, the navigation menu has 'Administration' expanded, with 'Security' and 'Certificate Management' selected. The main area is titled 'Certificate Management' and contains a 'Device Certificate' section. Under 'Device Certificate', there are two radio buttons: 'self-signed certificate' and 'Import'. The 'Import' option is selected. Below it, there are fields for 'CA Server Address (Primary)', 'CA Server Address (Secondary)', 'MFP's Address in Common Name in the Certificate' (with a dropdown menu set to 'IP Address'), 'Timeout' (set to 10 seconds), and 'CA Challenge'. There is also a 'SAN' field. At the bottom, there are 'Upload' and 'Delete' buttons. A note states: '(note: If successful adds CA certificate automatically)'. An example SAN string is provided: 'Ex: DNS=prod1.192.168.1.192.com|DNS=prod2.192.168.1.192.com|IP=2.2.2.2|URI=http://192.168.1.192.com|Email=user@192.168.1.192.com|OID=2.5.29.70=192.168.1.192|Printers -where | is the separator'. The 'Signature Algorithm' is set to 'SHA1' and 'Poll Interval' is set to '1 Minute'.

The Certificate Management page is displayed.

3 Select [SCEP(Automatic)] in [Device Certificate], and then click [Delete].



The confirmation dialog box appears.

Note

- A CA certificate already installed automatically will be deleted as well as the device certificate.
- Deleting is disabled when no device certificate has been installed automatically.

4 Click [OK].

The device certificate is deleted.

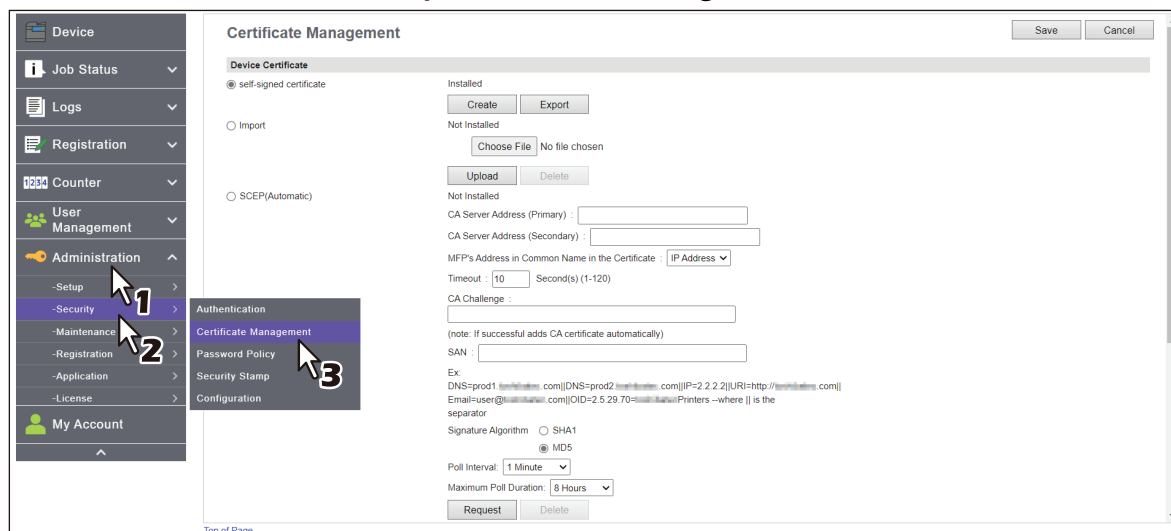
5 Click [Save] on the [Certificate Management] submenu.

■ Creating/Exporting a client certificate

1 Start TopAccess access policy mode.

P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].



The Certificate Management page is displayed.

3 Click [Create] under [Client Certificate].

Client Certificate

Not Created Create

Certificate Setting

Signature Algorithm:

SHA256

Public Key:

RSA2048

CA certificate

☒ CA Certificate (PEM)

Choose File

No file chosen

☐ CA certificate (DER)

Choose File

No file chosen

Upload

Delete

Certificate Files

The Create Client Certificate page is displayed.

