

MULTIFUNCTIONAL DIGITAL SYSTEMS

TopAccess Guide

Preface

Thank you for purchasing TOSHIBA Multifunctional Digital Systems or Multifunctional Digital Color Systems. This manual explains the instructions for administrators to set up and manage the Multifunctional Digital Systems or Multifunctional Digital Color Systems using TopAccess. Read this manual before using your Multifunctional Digital Systems or Multifunctional Digital Color Systems. Keep this manual within easy reach, and use it to configure an environment that makes best use of the e-STUDIO's functions.

The e-STUDIO455 Series and the e-STUDIO855 Series provide the scanning function as an option. However, this optional scanning function is already installed in some models.

■ How to read this manual

□ Symbols in this manual

In this manual, some important items are described with the symbols shown below. Be sure to read these items before using this equipment.

 **WARNING** Indicates a potentially hazardous situation which, if not avoided, could result in death, serious injury, or serious damage, or fire in the equipment or surrounding objects.

 **CAUTION** Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, partial damage to the equipment or surrounding objects, or loss of data.

 **Note** Indicates information to which you should pay attention when operating the equipment.

Other than the above, this manual also describes information that may be useful for the operation of this equipment with the following signage:

 **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.

□ 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-STUDIO5520C/6520C/6530C	e-STUDIO6530C Series
e-STUDIO2020C/2330C/2820C/2830C/3520C/3530C/4520C	e-STUDIO4520C Series
e-STUDIO555/655/755/855	e-STUDIO855 Series
e-STUDIO205L/255/305/355/455	e-STUDIO455 Series

□ Screens

- Illustrations for a control panel and a touch panel shown in this manual are those of the e-STUDIO4520C Series. The control panel and the touch panel, including buttons and their names and functions, are common to all of the e-STUDIO4520C Series, e-STUDIO6530C Series, e-STUDIO455 Series and e-STUDIO855 Series. The details on the touch panel menus may differ depending on how the equipment is used, such as the status of the installed options.
- The illustration screens used in this manual are for paper in the A/B format. If you use paper in the LT format, the display or the order of buttons in the illustrations may differ from that of your equipment.

□ Trademarks

- The official name of Windows 2000 is Microsoft Windows 2000 Operating System.
- The official name of Windows XP is Microsoft Windows XP Operating System.
- The official name of Windows Vista is Microsoft Windows Vista Operating System.
- The official name of Windows 7 is Microsoft Windows 7 Operating System.
- The official name of Windows Server 2003 is Microsoft Windows Server 2003 Operating System.
- The official name of Windows Server 2008 is Microsoft Windows Server 2008 Operating System.
- Microsoft, Windows, Windows NT, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- Apple, AppleTalk, Macintosh, Mac, Mac OS, Safari, and TrueType are trademarks of Apple Inc. in the US and other countries.
- Adobe, Adobe Acrobat, Adobe Reader, Adobe Acrobat Reader, and PostScript are trademarks of Adobe Systems Incorporated.
- Mozilla, Firefox and the Firefox logo are trademarks or registered trademarks of Mozilla Foundation in the U.S. and other countries.
- IBM, AT and AIX are trademarks of International Business Machines Corporation.
- NOVELL, NetWare, and NDS are trademarks of Novell, Inc.
- TopAccess is a trademark of Toshiba Tec Corporation.
- Other company names and product names in this manual are the trademarks of their respective companies.

CONTENTS

Preface.....	1

Chapter 1 OVERVIEW

TopAccess Overview	8
Accessing TopAccess End-User Mode	9
Accessing web utility TopAccess.....	9
TopAccess web site.....	15

Chapter 2 CHECKING DEVICE STATUS

TopAccess [Device] Tab Page	18
Equipment status icons	20

Chapter 3 MANAGING JOBS

Managing Print Jobs	24
Displaying print jobs	24
Deleting print jobs.....	25
Releasing print jobs.....	26
Managing Fax/Internet Fax Jobs.....	27
Displaying Fax/Internet Fax jobs	27
Deleting Fax transmission jobs.....	28
Managing Scan Jobs	29
Displaying scan jobs.....	29
Deleting scan jobs	30

Chapter 4 DISPLAYING JOB LOGS

Displaying Print Job Logs	32
Displaying Transmission Journals	33
Displaying Reception Journals	34
Displaying Scan Job Logs.....	35

Chapter 5 REGISTERING FROM TopAccess

Managing Templates	38
Registering private template groups.....	38
Registering private templates.....	45
Displaying public templates	77
Managing Address Book	78
Managing contacts in the Address Book	78
Managing groups in the Address Book.....	83
Managing Mailboxes	86
Setting up an Open Mailbox	87
Deleting an Open Mailbox	93

Chapter 6 MANAGING COUNTERS

Viewing Counters	96
Displaying the total counter	96
Displaying the department counter	98

Chapter 7 TopAccess ADMINISTRATOR MODE

Features and Functions	103
About setup from TopAccess	103
About maintenance from TopAccess	104
About registration from TopAccess	104
About other administrative functions in TopAccess	105
Accessing TopAccess Administrator Mode	106
Setting up From TopAccess	108
Setting up device settings	108
Setting up Network settings	118
Setting up Copier settings	168
Setting up Fax settings	171
Setting up Save as file settings	176
Setting up Email settings	183
Setting up InternetFax settings	186
Setting up Printer settings	188
Setting up Print Service settings	193
Setting up ICC Profile settings	199
Displaying version information	206
Maintenance From TopAccess	207
About the maintenance functions	207
Uploading the software	208
Removing the client software	209
Backing up data	210
Restoring data from backup file	213
Deleting the data from local folder	215
Managing directory service	216
Setting up notification	218
Importing and exporting the Address Book	223
Importing and exporting the department code	228
Exporting the logs, journals, and counters	231
Clearing the logs and journals	233
Rebooting the equipment	235
Registering From TopAccess	236
Registering public templates	236
Registering Fax and Internet Fax received forward	245
Displaying Message Log	259
Managing Department Code	260
Displaying the department list and counters	260
Clearing the department counters	262
Registering or modifying the department code	264
Deleting the department code	266
Setting up User Management	268
Enabling department management	268
Setting up User Management setting	271

Setting role information.....	301
Setting up User Authentication for Scan to Email.....	307

Chapter 8 OPTION SETUPS

About Option Setups.....	316
Setting up IP Security Function	317
Setting up IPsec	318
Registering policies	319
Installing IPsec certificate	326
Flushing out IPsec sessions.....	332
Setting up Meta Scan Function	333
Registering/Editing Meta Scan templates.....	333
Maintaining Meta Scan templates	349
Maintaining XML format files	355

Chapter 9 APPENDIX

Installing Certificates for a Client PC	362
INDEX	369

OVERVIEW

This chapter describes overview of the TopAccess functions.

TopAccess Overview	8
Accessing TopAccess End-User Mode	9
Accessing web utility TopAccess	9
TopAccess web site	15

TopAccess Overview

TopAccess is a web-based job and device management tool that allows you to access information about this equipment over the Internet.

TopAccess has two web sites available. One site is designed for end users and the other is for the administrators.

- The end-user site displays the equipment and job status and enables you to create and maintain private template groups and private templates.
- The administrator site enables network administrators to configure device settings, conduct maintenance, and update the address book, public template group and public templates.

Note

For instructions on how to use TopAccess in the administrator mode, see the following section.

 P.101 "TopAccess ADMINISTRATOR MODE"

End users can:

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

Notes

- Because TopAccess uses cookies to store information on the user's system, users must have cookies enabled in the browser.
- If TopAccess does not display the correct information in any pages, delete cookies and try again.

Accessing TopAccess End-User Mode

To operate TopAccess, this equipment should be connected to the network and be configured with the TCP/IP settings. After you complete the TCP/IP setup, you can access the TopAccess web site to operate various functions from your computer using a web browser such as Firefox or Internet Explorer.

You can use the TopAccess web-based utility from a Windows, Macintosh or UNIX operating system environment. The following browsers are supported:

Windows

- Internet Explorer 5.5 Service Pack 2 or later
(Internet Explorer 7.0 or later when IPv6 is used)
- Firefox 1.5.0.4 or later

Macintosh

- Safari 2.0 or later
- Firefox 1.5.0.4 or later

UNIX

- Firefox 1.5.0.4 or later

■ Accessing web utility TopAccess

You can access the web utility TopAccess by entering its URL on the address box of web browser. To access it under a Windows Vista/Windows 7/Windows Server 2008 environment, confirm the network connection status on the Network Map with the LLTD (= Link Layer Topology Discovery) feature of Windows Vista/Windows 7/Windows Server 2008, and then click the displayed icon of this equipment.

- P.9 “Accessing TopAccess by entering URL”
- P.10 “Accessing TopAccess from Network Map (Windows Vista/Windows 7/Windows Server 2008)”

Accessing TopAccess by entering URL

1 To navigate to TopAccess, enter the following URL on the address box of your Internet browser.

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



For example

When the IP address of the equipment is “10.10.70.105” (when IPv4 used):

`http://10.10.70.105`

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

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

or

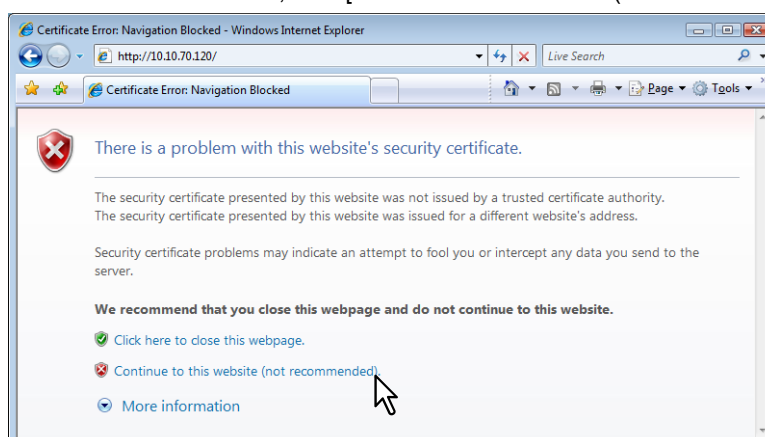
`http://[3ffe:1:1:10:280:91ff:fe4c:4f54]`

When the device name of this equipment is “mfp-00c67861”:

`http://mfp-00c67861`

Note

When SSL for the HTTP network service is enabled, an alert message may appear when you enter the URL in the address box. In that case, click [Continue to this website (not recommended).] to proceed.



2 The TopAccess web page for end users opens.

Tip

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

Accessing TopAccess from Network Map (Windows Vista/Windows 7/Windows Server 2008)

Confirm the network connection status on the Network Map with the LLTD feature of Windows Vista/Windows 7/Windows Server 2008, and then click the displayed icon of this equipment.

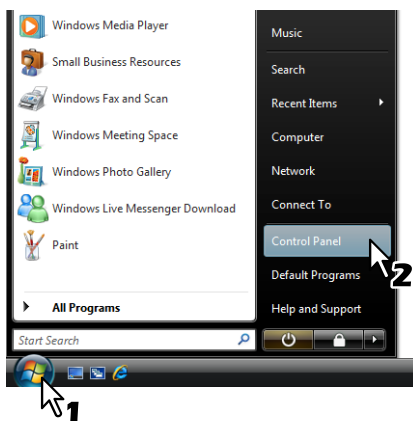
Tip

You can install the driver required for web services by right-clicking the icon and selecting [Install]. For the driver required for web services, refer to the ***Software Installation Guide***.

Notes

- Before using the LLTD feature, enable the LLTD setting. P.166 "Setting up LLTD Setting"
- Before beginning the installation of the driver required for web services, enable the Web Services setting. P.166 "Setting up Web Services Setting"

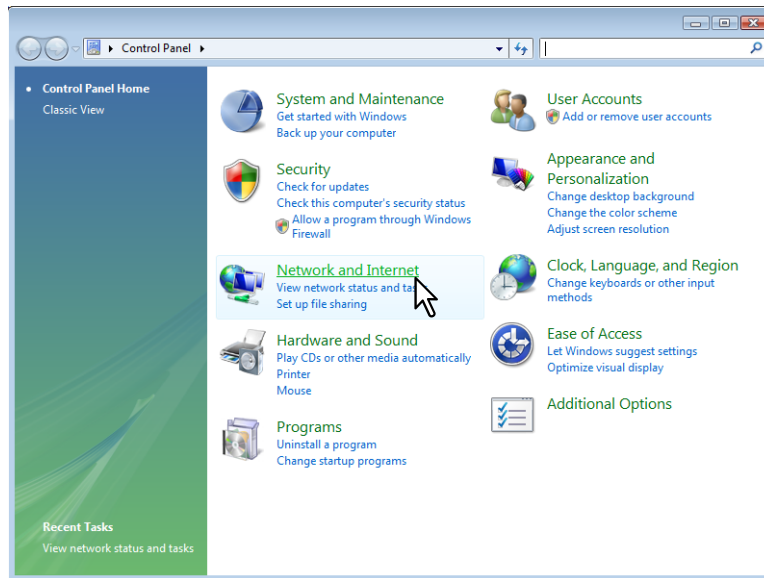
1 Click the [Start] icon and select [Control Panel].



The Control Panel window appears.

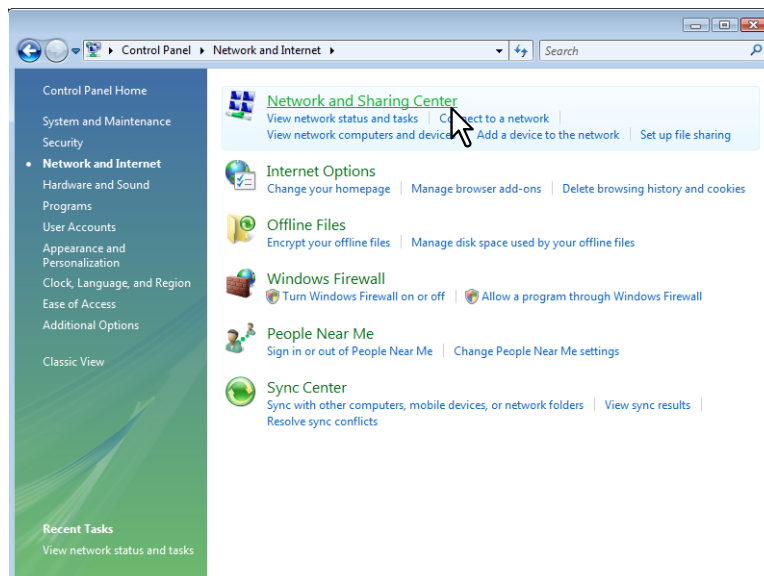
2 Click [Network and Internet].

1



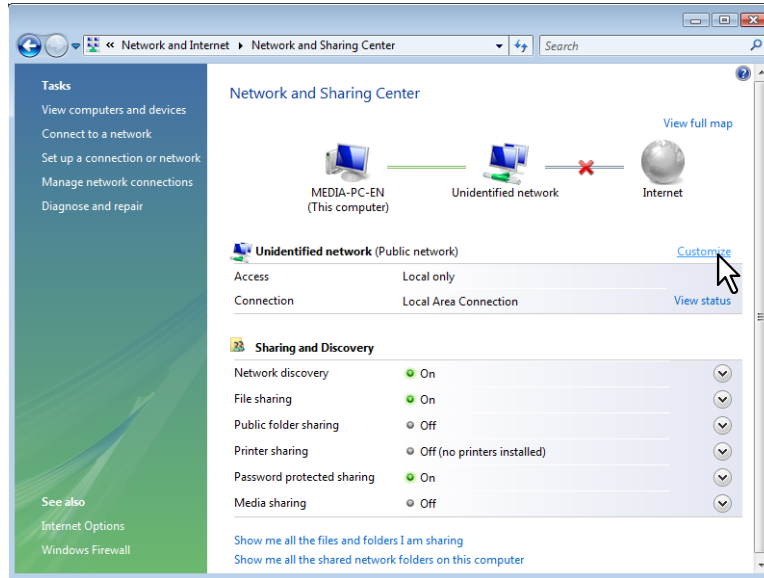
The Network and Internet window appears.

3 Click [Network and Sharing Center].



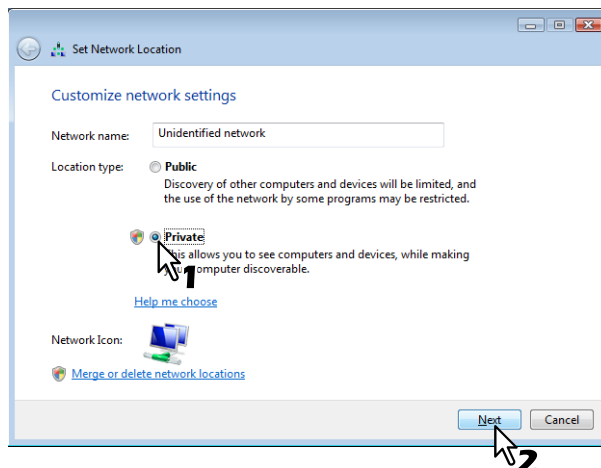
The Network and Sharing Center window appears.

4 Click [Customize] of [Unidentified network (Public network)].



The Set Network Location window appears.

5 Select [Private] of [Location type], and then click [Next].

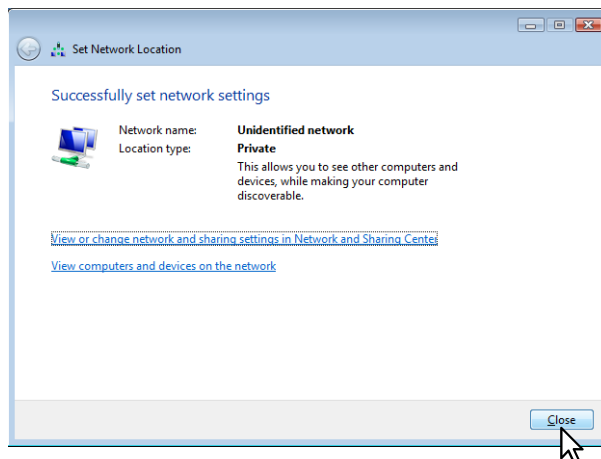


- The User Account Control dialog box appears.
- If the user account control is disabled, the Set Network Location – Successfully set network settings window appears. Go to step 7.

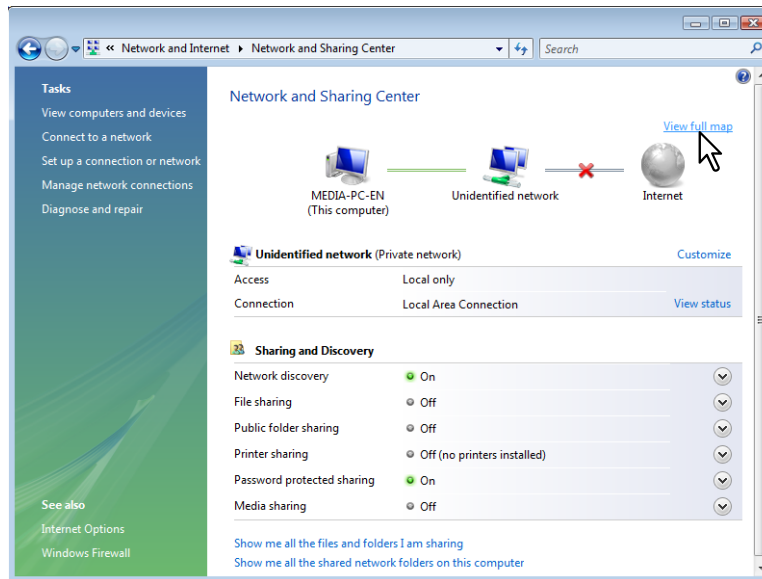
6 Click [Continue] in the User Account Control dialog box.

The Set Network Location – Successfully set network settings window appears.

7 Click [Close].

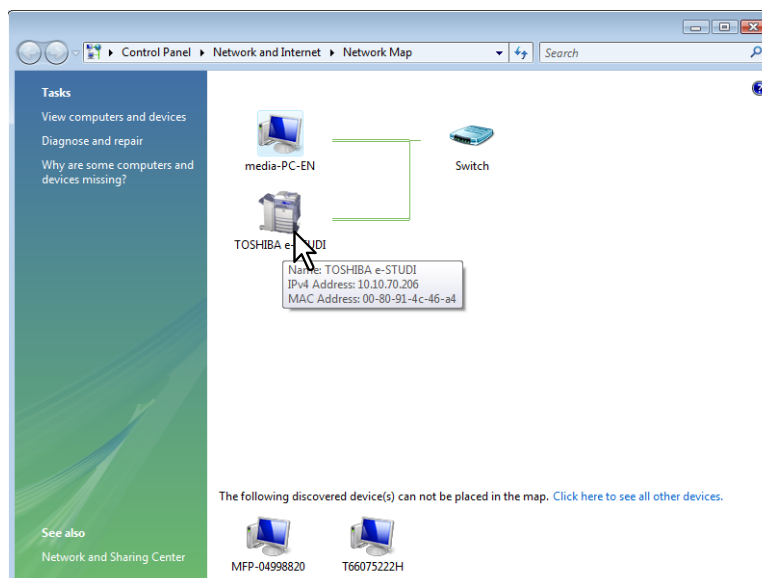


8 Click [View full map] in the Network and Sharing Center window.



Mapping of devices connected on the network appears in the Network Map window.

9 Click the icon of this equipment.



Notes

- The name, IP address and MAC address of the devices appear as a result of your placing a pointer over each icon.
- If the equipment is with the Finisher, its icon is displayed together with the Finisher icon. If not, it is displayed by itself.

10 The TopAccess web site appears.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Device REFRESH



Options	
Finisher	None
Hole Punch Unit	None
Fax	Not Installed

Toner	
Yellow(Y)	100 %
Magenta(M)	100 %
Cyan(C)	100 %
Black(K)	100 %

Device Information	
Status	Ready
Name	MFP-05212774
Location	
Copier Model	TOSHIBA e-STUDIO4520C
Main Memory Size	1024 MB
Page Memory Size	512 MB
Save as File Space Available	9994 MB
Store to e-Filing Space Available	13988 MB
Fax Transmission Space Available	3499 MB
Fax Reception Space Available	500 MB
Work Space Available	99 %
Contact Information	
Phone Number	
Message	
Alerts	•

Paper				
Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	550	Paper Available
Drawer 2	A3	Plain	550	Near Empty

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

■ TopAccess web site

1

When you access TopAccess, the general information page of the TopAccess web site is displayed.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Device REFRESH

Device Information

Status	Ready
Name	MFP-05212774
Location	
Copier Model	TOSHIBA e-STUDIO4520C
Main Memory Size	1024 MB
Page Memory Size	512 MB
Save as File Space Available	9994 MB
Store to e-Filing Space Available	13988 MB
Fax Transmission Space Available	3499 MB
Fax Reception Space Available	500 MB
Work Space Available	99 %
Contact Information	
Phone Number	
Message	
Alerts	•

Options

Finisher	None
Hole Punch Unit	None
Fax	Not Installed

Toner

Yellow(Y)	100 %
Magenta(M)	100 %
Cyan(C)	100 %
Black(K)	100 %

Paper

Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	550	Paper Available
Drawer 2	A3	Plain	550	Near Empty

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

From here, you can initiate most device monitoring and management functions.

The basic TopAccess page contains the following items:

TopAccess e-Filing

Device Job Status Logs **Registration** Counter User Management Administration

Template Address Book

Template Groups

Please select a group to edit below.

Public Template Groups

No.	Name	User Name
Public	Public Template Groups	

All Groups | Defined Groups

Jump to

001 011 021 031 041 051 061 071 081 091 101 111 121 131 141 151 161 171 181 191

No.	Name	User Name
001		
002	TEST	
003	Undefined	Undefined
004	Undefined	Undefined
005	Undefined	Undefined
006	Undefined	Undefined
007	Undefined	Undefined
008	Undefined	Undefined
009	Undefined	Undefined
010	Undefined	Undefined

Go to top of this page

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

1 2 3 4 5 6

1) Function tab

This provides access to main pages of TopAccess for each function.

2) Menu bar

This provides access to each menu page under the selected function tab.

3) Submenu bar

This provides access to each submenu page under the selected menu and function tab.

4) Install Software link

Click this to open the Install Client Software page to download the client software from TopAccess.

5) Top link

Click this to display the top of the page that is currently displayed.

6) Help link

Click this to display the Online Help.

Note

The TopAccess Online Help supports the following browsers:

- Internet Explorer

CHECKING DEVICE STATUS

This chapter describes the [Device] tab page in the TopAccess end-user mode.

TopAccess [Device] Tab Page	18
Equipment status icons	20

TopAccess [Device] Tab Page

TopAccess opens with the end-user [Device] tab, which includes a picture of the device. At any time, the end-user may click REFRESH to update the TopAccess status information.

This tab shows the following information about the device:

For the e-STUDIO4520C Series

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration Meta Scan

Device REFRESH

1 

2 **Options**

Finisher	None
Hole Punch Unit	None
Fax	Installed

3 **Toner**

Yellow(Y)	100 %
Magenta(M)	100 %
Cyan(C)	100 %
Black(K)	100 %

4 **Paper**

Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	550	Paper Available
Drawer 2	A3	Plain	550	Paper Available
Drawer 3	A4R	Plain	550	Paper Available
Drawer 4	B4	Plain	550	Paper Available

Device Information

Status	Ready
Name	MFP-05212915
Location	
Copier Model	TOSHIBA e-STUDIO4520C
Serial Number	CAK000000
Main Memory Size	1024 MB
Page Memory Size	512 MB
Save as File Space Available	9991 MB
Store to e-Filing Space Available	13349 MB
Fax Transmission Space Available	3499 MB
Fax Reception Space Available	500 MB
Work Space Available	96 %
Contact Information	
Phone Number	
Message	
Alerts	•

| Install Software | | Top | Help | © 2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

For the e-STUDIO6530C Series

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration Meta Scan

Device REFRESH

1 

2 **Options**

Finisher	None
Hole Punch Unit	None
Fax	Installed

3 **Toner**

Yellow(Y)	100 %
Magenta(M)	75 %
Cyan(C)	75 %
Black(K)	100 %

4 **Paper**

Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	540	Near Empty
Drawer 2	A4	Plain	540	Paper Available
Drawer 3	A3	Plain	540	Near Empty
Drawer 4	A4	Plain	540	Near Empty

Device Information

Status	Ready
Name	MFP-05212657
Location	
Copier Model	TOSHIBA e-STUDIO6530C
Serial Number	CU
Main Memory Size	1024 MB
Page Memory Size	1024 MB
Save as File Space Available	9995 MB
Store to e-Filing Space Available	13982 MB
Fax Transmission Space Available	3499 MB
Fax Reception Space Available	500 MB
Work Space Available	99 %
Contact Information	
Phone Number	
Message	
Alerts	•

| Install Software | | Top | Help | © 2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

For the e-STUDIO855 Series

2

TopAccess [e-Filing](#) [Logout](#)

Device Job Status Logs Registration Counter User Management Administration Meta Scan

Device [REFRESH](#)

1 

2 **Options**

Finisher	None
Hole Punch Unit	None
Fax	Not Installed
Optional Function kit	Printer/Scanner kit
Insertor	Not Installed

3 **Device Information**

Status	Ready
Name	MFP-06887401
Location	
Copier Model	TOSHIBA e-STUDIO855
Serial Number	CE
Save as File Space Available	7000 MB
Store to e-Filing Space Available	6997 MB
Fax Transmission Space Available	501 MB
Fax Reception Space Available	501 MB
Work Space Available	99 %
Contact Information	
Phone Number	
Message	
Alerts	•

Paper

Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	550	Paper Available
Drawer 2	A3	Plain	550	Paper Available
Tandem Large Capacity Feeder	A4	Plain	3000	Paper Available
External Large Capacity Feeder	A4	Plain	4500	Paper Available

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2009 TOSHIBA TEC CORPORATION All Rights Reserved

For the e-STUDIO455 Series

TopAccess [e-Filing](#) [Logout](#)

Device Job Status Logs Registration Counter User Management Administration

Device [REFRESH](#)

1 

2 **Options**

Finisher	None
Hole Punch Unit	None
Fax	Installed
Optional Function kit	Printer/Scanner kit

3 **Device Information**

Status	Ready
Name	MFP-06887424
Location	
Copier Model	TOSHIBA e-STUDIO455
Serial Number	CC
Save as File Space Available	9501 MB
Store to e-Filing Space Available	9497 MB
Fax Transmission Space Available	501 MB
Fax Reception Space Available	501 MB
Work Space Available	99 %
Contact Information	
Phone Number	
Message	
Alerts	•

Paper

Drawer	Size	Type	Capacity	Status
Drawer 1	A4	Plain	600	Paper Available
Drawer 2	A3	Plain	600	Paper Available
Drawer 3	A4R	Plain	600	Paper Available
Drawer 4	B4	Plain	600	Paper Available

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2009 TOSHIBA TEC CORPORATION All Rights Reserved

1) Device Information

The Device Information list shows the following information.

- **Status** — Displays the device status.
- **Name** — Displays the name of this equipment.
- **Location** — Displays the equipment's location.
- **Copier Model** — Displays the model name of this equipment.
- **Serial Number** — Displays the serial number of this equipment.
- **Main Memory Size** — Displays the main memory size.
- **Page Memory Size** — Displays the page memory size.
- **Save as File Space Available** — Displays the available size to store the Save as file documents.
- **Store to e-Filing Space Available** — Displays the available size to store the e-Filing documents.
- **Fax Transmission Space Available** — Displays the available size to send the fax data.
- **Fax Reception Space Available** — Displays the available size to receive the fax data.
- **Work Space Available** — Displays the percentages of available hard disk space to store the temporary data.
- **Contact Information** — Displays the contact name of the person responsible for managing this device.
- **Phone Number** — Displays the phone number of the person responsible for managing this device.
- **Message** — Displays the administrative message.
- **Alerts** — Displays the alert message. Errors are in red and warnings are in yellow.

Tip

[Main Memory Size] and [Page Memory Size] are displayed only on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series.

2) Options

The Options list shows the status of optional units.

- **Finisher** — Displays the type of finisher installed.
- **Hole Punch Unit** — Displays whether the hole punch unit is installed.
- **Fax** — Displays whether the Fax Unit is installed.
- **Optional Function kit** — Displays in which optional kits are installed.
- **Insertor** — Displays whether the Insertor (optional) is installed.

Tips

- [Optional Function kit] is displayed only on the TopAccess menu of the e-STUDIO455 Series and the e-STUDIO855 Series.
- [Insertor] is displayed only on the TopAccess menu of the e-STUDIO855 Series.

3) Paper

The Paper list shows the drawer status.

- **Drawer** — Lists the installed drawers.
- **Size** — Displays the paper size set in each drawer.
- **Type** — Displays the paper type set in each drawer.
- **Capacity** — Displays the maximum paper capacity that can be set in each drawer.
- **Status** — Displays the remaining amount of paper in each drawer.

Note

The paper size for each drawer cannot be set from TopAccess. Set it from the touch panel of the equipment. For instructions on how to set the paper size for each drawer, refer to the **Copying Guide**.

4) Toner

The Toner list shows the toner quantity.

Equipment status icons

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

- Printer Error 1



This icon indicates a non-recommended toner cartridge is used and the equipment stopped printing. For information on resolving the error condition, refer to “Replacing a Toner Cartridge” in the **Troubleshooting Guide**.

- Printer Error 2



This icon indicates:

- You need to remove paper from the receiving tray.
- You need to remove paper from the Finisher tray.
- You need to remove the staples jammed in the Finisher. For information on resolving the error condition, refer to “Staple Jam in the Finisher” in the **Troubleshooting Guide**.
- You need to remove the staples jammed in the Saddle Stitch unit. For information on resolving the error condition, refer to “Staple Jam in the Saddle Stitch unit” in the **Troubleshooting Guide**.
- You need to clear the hole punch paper bits from the Hole Punch Unit. For information on resolving the error condition, refer to “Cleaning the Hole Punch Dust Bin” in the **Troubleshooting Guide**.
- An unrecommended toner cartridge is being used. For information on resolving the error condition, refer to “Replacing a Toner Cartridge” in the **Troubleshooting Guide**.
- You performed saddle stitch printing with the paper of the different sizes.
- The equipment cannot load paper from the Large Capacity Feeder.
- The equipment cannot eject the paper to the inner tray. (e-STUDIO4520C Series only)

- Cover Open



This icon indicates the front cover is open.

- Toner Empty



This icon indicates no toner is left. It also indicates which color is empty. For information on resolving the error condition, refer to “Replacing a Toner Cartridge” in the ***Troubleshooting Guide***.

- Waste Toner Full



This icon indicates the waste toner box is full and requires replacing. For information on resolving the error condition, refer to “Replacing the Waste Toner Box” in the ***Troubleshooting Guide***.

- Paper Empty



This icon indicates no paper is left in a drawer. For information on resolving the error condition, refer to the ***Copying Guide***.

- Paper Jam



This icon indicates a paper jam occurred. It also indicates the location of the paper jam. For information on resolving the error condition, refer to “Clearing a Paper Jam” in the ***Troubleshooting Guide***.

- Staples Empty



This icon indicates no staples are left in the Finisher. For information on resolving the error condition, refer to “Refilling the Staple” in the ***Troubleshooting Guide***.

- Call for Service



Contact your service representative to have the equipment inspected.

MANAGING JOBS

Using TopAccess, end users can display and delete print jobs, fax transmission jobs, and scan jobs released by end users.

Managing Print Jobs	24
Displaying print jobs	24
Deleting print jobs.....	25
Releasing print jobs.....	26
Managing Fax/Internet Fax Jobs.....	27
Displaying Fax/Internet Fax jobs	27
Deleting Fax transmission jobs	28
Managing Scan Jobs.....	29
Displaying scan jobs.....	29
Deleting scan jobs	30

Managing Print Jobs

Using TopAccess, you can display, delete and release print jobs that are currently in the queue.

📖 P.24 “Displaying print jobs”

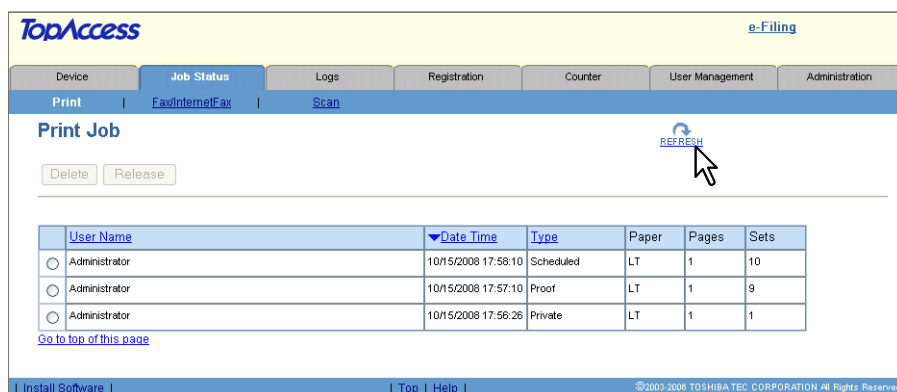
📖 P.25 “Deleting print jobs”

📖 P.26 “Releasing print jobs”

■ Displaying print jobs

Accessing the Print Job page in the [Job Status] tab

- 1 Click the [Job Status] tab and click the [Print] menu.
The Print Job page is displayed.
- 2 If your print job previously released is not displayed in the list, click the [REFRESH] icon at the upper right of the page.



Tips

- Print jobs that have finished being printed are displayed in the [Logs] tab.
- To sort the print jobs list so that a particular job is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

The Print Job page display the following information for each print job.

