TOSHIBA

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for the Latest Functions

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

© 2021 - 2024 Toshiba Tec Corporation All rights reserved
Under the copyright laws, this manual cannot be reproduced in any form without prior written permission of Toshiba Tec Corporation.

Preface

Thank you for purchasing our product.
This manual describes the latest functions embedded in this equipment.
Read this manual before using the functions.

■ 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.
🕮	Pages describing items related to what you are currently doing. See these pages 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-STUDIO2010AC/2510AC	e-STUDIO5015AC Series
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC	
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A	e-STUDIO5018A Series
e-STUDIO5516AC/6516AC/7516AC	e-STUDIO7516AC Series
e-STUDIO5518A/6518A/7518A/8518A	e-STUDIO8518A Series
e-STUDIO330AC/400AC	e-STUDIO400AC Series

❑ Optional equipment

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

❑ 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.

❑ 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

AirPrint, iPad, and macOS are trademark of Apple Inc., registered in the U.S. and other countries.
For other trademarks, refer to the **Safety Information**.

CONTENTS

Preface **3**

Chapter 1 Overview

Information about Equipment **8**
Options 8
Available USB storage devices 8

Chapter 2 Home Screen

About Home Screen **10**
Simple Scan 10
Fax 10

Chapter 3 User Functions

User **12**
Fax 12
Admin **15**
General 15
USB Cable Print 18
Appendix **19**
Inputting Characters 19
List Print 20

Chapter 4 TopAccess

[User Management] Tab **24**
[User Management] Tab Page Overview 24
[Administration] Tab **31**
[Setup] Item List 31
[Security] Item List 61
[Maintenance] Item List 75
[Application] Item List 80

Chapter 5 AirPrint Function

Setting up AirPrint in TopAccess **88**
When Security Certificate Expired and AirPrint Becomes Unusable 88
Precautions for AirPrint **89**
When using AirPrint Fax 89
When printing is carried out by using thick paper and special paper (e-STUDIO330AC/400AC) 89

Chapter 6 Troubleshooting

Troubleshooting for the Hardware **92**
When This Screen Is Displayed 92
Questions for Error Messages 93
Checking the equipment status with TopAccess **94**
Error Codes 94

INDEX 95

1

Overview

Information about Equipment

■ Options

The following is sold separately, and upgrade the performance of the equipment. For details, contact your service technician or representative.

For e-STUDIO330AC/400AC

- **OCR Enabler (GS-1110)**
  Allows you to use the OCR function.

■ Available USB storage devices

USB storage devices must meet requirements below. However, some USB storage devices may not be used with this equipment even though the requirements below are met.

- USB2.0 (High Speed)
- FAT16, FAT32 or exFAT format
- Single-partition (USB storage devices with multiple partitions are not supported.)

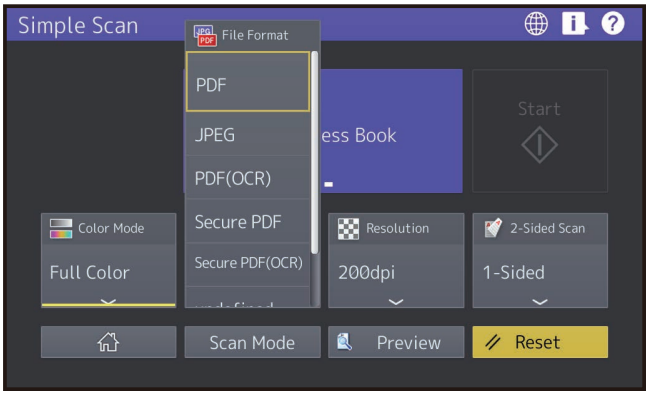
2

Home Screen

■ Simple Scan

❑ File Format

The file format of the scanned data can be specified by pressing [File Format].



There are 4 file formats as shown below.

- JPEG
- PDF
- Secure PDF
- Slim PDF

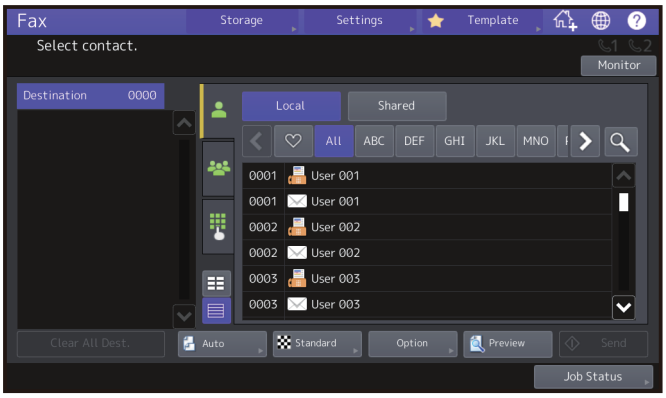
Tip

- [JPEG] is available only when [Full Color] or [Gray Scale] is selected for the color mode setting.
- The OCR option is necessary to use the OCR function.

■ Fax

❑ Address book

A mode to display only the name in the address book list has been added. Due to this, a longer name can be checked easily. For details about the setting, see the following reference:
P.12 “Fax”

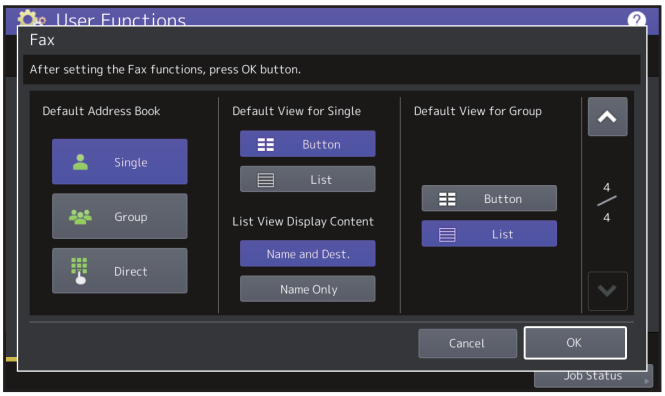


3

User Functions

■ Fax

A setting of [List View Display Content] for the address book has been added to the fax setting.



Item name	Description
Resolution	Select the resolution based on the fineness of the original. • **Standard** — This option is suitable for an original with regular size text. • **Fine** — This option is suitable for an original with small size text and fine illustrations. • **U-Fine** — This option is suitable for an original with small size text and detailed illustrations. Tip If the recipient's fax machine is not capable of receiving originals at the same resolution, the resolution is automatically converted before being sent it to the recipient. The higher the resolution is, the longer it takes to send an original.
Original Mode	Select the scanning mode based on the type of the original. • **Text** — This option is suitable for an original with text and line drawings. • **Text/Photo** — This option is suitable for an original with a mixture of text and photos. • **Photo** — This option is suitable for an original with photos. Tip In the Text/Photo mode or Photo mode, transmission time may be longer than in the TEXT mode.
Tx Type	Set the fax transmission mode. • **Memory Tx** — Send the original after the scanned data are saved in the memory. Up to 100 transmissions of up to 1000 pages per 1 transmission can be reserved. • **Direct Tx** — Send the original directly as it is being scanned. Once a page has been scanned and sent, the next page is scanned and sent. Therefore, it takes longer to scan and send all pages. However, you can confirm on the fly that each page is sent to the recipient.
Exposure	Select the desired exposure for the original. When setting the contrast manually, press [◐] or [◑] to set the desired contrast. When setting the contrast automatically in accordance with the original, press [Auto].

Item name	Description
Secure Receive Forced Setting	You can enable or disable the Secure Receive function. This is available only when the Weekly Schedule function is set. • **Enable** — This enables the Secure Receive function. Tip It becomes disabled at the time set by Weekly Schedule. • **Disable** — This disables the Secure Receive function. Tip • It becomes enabled at the time set by Weekly Schedule. • An administrator password is required.
RTI for G3	Switch the RTI recording On or Off for G3 fax. To enable this feature, the Terminal ID must be registered to this equipment in advance.
TTI for G3	Switch the TTI recording On or Off for G3 fax. To enable this feature, the Terminal ID must be registered to this equipment in advance. Tip Setting this item may not be required since it may not be displayed on the screen (it depends on your country or region).
ECM for G3	Switch the ECM (Error Correction Mode) communication On or Off for G3 fax. ECM is an internationally standardized communication mode that automatically corrects errors that occur during fax transmissions. With this setting option ON, even when the transmitted data have been affected by noise during communication, this mode allows good communication without image distortion by automatically resending the part that have been affected. Tip • Both the sender and the receiver must have the ECM function to make ECM communication available. • When affected by noise during communication, communication time is slightly longer than usual. Even when the ECM communication is used, an error may occur depending on the line status. • The ECM communication is not available for voice communication.
Multi Dest. Confirmation	Select whether to display the confirmation screen when multiple destinations are specified.
Preview Setting	Enabling the Preview function allows you to preview the scanned image before transmitting the fax/Internet Fax job. • **On** — Press this button to enable the function. • **Off** — Press this button to disable the function.
Tx Speed Limit	The transmission with V.34 may fail depending on the communication quality of your line. Transmission failures may be avoided when this setting is set to On.
Rx Speed Limit	The reception with V.34 may fail depending on the communication quality of your line. Reception failures may be avoided when this setting is set to On. • **Line 1** — Selects whether to enable the Rx speed limit for the 1st line. • **Line 2** — Selects whether to enable the Rx speed limit for the 2nd line.
Default Address Book	Select the default tab displayed in the address book.
Default View for Single	Select the default display format for the single tab of the address book.

Item name	Description
List View Display Content	Select the list view format in the address book. • **Name and Dest.** — Press this button to show names and destinations on the list of the address book. • **Name Only** — Press this button to show only names on the list of the address book. You can check long names easily.
Default View for Group	Select the default display format for the group tab of the address book.

■ General

Tip

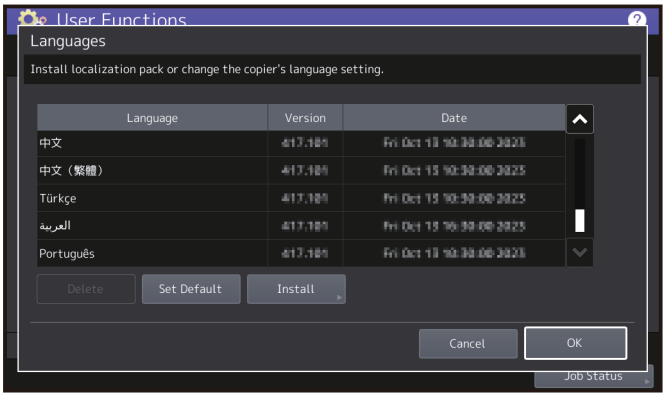
For instructions on how to display the General menu, see the **MFP Management Guide**.

❑ Adding or removing display languages

"Portuguese" and "Arabic" have been added to the language pack installed as the standard.

Tip

This settings are linked to the settings on the [Maintenance] Tab > [Languages] > [Current Language Pack List] screen of **TopAccess**.
P.76 "Setting up Current Language Pack List"



Tip

- The following language packs are initially installed on the equipment.

English (US)	English (UK)	German	French	Spanish
Italian	Danish	Finnish	Norwegian	Swedish
Dutch	Polish	Russian	Japanese	Simplified Chinese
Traditional Chinese	Turkish	Portuguese	Arabic	

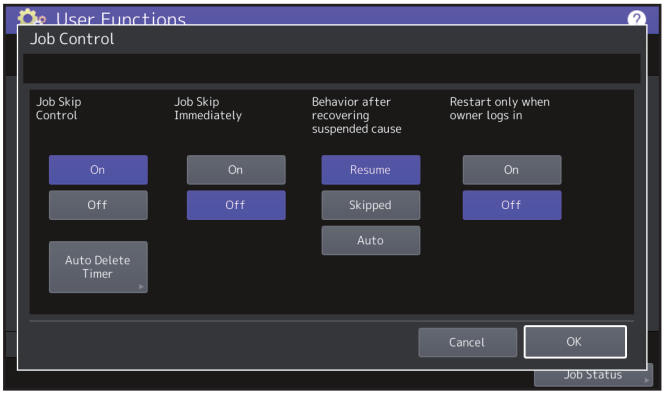
- When adding a language, store the desired language pack in the root directory of your USB storage device in advance.
- For information of languages which can be newly added, contact your service technician.

❑ Setting the job control

The Job Skip function has been changed.

Tip

This settings are linked to the settings on the [Administrator] Tab > [Setup] > [General settings] > [Job Skip Control] screen of **TopAccess**.
🕮 P.31 “Setting up Job Skip Control”



Item name	Description
Job Skip Control	• **On** — Press this button to enable the function. • **Off** — Press this button to disable the function. • **Auto Delete Timer** — Press this button so that you can set the time to delete the skipped jobs. Press [No Limit] not to delete them automatically. This setting is available only if [Job Skip Control] is turned on.
Job Skip Immediately	You can select whether to skip jobs immediately. This setting is available only if [Job Skip Control] is turned on. • **On** — Press this button to enable this function. • **Off** — Press this button to disable this function.
Behavior after recovering suspended cause	You can select the operation after clearing the cause that has suspended jobs. This setting is available only if [Job Skip Control] is turned on. • **Resume** — Press this button to resume the suspended jobs automatically. • **Skipped** — Press this button to leave the jobs skipped to cope with them manually. • **Auto** — Press this button to restart only undefined user’s jobs, for example fax received print and others.
Restart only when owner logs in	You can select whether to allow only the log-in job owner to restart the skipped jobs when the user authentication is enabled. This setting is available only if [Job Skip Control] is turned on. • **On** — Press this button to enable this function. • **Off** — Press this button to disable this function. Note When the user authentication is disabled, any user can restart skipped jobs regardless of this setting.

Tip

For instructions on how to resolve the cause of a skipped copy or print job, see the **Software Troubleshooting Guide**.

Combination of Settings

Set the job control, referring to the table below that shows a typical combination of the settings.

Purposes	Job Skip Control	Auto Delete Timer	Job Skip Immediately	Behavior after recovering suspended cause	Restart only when owner logs in	Remarks
Keep the print order.	Off	-	-	-	-	The equipment does not enter the energy saver mode if the suspended jobs are left as they are. After the suspension, the jobs of other owners are resumed.
Resume the skipped jobs automatically after clearing the causes of suspension.	On	Arbitrary choice	Off	Resume	Arbitrary choice	The skipped jobs might not be resumed depending on the causes of suspension.
Do not resume the suspended jobs automatically.	On	Arbitrary choice	On	Skipped	Arbitrary choice	Received faxes could be left skipped. Set [Auto] for [Behavior after recovering suspended cause] to avoid this situation.
Allow only the log-in job owner to restart the suspended jobs.	On	Arbitrary choice	On	Skipped	On	Received faxes could be left skipped. Set [Auto] for [Behavior after recovering suspended cause] to avoid this situation.
Enter the energy saver mode as soon as possible even if jobs are left.	On	Arbitrary choice	On	Arbitrary choice	Arbitrary choice	-
Delete the left jobs after the specific time.	On	On (Select the time.)	On	Arbitrary choice	Arbitrary choice	If [Job Skip Immediately] is set to [Off], the jobs left suspended cannot be deleted.

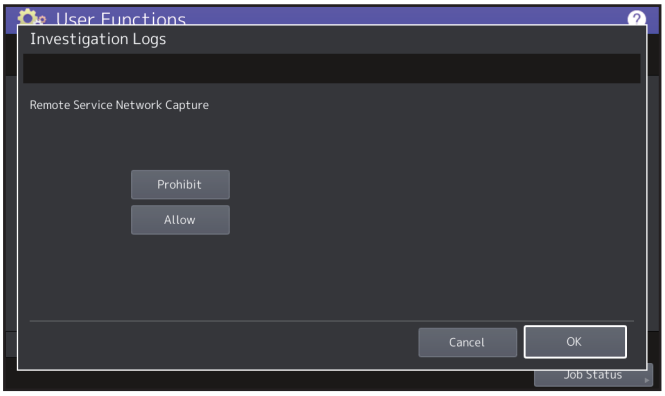
Note

Regardless of the job control settings, jobs are not skipped and they are left suspended in the following situations:

- Consecutive copy printing is suspended.
- The first proof copy printing is suspended.
- Interrupt copy printing is suspended.

❑ Allowing the acquisition of the investigation logs

You can set whether to allow the service technician to get the investigation logs.



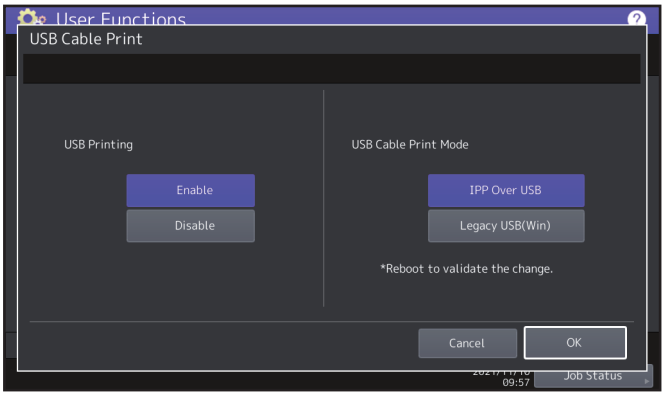
Item name	Description
Prohibit	Select this to prohibit the service technician from getting the investigation logs.
Allow	Select this to allow the service technician to get the investigation logs.