4 Enter the following items and click [Save].

Create Client Certificate

Country/Region: JP

State or Province: Tokyo

Locality Name: abcdefghijklm

Organization Name: ABC CORPORATION

Organizational Unit Name: ABC Department

Common Name: ABC

Validity Period: 36 month(s)(1-99)

Password: *****

Buttons: Save, Cancel

You can set the following in this page.

 P.260 “[Create Client Certificate] screen”

5 Click [OK].

6 Click the link for the file name of the certificate to be exported.

Client Certificate

Choose File

No file chosen

Create

Certificate Setting

Signature Algorithm

SHA256

Public Key

RSA2048

CA certificate

☒ CA Certificate (PEM)

Choose File

No file chosen

☐ CA certificate (DER)

Choose File

No file chosen

Upload

Delete

Certificate Files

The file is downloaded.

Tip

If you have not installed a client certificate, enter the password in [Password] and click [Create] to create a certificate.

■ Installing CA certificate

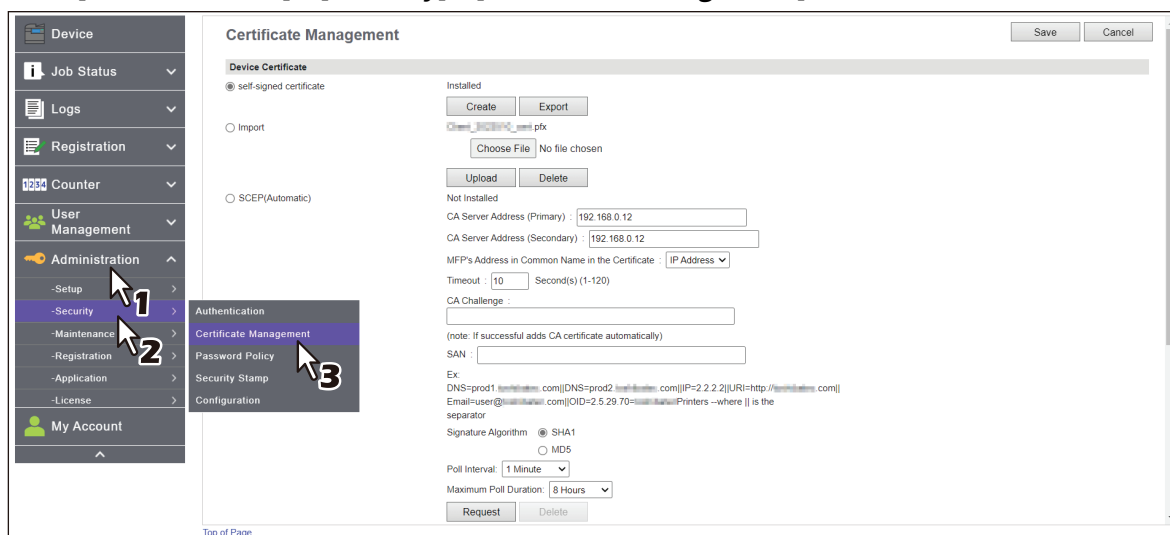
When you want to enable SSL/TLS and verify with a CA certificate for the SMTP Client, POP3 Network Service, FTP Client, Directory Service, or Syslog Setting, you must install the CA certificate. You can install up to 10 CA certificates in this equipment.

□ Installing CA certificate

1 Start TopAccess access policy mode.

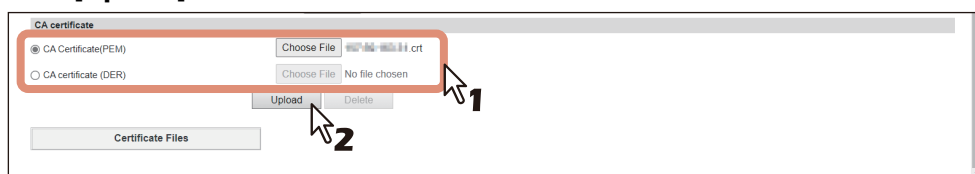
📖 P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].



The Certificate Management page is displayed.

3 Select the encryption of CA certificate and click [Choose File] to select a CA certificate file. Then click [Upload].



The CA certificate is installed.

4 Click [Save] on the [Certificate management] submenu.

5 Then you can enable SSL/TLS by selecting [Verify with imported CA certification(s)] for the following network settings.