- **User Name**
Displays the login user name of a computer from which a print job was sent.
- **Date Time**
Displays the date and time when the print job was released from the client computers.
- **Type**
Displays the print job type.
- **Paper**
Displays the paper size of the print jobs.
- **Pages**
Displays the number of pages the print job contains.
- **Sets**
Displays the number of copies set in the print jobs.

■ Deleting print jobs

You can delete jobs that are stored in the queue.

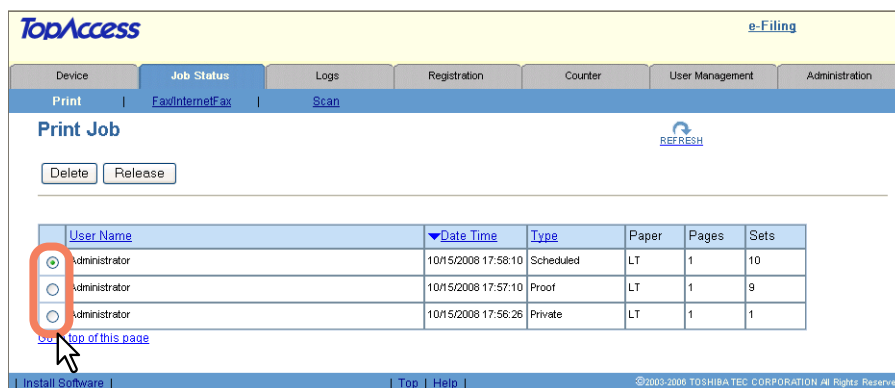
Note

To delete private print jobs and hold print jobs on the TopAccess menu, you must log in as an administrator in the [Administration] tab page first, and then display the Print Job page on the [Job] tab page. If you logged in as an administrator, [Delete All Private Print Jobs] and [Delete All Hold Print Jobs] are displayed next to [Release]. Click [Delete All Private Print Jobs] to delete all private jobs in the list. Or click [Delete All Hold Print Jobs] to delete all hold jobs in the list. It may take a while to delete all private or hold jobs.

3

Deleting a print job

- 1 Click the [Job Status] tab and click the [Print] menu.
The Print Job page is displayed.
- 2 Select an option button at the left of the print job that you want to delete.



You can select only one print job at a time.

- 3 Click [Delete].
The selected print job is deleted.

■ Releasing print jobs

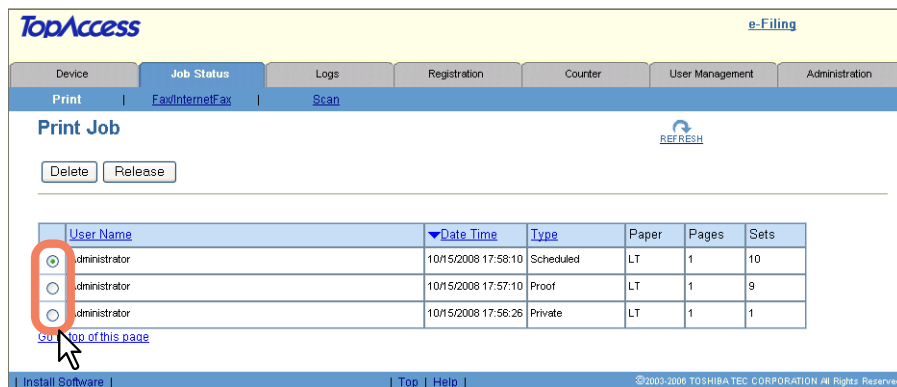
You can print jobs that are stored in the queue.

Note

Private print jobs and hold print jobs cannot be released from the TopAccess.

Releasing print jobs

- 1 Click the [Job Status] tab and click the [Print] menu.**
The Print Job page is displayed.
- 2 Select an option button at the left of the print job that you want to release.**



You can select only one print job at a time.

- 3 Click [Release].**
The selected print job is immediately printed.

Managing Fax/Internet Fax Jobs

Using TopAccess, you can display and delete fax transmission jobs including fax transmissions and Internet Fax transmissions.

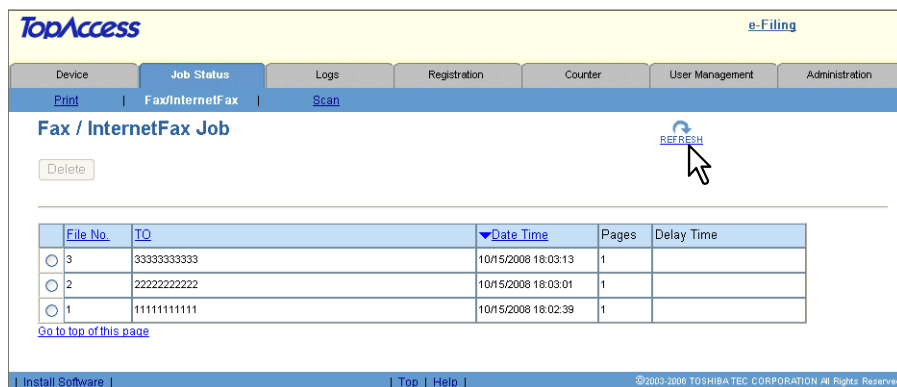
📖 P.27 “Displaying Fax/Internet Fax jobs”

📖 P.28 “Deleting Fax transmission jobs”

■ Displaying Fax/Internet Fax jobs

Accessing the Fax/InternetFax Job page in the [Job Status] tab

- 1** Click the [Job Status] tab and click the [Fax/Internet Fax] menu.
The Fax/InternetFax Job page is displayed.
- 2** If your fax transmission job previously released is not displayed in the list, click the [REFRESH] icon at the upper right of the page.



Tips

- Transmission jobs that have finished their transmission are displayed in the [Logs] tab.
- To sort the fax transmission jobs list so that a particular job is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

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

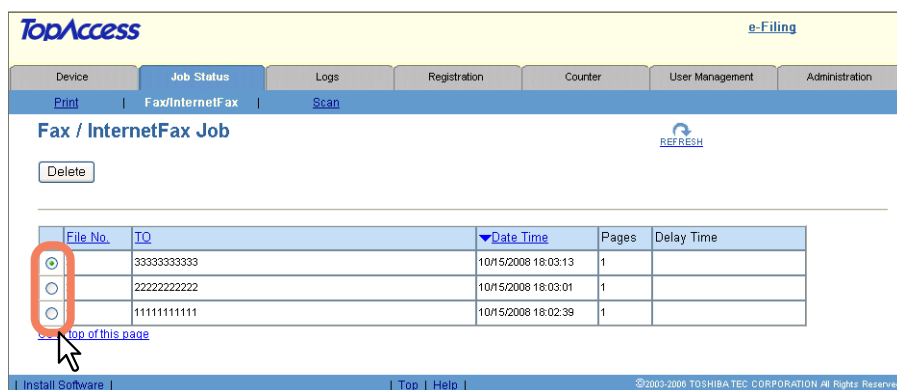
- **File No.**
Displays the file number to identify the fax transmission job.
- **TO**
Displays the destinations set for the fax transmission job.
- **Date Time**
Displays the date and time when the fax transmission job is released from the touch panel or client computer using the N/W-Fax driver.
- **Pages**
Displays the number of pages the fax transmission job contains.
- **Delay Time**
Displays the delayed time set for the fax transmission job.

■ Deleting Fax transmission jobs

You can delete a fax transmission job.

Deleting a fax transmission job

- 1 Click the [Job Status] tab and click the [Fax/Internet Fax] menu.**
The Fax/InternetFax Job page is displayed.
- 2 Select an option button at the left of the fax transmission job that you want to delete.**



You can select only one fax transmission job at a time.

- 3 Click [Delete].**
The selected fax transmission job is deleted.

Managing Scan Jobs

Using TopAccess, you can display and delete scan jobs that are currently in the queue.

📖 P.29 “Displaying scan jobs”

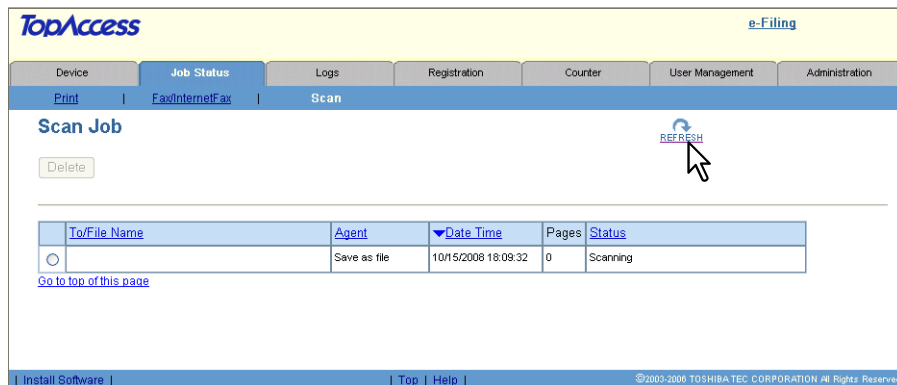
📖 P.30 “Deleting scan jobs”

■ Displaying scan jobs

Accessing the Scan Job page in the [Job Status] tab

3

- 1 Click the [Job Status] tab and click the [Scan] menu.
The Scan Job page is displayed.
- 2 If your scan job previously released is not displayed in the list, click the [REFRESH] icon at the upper right of the page.



Tips

- Scan jobs that have finished being scanned are displayed in the [Logs] tab.
- To sort the scan jobs list so that a particular job is easier to find, click the appropriate table heading. The page refreshes to display the information in the order requested.

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

- **To/File Name**

When the job performs the Scan to File or USB or Scan to e-Filing, it displays the document name to be stored. When the job performs the Scan to Email, it displays the destinations to which the scanned document will be sent.

Tip

When [OFF] is selected for the [Bcc Address Display] setting, [Bcc Address] is displayed instead of the actual Bcc e-mail address.

📖 P.184 “Setting up Email Setting”

- **Agent**

Displays the agent of the scan job. When scanning is performed with multiple agents, this displays “Dual Agent”.

- **Date Time**

Displays the date and time when the scan job is released from the touch panel.

- **Pages**

Displays the number of pages the scan job contains.

- **Status**

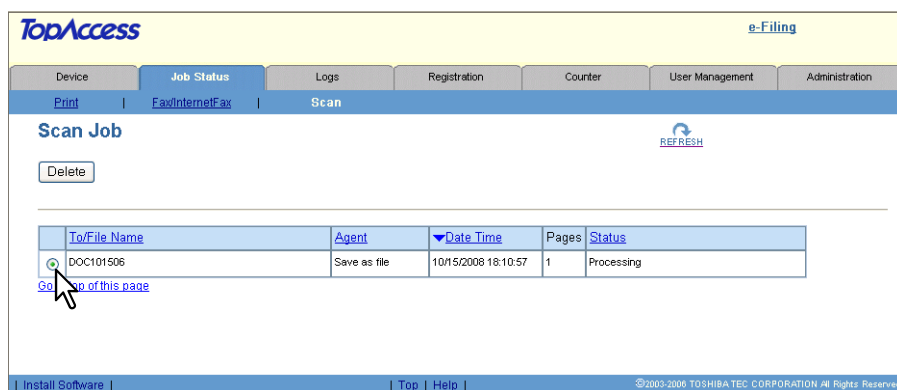
Displays the detailed status of the scan job.

■ Deleting scan jobs

You can delete a scan job.

Deleting scan jobs

- 1 Click the [Job Status] tab and click the [Scan] menu.**
The Scan Job page is displayed.
- 2 Select an option button at the left of the scan job that you want to delete.**



You can select only one scan job at a time.

- 3 Click [Delete].**
The selected scan job is deleted.

DISPLAYING JOB LOGS

Using TopAccess, end users can display print job logs, transmission journals, reception journals, and scan job logs.

Displaying Print Job Logs	32
Displaying Transmission Journals	33
Displaying Reception Journals	34
Displaying Scan Job Logs.....	35

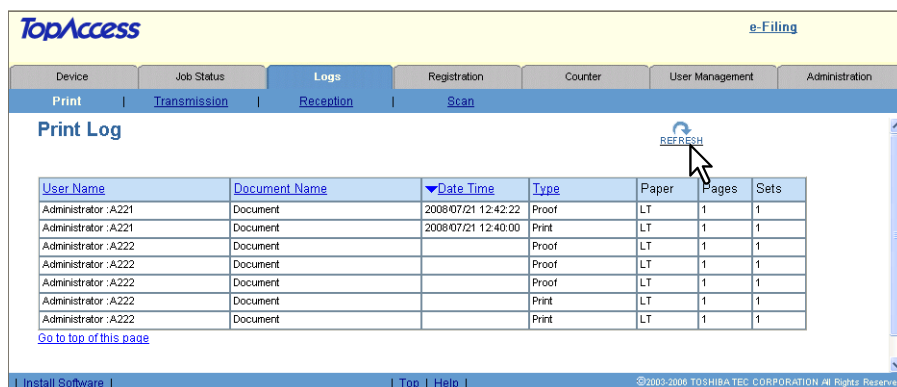
Displaying Print Job Logs

Using TopAccess, you can display logs of print jobs performed on this equipment.

Up to 100 logs are displayed in chronological order, with the most recent first. When the number of logs exceeds 100, logs are deleted, beginning with the oldest one.

Accessing the Print Log page in the [Logs] tab

- 1 Click the **[Logs]** tab and click the **[Print]** menu.
The Print Log page is displayed.
- 2 Click the **[REFRESH]** icon at the upper right of the page to update the information.



User Name	Document Name	Date Time	Type	Paper	Pages	Sets
Administrator :A221	Document	2008/07/21 12:42:22	Proof	LT	1	1
Administrator :A221	Document	2008/07/21 12:40:00	Print	LT	1	1
Administrator :A222	Document		Proof	LT	1	1
Administrator :A222	Document		Proof	LT	1	1
Administrator :A222	Document		Proof	LT	1	1
Administrator :A222	Document		Print	LT	1	1
Administrator :A222	Document		Print	LT	1	1

Tip

To sort the print job logs list so that a particular job log is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

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

- **User Name**
Displays the login user name of a computer from which a print job was sent. Click the header link to sort the print job list by user name.
- **Document Name**
Displays the document name of the print job. Click the header link to sort the print job list by document name.
- **Date Time**
Displays the date and time that the print job was released from the client computers. Click the header link to sort the print job list by Date and Time.
- **Type**
Displays the print job type. Click the header link to sort the print job list by print job type.
- **Paper**
Displays the paper size of the print jobs.
- **Pages**
Displays the number of pages the print job contains.
- **Sets**
Displays the number of copies set for print jobs.

Displaying Transmission Journals

Using TopAccess, you can display the transmission journals that this equipment sent by fax, Internet Fax transmission, and E-mail.

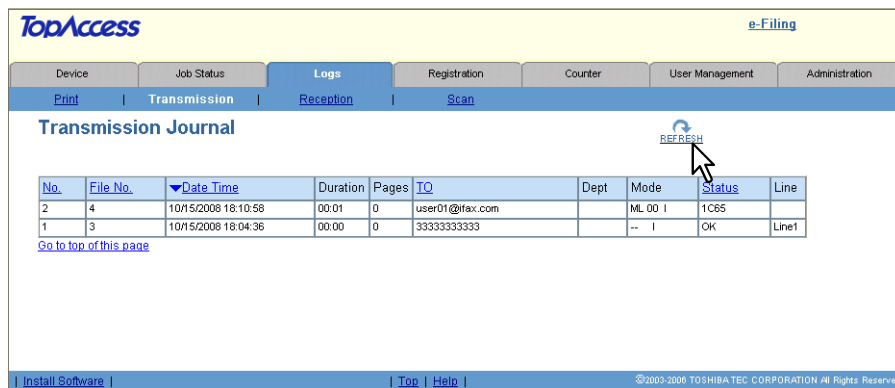
Up to 100 logs are displayed in chronological order, with the most recent first. When the number of logs exceeds 100, logs are deleted, beginning with the oldest one.

Accessing the Transmission Journal page in the [Logs] tab

1 Click the [Logs] tab and click the [Transmission] menu.

The Transmission Journal page is displayed.

2 Click the [REFRESH] icon at the upper right of the page to update the information.



Tip

To sort the transmission journals list so that a particular transmission journal is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

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

- **No.**
Displays the serial number of the journals.
- **File No.**
Displays the file number to identify the transmission job.
- **Date Time**
Displays the date and time the transmission job was performed.
- **Duration**
Displays the time length taken for the transmissions. If it takes more than 1 hour, "59:59" is indicated.
- **Pages**
Displays the number of pages the transmission job contains.
- **TO**
Displays the destinations set for the transmission job.
- **Dept**
Displays the department code if the department management is enabled.
- **Mode**
Displays the transmission mode.
The transmission mode is displayed by a combination of a 2-digit alphabet code, a 3-digit numeric code, and up to a 4-digit supplemental code.
For example: EC 603

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

- **Status**
Displays the result of the transmission.
- **Line**
Displays the line used.

Displaying Reception Journals

Using TopAccess, you can display the reception journals that this equipment received by fax, Internet Fax transmission, and E-mail.

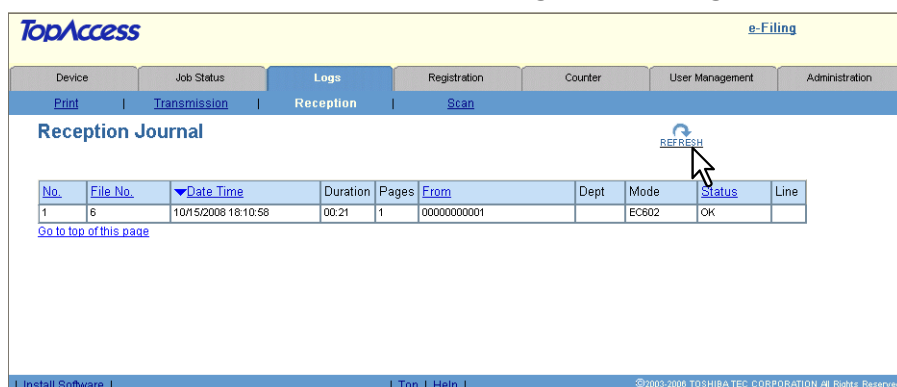
Up to 100 logs are displayed in chronological order, with the most recent first. When the number of logs exceeds 100, logs are deleted, beginning with the oldest one.

Accessing the Reception Journal page in the [Logs] tab

1 Click the [Logs] tab and click the [Reception] menu.

The Reception Journal page is displayed.

2 Click the [REFRESH] icon at the upper right of the page to update the information.



Tip

To sort the reception journals list so that a particular reception journal is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

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

- **No.**
Displays the serial number of the journals.
- **File No.**
Displays the file number to identify the received job.
- **Date Time**
Displays the date and time of receiving the job.
- **Duration**
Displays the time taken for the receptions. If it takes more than 1 hour, "59:59" is indicated.
- **Pages**
Displays the number of pages the received job contains.
- **From**
Displays the sender's email address or fax number of the received job.
- **Dept**
Displays the department code if the department management is enabled.
- **Mode**
Displays the reception mode.
The reception mode is displayed by a combination of a 2-digit alphabet code, a 3-digit numeric code, and up to a 4-digit supplemental code.
For example: EC 603

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

- **Status**
Displays the result of the reception.
- **Line**
Displays the line used.

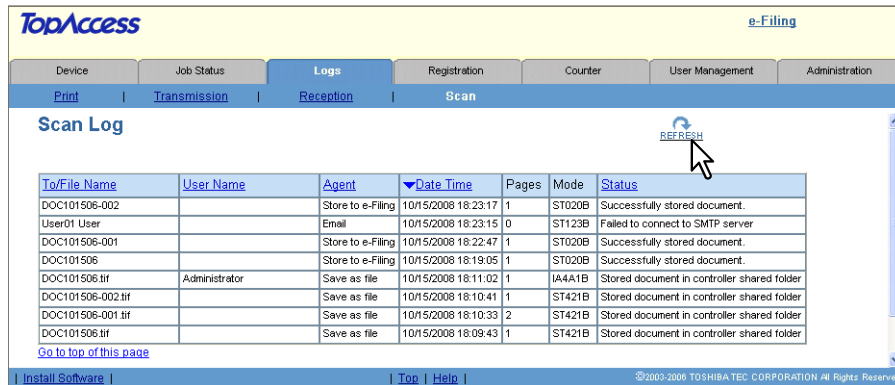
Displaying Scan Job Logs

Using TopAccess, you can display scan job logs that this equipment performed.

Up to 100 logs are displayed in chronological order, with the most recent first. When the number of logs exceeds 100, logs are deleted, beginning with the oldest one.

Accessing the Scan Log page in the [Logs] tab

- 1 Click the [Logs] tab and click the [Scan] menu.
The Scan Log page is displayed.
- 2 Click the [REFRESH] icon at the upper right of the page to update the information.



Tip

To sort the scan job logs list so that a particular scan job log is easier to find, click the appropriate table heading. The page refreshes to display the information in the order you requested.

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

- **To/File Name**

When the job performed the Scan to File or USB or Scan to e-Filing, it displays the document name that was stored. When the job performed the Scan to Email, it displays the destinations where the scanned document was sent.

Note

When [OFF] is selected for the [Bcc Address Display] setting, [Bcc Address] is displayed instead of the actual Bcc e-mail address.

📖 P.184 "Setting up Email Setting"

- **User Name**

Displays the account name of the user who has performed the scan job, when the User Management Setting is enabled.

- **Agent**

Displays the agent of the scan job.

- **Date Time**

Displays the date and time when the scan job was released from the control panel.

- **Pages**

Displays the number of pages the scan job contains.

- **Mode**

Displays the transmission mode using 6 character codes. Each code describes the details of the transmission mode as below.

Code Format: AA B C D E

AA: This describes the job type.

- CA: Copy and File, Copy and Store to e-Filing
- CT: Copy to e-Filing (without printing)
- FS: Relay Mailbox Transmission
- FF: Fax Received Forward
- FE: Internet Fax Received Forward
- ST: Scan to File or USB, Scan to e-Filing, Scan to Email
- FA: Fax and Save as File
- PA: Print and e-Filing
- PT: Print to e-Filing
- IA: N/W-Fax and Save as File
- BE: e-Filing to Email

- RS: Remote Scan

B: This describes the transmission type.

- 0: e-Filing
- 1: Email (SMTP)
- 2: FTP
- 3: SMB
- 4: Local
- 5: NetWare IPX/SPX
- 6: USB
- 7: NetWare TCP/IP
- 9: Remote Scan or Web Services Scan

C: This describes the resolution.

- 0: 100 dpi
- 1: 150 dpi
- 2: 200 dpi
- 3: 300 dpi
- 4: 400 dpi
- 5: 600 dpi
- A: 8x3.85 (line/mm) (203x98)
- B: 8x7.7 (line/mm) (203x196)
- C: 8x15.4 (line/mm) (203x391)
- D: 16x15.4 (line/mm) (400x391)

D: This describes the file format.

- 0: e-Filing
- 1: TIFF (Multi)
- 2: TIFF (Single)
- 3: PDF (Multi) or Encrypt PDF (Multi)
- 4: JPEG
- 5: PDF (Single) or Encrypt PDF (Single)
- 6: Slim PDF (Multi)
- 7: Slim PDF (Single)
- 8: XPS (Multi)
- 9: XPS (Single)
- A: DIB

E: This describes the file color mode.

- B: Black
- G: Gray Scale
- C: Color
- M: Mix

- **Status**

Displays the detailed result status of the scan job.

REGISTERING FROM TopAccess

This chapter contains instructions on how to register templates, the address book, and mailboxes.

Managing Templates	38
Registering private template groups	38
Registering private templates	45
Displaying public templates	77
Managing Address Book	78
Managing contacts in the Address Book	78
Managing groups in the Address Book	83
Managing Mailboxes	86
Setting up an Open Mailbox	87
Deleting an Open Mailbox	93

Managing Templates

Templates contain preset information for the operation of the copiers, scans, and fax and Internet Fax transmissions so that users can perform these operations easily by selecting the template button on the touch panel.

Templates are stored in groups. There are up to 200 private template groups and one public group. Each group can contain up to 60 templates.

Tips

- In the [Useful Template] group, useful templates have been registered in the private template group.
- Templates in the public group are created and maintained by the administrator. The public group can be accessed by all users, but some of the templates may be designed for specific purposes and have passwords assigned to them. For more information about setting up the public templates, see the following section.
 P.236 “Registering public templates”

Templates in private template groups are based on particular group profiles. Private groups can be assigned passwords. You can also assign passwords to individual templates. If it has no password assigned at either the template or group level, a [private] template is accessible to all users.

In practice, you may not need to create templates or groups yourself. The administrator and other users may have set up all the templates you need for your work. Before creating any template, look on your system to see what templates are available.

When users set up the templates and template group for the first time, you must first create a template group according to how templates are grouped, and then register the template that you require.

 P.38 “Registering private template groups”

 P.45 “Registering private templates”

In addition, you can also display the templates list registered in the public group.

 P.77 “Displaying public templates”

Tip

Templates can be managed using the touch panel. For managing templates from the touch panel, refer to the *Copying Guide*.

■ Registering private template groups

Before registering private templates, you have to register the private template group. You can classify the private templates according to every department, every user, and a use by registering the private template groups.

Also each private template group can be protected by the password.

 P.38 “Setting group information”

 P.40 “Setting group password”

 P.43 “Resetting group information”

□ Setting group information

You can define up to 200 private template groups. To define the private template groups, you can specify the group name, owner, and email notification setting.

Setting a private template group information

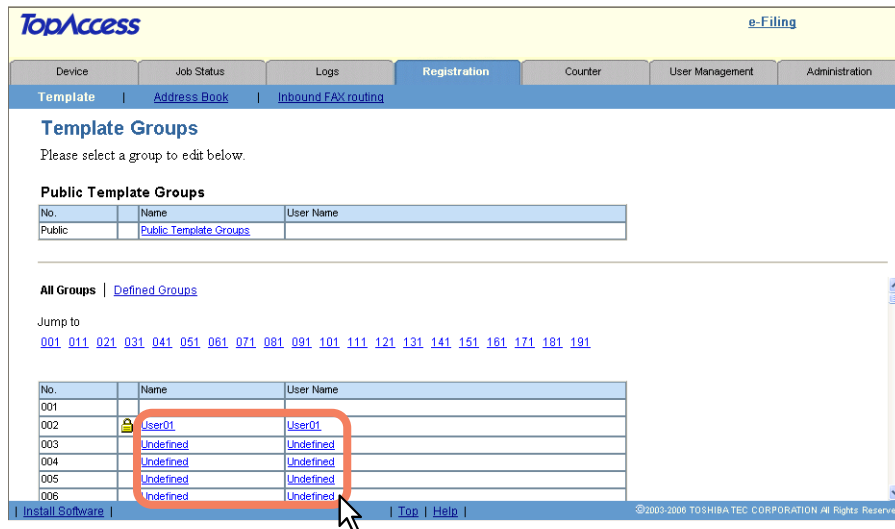
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can login to the [Registration] tab page.

- 2** Click the [Undefined] group name link to define a new private template group, or click the group name link that has been defined to edit the private template group information.

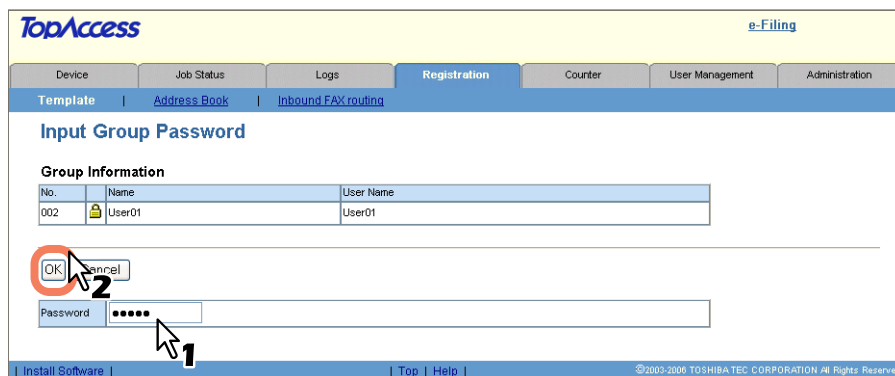


- If you select the private template group that has not been defined, the Group Properties page is displayed. Skip to step 5.
- If you select the defined private template group that is not protected by a password, the Private Templates page is displayed. Skip to step 4.
- If you select the defined private template group that is protected by a password, the Input Group Password page is displayed. Go to the next step.

Tips

- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups in default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

- 3** When the Input Group Password page is displayed, enter a 5-digit password for the selected private template group (or administrator's password) and click [OK].



The Private Templates page is displayed.

4 Click [Edit] to define or edit the group information.

TopAccess e-Filing

Device Job Status Logs **Registration** Counter User Management Administration

Template Address Book Inbound FAX routing

Private Templates [Template Groups](#)

Group Information

[Edit](#) [Change Password](#) [Reset](#)

No.	Name	User Name
002	User01	User01

Panel View [List View](#)

Please click a template picture to edit.

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Group Properties page is displayed.

5 Enter the items below as required.

TopAccess e-Filing

Device Job Status Logs **Registration** Counter User Management Administration

Template Address Book Inbound FAX routing

Group Properties

Group Information

No.	Name	User Name
002	User01	User01

[Save](#) [Cancel](#)

*Required

Number 002

Name User01

User Name User01

Notification This email address is used as default recipient each for template.
Email to user01@ifax.com

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

Number — Displays the number of the private template group.

Name — Enter the name of the private template group.

User Name — Enter the owner name of the private template group.

Notification — Enter the default email address to which the notification will be sent. The email address entered here will be displayed in the Panel Setting page and can be selected for the destination of the notifications when creating a private template in this group.

6 Click [Save] to apply changes.

7 You can continue setting the group password, or registering or editing templates in the group, as required.

P.40 "Setting group password"

P.45 "Registering private templates"

□ Setting group password

To set the group password, you must register the private template group first. You can set the password for the group that you have already registered.

Setting the group password

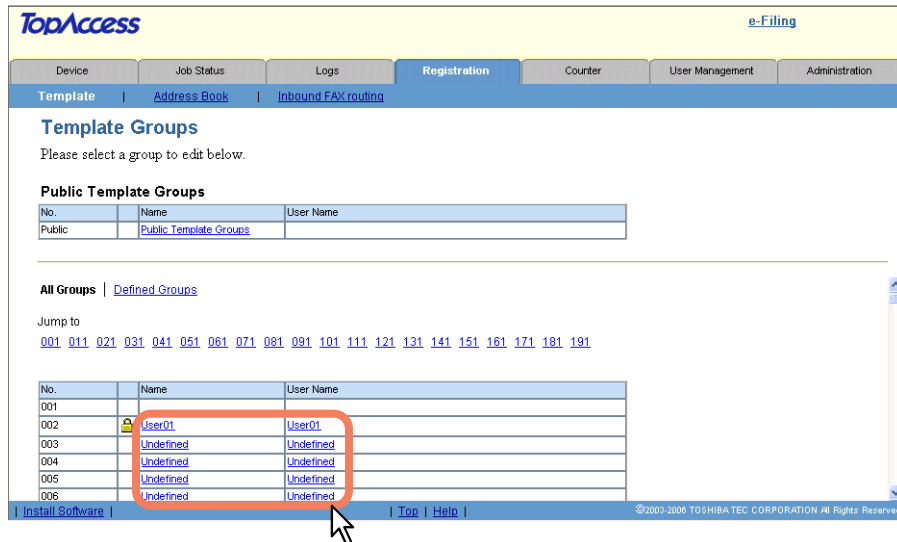
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can login to the [Registration] tab page.

2 Click the group name link that you want to set or to modify the group password.

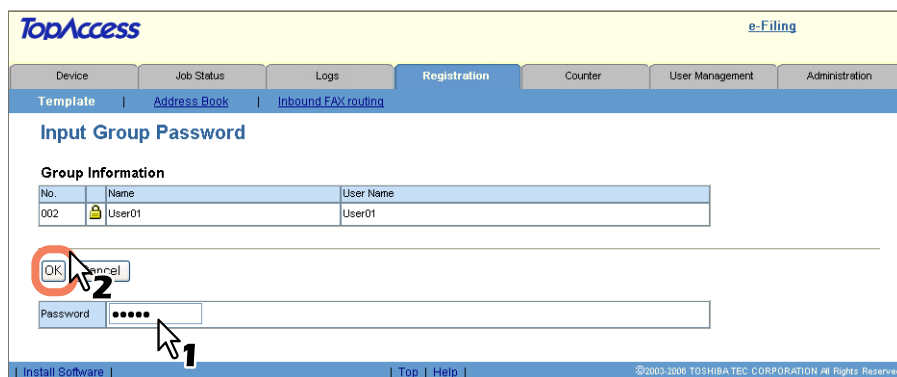


- If you select the private template group that is not protected by a password, the Private Templates page is displayed. Skip to step 4.
- If you select the private template group that is protected by a password, the Input Group Password page is displayed. Go to the next step.

Tips

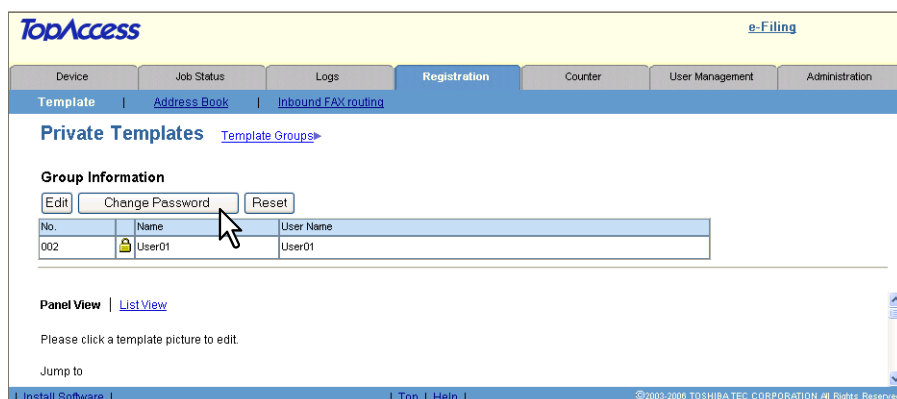
- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups in default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

3 When the Input Group Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template group and click [OK].



The Private Templates page is displayed.

4 Click [Change Password] to set or change the password for the private template group.



The Change Group Password page is displayed.

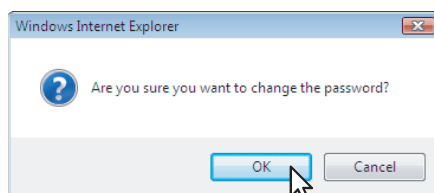
5 Enter the old password in the [Old Password] box, and new password in the New Password and [Retype Password] boxes.

- You can only use 5-digit numbers for the password.
- You can also enter the administrator password in the [Old Password] box.
- If the password has not been set for the group, leave the [Old Password] box blank.
- Leaving the [New Password] and [Retype Password] box blank releases password protection for the group.

6 Click [Save].

The confirmation dialog box appears.

7 Click [OK].



The group password is set or modified.

❑ Resetting group information

You can reset the group information that you no longer require and turn it to an undefined group.

Note

If you reset the group information, all private templates registered in the group will be deleted.