■ USB Cable Print

A setting to enable or disable USB Cable Print has been added.

Tip

This settings are linked to the settings on the [Administrator] Tab > [Setup] > [Print Service settings] > [USB Cable Print] screen of **TopAccess**.
🕮 P.58 “Setting up USB Cable Print”

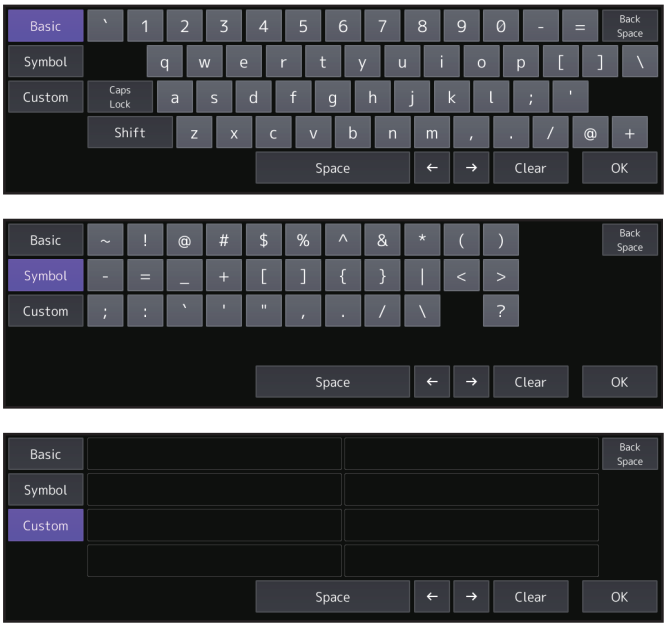


Item name	Description
USB Printing	Set whether to enable or disable USB cable printing.
USB Cable Print Mode	Select the mode used for printing via a USB connection. • **IPP Over USB**— Normally use this mode. Tip Select this item to print using the AirPrint function. • **Legacy USB (Win)**— Use this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

■ Inputting Characters

❑ On-screen keyboard

A Custom keyboard has been added.



Item name	Description
Basic	Press this to access the basic keys.
Symbol	Press this to access the symbol keys.
Custom	Press this to show the custom keyboard that facilitates typing the fixed expressions and E-mail addresses in the entry box. Tip The custom keyboard needs to be set up via **TopAccess**. For details, see the reference below: 📖 P.76 “Custom Keyboard Setting”
Caps Lock	Press this to switch capital letters and small letters.
Shift	Press this to enter capital letters.
Space	Press this to enter a space.
← →	Press these to move the cursor.
Clear	Press this to delete all characters entered.
Close	Press this to close the on-screen keyboard.
Back Space	Press this to delete the character before the cursor.

■ List Print

❑ Function List (Administrator)

GENERAL

Function	Description	User
JOB CONTROL - ENABLE JOB SKIP CONTROL	Shows whether the Job Skip Control is enabled or disabled.	NO
JOB CONTROL - JOB SKIP IMMEDIATELY	Shows whether to skip jobs immediately.	NO
JOB CONTROL - BEHAVIOR AFTER RECOVERING SUSPENDED CAUSE	Shows the operation after clearing the cause of the suspension.	NO
JOB CONTROL - RESTART ONLY IF OWNER LOGS IN	Shows whether only the log-in job owner can restart the skipped jobs.	NO
JOB CONTROL - AUTO DELETE TIMER	Shows the time to delete the skipped jobs automatically.	NO

FAX

Function	Description	User
Received Forward Setting for Application - Enable Received Forward?	Shows whether Fax Received Forward is enabled or disabled.	NO
Received Forward Setting for Application - Backup Setting?	Shows whether backing up of a received fax is enabled or disabled.	NO

NETWORK SETTING - SESSION - SMB SESSION

Function	Description	User
SMB 1.0 SUPPORT FOR SERVER	Shows whether the SMB 1.0 server is enabled or disabled.	NO
SMB 1.0 SUPPORT FOR CLIENT	Shows whether the SMB 1.0 client is enabled or disabled.	NO

NETWORK SETTING - SESSION - BONJOUR SESSION

Function	Description	User
CHROME OS PRINT	Shows whether the Chrome OS Print service is enabled or disabled.	NO

NETWORK SETTING - NETWORK SERVICE - SSL/TLS SETTING *1

Function	Description	User
TLS VERSIONS	Shows whether TLS 1.2 and TLS 1.3 are enabled or disabled.	NO
CIPHER SETTINGS FOR TLS 1.2 - KEY EXCHANGES	Shows whether ECDHE, DHE, and RSA are enabled or disabled.	NO
CIPHER SETTINGS FOR TLS 1.2 - ENCRYPTION ALGORITHMS	Shows whether AES256-GCM, AES128-GCM, AES256, and AES128 are enabled or disabled.	NO
CIPHER SETTINGS FOR TLS 1.2 - HASH ALGORITHMS	Shows whether SHA384, SHA256, and SHA1 are enabled or disabled.	NO

*1 This function is not available for some models.

OFF DEVICE CUSTOMIZATION ARCHITECTURE

Function	Description	User
SOAP - ENABLE PORT	Shows whether the port is enabled or disabled.	NO
SOAP - PORT NUMBER	Shows the port number.	NO
SOAP - ENABLE SSL/TLS	Shows whether SSL/TLS is enabled or disabled.	NO
SOAP - SSL/TLS PORT NUMBER	Shows the SSL/TLS port number.	NO
SOAP - SESSION TIMEOUT	Shows the session timeout period.	NO
REST - ENABLE PORT	Shows whether the port is enabled or disabled.	NO
REST - PORT NUMBER	Shows the port number.	NO
REST - ENABLE SSL/TLS	Shows whether SSL/TLS is enabled or disabled.	NO
REST - SSL/TLS PORT NUMBER	Shows the SSL/TLS port number.	NO
REST - SESSION TIMEOUT	Shows the session timeout period.	NO

4

TopAccess

■ [User Management] Tab Page Overview

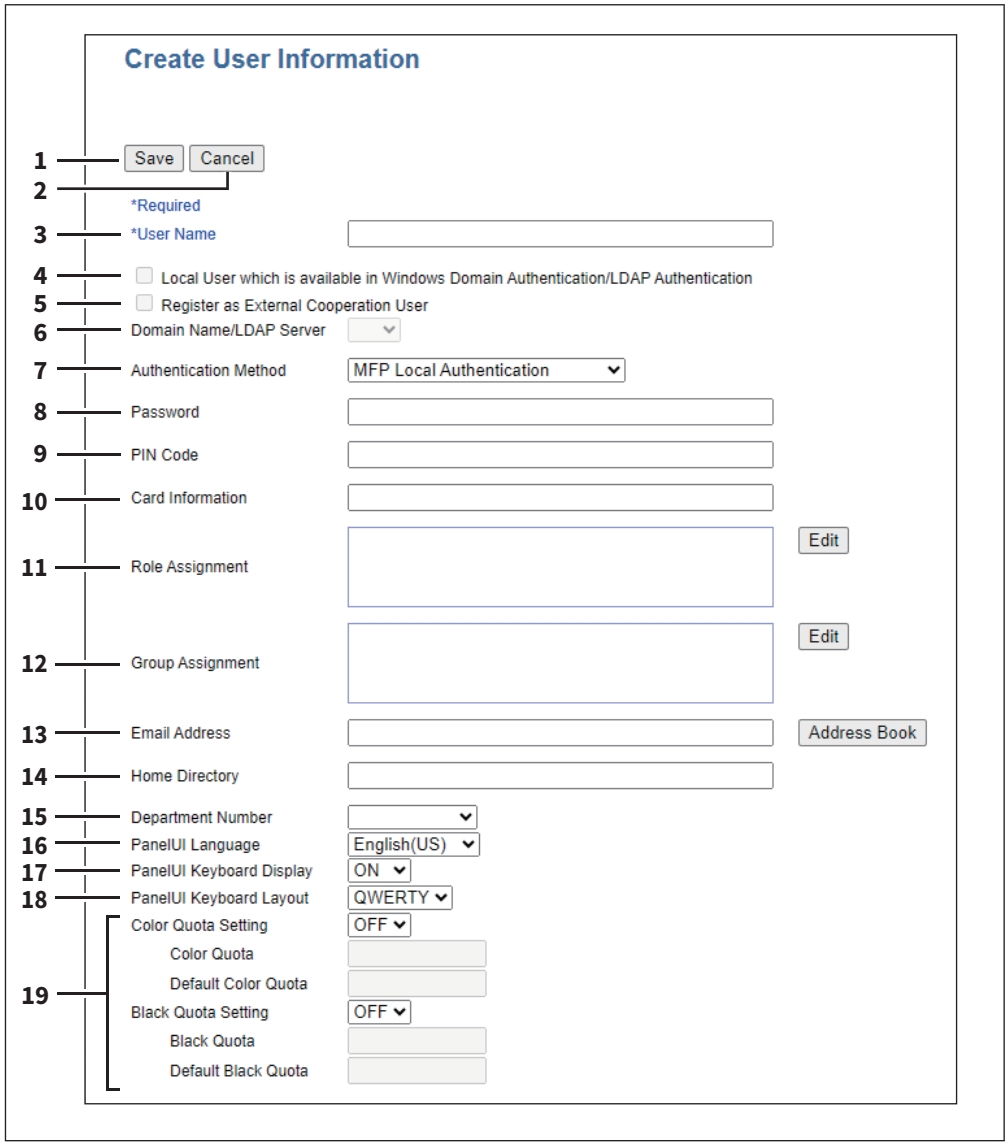
P.24 “[User Accounts] Item list <access policy mode>”

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

P.24 “[Create User Information] screen”
P.27 “[Edit User Information] screen”

[Create User Information] screen

You can register new user information.



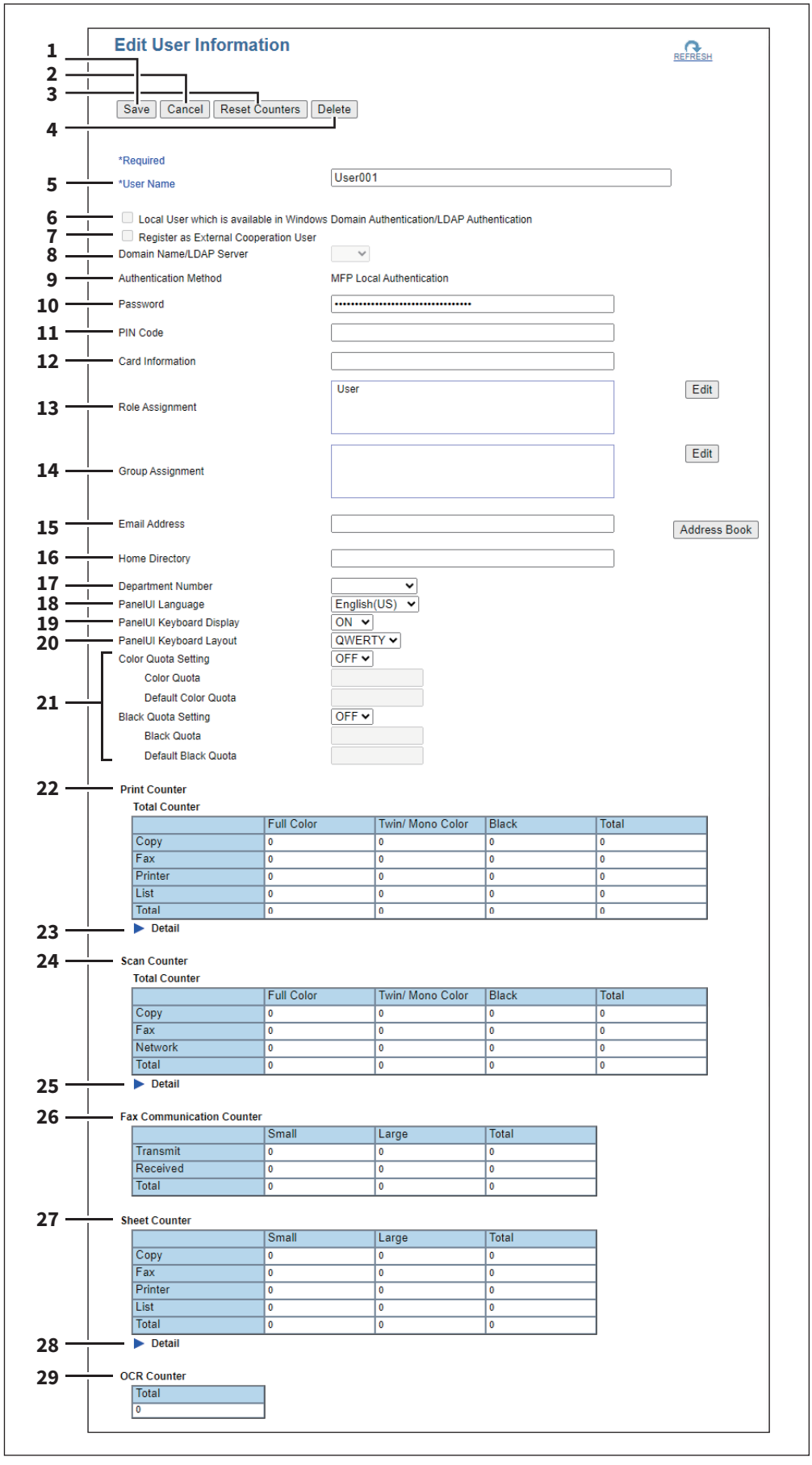
	Item name	Description
1	[Save] button	Saves the entered user information.
2	[Cancel] button	Cancels creating user information.
3	User Name	Enter the user name. You can enter up to 128 alphanumerical characters and symbols (except the following: " * + , / : ; < = > ? [\ ] | space).

	Item name	Description
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.68 “Windows Domain Authentication” P.70 “LDAP Authentication”	
5	Register as External Cooperation User	Contact your service technician for details.
6	Domain Name/LDAP Server	Select the domain name or LDAP server.
7	Authentication Method	Select the user authentication method. • **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.
8	Password	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the password. You can enter up to 64 alphanumerical characters and symbols (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \ space).
9	PIN Code	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the PIN code for the user authentication.
	Note • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. P.61 “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.	
10	Card Information	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Enter the information necessary for card authentication.
11	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.
12	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.
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 128 half-width alphanumerical characters and symbols.

	Item name	Description
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	Select from the registered departments.
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 pattern displayed on the touch panel.
19	Quota Setting	Select this to perform the quota setting of the department according to the setting specified in the [Quota Setting] screen on the [Counter] tab. • **OFF** — Not performed • **ON** — Performed
	Quota	Displays the quota amount. This value decreases according to the weight set in the [Quota Setting] screen on the [Counter] tab, 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 in the [Quota Setting] screen on the [Counter] tab, you can enter up to 99,999,999. When [Job Quota] is set in the [Quota Setting] screen on the [Counter] tab, you can enter up to 99,999,999.99.

[Edit User Information] screen

You can update registered user information.



	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.
5	User Name	Displays the user name.
	Note If you change any settings, the changes will be reflected from the next time you log in.	
6	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.
	Note The above setting is available only when the [Local User which is available in Windows Domain Authentication/LDAP Authentication] checkbox is selected. 📖 P.68 “Windows Domain Authentication” 📖 P.70 “LDAP Authentication”	
7	Register as External Cooperation User	Contact your service technician for details.
8	Domain Name/LDAP Server	Displays the registered domain name or LDAP server. Select this item if you want to change. You can select this item only when the authentication method is [Windows Domain Authentication] or [LDAP Authentication].
9	Authentication Method	Displays the user authentication method. • **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.
10	Password	You can change the password only when the authentication method is [MFP Local Authentication].
	Note If you change any settings, the changes will be reflected from the next time you log in.	
11	PIN Code	Displays the PIN code for the user authentication. You can set this item only when the authentication method is [MFP Local Authentication].
	Note • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. 📖 P.61 “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.	
12	Card Information	Enter the information necessary for card authentication. You can set this item only when the authentication method is [MFP Local Authentication].

	Item name	Description
13	Role Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Displays the registered roles. Click the [Edit] button and select roles from the displayed screen.
	Note If you change any settings, the changes will be reflected from the next time you log in.	
14	Group Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Displays the registered groups. Click the [Edit] button and select groups from the displayed screen.
	Note If you change any settings, the changes will be reflected from the next time you log in.	
15	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.
16	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".
17	Department Number	Displays the registered departments. Select this item if you want to change.
18	PanelUI Language	Displays the registered display languages of the touch panel. Select this item if you want to change.
19	PanelUI Keyboard Display	Select whether to display the soft-keyboard when entering characters with the touch panel.
20	PanelUI Keyboard Layout	Displays the registered keyboard patterns for the touch panel. Select this item if you want to change.
21	Quota Setting	Select this to perform the quota setting of the department according to the setting specified in the [Quota Setting] screen on the [Counter] tab. • **OFF** — Not performed • **ON** — Performed
	Quota	Displays the quota amount. This value decreases according to the weight set in the [Quota Setting] screen on the [Counter] tab, 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 in the [Quota Setting] screen on the [Counter] tab, you can enter up to 99,999,999. When [Job Quota] is set in the [Quota Setting] screen on the [Counter] tab, you can enter up to 99,999,999.99.
22	Print Counter	Displays the output total count value.