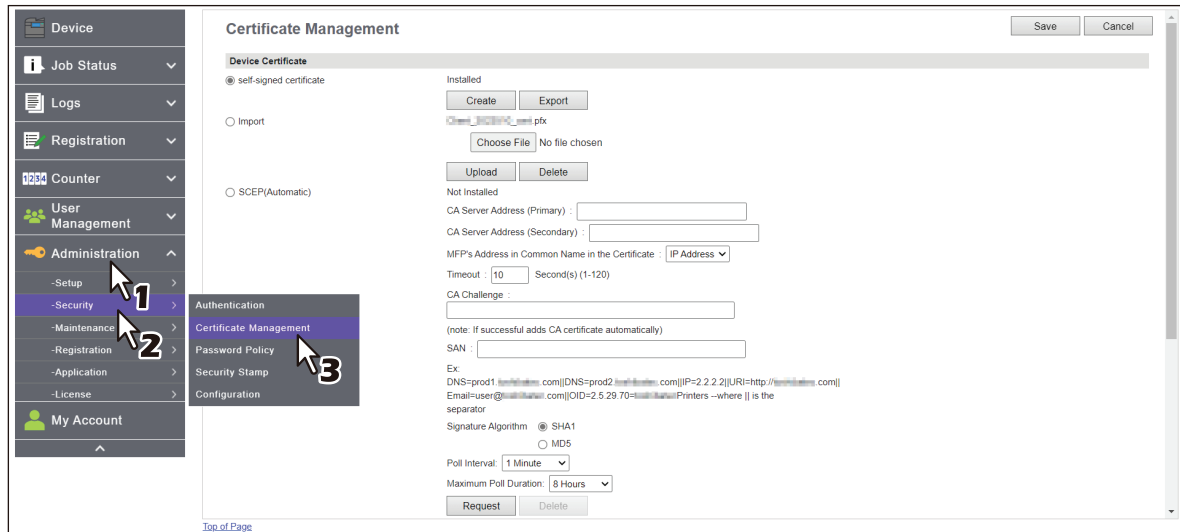
- 📖 P.148 “Setting up WSD”
- 📖 P.151 “LDAP Client settings”
- 📖 P.155 “Setting up SMTP Client”
- 📖 P.158 “Setting up POP3 Client”
- 📖 P.160 “Setting up FTP Client”
- 📖 P.166 “Syslog Setting”
- 📖 P.236 “Off Device Customization Architecture settings”

❑ Deleting CA certificate

1 Start TopAccess access policy mode.

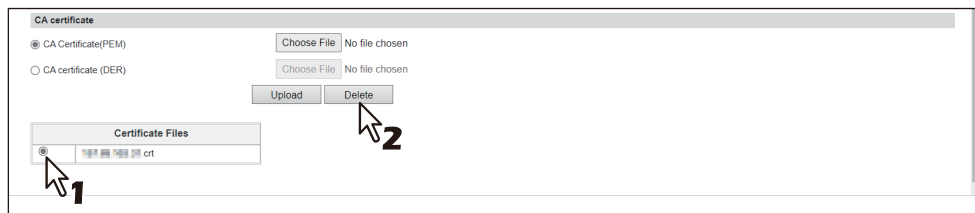
P.14 “Access Policy Mode”

2 Click [Administration] > [Security] > [Certificate Management].



The Certificate Management page is displayed.

3 Select the CA certificate file that you want to delete in the [Certificate Files] list, and click [Delete].



The confirmation dialog box appears.

4 Click [OK].

The CA certificate is deleted.

5 Click [Save] on the [Certificate Management] submenu.

INDEX

A

Access policy mode	10, 14
Accessing TopAccess	12
Accessing TopAccess by entering URL	12
Activate	368
Add Filter	132
Add IKE	135
Add Manual Key	134
Add New LPR Queue	210
Add New URL	235
Add Policy	141
Add Profile	139
Address Book	42
Address Book Item list	42
Administration	99
Application Data	365
Application Item List	360
Application List	360
Application Log	36
Application Settings	363
Apply Remote Command File	293
Assignment for Programmable button	114
Authentication settings	238
Available USB Device List	366

B

Basic Setting	118
Box Setting	324
Box Setting (Mailbox)	58
Box Setting (Received Forward Setting for Application)	181