Resetting group information

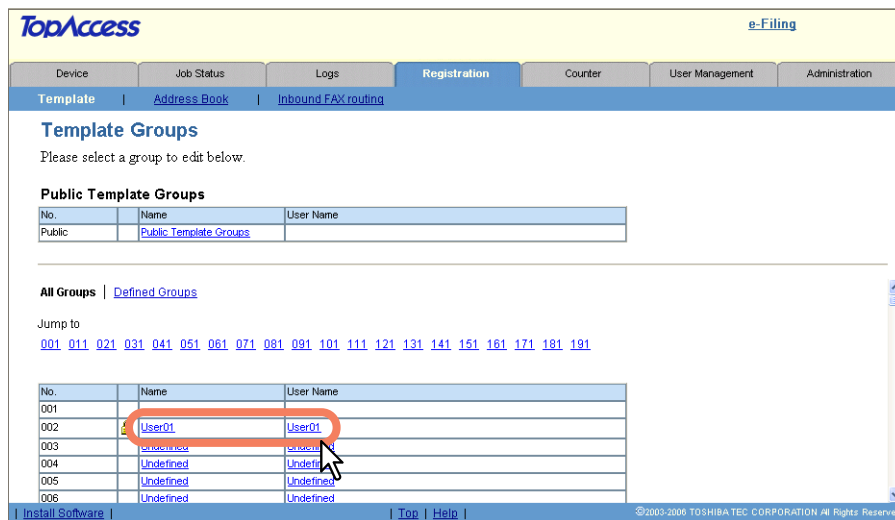
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can login to the [Registration] tab page.

2 Click the group name link that you want to reset.



- If you select the private template group that is not protected by a password, the Private Templates page is displayed. Skip to step 4.
- If you select the private template group that is protected by a password, the Input Group Password page is displayed. Go to the next step.

Tips

- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups in default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

- 3** When the Input Group Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template group and click [OK].

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Input Group Password

Group Information

No.	Name	User Name
002	User01	User01

OK Cancel

Password:

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Private Templates page is displayed.

- 4** Click [Reset].

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Private Templates

Template Groups

Group Information

Edit Change Password Reset

No.	Name	User Name
002	User01	User01

Panel View | List View

Please click a template picture to edit.

Jump to

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The confirmation dialog box appears.

- 5** Click [OK].

Windows Internet Explorer

Do You really want to Reset?

OK Cancel

The group information is reset.

■ Registering private templates

In each private template group, you can create up to 60 templates. To define the private template, specify the panel settings that will be displayed in the touch panel and agent settings. Each private template can also be protected by a password.

📖 P.45 “Registering or editing private templates”

📖 P.70 “Setting template password”

📖 P.74 “Resetting private templates”

□ Registering or editing private templates

Each template can be created in combination of the following agents:

- Copy template can be combined with the Save as file or Store to e-Filing agent.
- Fax/Internet Fax template can be combined with the Save as file agent.
- Scan template can be created with up to two agents in combination of the Save as file, Email, and Store to e-Filing agents.

Registering or editing a private template

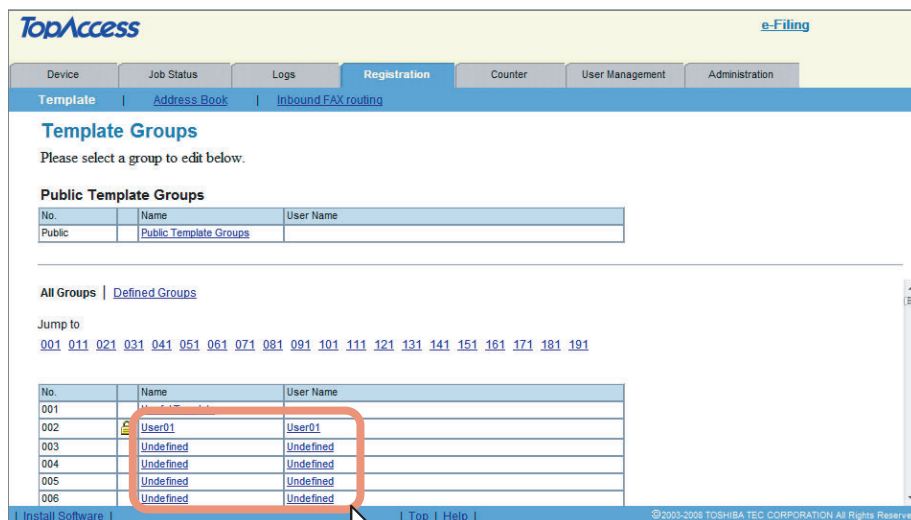
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can login to the [Registration] tab page.

2 Click the group name link where you want to register or edit the private template.



- If you select the private template group that is not protected by a password, the Private Templates page is displayed. Skip to step 4.
- If you select the private template group that is protected by a password, the Input Group Password page is displayed. Go to the next step.

Tips

- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups in default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

- 3** When the Input Group Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template group and click [OK].

The screenshot shows the 'Input Group Password' page in the TopAccess application. It features a 'Group Information' table with one entry: No. 002, Name User01, and User Name User01. Below the table is a password input field with a red circle around it and a mouse cursor pointing to it, labeled '1'. To the left of the password field is an 'OK' button with a red circle around it and a mouse cursor pointing to it, labeled '2'.

The Private Templates page is displayed.

- 4** From the templates list, click the [Undefined] icon to register a new template, or click defined icon to edit the template.

The screenshot shows the 'Private Templates' page in the TopAccess application. It features a 'Group Information' table with one entry: No. 002, Name User01, and User Name User01. Below the table is a 'Panel View' section with a 'List View' link. The 'List View' section shows a table of templates. The first row is highlighted with a red circle and a mouse cursor pointing to it, labeled '1'. The second row is also highlighted with a red circle and a mouse cursor pointing to it, labeled '2'.

- If the templates list is displayed in the List view, click the [Undefined] template name to register new template, or click the defined template name to edit the template.
- If you select the private template that has not been defined, the Template Properties page to select agents is displayed. Skip to step 7.
- If you select the defined private template that is not protected by a password, the Template Properties page is displayed. Skip to step 6.
- If you select the defined private template that is protected by a password, the Input Template Password page is displayed. Go to the next step.

Tips

- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which private template you want to define or edit, click the number of the private template in the [Jump to] links.

- 5** When the Input Template Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template and click [OK].

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Input Template Password

Group Information

No.	Name	User Name
2	User01	User01

Template Information

No.	Name	User Name
1	COPY MODE	

OK Cancel

Password: [5-digit masked input]

1 2

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The Template Properties page is displayed.

- 6** Click [Edit] to define or edit the template properties.

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Template Properties

Template Groups Private Templates

Group Information

No.	Name	User Name
2	User01	User01

Template Information

No.	Name	User Name
1	COPY MODE	

Edit Change Password Reset Template

Panel

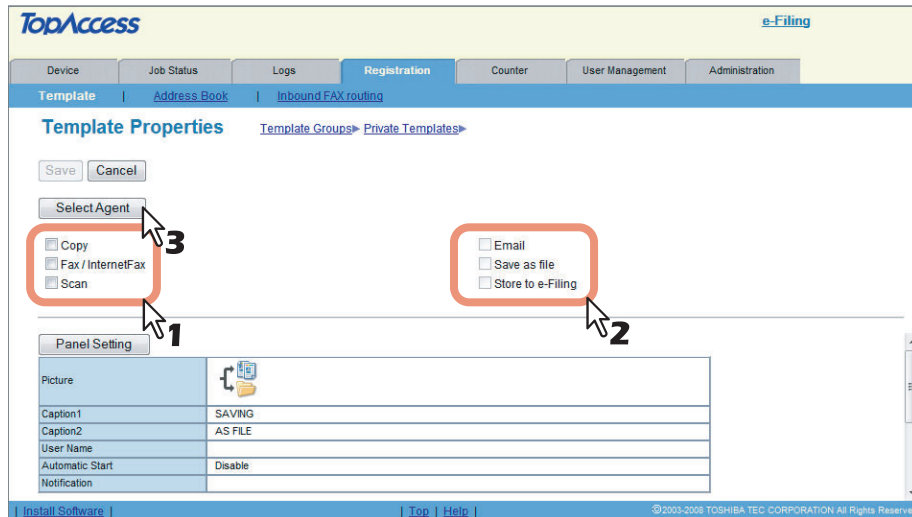
COPY MODE

Notification	
Automatic Start	Disable
Agent	Copy
Scanner	

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The Template Properties page to select agents is displayed.

7 Select agents and click [Select Agent].



You can select one of the following templates:

Copy — Select this to create a copy template. Usually, this is selected to print copies as well as sending originals to other destinations. This agent can also be combined with the Save as file agent or Store to e-Filing agent.

Fax/InternetFax — Select this to create a fax and Internet Fax transmission template. This agent can be combined with the Save as file agent.

Scan — Select this to create a scan template combined with the Email, Save as file, and Store to e-Filing agents. When you select this, select the agent from [Email], [Save as file], or [Store to e-Filing]. You can specify up to two agents for a scan template.

8 Click each button displayed in the page to specify or edit the associated template properties.

[Panel Setting] — Click this to specify the icon settings for the template.

P.51 “Panel Setting (Private template)”

Panel Setting	
Picture	
Caption1	SAVING
Caption2	AS FILE
User Name	
Automatic Start	Disable
Notification	

[Destination Setting] — Click this to specify the document’s destination. This can be set only when creating the Fax/Internet Fax agent or Scan to Email agent.

P.52 “Destination Setting (Private template)”

When Creating a Fax/Internet Fax agent:

Destination Setting	
Destination	

When Creating a Scan to Email agent:

To: Destination Setting	
To: Destination	

Cc: Destination Setting	
Cc: Destination	

Tip

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

P.184 “Setting up Email Setting”

To: Destination Setting	
To: Destination	

Bcc: Destination Setting	
Bcc: Destination	

[InternetFax Setting] — Click this to specify how the document will be sent. This can be set only when creating a Fax/Internet Fax agent.

P.58 “InternetFax Setting (Private template)”

InternetFax Setting	
Subject	Scanned from (Device Name)((Template Name))(Date)(Time)
From Address	
From Name	
Body	
File Format	TIFF-S
Fragment Page Size	No Fragmentation

[Fax Setting] — Click this to specify how the document will be sent. This can be set only when creating a Fax/Internet Fax agent.

P.59 “Fax Setting (Private template)”

Fax Setting	
Resolution	Standard
Original Mode	Text
Exposure	Auto
Transmission Type	
ECM	ON
Line Select	
Quality Transmit	
SUB/SEP	
Polling	
Delayed Transmit	00 00:00
Priority Transmit	OFF

[Email Setting] — Click this to specify how the document will be sent. This can be set only when creating a Scan to Email agent.

P.61 “Email Setting (Private template)”

Email Setting	
Subject	
From Address	mfp-00c67861@fax.com
From Name	MFP-00C67861
Body	
File Format	PDF(Multi)
File Name	DocMMDDYY(MMDDYY is a date)
Fragment Message Size	No Fragmentation

[Save as file Setting] — Click this to specify how the document will be stored in a local hard disk or network folder. This can be set only when creating a Save as file agent.

P.63 “Save as file Setting (Private template)”

Save as file Setting	
File Format	TIFF(Multi)
Destination	WMFP-0499820(FILE_SHARE)
File Name	DocMMDDYY(MMDDYY is a date)

[Box Setting] — Click this to specify how the document will be stored in a Box. This can be set only when creating a Scan to e-Filing agent.

P.66 “Box Setting (Private template)”

Box Setting	
Destination	000
Folder Name	
Document Name	DocMMDDYY(MMDDYY is a date)

[Scan Setting] — Click this to specify how the document will be scanned. This can be set only when creating the Save as file agent, Scan to Email agent, and Scan to e-Filing agent. This cannot be set when combining a Fax/Internet Fax agent.

P.67 “Scan Setting (Private template)”

Scan Setting	
Preview	OFF
Single/2-Sided Scan	Single
Rotation	
Color Mode	Black
Resolution	600dpi
Compression	
Original Mode	Text
Exposure	Auto
Original Size	Auto
Background	0
Contrast	0
Sharpness	0
Saturation	0
RGB Adjustment	Red: 0 Green: 0 Blue: 0
Omit Blank Page	OFF
Outside Erase	OFF

9 After configuring the desired template properties, click [Save].

The template properties are registered.

10 The template has been registered or edited. You can click the Template Groups link at the upper side of the page to return to the Template Groups page.

Panel Setting (Private template)

In the Panel Setting page, specify how the icon for the template is displayed in the touch panel, and the notification settings for the template.

- 1) **Picture**
This indicates the icon that will be displayed in the touch panel. The icon is automatically designated according to the agent that you select.
- 2) **Caption1**
Enter the text that will be displayed next to the icon in the touch panel. You can enter up to 11 alphanumeric characters.
- 3) **Caption2**
Enter the text that will be displayed next to the icon in the touch panel. You can enter up to 11 alphanumeric characters.
- 4) **User Name**
Enter the owner name of the template. You can enter up to 30 alphanumeric characters.

5) Automatic Start

Select whether the automatic start function is enabled or disabled. When this is enabled, the operation will be automatically started when you press the template button from the TEMPLATE menu on the touch panel without pressing the [START] button or [SCAN].

Note

If the user names or passwords of the User Authentication for Scan to E-mail and the User Management Setting are different, or only the User Authentication for Scan to E-mail is enabled, you need to enter the user name and password of the User Authentication for Scan to E-mail also when recalling the template with the automatic start function enabled.

6) Notification — Send email when an error occurs

Select this to send a notification message to the specified email address when an error occurs.

7) Notification — Send email when job is completed

Select this to send a notification message to the specified email address when a job is completed.

8) Notification — Email to

Select to send the notification message to the email address that is set to the public group, or enter an email address to which the notification message will be sent.

Note

When you enable the Notification setting, make sure to set up the Email settings in the [Email] submenu of the [Setup] menu in the TopAccess Administrator's mode. For instructions on how to set up the Email settings, see the following section.

 P.183 "Setting up Email settings"

Destination Setting (Private template)

In the Recipient List page, you can specify the destinations to which the fax, Internet Fax, or Scan to Email document will be sent.

When you are setting up the destinations for the Scan to Email agent, you can only specify the email addresses for the destinations.

When you are setting up the destinations for the Fax/Internet Fax agent, you can specify both fax numbers and email addresses for the destinations.

Note

The optional Fax Unit must be installed in this equipment to specify the fax numbers of the destinations.

You can specify the recipients by entering their email addresses or fax numbers manually, selecting recipients from the address book, selecting recipient groups from the address book, or searching for recipients in the LDAP server.

 P.52 "Entering the recipients manually"

 P.53 "Selecting the recipients from the address book"

 P.55 "Selecting the groups from the address book"

 P.56 "Searching for recipients in the LDAP server"

 P.58 "Removing the contacts from the recipient list"

Entering the recipients manually

You can add a recipient manually to the Recipient List.

1 Click [Destination Setting] to open the Recipient List page.**Tip**

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

 P.184 "Setting up Email Setting"

2 Click [New].

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐		

The Contact Property page is displayed.

3 Enter the email address or fax number of the recipient, in the [Destination] box.

Contact Property

OK Cancel Reset

*Required

Destination user01@ifax.com

Note

You can specify the fax number for the destination only when the optional Fax Unit is installed.

4 Click [OK].

The recipient is added to the Recipient List page.

5 Repeat steps 2 to 4 to add all additional recipients that you require.**Tip**

You can remove the contacts that you added to the recipient list before submitting the destination settings.
 P.58 "Removing the contacts from the recipient list"

6 Click [Save].

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐		user01@ifax.com

The contacts are added as destinations.

Selecting the recipients from the address book

You can select recipients from the address book in this equipment.

1 Click [Destination Setting] to open the Recipient List page.**2 Click [Address Book].**

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐		

The Address Book page is displayed.

3 Select the [Email] check boxes of users you want to add as the Email recipients or Internet Fax recipients, and Select the [Fax] check boxes of users you want to add as the Fax recipients.

Address Book

Group: All Groups

Add Cancel

Email	Fax	Name	Email Address	Fax Number
☒	☒	User99 User	user99@ifax.com	10000000099
☒	☒	User98 User	user98@ifax.com	10000000098
☒	☒	User97 User	user97@ifax.com	10000000097
☒	☒	User96 User	user96@ifax.com	10000000096
☐	☐	User95 User	user95@ifax.com	10000000095
☐	☐	User94 User	user94@ifax.com	10000000094
☐	☐	User93 User	user93@ifax.com	10000000093
☐	☐	User92 User	user92@ifax.com	10000000092
☐	☐	User91 User	user91@ifax.com	10000000091
☐	☐	User90 User	user90@ifax.com	10000000090
☐	☐	User89 User	user89@ifax.com	10000000089

Notes

- When you are creating a Scan to Email template, only the [Email] check boxes are displayed in the Address Book page.
- You can specify the fax number for the destination only when the optional Fax Unit is installed.

Tip

If you want to sort the recipient list by a specific group, select the desired group name in the [Group] box.

4 Click [Add].

Selected recipients are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before submitting the destination settings.

P.58 "Removing the contacts from the recipient list"

5 Click [Save].

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐	User99 User	user99@ifax.com
☐	User99 User	10000000099
☐	User98 User	user98@ifax.com
☐	User98 User	10000000098
☐	User97 User	user97@ifax.com
☐	User97 User	10000000097
☐	User96 User	user96@ifax.com
☐	User96 User	10000000096

The contacts are added as destinations.

Selecting the groups from the address book

You can select groups from the address book.

1 Click [Destination Setting] to open the Recipient List page.

2 Click [Address Group].

The Address Group page is displayed.

3 Select the [Group] check boxes that contain the desired recipients.

4 Click [Add].

All recipients in the selected groups are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before submitting the destination settings.
 P.58 "Removing the contacts from the recipient list"

5 Click [Save].

The contacts are added as destinations.

Searching for recipients in the LDAP server

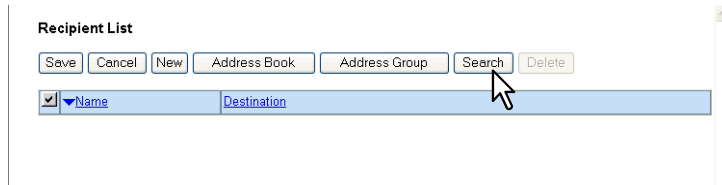
You can search for recipients in the registered LDAP server and in the address book.

Note

The LDAP server must be registered by an administrator.

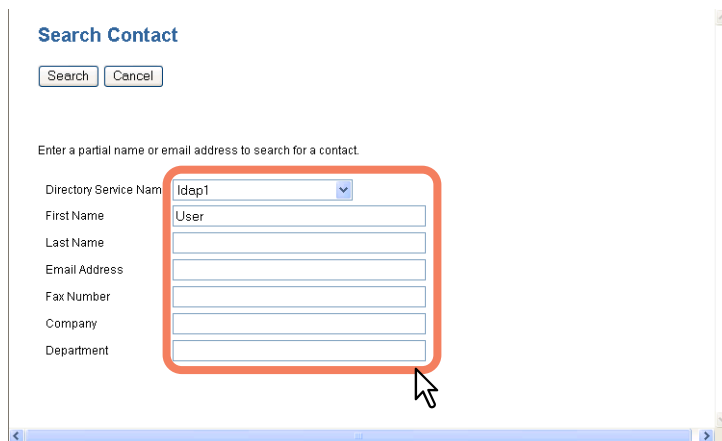
📖 P.216 “Managing directory service”

- 1 Click **[Destination Setting]** to open the Recipient List page.
- 2 Click **[Search]**.



The Search Contact page is displayed.

- 3 Select the directory service name that you want to search for in the **[Directory Service Name]** box, and enter the search terms in the boxes that you want to search.



Tips

- If you select the model name of this equipment at the **[Directory Service Name]** box, you can search for recipients in the address book of this equipment.
- TopAccess will search for recipients who match the entries.
- Leaving the box blank allows wild card searching. (However, you must specify at least one.)

- 4 Click **[Search]**.

TopAccess will start searching for recipients in the LDAP server and the Search Address List page will display the results.

5 Select the [Email] check boxes of users to add the Email recipients or Internet Fax recipients, and select the [Fax] check boxes of users to add the Fax recipients.

Search Address List

Add

Cancel

Email	Fax	Name	company	department	Email Address	Fax Number
☒	☒	User09 User	abcdef	ghijklmn	user09@ifax.com	412

View report

Go page

Notes

- When you are creating a Scan to Email template, the ID check boxes are displayed in the Search Address List page.
- You can specify the fax number for the destination only when the optional Fax Unit is installed.
- The value of [company] and [department] will depend on the settings determined by the administrator.

5

6 Click [Add].

The selected recipients are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before submitting the destination settings.

P.58 "Removing the contacts from the recipient list"

7 Click [Save].

Recipient List

Save

Cancel

New

Address Book

Address Group

Search

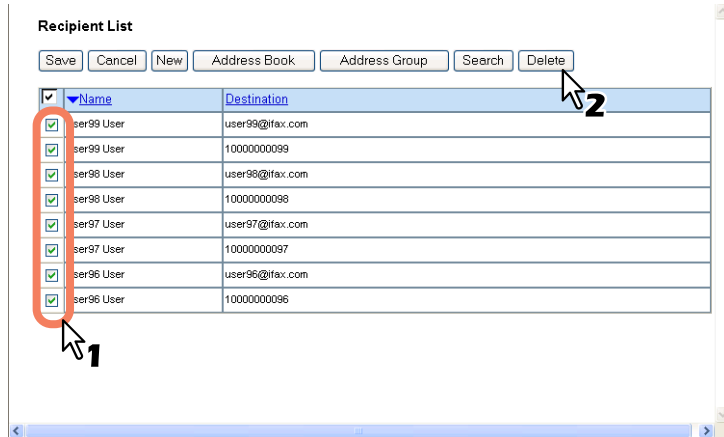
Delete

☒	Name	Destination
☐		user99@ifax.com
☐		10000000099
☐		user98@ifax.com
☐		10000000098
☐		user97@ifax.com
☐		10000000097
☐		user96@ifax.com
☐		10000000096

The contacts are added as destinations.

Removing the contacts from the recipient list

- 1 Click [Destination Setting] to open the Recipient List page.
- 2 Select the check boxes of the contacts that you want to remove from the recipient list, and click [Delete].



The selected contacts are removed from the recipient list.

InternetFax Setting (Private template)

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

The screenshot shows the 'InternetFax Setting' page. At the top, there are buttons: Save and Cancel. Below these are several fields, each with a number indicating its position in the list:

- 1 Subject: A dropdown menu with two options: 'Scanned from (Device Name)[(Template Name)](Date)(Time)' (selected) and an empty box.
- 2 *From Address: A text input field containing 'admin@ifax.com'.
- 3 From Name: A text input field containing 'admin'.
- 4 Body: A large text area for entering the body message.
- 5 File Format: A dropdown menu with 'TIFF-S' selected.
- 6 Fragment Page Size: A dropdown menu with 'No Fragmentation' selected.

- 1) **Subject**
This sets the subject of the Internet Faxes. Select [Scanned from (Device Name) [(Template Name)] (Date) (Time)] to automatically insert the subject or enter the desired subject in the box.
- 2) **From Address**
Enter the email address of the sender. When the recipient replies to a received document, the message will be sent to this email address.
- 3) **From Name**
Enter the sender name of the Internet Fax.
- 4) **Body**
Enter the body message of the Internet Fax. You can enter up to 1000 characters (including spaces).
- 5) **File Format**
Only [TIFF-S] (TIFF-FX (Profile S)) format can be selected.
- 6) **Fragment Page Size**
Select the size of the message fragmentation.

Fax Setting (Private template)

In the Fax Setting page, you can specify how the fax will be sent.

1) Resolution

Select the resolution for sending faxes.

- **Standard** — Select the Standard mode as the resolution for originals with regular size text.
- **Fine** — Select this to set the Fine mode as the resolution for originals with small text or detailed drawings.
- **Ultra Fine** — Select this to set the Ultra-Fine mode as the resolution for originals with particularly small text or precision drawings.

2) Original Mode

Select the image quality mode for sending faxes.

- **Text** — Select the Text mode as the image quality mode appropriate for sending text originals.
- **Text/Photo** — Select the Text/Photo mode as the image quality mode appropriate for sending originals containing both text and photos.
- **Photo** — Select the Photo mode as the image quality mode appropriate for sending photo originals.

3) Exposure

Select the exposure for sending faxes.

Select [Auto] to automatically apply the ideal contrast, or adjust the contrast manually in 11 stages.

4) Transmission Type

Select the send mode.

- **Memory Transmit** — Select the Memory TX mode to automatically send the document after it has been temporarily stored to memory. This mode is useful if you want to return original files immediately. You can also send the same originals to two or more remote Faxes.
- **Direct Transmit** — Select the Direct TX mode to send the original as it is being scanned. This mode is useful if you want confirmation from the remote party. Originals are not stored to memory, and you can specify only one remote Fax at a time.

Tip

You can select [Direct Transmit] when you have created a template for Fax/InternetFax (not for Saved as file).

5) ECM

Enable or disable the ECM (Error Correction Mode) to automatically resend any portion of the document affected by phone line noise or distortion.

6) Line Select

Select whether specifying the line to be used.

- **Auto** — Select not to specify the line to be used.
- **Line1** — Select to use Line 1 for this Fax agent.
- **Line2** — Select to use Line 2 for this Fax agent if installed.

7) Quality Transmit

Select this to send a document in the Quality TX mode. This feature sends a document at a slower speed than normal so the transmission will be less affected by line conditions.

8) SUB/SEP

Enter the SUB number or SEP number if you want to set the mailbox transmission.

9) SID/PWD

Enter the password for SUB or SEP if required.

10) Polling

Select this to set Polling communications.

- **(Blank)** — Select the blank box when you do not want to perform polling.
- **Transmit** — Select this to perform Polling Reservation that allows users to store the document in the memory.
- **Received** — Select this to perform Turnaround Polling that allows users to poll another fax after transmitting documents to the remote Fax on the same phone call.

Note

You can select [Transmit] when you have created a template for Fax/InternetFax (not to be Saved as file). When Fax/InternetFax and Save as file settings are combined, this item will be unselectable and will not be displayed.

11) Password

Enter the 4-digit security code for the document to be stored or received.

12) Fax Number (Security)

When you select [Transmit] at the [Polling] box, enter the security fax number that allows polling of stored document. When you select [Received] at the [Polling] box, enter the security fax number to poll the documents from remote Faxes.

13) Delayed Transmit

If you enable the delayed communications for this agent, enter the day and time to send a document.

14) Priority Transmit

Select whether the document will be sent prior to other jobs.

Email Setting (Private template)

In the Email Setting page, you can specify the content of the Scan to Email document to be sent.

1) Subject

This sets the subject of the Scan to Email documents. Select [Send data from (Device name) [(Template Name)]] set by default, or enter the desired subject in the box.

When you want to add the date and time to the subject, select the [Add the date and time to the subject] check box.

2) From Address

Enter the email address of the sender. When the recipient replies, the message will be sent to this email address.

3) From Name

Enter the sender name of the Scan to Email document.

4) Body

Enter the body message of the Scan to Email documents. You can enter up to 1000 characters (including spaces).

5) File Format

Select the file format of the scanned image.

- **TIFF (Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF (Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF (Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF (Single)** — Select this to save scanned images separately as Single-page PDF files.
- **Slim PDF (Multi)** — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. When no optional memory is installed, Slim PDF will not apply for scanning more than Letter or A4 size originals.
- **Slim PDF (Single)** — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. When no optional memory is installed, Slim PDF will not apply for scanning more than Letter or A4 size originals.
- **XPS (Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS (Single)** — Select this to save scanned images separately as Single-page XPS files.
- **JPEG** — Select this to save scanned images as JPEG files.

Tips

- If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, refer to the ***MFP Management Guide***.
- Files saved in an XPS format can be used in Windows Vista/Windows 7/Windows Server 2008 SP1, or Windows XP SP2/Windows Server 2003 SP1 or later versions with Net Framework 3.0 installed.

6) Encryption

Set this for encrypting PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.

Encryption

Select this if you want to encrypt PDF files.

User Password

Enter a password for opening encrypted PDF files.

Master Password

Enter a password for changing the Encrypt PDF setting.

Tips

- If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, refer to the ***MFP Management Guide***.
- The user password and the master password are not set at the factory shipment.
- Passwords must be from 1 to 32 one-byte alphanumeric characters.
- The user password must differ from the master password.

Notes

- These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. Ask the administrator for resetting these passwords.
- For the details of the encryption setting, refer to the ***MFP Management Guide***.

Encryption Level

Select the desired encryption level.

- **40-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1.
- **128-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4.
- **128-bit AES** — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6.

Authority

Select the desired types of authority for Encrypt PDF.

- **Printing** — Press this to authorize users to print documents.
- **Change of Documents** — Press this to authorize users to change documents.
- **Content Copying or Extraction** — Press this to authorize users to copy and extract the contents of documents.
- **Content Extraction for accessibility** — Press this to enable the accessibility feature.

7) File Name

Select how the scanned file will be named. Select [DocYYMMDD] to name it as described, or enter the desired file name in the box. When you want to add the date and time in the file name, select the [Add the date and time to a file name] check box.

8) Fragment Message Size

Select the size of the message fragmentation.

Save as file Setting (Private template)

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

The screenshot shows the 'Save as file Setting' dialog box. It has a title bar with 'Save' and 'Cancel' buttons. The dialog is divided into several sections, with numbered callouts 1 through 7 pointing to specific areas:

- 1** points to the 'File Format' section, which includes a dropdown menu currently set to 'TIFF(Multi)'.
- 2** points to the 'Encryption' section, which includes checkboxes for 'Encryption', 'User Password', 'Master Password', 'Encryption Level' (set to '128-bit RC4'), and 'Authority'. There are also checkboxes for 'Printing', 'Change of Documents', 'Content Copying or Extraction', and 'Content Extraction for accessibility'.
- 3** points to the 'Select following 2 items' section, which includes a checked checkbox for 'Use local folder' and an unchecked checkbox for 'Save to USB Media'.
- 4** points to the 'Remote 1' section, which includes an unchecked checkbox for 'Remote 1' and a radio button for 'Use Administrator Setting'.
- 5** points to the 'Destination' section, which includes a radio button for 'Use User Setting' and fields for 'Protocol' (SMB, FTP, NetWare IPX/SPX, NetWare TCP/IP), 'Server Name', 'Port Number(Command)', 'Network Path', 'Login User Name', 'Password', and 'Retype Password'.
- 6** points to the 'Remote 2' section, which includes an unchecked checkbox for 'Remote 2' and a radio button for 'Use Administrator Setting'.
- 7** points to the 'File Name' section, which includes a radio button for 'DocYYMMDD(YYMMDD is a date)' and an unchecked checkbox for 'Add the date and time to a file name'.

1) File Format

Select the file format for the scanned file to be stored.

- **TIFF (Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF (Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF (Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF (Single)** — Select this to save scanned images separately as Single-page PDF files.
- **Slim PDF (Multi)** — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. When no optional memory is installed, Slim PDF will not apply for scanning more than Letter or A4 size originals.
- **Slim PDF (Single)** — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image. When no optional memory is installed, Slim PDF will not apply for scanning more than Letter or A4 size originals.
- **XPS (Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS (Single)** — Select this to save scanned images separately as Single-page XPS files.

- **JPEG** — Select this to save scanned images as JPEG files.

Tips

- If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, refer to the **MFP Management Guide**.
- Files saved in an XPS format can be used in Windows Vista/Windows 7/Windows Server 2008 SP1, or Windows XP SP2/Windows Server 2003 SP1 or later versions with Net Framework 3.0 installed.

2) Encryption

Set this for encrypting PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.

Encryption

Select this if you want to encrypt PDF files.

User Password

Enter a password for opening encrypted PDF files.

Master Password

Enter a password for changing the Encrypt PDF setting.

Tips

- If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, refer to the **MFP Management Guide**.
- The user password and the master password are not set at the factory shipment.
- Passwords must be from 1 to 32 one-byte alphanumeric characters.
- The user password must differ from the master password.

Notes

- These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. Ask the administrator for resetting these passwords.
- For the details of the encryption setting, refer to the **MFP Management Guide**.

Encryption Level

Select the desired encryption level.

- **40-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1.
- **128-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4.
- **128-bit AES** — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6.

Authority

Select the desired types of authority for Encrypt PDF.

- **Printing** — Press this to authorize users to print documents.
- **Change of Documents** — Press this to authorize users to change documents.
- **Content Copying or Extraction** — Press this to authorize users to copy and extract the contents of documents.
- **Content Extraction for accessibility** — Press this to enable the accessibility feature.

3) Destination — Use local folder

Select this to save a scanned file to the "FILE_SHARE" folder.

Note

This option cannot be selected when the [Save to USB Media] option is selected.

4) Destination — Save to USB Media

Select this to save a scanned file to the USB media.

Notes

- This option cannot be selected when the [Use local folder] option is selected.
- This equipment has two USB connectors. All connectors can be used to store the data. However, if both USB media are connected, the data will be stored in the first one.
- Storing to the USB media may take some time depending on the number of pages.

5) Destination — Remote 1

Select this check box to save a scanned file to Remote 1. How you can set this item depends on how your administrator configured the Save as file settings.

If Remote 1 does not allow to specify a network folder, you can only select [Use Administrator Settings]. The protocol and the network path are displayed below this item.

If Remote 1 allows to specify a network folder, you can select [Use User Settings] and specify the network folder settings by entering the following items:

Protocol

Select the protocol to be used for uploading a scanned file to the network folder.

- **SMB** — Select this to send a scanned file to the network folder using the SMB protocol.
- **FTP** — Select this to send a scanned file to the FTP server.
- **NetWare IPX/SPX** — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol.
- **NetWare TCP/IP** — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol.

Server Name

When you select [FTP] as the protocol, enter the FTP server name or IP address where a scanned file will be sent.

For example, to send a scanned file to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box. You can specify the directory at the [Network Path] box.

When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).

When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.

Port Number (Command)

Enter the port number to be used for controls if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number.

Network Path

Enter the network path to store a scanned file.

When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”.

When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”.

When you select “NetWare IPX/SPX” or “NetWare TCP/IP” as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “sys\scan”.

Login User Name

Enter the login user name to access an SMB server, FTP server, or NetWare file server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank.

Password

Enter the password to access an SMB server, FTP server, or NetWare file server, if required.

Retype Password

Enter the same password again for a confirmation.

6) Destination — Remote 2

Select this check box to save a scanned file to the Remote 2. How you can set this item depends on how your administrator configured the Save as file settings.

If the Remote 2 does not allow you to specify a network folder, you can only select [Use Administrator Settings]. The protocol and the network path are displayed below this item.

If the Remote 2 allows you to specify a network folder, you can specify the network folder settings. See the description of the Remote 1 option for each item.

7) File Name

Select how the scanned file will be named. Select [DocYYMMDD] to name it as described, or enter the desired file name in the box. When you want to add the date and time in the file name, select the [Add the date and time to a file name] check box.

Box Setting (Private template)

In the Box Setting page, you can specify how scanned images will be stored in the Box.

The screenshot shows the 'Box Setting' form. At the top, there are 'Save' and 'Cancel' buttons. Below them, the form is divided into sections. A vertical line on the left has numbers 1, 2, and 3 pointing to specific fields:

- 1** points to the 'Destination' section, which includes a 'Box Number' dropdown menu (currently showing '000 : Public Box'), a 'Password' text field, and a 'Retype Password' text field.
- 2** points to the 'Folder Name' text field.
- 3** points to the 'Document Name' section, which has two radio button options: 'DocMMDDYY(MMDDYY is a date)' (which is selected) and an empty text field.

1) Destination

Specify the destination box number for e-Filing.

Box Number

Select the Box number where scanned images will be stored.

Password

Enter the password if the specified Box number requires a password.

Retype Password

Enter the password again if the specified Box number requires a password.

2) Folder Name

Enter the name of the folder where scanned images will be stored. If the specified named folder does not exist, the folder will be created automatically.