	Item name	Description
23	Detail	Displays details of the total output count value when you click [▶]. **Copy Counter**: Displays the number of pages printed by copy operations for paper sizes set on your equipment. **Fax Counter**: Displays the number of pages printed by fax reception for paper sizes set on your equipment. **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. **List Counter**: Displays the number of pages printed by system page print operations for paper sizes set on your equipment.
24	Scan Counter	Displays the total count value of scanned documents.
25	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.
26	Fax Communication Counter	Displays the communication record.
27	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.
28	Detail	Displays details of the number of printed sheets when you click [▶]. **Copy Counter**: Displays the number of sheets printed by copy operations for paper sizes set on your equipment. **Fax Counter**: Displays the number of sheets printed by fax reception for paper sizes set on your equipment. **Printer Counter:** Displays the number of sheets printed by print operations and E-mail reception (Internet Fax reception) for paper sizes set on your equipment. **List Counter:** Displays the number of sheets printed by system page print operations for paper sizes set on your equipment.
	Note This item is available only for some models.	
29	OCR Counter	Displays the number of images to which an OCR process has been performed.
	Tip This OCR Counter appears only when an OCR Enabler is installed.	

■ [Setup] Item List

P.31 “General Settings”
P.32 “Network Settings”
P.46 “Fax Settings”
P.47 “Setting up InternetFax Setting”
P.49 “MFP Collaboration”
P.58 “Print Service Settings”
P.59 “Embedded Web Browser settings”
P.59 “Off Device Customization Architecture settings”

Tip

Users who have been granted administrator authority in access policy mode can access the [Setup] menu from the [Administration] tab.
See the **TopAccess Guide** for details on accessing.

❑ General Settings

P.31 “Setting up Job Skip Control”

Tip

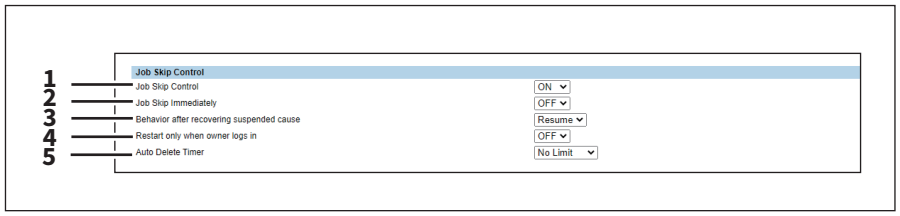
The [General] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
P.31 “[Setup] Item List”

Setting up Job Skip Control

Settings for [Job Skip immediately], [Behavior after recovering suspended cause], [Restart only when owner logs in] and [Auto Delete Timer] have been added.

Tip

This settings are linked to the settings on the [SETTING ITEM (Admin)] > [General] > [Job Control] > [Job Skip Control] screen of **User Functions**.
P.16 “Setting the 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. • **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	Select whether to allow only the log-in job owner to restart the skipped jobs when the user authentication is enabled. Note When the user authentication is disabled, any user can restart skipped jobs regardless of this setting.
5	Auto Delete Timer	Set the time to delete the skipped jobs. [No Limit] does not delete skipped jobs.

❑ Network Settings

P.32 “SSL/TLS Settings”
P.33 “Setting up SMB”
P.37 “Setting up SMTP Client”
P.40 “Setting up POP3 Client”
P.43 “Setting up Bonjour”
P.44 “Setting up SLP”
P.44 “VNC Setting”

Tip

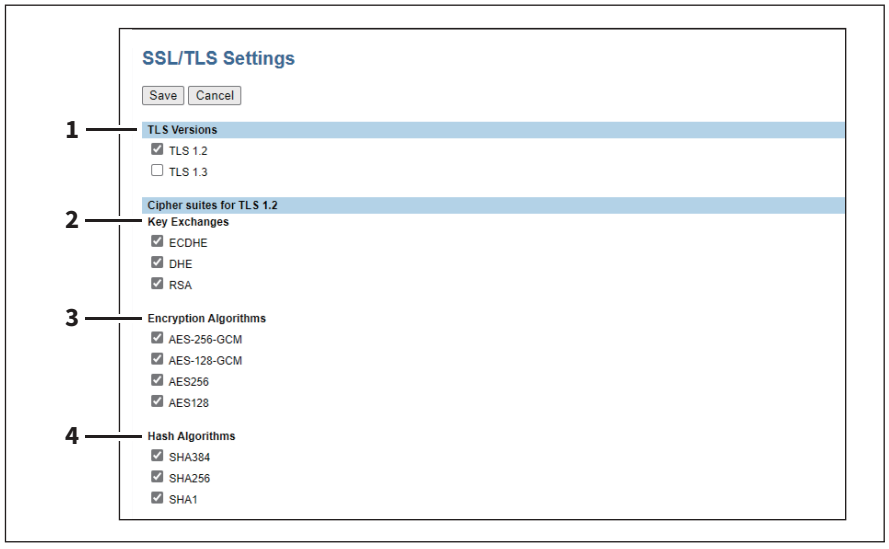
The [Network] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
P.31 “[Setup] Item List”

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.

Note

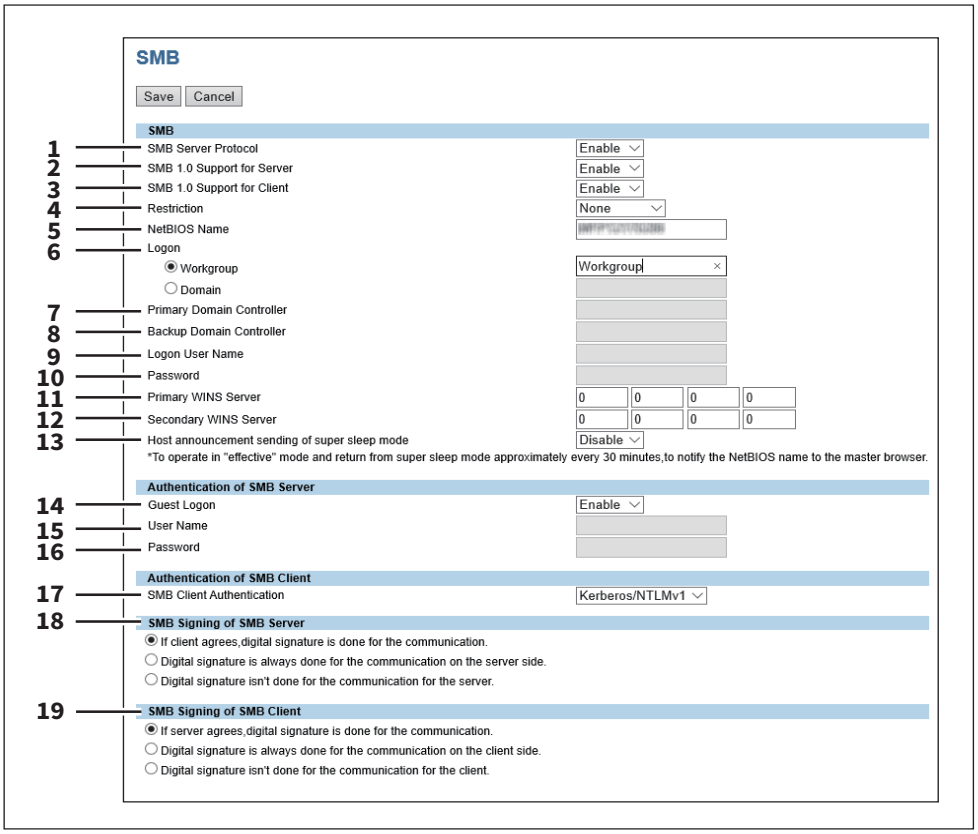
This function is not available for some models.



	Item name	Description
1	TLS Versions	Select the versions of TLS 1.2 and 1.3. Note • 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 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.



	Item name	Description
1	SMB Server Protocol	Select whether the SMB protocol is enabled or disabled. • **Enable** — Select this to enable SMB. • **Disable** — Select this to disable SMB.
2	SMB 1.0 Support For Server	Select whether the SMB 1.0 server is enabled or disabled. • **Enable** — Select this to enable the SMB 1.0 server. • **Disable** — Select this to disable the SMB 1.0 server.

	Item name	Description
3	SMB 1.0 Support For Client	Select whether the SMB 1.0 client is enabled or disabled. • **Enable** — Select this to enable the SMB 1.0 client. • **Disable** — Select this to disable the SMB 1.0 client.
4	Restriction	Specify restrictions on SMB. • **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.
5	NetBIOS Name	Enter the NetBIOS name of this equipment. The equipment uses “MFP<NIC Serial Number>” as the default NetBIOS name.
	Note You can enter only alphanumerical characters and “-” (a hyphen) for NetBIOS names. If you use any other characters, a warning message will be displayed.	
6	Logon	Enter the workgroup or domain that this equipment joins. • **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.
	Note 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.	
7	Primary Domain Controller	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).
8	Backup Domain Controller	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).
	Note 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.	
9	Logon User Name	Enter a valid user name to log on to the specified domain. You can enter up to 128 alphanumerical characters and symbols other than " / \ [ ] : ; | = , + * ? < >.
10	Password	Enter the password for the specified log on user name to log on the domain network. You can enter up to 128 alphanumerical characters.

	Item name	Description
11	Primary WINS Server	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.
	Tip 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.	
12	Secondary WINS Server	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.
	Tip 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. Note If “0.0.0.0” is entered for the Primary WINS Server and Secondary WINS Server, this equipment will not use the WINS server.	
13	Host announcement sending of super sleep mode	Specify this to display this equipment’s icon in the “Network” folder on the Windows computer even in super sleep mode. • **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.
	Note 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.	
14	Guest Logon	Select whether a guest user can log on to the SMB server. [Enable] is set as the default.
15	User Name	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 " / \ [ ] : ; | = , + * ? < >.
	Note 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.	
16	Password	Enter a password of the specified user if [Guest Logon] is set to [Disable]. You can enter up to 128 alphanumerical characters and symbols.
	Note 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.	

	Item name	Description
17	SMB Client Authentication	Specify the authentication method for the SMB clients. • **Kerberos/NTLMv2** — Specify this when connecting to an SMB server using Kerberos/NLTMv2 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.
	Note SMB servers running Mac OS X 10.10 or later do not support NTLMv1 authentication.	
18	SMB Signing of SMB Server	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. • **If server 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.
	Note 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.	

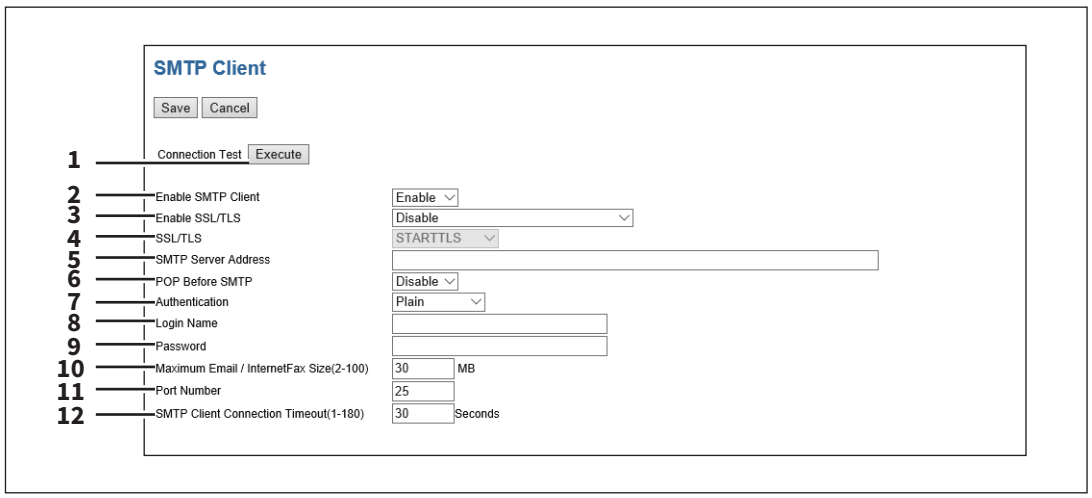
	Item name	Description
19	SMB Signing of SMB Client	Select whether SMB Signing is enabled or disabled when this equipment accesses the clients using SMB, such as when this equipment stores the scanned data in the network folder using SMB. • **If server agrees, digital signature is done for the communication.** — 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.
	Note • 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. 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.	

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 following sections:
The From Address can be also determined automatically when the User Management Setting is enabled.



	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. • **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.
	Note • When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment. • Not all operating systems support SSL/TLS for all protocols.	
4	SSL/TLS	Select the protocol for the SSL/TLS when the [Enable SSL/TLS] option is enabled. • **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).
	Note 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.	
5	SMTP Server Address	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).
	Note If you use FQDN to specify the SMTP server, you must configure the DNS server and enable the DNS in the DNS Session. Tip 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.	
6	POP Before SMTP	Select whether the POP Before SMTP authentication is enabled or disabled. [Disable] is set as the default.

	Item name	Description
7	Authentication	Select the type of authentication to access the SMTP server. • **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. • **Application** — Select this to access the SMTP 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 selected application name has appeared on the right side of the [Assignment] button, click [Save] 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 the email cloud service you want to use from the list and enter the account name for the email cloud service. Then select [Send Email] and click [Account Registration] to sign in the service.

Note

If you select [Application], take note of the following points:

- 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 SMTP server. Install or update the application with the renewed credentials. For details, contact your service technician or representative.
- When an attempt is made to use an address differing from the account registered in the email cloud service for [From Address] of [Email Settings], there is a upper limitation in the number of the addresses which can be sent by the email cloud service. For details, contact your service technician or representative.
- [Application] cannot be selected in [Email Authentication].
- [Single Sign On Setting] will be disabled.
- When you use different cloud services on the SMTP server and the POP3 server, enter different account names (email addresses) for each.

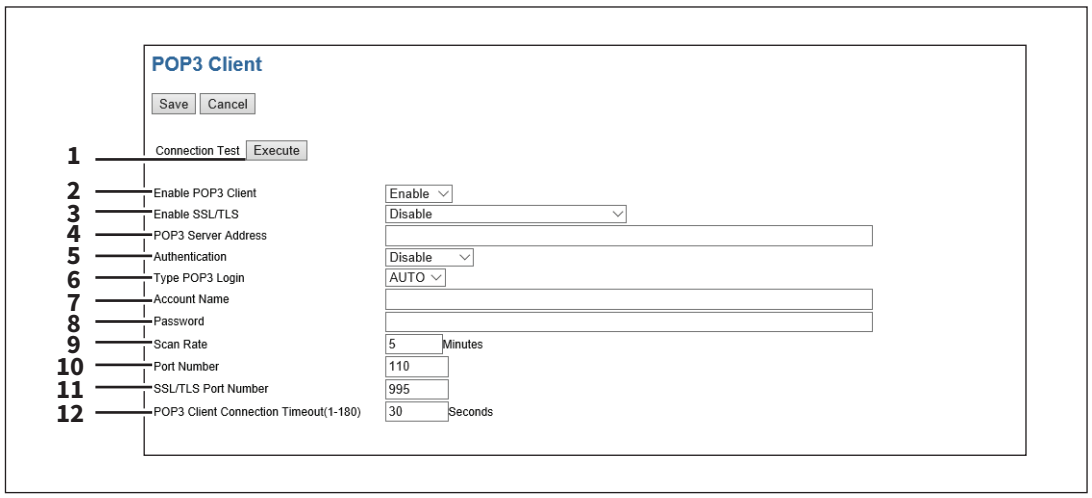
Tip

- 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].

	Item name	Description
8	Login Name	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.
	Note • Enter the account name for accessing a POP3 server when the POP Before SMTP authentication is enabled. P.40 “Setting up POP3 Client” • Enter the same account name you have registered on the setting screen of the application when [Application] is selected in the [Authentication] option.	
9	Password	Enter the password to access the SMTP server if the SMTP authentication is enabled. You can enter up to 128 alphanumerical characters and symbols.
	Note Enter the password for accessing a POP3 server when the POP Before SMTP authentication is enabled. P.40 “Setting up POP3 Client” **Tip** You cannot enter any passwords, which are not required, when [Application] is selected in the [Authentication] option.	
10	Maximum Email / InternetFax Size (2-100)	Select the maximum size that this equipment is allowed to send using the SMTP. Specify within the range from 2 to 100 MB.
	Note 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.	
11	Port Number	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.
	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.	
12	SMTP Client Connection Timeout(1-180)	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.

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	Select whether the SSL (Secure Sockets Layer)/TLS (Transport Layer Security) is enabled or disabled for POP3 transmission. • **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.
	Note • When [Verify with imported CA certification(s)] is selected, you must import the CA certificate in this equipment. • Not all operating systems support SSL/TLS for all protocols.	
4	POP3 Server Address	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).
	Note If you use FQDN to specify the POP3 server, you must configure the DNS server and enable the DNS in the DNS Session. Tip 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.	