C

Card Authentication Guidance Image	339
Certificate Management settings	257
Change Password	372
Checking logs of Meta Scan	389
Checking Meta Scan Enabler	379
Close Button Setting	281
Common Settings	223
Configuration settings	266
Confirm Permission	376
Contact Property	343
Contacts	42
Contents Setting	283
Copier settings	169
Counter	59
Counter Item list	60
Counter Overview	60
Create Client Certificate	260
Create Clone File settings	270
Create Destination information	48
Create Group Information	83
Create Group information	52
Create LDAP Information	152
Create New Role	87
Create self-signed certificate	259
Create SNMP V3 User Information	164
Create User Information	75
Creating/Exporting a client certificate	403
Creating/exporting a self-signed certificate	396

Custom Keyboard Setting	292
-------------------------------	-----

D

Data Backup	295
DDNS	126
Default Home	336
Default Home Settings	336
Default roles and privileges	85
Default XML file format	380
Defining the role information setting file	393
Definition Properties	359
Delete Shared Files settings	286
Deleting a device certificate installed automatically	402
Deleting an imported device certificate	400
Deleting CA certificate	406
Department Counter	63
Department Information	64, 91
Department Management Item list	90
Destination Setting	307
Destination Setting (Mailbox)	57
Device	17
Device Item list	18
Display Timing	281
Displayed icons	20
DNS	125
DNS (Secondary)	125

E

Edit Department Information	92
Edit Destination information	48
Edit Group Information	83
Edit Group information	52
Edit LDAP Information	152
Edit Role	89
Edit Settings	373
Edit Settings for folders	302
Edit Settings for templates	301
Edit User Information	78
Editing XML format file	379
Email Setting	316
Email Setting (Mailbox)	58
Email settings	192
Embedded Application Setting	364
Embedded Web Browser settings	233
Enabling the role base access setting	394
End-user mode	10
Enter Password	77
Entering the destinations manually	308
Export	47, 95
Export Logs Item list	38
Export settings	277
Export/Import Item list	95
Exporting the role information setting file	393
Extended Field Properties	333
Extended Field settings	333
Extended Fields	355
Extended Fields Properties	357

F

Favorite Contact	43
------------------------	----

Favorite Groups.....	44
Fax Received Forward and InternetFAX Received	
Forward settings.....	340
Fax Setting.....	49, 313
Fax settings.....	173
Fax/InternetFax Job Item list	26
From Name Registration.....	178, 201

G

General	363
General Setting	119, 280
General Setting (Secondary)	119
General settings	101
Group.....	44
Group Assignment.....	82
Group Management Item list.....	82

H

Home Data List.....	340
Home Screen setting.....	372
Home Setting	113

I

ICC Profile settings.....	220
Idle Screen.....	280
Image/Icon Management	338
Import.....	46, 96
Import Application Data	365
Import settings.....	275
Importing the role information setting file.....	394
Inbound FAX routing.....	53
Inbound FAX routing Item list.....	53
Install Card Reader Firmware.....	299
Install Clone File settings.....	272
Install Language Pack.....	365
Installing a device certificate.....	396
Installing a device certificate automatically.....	401
Installing an imported device certificate	399
Installing CA certificate.....	405
Installing Certificates	396
InternetFax Setting	312
InternetFax Setting (Mailbox).....	57
InternetFax settings.....	199
IPv4	120
IPv4 (Secondary)	120
IPv6	123
IPv6 (Secondary)	123

J

Job Status.....	23
Job Status Overview	24

L

Languages settings	290
LDAP Authentication.....	251
LDAP Client settings.....	151
License Item List	368
License List.....	368
LLMNR.....	128
LLMNR (Secondary).....	128
Log Settings Item list	40
Log size	40

Logs.....	29
Logs Overview	30
Long File Name Setting	104

M

MailBox Setting (Mailbox)	55
MailBoxes Properties.....	54
Maintenance Item list.....	267
Message Log	37
Meta Scan	355, 389
MFP Collaboration.....	223
MFP Local Authentication	244
Modify Filter.....	132
Modify IKE.....	135
Modify Manual Key	134
Modify Policy	141
Modify Profile.....	139
Multi Station Print	230
Multi Station Print Job Item list.....	28
My Account	369
My Account Item list.....	370
My Account Overview	370