3) Document Name

Select how the scanned file will be named. Select [DocYYMMDD] to name it as described, or enter the desired file name in the box.

Scan Setting (Private template)

In the Scan Setting page, you can specify how originals are scanned for the Scan to File, Scan to Email, and Scan to e-Filing agent.

For the e-STUDIO4520C Series and the e-STUDIO6530C Series

Scan Setting

1	Preview	OFF ▾
2	Single/2-Sided Scan	Single ▾
3	Rotation	☒ [A] → [A] ☐ [A] → [A] ☐ [V] → [A] ☐ [A] → [A]
4	Color Mode	Black ▾
5	Resolution	600dpi ▾
6	Compression	Middle ▾
7	Original Mode	Text ▾
8	Exposure	☒ Auto ☐ ☐ ☐ ☐ [⊙] ☐ ☐ ☐ ☐
9	Original Size	Auto ▾
10	Background	☐ ☐ ☐ ☒ [⊙] ☐ ☐ ☐ ☐
11	Contrast	☐ ☐ ☐ [⊙] ☐ ☐ ☐
12	Sharpness	☐ ☐ ☐ [⊙] ☒ ☐ ☐
13	Saturation	☐ ☐ [⊙] ☐ ☐
14	RGB Adjustment	Red: ☐ ☐ [⊙] ☐ ☐
		Green: ☐ ☐ [⊙] ☐ ☐
		Blue: ☐ ☐ [⊙] ☐ ☐
15	Omit Blank Page	OFF ▾
16	Outside Erase	☒ OFF ☐ ☐ [⊙] ☐ ☐

For the e-STUDIO455 Series

[illegible]

For the e-STUDIO855 Series

1) Preview

Select whether to display the scanned image on the control panel after the scanning an original.

- **OFF** — Select this not to display the scanned image.
- **ON** — Select this to display the scanned image.

Tip

This setting is available only for e-STUDIO4520C and e-STUDIO6530C Series.

2) Single/2-Sided Scan

Select whether to scan one side or both sides an original.

- **Single** — Select this to scan one side of an original.
- **Duplex Book** — Select this to scan both sides of originals when the pages are printed vertically in the same direction and bound along the vertical side of the paper.
- **Duplex Tablet** — Select this to scan both sides of originals with a vertical reversal to be bound along the horizontal side of the paper.

3) Rotation

Select how the scanned images will be rotated.

4) Color Mode

Select the color mode for scanning.

- **Black** — Select this to scan in black mode.
- **Gray** — Select this to scan in gray scale mode.
- **Full Color** — Select this to scan in full color mode.
- **Auto Color** — Select this to scan in auto color mode.

Notes

- The [Color Mode] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting.
- When [Auto Color] is selected, you cannot select JPEG or TIFF (Multi) for the file format. Also when [Black] is selected, JPEG is not allowed.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

5) Resolution

Select the resolution for scanning.

Note

The [Resolution] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting.

6) Compression

Select the compression for scanning.

Notes

- This cannot be set when [Black] is selected at the [Color Mode] box.
- The [Compression] option cannot be set when [Slim PDF (Multi)] or [Slim PDF (Single)] is selected in the [File Format] option in the Save as File Settings and that in the Email Setting.

7) Original Mode

Select the document type of the originals.

- **Text** — Select this to set the Text mode as the default original mode.
- **Text/Photo** — Select this to set the Text/Photo mode as the default original mode. This can be selected only when [Black] is selected in the [Color Mode] box.
- **Photo** — Select this to set the Photo mode as the default original mode.
- **Printed Image** — Select this to set the Printed Image mode as the default original mode. This can be selected only when [Full Color] or [Auto Color] is selected in the [Color Mode] box.

Note

This cannot be set when [Gray] is selected in the [Color Mode] box.

8) Exposure

Select the exposure for scanning.

Select [Auto] to automatically apply the ideal contrast according to the original, or adjust the contrast manually in 11 stages. The farther to the right that you set the value, the darker the density of the scanned image will become.

Note

[Auto] is not available when [Gray], [Full Color], or [Auto Color] is selected at the [Color Mode] box. In that case, set the exposure manually.

9) Original Size

Select the original size.

Select [Auto] to automatically detect the original paper size, [Mixed Original Sizes] to allow scanning mixed original sizes, or a desired paper size.

10) Background

Select the density level of the background of the scanned image. Density can be adjusted in 9 levels. The farther to the right that you set the value, the darker the density of the background will become.

11) Contrast

Select the contrast level of the scanned image. Contrast can be adjusted in 9 levels. The farther to the right that you set the value, the higher the contrast level will become.

Note

This is not available when [Black] or [Gray] is selected at the [Color Mode] box.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

12) Sharpness

Select the sharpness level of the scanned image. Sharpness can be adjusted in 9 levels. The farther to the right that you set the value, the sharper the scanned image will become.

13) Saturation

Select the saturation level of the scanned image. Saturation can be adjusted in 7 levels. The farther to the right you set the value, the more vivid the scanned image will become.

Note

This is not available when [Black] or [Gray] is selected at the [Color Mode] box.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

14) RGB Adjustment

Select the RGB density level of the scanned image. RGB density can be adjusted in 9 levels for each color. The farther to the right you set the value, the darker the density of the selected color will become.

Note

This is not available when [Black] or [Gray] is selected at the [Color Mode] box.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

15) Omit Blank Page

Select whether to automatically omit a blank page in the scanned image if it is included in originals.

- **OFF** — The blank page is not omitted.
- **ON** — The blank page is omitted.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

16) Outside Erase

Select whether to erase a shade that appears outside of the scanned image when an original is placed on the original glass while the Original Cover (optional) is left open. The erased shade will be whitened.

If you want to erase it, you can select the criteria in 7 levels for judging if it is an area to be erased. The farther to the right you select, the larger the area that will be erased. [OFF] is selected by default.

Tip

This setting is available only for the e-STUDIO455 Series, e-STUDIO4520C and e-STUDIO6530C Series.

□ Setting template password

Users can set the password to the private template.

To set the template password, you must register the private template first.

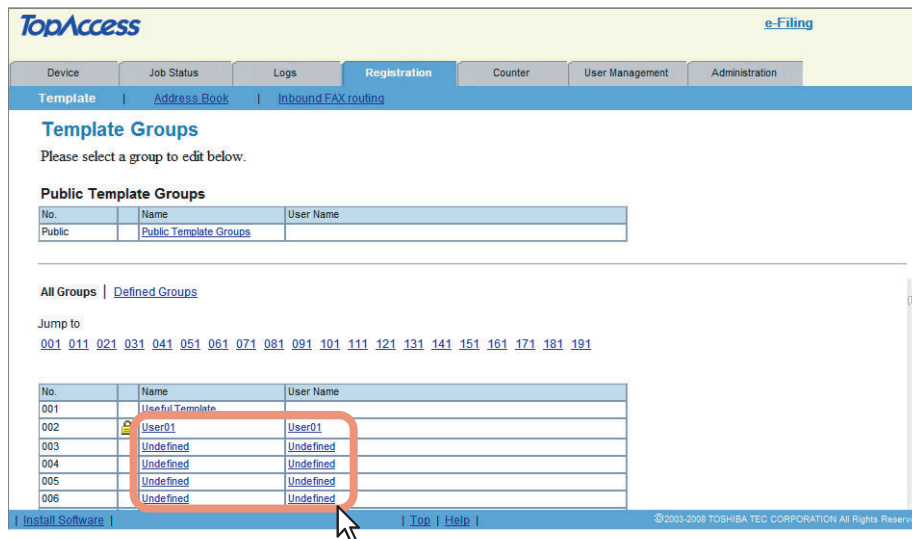
Setting the template password**1 Click the [Registration] tab and the [Template] menu.**

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the group name link that contains the private template that you want to edit.

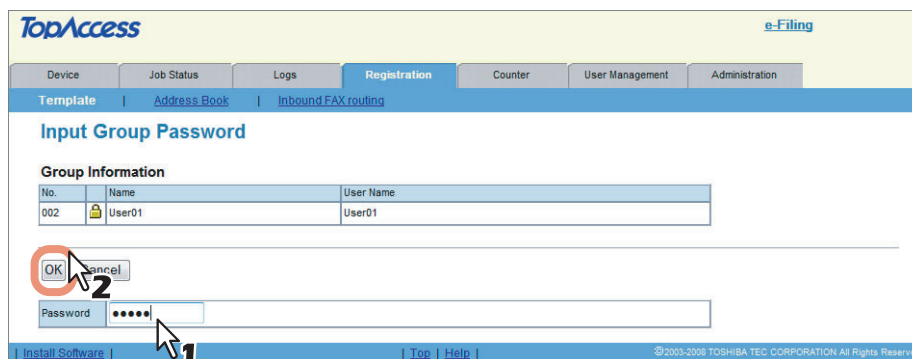


If the selected private template group is protected by a password, the Input Group Password page is displayed. If not, the Group Information page is displayed.

Tips

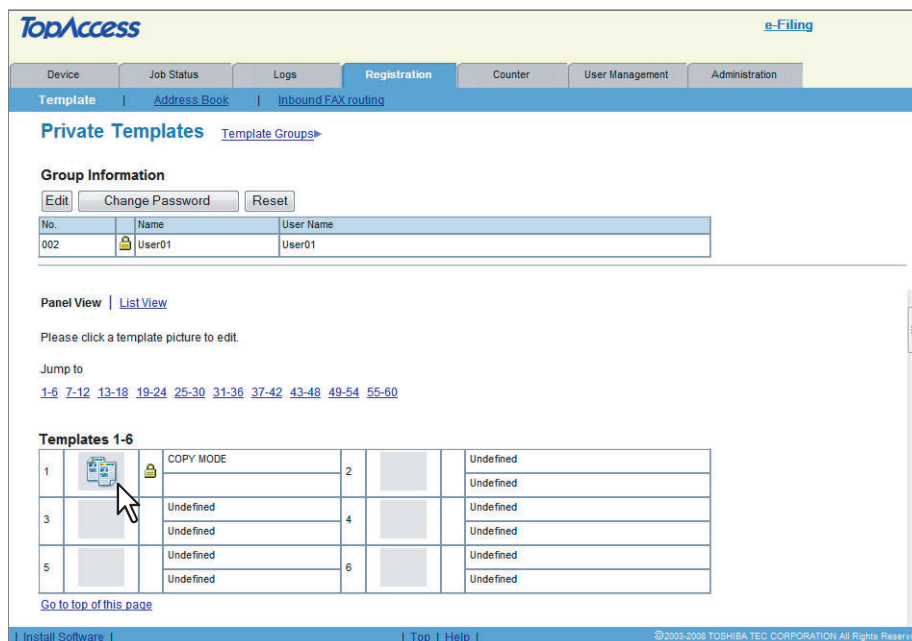
- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups as a default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

3 When the Input Group Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template group and click [OK].



The Group Information page is displayed.

4 From the template list, click the template icon that you want to set or change the password.

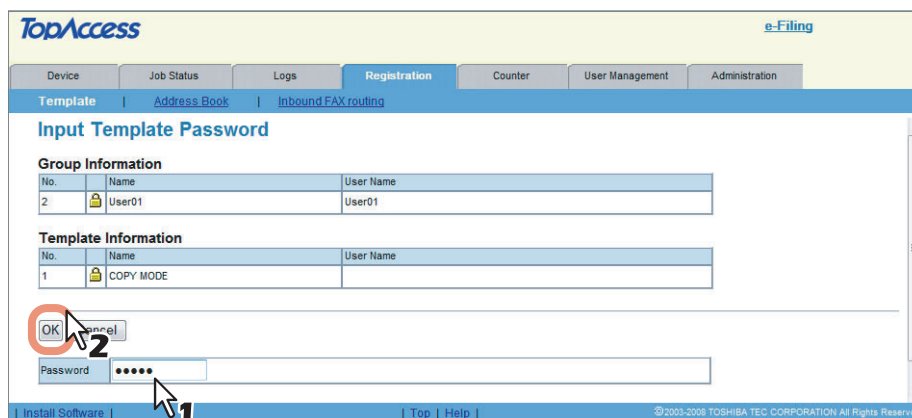


- If the template list is displayed in the List view, click the template name that you want to set or modify the password.
- If the selected private template is protected by a password, the Input Template Password page is displayed. If not, the Template Information page is displayed.

Tips

- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which private template you want to define or edit, click the number of the private template in the [Jump to] links.

5 When the Input Template Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template and click [OK].



The Template Information page is displayed.

6 Click [Change Password] to set the password for the private template.

The screenshot shows the 'Template Properties' page in the TopAccess application. The 'Registration' tab is selected. Under 'Template Groups', 'Private Templates' is chosen. The 'Group Information' table shows a group named 'User01'. The 'Template Information' table shows a template named 'COPY MODE'. Below these tables, there are buttons for 'Edit', 'Change Password', and 'Reset Template'. The 'Change Password' button is highlighted with a mouse cursor. The bottom of the page shows a status bar with 'Install Software', 'Top', 'Help', and a copyright notice for Toshiba TEC Corporation.

The Change Template Password page is displayed.

7 Enter the old password in the [Old Password] box, and the new password in the [New Password] and [Retype Password] boxes.

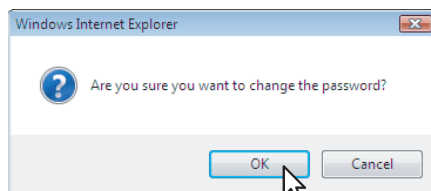
The screenshot shows the 'Change Template Password' page in the TopAccess application. The 'Group Information' and 'Template Information' tables are visible. Below them are 'Save' and 'Cancel' buttons. The 'Old Password', 'New Password', and 'Retype Password' fields are highlighted with a red box, and a mouse cursor is pointing at the 'Retype Password' field. The bottom of the page shows a status bar with 'Install Software', 'Top', 'Help', and a copyright notice for Toshiba TEC Corporation.

- You can only use 5-digit numbers for the password.
- You can also enter the administrator password in the [Old Password] box.
- If the password has not been set for the template, leave the [Old Password] box blank.
- Leaving the [New Password] and [Retype Password] box blank releases the password protect for the template.

8 Click [Save].

The confirmation dialog box appears.

9 Click [OK].



The password is set or modified.

❑ Resetting private templates

Users can reset the private template.

Resetting the private template

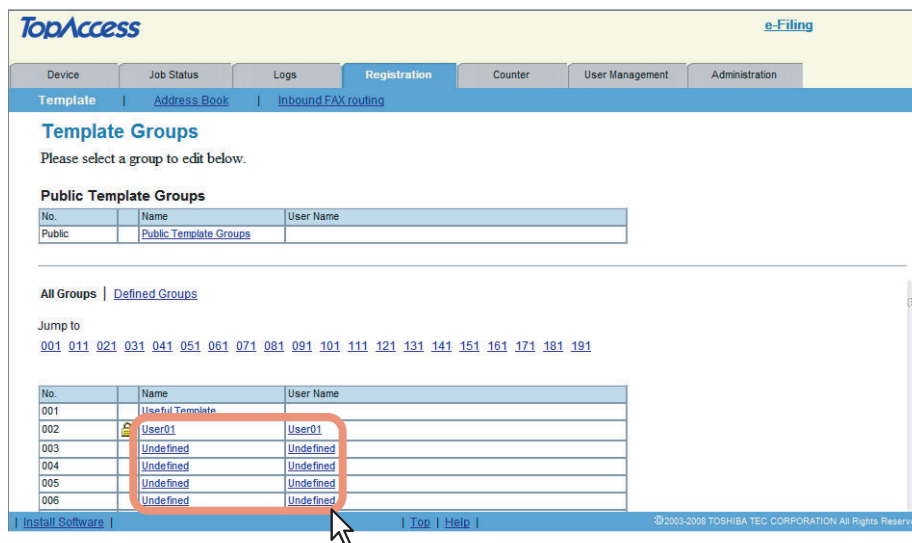
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the group name link that contains the private template that you want to reset.

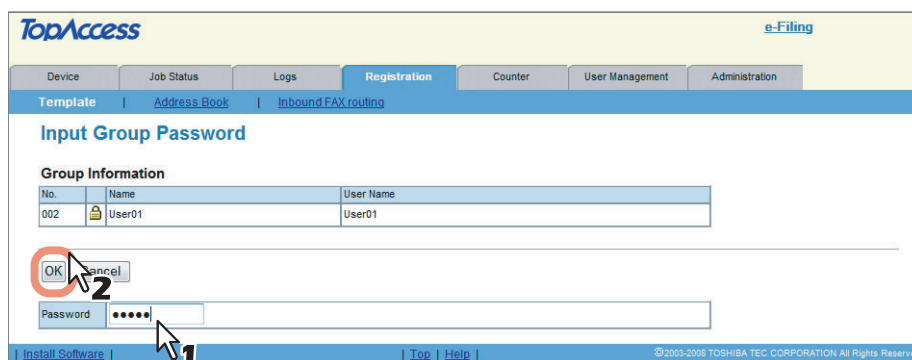


- If you select the private template group that is not protected by a password, the Private Templates page is displayed. Skip to step 4.
- If you select the private template group that is protected by a password, the Input Group Password page is displayed. Go to the next step.

Tips

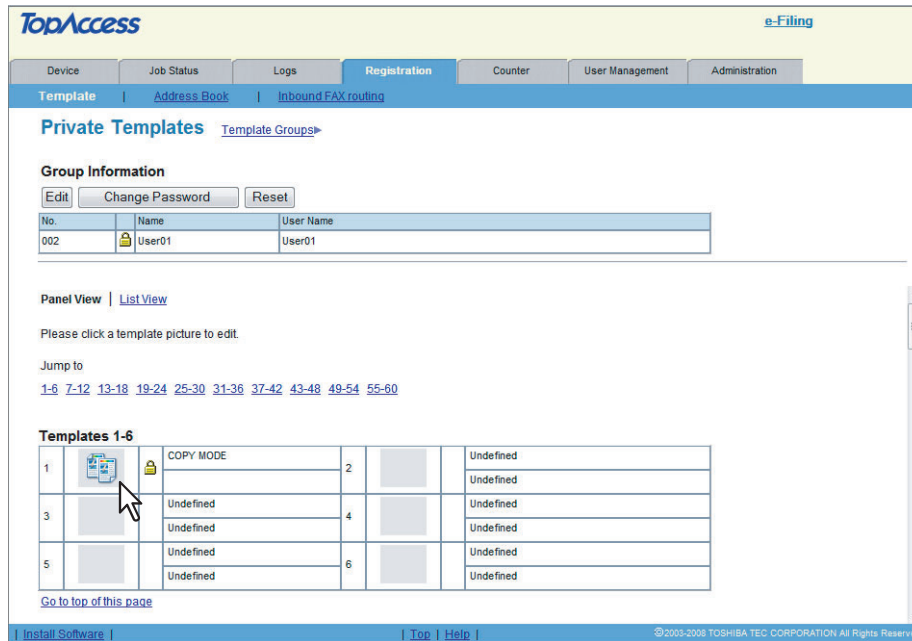
- You can display only defined private template groups by clicking on the [Defined Groups] link. The page displays all 200 private template groups as a default page view.
- If you know which private template group you want to define or edit, click the number of the private template group in the [Jump to] links.

3 When the Input Group Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template group and click [OK].



The Private Templates page is displayed.

4 From the templates list, click the template icon that you want to reset.

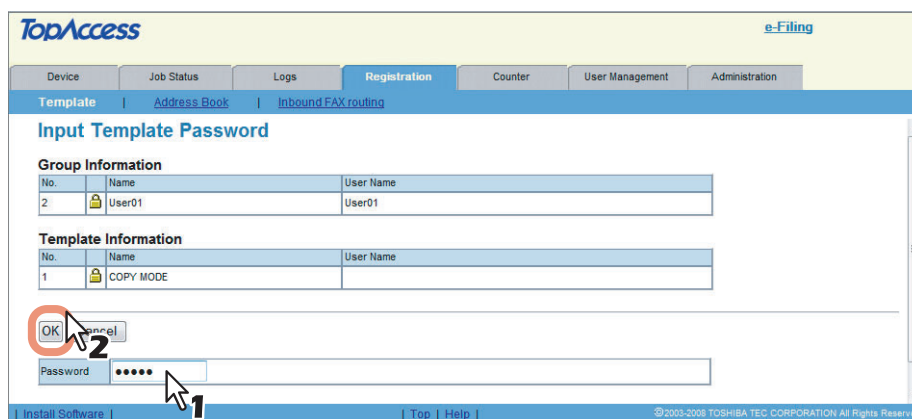


- If the templates list is displayed in the List view, click the template name that you want to reset.
- If you select the private template that is not protected by a password, the Template Properties page is displayed. Skip to step 6.
- If you select the private template that is protected by a password, the Input Template Password page is displayed. Go to the next step.

Tips

- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which private template you want to reset, click the number of the private template in the [Jump to] links.

5 When the Input Template Password page is displayed, enter the 5-digit password (or administrator's password) for the selected private template and click [OK].



The Template Properties page is displayed.

6 Click [Reset Template].

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Template Properties Template Groups» Private Templates»

Group Information

No.	Name	User Name
2	User01	User01

Template Information

No.	Name	User Name
1	COPY MODE	

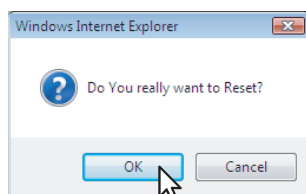
Edit | Change Password | **Reset Template**

Panel		COPY MODE
Notification		
Automatic Start	Disable	
Agent	Copy	
Scanner		

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The confirmation dialog box appears.

7 Click [OK].



The selected template is reset.

■ Displaying public templates

End users can also display the templates list in the public group so that users can see what templates are available.

Displaying templates in the public group

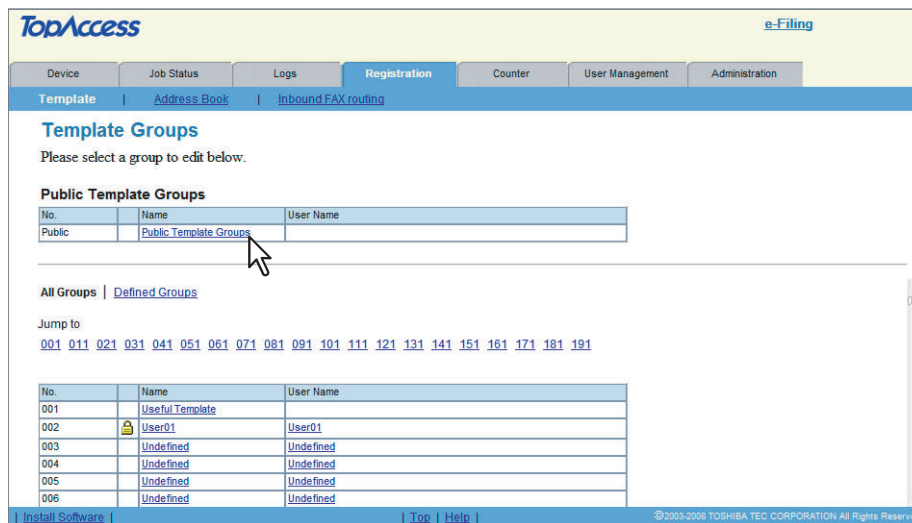
1 Click the [Registration] tab and the [Template] menu.

The Template Groups page is displayed.

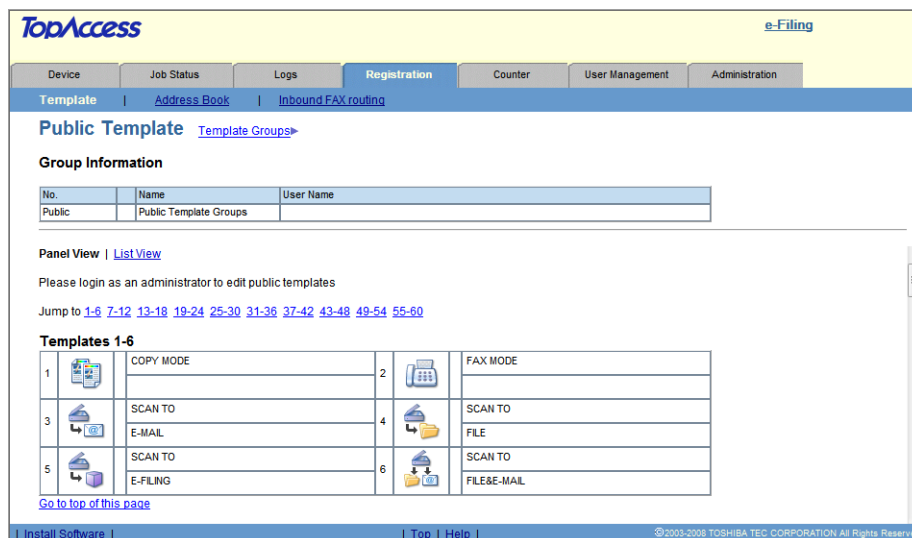
Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the group name link for the Public Template Groups list.



3 The templates list in the public group is displayed.



Tips

- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which public template you want to view, click the number of the public template in the [Jump to] links.

Managing Address Book

This equipment comes with the Address Book feature that enables users to manage who receives Scan to Email, Internet Fax transmission, and fax transmission.

In the [Address Book] menu at the [Registration] tab in TopAccess, you can add, edit, and delete recipient information. You can also create groups to which multiple contacts can be assigned.

📖 P.78 “Managing contacts in the Address Book”

📖 P.83 “Managing groups in the Address Book”

Tip

Address Book can be also managed using the touch panel. Refer to the *MFP Management Guide*.

■ Managing contacts in the Address Book

There are two ways to manage contacts in the Address Book:

- Add, edit, or delete a contact manually.
📖 P.78 “Adding, editing, or deleting contacts manually”
- Add new contact searching for a recipient from the LDAP server.
📖 P.82 “Adding new contact from the LDAP server”

□ Adding, editing, or deleting contacts manually

You can add or edit a contact by entering recipient information manually. You can also delete the contact from the Address Book.

📖 P.78 “Adding or editing a contact”

📖 P.81 “Deleting a contact”

Adding or editing a contact

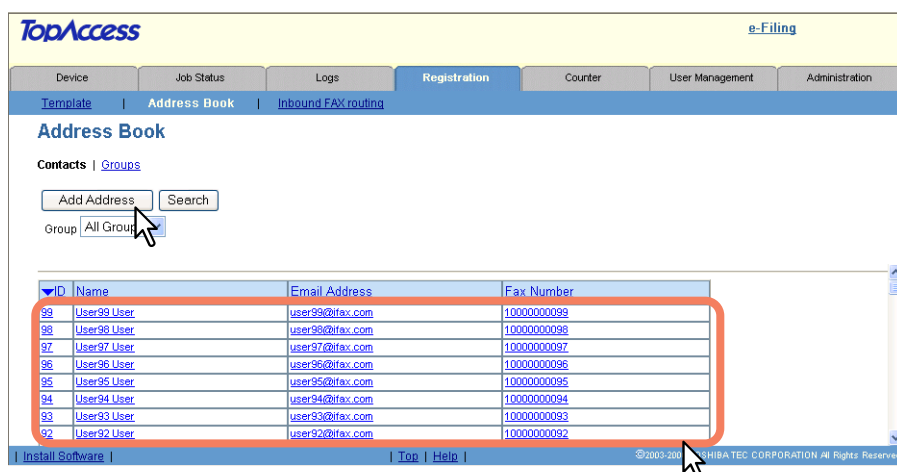
1 Click the [Registration] tab and the [Address Book] menu.

The Address Book page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click [Add Address] to add a new contact, or click the contact link that you want to edit in the contacts list.



The Contact Property page is displayed.

3 Enter the following items to specify the recipient information.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Template Address Book Inbound FAX routing

Contact Property Address Book >

Save Cancel Reset Delete

Fax Setting

*Either
**Either

*First Name	User100
*Last Name	User
**Email Address	user100@fax.com
**Fax Number	10000000100
2nd Fax Number	20000000100
Company	12345 COMPANY
Department	Dept11
Keyword	

Install Software | Top | Help | ©2003 SHIBATEC CORPORATION All Rights Reserved

First Name — Enter the first name of the recipient. You can enter up to 32 characters.

Last Name — Enter the last name of the recipient. You can enter up to 32 characters.

Email Address — Enter the email address of the recipient. You can enter up to 192 characters.

Fax Number — Enter the fax number of the recipient. You can enter up to 128 characters.

2nd Fax Number — Enter the 2nd fax number of the recipient. You can enter up to 128 characters.

Company — Enter the company name of the recipient. You can enter up to 64 characters.

Department — Enter the department name of the recipient. You can enter up to 64 characters.

Keyword — Enter the comment of the recipient. You can enter up to 256 characters.

Notes

- You must specify either the [First Name] or [Last Name] box and either the [Email Address] or [Fax Number] box to register the contact.
- You cannot send originals to the fax numbers without the optional Fax Unit even if you set up the contact for which the fax number is specified.
- If you enter “-” in the [Fax Number] and [2nd Fax Number], a three-second pause is added for dialing the fax number.

Tips

- You can clear the entered values in each box by clicking [Reset].
- You can cancel adding or editing a contact by clicking [Cancel].

4 If you are registering a fax recipient, click [Fax Setting]. Otherwise, skip to Step 6.

The Fax Settings page is displayed.

5 Enter the following items according to the capabilities of recipient facsimile, and click [Save].

The screenshot shows the 'Fax Setting' page in the TopAccess web interface. The page has a navigation bar with tabs: Device, Job Status, Logs, Registration, Counter, User Management, and Administration. Below the navigation bar, there are links for Template, Address Book, and Inbound FAX routing. The main content area is titled 'Fax Setting' and includes a 'Save' button and a 'Reset' button. A red box highlights the form fields, and a mouse cursor points to the Save button. A large number '2' is overlaid on the Save button.

SUB	100
SID	...
SEP	
PWD	
ECM	ON
Line Select	Line1
Quality Transmit	ON
Transmission Type	Memory Transmit

SUB — Enter the mailbox number if you want to send originals to the mailbox in the recipient facsimile. You can enter up to 20 characters including numbers and hyphenations (-), #, *.

SID — Enter the password to input a fax into the mailbox in the recipient facsimile. You can enter up to 20 characters including numbers and hyphenations (-), #, *.

SEP — Enter the mailbox number if you want to retrieve a document from the mailbox in the recipient facsimile. You can enter up to 20 characters including numbers and hyphenations (-), #, *.

PWD — Enter the password to retrieve a document from the mailbox in the recipient facsimile. You can enter up to 20 characters including numbers and hyphenations (-), #, *.

ECM — Enable or disable the ECM (Error Correction Mode). If enabled, it facilitates error free communications by automatically resending any portion of the document affected by phone line noise or distortion.

Line Select — Select the line to be used. If this is set to [Auto], this equipment automatically selects the line to be used. However, [Line 2] can be applicable only when the 2nd Line for Fax Unit is installed.

Quality Transmit — Select if you want to send documents in the Quality TX mode. This feature sends documents at a slower speed than normal so that the transmission will be less affected by line condition.

Transmission Type — Select whether the document will be sent in the Memory TX mode or Direct TX mode.

Tip

If you want to clear the fax settings of the contact, click [Reset].

6 In the Contact Property page, click [Save] to add a new contact.

The screenshot shows the 'Contact Property' page in the TopAccess web interface. The page has a navigation bar with tabs: Device, Job Status, Logs, Registration, Counter, User Management, and Administration. Below the navigation bar, there are links for Template, Address Book, and Inbound FAX routing. The main content area is titled 'Contact Property' and includes a 'Save' button, a 'Cancel' button, a 'Reset' button, and a 'Delete' button. A mouse cursor points to the Save button.

*First Name	User100
*Last Name	User
**Email Address	user100@ifax.com
**Fax Number	10000000100
2nd Fax Number	20000000100
Company	12345 COMPANY
Department	Dept11
Keyword	

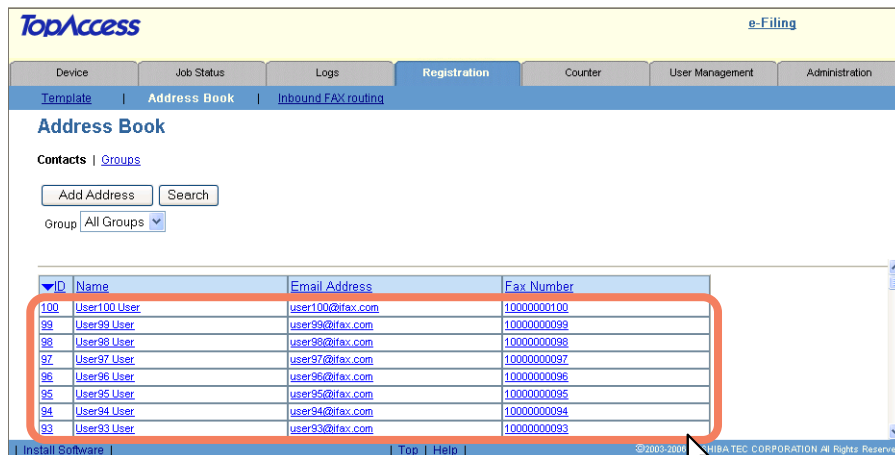
Deleting a contact

- 1 Click the **[Registration]** tab and the **[Address Book]** menu.
The Address Book page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed.
When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

- 2 Click the link that you want to delete in the contacts list.



The Contact Property page is displayed.

- 3 Click **[Delete]**.

Save Cancel Reset **Delete**

Fax Setting

*Either
**Either

*First Name	User100
*Last Name	User
**Email Address	user100@tifax.com
**Fax Number	10000000100
2nd Fax Number	20000000100
Company	12345 COMPANY
Department	Dept11
Keyword	

The contact is deleted from the Address Book.

❑ Adding new contact from the LDAP server

You can search for contacts in the LDAP server and add them to the Address Book. To use the LDAP search feature, the administrator must configure the directory service. Before operating the LDAP search, ask your administrator if the Directory Service has been configured.

Adding new contact from the LDAP server

1 Click the [Registration] tab and the [Address Book] menu.

The Address Book page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click [Search].

ID	Name	Email Address	Fax Number
99	User99 User	user99@tfx.com	10000000099
98	User98 User	user98@tfx.com	10000000098
97	User97 User	user97@tfx.com	10000000097
96	User96 User	user96@tfx.com	10000000096
95	User95 User	user95@tfx.com	10000000095
94	User94 User	user94@tfx.com	10000000094
93	User93 User	user93@tfx.com	10000000093
92	User92 User	user92@tfx.com	10000000092

The Search Contact page is displayed.

3 Select the directory service name that you want to search for in the [Directory Service Name] box, and enter the search terms in the boxes that you want to search.

Tips

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

4 Click [Search].

TopAccess will start searching for recipients in the LDAP server and the Search Address List page will display the results.

5 Select the check boxes of contacts that you want to add to the Address Book.

Search Address List

Add Cancel

☒	Name	company	department	Email Address	Fax Number
☒	User09 User	abcdef	ghijklmn	user09@fax.com	444-4444-4444

[Go to top of this page](#)

You can select all users in the list by clicking on the ☒ button.

Note

The value of [company] and [department] will depend on the settings determined by the administrator.

6 Click [Add].

Selected contacts are added to the Address Book.

Managing groups in the Address Book

You can create groups that contain the multiple recipients. This enables you to specify the groups for the destinations instead of specifying each recipient separately when operating Scan to Email, or fax or Internet Fax transmission. You can also delete groups.

P.83 "Adding or editing a group"

P.85 "Deleting a group"

Adding or editing a group

1 Click the [Registration] tab and the [Address Book] menu.

The Address Book page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the [Groups] submenu.

The Group Lists is displayed.