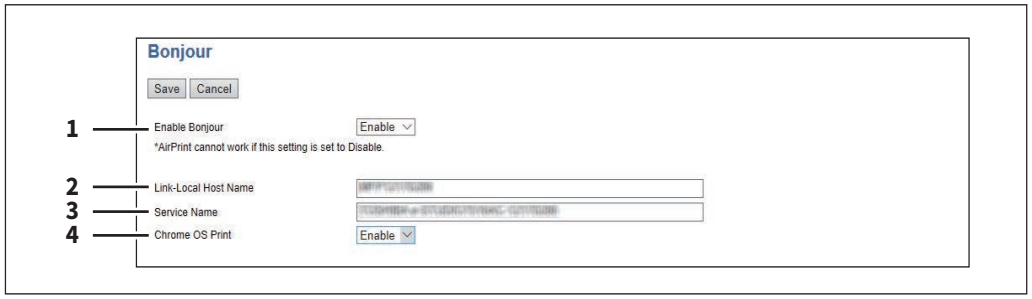
<table>
<tr><th></th><th>Item name</th><th>Description</th></tr>
<tr><td>5</td><td>Authentication</td><td>Enable or disable the authentication for accessing the POP3 server.
• <u>Disable</u> — Select this to disable the authentication.
• NTLM/SPA — Select this to access the POP3 server using the NTLM/SPA 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 selected application name has appeared on the right side of the [Assignment] button, click [Save] 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 the email cloud service you want to use from the list and enter the account name for the email cloud service. Then select [Receive Email] and click [Account Registration] to sign in the service.</td></tr>
<tr><td></td><td colspan="2">Note
If you select [Application], take note of the following points:
• 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. For details, contact your service technician or representative.
• When you use different cloud services on the SMTP server and the POP3 server, enter different account names (email addresses) for each.

Tip
• 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].</td></tr>
<tr><td>6</td><td>Type POP3 Login</td><td>Select the POP3 login type.
• <u>AUTO</u> — 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.</td></tr>
<tr><td></td><td colspan="2">Note
• 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.</td></tr>
</table>

	Item name	Description
7	Account Name	Enter the account name for this equipment to access the POP3 server. You can enter up to 96 alphanumerical characters and symbols.
	Note • 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	Enter the password for this equipment to access the POP3 server. You can enter up to 96 alphanumerical characters and symbols.
	Tip You cannot enter any passwords, which are not required, when [Application] is selected in the [Authentication] option.	
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 Bonjour

In Bonjour, you can enable or disable Bonjour (mDNS) that is available for macOS or Windows OS.



	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 the Chrome OS Print service is enabled or disabled. [Enable] is set as the default.

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.

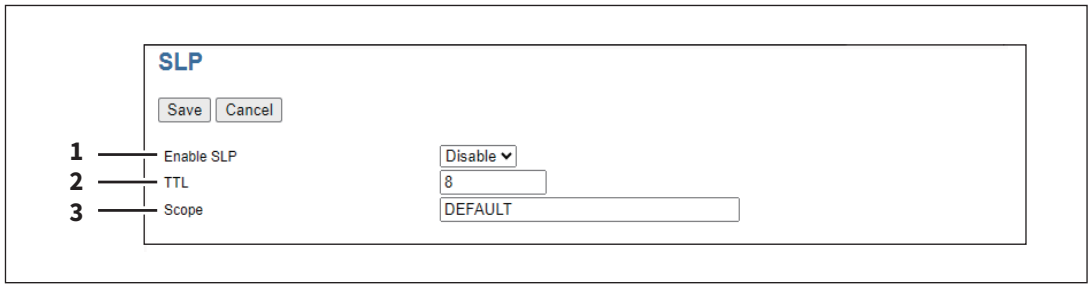
Tip

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] tab page, and that of the [Location] field of [Device Information] on the [Device] tab 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. [Disable] 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”.
	Tip • 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).	

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.

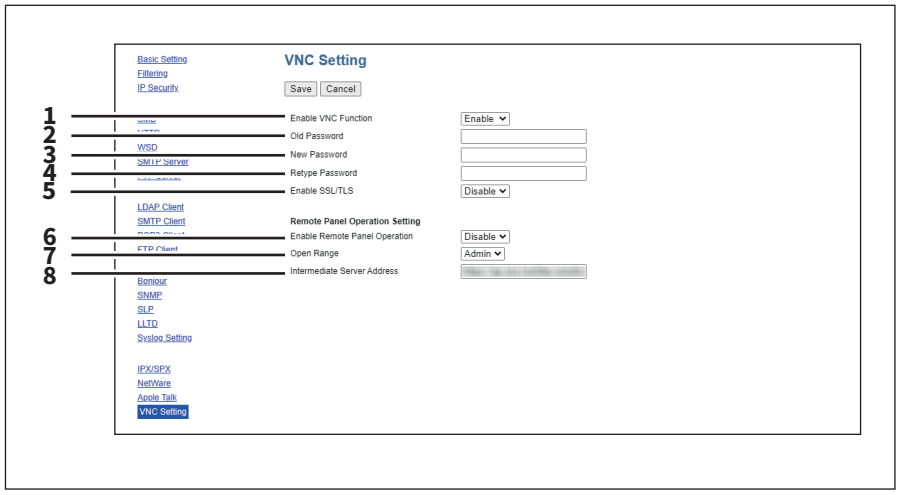
Note

- 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.



	Item name	Description
1	Enable VNC Function	Select whether the VNC function is enabled or disabled. • **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. • **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. • **Enable** — Select this to enable the remote panel operation function. • **Disable** — Select this to disable the remote panel operation function. Note For the details about [Enable Remote Panel Operation], contact your service technician or representative.
7	Open Range	Select the disclosure range of the remote panel operation function. • **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.

❑ Fax Settings

📖 P.46 “Received Forward Setting for Application”
📖 P.47 “Box Setting (Received Forward Setting for Application)”

Tip

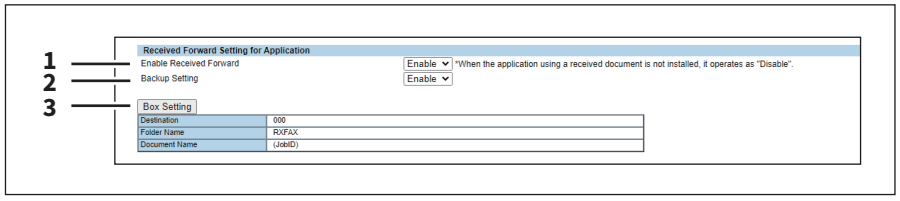
The [Fax] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
📖 P.31 “[Setup] Item List”

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.



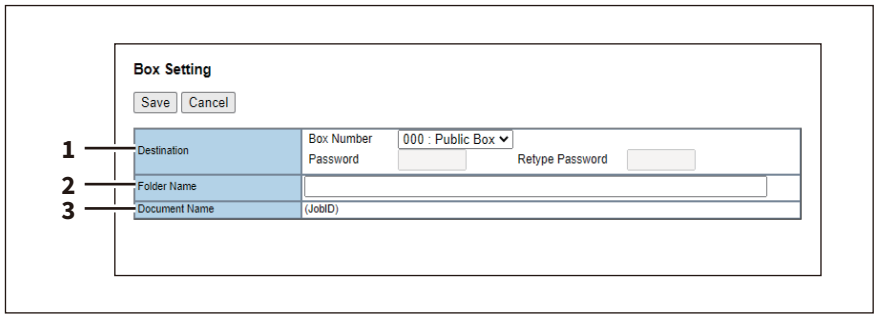
	Item name	Description
1	Enable Received Forward	Select [Enable] to save the received document in the storage area of the application. [Disable] is the default setting. Note When [Enable] is selected for [Enable Received Forward], the Received Forward to Applications setting is taken as the top priority even if other forward settings are also enabled.
2	Backup Setting	Select [Enable] to save the received document in the specified box as a backup file. [Disable] is the default setting. Tip This will be displayed when [Enable] is selected for [Enable Received Forward].
3	[Box Setting] button	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. Tip You can change the settings when [Enable] is selected for [Backup Setting].

Box Setting (Received Forward Setting for Application)

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

Note

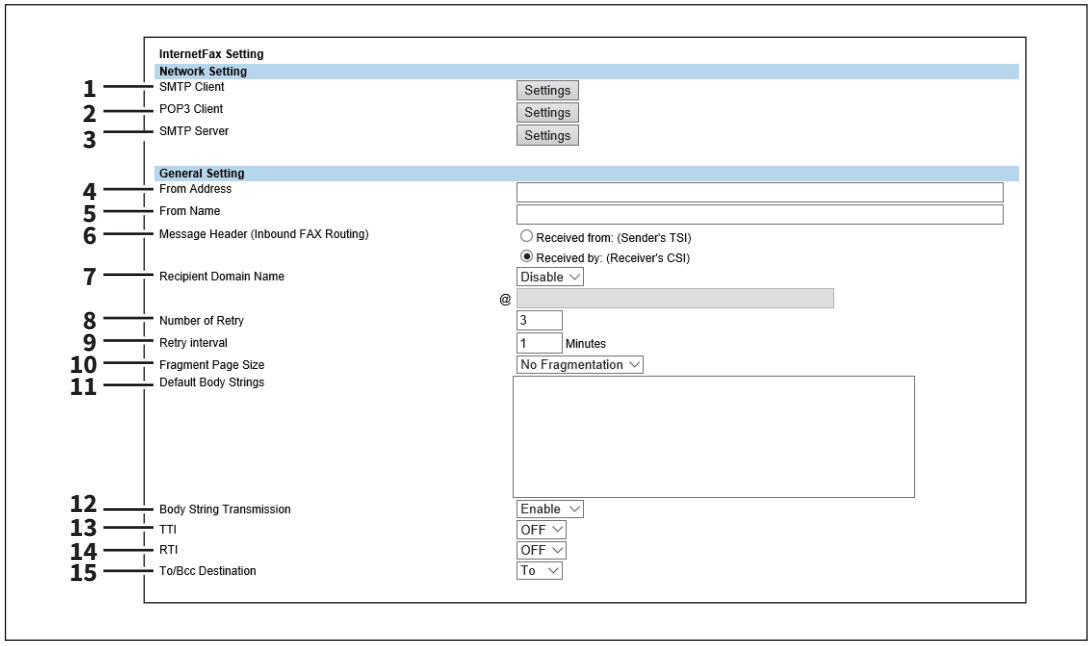
Up to 400 documents can be stored in a box or folder, and up to 200 pages can be contained in a document. If an attempt is made to store documents exceeding the available numbers, storing to e-Filing will fail. Delete unnecessary documents in a box or e-Filing periodically. Alternatively, specify the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



	Item name	Description
1	Destination	Set the box to save the received document. **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	Enter the folder name in the box where the received document is saved. You can enter up to 64 characters.
3	Document Name	A job ID applied automatically by means of the equipment is displayed. This cannot be changed.

❑ Setting up InternetFax Setting

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



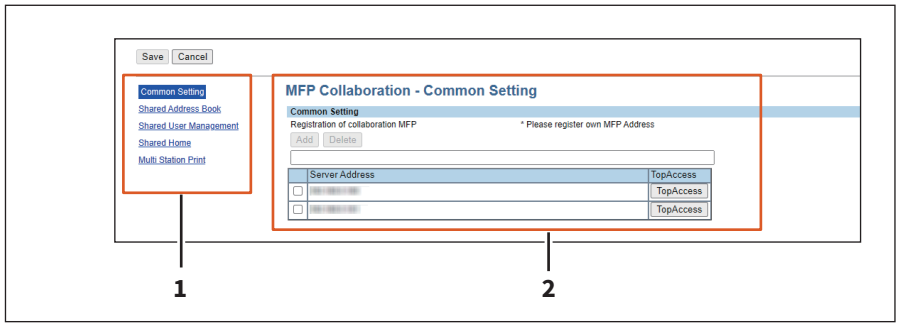
	Item name	Description
1	SMTP Client	Specify SMTP transmission for InternetFax.
	Tip See the following for how to set SMTP Client. 📖 P.37 “Setting up SMTP Client”	
2	POP3 Client	Specify the POP3 server that receives InternetFax print jobs.
	Tip See the following for how to set POP3 Client. 📖 P.40 “Setting up POP3 Client”	
3	SMTP Server	Specify SMTP reception for InternetFax.
4	From Address	Enter the E-mail address of this equipment.
	Note The [From Address] must be entered to enable Internet Fax transmission.	
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	Enable or disable automatic addition of a domain name while a destination is being entered. **Enable**: Select this to add a domain name. **Disable**: Select this not to add a domain name. 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).
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	Enter the interval to try sending the Internet Faxes when it fails. [1minutes] is set as the default.
	Note 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.	
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	You can set the destination of the internet fax to be sent only to To or Bcc.
	Note 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.	

❑ MFP Collaboration

You can make the necessary settings all at one screen for registration and collaboration of MFPs.
🕮 P.50 “Common Setting”
🕮 P.51 “Shared Address Book”
🕮 P.52 “Shared User Management”
🕮 P.54 “Shared Home”
🕮 P.56 “Multi Station Print”

Tip

The [MFP Collaboration] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
🕮 P.31 “[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. Note You need the Multi Station Print Enabler option to use the [Multi Station Print] function. Contact your service technician for details.

Common Setting

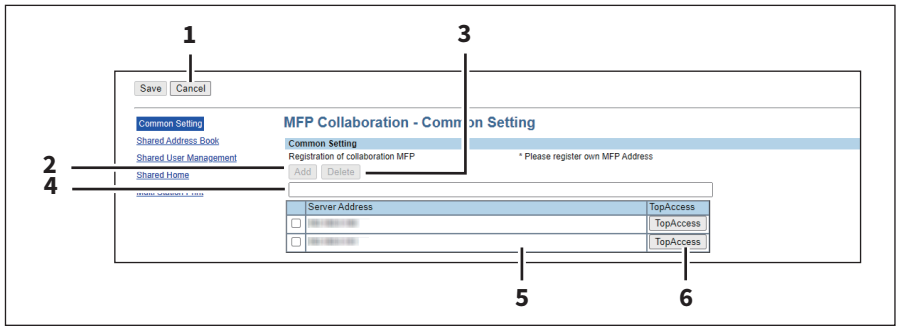
You can register MFPs all at once on this screen to set up them for collaboration.

Note

Be sure to register this equipment as a collaborating MFP.

Tip

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

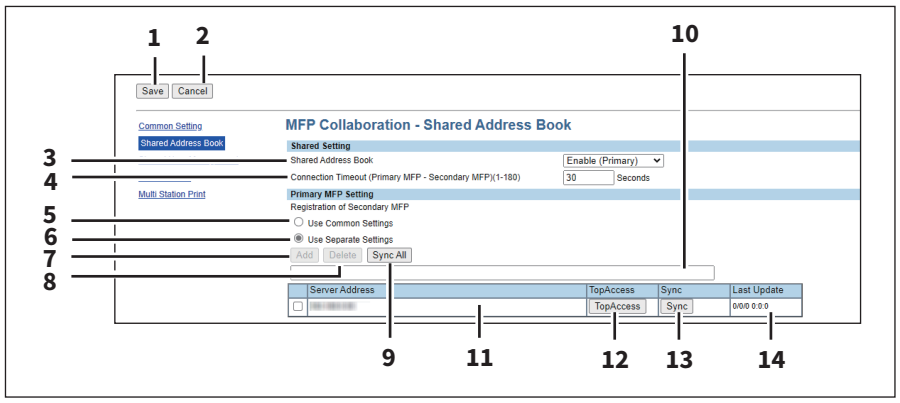
You can set the address book that is shared on the collaborating MFPs. The settings are applied to the MFPs registered in the list.
By selecting [Use Common Settings], registration information of the collaborating MFPs set in a common setting can be shared.

Note

Register MFPs on the [Common Setting] screen in advance to select the [Use Common Settings] setting.
P.50 “Common Setting”

Tip

The [Shared Address Book] settings are linked to the settings on the [Registration] Tab > [Address Book] > [Shared Setting] screen. For details, see the **TopAccess Guide**.



	Item name	Description
1	[Save] button	Saves the settings.
2	[Cancel] button	Cancels the settings.
3	Shared Address Book	Select whether this equipment should act as a primary or secondary MFP when managing the Shared Address Book in sync with other MFPs. • **Disable** — Does not synchronize. • **Enable (Primary)** — Synchronizes as a primary MFP. • **Enable (Secondary)** — Synchronizes as a secondary MFP. **Note** 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.
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	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.

	Item name	Description
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

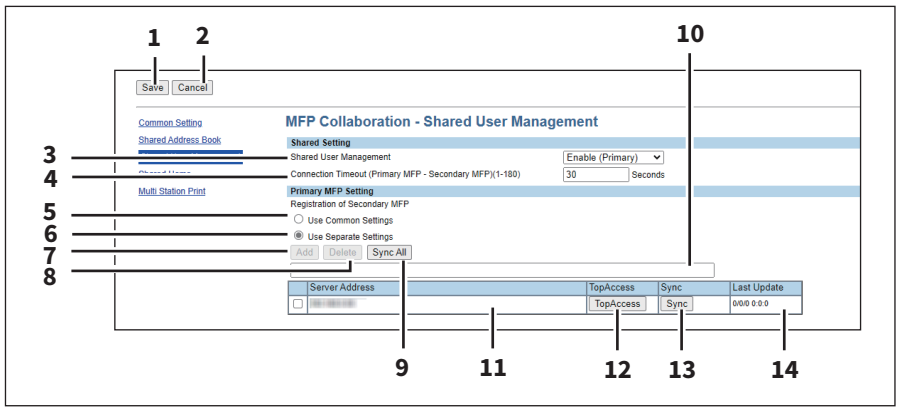
You can set the management of user information that is shared on the collaborating MFPs. The settings are applied to the MFPs registered in the list.
By selecting [Use Common Settings], registration information of the collaborating MFPs set in a common setting can be shared.