N

Network Composition	118
Network settings	117
Notification Events.....	236
Notification settings.....	287

O

OCR Setting.....	115
Off Device Customization Architecture settings.....	236

P

Panel Background Image.....	338
Panel Icon Image.....	338
Panel View.....	279
Password Policy settings	262
PDF/A Fileformat Setting	116
Preparing a driver file for uploading	268
Preset Print Setting	285
Print Counter	62
Print Data Converter settings	222
Print Job Item list	24
Print Service settings	212
Printer settings	205
Printer/e-Filing settings	204
Procedure for Email Setting.....	395
Procedure for Home Data Synchronization	392
Procedure for using Meta Scan	378
Project Management Item list	94
Proxy Setting	285, 364
Public Box Authentication	257
Public Home	42, 300
Public Home Settings.....	42, 335
Public Theme Settings	42, 334

Q

Quota Setting	71
---------------------	----

R

Reboot settings	299
-----------------------	-----

Received Forward Setting for Application	180	Setting up Clone File Information	273
Reception Journal.....	32	Setting up CMYK Source Profile	221
Recovery Information	25	Setting up Combined	276, 278
Register from Application	305	Setting up Confidentiality Setting	106
Register from Function List	304	Setting up Configuration.....	236
Register from Home	305	Setting up Copy Job Enforcement Continue	172
Register from Job History	303	Setting up Current Language Pack List	291
Register from Recommendation	304	Setting up Current Software List	299
Register from URL List	304	Setting up Customized RGB Profile	222
Registering Extended Field Definition	383	Setting up Date & Time	111
Registering templates for Meta Scan	386	Setting up Daylight Savings Time Setting	112
Registering XML format file.....	383	Setting up Default Direct Print Setting	206
Registration	41	Setting up Default Raw Job Setting	208
Registration Item list.....	300	Setting up Default setting	169
Registration Overview	42	Setting up Default Setting for PanelUI	292
Relay End Terminal Report (Mailbox)	57	Setting up Definition Information	355
Remote Command	293	Setting up Department Setting	238
Remote Command Execution History.....	294	Setting up Destination	183
Remote Setting List.....	188	Setting up Destination Profile	221
Remote Setting screen.....	189	Setting up Destination Setting (Fax/Internet Fax Received Forward)	342
Remove Software settings.....	269	Setting up Device Certificate	257
Removing the contacts from the Recipient List	312	Setting up Device Information.....	102
Report Settings	179, 202	Setting up Document Print (Fax/InternetFax Received Forward)	342
Resource Management	367	Setting up Driver Customization Packages Setting.....	207
Restriction of Destination Selection Method.....	105	Setting up e-Filing Notification Events.....	104
Role Assignment	81	Setting up Email	395
Role Management Item list.....	84	Setting up Email Address Setting	254
S		Setting up Email Authentication	253
Save as file Setting	319	Setting up Email Print	216
Save as file Setting (Mailbox).....	58	Setting up Email Setting	192, 287
Save as File settings	182	Setting up Email Setting (Fax/InternetFAX Received Forward)	350
Scan Counter.....	62	Setting up Energy Save	107
Scan Job Item list.....	27	Setting up EWB History Setting	234
Scan Log	33	Setting up Extended Field settings.....	356
Scan Setting	327	Setting up Fax Setting	173
Search Address List.....	51	Setting up File Composition	185
Search Contact.....	50	Setting up File Upload.....	273
Search User Account.....	75	Setting up Filtering.....	128
Searching for destinations in the LDAP server	311	Setting up Folder Name	183
Security Item list	238	Setting up Format	184
Security Stamp setting	265	Setting up FTP Client.....	160
Select Home Type	301	Setting up FTP Print	215
Select Image.....	374	Setting up FTP Server.....	150
Selecting the destinations from the address book	309	Setting up Functions	103
Selecting the groups from the address book	310	Setting up General Setting.....	205
Server Assignment screen	154	Setting up Home Directory Setting	256
Setting for saving meta data	382	Setting up Home Page Setting.....	233
Setting Home Data Synchronization.....	392	Setting up HTTP	146
Setting up Address Book	275, 277	Setting up Install Language Pack	291
Setting up Application	290	Setting up Install Software Package	298
Setting up Bonjour.....	161	Setting up InternetFax Setting	199
Setting up Box Setting (Fax/InternetFAX Received Forward).....	354	Setting up InternetFax Setting (Fax/Internet Fax Received Forward).....	343
Setting up CA Certificate.....	261	Setting up IP Security.....	130
Setting up Category Setting	271	Setting up IPP Print	213
Setting up Certificate Files	261	Setting up IPX/SPX	167
Setting up Certificate Setting.....	261	Setting up Job Control	104
Setting up Client Certificate	260		
Setting up Clone File.....	271		