3 Click [New] to add a new group, or click the group link that you want to edit in the groups list.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Template Address Book Inbound FAX routing

Address Book

Contacts Groups

New

ID	Group Name	Contacts
12	Group12	4
11	Group11	12
10	Group10	8
9	Group09	8
8	Group08	8
7	Group07	8
6	Group06	8
5	Group05	8
4	Group04	8
3	Group03	8

Instant.com Top Help ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Group Properties page is displayed.

4 Enter the group name in the corresponding space.

TopAccess e-Filing

Device | Job Status | Logs | **Registration** | Counter | User Management | Administration

Template | Address Book | Inbound FAX routing

Group Properties [Address Book ▶](#)

OK Cancel Reset Delete

*Required
*Group Name

ID	Email	Fax	Name	Email Address	Fax Number
99	☒	☒	User99 User	user99@fax.com	10000000099
98	☒	☒	User98 User	user98@fax.com	10000000098
97	☒	☒	User97 User	user97@fax.com	10000000097
96	☒	☒	User96 User	user96@fax.com	10000000096
95	☒	☒	User95 User	user95@fax.com	10000000095
94	☐	☐	User94 User	user94@fax.com	10000000094

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

Group Name — Enter the group name.

Tips

- You can clear the entered values in each field by clicking [Reset].
- You can cancel adding or editing a group by clicking [Cancel].

5 Select the [Email] check boxes of users to add Internet Fax recipients, and select the [Fax] check boxes of users to add Fax recipients.

Note

To perform the fax transmission, the optional Fax Unit is required. If the optional Fax Unit is not installed, you cannot perform the fax transmission even if you specify the fax number.

6 Click [OK].

The group is created.

Deleting a group

1 Click the [Registration] tab and the [Address Book] menu.

The Address Book page is displayed.

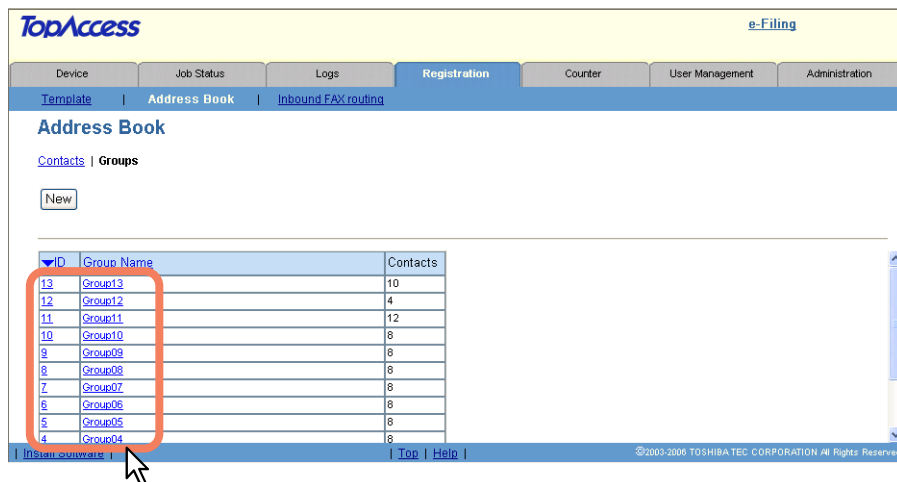
Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the [Groups] submenu.

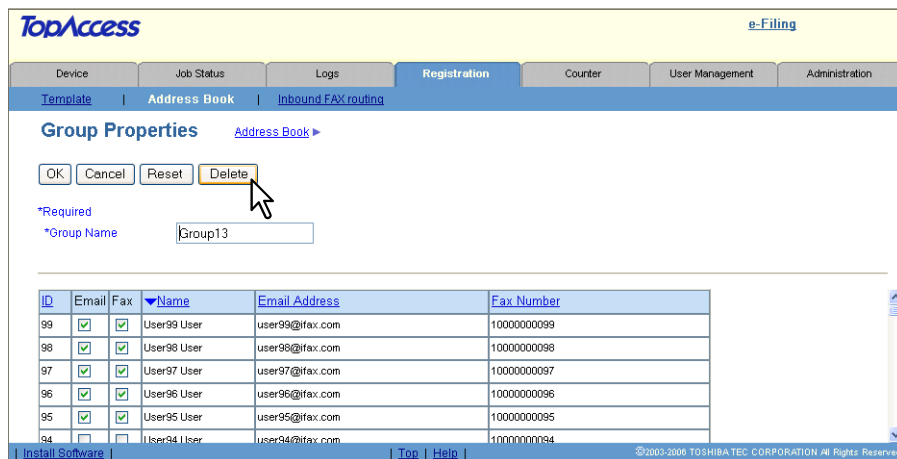
The groups list is displayed.

3 Click the group link that you want to delete in the groups list.



The Group Properties page is displayed.

4 Click [Delete].



The selected group is deleted.

Managing Mailboxes

Note

Mailboxes can be managed only when the optional Fax Unit is installed.

Tip

Mailboxes can be managed using the touch panel. Refer to the ***GD-1250/GD-1260/GD-1270 Operator's Manual for FAX Unit***.

This equipment supports the ITU-T compatible mailboxes that allow storage and retrieval of documents via mailboxes that are already set up in a mailbox hub.

The following three types of Mailboxes are available:

Confidential mailbox

The Confidential Box allows a one-time document retrieval from the mailbox. Once a document is retrieved, it is cleared. If a new document is sent to the same box number where another document is stored, it is added to the existing box. You can also set up a password requirement for accessing the Confidential Box for document retrieval to prevent unauthorized retrieval of documents.

Bulletin Board mailbox

The Bulletin Board Box allows multiple document retrievals from the same mailbox. Once a document is retrieved, it is not cleared. If a new document is sent to the same Box, it replaces the existing one. You can set up a password requirement for accessing the Bulletin Board Box for document reservation.

Forward mailbox

The Forward mailbox allows you to transmit a received fax to various destinations, using the following agents:

- **Internet/Fax (Relay) agent** — When a document has been sent to a mailbox, this equipment can call up the remote Fax via the public switched telephone line, or send the Internet Fax via the Internet according to the destinations registered in the mailbox. After the relay transmission, the transmission result list will be sent to a specified remote Fax. It is also possible to set up a password requirement.
- **Save as file agent** — The received faxes in this mailbox are forwarded to the local folder in this equipment or network folders.
- **Email agent** — The received faxes in this mailbox are forwarded to the email addresses recipients specified in the mailbox.
- **Store to e-Filing agent** — The received faxes in this mailbox are forwarded to the Box in this equipment. The data stored in the Box can be printed later, and also can be managed using the e-Filing web utility, which is a web-based utility that allows you to display, print, and merge the files in the Box.

Note

Sending and storage of documents to a mailbox hub and retrieval of documents from a mailbox hub are possible only on an ITU-T compliant facsimile. Only ITU-T compliant facsimiles can be used as Mailbox hubs. This equipment is provided with mailbox hub functions.

Using TopAccess, you can set up, edit, and delete mailboxes on this equipment.

📖 P.87 "Setting up an Open Mailbox"

📖 P.93 "Deleting an Open Mailbox"

■ Setting up an Open Mailbox

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

Setting up or editing a mailbox

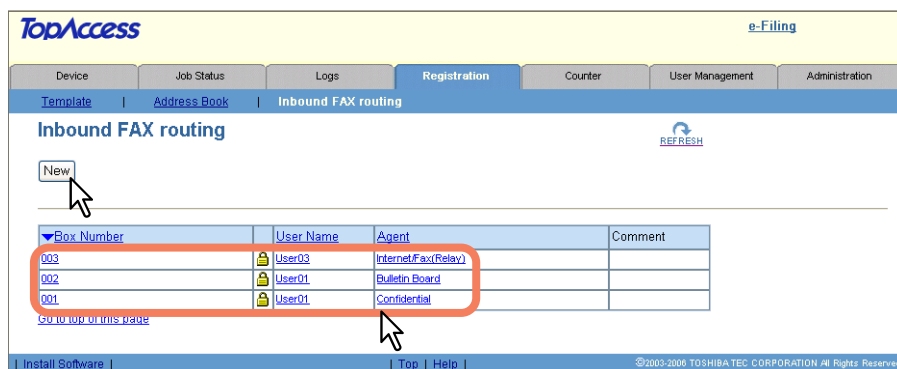
1 Click the [Registration] tab and the [Inbound FAX routing] menu.

The Inbound FAX routing page is displayed.

Note

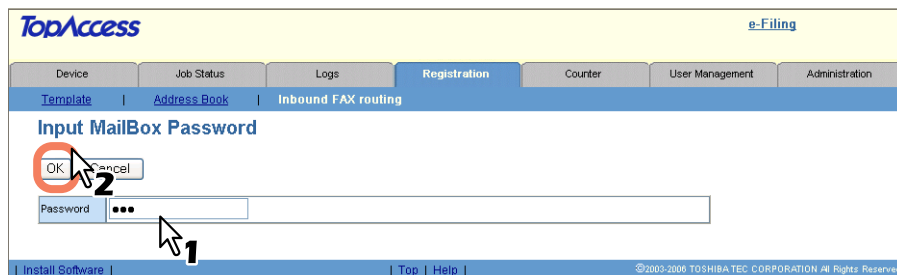
When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click [New] to set up a new mailbox, or click the box number link that you want to edit in the mailboxes list.

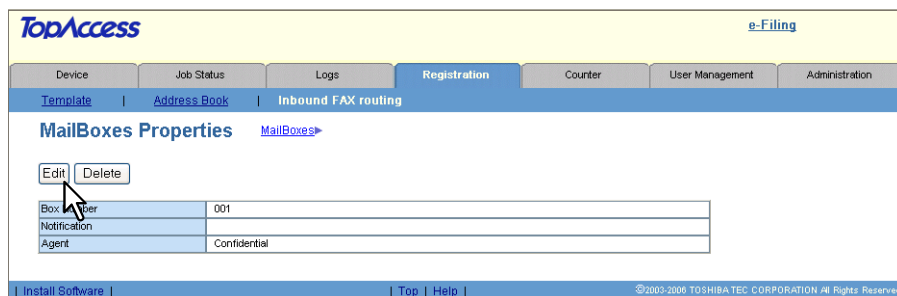


- If you click [New], skip to step 5.
- If you click the box number link that is not protected by a password, skip to step 4.
- If you click the box number link that is protected by a password, go to the next step.

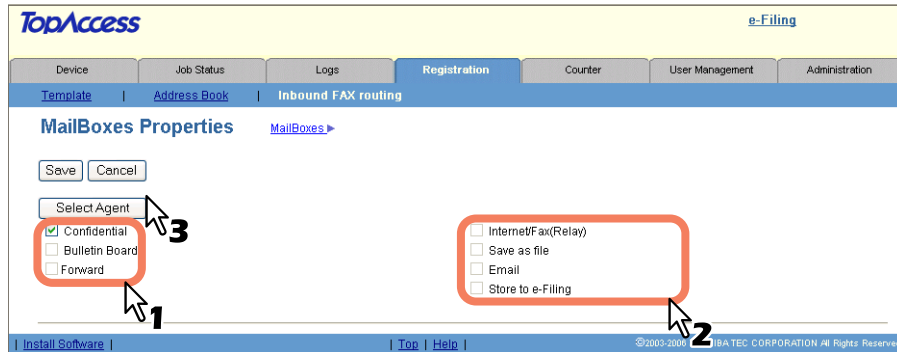
3 Enter a 5-digit password for the mailbox (or administrator's password) and click [OK].



4 Click [Edit].



5 Select agents and click [Select Agent].



Confidential — Select this to create a Confidential mailbox.

Bulletin Board — Select this to create a Bulletin Board mailbox.

Forward — Select this to create a relay station mailbox. When you select this, select the agent from [Internet/Fax(Relay)], [Save as file], [Email], or [Store to e-Filing].

- **Internet/Fax(Relay)** — Select this to create a Forward mailbox of Internet/Fax (Relay) agent. This agent can be combined with the Save as file or Store to e-Filing agent.
- **Save as file** — Select this to create a Forward mailbox of the Save as file agent. This agent can be combined with the Internet/Fax(Relay), Email, or Store to e-Filing agent.
- **Email** — Select this to create a Forward mailbox of the Email agent. This agent can be combined with the Save as file agent or Store to e-Filing agent.
- **Store to e-Filing** — Select this to create a Forward mailbox of the Store to e-Filing agent. This agent can be combined with the Internet/Fax(Relay) agent, Save as file agent, or Email agent.

6 Click each button displayed in the page to set the template properties.

[MailBox Setting] — Click this to specify the mailbox settings.

P.90 “MailBox Setting”

MailBox Setting	
Box Number	001
User Name	User01
Comment	
Notification	
Document Print	Always

[Destination Setting] — Click this to specify the destinations to be sent. This can be set only when creating an Internet/Fax(Relay) agent or Email agent.

P.91 “Destination Setting (Mailbox)”

When Creating an Internet/Fax(Relay) agent:

Destination Setting	
Destination	

When Creating an Email agent:

To: Destination Setting	
To: Destination	

Cc: Destination Setting	
Cc: Destination	

Tip

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

P.184 “Setting up Email Setting”

To: Destination Setting	
To: Destination	

Bcc: Destination Setting	
Bcc: Destination	

[InternetFax Setting] — Click this to specify how the document will be sent. This can be set only when creating an Internet/Fax(Relay) agent.

P.91 “InternetFax Setting (Mailbox)”

InternetFax Setting	
Subject	Scanned from (Device Name)(Template Name)(Date)(Time)
From Address	admin@fax.com
From Name	admin
Body	
File Format	TIFF-S
Fragment Page Size	No Fragmentation

[Relay End Terminal Report] — Click this to specify where the transmission result list will be sent. This can be set only when creating an Internet/Fax(Relay) agent.

P.92 “Relay End Terminal Report”

Relay End Terminal Report	
Relay End Terminal Report	

[Email Setting] — Click this to specify how the document will be sent. This can be set only when creating an Email agent.

P.92 “Email Setting (Mailbox)”

Email Setting	
Subject	Scanned from (Device Name)(Template Name)(Date)(Time)
From Address	mfp-00c67861@fax.com
From Name	MFP-00C67861
Body	
File Format	PDF(Multi)
File Name	(Sender)-NNN (NNN is a sequential number)
Fragment Message Size	No Fragmentation

[Save as file Setting] — Click this to specify how the document will be stored in the local hard disk or network folder. This can be set only when creating a Save as file agent.

P.92 “Save as file Setting (Mailbox)”

Save as file Setting	
Format	TIFF(Multi)
Destination	\\MFP-04998820\\FILE_SHARE\\
File Name	(Sender)-NNN (NNN is a sequential number)

[Box Setting] — Click this to specify how the document will be stored in the Box. This can be set only when creating a Store to e-Filing agent.

 P.92 “Box Setting (Mailbox)”

Box Setting	
Destination	000
Folder Name	
Document Name	(Sender)-NNNN (NNNN is a sequential number)

7 After configuring the desired mailbox properties, click [Save].

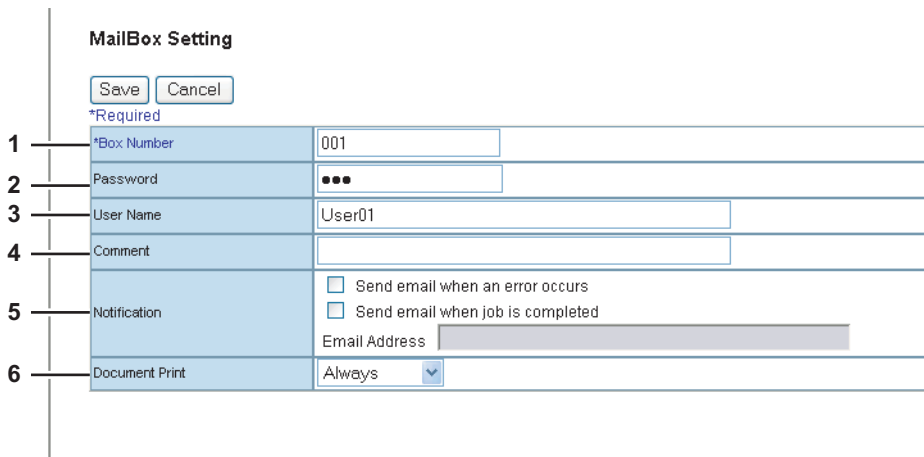
The mailbox properties are registered.

□ MailBox Setting

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

Notes

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



MailBox Setting

Save Cancel

*Required

- 1 Box Number: 001
- 2 Password: ●●●
- 3 User Name: User01
- 4 Comment:
- 5 Notification:
 - ☐ Send email when an error occurs
 - ☐ Send email when job is completed
 - Email Address:
- 6 Document Print: Always

1) Box Number

Enter the box number of the mailbox. You can enter up to 20 characters including numbers, sharp marks (#), and asterisks (*).

You can also specify the sender's fax number to enable the Inbound Fax Routing when registering a Forward mailbox. If you specify the sender's fax number here, the faxes that are received from the specified fax number will be routed according to the mailbox settings.

Notes

- The Inbound Fax Routing is available only for a Forward mailbox. If you select [Confidential] or [Bulletin Board] as an agent, you cannot specify the fax number.
- When a fax is sent from the specified fax number with a box number (or sub address), the Inbound Fax Routing will not apply to the transmission and it is processed according to the specified box number (or sub address) settings.

2) Password

Enter the box password if you want to protect the mailbox by the password. You can enter up to 20 characters including numbers, sharp marks (#), and asterisks (*).

3) User Name

Enter the user name of this mailbox. You can enter up to 30 characters.

4) Comment

Enter the comment. You can enter up to 64 characters.

5) Notification

This specifies how the notification message will be sent if an error occurs.

Send email when an error occurs

Select this to send a notification message to the specified email address if an error occurs.

Send email when job is completed

Select this to send a notification message to the specified email address when a job is completed.

Email Address

Enter an email address to which the notification message will be sent.

Note

When you enable the Notification setting, make sure to set up the Email settings in the [Email] submenu of the [Setup] menu in the TopAccess Administrator's mode. For instructions on how to set up the Email settings, see the following section.

 P.183 "Setting up Email settings"

5**6) Document Print**

Select whether to print a document sent to this mailbox.

□ Destination Setting (Mailbox)

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

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

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

You can specify the recipients by entering their email addresses or fax numbers manually, selecting recipients from the address book, selecting recipient groups from the address book, or searching for recipients in the LDAP server.

Note

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

The instructions on how to setting up the destination setting for the mailbox is same as setting up the destination setting for the private template.

 P.52 "Destination Setting (Private template)"

□ InternetFax Setting (Mailbox)

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

The instructions on how to setting up the Internet Fax settings for the mailbox is same as setting up the Internet Fax settings for the private template.

 P.58 "InternetFax Setting (Private template)"

□ Relay End Terminal Report

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

Adding the relay end terminal report recipients

1 Click [Relay End Terminal Report].

The Relay End Terminal Report page is displayed.

2 Enter the fax number or Email address, or select an Email or Fax option button of a user to whom you want to send the transmission result list.

Relay End Terminal Report

Add Cancel Reset

2

Email	Fax	ID	Name	Email Address	Fax Number
☒	☐	9	User99 User	user99@fax.com	10000000099
☐	☐	8	User98 User	user98@fax.com	10000000098
☐	☐	7	User97 User	user97@fax.com	10000000097
☐	☐	6	User96 User	user96@fax.com	10000000096
☐	☐	5	User95 User	user95@fax.com	10000000095
☐	☐	4	User94 User	user94@fax.com	10000000094
☐	☐	3	User93 User	user93@fax.com	10000000093
☐	☐	2	User92 User	user92@fax.com	10000000092
☐	☐	1	User91 User	user91@fax.com	10000000091
☐	☐	0	User90 User	user90@fax.com	10000000090
☐	☐	9	User89 User	user89@fax.com	10000000089

1

Tip

You can clear the selected option button by clicking [Reset].

Note

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

3 Click [Add].

The selected recipient is set for the transmission result list recipient.

□ Email Setting (Mailbox)

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

Instructions on how to do the Email setting for the mailbox are the same as for the Email setting for a private template.

📖 P.61 “Email Setting (Private template)”

□ Save as file Setting (Mailbox)

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

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

📖 P.63 “Save as file Setting (Private template)”

□ Box Setting (Mailbox)

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

Instructions on how to do the Box setting for the mailbox are the same as for the Box setting for a private template.

📖 P.66 “Box Setting (Private template)”

■ Deleting an Open Mailbox

You can delete an existing Open Mailbox from TopAccess.

Note

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

Deleting an mailbox

1 Click the [Registration] tab and the [Inbound FAX routing] menu.

The Inbound FAX routing page is displayed.

Note

When User Management Setting and Role Based Access Control are enabled, the login page will be displayed. When Role Based Access Control is enabled, only users who have registration privileges can log in to the [Registration] tab page.

2 Click the box number link that you want to delete in the mailboxes list.

Box Number	User Name	Agent	Comment
003	User03	InternetFax(Relay)	
002	User01	Bulletin Board	
001	User01	Confidential	

- If you click the box number link that is not protected by a password, skip to step 4.
- If you click the box number link that is protected by a password, go to the next step.

3 Enter the password for the mailbox and click [OK].

Input MailBox Password

OK Cancel

Password

The MailBoxes Properties page is displayed.

4 Click [Delete].

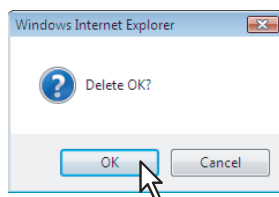
MailBoxes Properties

Edit Delete

Box Number	001
Notification	
Agent	Confidential

The confirmation dialog box appears.

5 Click [OK].



The selected mailbox is deleted.

MANAGING COUNTERS

This chapter explains the [Counter] tab page in TopAccess end-user mode.

Viewing Counters	96
Displaying the total counter	96
Displaying the department counter	98

Viewing Counters

This equipment maintains a set of counters that keep track of the number of pages printed, copied and scanned. These statistics can be displayed in totals or broken down by department. This section explains how to display the statistics and manage the department counters.

📖 P.96 “Displaying the total counter”

📖 P.98 “Displaying the department counter”

Note

Neither an end user nor an administrator can reset counters from TopAccess. However, an administrator can reset the department counters from the control panel. Refer to the ***MFP Management Guide***.

■ Displaying the total counter

In the [Total Count] menu, you can display the total counter information for the copy/print counter for small paper, copy/print counter for large paper, and scan counter.

Displaying the total counter

1 Click the [Counter] tab and the [Total Count] menu.

The Total Count page is displayed.

2 You can check the total counter in this page.

For the e-STUDIO4520C Series and the e-STUDIO6530C Series

TopAccess

e-Filing

Device

Job Status

Logs

Registration

Counter

User Management

Administration

Meta Scan

Total Count

Department

Total Count

Print Counter

	Copy	Fax	Printer	List	Total
Full Color	542	-	17178	-	17720
Twin Color	45	-	10	-	55
Black	110	0	9544	26	9680

Print Counter(small paper)

	Copy	Fax	Printer	List	Total
Full Color	500	-	16617	-	17117
Twin Color	0	-	10	-	10
Black	110	0	9446	26	9582

Print Counter(large paper)

	Copy	Fax	Printer	List	Total
Full Color	42	-	561	-	603
Twin Color	45	-	0	-	45
Black	0	0	98	0	98

Scan Counter

	Copy	Network	Fax	Total
Full Color	1420	288	-	1708
Twin Color	8	-	-	8
Black	961	172	4	1137

Scan Counter(small paper)

	Copy	Network	Fax	Total
Full Color	1398	262	-	1660
Twin Color	0	-	-	0
Black	961	170	0	1131

Scan Counter(large paper)

	Copy	Network	Fax	Total
Full Color	22	26	-	48
Twin Color	8	-	-	8
Black	0	2	4	6

1 Install Software | 1 Top | Help | ©2003-2009 TOSHIBA TEC CORPORATION All Rights Reserved

For the e-STUDIO455 Series

TopAccess [e-Filing](#)
[Logout](#)

Device Job Status Logs Registration **Counter** User Management Administration

Total Count | [Department](#)

Total Count

Print Counter

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

Scan Counter

	Copy	Network	Fax	Total
Small(Full Color)	-	0	-	0
Large(Full Color)	-	0	-	0
Small(Black)	0	0	0	0
Large(Black)	0	0	0	0
Total	0	0	0	0

[Install Software](#) | [Top](#) | [Help](#) | ©2003-2009 TOSHIBA TEC CORPORATION. All Rights Reserved.

6

For the e-STUDIO855 Series

TopAccess [e-Filing](#)

Device Job Status Logs Registration **Counter** User Management Administration Meta Scan

Total Count | [Department](#)

Total Count

Print Counter

	Copy	Fax	Printer	List	Total
Small	10276	0	0	0	10276
Large	6	0	0	0	6
Total	10282	0	0	0	10282

Scan Counter

	Copy	Network	Fax	Total
Small	1012	0	0	1012
Large	19	2	0	21
Total	1031	2	0	1033

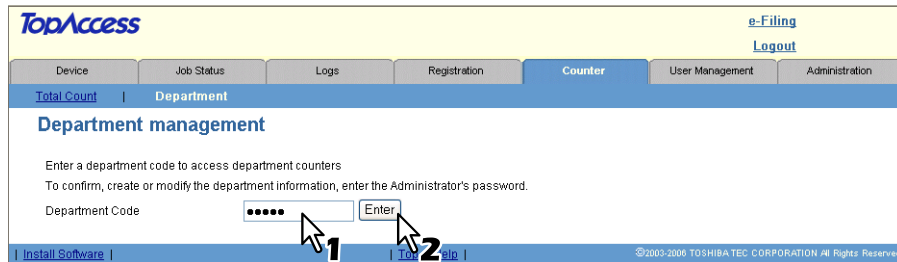
[Install Software](#) | [Top](#) | [Help](#) | ©2003-2009 TOSHIBA TEC CORPORATION. All Rights Reserved.

■ Displaying the department counter

In the [Department] menu, you can display the counter information of a specific department. If you want to display the department counter, you must enter the department code.

Displaying the department counter

- 1** Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2** Enter a department code for the counter to be displayed in the [Department Code] box and click [Enter].



TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

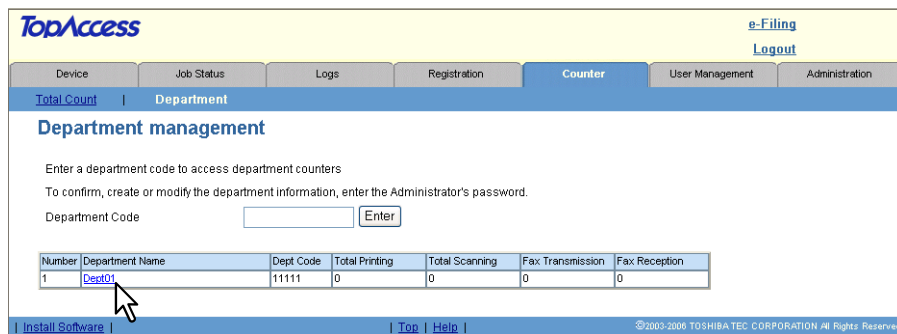
Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code

Install Software | Top Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The department counter for the specified department is displayed.

- 3** Click the department name link to display the detailed counters for the department.



TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	11111	0	0	0	0

Install Software | Top Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

4 The Department Information page opens.

For the e-STUDIO4520C Series and the e-STUDIO6530C Series

Department Information

Close

Department Number 1
 Department Name Dept01
 Department Code 11111

Total Counter

	Full Color	Twin Color	Black	Total
Copy	0	0	0	0
Fax	-	-	0	0
Printer	0	0	0	0
List	-	-	0	0
Total	0	0	0	0

Copy Counter

	Full Color	Twin Color	Black	Total
Small	0	0	0	0
Large	0	0	0	0

Fax Counter

For the e-STUDIO455 Series

Department Information

Close

Department Number 1
 Department Name Dept01
 Department Code 10001

Print Counter

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

Scan Counter

	Copy	Fax	Network	Total
Small(Full Color)	-	-	0	0
Large(Full Color)	-	-	0	0
Small(Black)	0	0	0	0
Large(Black)	0	0	0	0
Total	0	0	0	0

Fax Communication Counter

	Transmit	Received	Total
Small	-	-	0
Large	-	-	0

For the e-STUDIO855 Series

Department Information

Close

Department Number 2
 Department Name Dept01
 Department Code 10001

Print Counter

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

Scan Counter

	Copy	Fax	Network	Total
Small	0	0	0	0
Large	0	0	0	0
Total	0	0	0	0

Fax Communication Counter

	Transmit	Received	Total
Small	-	-	0
Large	-	-	0

TopAccess ADMINISTRATOR MODE

This chapter explains the administrative functions of TopAccess.

Features and Functions	103
About setup from TopAccess	103
About maintenance from TopAccess	104
About registration from TopAccess	104
About other administrative functions in TopAccess	105
Accessing TopAccess Administrator Mode	106
Setting up From TopAccess	108
Setting up device settings	108
Setting up Network settings	118
Setting up Copier settings	168
Setting up Fax settings	171
Setting up Save as file settings	176
Setting up Email settings	183
Setting up InternetFax settings	186
Setting up Printer settings	188
Setting up Print Service settings	193
Setting up ICC Profile settings	199
Displaying version information	206
Maintenance From TopAccess	207
About the maintenance functions	207
Uploading the software	208
Removing the client software	209
Backing up data	210
Restoring data from backup file	213
Deleting the data from local folder	215
Managing directory service	216
Setting up notification	218
Importing and exporting the Address Book	223
Importing and exporting the department code	228
Exporting the logs, journals, and counters	231
Clearing the logs and journals	233
Rebooting the equipment	235
Registering From TopAccess	236
Registering public templates	236
Registering Fax and Internet Fax received forward	245
Displaying Message Log	259
Managing Department Code	260
Displaying the department list and counters	260
Clearing the department counters	262
Registering or modifying the department code	264

Deleting the department code 266

Setting up User Management 268

Enabling department management 268

Setting up User Management setting..... 271

Setting role information 301

Setting up User Authentication for Scan to Email 307

Features and Functions

With the TopAccess web-based device management utility in the administrator mode, you can configure and device settings, display and filter message and job logs, and control current jobs using a web browser.

📖 P.103 “About setup from TopAccess”

📖 P.104 “About maintenance from TopAccess”

📖 P.104 “About registration from TopAccess”

📖 P.105 “About other administrative functions in TopAccess”

■ About setup from TopAccess

The following setup options are performed from TopAccess in the administrator mode:

Configuring device settings

An administrator can configure the device settings such as device information, energy save, date and time, and language for TopAccess web utility.

Configuring network settings

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

Configuring copier settings

An administrator can configure the default copier settings such as color mode, original mode for color, original mode for black, exposure for color, exposure for black, bypass feed, book > 2, magazine sort, 2in1/4in1, maximum copies, auto 2-sided mode, and sorter mode priority.

Tips

- [Color Mode], [Original Mode for Color], [Exposure for Color] are displayed only on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series.
- On the TopAccess menu of the e-STUDIO855 Series and the e-STUDIO455 Series, [Original Mode for Black] is displayed as [Original Mode], and [Exposure for Black] is displayed as [Exposure].

Configuring fax settings

An administrator can configure the facsimile device settings such as terminal ID, fax number, line 2 number, ringer volume, monitor volume, completion tone volume, reception mode, remote RX, dial type, dial type (line 2), line-2 mode, resolution, original mode, exposure, TTI, RTI, ECM, discard, reduction, duplex print, rotate sort, recovery transmit, journal auto print, memory transmission report, multi transmission report, polling report, and relay originator.

Note

The fax settings are available only when the fax option is installed on this equipment.

Configuring save as file settings

An administrator can configure the save as file settings such as storage maintenance, destination, remote 1, remote 2, N/W-Fax destination, and N/W-Fax folder.

Configuring Email settings

An administrator can configure the Email settings such as from address, from name, file format, fragment message size, and default body strings.

Configuring Internet Fax settings

An administrator can configure the Internet Fax settings such as from address, from name, subject, file format, fragment page size and default body strings.

Configuring printer settings

An administrator can configure the default printer settings such as number of days to save private, proof and invalid jobs, duplex printing, default paper size, default paper type, default orientation, default stapling, default output tray, PCL form line, PCL font pitch, PCL font point size, PCL font number, auto paper size conversion, wide A4 mode (for PCL), and print startup page.

Configuring print service settings

An administrator can configure the print services such as Raw TCP/IP print, LPD print, IPP print, FTP print, NetWare print, and Email print.

■ About maintenance from TopAccess

The following maintenance options are performed from TopAccess in the administrator mode:

Updating client software

An administrator can update the client software saved in this equipment. When a new version of client software is released, an administrator should update the client software in this equipment so clients can install new versions of their client software from TopAccess.

Removing client software

An administrator can remove client software saved in this equipment.

Creating backup files

An administrator can save the data in the address book, mailboxes, and templates as files for backups.

Restoring data from backup files

An administrator can restore the data in the address book, mailboxes, and templates using the backup files.

Deleting data in hard disk

An administrator can delete data such as scan, transmission, and reception data in the hard disk. Use this feature to delete data periodically for restoring the hard disk space if there is not enough disk space for operation.

Registering the directory service

An administrator can add or delete directory service for LDAP servers. If any LDAP servers are registered, clients can search for data using the registered LDAP servers to add new Email addresses to the address book.

Setting up the notification settings

An administrator can enable or disable Email notifications for specific events that occur in this equipment. An administrator specifies the Email address to send a notification.

Importing and exporting address book data

An administrator can import/export the address book data in CSV format.

Importing and exporting department code data

An administrator can import/export the department code data in CSV format.

Exporting logs

An administrator can export the logs and journals in CSV format such as print job logs, fax transmit journals, fax reception journals, scan logs, and message logs.

Clearing logs

An administrator can clear the logs and journals in CSV format such as print job logs, fax transmit journals, fax reception journals, scan logs, and message logs.

Rebooting the equipment

An administrator can reboot the equipment.

■ About registration from TopAccess

Registering is performed from TopAccess in the administrator mode:

Registering public templates

An administrator can register public templates that are available for all users.

Registering Fax or Internet Fax Received Forward

An administrator can register the agents for the relay transmission of received faxes or Internet Faxes. Using these agents, an administrator can collect all the received faxes by transmitting them to another internet fax device, saving them as a file in the hard disk or network folders, sending them to specific Email addresses, or storing to e-Filing.

Note

The Fax Received Forward is available only when the fax option is installed on this equipment.

■ About other administrative functions in TopAccess

Displaying message logs

An administrator can display the message logs from TopAccess in the administrator mode.

Registering department codes

An administrator can manage department codes from the [Counter] tab.

Setting up authentication

An administrator can configure the authentication for the operations in this equipment.

Accessing TopAccess Administrator Mode

TopAccess, web-based utility available on this equipment, allows you to manage this equipment remotely via the Internet or via your company's intranet.

To operate TopAccess, this equipment should be connected to the network and configured with the TCP/IP settings. After you complete the TCP/IP setup, you can access the TopAccess web site to operate various functions from your computer using a Web browser such as Firefox or Internet Explorer.

You can use the TopAccess web-based utility from a Windows, Macintosh or UNIX operating system environment.

Accessing TopAccess in the administrator mode

You can access the web utility TopAccess by entering its URL on the address box of web browser. To access it under a Windows Vista environment, confirm the network connection status on the Network Map with the LLTD (= Link Layer Topology Discovery) feature of Windows Vista, and then click the icon of this equipment.

This section describes how to access it by entering its URL on the address box of web browser.