Note

- Register MFPs on the [Common Setting] screen in advance to select the [Use Common Settings] setting.
P.50 “Common Setting”
- 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] Tab > [Shared Setting] screen. For details, see the **TopAccess Guide**.
- The [Shared User Management] and [Connection Timeout] settings are linked to the settings at [Administration] Tab > [Security] > [Authentication] > [User Authentication Setting] > [Shared Setting]. For details, see the **TopAccess Guide**.



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

	Item name	Description
3	Shared User Management	Select whether this equipment should act as a primary or secondary MFP when managing user information in sync with other MFPs. • **Disable** — Does not synchronize. • **Enable(Primary)** — Synchronizes as a primary MFP. • **Enable(Secondary)** — Synchronizes as a secondary MFP. Note 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.
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	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.
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 user information.
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.
By selecting [Use Common Settings], registration information of the collaborating MFPs set in a common setting can be shared.

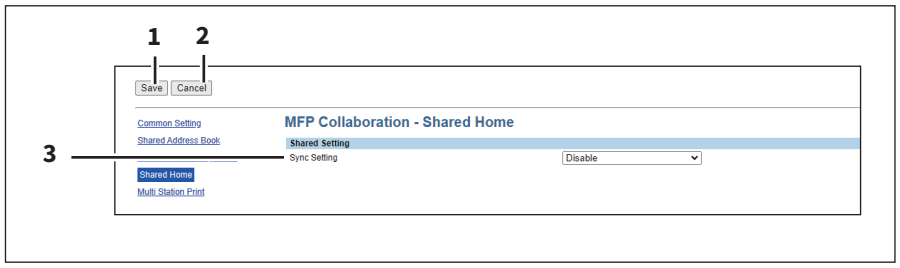
Note

Register MFPs on the [Common Setting] screen in advance to select the [Select from Common Settings] setting.
📖 P.50 “Common Setting”

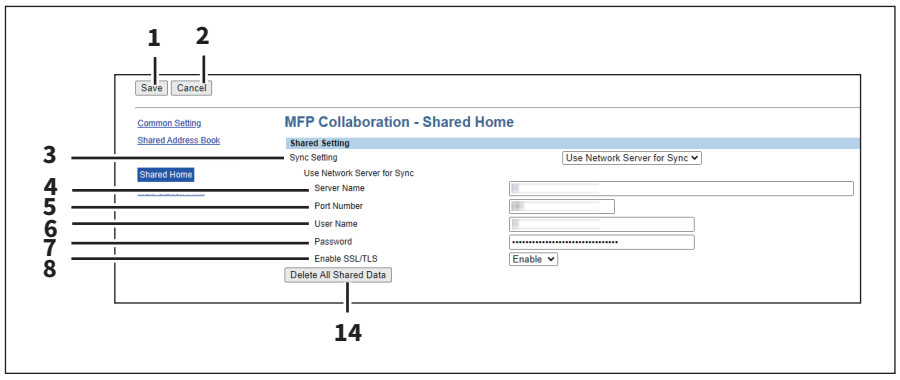
Tip

The [Shared Home] settings are linked to the settings on the [Administration] Tab > [Setup] > [General] > [Home Setting] screen. For details, see the **TopAccess Guide**.

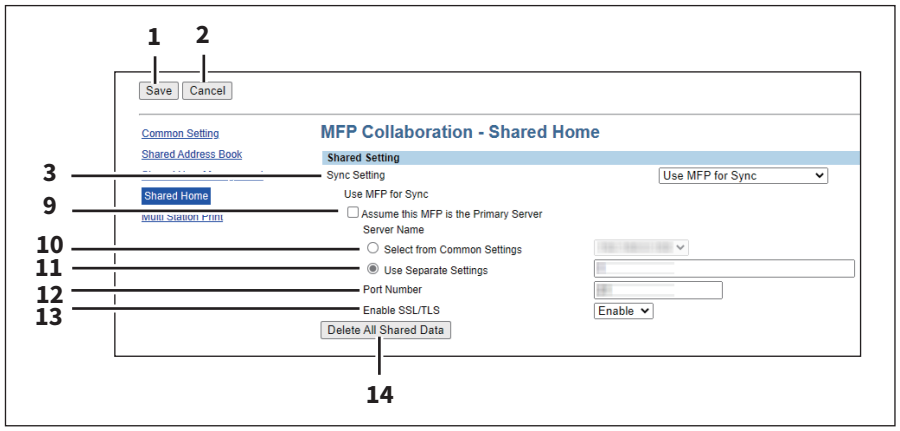
When [Disable] is selected from [Sync Setting]



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



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



	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. • **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. Note If the FTP server is disabled, you cannot set this MFP as the primary server.
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

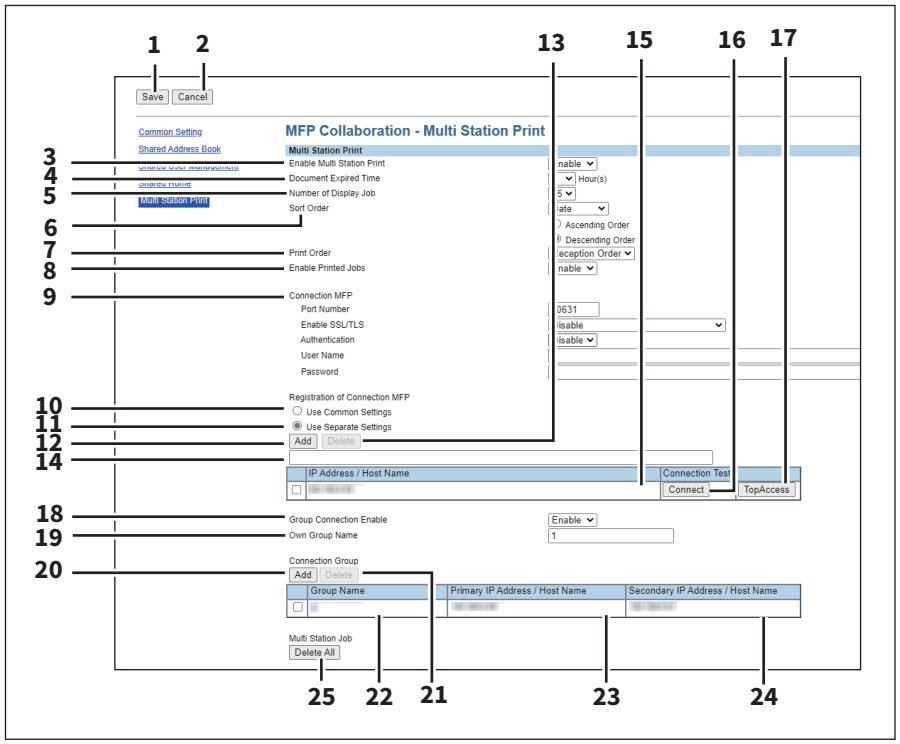
You can set the multi station print function that is used on the collaborating MFPs.
By selecting [Use Common Settings], registration information of the collaborating MFPs set in a common setting can be shared.

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.50 “Common Setting”

Tip

The [Multi Station Print] settings are linked to the settings on the [Administration] Tab > [Setup] > [Print Service] > [Multi Station Print] screen. For details, see the **TopAccess Guide**.



	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.
7	Print Order	Specify the print order. Tip When you select [Indication Order] from [Print Order], documents are printed according to the [Sort Order] setting at the item 6.
8	Enable Printed Jobs	Specify whether to enable or disable reprinting.

	Item name	Description
9	Connection MFP	Specify the following communication settings for the multi station print. • **Port Number** — Enter the port number. • **Enable SSL/TLS** — Select the SSL/TLS setting for the multi station print. - **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 alphanumerical characters and symbols except = ; # @ \. • **Password** — Enter the password of the user. You can enter up to 127 alphanumerical characters and symbols except = ; # \. Note All MFPs should have the same settings for the connection. Tip 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.
10	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.
11	Use Separate Settings	Uses information of the MFPs registered in the following list.
12	[Add] button	Allows you to add the device to connect.
13	[Delete] button	Allows you to delete the selected device.
14	Connection MFP entry field	Enter the IP address or host name of the MFP you want to register. Tip If the user authentication is disabled with more than one address registered in the [Connection MFP] list, the [Connection MFP] settings are not displayed.
15	Server Address	Shows the IP address or host name of the registered MFP.
16	[Connect] button	Tests the connection with the specified MFP to check if the communications can be established. Note Be sure to save the Multi Station Print settings with the [Save] button before you test the MFP connection with the [Connect] button.
17	[TopAccess] button	Starts TopAccess.
18	Group Connection Enable	Select whether to connect the MFP groups. [Disable] is set as the default.
19	Own Group Name	Enter a group name to which this MFP belongs. You can enter up to 12 characters. Note All groups should share the same name of each group for the connection.

	Item name	Description
20	[Add] button	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. • **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.
21	[Delete] button	Allows you to delete the selected group.
22	Group Name	Shows the name of the added connection group.
23	Primary IP Address / Host Name	Shows the IP address or host name of the primary device which represents the added connection group.
24	Secondary IP Address / Host Name	Shows the IP address or host name of the secondary device which represents the added connection group.
25	[Delete All] button	Deletes all of the multi station print jobs.

❑ Print Service Settings

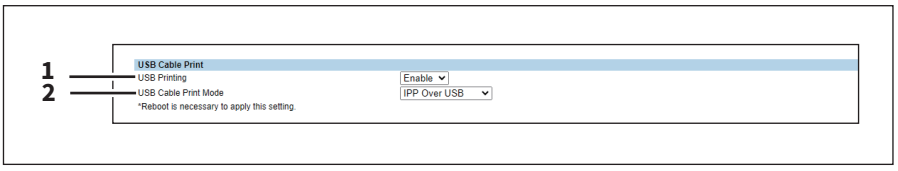
📖 P.58 “Setting up USB Cable Print”

Tip

The [Print Service] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
📖 P.31 “[Setup] Item List”

Setting up USB Cable Print

A setting to enable or disable USB Cable Print has been added.



	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.

❑ Embedded Web Browser settings

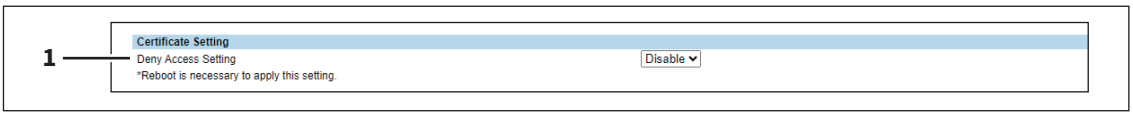
📖 P.59 “Setting up Certificate Setting”

Tip

The [EWB] submenu can be accessed from the [Setup] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
📖 P.31 “[Setup] Item List”

Setting up Certificate Setting

You can set the deny access setting for the EWB function.



	Item name	Description
1	Deny Access Setting	Makes the deny access setting. The connection of EWB is denied when this setting is enabled while [Enable SSL/TLS] is enabled in HTTP and an invalid certificate (CA certificate) is used.

❑ Off Device Customization Architecture settings

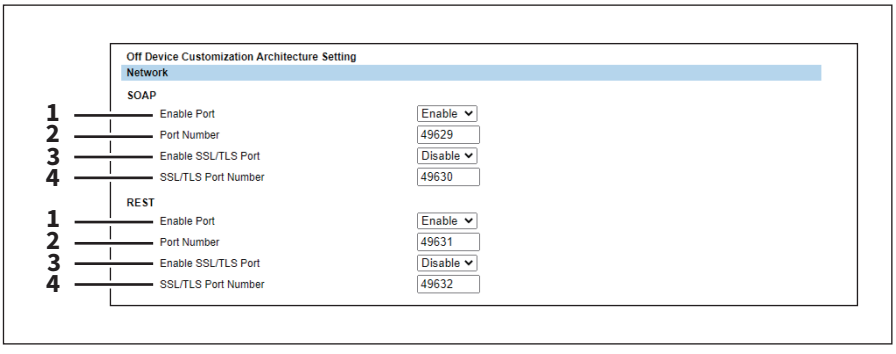
Set ODCA (Off Device Customization Architecture) when you are linking external application software to services provided by this equipment.
For details, refer to the application software manual.
📖 P.59 “Setting up Network”
📖 P.60 “Setting up Configuration”
📖 P.60 “Notification Events”

Tip

The [ODCA] submenu can be accessed from the [Setup] menu on the [Administration] page.
See the **TopAccess Guide** for how to access it and the following page for information on the [Setup] menu:
📖 P.31 “[Setup] Item List”

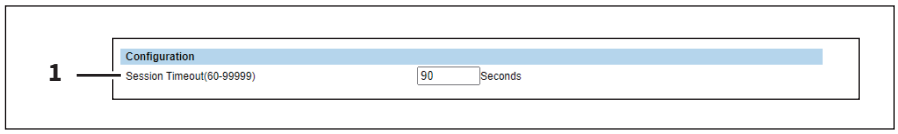
Setting up Network

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



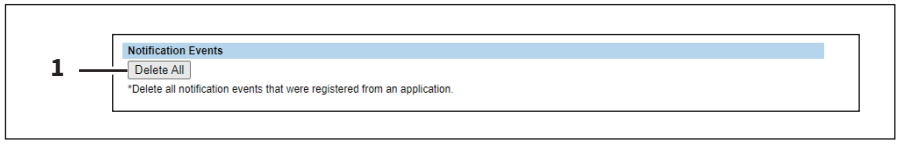
	Item name	Description
1	Enable Port	Select whether the external connection is enabled or disabled.
2	Port Number	Specify the port number where the external connection is enabled.
3	Enable SSL/TLS Port	Port Select whether SSL/TLS is enabled or disabled for the external connection.
4	SSL/TLS Port Number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

■ [Security] Item List

P.61 “Authentication settings”
P.72 “Certificate management settings”

❑ Authentication settings

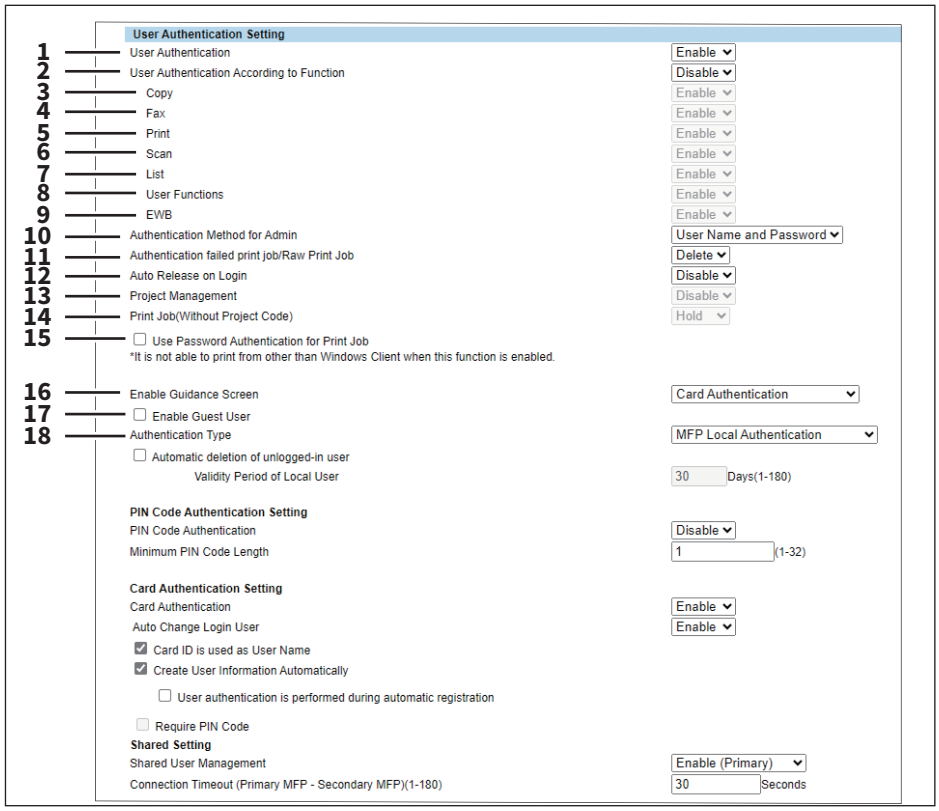
You can restrict user operations using the authentication function of your equipment.
P.61 “Setting up User Authentication Setting”

Tip

The [Authentication] submenu can be accessed from the [Security] menu on the [Administration] tab.
See the **TopAccess Guide** for details on accessing.

Setting up User Authentication Setting

You can configure user authentication to access your equipment.