Setting up Job Notification Events	289	Supported browsers.....	11
Setting up License.....	290	Syslog Setting.....	166
Setting up Local Storage Path.....	182	System Protection.....	266
Setting up LPD Print.....	212	System Updates settings	298
Setting up MailBoxes	276, 278	T	
Setting up Meta Scan Function	378	Template Data Conversion	276
Setting up Mobile Scan(eSCL)	161	Template settings.....	306
Setting up Multi Station Print.....	217	Theme Settings.....	374
Setting up N/W-Fax Destination	190	TopAccess Conditions	11
Setting up N/W-Fax Folder.....	190	TopAccess Overview.....	10
Setting up NetWare.....	167	TopAccess screen descriptions.....	13
Setting up NetWare Print.....	215	Total Count	60
Setting up Network.....	236	Transmission Journal.....	31
Setting up Policy	264	U	
Setting up Policy for Administrator, Auditor	263	Upload Software settings	267
Setting up Policy for Users	262	User Accounts Item list	74
Setting up POP3 Client	158	User Counter.....	67
Setting up Printer/e-Filing Job		User Extended Information.....	366
Enforcement Continue	204	User Information	68
Setting up Proxy Setting	233	User Management	73
Setting up Raw Job Setting	209	User Management Overview	74
Setting up Raw TCP Print.....	212	User Paper Type	297
Setting up Remote 1 and Remote 2	186	Using the attribute of the external authentication	
Setting up Restriction on		as a role of the MFP	393
Address Book Operation by Administrator	105	V	
Setting up RGB Source Profile	220	Variables of XML format files.....	379
Setting up Save as file Setting		Version	237
(Fax/InternetFAX Received Forward).....	344	View Home	373
Setting up Searching Interval.....	186	View Logs Item list.....	30
Setting up Server Registration Setting	234	VNC Setting	168
Setting up Setting data included in Clone File	273	W	
Setting up Single Page Data Saving Directory.....	185	When setting multiple roles to one attribute.....	393
Setting up Single Sign On Setting	256	When setting one role to multiple attributes.....	394
Setting up SLP	165	When setting one role to one attribute	393
Setting up SMB.....	142	Windows Domain Authentication.....	248
Setting up SMTP Client	155	X	
Setting up SMTP Server	149	XML Format File	359
Setting up SNMP	162		
Setting up SNTP Service	111		
Setting up System Message Notification Events	288		
Setting up URL List for Menu Screen.....	235		
Setting up URL Transmission Settings.....	197		
Setting up USB Cable Print.....	216		
Setting up User Authentication Setting.....	240		
Setting up User Name and Password			
at User Authentication for Save as File.....	185		
Setting up WEB General Setting.....	112		
Setting up WSD.....	148		
Settings.....	375		
Setup Item list	101		
Shared Address Book.....	224		
Shared Home.....	228		
Shared Setting.....	45		
Shared Settings Item list.....	97		
Shared User Management	225		
Shutdown Setting	110		
Simple Screen Settings.....	337		
SSL/TLS Settings	130		
Status Message.....	116		
Store to USB Device Setting	324		

**MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS**

TopAccess

e-STUDIO2020AC/2520AC

e-STUDIO2525AC/3025AC/3525AC/4525AC/5525AC/6525AC

e-STUDIO2528A/3028A/3528A/4528A/5528A/6528A

e-STUDIO6526AC/6527AC/7527AC

e-STUDIO6529A/7529A/9029A

Toshiba Tec Corporation

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN

© 2021, 2022 Toshiba Tec Corporation All rights reserved
Patent; <https://www.toshibatec.com/en/patent/>



OME210036A0
R210220X7201-TTEC
Ver01 F1 Issued in Oct. 2022