For instruction on how to access it from the Network Map of Windows Vista, see P.10 "Accessing TopAccess from Network Map (Windows Vista/Windows 7/Windows Server 2008)". The procedure after displaying the TopAccess web page is the same as that in other OSs.

1 To navigate to TopAccess, enter the following URL on the address box of your Internet browser.

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

Address `http://10.10.70.120`

For example

When the IP address of the equipment is "10.10.70.105" (when IPv4 used):

`http://10.10.70.105`

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

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

or

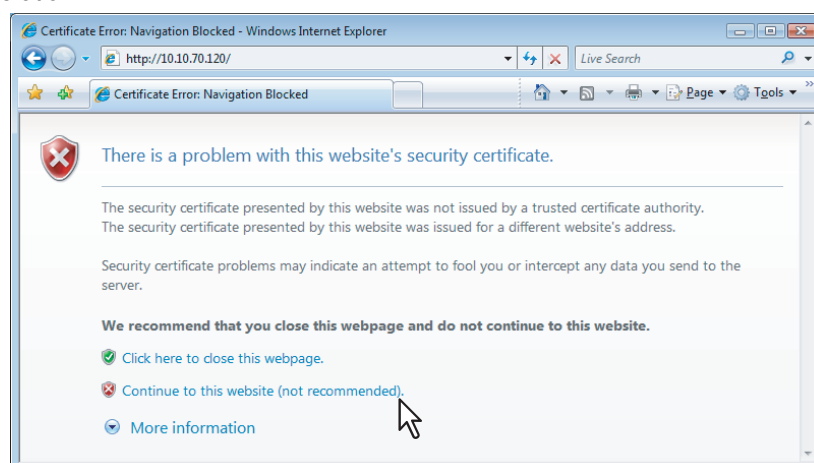
`http://[3ffe:1:1:10:280:91ff:fe4c:4f54]`

When the device name of this equipment is "mfp-00c67861":

`http://mfp-00c67861`

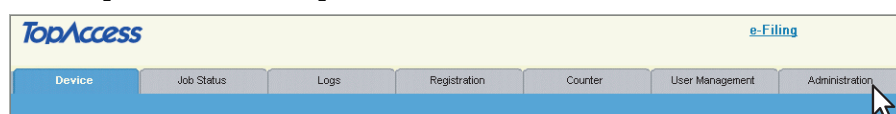
Note

When SSL for the HTTP network service is enabled, an alert message may appear when you enter the URL in the address box. In that case, click [Continue to this website (not recommended).] to proceed with the operation.



2 The TopAccess web page opens.

3 Click the [Administration] tab.



The Login page is displayed.

4 Enter the administrator password in the [Password] box. Then click [Login].

- You cannot change a name in the [User Name] box. It must always be “Admin” to log in to TopAccess in the administrator mode.
- The Setup page is displayed.

Tip

The default administrator password is “123456”.

5 Click the menu and submenu to display the desired page.

Tip

To log out from the administrator mode, click the Logout link that is displayed in the upper right.

Setting up From TopAccess

This section describes how to set up the equipment using TopAccess.

- 📖 P.108 “Setting up device settings”
- 📖 P.118 “Setting up Network settings”
- 📖 P.168 “Setting up Copier settings”
- 📖 P.171 “Setting up Fax settings”
- 📖 P.176 “Setting up Save as file settings”
- 📖 P.183 “Setting up Email settings”
- 📖 P.186 “Setting up InternetFax settings”
- 📖 P.188 “Setting up Printer settings”
- 📖 P.193 “Setting up Print Service settings”
- 📖 P.199 “Setting up ICC Profile settings”
- 📖 P.206 “Displaying version information”

Note

The paper size for each drawer cannot be set from TopAccess. Set from the touch panel of the equipment. For instructions on how to set the paper size for each drawer, refer to the **Copying Guide**.

■ Setting up device settings

In the [General] submenu in the [Setup] menu, an administrator can configure the general settings such as Device Information, Energy Save, Date and Time, and Web General Setting.

Note

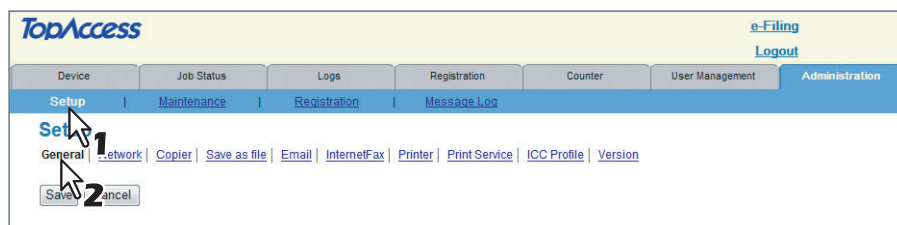
Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting the device settings

1 Access TopAccess in the administrator mode.

- 📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [General] submenu.



The General submenu page is displayed.

3 In the General submenu page, set the device settings as required.

TopAccess e-Filing Logout

Device | Job Status | Logs | Registration | Counter | User Management | Administration

Setup | Maintenance | Registration | Message Log

Setup

General | Network | Copier | Save as file | Email | InternetFax | Printer | Print Service | ICC Profile | Version

Save Cancel

General Setting

Device Information

Name	MFP-05212774
Copier Model	TOSHIBA e-STUDIO4520C
Save as File Space Available	9994 MB
Store to e-Filing Space Available	13988 MB
Fax Transmission Space Available	3499 MB
Fax Reception Space Available	500 MB
Work Space Available	99 %
Department Code	Disable
Department Code Enforcement	ON
e-Filing	Enable
Data Cloning Function	Enable

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

In the General submenu page, you can set the following:

- 📖 P.110 "Setting up Device Information"
- 📖 P.112 "Setting up e-Filing Notification Events"
- 📖 P.112 "Setting up Energy Save"
- 📖 P.114 "Setting up Date & Time"
- 📖 P.114 "Setting up Daylight Savings Time Setting"
- 📖 P.115 "Setting up WEB General Setting"
- 📖 P.115 "Setting up EWB Setting"

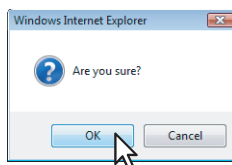
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the General page immediately after changing the settings and clicking [Save]. If that happens, click the [General] submenu to refresh the page.

□ Setting up Device Information

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

Device Information		
1	Name	MFP-06904266
2	Copier Model	TOSHIBA e-STUDIO755
3	Serial Number	CDA900112
4	Save as File Space Available	7000 MB
5	Store to e-Filing Space Available	6997 MB
6	Fax Transmission Space Available	501 MB
7	Fax Reception Space Available	501 MB
8	Work Space Available	99 %
9	Department Code	Disable
10	Department Code Enforcement	ON
11	Department Management (Copy)	Enable
12	Department Management (FAX)	Enable
13	Department Management (Print)	Enable
14	Department Management (Scan)	Enable
15	Department Management (List)	Enable
16	e-Filing	Enable
17	Data Cloning Function	Enable
18	Save to USB Media	Enable
19	USB Direct Print	Enable
20	Document Name Expression	Display
21	Queue name	print
22	Location	
23	Contact Information	
24	Service Phone Number	
25	Administrative Message	
26	Administrator's Password	••••••
27	Confirm Password	••••••

- 1) **Name**
This displays the equipment's device name.
- 2) **Copier Model**
This displays the equipment's model name.
- 3) **Serial Number**
This displays the serial number of this equipment.
- 4) **Save as File Space Available**
This displays the available size to store the Save as file documents.
- 5) **Store to e-Filing Space Available**
This displays the available size to store the e-Filing documents.
- 6) **Fax Transmission Space Available**
This displays the available size to send the fax data. This is displayed only when the Fax Unit is installed.
- 7) **Fax Reception Space Available**
This displays the available size to receive the fax data. This is displayed only when the Fax Unit is installed.
- 8) **Work Space Available**
This displays the percentages of available hard disk space to store the temporary data.
- 9) **Department Code**
Select whether the department management is enabled or disabled.
- 10) **Department Code Enforcement**
Select whether invalid jobs, for which a department code is not specified or an invalid department code is specified, are printed or stored in the invalid job list when the department code is enabled.
 - **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
 - **Print** — Select this to print the invalid jobs.
 - **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Notes

- If the Department Code Enforcement is set to ON and the SNMP communication is enabled in the printer driver, the user will be prompted to enter the correct department code if an invalid department code was entered in the printer driver.
- The Department Code Enforcement setting is not applied when the User Management Setting is enabled.

11) Department Management (Copy)

When this function is enabled, the following counters are managed in each department.

- Number of copied sheets of paper.
- Number of originals scanned when copying is performed.

12) Department Management (FAX)

When this function is enabled, the following counters are managed in each department.

- Number of sent faxes
- Number of originals scanned when faxes are sent
- Number of received faxes
- Number of outputs in printing received faxes*1

*1 The number of outputs are only counted for received faxes, in which the department code needs to be entered, such as manual reception, polling reception or the printing of originals stored in the confidential mailbox and the bulletin mailbox.

13) Department Management (Print)

When this function is enabled, the number of outputs in printing (for printing, received Email and InternetFax) is managed in each department.

14) Department Management (Scan)

When this function is enabled, the number of originals scanned such as when they are stored in the shared folder is managed in each department.

15) Department Management (List)

When this function is enabled, the number of system page outputs is managed in each department.

16) e-Filing

Select whether the e-Filing functions are enabled or disabled.

17) Data Cloning Function

When this function is enabled, the service technician can move user data such as address books to other equipment. Set to [Enable] upon request from the service technician. Be sure to set it back to [Disable] after the operation is finished.

18) Save to USB Media

Select whether the functions using USB media are enabled or disabled.

19) USB Direct Print

Select whether the USB Direct Print function is enabled or disabled.

20) Document Name Expression

Select the display format from Display, No Display or Asterisk for the Document Name and To/File Name of Scan Job in the [Job Status] tab, Print Log and Scan Log in the [Logs] tab.

21) Queue name

Display the queue name for SMB printing. This queue name is used when users use the discovery function of the installer to obtain the network queue during the installation.

22) Location

Enter the name of the department or site. This is displayed in the [Device] tab page that appears first when accessing the TopAccess web site for users.

23) Contact Information

Enter the name or title of the contact person for this equipment. This is displayed in the [Device] tab page that appears first when accessing the TopAccess web site for users.

24) Service Phone Number

Enter the phone number for service on this equipment. This is displayed in the [Device] tab page that appears first when accessing the TopAccess web site for users.

25) Administrative Message

Enter the message about this equipment for all users to read. This is displayed in the [Device] tab page that appears first when accessing the TopAccess web site for users.

26) Administrator's Password

If you want to change the administrator's password used to log in functions from the touch panel and TopAccess, enter a new password. The password must be between 6 and 10 alphanumeric characters long. You cannot leave this box blank.

27) Confirm Password

Enter a new password that you entered in the [Administrator's Password] box.

□ Setting up e-Filing Notification Events

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

e-Filing Notification Events

1 — Advance automatic delete notification 0 Days

1) Advance automatic delete notification

Select when an Email notifying you of the approaching of the expiration date of data in e-Filing boxes is to be sent. You can select how many days before the expiration date from 0 (not notified) to 99 days.

□ Setting up Energy Save

You can set a period of time for clearing the touch panel display and setting to the default, and a period of time for entering the Automatic Energy Save mode, Sleep mode or Super Sleep mode. For the types of energy saving modes and procedures for entering each mode, refer to the Quick Start Guide.

Energy Save

1 — Auto Clear 45 Seconds

2 — Auto Power Save 60 Minutes

3 — Sleep Timer 240 Minutes

4 — Super Sleep Enable

1) Auto Clear

Select how long this equipment can remain inactive before the touch panel automatically returns to the default display and settings.

2) Auto Power Save

Select how long this equipment remains inactive before entering the Automatic Energy Save mode.

3) Sleep Timer

Select how long this equipment remains inactive before entering the Sleep mode or the Super Sleep mode.

Tips

- In the Sleep mode and the Super Sleep mode, power to the unused sections of this equipment is shut off while this equipment is in the standby status. Power consumption in the standby status becomes smallest in the Super Sleep mode. In the standby status, power consumption in the Sleep mode is larger than that in the Super Sleep mode but is smaller than that in the Automatic Energy Save mode.
- [Sleep Timer] is displayed as [Sleep/Auto Shut Off] on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series.
- The equipment may not enter this mode at the set timing depending on its operating status.

4) Super Sleep

Select whether this equipment enters the Sleep mode or the Super Sleep mode when a specified period of time has passed in the Automatic Energy Save mode or when the [ENERGY SAVE] button on the control panel is pressed. It enters the Super Sleep mode when [Enable] is selected for this setting.

Notes

- When any of the options such as the Wireless LAN Module, Bluetooth Module or e-BRIDGE ID Gate is installed in this equipment or when the optional IPsec feature is enabled, this equipment does not enter the Super Sleep mode even if [Enable] is selected for this setting.
- If this equipment cannot be connected to a network (such as the case that this equipment in the Super Sleep mode cannot be discovered over the network), retry searching.
- This setting is available only for the e-STUDIO455 Series and the e-STUDIO855 Series.

To use the Super Sleep mode for this equipment, perform the following network settings in advance:

- Select [Static IP] for [Address Mode] in the TCP/IP setting.
 P.120 "Setting up TCP/IP"
- Select [Disable] for [Enable IPv6] or select [Manual] for [Link Local Address] in the IPv6 setting.
 P.123 "Setting up IPv6"

- Select [Disable] for [Enable IPX/SPX] in the IPX/SPX setting.
 P.124 "Setting up IPX/SPX"
- Select [Disable] for [Enable Apple Talk] in the Apple Talk setting.
 P.125 "Setting up AppleTalk"
- Select [0] for [Scan Rate] in the POP3 network service setting.
 P.137 "Setting up POP3 Network Service"
- Select [Enable] for [Enable IPsec] of [IP Security].
 P.317 "Setting up IP Security Function"
- Disable IEEE802.1X authentication.
 For the IEEE802.1X authentication method under the wired LAN environment, refer to the following chapter in the MFP Management Guide.
 Chapter 2: "SETTING ITEMS (ADMIN) - IEEE802.1X Authentication Setting"

For the network access setting during the Super Sleep mode, see the following page:

 P.167 "Setting up Wake Up setting"

□ Setting up Date & Time

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

Date & Time				
	Year	Month	Date	Time
1 —	2009	October	26	14 : 39
2 —	(GMT+9:00) Osaka, Sapporo, Tokyo			
3 —	Date Format			YY/MM/DD

1) Year/Month/Date/Time

To adjust the date, select the year in the [Year] box, select the month in the [Month] box, and enter the day in the [Date] box.

To adjust the time, enter the time in the [Time] boxes.

2) Time Zone

Select the time zone where this equipment is located.

3) Date Format

Select the date format.

□ Setting up Daylight Savings Time Setting

Make the required settings for daylight savings time.

Daylight Savings Time Setting									
1 —	Daylight Savings Time				Enable				
2 —	Offset				+1:00				
3 —	Dates				Month	Week	Day of Week	Time	
Start					Jan	1st	Sun	00	: 00
End					Jan	1st	Sun	00	: 00

1) Daylight Savings Time

Select [Enable] to shift the clock to the daylight savings time. The default setting is [Disable].

2) Offset

Select the desired offset (time difference) from the local standard time. You can select from between -2 and +2 hours, excluding 0 hour, in 30-minute increments. The default setting is +1 hour.

3) Dates

Select the applicable period for the daylight savings time.

- Start: Select or enter the start date and time of daylight savings time.
- End: Select or enter the end date and time of daylight savings time.

Tips

- If you change the settings during the daylight saving time period, the changes will be reflected to the equipment's clock. If you disable the settings during the applicable period, the equipment's clock will shift to the standard time.
- If the equipment is turned off at the start or end date and time, the equipment will shift the clock the next time it is turned on.
- After the clock shifts, the daylight saving time will also apply to the weekly timers.

Notes

- Select the Start and the End dates and times based on the time set for the equipment.
P.114 "Setting up Date & Time"
- If the same month is specified for the Start and the End dates, the equipment does not shift the clock automatically.

□ Setting up WEB General Setting

You can set the display language for TopAccess, and session timer to automatically log out from the administrator mode.

WEB General Setting

1 — WEB Language English ▼

2 — Session Timer 10 Minutes

1) WEB Language

Select the display language for TopAccess.

2) Session Timer

Enter how long you want this equipment to preserve the session data of TopAccess. You can enter any integer between 5 to 999. This setting also applies to the session data of e-Filing web utility.

□ Setting up EWB Setting

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

Note

The EWB function is available only when the External Interface Enabler (GS-1020, optional) is installed on this equipment.

EWB Setting

1 — Default Page

☒ Factory Default Page

☐ Import HTML Page _____ Browse... Import

☐ External URL _____

2 — Server Registration _____

Add Delete

_____ Server Address

1) Default Page

Enter the address of the default page to be used for the EWB function.

- **Factory Default Page** — Select this to use the default page set at the factory shipment.
- **Import HTML Page** — Select this to import the default page to be used for the EWB feature to this equipment as an HTML file. When this HTML file is imported to this equipment, the default page setting turns to a link to the imported HTML file.
- **External URL** — Enter the address of the default page to be used for the EWB feature.

2) Server Registration

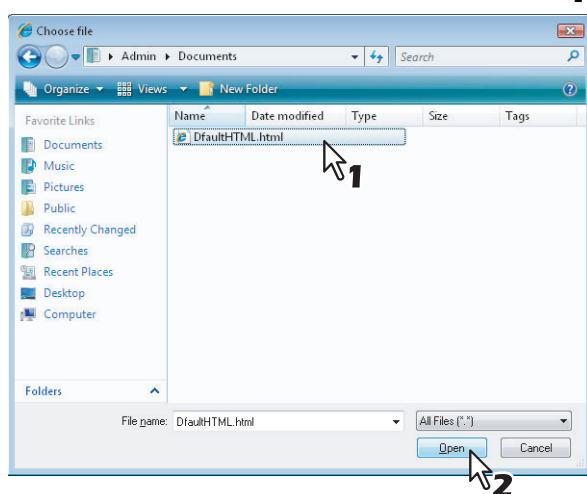
Enter the address of the server to be used for the EWB function.

Importing the default HTML file for the EWB function

- 1 To import the default HTML file for the EWB feature, select [Import HTML Page] and then click [Browse].

The Choose File dialog box appears.

- 2 Select the desired HTML file and then click [Open].



- 3 Click [Import].

The HTML file is imported to this equipment.

- 4 Click [Save] on the [General] submenu.

Registering a server

- 1 To register a server for the EWB function, enter the server address and then click [Add].

EWB Setting

Default Page

☒ Factory Default Page

☐ Import HTML Page

☐ External URL

Server Registration

157.69.69.195

Add Delete

2

1

Server Address

The server is registered.
To register more than one server, repeat this procedure.

- 2 Click [Save] on the [General] submenu.

7

Deleting a server

- 1 To delete a server registered for the EWB function, select the server that you want to delete, and then click [Delete].

EWB Setting

Default Page

☒ Factory Default Page

☐ Import HTML Page

☐ External URL

Server Registration

Add Delete

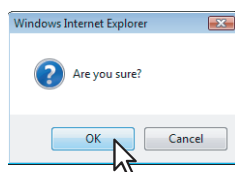
2

1

Server Address

157.69.69.195

- 2 Click [OK].



The server is deleted.

- 3 Click [Save] on the [General] submenu.

■ Setting up Network settings

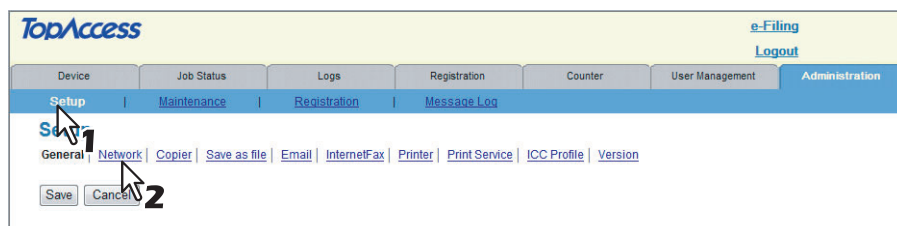
In the [Network] submenu in the [Setup] menu, an administrator can configure the network settings such as TCP/IP, Filtering, IPX/SPX, AppleTalk, Bonjour, LDAP Session, DNS Session, DDNS Session, SMB Session, NetWare Session, HTTP Network Service, SMTP Client, SMTP Server, POP3 Network Service, SNTP Service, FTP Client, FTP Server, SNMP Network Service, and Security Service.

Setting the network settings

1 Access TopAccess in the administrator mode.

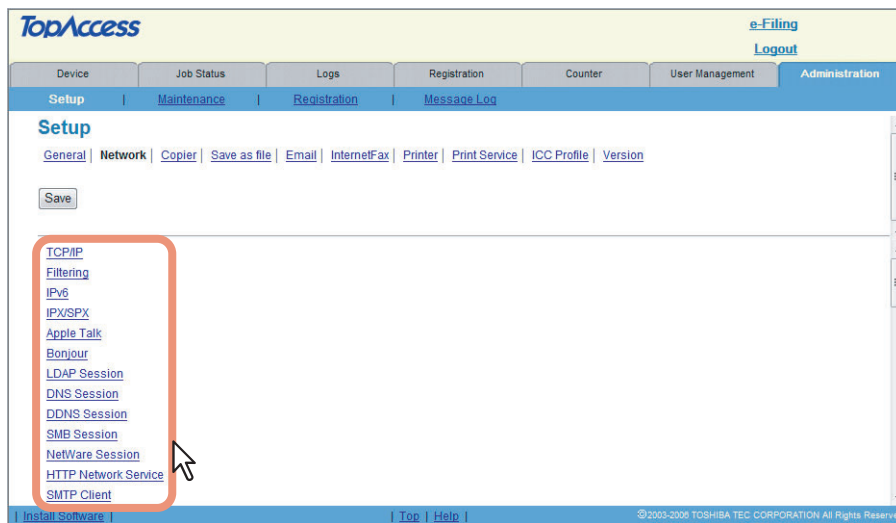
 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Setup] menu and [Network] submenu.



The Network submenu page is displayed.

- 3** In the Network submenu page, click link or scroll the page to find the setting table, and click the button of the setting to set the network settings as required.



In the Network submenu page, you can set the following:

- 📖 P.120 "Setting up TCP/IP"
- 📖 P.122 "Setting up Filtering"
- 📖 P.123 "Setting up IPv6"
- 📖 P.124 "Setting up IPX/SPX"
- 📖 P.125 "Setting up AppleTalk"
- 📖 P.125 "Setting up Bonjour"
- 📖 P.126 "Setting up LDAP Session"
- 📖 P.127 "Setting up DNS Session"
- 📖 P.128 "Setting up DDNS Session"
- 📖 P.130 "Setting up SMB Session"
- 📖 P.132 "Setting up NetWare Session"
- 📖 P.133 "Setting up HTTP Network Service"
- 📖 P.134 "Setting up SMTP Client"
- 📖 P.136 "Setting up SMTP Server"
- 📖 P.137 "Setting up POP3 Network Service"
- 📖 P.138 "Setting up SMTP Service"
- 📖 P.139 "Setting up FTP Client"
- 📖 P.139 "Setting up FTP Server"
- 📖 P.140 "Setting up SLP"
- 📖 P.141 "Setting up SNMP Network Service"
- 📖 P.146 "Setting up Security Service"
- 📖 P.166 "Setting up Web Services Setting"
- 📖 P.166 "Setting up LLTD Setting"
- 📖 P.167 "Setting up Wake Up setting"

- 4** Click [Set] to save the settings and close the sub window.

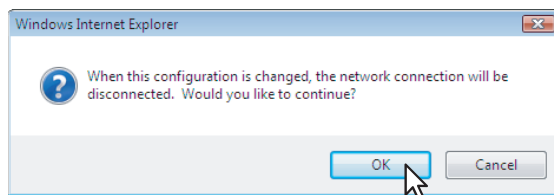
- 5** Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

6 Click [OK] to apply the changes.



This equipment starts initializing the network interface card to apply the changes

Note

During the initialization of the network interface card, the network will not be available. TopAccess will display "Please restart after waiting a few minutes." During the initialization, the touch panel will display "NETWORK INITIALIZING". When this message disappears, TopAccess will once again be available.

□ Setting up TCP/IP

You can set the TCP/IP protocol to enable communication over TCP/IP. The TCP/IP must be configured to enable TopAccess, SMB printing, Raw TCP or LPR printing, IPP printing, Save as file to network folder, Scan to Email, and Internet Fax.

TCP/IP

OK Cancel Selecting 'Save' in the Main Window is required to Save the new settings.

1	Ethernet Speed Duplex Mode	AUTO			
2	Address Mode	Static IP			
3	Obtain a Domain Name automatically	Enable			
4	Obtain a Domain Server Address automatically	Enable			
5	Obtain a WINS Server Address automatically	Enable			
6	Obtain a SMTP Server Address automatically	Disable			
7	Obtain a POP3 Server Address automatically	Disable			
8	Obtain a SNTP Server Address automatically	Disable			
9	IP Conflict Detect	Enable			
10	IP Address	10	10	70	120
11	Subnet Mask	255	255	255	0
12	Default Gateway	0	0	0	0

1) Ethernet Speed Duplex Mode

Select the ethernet speed.

Tips

- When you select a specific ethernet speed, you must select the same ethernet speed as set in the connected network. If you do not know the ethernet speed that must be used, select [AUTO].
- If the network is not stable, power OFF the equipment then ON.

2) Address Mode

Select how to set the IP address.

- **Static IP** — Select this to assign the static IP address manually. When this is selected, enter the static IP address in the [IP Address] box.
- **Dynamic** — Select this to assign the IP address using the DHCP with Auto-IP addressing enabled. When this is selected, the IP address, subnet mask, default gateway, primary WINS server address, secondary WINS server address, POP3 server address, and SMTP server address can be automatically obtained from the DHCP server if the network supports the DHCP, and the IP address can be also assigned using Auto-IP addressing even if the network does not support the DHCP.
- **No AutoIP** — Select this to assign the IP address using the DHCP with Auto-IP addressing disabled. When this is selected, the IP address, subnet mask, default gateway, primary WINS server address, secondary WINS server address, POP3 server address, and SMTP server address can be automatically obtained from the DHCP server if the network supports the DHCP, but the last IP address will not be used if the equipment cannot communicate with the DHCP server.

3) Obtain a Domain Name automatically

Select [Enable] when you want to obtain a domain name automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a domain name, the data are left blank in the domain name even if you set the correct domain name manually in the DDNS Session. In that case, select [Disable] here and set the correct domain name in the DDNS Session.

 P.128 "Setting up DDNS Session"

4) Obtain a Domain Server Address automatically

Select [Enable] when you want to obtain a domain server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a primary and secondary DNS server addresses, the data are left blank in the primary and secondary DNS server addresses even if you set the correct primary and secondary DNS server addresses manually in the DNS Session. In that case, select [Disable] here and set the correct primary and secondary DNS server address in the DNS Session.

 P.127 "Setting up DNS Session"

5) Obtain a WINS Server Address automatically

Select [Enable] when you want to obtain a primary or secondary WINS server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a primary and secondary WINS server addresses, the data are left blank in the primary and secondary WINS server addresses even if you set the correct primary and secondary WINS server addresses manually in the SMB Session. In that case, select [Disable] here and set the correct primary and secondary WINS server address in the SMB Session.

 P.130 "Setting up SMB Session"

6) Obtain a SMTP Server Address automatically

Select [Enable] when you want to obtain a SMTP server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a SMTP server address, the data are left blank in the SMTP server address even if you set the correct SMTP server address manually in the SMTP Client. In that case, select [Disable] here and set the correct SMTP server address in the SMTP Client.

 P.134 "Setting up SMTP Client"

7) Obtain a POP3 Server Address automatically

Select [Enable] when you want to obtain a POP3 server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a POP3 server address, the data are left blank in the POP3 server address even if you set the correct POP3 server address manually in the POP3 Network Service. In that case, select [Disable] here and set the correct POP3 server address in the POP3 Network Service.

 P.137 "Setting up POP3 Network Service"

8) Obtain a SNTP Server Address automatically

Select [Enable] when you want to obtain a SNTP server address automatically using the DHCP server. This setting will apply only when [No AutoIP] or [Dynamic] is selected in the Address Mode option.

Note

When the DHCP server does not have a SNTP server address, the data are left blank in the SNTP server address even if you set the correct SNTP server address manually in the SNTP Network Service. In that case, select [Disable] here and set the correct SNTP server address in the SNTP Network Service.

 P.140 "Setting up SLP"

9) IP Conflict Detect

Select [Enable] to display a message on the control panel when an IP address conflict is detected.

10) IP Address

Enter the static IP address that is assigned to this equipment when [Static IP] is selected in the [Address Mode] box.

11) Subnet mask

Enter the subnet mask if required when [Static IP] is selected in the [Address Mode] box.

12) Default Gateway

Enter the gateway address if required when [Static IP] is selected in the [Address Mode] box.

□ Setting up Filtering

You can set filtering in order to restrict access from client computers to this equipment. Filtering can be specified with an IP address or a MAC address.

Note

MAC address filtering is given priority over IP address filtering.

Filtering

OK Cancel Selecting "Save" in the Main Window is required to Save the new settings.

1 Enable IP Filtering Enable

2 IP Filtering Rule Permit

3

IP Filtering	Start Address	End Address
Filter 1	0 0 0 0	0 0 0 0
Filter 2	0 0 0 0	0 0 0 0
Filter 3	0 0 0 0	0 0 0 0
Filter 4	0 0 0 0	0 0 0 0
Filter 5	0 0 0 0	0 0 0 0
Filter 6	0 0 0 0	0 0 0 0
Filter 7	0 0 0 0	0 0 0 0
Filter 8	0 0 0 0	0 0 0 0
Filter 9	0 0 0 0	0 0 0 0
Filter 10	0 0 0 0	0 0 0 0

4 Enable MAC Address Filtering Disable

5 MAC Address Filtering Rule Permit

6

MAC Address Filtering	MAC Address
Filter 1	
Filter 2	
Filter 3	
Filter 4	
Filter 5	
Filter 6	
Filter 7	
Filter 8	
Filter 9	
Filter 10	

1) Enable IP Filtering

Select [Enable] for IP address filtering. When [Enable] is selected, access from devices on a network to which the IP address (specified in [IP Filtering]) is set is restricted under conditions set in [IP Filtering Rule].

Note

IP address filtering is enabled only under IPv4 network environment and it is disabled under IPv6 environment. If you need to use IP address filtering under IPv6 environment, select MAC address filtering.

2) IP Filtering Rule

Select IP address filtering rules.

- **Permit** — Select this to permit access from devices on a network to which the IP address (specified in [IP Filtering]) is set.
- **Deny** — Select this to deny access from devices to which the specified IP address is set.

3) IP Filtering

Enter the starting IP address and the ending IP address of a target client computer for IP filtering. Up to 10 addresses can be specified.

Note

Only IPv4 addresses are available. An IPv6 address cannot be specified.

4) Enable MAC Address Filtering

Select [Enable] for MAC address filtering. When [Enable] is selected, access from devices on a network to which the MAC address (specified in [MAC Address Filtering]) is set is restricted under conditions set in [MAC Address Filtering Rule].

5) MAC Address Filtering Rule

Select MAC address filtering rules.

- **Permit** — Select this to permit access from devices on a network to which the MAC address (specified in [MAC Address Filtering]) is set.
- **Deny** — Select this to deny access from devices to which the specified MAC address is set.

6) MAC Address Filtering

Enter the MAC address of a target client computer for MAC address filtering. Up to 10 addresses can be specified.

□ Setting up IPv6

You can set the IPv6 protocol to enable the communication over IPv6.

IPv6

OK Cancel Selecting "Save" in the Main Window is required to Save the new settings.

1 **Enable IPv6** Enable

2 **LLMNR** Disable

3 **Link Local Address**

4 **Manual**

IP Address

Prefix Length 0

Gateway

☐ Use DHCPv6 Server for options

5 **Use Stateless Address**

☐ Keep Configuration (If router setting is changed)

☐ Use DHCPv6 Server for IP Address (M flag)

☐ Use DHCPv6 Server for options (O flag)

No.	IP Address	Prefix Length	Gateway
1:		0	
2:		0	
3:		0	
4:		0	
5:		0	
6:		0	
7:		0	

6 **Use Stateful Address**

☐ Use DHCPv6 Server for IP Address

☐ Use DHCPv6 Server for options

IP Address	Prefix Length	Gateway
	0	

1) Enable IPv6

Select whether the IPv6 protocol is enabled or disabled.

2) LLMNR

If IPv6 is enabled, select whether LLMNR is enabled or disabled.

3) Link Local Address

The unique address used for the IPv6 is displayed.

4) Manual

You assign the IPv6 address, prefix and default gateway manually. In this mode, you can assign one IPv6 address to this equipment.

- **IP Address** — Assign the IPv6 address for this equipment.
- **Prefix Length** — Assign the prefix for the IPv6 address.
- **Gateway** — Assign the default gateway.

- **Use DHCPv6 Server for options** — Select whether or not the optional information (IPv6 address for the DNS server, etc.) except the IPv6 address for this equipment, which is issued from the DHCPv6 server is used on this equipment.

Tips

- When [Manual] is selected, a stateful address cannot be set.
- If the selected IPv6 address is already assigned, DAD (Duplicate Address Detection) detects it and notifies you on the control panel of this equipment.

5) Use Stateless Address

Use the IPv6 addresses (Stateless addresses) issued from routers.

- **Keep Configuration(If router setting is changed)** — Select the method for handling IPv6 address data when new IPv6 address is provided from the same router providing the current IPv6 address to this equipment.
- **Use DHCPv6 Server for IP Address(M flag)** — Use the IPv6 address issued from the DHCPv6 server in the stateless network environment.
- **Use DHCPv6 Server for options(O flag)** — Use the optional information (IPv6 address for the DNS server, etc.) issued from the DHCPv6 server in the stateless network environment.
- **IP Address** — Stateless Addresses obtained from routers are displayed. Up to 7 IPv6 addresses can be retained.

Tip

When this equipment receives a router advertisement (RA) from a router, of which M flag configuration is “0”, the DHCPv6 function is disabled. If you change a router advertisement (RA) M flag configuration from “0” to “1”, it is necessary to reboot this equipment to enable the DHCPv6 function.

6) Use Stateful Address

Use the Stateful address issued from DHCPv6 server.

- **Use DHCPv6 Server for IP Address** — Select whether or not the IPv6 address which is issued from the DHCPv6 server is used for this equipment.
- **Use DHCPv6 Server for options** — Select whether or not the optional information (IPv6 address for the DNS server, etc.) except the IPv6 address for this equipment, which is issued from the DHCPv6 server is used on this equipment.
- **IP Address** — A stateful address, Prefix Length and Gateway1-7 obtained from DHCPv6 Server are displayed.

□ Setting up IPX/SPX

You can set the IPX/SPX protocol to enable the communication over IPX/SPX. The IPX/SPX must be configured to enable Novell printing with NetWare server 5.1, 6.0, 6.5 over IPX/SPX.

1) Enable IPX/SPX

Select whether the IPX/SPX protocol is enabled or disabled. Enable this when configuring Novell printing over the IPX/SPX network.

2) Frame Type

Select the desired frame type for IPX/SPX.

- **Auto Sense** — Select this to use an appropriate frame type that the equipment found first.
- **IEEE 802.3/Ethernet II/IEEE 802.3 Snap/IEEE802.2** — Instead of [Auto Sense], select the frame types to be used from these options.

3) Actual Frame

This displays the actual frame type of the equipment.