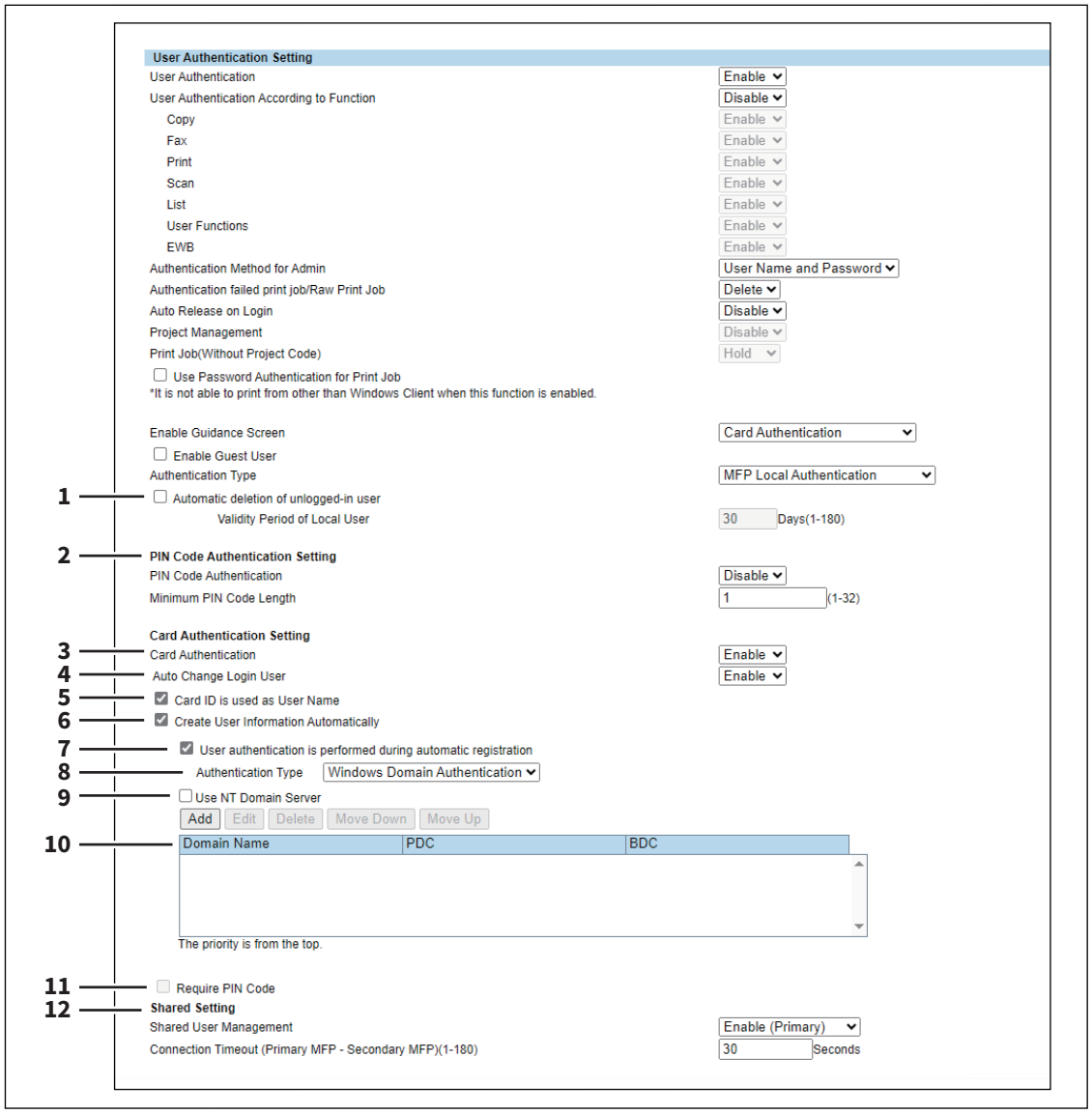


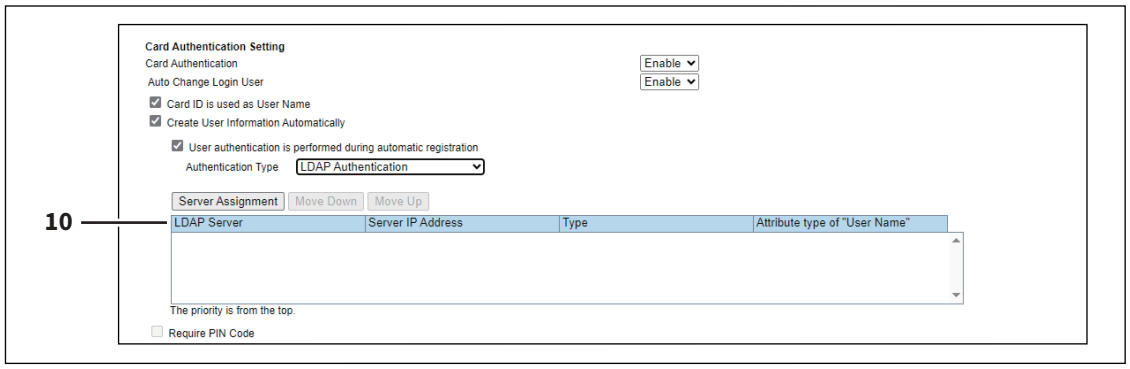
	Item name	Description
1	User Authentication	Select whether or not to enable user authentication. [Disable] is set as the default.
	Note • You cannot configure “E-mail authentication” if you enable user authentication. • The No Limit Black function becomes unavailable if you enable user authentication. For details of the No Limit Black function, refer to the **MFP Management Guide**.	
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	Enable or disable user authentication when the FAX function is used. [Enable] is set as the default.
	Note 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.	
5	Print	Enable or disable user authentication when the Print function is used. [Enable] is set as the default.
	Note When you want to set [Disable] for this function, use the latest version of a printer driver. For details, contact your service technician.	
6	Scan	Enable or disable user authentication when the Scan function is used. [Enable] is set as the default.
7	List	Enable or disable user authentication when the List function is used. [Enable] is set as the default.
8	User Functions	Enable or disable user authentication when the User Functions are used. [Enable] is set as the default.
9	EWB	Specify whether or not to enable the EWB (Embedded Web Browser) function. You need the External Interface Enabler option to use EWB.
10	Authentication Method for Admin	Select the administrator authentication method. • **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	Select whether or not to print jobs which have failed user authentication. • **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.
	Note When the N/W-Fax driver is used, selecting [Hold] deletes the job.	
12	Auto Release on Login	Specify whether to process private jobs and hold jobs at login. • **Disable** — Select this not to print at login. • **Enable** — Select this to print at login.
13	Project Management	Specify whether or not to enable project management.
14	Print Job(Without Project Code)	Specify whether or not to print the print jobs without project codes when Project Management is enabled. • **Hold** — Registers print jobs to Hold. • **Print** — Prints print jobs that failed authentication. • **Delete** — Deletes print jobs that failed authentication.
15	Use Password Authentication for Print Job	Performs user authentication for each print job. The user name and password are required to execute printing.
16	Enable Guidance Screen	Select the screen dedicated to the card authentication.
	Note For the details of the card authentication setting, contact your service technician.	
17	Enable Guest User	Enables operations by the guest user.

	Item name	Description
18	Authentication Type	Select the authentication method. • **MFP Local Authentication** 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.64 “MFP Local Authentication” • **Windows Domain Authentication** 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 is registered in the Windows domain to operate the touch panel. 📖 P.68 “Windows Domain Authentication” • **LDAP Authentication** 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 is registered in the LDAP server to operate the touch panel. 📖 P.70 “LDAP Authentication”

MFP Local Authentication





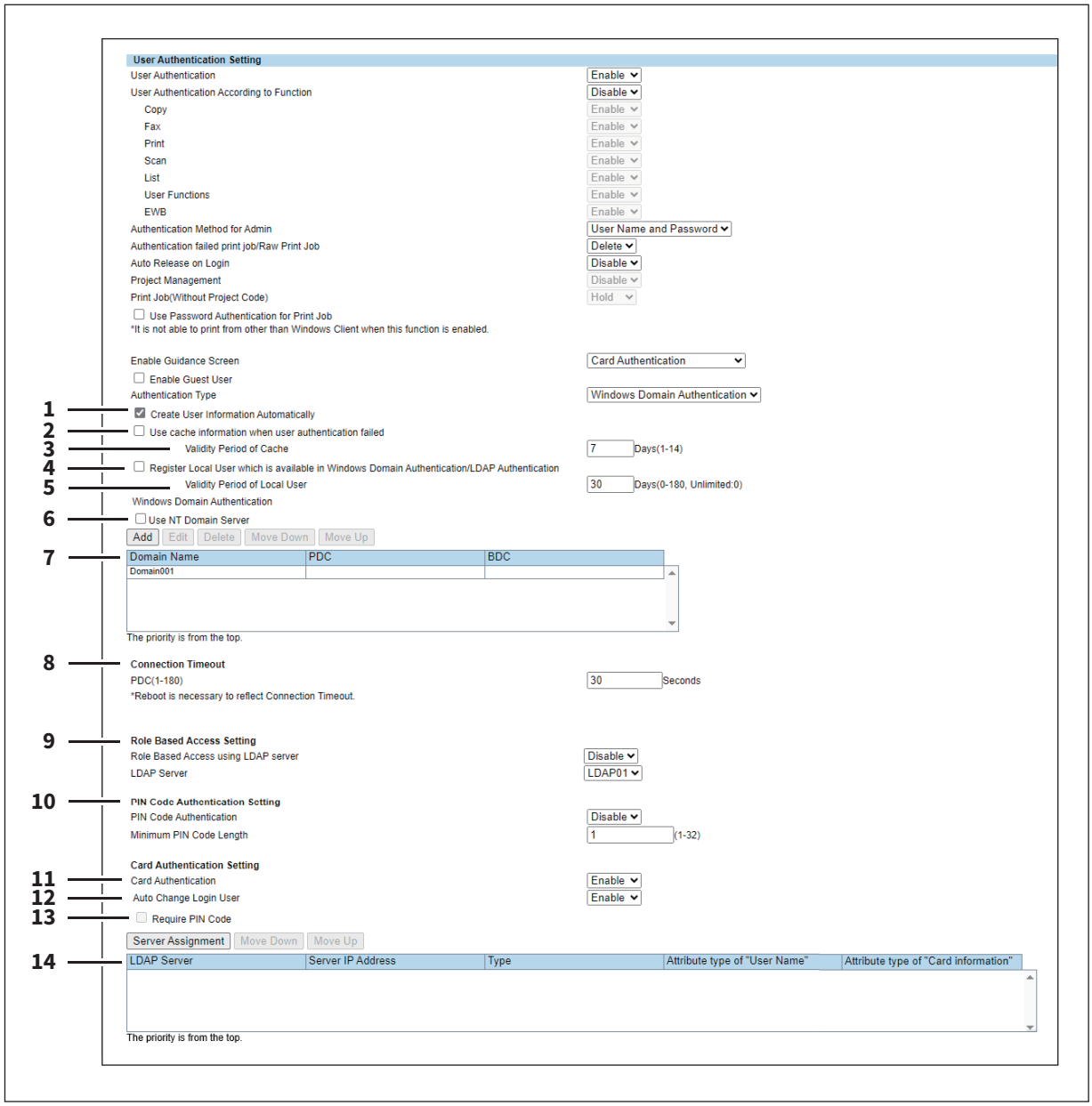
	Item name	Description
1	Automatic deletion of unlogged-in user	Enables the function to delete unlogged-in local users automatically after the specified period. If the days set in [Validity Period of Local User] have passed after local users logged out last, they are automatically deleted every 24 hours or at the restart of the equipment.

	Item name	Description
2	PIN Code Authentication Setting	**PIN Code Authentication** — Select the PIN code authentication method. • **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. **Minimum PIN Code Length** — Enter a figure that specifies the minimum digits for the PIN code.
3	Card Authentication	Select whether or not to enable card authentication. Note For the details of the card authentication setting, contact your service technician.
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	Select the authentication method for the automatic user registration when [User authentication is performed during automatic registration] is enabled. • **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	Displays up to 16 user authentication domains or servers in the list depending on the [Authentication Type] setting. • **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. **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. Note • 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. • **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.
11	Require PIN Code	Select whether or not to require PIN code when authenticating users with the card. Tip This function is available only on the equipment that supports the PIN code input.

	Item name	Description
12	Shared Setting	**Shared User Management** —Select whether this equipment should act as a primary or secondary MFP when managing user information in sync with other MFPs. • **Disable** — Does not synchronize. • **Enable(Primary)** — Synchronizes as a primary MFP. • **Enable(Secondary)** — Synchronizes as a secondary MFP. **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. Note • The [Shared User Management] and [Connection Timeout] settings are linked to the same settings on the [MFP Collaboration] > [Shared User Management] screen. • 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

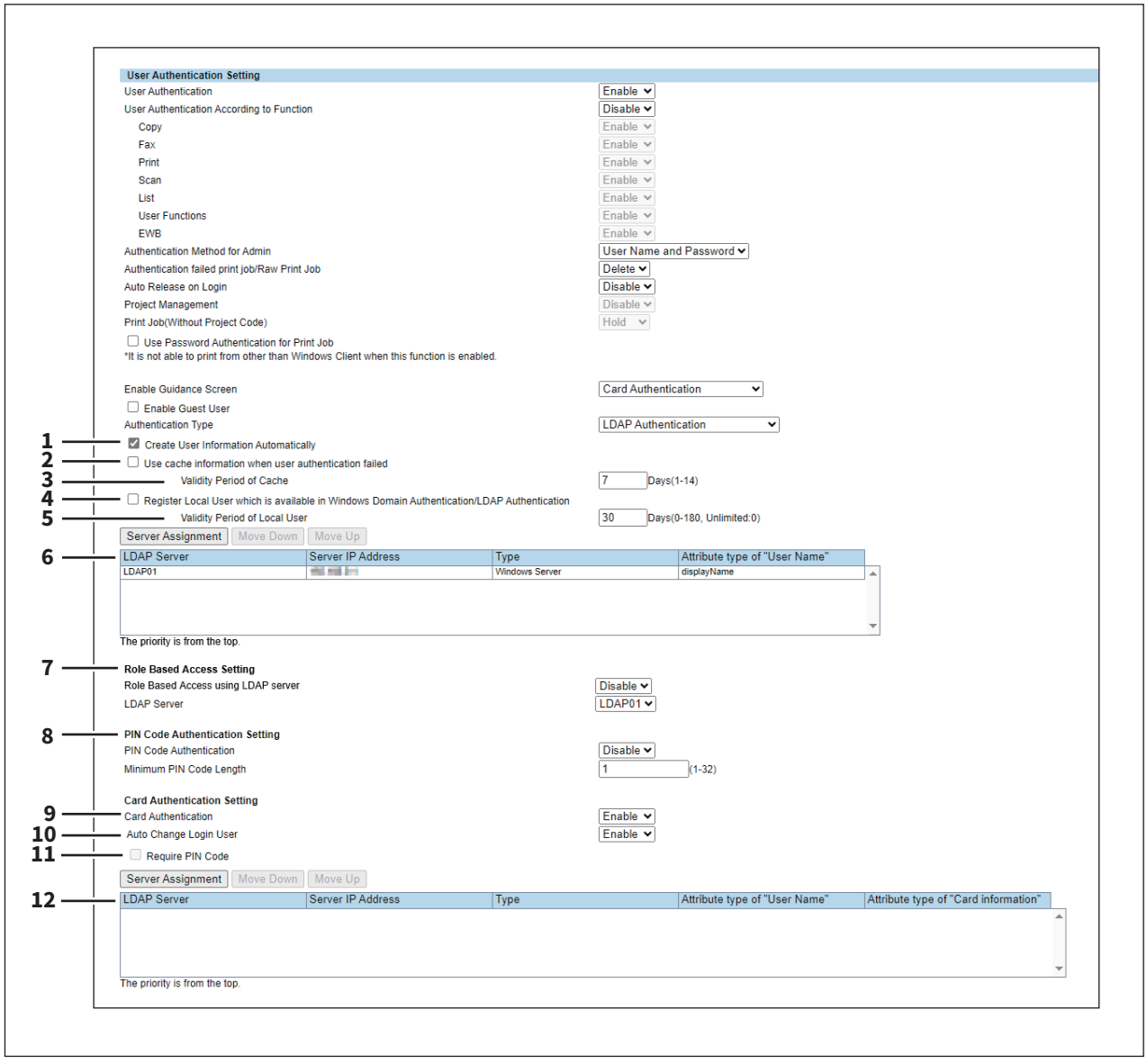


	Item name	Description
1	Create User Information Automatically	Select whether or not to register user information automatically to this equipment. This item is selected as the default. By registering user accounts to the printer, you can manage counters and quotas for each user.
	Tip When automatically adding a user while printing from the printer driver, enable [Use Password Authentication for Print Job] on the [User Authentication Setting] screen. P.61 “Setting up User Authentication Setting”	
2	Use cache information when user authentication failed	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.
	Tip 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.	

	Item name	Description
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	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. **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.
	Note • 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.
9	Role Based Access Setting	Configure role based access using an LDAP server. **Role Based Access using LDAP server** — Select whether enable or disable role based access. [Disable] is set as the default. **LDAP Server** — Select the LDAP server that manages the Role Based Access Control.
10	PIN Code Authentication Setting	**PIN Code Authentication** — Select the PIN code authentication method. • **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. **Minimum PIN Code Length** — Enter a figure that specifies the minimum digits for the PIN code.
11	Card Authentication	Select whether or not to enable card authentication.
	Note For the details of the card authentication setting, contact your service technician.	
12	Auto Change Login User	Select whether or not to enable the function to change login users automatically when authenticating users with the card.