□ Setting up AppleTalk

You can set the protocol to enable communication over AppleTalk. AppleTalk must be configured to enable AppleTalk printing from Macintosh computers.

1) Enable Apple Talk

Select whether the AppleTalk protocol is enabled or disabled. Enable this when configuring AppleTalk printing.

2) Device Name

Enter the device name of the equipment that will be displayed in the AppleTalk network.

3) Desired Zone

Enter the zone name where the equipment will connect — if required. If you leave an asterisk in this box, the equipment will connect to the default zone.

□ Setting up Bonjour

In Bonjour, you can enable or disable the Bonjour networking that is available for Mac OS X.

1) Enable Bonjour

Select whether Bonjour is enabled or disabled.

2) Link-Local Host Name

Enter the DNS host name of this equipment.

3) Service Name

Enter the device name of this equipment that will be displayed in the Bonjour network.

□ Setting up LDAP Session

In LDAP Session, you can enable or disable the LDAP directory service.

1) Enable LDAP

Select whether the LDAP directory service is enabled or disabled.

2) Enable SSL

Select whether the SSL (Secure Sockets Layer) is enabled or disabled for communicating the LDAP directory service.

- **Disable** — Select this to disable the SSL for communicating the LDAP directory service.
- **Verify with imported cert** — Select this to enable the SSL using the imported CA certificate.
- **Accept all certificates without CA** — Select this to enable the SSL without using imported CA certificate.

Notes

- When [Verify with imported cert] is selected, you must import the CA certificate in this equipment.
 P.146 “Setting up Security Service”
- If at least one of the registered LDAP directory services requires the SSL, you must enable the [Enable SSL] option. When the [Enable SSL] option is enabled, this equipment will connect the registered LDAP directory services using SSL first. Then if the connection fails using SSL, this will connect to the registered LDAP directory service without using SSL. Therefore, even if you enable the [Enable SSL] option, this equipment can also connect to an LDAP directory service that does not require the SSL.
- The SSL port number can be set for each LDAP directory service when it is registered.
 P.216 “Managing directory service”
- Not all operating systems support SSL for all protocols.

3) Attribute 1

Enter the name of the schema corresponding to the LDAP server configuration.

4) Attribute 2

Enter the name of the schema corresponding to the LDAP server configuration.

5) Search Method

Select search conditions for LDAP searching.

- **Partial match** — Select this to search information partially matching the search conditions.
- **Prefix match** — Select this to search information that starts with contents matching the search conditions.
- **Suffix match** — Select this to search information that ends with contents matching the search conditions.
- **Full match** — Select this to search information fully matching the search conditions.

□ Setting up DNS Session

In DNS Session, you can specify the DNS server to enable the FQDN (Fully Qualified Domain Name) rather than the IP address on specifying each server address such as SMTP server, POP3 server, and LDAP server.

Tip

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

📖 P.128 "Setting up DDNS Session"

DNS Session

OK Cancel Selecting 'Save' in the Main Window is required to Save the new settings.

- 1 Enable DNS
- 2 Primary DNS Server Address
- 3 Secondary DNS Server Address
- 4 Primary DNS Server Address(IPv6)
- 5 Secondary DNS Server Address(IPv6)

Enable

0 0 0 0

0 0 0 0

1) Enable DNS

Select whether the DNS server is enabled or not.

2) Primary DNS Server Address

Specify the IP address of the primary DNS server when the DNS service is enabled.

3) Secondary DNS Server Address

Specify the IP address of the secondary DNS server when the DNS service is enabled, as you require.

4) Primary DNS Server Address(IPv6)

Specify the IP address of the primary DNS server when the DNS service is enabled in IPv6.

5) Secondary DNS Server Address(IPv6)

Specify the IP address of the secondary DNS server when the DNS service is enabled in IPv6, as required.

Tip

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

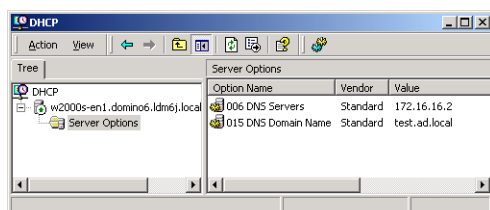
📖 P.120 "Setting up TCP/IP"

□ Setting up DDNS Session

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

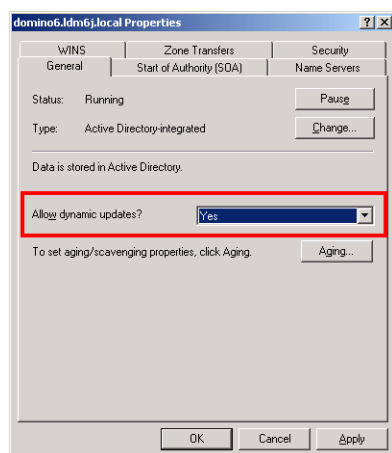
Notes

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

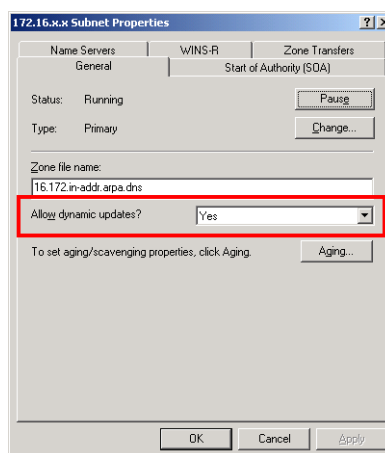


- When using DDNS, make sure the “Allow dynamic updates?” option is set to “Yes” (for Windows 2000 Server) or “Nonsecure and secure” (for Windows Server 2003) for the Forward Lookup Zones and Reversed Lookup Zones. If the setting of Windows Server 2003 is “Secure” mode or “None” for this DDNS function, you need to set the correct primary login name and primary password to update the DNS server by DDNS. If you do not want to use DDNS such as managed by primary and secondary login name and password, you need to add the equipment’s host name manually in the Forward and Reversed Lookup Zone.

Forward Lookup Zones
(Windows 2000 Server)



Reversed Lookup Zones
(Windows 2000 Server)



1) Enable DDNS

Select whether the dynamic DNS service is enabled or disabled.

2) Host Name

Enter the host name that will be added to the DNS server using DDNS.

3) Domain Name

Enter the domain name that will be added to the DNS server using DDNS.

Tip

When the [Obtain a Domain Name automatically] option is enabled in the TCP/IP settings, the domain name can be obtained using the DHCP server.

P.120 "Setting up TCP/IP"

4) Security Method

Enter the security method.

- GSS-TSIG

Select this to perform a secure DDNS session using GSS-TSIG. You must set a login name and a password. If both are not set, the secure DDNS session will not be available.

- TSIG

Select this to perform a secure DDNS session using TSIG. To select this, you must upload a key file and a private key file. If any of them is uploaded, the security setting will be disabled.

- SIG (0)

Select this to perform a secure DDNS session using SIG(0). To select this, you must upload a key file and a private key file. If any of them is uploaded, the security setting will be disabled.

5) Primary Login Name

Enter the primary login name if the security method selected in the above setting is GSS-TSIG.

6) Primary Password

Enter the primary password if the security method selected in the above setting is GSS-TSIG.

7) Secondary Login Name

Enter the secondary login name if the security method selected in the above setting is GSS-TSIG.

8) Secondary Password

Enter the secondary password if the security method selected in the above setting is GSS-TSIG.

9) TSIG/SIG (0) Key file

Use this setting to upload or delete a key file to be used for TSIG and SIG (0). To upload it, click [Browse..] and specify a key file to be uploaded, and then click [Upload]. To delete it, click [DELETE].

10) TSIG/SIG (0) Private Key file

Use this setting to upload or delete a private key file to be used for TSIG and SIG(0). To upload it, click [Browse..] and specify a private key file to be uploaded, and then click [Upload]. To delete it, click [DELETE].

□ Setting up SMB Session

In SMB Session, 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.

SMB Session

OK Cancel Selecting 'Save' in the Main Window is required to Save the new settings.

SMB

1 SMB Server Protocol Enable

2 Internet Protocol Version

• IPv4

• IPv6

3 NetBIOS Name MFP-05212774

4 Logon

• Workgroup

• Domain

5 Primary Domain Controller

6 Backup Domain Controller

7 Logon User Name

8 Password

9 Primary WINS Server 0 0 0 0

10 Secondary WINS Server 0 0 0 0

SMB Signing of SMB Server

• If client agrees, digital signature is done for the communication.

• Digital signature is always done for the communication on the server side.

• Digital signature isn't done for the communication for the server.

SMB Signing of SMB Client

• If server agrees, digital signature is done for the communication.

• Digital signature is always done for the communication on the client side.

• Digital signature isn't done for the communication for the client.

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.
- **Disable Print Share** — Select this to enable the file sharing service using SMB, but disable SMB printing.
- **Disable File Share** — Select this to enable SMB printing, but disable the file sharing service using SMB.

2) Internet Protocol Version

Select an Internet Protocol Version.

- **IPv4** — Select this to enable IPv4. IPv6 is disabled.
- **IPv6** — Select this to enable IPv6. IPv4 is disabled.

Note

Switching the SMB internet protocol version requires you to restart the equipment to reflect the change. When “Reboot the machine” appears on the control panel of the equipment, turn the power OFF and then back ON.

3) 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 alphanumeric characters and “-” (hyphenation) for NetBIOS name. If you use any other characters, a warning message will be displayed.

4) Logon

Enter the workgroup or domain that this equipment joins.

- **Workgroup** — Select this and enter the workgroup name when the equipment will logon in the workgroup. 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 logon 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.

Tip

When the [Obtain a Domain Name automatically] option is enabled in the TCP/IP settings, the domain name can be obtained using the DHCP server.

 P.120 "Setting up TCP/IP"

Note

You can enter only alphanumeric characters and symbols except the following characters for Workgroup.

; : " < > * + = \ | ? ,

If you use any other characters, a warning message will be displayed.

5) Primary Domain Controller

Specify the server name or IP address of the primary domain controller when this equipment will logon the domain network.

6) Backup Domain Controller

Specify the server name or IP address of the backup domain controller when this equipment will logon the domain network, if required. If the Primary Domain Controller is unavailable, the Backup Domain Controller will be used to log on.

Note

If the wrong primary or backup domain controller is specified, the NETWORK INITIALIZING message will be displayed for 5 to 10 minutes while this 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.

7) Logon User Name

Enter a valid user name to logon to the specified domain.

8) Password

Enter the password for the specified logon user name to logon the domain network.

9) 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.

 P.120 "Setting up TCP/IP"

10) 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.

 P.120 "Setting up TCP/IP"

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.

11) 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 client agrees, digital signature is done for the communication.** — Select this to use the digital signature to secure the 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 a 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.

12) 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 a 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 a 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 a SMB server with a digital signature. When the SMB Signing of SMB Server is disabled in a SMB server, the communication is not allowed.
- **Digital signature isn't done for the communication for the client.** — Select this to communicate to a SMB server without the digital signature. If the SMB Signing of SMB Server is always enabled in a SMB server, the communication is not allowed.

Notes

- 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.
- When communicating the Windows Server 2003 as a SMB server, it is recommended to select [If server agrees, digital signature is done for the communication.] or [Digital signature is always done for the communication on the client side.], because the SMB Signing of SMB Server is enabled on the Windows Server 2003 as the default.

□ Setting up NetWare Session

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

1) Enable Bindery

Select whether the NetWare Bindery mode for Novell printing is enabled or disabled. When you configure a Novell printing environment with the NetWare server in bindery mode, you must enable this.

2) Enable NDS

Select whether the NetWare NDS mode for Novell printing is enabled or disabled. When you configure a Novell printing environment with the NetWare server in NDS mode, you must enable this. When this is enabled, you should also specify the context and tree for the NDS.

3) Context

Enter the NDS context where the NetWare print server for this equipment is located.

4) Tree

Enter the NDS tree.

5) Search root

Enter the NetWare server name that this equipment preferentially searches for the queues.

□ Setting up HTTP Network Service

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

1) Enable HTTP Server

Select whether the Web-based services such as TopAccess and e-Filing web utility are enabled or disabled.

2) Enable SSL

Select whether the SSL (Secure Sockets Layer) is enabled or disabled.

When this is enabled, the data transferred between the equipment and client computers will be encrypted using a private key when operating TopAccess and e-Filing web utility.

Notes

- To enable SSL, you must create a self-signed certificate or import a server certificate in Security Service. If the self-signed certificate is not created or a server certificate is not imported, the SSL will not work correctly. For Windows Vista, you need to import certificates also to the client PC.
[P.146 "Setting up Security Service"](#)
[P.362 "Installing Certificates for a Client PC"](#)
- Not all operating systems support SSL for all protocols.

3) Primary Port Number

Enter the port number for the NIC HTTP server. Generally "80" is used for this port.

4) Secondary Port Number

Enter the port number for TopAccess and the e-Filing web utility. Generally "8080" is used for this port.

5) SSL Port Number

Enter the port number for the SSL. Generally "10443" is used for this port.

□ Setting up SMTP Client

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

Note

A From Address setting is also required to send Internet Fax and Emails. For information about the From Address setting, see the following sections.

📖 P.183 “Setting up Email settings”

📖 P.186 “Setting up InternetFax settings”

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

📖 P.268 “Setting up User Management”

1) Enable SMTP Client

When this is enabled, this equipment sends an Internet Fax and an Email to the specified SMTP server for transmission over the Internet.

2) Enable SSL

Select whether the SSL (Secure Sockets Layer) is enabled or disabled for SMTP transmission.

- **Disable** — Select this to disable the SSL for SMTP transmission.
- **Verify with imported cert** — Select this to enable the SSL using the imported CA certificate.
- **Accept all certificates without CA** — Select this to enable the SSL without using imported CA certificate.

Notes

- When [Verify with imported cert] is selected, you must import the CA certificate in this equipment.
📖 P.146 “Setting up Security Service”
- Not all operating systems support SSL for all protocols.

3) SSL/TLS

Select the protocol for the SSL when the [Enable SSL] 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** — Select this to send a message in SLL (Secure Socket Layer).

Note

When you select [Over SSL], make sure to change the port number correctly. Generally, “465” port is used for the Over SSL instead of “25” port.

4) SMTP Server Address

Enter the IP address or FQDN (Fully Qualified Domain Name) of the SMTP server when [Enable SMTP Client] is enabled.

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.

 P.120 "Setting up TCP/IP"

5) POP Before SMTP

Select whether the POP Before SMTP authentication is enabled or disabled.

6) Authentication

Select the type of the 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 the plain authentication.
- **Login** — Select this to access the SMTP server using the login authentication.
- **CRAM-MD5** — Select this to access the SMTP server using the CRAM-MD5 authentication.
- **Digest-MD5** — Select this to access the SMTP server using the Digest-MD5 authentication.
- **Kerberos** — Select this to access the SMTP server using the Kerberos authentication.
- **NTLM(IWA)** — Select this to access the SMTP server using the NTLM (IWA) authentication.
- **Auto** — Select this to access the SMTP server using the appropriate authentication that this equipment detects.

7) Login Name

Enter the login name to access the SMTP server if the SMTP authentication is enabled.

8) Password

Enter the password to access the SMTP server if the SMTP authentication is enabled.

9) Maximum Email / InternetFax Size

Select the maximum size (2-100 MB) that this equipment is allowed to send using the SMTP.

10) 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. Generally "25" is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

11) SMTP Client Connection Timeout(1-180)

Enter timeout period for quitting communication when no response is received from SMTP server from 1 to 180 seconds.

□ Setting up SMTP Server

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

1) Enable SMTP Server

Select whether this equipment works as an SMTP server or not. This must be enabled when you enable the Offramp Gateway feature. When this is enabled, this equipment can receive Internet Faxes or Emails that are forwarded through the SMTP to the domain of this equipment.

2) Port Number

Enter the port number to transmit an Internet Faxes or Emails. Generally "25" is used for the SMTP transmission.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

3) Email Address

Enter the Email address of this equipment. When this equipment works as an SMTP server, it can receive all Internet Faxes and Emails that contain its domain name. If the Email address of the received document matches the address you set here, this equipment prints it.

4) Enable OffRamp Gateway

Select whether the Offramp Gateway transmission is enabled or disabled.

5) OffRamp Security

Select whether the Offramp Security is enabled or disabled. When this is enabled, this equipment cancels the offramp gateway transmissions that are forwarding to the fax numbers not registered in the Address Book of this equipment. This can prevent the unauthorized offramp gateway transmission.

6) OffRamp Print

Select whether this equipment should print documents sent using the offramp gateway transmission. When this is enabled, this equipment automatically prints documents sent using offramp gateway transmission, so that they can be confirmed.

□ Setting up POP3 Network Service

In POP3 Network Service, you can specify the POP3 server to receive an Internet Fax and Emails.

1) Enable POP3 Client

Select whether retrieving an Internet Fax and an Email from the POP3 server is enabled or disabled.

2) Enable SSL

Select whether the SSL (Secure Sockets Layer) is enabled or disabled for POP3 transmission.

- **Disable** — Select this to disable the SSL for POP3 transmission.
- **Verify with imported cert** — Select this to enable the SSL using the imported CA certificate.
- **Accept all certificates without CA** — Select this to enable the SSL without using imported CA certificate.

Notes

- When [Verify with imported cert] is selected, you must import the CA certificate in this equipment.
[P.146 “Setting up Security Service”](#)
- Not all operating systems support SSL for all protocols.

3) POP3 Server Address

Enter the IP address or FQDN (Fully Qualified Domain Name) of the POP3 server when [Enable POP3 Client] is enabled.

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, the POP3 server address can be obtained using the DHCP server.

[P.120 “Setting up TCP/IP”](#)

4) Authentication

Enable or disable the authentication for accessing the POP3 server.

- **Disable** — Select this to disable the authentication.
- **NTLM/SPA** — Select this to access the POP3 server using the NTLM/SPA authentication.
- **Kerberos** — Select this to access the POP3 server using the Kerberos authentication.

5) Type POP3 Login

Select the POP3 login type.

- **Auto** — Select this to automatically designate the POP3 login type of the POP3 server.
- **POP3** — Select this to use the general POP3 login type.
- **APOP** — Select this to use the APOP login type. APOP allows users to access the POP3 server by encrypting the user name and password.

Note

If it is not possible to login to the mail server using [Auto], manually set the type of POP3 Login to either [POP3] or [APOP].

6) Account Name

Enter the account name for this equipment to access the POP3 server.

Note

Enter the account name without the domain name when [NTLM/SPA] or [Kerberos] is selected in the [Authentication] option.

7) Password

Enter the password for this equipment to access the POP3 server.

8) Scan Rate

Enter how often this equipment should access the POP3 server for new messages.

9) Port Number

Enter the port number to access the POP3 server. The port number depends on the port setting in the POP3 server. Generally "110" is used.

10) SSL Port Number

Enter the port number to access the POP3 server using SSL. The SSL port number depends on the port setting in the POP3 server. Generally "995" is used.

11) POP3 Client Connection Timeout(1-180)

Enter timeout period for quitting communication when no response is received from the POP3 server from 1 to 180 seconds.

□ Setting up SNTP Service

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

1) Enable SNTP

Select whether the SNTP service is enabled or disabled. When this is enabled, the time settings of this equipment can be adjusted using the SNTP service.

2) Primary SNTP Address

Specify the IP address of the primary SNTP server when the SNTP service is enabled.

3) Secondary SNTP Address

Specify the IP address of the secondary SNTP server as required.

Tip

When the [Obtain a SNTP Server Address automatically] option is enabled in the TCP/IP settings, the SNTP server address can be obtained using the DHCP server.

P.120 "Setting up TCP/IP"

4) Scan Rate

Enter how often this equipment should access the SNTP server.

5) Port Number

Enter the port number for the SNTP service. Generally "580" is used for the SNTP port number.

□ Setting up FTP Client

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

1) Default Port Number

Enter the port number to access the FTP site. The port number depends on the port setting in the FTP site. Generally “21” is used.

□ Setting up FTP Server

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

1) Enable FTP Server

Select whether the FTP server is enabled or disabled. Select Enable to enable the following functions.

- FTP printing
- Reading/writing the address book data using the Address Book Viewer
- Backing up/Restoring the e-Filing data using the e-Filing Backup/Restore Utility

2) Enable SSL

Select whether the SSL (Secure Sockets Layer) is enabled or disabled for the FTP server.

Notes

- To enable SSL, you must create a self-signed certificate or import a server certificate in Security Service. If the self-signed certificate is not created or a server certificate is not imported, the SSL will not work correctly. For Windows Vista, you need to import certificates also to the client PC.
 - 📖 P.146 “Setting up Security Service”
 - 📖 P.362 “Installing Certificates for a Client PC”
- Not all operating systems support SSL for all protocols.

3) Default Port Number

Enter the port number for the FTP server. Generally “21” is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

4) SSL Port Number

Enter the port number that is used to access this equipment using FTP with SSL. Generally “990” is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

□ 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 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. If you have changed the setting of the [Location] field on the [Device] tab page, turn the power of this equipment and then back ON, so that the "printer-location" information of SLP will be overwritten with a new one.

The screenshot shows the 'SLP Session' configuration window. On the left, there is a vertical list of three items: 1) 'Enable SLP', 2) 'TTL', and 3) 'Scope'. To the right of these items are the corresponding configuration fields: a dropdown menu for 'Enable SLP' (currently set to 'Disable'), a text box for 'TTL' (containing the value '8'), and an empty text box for 'Scope'. At the top of the window, there are 'OK' and 'Cancel' buttons, and a message that reads: 'Selecting 'Save' in the Main Window is required to Save the new settings.'

1) Enable SLP

Select whether SLP service is enabled or disabled.

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".

Tips

- More than one group can be entered for [Scope] by separating them with a comma.
- Characters () \ ! < = > ~ ; * + cannot be entered in this field.
- 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).

❑ Setting up SNMP Network Service

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

1) Enable SNMP V1/V2

Select whether the SNMP V1/V2 monitoring with MIB is enabled or disabled. This must be enabled to allow users to connect using TopAccessDocMon, TWAIN driver, File Downloader, or the Address Book Viewer.

2) Read Community

Enter the SNMP read community name for the SNMP access.

Note

If you specify a community name other than “public” for the Read Community, the applications that use MIB (TopAccessDocMon, TWAIN driver, File Downloader, and Address Book Viewer) will be unavailable. The SNMP communication of the printer driver also will be unavailable, so that obtaining the configurations, confirming the department code, and obtaining the available boxes in e-Filing will be disabled.

3) Read Write Community

Enter the SNMP Read Write community name for the SNMP access.

Notes

- If you specify a community name other than “private” for the Read Write Community, the applications that use MIB (TWAIN driver, File Downloader, and Address Book Viewer) will be unavailable. The SNMP communication of the printer driver also will be unavailable, so that the obtaining the configurations, confirming the department code, and obtaining the available boxes in e-Filing will be disabled.
- When you leave the [Read Write Community] option blank, the SNMP communication between the SNMP Browser of the Client computer and this equipment will be disabled.

4) Enable SNMP V3

Select whether SNMP V3 monitoring with MIB is enabled or disabled. This must be enabled to allow users to connect using TopAccessDocMon, TWAIN driver, File Downloader and the AddressBook Viewer.

5) Create SNMP User Information

SNMP user information registered into this equipment is displayed in a list. SNMP user information can be registered, edited, deleted or exported. For the details, see the following:

- 📖 P.143 “Registering or editing SNMP user information”
- 📖 P.144 “Exporting SNMP user information”
- 📖 P.145 “Deleting SNMP user information”

6) Enable SNMP V3 Trap

Select whether SNMP V3 Trap is sent or not.

7) SNMP V3 Trap User Name

Enter an SNMP V3 Trap User Name.

8) SNMP V3 Trap Authentication Protocol

Select an authentication protocol.

- HMAC-MD5—Select this to use HMAC-MD5.
- HMAC-SHA—Select this to use HMAC-SHA.

9) SNMP V3 Trap Authentication Password

Enter an authentication password.

10) SNMP V3 Trap Privacy Protocol

Select a protocol for data encryption.

- None—Select this not to encrypt data.
- CBC-DES—Select this to use CBC-DES.

11) SNMP V3 Trap Privacy Password

Enter a privacy password.

12) Enable Authentication Trap

Select whether to send SNMP Traps when this equipment is accessed using SNMP V1/V2 from a different read community.

13) Enable Alerts Trap

Select whether to send SNMP V1/V2 Traps when an alert condition occurs.

14) IP Trap Address 1 to 10

Enter the IP address where the SNMP Traps will be sent. You can specify up to 10 addresses.

15) IP Trap Community

Enter the trap community name for the IP Traps.

16) IPX Trap Address

Enter the IPX address where the SNMP Traps will be sent.

Note

When you want to use a user name registered in the SNMP V3 User Information list as an SNMP V3 Trap User Name, you must enter the same protocols and passwords registered for the authentication protocol, authentication password (not displayed on the list), privacy protocol and password (not displayed on the list) into the fields such as [SNMP V3 Trap Authentication Protocol], [SNMP V3 Trap Authentication Password], [SNMP V3 Trap Privacy Protocol] and [SNMP V3 Trap Privacy Password]. If they do not match, information registered in the list will be adopted.

Registering or editing SNMP user information

- 1 Click [New] to create new SNMP user information. Click the desired user name on the list to edit SNMP user information already registered.

The screenshot shows the 'SNMP Network Service' configuration window. It has tabs for 'SNMP V1/V2' and 'SNMP V3'. The 'SNMP V3' tab is active. Below the tabs are fields for 'Enable SNMP V1/V2' (set to 'Enable'), 'Read Community' (set to 'public'), 'Read Write Community' (set to 'private'), and 'Enable SNMP V3' (set to 'Disable'). There are buttons for 'New', 'Delete', 'Delete All', and 'Export'. Below these is a table titled 'SNMP V3 User Information' with columns: 'Number', 'User Name', 'Authentication Protocol', 'Privacy Protocol', and 'Permissions Level'. The table contains one entry: '1', 'User001', 'HMAC-MD5', 'None', and 'Read Only'. Below the table are fields for 'Enable SNMP V3 Trap' (set to 'Disable'), 'SNMP V3 Trap User Name', and 'SNMP V3 Trap Authentication Protocol' (set to 'HMAC-MD5').

The Create SNMP User Information page is displayed.

- 2 Select the items below and click [Save].

The screenshot shows the 'Create SNMP User Information' form. It has buttons for 'Save' and 'Cancel'. The form fields are: 'Context Name', 'User Name', 'Authentication Protocol' (set to 'HMAC-MD5'), 'Authentication Password' (masked with '****'), 'Privacy Protocol' (set to 'None'), 'Privacy Password', and 'Permissions Level' (set to 'Read Only'). A red box highlights the 'Authentication Protocol', 'Authentication Password', 'Privacy Protocol', and 'Permissions Level' fields.

Context Name — Context name is displayed.

User Name — Enter a user name within 31 characters.

Authentication Protocol — Select an authentication protocol.

- **HMAC-MD5** — Select this to use HMAC-MD5.
- **HMAC-SHA** — Select this to use HMAC-SHA.

Authentication Password — Enter an authentication password within 31 characters.

Privacy Protocol — Select a protocol for data encryption.

- **None** — Select this not to encrypt data.
- **CBC-DES** — Select this to use CBC-DES.

Privacy Password — Enter a user information password within 31 characters.

Permissions Level — Select a level for permitting access from SNMP users.

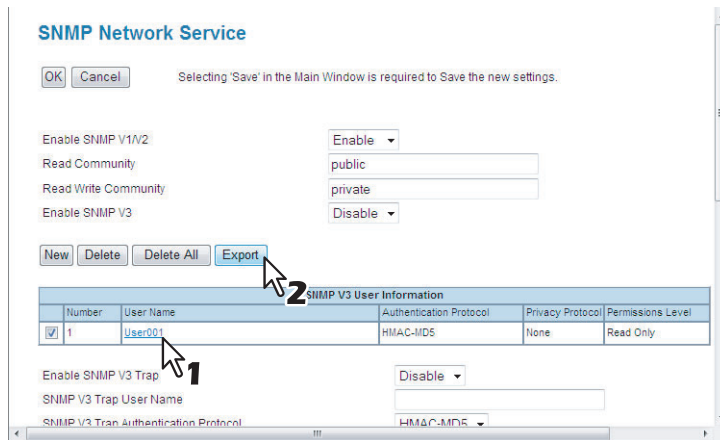
- **Read Only** — Select this to permit only the reading of data.
- **Read Write** — Select this to permit both the reading and writing of data.

The Create SNMP User Information page is closed and the newly created user information is registered on the SNMP user information list.

- 3 Click [OK] to close the SNMP Setup page.
- 4 Click [Save] on the Network submenu page.

Exporting SNMP user information

- 1 Select the check box of SNMP user information that you want to export from the SNMP user information list, and then click [Export].

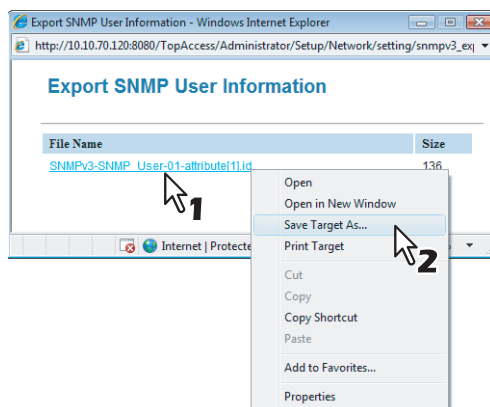


The Export SNMP User Information page is displayed.

Note

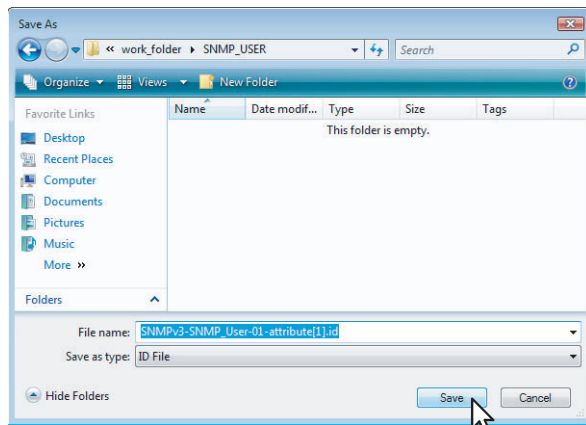
When “Please save the Network settings before exporting the user information” appears, click [Save] on the Network submenu page, and then perform exporting.

- 2 Right-click the link for the file name of user information to be exported, and then select [Save Target As].

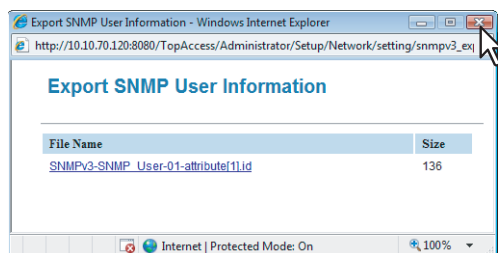


The [Save As] dialog box appears.

- 3 Specify a directory to which the information is to be saved, and then select [Save].



4 Close the Export SNMP User Information page.



Note

Exporting may be unstable if the administrator is accessing this equipment from more than one computer simultaneously in the administrator mode to export information. Be sure that the administrator accesses this equipment from only one computer to export.

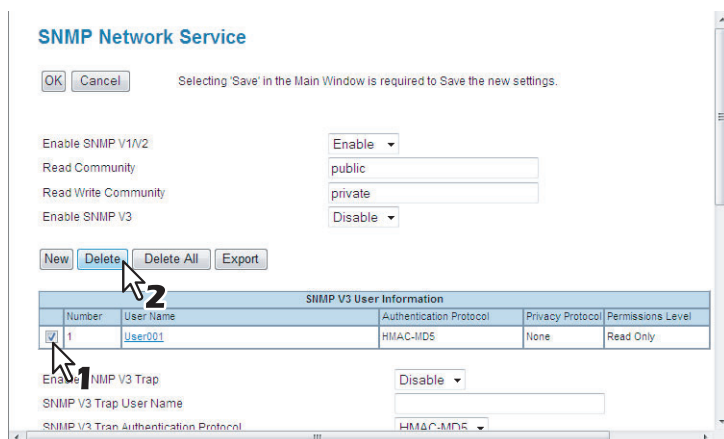
Deleting SNMP user information

1 Select the check box of SNMP user information that you want to delete from the SNMP user information list, and then click [Delete].

7

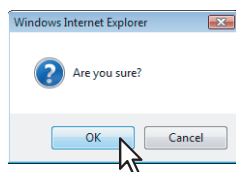
Tip

Click [Delete All] to delete all the SNMP user information.



The confirmation dialog box appears.

2 Click [OK].



The SNMP user information is deleted.

3 Click [OK] to close the SNMP Network Service page.

4 Click [Save] on the Network submenu page.

□ Setting up Security Service

In the Security Service page, you can install a wireless LAN certificate for authentication with the RADIUS server, install and export a server certificate to enable SSL and set up its SCEP (automatic installation), install CA certificate, and install certificates for IEEE802.1X authentication and set up its SCEP.

📖 P.146 “Installing Certificate for wireless LAN”

📖 P.147 “Installing server certificate”

📖 P.157 “Installing user certificate for IEEE802.1X”

📖 P.164 “Installing CA certificate”

Installing Certificate for wireless LAN

When you want to set the IEEE802.1X authentication with the RADIUS server for the optional Wireless LAN Module (GN-1050), you must install user certificate and CA certificate as required.

Notes

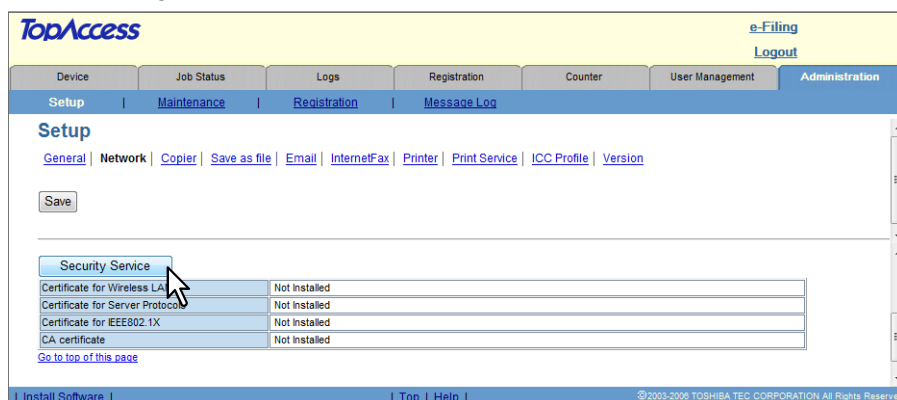
- This equipment supports CA certificate and User certificate that are in the following encoding formats.
 - CA Certificate: DER, BASE64, PKCS#7
 - User Certificate: PKCS#12
- This equipment supports md5RSA and sha1RSA certificate. Make sure to use the certificate in these algorithms.
- When you install the User Certificate in this equipment, it is recommended to connect this equipment and a client computer using a crossing cable for ensuring security.

Tip

For further information about the Wireless LAN, refer to the *GN-1050 Operator's Manual for Wireless LAN Module*.

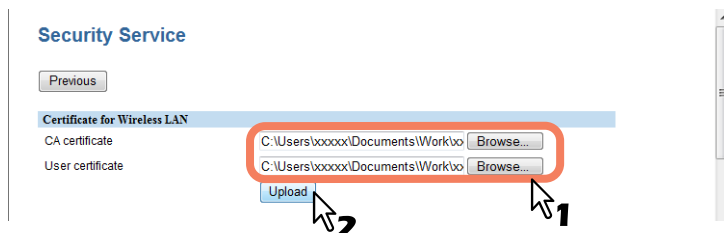
Installing certificate for wireless LAN

1 Click [Security Service].



The Security Service page is displayed.