	Item name	Description
13	Require PIN Code	Select whether or not to require PIN code when authenticating users with the card.
	Tip This function is available only on the equipment that supports the PIN code input.	
14	LDAP Server List	Displays a list of servers that are assigned for PIN 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.
	Tip If [Windows Server] is selected as an LDAP server for the PIN code or IC 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. • 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



	Item name	Description
1	Create User Information Automatically	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.
	Tip 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.61 "Setting up User Authentication Setting"	
2	Use cache information when user authentication failed	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.
	Tip 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.	
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	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]. Use [Move Up] and [Move Down] to change the priority order in the list.
7	Role Based Access Setting	Configure role based access using an LDAP server. **Role Based Access using LDAP server** — Select whether enable or disable role based access. [Disable] is set as the default. **LDAP Server** — Select the LDAP server that manages the Role Based Access Control.
8	PIN Code Authentication Setting	**PIN Code Authentication** — Select the PIN code authentication method. • **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. **Minimum PIN Code Length** — Enter a figure that specifies the minimum digits for the PIN code.
9	Card Authentication	Select whether or not to enable card authentication.
	Note For the details of the card authentication setting, contact your service technician.	
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	Select whether or not to require PIN code when authenticating users with the card.
	Tip This function is available only on the equipment that supports the PIN code input.	

	Item name	Description
12	LDAP Server List	Displays a list of servers that are assigned for PIN 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.

Tip

If [Windows Server] is selected as an LDAP server for the PIN code or IC 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.

- 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

❑ Certificate management settings

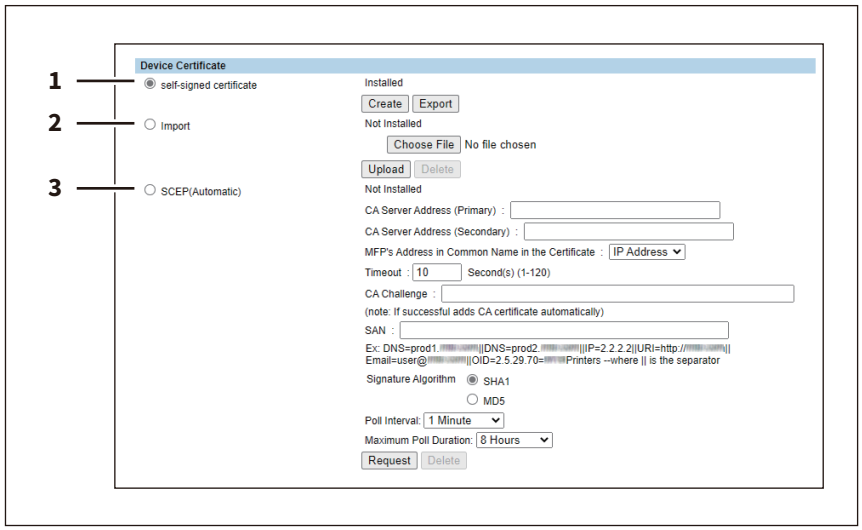
You can manage device certificates and client certificates.
🕮 P.72 “Setting up Device Certificate”

Tip

The [Certificate Management] submenu can be accessed from the [Security] menu on the [Administration] tab. See the **TopAccess Guide** for details on accessing.

Setting up Device Certificate

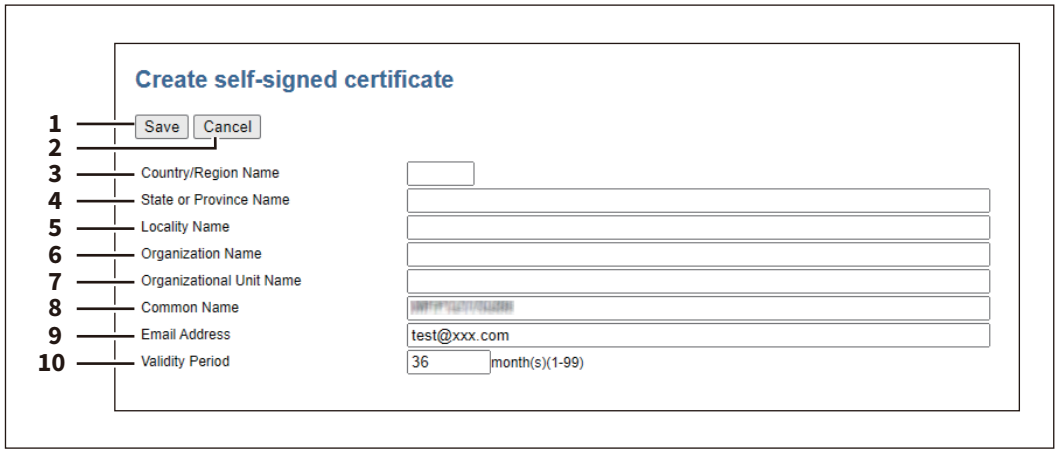
You can configure the device certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS.



	Item name	Description
1	self-signed certificate	Creates a certificate for encrypted communications using SSL/TLS on your device. **[Create] button** — Displays the [Create self-signed certificate] screen. Specify items necessary for the certificate to create the self-signed certificate. 🕮 P.73 “[Create self-signed certificate] screen” **[Export] button** — Exports the created self-signed certificate.
2	Import	Import the certificate for encrypted communications using wireless LAN, IEEE 802.1X authentication, IPsec, or SSL/TLS. **[Browse] button** — Allows you to select the certificate file. **[Upload] button** — Uploads the selected certificate file. **[Delete] button** — Deletes the registered certificate file.

	Item name	Description
3	SCEP(Automatic)	Automatically acquires the certificate for encrypted communications using IP sec or SSL/TLS. **CA Server Address (Primary)** — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols. **CA Server Address (Secondary)** — Enter the IP address of FQDN of the CA server. You can enter up to 128 alphanumerical characters and symbols. **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. **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. **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. **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. DNS: You can enter up to 253 letters with alphanumerical characters and symbols "." and "-". URI: You can use alphanumerical characters and symbols "- . _ ~ : / ? # ! @ $ ' ( ) * + ; =". e-mail address: You need to enter "@" and "." in the address. **Signature Algorithm** — Select SHA1 or MD5 as the signature algorithm. **Poll Interval** — Specify the polling interval. [1 Minute] is set as the default. **Maximum Poll Duration** — Specify the polling duration. [8 Hours] is set as the default. **[Request] button** — Click this button to request the certificate. **[Delete] button** — Deletes the registered certificate.

[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.

	Item name	Description
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.

■ [Maintenance] Item List

P.75 “Notification settings”
P.76 “Languages settings”
P.77 “Remote Command”
P.79 “System Updates settings”

Tip

Users who have been granted administrator authority in access policy mode can access the [Maintenance] menu from the [Administration] tab.
See the **TopAccess Guide** for details on accessing.

❑ Notification settings

P.75 “Setting up Job Notification Events”

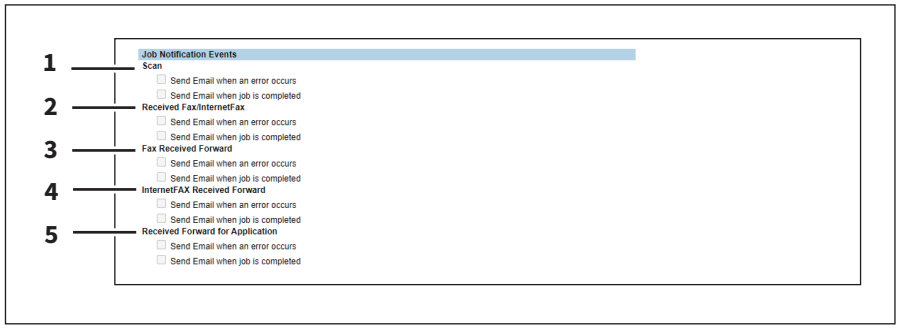
Tip

The [Notification] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Maintenance] menu:

P.75 “[Maintenance] Item List”

Setting up Job Notification Events

A setting of [Received Forward for Application] has been added.



You can select jobs to be notified.

	Item name	Description
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**

❑ Languages settings

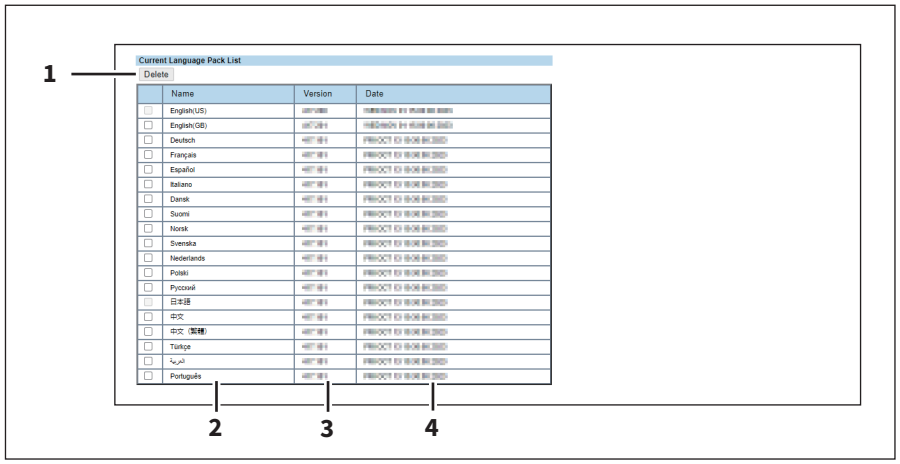
🕮 P.76 “Setting up Current Language Pack List”
🕮 P.76 “Custom Keyboard Setting”

Tip

The [Languages] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Maintenance] menu:
🕮 P.75 “[Maintenance] Item List”

Setting up Current Language Pack List

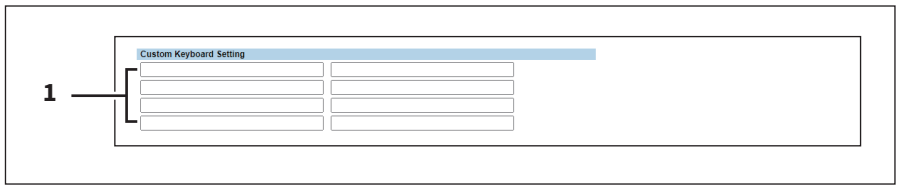
“Portuguese” and “Arabic” have been added to the language pack installed as the standard.



	Item name	Description
1	[Delete] button	Select unnecessary language packs and click the [Delete] button to delete them. Tip 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.

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.



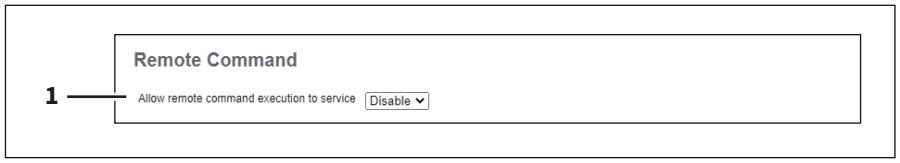
	Item name	Description
1	(Registration areas)	Register up to eight patterns of strings with up to 64 alphanumeric characters and symbols. The control panel shows them in the same order as the registration. Note The number of characters and the prohibited characters for entry vary from area to area on the control panel. • 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.
📖 P.78 “Apply Remote Command File”
📖 P.78 “Remote Command Execution History”

Tip

The [Remote Command] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Maintenance] menu:
📖 P.75 “[Maintenance] Item List”



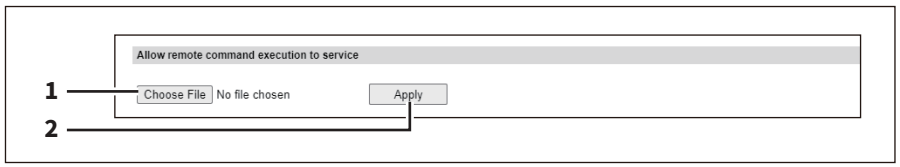
	Item name	Description
1	Allow remote command execution to service	Select whether to allow your service technician to do the remote maintenance. • **Enable** — Allows your service technician to execute the remote command from a remote place. • **Disable** — Prohibits your service technician from executing 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

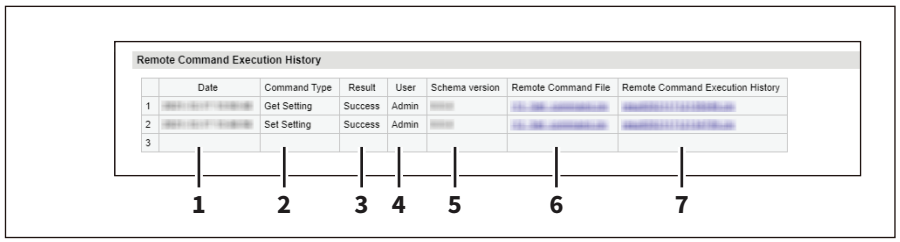
For the remote command file, contact your service representative.



	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. • 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.



	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. • **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. • **OK** — 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.

	Item name	Description
4	User	Shows the executor of the remote command. • **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.

❑ System Updates settings

📖 P.79 “Install Card Reader Firmware”

Tip

The [System Updates] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Maintenance] menu:
📖 P.75 “[Maintenance] Item List”

Install Card Reader Firmware

Contact your service technician for details.

Note

This function is not available for some models.

■ [Application] Item List

📖 P.80 “Application List”
📖 P.83 “Application Settings”
📖 P.86 “User Extended Information”

Tip

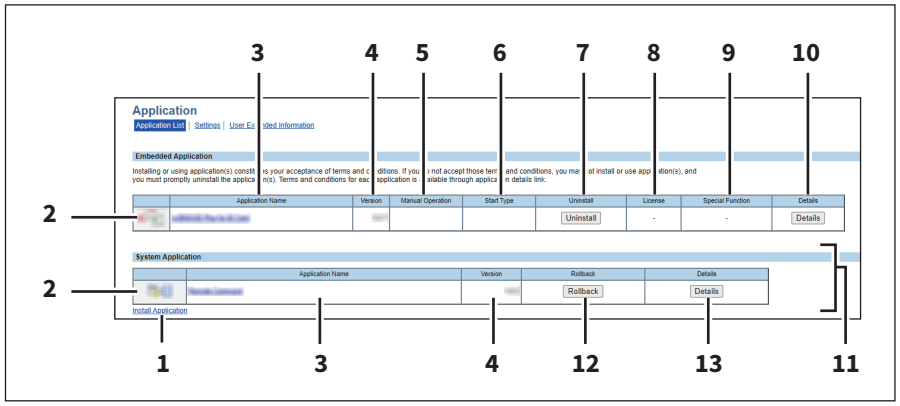
Users who have been granted administrator authority in access policy mode can access the [Application] menu from the [Administration] tab.
See the **TopAccess Guide** for details on accessing.

❑ 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.

Tip

The [Application List] submenu can be accessed from the [Application] menu on the [Administration] tab.
See the **TopAccess Guide** for how to access it and the following page for information on the [Application] menu:
📖 P.80 “[Application] Item List”



	Item name	Description
1	[Install Application] button	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. When you install the system application, follow instructions to select one that you want to install and agree to the end user license agreement. Note Only one application which uses the received document can be installed per MFP. Tip • 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.
2	Application Icon	Displays the application icon.
3	Application Name	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.
4	Version	Displays the application version.
5	Manual Operation	Allows you to start and stop the application manually. This is displayed only when the application package includes the background application. • **Start** — Select this to start the application. • **Stop** — Select this to close the application.
6	Start Type	Changes the applications startup method. This is displayed only when the application package includes the background application. • **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	Uninstalls the application. Click this button to display the uninstallation page for the application.
8	License	Displays the installation status of license files to utilize applications. • **-** — 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	Contact your service technician or representative for details on Special Function.

	Item name	Description
10	Details	Opens the screen that shows detailed information and settings of the application. • 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. • If the application can make use the received fax images, [Use Received Document] reads “Used”. If not possible, nothing appears for this function. Tip • To authenticate users at the startup of the embedded application, enable “User Authentication According To Function”. 🕮 P.61 “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	Displays the system applications installed in the equipment. Tip You need to set up [Cloud Authentication for Email] at [Administration] > [Setup] > [Network] > [SMTP Client] or [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.37 “Setting up SMTP Client” 🕮 P.40 “Setting up POP3 Client”
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

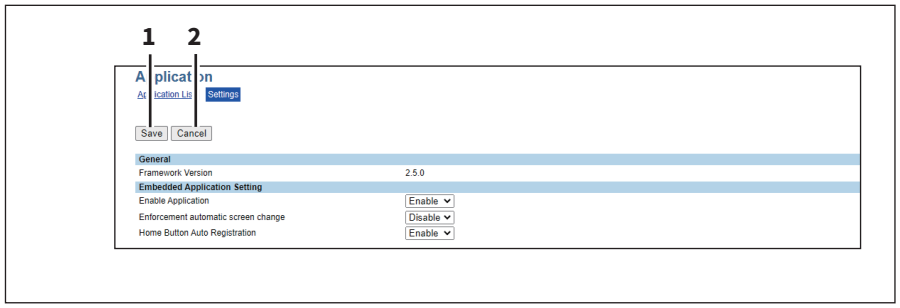
You can perform operations such as application settings, proxy settings, and debugging levels for all of the applications that are installed.

📖 P.83 “General”
📖 P.84 “Embedded Application Setting”
📖 P.84 “Proxy Setting”
📖 P.85 “Install Language Pack”
📖 P.85 “Import Application Data”
📖 P.85 “Application Data”
📖 P.86 “Available USB Device List”

Tip

The [Application Settings] submenu can be accessed from the [Application] menu on the [Administration] tab. See the **TopAccess Guide** for how to access it and the following page for information on the [Application] menu:

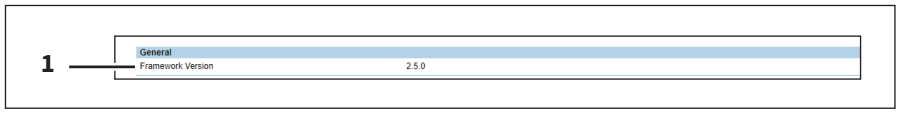
📖 P.80 “[Application] Item List”



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

General

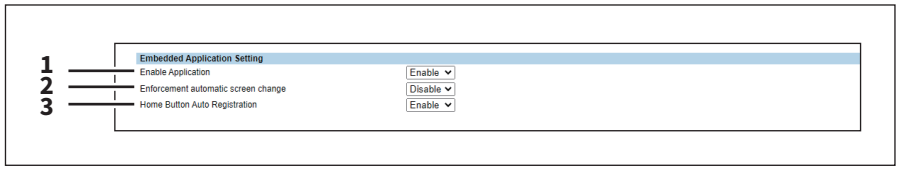
You can check the framework version.



	Item name	Description
1	Framework Version	Displays the framework version.

Embedded Application Setting

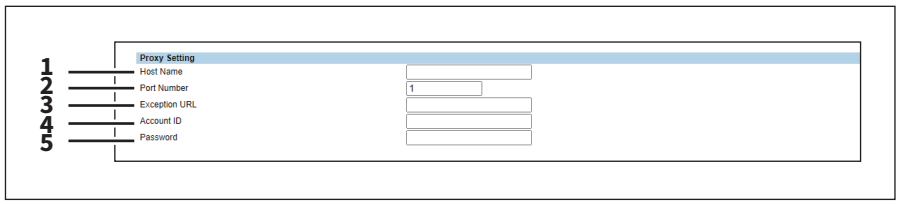
You can enable or disable embedded application functions.



	Item name	Description
1	Enable Application	Sets the application to enable/disable. • **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. Tip You can always install, roll back and make settings of the system applications without being affected by this setting.
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.



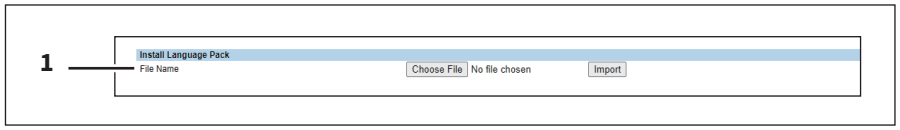
	Item name	Description
1	Host Name	Enter a host name for the proxy server.
2	Port Number	Enter a port number for the proxy server.
3	Bypass proxy settings for these addresses	Enter URLs that proxy server is not used by dividing them using semicolons (;).
4	Account ID	Enter the account ID of the proxy 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.

Install Language Pack

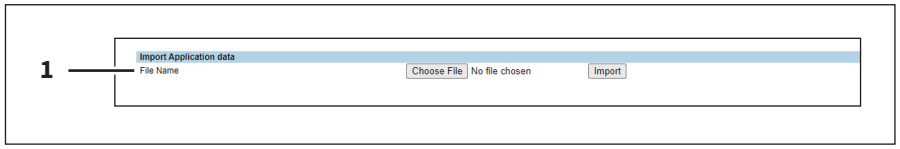
You can install the language packs for the applications.



	Item name	Description
1	File Name	Select the language pack file that you install. • **[Choose File] button** — Allows you to select the language pack file. • **[Import] button** — Imports the selected language pack file.

Import Application Data

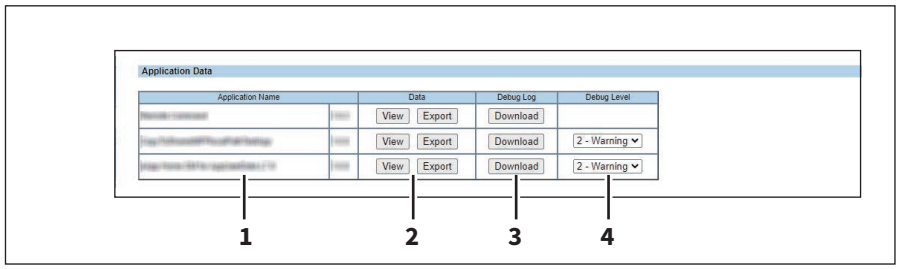
You can deliver the application data files.



	Item name	Description
1	File Name	Select the application data file that you deliver. • **[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.



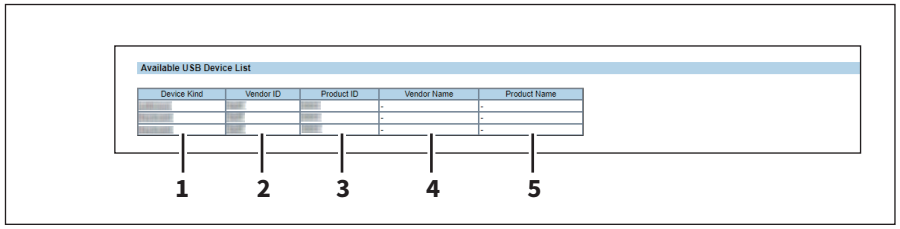
	Item name	Description
1	Application Name	Shows the application name.
2	Data	Collects the data files of the application so that you can check them. • **[View] button** — Shows information of the application data files. • **[Export] button** — Exports the application data files.
3	Debug Log	Collects the debug log files of the applications. • **[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.

Note

USB hubs do not work stably.



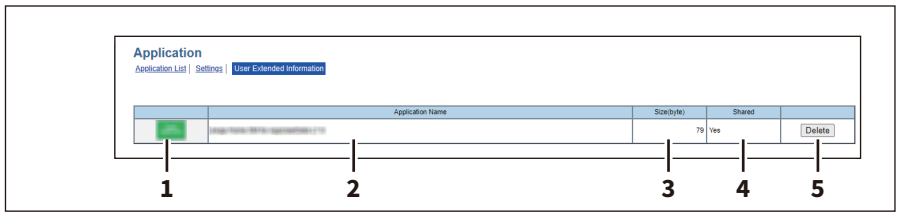
	Item name	Description
1	Device Kind	Displays the kind of the USB device.
2	Vendor ID	Displays the vendor ID of the USB device.
3	Product ID	Displays the product ID of the USB device.
4	Vendor Name	Displays the vendor name of the USB device.
5	Product Name	Displays the product name of the USB device.

❑ User Extended Information

You can check and delete the user extended information file of the application.

Tip

The [User Extended Information] submenu can be accessed from the [Application] menu on the [Administration] tab. See the **TopAccess Guide** for how to access it and the following page for information on the [Application] menu:
🕮 P.80 “[Application] Item List”



	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. • **[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.

5

AirPrint Function

■ When Security Certificate Expired and AirPrint Becomes Unusable

When expiration of the qualification information of the encryption is displayed on the macOS screen being operated and macOS AirPrint Print, macOS AirPrint Fax and macOS AirPrint Scan which use the security communication (*1 or *2) for AirPrint have become unusable, reperform the creation in [self-signed certificate] of [Device Certificate] on TopAccess. For details, see the following reference.
TopAccess Guide: “Chapter 8: [Administration] Tab” - “[Security] How to Set and How to Operate” - “Installing a device certificate”

*1: Enable IPP: Enable, Enable SSL/TLS: Enable
For details, see the following reference.
TopAccess Guide: “Chapter 8: [Administration] Tab” - “[Setup] How to Set and How to Operate” - “Print Service settings”

*2: Secure Scan (SSL/TLS): Enable
For details, see the following reference.
Operator’s Manual for AirPrint: “Chapter 1: USING THE AirPrint FUNCTION” - “Setting up AirPrint in TopAccess” - “Enabling or Disabling AirPrint”

Tip

- iOS AirPrint Print can be used.
- From the viewpoint of the security measures, it is recommended to set 13 months for [Validity Period] of [self-signed certificate].
- After new settings have been made for [self-signed certificate], click [Resume] on the print restart pop-up screen displayed at the first use of AirPrint. After the second time, this pop-up screen is not displayed.

Precautions for AirPrint

■ When using AirPrint Fax

You can use numbers 0 to 9 and symbols “*”, “#”, “-” and “p”. “-” and “p” function as pause and “#” functions as tone switching, too. In the transmission history of this equipment, “p” is indicated by “-”.

■ When printing is carried out by using thick paper and special paper (e-STUDIO330AC/400AC)

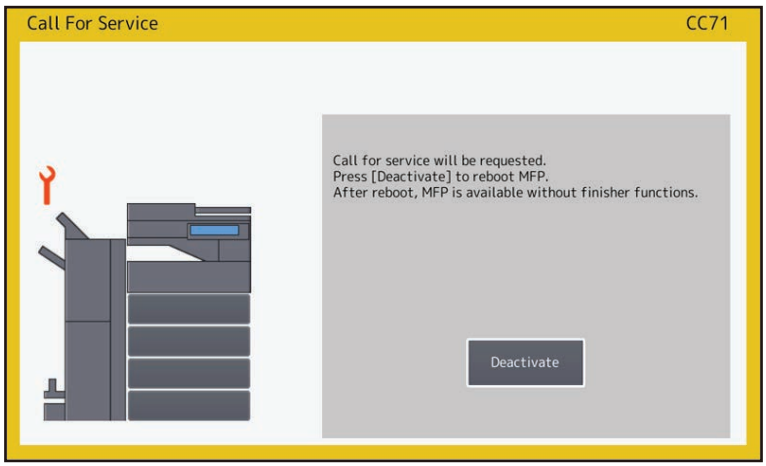
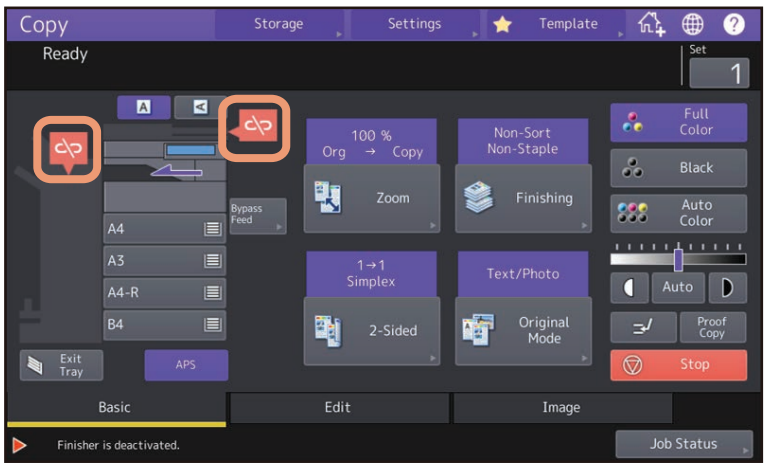
When printing is carried out by using thick and special paper in e-STUDIO330AC/400AC, load the paper in the drawer or bypass tray in advance. For details on how to load the paper, refer to the **Paper Preparation Guide**.

6

Troubleshooting

■ When This Screen Is Displayed

Various screens are displayed on the touch panel depending on the state of the equipment. This section describes how to solve problems with screen examples.

Screen	Description / Remedy
 	The equipment requires adjusting by a service technician. Contact your service representative with the error code displayed on the right side of the touch panel. Depending on the location where the problem has occurred, [Deactivate] will be displayed. When you press [Deactivate], you can use the equipment by excluding the separated functions. To release this separated status, adjustment by a service technician is required. ⚠ WARNING **Never attempt to repair, disassemble or modify the equipment by yourself.** You could cause a fire or get an electric shock. Always contact your service representative for maintenance or repair of the internal parts of the equipment.
	The options with the mark indicated in the figure are not usable. To release the detaching condition of the options, adjustment by a service technician is required.

■ Questions for Error Messages

A message appears on the upper part of the screen to notify users of a problem, etc. The major examples of problems and how to solve them are described in the table below.

Message	Problem Description	Corrective Action
*** toner cartridge was replaced before empty. Please reinsert cartridge. And use until empty." is displayed.	The toner cartridge was replaced before the toner in it has been used up completely. (For color models, "***" indicates the applicable color.) (The colors are shown abbreviated when two or more toners are running out: Y: yellow, M: magenta, C: cyan, K: black)	Reinstall the removed toner cartridge. If you do not have it, ask your service technician.

■ Error Codes

❑ Error codes on print jobs

Error code	Description	Corrective action
4012	Auto deletion of expired job	Expired job has been deleted automatically.
4731	Multi Station Print Job List corruption error	Jobs were removed since an abnormality has occurred in the Multi Station Print job list. Register the removed jobs again.

❑ Error codes on transmission and reception

Error code	Description	Corrective action
1C69	SMTP server connection error	Set the login name and password of the SMTP and confirm that the SMTP server is operating properly. In addition, confirm that From Address of [E-mail] is set correctly. Set the SMTP address again and reattempt the operation. If the error still persists, turn the power OFF and then back ON. Then reattempt the job in error.
1C71	SMTP authentication error	Confirm that the Authentication method, login name and password are correct. In addition, if SSL/TLS is enabled, make sure that the SSL/TLS setting and port number are correctly set. When [Application] is selected for [Authentication], register the account from the setting management screen of the connected application. If the account has already been created, delete it and then register it again.
3E30	POP3 login error	Check that the POP3 user name and password are set correctly. When [Application] is selected for [Authentication], register the account from the setting management screen of the connected application.

❑ Error codes on scan jobs

Email

Error code	Description	Corrective action
2C65, 2C66, 2C69	Failure to connect to SMTP server	Check whether the SMTP server is operating properly or the correct SMTP server is selected. In addition, confirm that From Address of [E-mail] is set correctly. Set the SMTP address again and reattempt the operation. If the error still persists, turn the power OFF and then back ON. Then reattempt the job in error.
2C71	SMTP authentication error	Confirm that the Authentication method, login name and password are correct. In addition, if SSL/TLS is enabled, make sure that the SSL/TLS setting and port number are correctly set. When [Application] is selected for [Authentication], register the account from the setting management screen of the connected application. If the account has already been created, delete it and then register it again.

INDEX

A

About Home Screen 10
Adding or removing display languages 15
Address book 10
Admin 15
Administration Tab 31
AirPrint FUNCTION 87
Allowing the acquisition of the investigation logs 18
Appendix 19
Application Data 85
Application Item List 80
Application List 80
Application Settings 83
Apply Remote Command File 78
Authentication settings 61
Available USB Device List 86

B

Behavior after recovering suspended cause 16
Box Setting
(Received Forward Setting for Application) 47

C

Certificate management settings 72
Common Setting 50
Create self-signed certificate screen 73
Create User Information 24
Custom Keyboard Setting 76

D

Default Address Book 13
Default View for Group 14
Default View for Single 13

E

ECM for G3 13
Edit User Information 27
Embedded Application Setting 84
Embedded Web Browser settings 59
Exposure 12

F

Fax 10, 12
Fax Settings 46
File Format 10
Function List (Administrator) 20

G

General 15, 83
General settings 31

H

Home Screen 9

I

Import Application Data 85
Information about Equipment 8
Inputting Characters 19
Install Card Reader Firmware 79
Install Language Pack 85

J

Job Skip Control 16
Job Skip Immediately 16

L

Languages settings 76
LDAP Authentication 70
List View Display Content 14

M

Maintenance Item List 75
MFP Collaboration 49
Multi Dest. Confirmation 13
Multi Station Print 56

N

Network Settings 32
Notification Events 60
Notification settings 75

O

Off Device Customization Architecture settings 59
On-screen keyboard 19
Options 8
Original Mode 12
Overview 7

P

Precautions for AirPrint 89
Preview Setting 13
Print Service Settings 58
Proxy Setting 84

Q

Questions for Error Messages 93

R

Received Forward Setting for Application 46
Remote Command 77
Remote Command Execution History 78
Resolution 12
Restart only when owner logs in 16
RTI for G3 13
Rx Speed Limit 13

S

Secure Receive Forced Setting 13
Security Item List 61
Setting the job control 16
Setting up AirPrint in TopAccess 88
Setting up Bonjour 43
Setting up Certificate Setting 59
Setting up Configuration 60
Setting up Current Language Pack List 76
Setting up Device Certificate 72
Setting up InternetFax Setting 47
Setting up Job Notification Events 75
Setting up Job Skip Control 31
Setting up Network 59
Setting up POP3 Client 40
Setting up SLP 44
Setting up SMB 33
Setting up SMTP Client 37
Setting up USB Cable Print 58
Setting up User Authentication Setting 61

Setup Item List 31
Shared Address Book 51
Shared Home 54
Shared User Management 52
Simple Scan 10
SSL/TLS Settings 32
System Updates settings 79

T

TopAccess 23
Troubleshooting 91
Troubleshooting for the Hardware 92
TTI for G3 13
Tx Speed Limit 13
Tx Type 12

U

USB Cable Print 18
USB Cable Print Mode 18
USB Printing 18
USB storage devices 8
User 12
User Extended Information 86
User Function 11
User Management Tab 24

V

VNC Setting 44

W

When This Screen Is Displayed 92
Windows Domain Authentication 68

FC-2010AC/2510AC
FC-2515AC/3015AC/3515AC/4515AC/5015AC
DP-2018A/2518A/3018A/3518A/4518A/5018A
FC-5516AC/6516AC/7516AC
DP-5518A/6518A/7518A/8518A
FC-330AC/400AC
OME210071B0

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for the Latest Functions

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

Toshiba Tec Corporation

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN

QUALITY SERVICE

© 2021 - 2024 Toshiba Tec Corporation All rights reserved
Patent; http://www.toshibatec.com/en/patent/

R210420Y0202-TTEC
Ver02 F Issued in Feb. 2024