2 Click [Browse] to select a CA certificate and user certificate file as required. Then click [Upload].

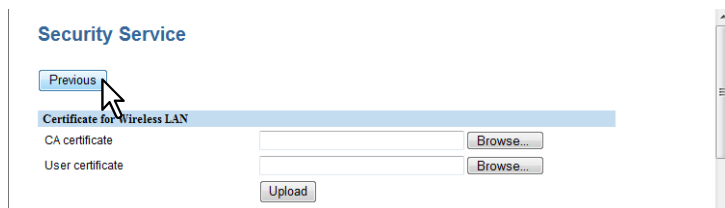


Certificate installation begins.

Note

Wait until the installation is completed and the Security Service page is displayed.

3 Click [Previous] to close the Security Service page.



4 Click [Save] on the Network submenu page.

Installing server certificate

To enable SSL for HTTP setting, FTP server setting, IPP Print Service and Web Services Print, you must install a server certificate for each.

To install these server certificates, you need to create a self-signed certificate, install it from an authentication agency or install it from the CA server. You can also install it automatically from the CA server using SCEP.

📖 P.148 “Creating/exporting a self-signed certificate”

📖 P.150 “Deleting a self-signed certificate”

📖 P.151 “Installing an imported server certificate”

📖 P.153 “Deleting an imported server certificate”

📖 P.154 “Installing server certificate automatically”

📖 P.155 “Deleting server certificate installed automatically”

Tip

When you want to enable SSL for the HTTP Network Service, FTP Server, IPP Print, and Web Service Print Service, the certificates required to install to the equipment and the client PC are as follows:

Use SSL for...	Certificates Required for e-STUDIO			Certificates Required for Client PC		
	Server Certificate		CA Certificate	Self-signed Certificate	Client Certificate	CA Certificate
	Self-signed Certificate	Server certificates installed from authentication agency / CA server				
HTTP, FTP, IPP Print*1	Required	-	-	(Required) *2	-	-
	-	Required	-	-	-	(Required) *2
Web Service Print	-	Required	Required	-	Required	Required
	Required	-	-	Required	-	-

*1 In the HTTP Network Service, FTP Server, and IPP Print, if you create a self-signed certificate for the equipment, you need to install the self-signed certificate to the client PC. If you select to install an imported server certificate to the equipment, also install the CA certificate to the client PC.

*2 For Windows Vista/XP/2000, you can enable SSL by installing certificates only in the equipment. In this case, the following message appears when you operate the system. Select the specified item.

Windows Vista: “There is a problem with this website’s security certificate” appears. Select [Continue to this website (not recommended)].

Windows XP/2000: “Security Alert” appears. Select [Yes].

If you want to further enhance the security, install certificates also in the client PC.

📖 P.164 “Installing a CA certificate”

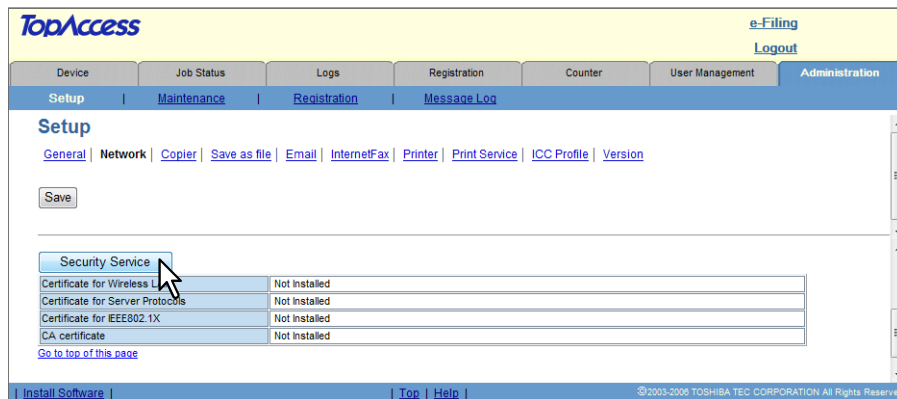
📖 P.362 “Installing Certificates for a Client PC”

Note

When you install the User Certificate in this equipment, it is recommended to connect this equipment and a client computer using a crossing cable for ensuring security.

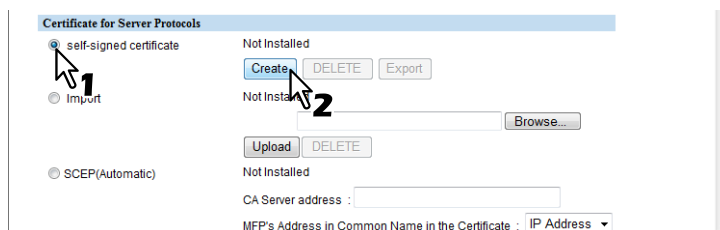
Creating/exporting a self-signed certificate

1 Click [Security Service].



The Security Service page is displayed.

2 Select [self-signed certificate] below [Certificate for Server Protocols] and click [Create].



The Create self-signed certificate page is displayed.

3 Enter the following items and click [Save].



Country Name — Enter the country or region code using two alphabet characters.

State or Province Name — Enter the State or Province Name.

Locality Name — Enter the city or locality name.

Organization Name — Enter the company name or organization name.

Organizational Unit Name — Enter the department name or organization unit name.

Common Name — Enter your name or common name.

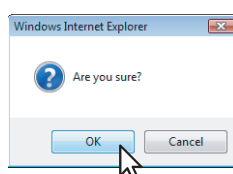
Email Address — Enter your Email address.

Note

Enter the following items in [Common Name] according to the types of certificates.

- Enter the FQDN or the IP address of this equipment for a server certificate (crt).
- Enter the FQDN or the IP address of a client computer that uses a certificate for a client certificate (pfx).

4 Click [OK].



5 A self-signed certificate is created.

Certificate for Server Protocols

☒ self-signed certificate Installed
 Create DELETE Export

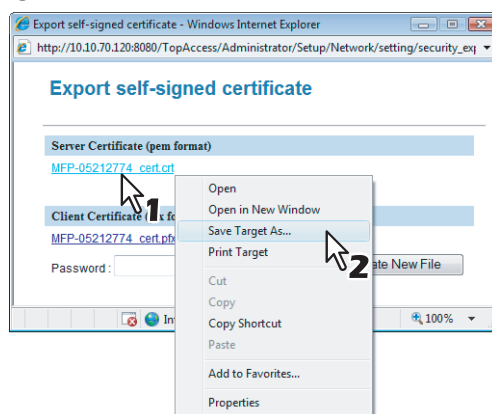
☐ Import Not Installed
 Browse...

☐ SCEP(Automatic) Not Installed
 Upload DELETE

CA Server address : 10.10.70.120
 MFP's Address in Common Name in the Certificate : IP Address

- To export the self-signed certificate to a client computer, click [Export]. The Export Self-Signed Certificate page is displayed. Go to the next step.
- When you want to finish the operation, click [Previous] to close the Security Service page. Then click [Save] on the Network submenu page to save the changes.

6 Right-click the link for the file name of the certificate to be exported in [Server Certificate (pem format)] or [Client Certificate (pfx format)], and then select [Save Target As].

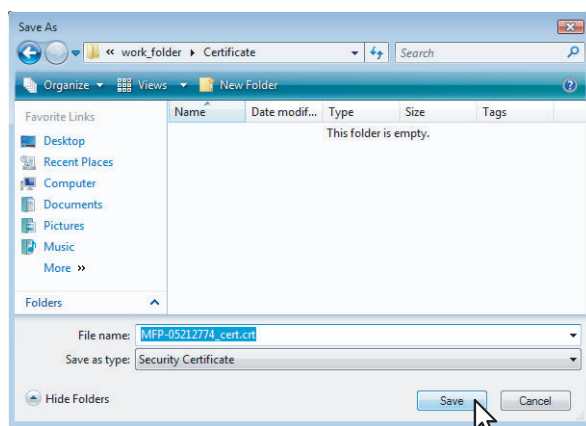


The [Save As] dialog box appears.

Tip

If a client certificate is not installed yet, enter a password in [Password] and then click [Create New File] to create a new certificate.

7 Specify a directory to which the certificate is to be saved and then click [Save].



8 Close the Export Self-Signed Certificate page, and then click [Previous] to close the Security Service page.

Security Service

Previous

Certificate for Wireless LAN

CA certificate Browse...

User certificate Browse...

Upload

9 Click [Save] on the Network submenu page.

Note

You can upgrade the security level of a client computer by installing the exported certificate into the computer. For instructions on how to install it into a client computer, see the following:

📖 P.362 “Installing Certificates for a Client PC”

10 Then you can enable SSL for the following network settings.

📖 P.133 “Setting up HTTP Network Service”

📖 P.139 “Setting up FTP Server”

📖 P.166 “Setting up Web Services Setting”

📖 P.196 “Setting up IPP Print”

Deleting a self-signed certificate

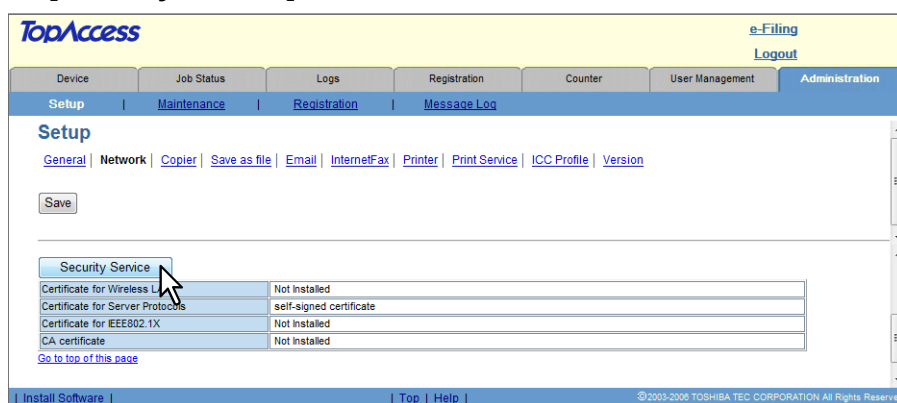
Note

If you delete a self-signed certificate registered to this equipment while SSL for HTTP network service is enabled, access to the TopAccess is refused. In this case, temporarily disable SSL for HTTP network service on the control panel and then access TopAccess. Then enable SSL again.

For HTTP network service, see the following page. For instructions on how to set it on the control panel, refer to the **MFP Management Guide**.

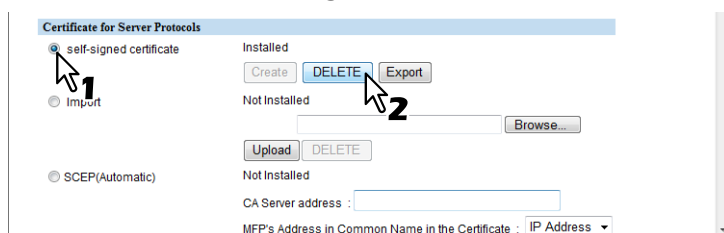
📖 P.133 “Setting up HTTP Network Service”

1 Click [Security Service].



The Security Service page is displayed.

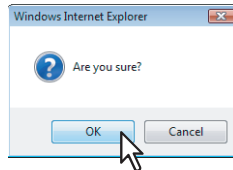
2 Click [DELETE] of [self-signed certificate] in [Certificate for Server Protocols].



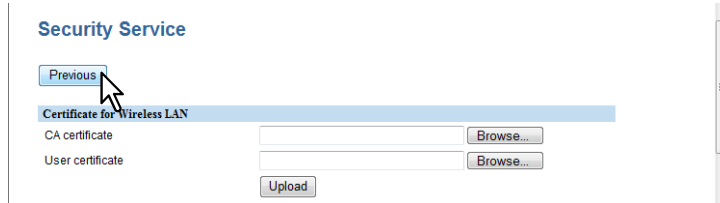
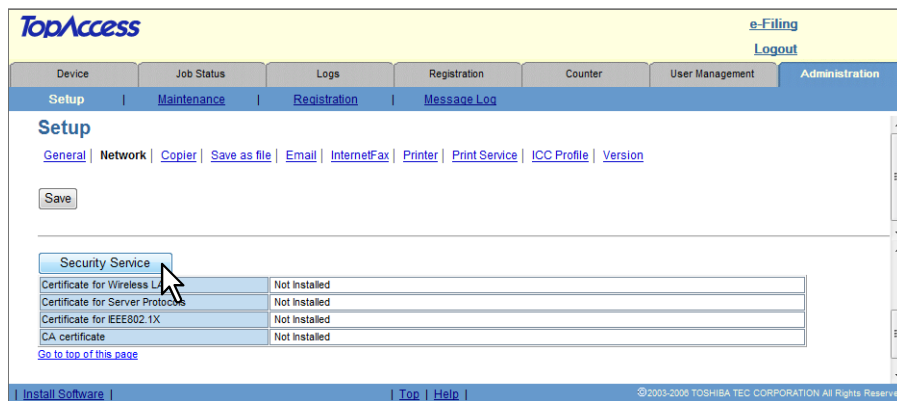
The confirmation dialog box appears.

Note

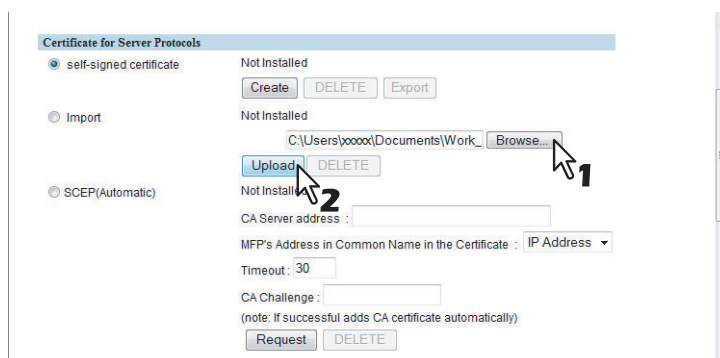
If the self-signed certificate has not been created, you cannot delete the self-signed certificate.

3 Click [OK].

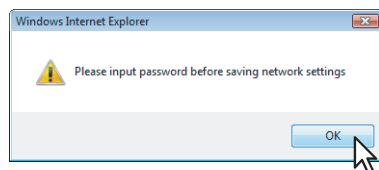
The self-signed certificate is deleted.

4 Click [Previous] to close the Security Service page.**5 Click [Save] on the Network submenu page.****Installing an imported server certificate****7****1 Click [Security Service].**

The Security Service page is displayed.

2 Click [Browse] of [Import] in [Certificate for Server Protocols] to select a server certificate file, and then click [Upload].

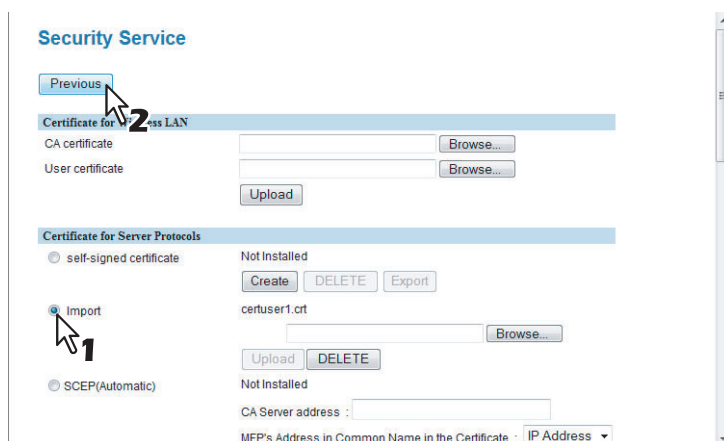
The alert message dialog box appears.

3 Click [OK].

The server certificate is imported.

Tip

This alert message shows that you must enter a password on the control panel of this equipment after you installed the server certificate. The certificate cannot be used unless you enter a password.

4 Select [Import] in [Certificate for Server Protocols], and then click [Previous] to close the Security Service page.**5 Click [Save] on the Network submenu page.****6 Before enabling SSL, you must input the password for the imported server certificate from the touch panel of the equipment.**

For instructions on how to input the password, refer to the following section in the *MFP Management Guide*.

Chapter 2 "SETTING ITEMS (ADMIN)"

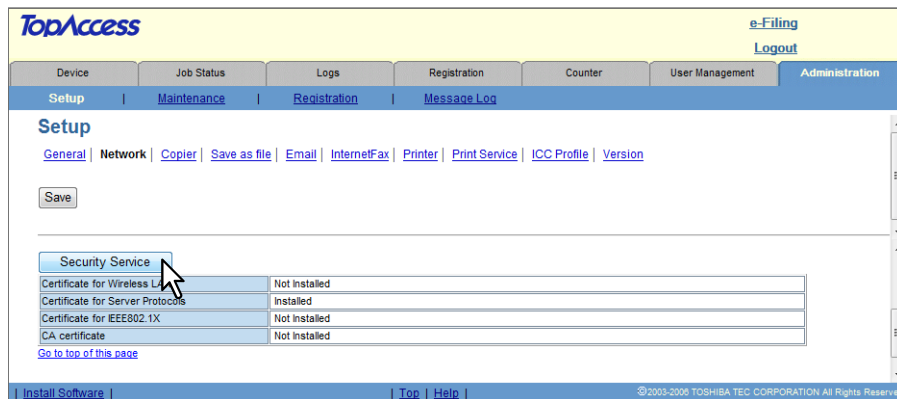
- "Setting Network Functions"
- "Decrypting the user certificate"

7 Then you can enable SSL for the following network settings.

- 📖 P.133 "Setting up HTTP Network Service"
- 📖 P.139 "Setting up FTP Server"
- 📖 P.166 "Setting up Web Services Setting"
- 📖 P.196 "Setting up IPP Print"

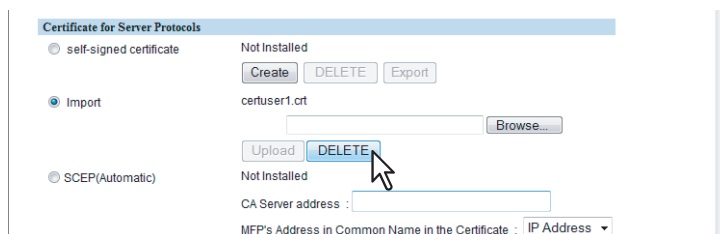
Deleting an imported server certificate

1 Click [Security Service].



The Security Service page is displayed.

2 Click [DELETE] of [Import] in [Certificate for Server Protocols].

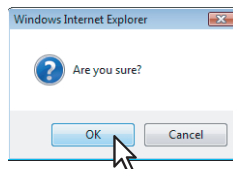


The confirmation dialog box appears.

Note

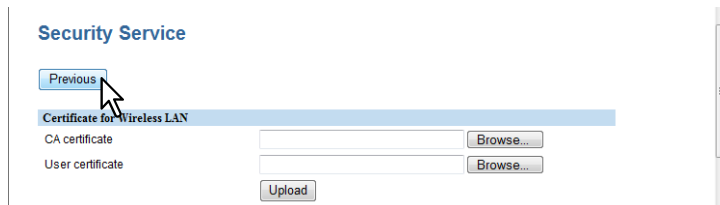
If the server certificate has not been imported, you cannot delete the server certificate.

3 Click [OK].



The server certificate is deleted.

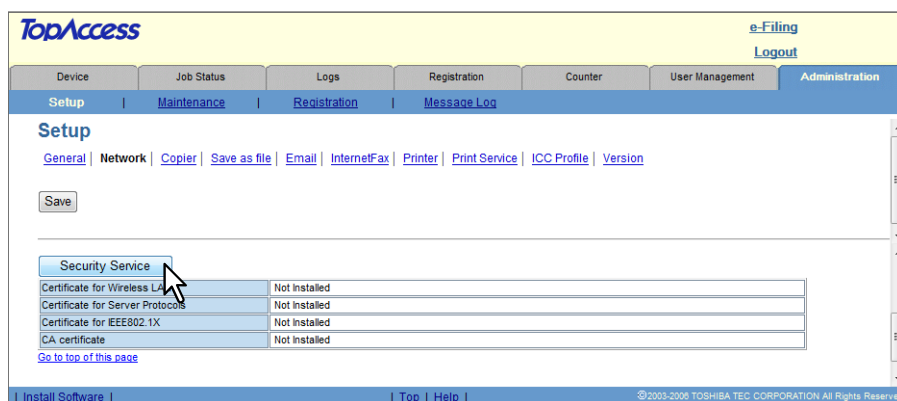
4 Click [Previous] to close the Security Service page.



5 Click [Save] on the Network submenu page.

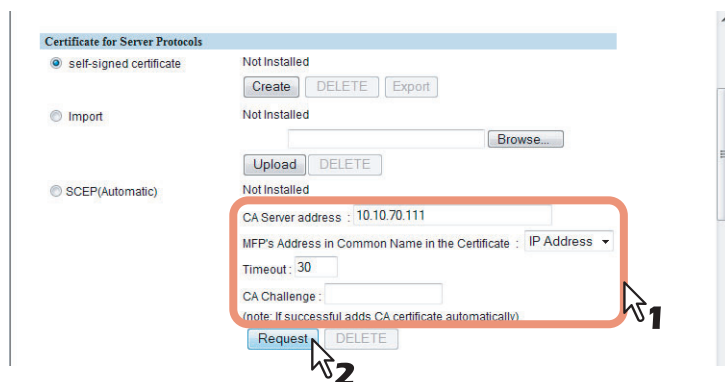
Installing server certificate automatically

1 Click [Security Service].



The Security Service page is displayed.

2 Enter the items below, and then click [Request] in [Certificate for Server Protocols].



CA Server address — Enter the IP address or FQDN of a CA server within 128 characters.

MFP's Address in Common Name in the Certificate — Select whether to use the IP address or FQDN as the address of this equipment to be entered in the [Common Name] box of the certificate.

Timeout — Enter a timeout period for quitting communication when no response is received from the CA server.

CA Challenge — Enter the CA challenge.

Notes

- If FQDN is used in [CA Server address], you need to configure a DNS server and enable DNS settings.
- If [FQDN] is selected in [MFP's Address in Common Name in the Certificate], the IP address of this equipment must be registered in the DNS server.

A server certificate is installed.

3 Select [SCEP(Automatic)] in [Certificate for Server Protocols], and then click [Previous] to close the Security Service page.

Certificate for Server Protocols

☐ self-signed certificate Not Installed
Create DELETE Export

☐ Import Not Installed
Browse...

☒ SCEP(Automatic)
Upload DELETE
certuser1.crt
CA Server address : 10.10.70.111
MFP's Address in Common Name in the Certificate : IP Address
Timeout : 30
CA Challenge :
(note: If successful adds CA certificate automatically)
Request DELETE

Note

A CA certificate is installed automatically as well as a server certificate. If a CA certificate is already installed, delete the existing one by clicking [DELETE] of SCEP in [Certificate for Server Protocols]. Then click [Request] to install a new CA certificate.

4 Click [Save] on the Network submenu page.

5 Then you can enable SSL for the following network settings.

- 📖 P.126 "Setting up LDAP Session"
- 📖 P.133 "Setting up HTTP Network Service"
- 📖 P.134 "Setting up SMTP Client"
- 📖 P.137 "Setting up POP3 Network Service"
- 📖 P.139 "Setting up FTP Server"
- 📖 P.166 "Setting up Web Services Setting"
- 📖 P.196 "Setting up IPP Print"

Deleting server certificate installed automatically

1 Click [Security Service].

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Setup Maintenance Registration Message Log

Setup
General Network Copier Save as file Email InternetFax Printer Print Service ICC Profile Version

Save

Security Service

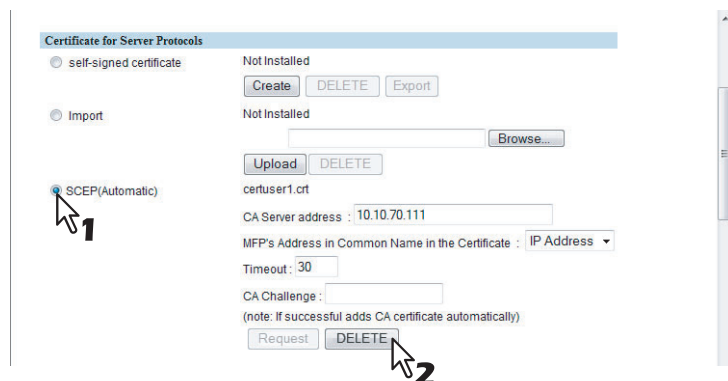
Certificate for Wireless LAN	Not Installed
Certificate for Server Protocols	Installed
Certificate for IEEE802.1X	Not Installed
CA certificate	Installed

[Go to top of this page](#)

Install Software | Top | Help | ©2005-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Security Service page is displayed.

2 Select [SCEP(Automatic)] in [Certificate for Server Protocols], and then click [DELETE].

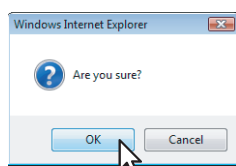


The confirmation dialog box appears.

Notes

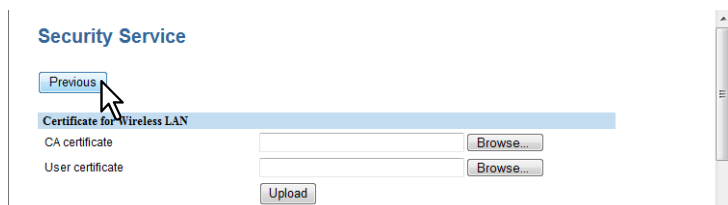
- A CA certificate already installed automatically will be deleted as well as the server certificate.
- Deleting is disabled when no server certificate has been installed automatically.

3 Click [OK].



The server certificate is deleted.

4 Click [Previous] to close the Security Service page.



5 Click [Save] on the Network submenu page.

Installing user certificate for IEEE802.1X

When you set up an IEEE802.1X authentication using the RADIUS server on a wired LAN network, you need to install a user certificate or a CA certificate as required.

Notes

- This equipment supports CA certificate and User certificate that are in the following encoding formats.
 - CA Certificate: DER, BASE64, PKCS#7
 - User Certificate: PKCS#12
- This equipment supports md5RSA and sha1RSA certificate. Make sure to use the certificate in these algorithms.
- When you install the User Certificate in this equipment, it is recommended to connect this equipment and a client computer using a crossing cable for ensuring security.

P.157 "Installing an imported user certificate for IEEE802.1X"

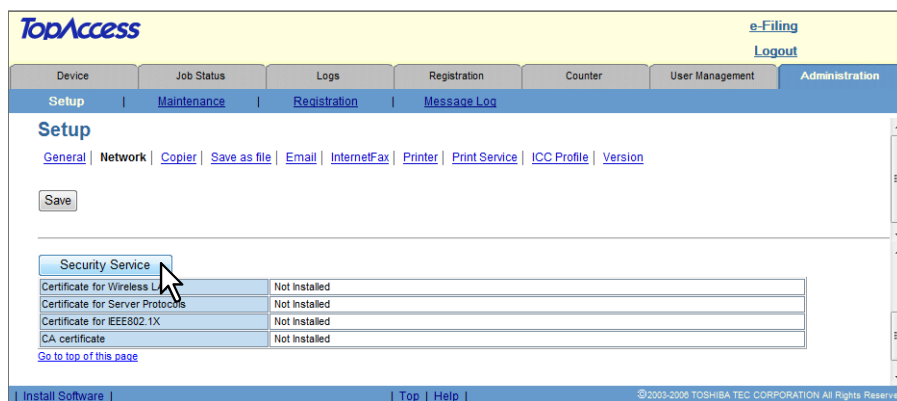
P.159 "Deleting an imported user certificate for IEEE802.1X"

P.160 "Installing user certificate for IEEE802.1X automatically"

P.163 "Deleting user certificate for IEEE802.1X installed automatically"

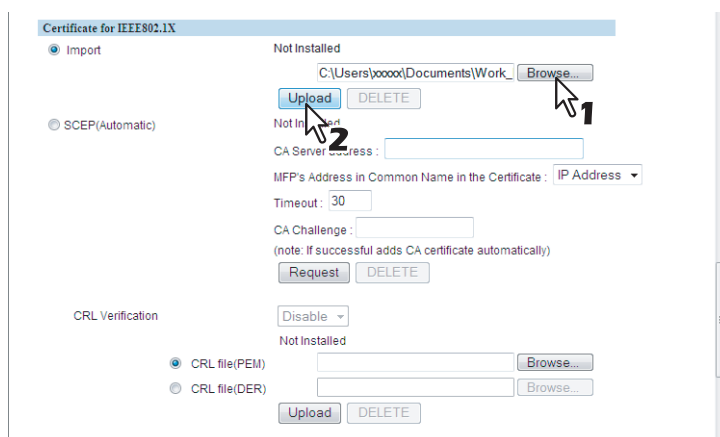
Installing an imported user certificate for IEEE802.1X

1 Click [Security Service].



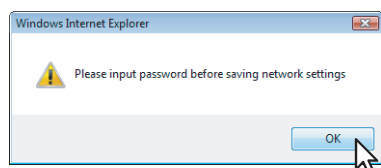
The Security Service page is displayed.

2 Click [Browse] of [Import] in [Certificate for IEEE802.1X] to select a user certificate file for IEEE802.1X, and then click [Upload].



The alert message dialog box appears.

3 Click [OK].

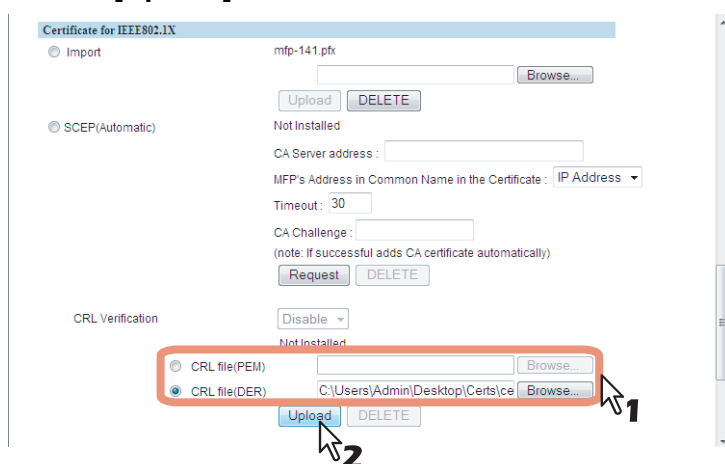


The user certificate for IEEE802.1X is imported.
If you want to enable CRL Verification, go to the next step. If not, go to step 6.

Tip

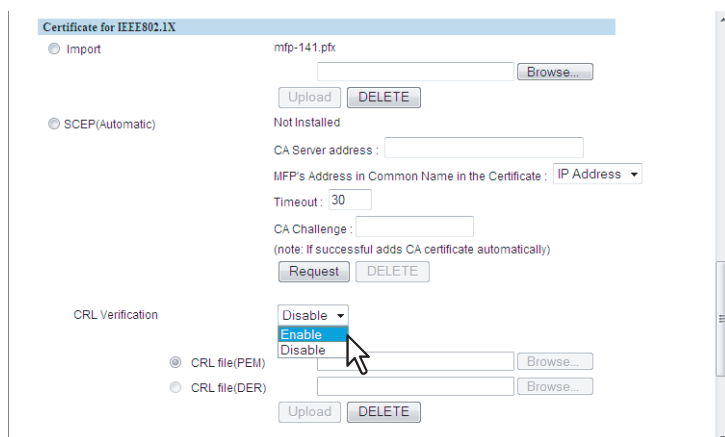
This alert message shows that you must enter a password on the control panel of this equipment after you installed the user certificate for IEEE802.1X. The certificate cannot be used unless you enter a password.

4 Select either of [CRL file (PEM)] and [CRL file (DER)] according to the format of a CRL file that you want to use. Then click [Browse..] to specify a CRL file to be uploaded, and then click [Upload].



The selected CRL file is uploaded.

5 Select [Enable] of [CRL Verification].



6 Select [Import], and then click [Previous] to close the Security Service page.

7 Click [Save] on the Network submenu page.

8 You must enter a password for user certificate on the control panel of this equipment before setting up the IEEE802.1X.

For instructions on how to input the password, refer to the following section in the *MFP Management Guide*.

Chapter 2 "SETTING ITEMS (ADMIN)"

- "Setting Network Functions"
- "Decrypting the user certificate"

9 Then you can enable IEEE802.1X for the following settings.

For instructions on how to enable the IEEE802.1X, refer to the following section in the *MFP Management Guide*.

Chapter 2 "SETTING ITEMS (ADMIN)"

- "IEEE 802.1X Authentication Setting"

Deleting an imported user certificate for IEEE802.1X

Note

You cannot delete a user certificate for IEEE802.1X being used.

1 Click [Security Service].

The Security Service page is displayed.

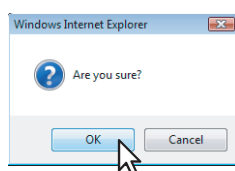
2 Click [DELETE] of [Import] in [Certificate for IEEE802.1X].

The confirmation dialog box appears.

Note

If the user certificate for IEEE802.1X has not been imported, you cannot delete the user certificate for IEEE802.1X.

3 Click [OK].



The user certificate for IEEE802.1X is deleted.

4 Click [Previous] to close the Security Service page.

5 Click [Save] on the Network submenu page.

Installing user certificate for IEEE802.1X automatically

1 Click [Security Service].

Device	Job Status	Logs	Registration	Counter	User Management	Administration
Setup Maintenance Registration Message Log						
General Network Copier Save as file Email InternetFax Printer Print Service ICC Profile Version						
Save						
Security Service						
Certificate for Wireless LAN		Not Installed				
Certificate for Server Protocols		Not Installed				
Certificate for IEEE802.1X		Not Installed				
CA certificate		Not Installed				
Go to top of this page						

The Security Service page is displayed.

2 Enter the items below, and then click [Request] in [Certificate for IEEE802.1X].

CA Server address — Enter the IP address or FQDN of a CA server within 128 characters.

MFP's Address in Common Name in the Certificate — Select whether to use the IP address or FQDN as the address of this equipment to be entered in the [Common Name] box of the certificate.

Timeout — Enter a timeout period for quitting communication when no response is received from the CA server.

CA Challenge — Enter the CA challenge.

Notes

- If FQDN is used in [CA Server address], you need to configure a DNS server and enable DNS settings.
- If [FQDN] is selected in [MFP's Address in Common Name in the Certificate], the IP address of this equipment must be registered in the DNS server.

A server certificate is installed.

If you want to enable CRL Verification, go to the next step. If not, go to step 5.

3 Select either of [CRL file (PEM)] and [CRL file (DER)] according to the format of a CRL file that you want to use. Then click [Browse..] to specify a CRL file to be uploaded, and then click [Upload].

The selected CRL file is uploaded.

4 Select [Enable] of [CRL Verification].

Certificate for IEEE802.1X
☐ Import Not Installed

☒ SCEP(Automatic)
 certuser1.crt
 CA Server address : 10.10.70.111
 MFP's Address in Common Name in the Certificate : IP Address
 Timeout : 30
 CA Challenge :
 (note: If successful adds CA certificate automatically)

 CRL Verification
 Disable
 Enable
 Disable
☒ CRL file(PEM)
☐ CRL file(DER)

5 Select [SCEP(Automatic)] in [Certificate for IEEE802.1X], and then click [Previous] to close the Security Service page.

Certificate for IEEE802.1X
☐ Import Not Installed

☒ SCEP(Automatic)
 certuser1.crt
 CA Server address : 10.10.70.111
 MFP's Address in Common Name in the Certificate : IP Address
 Timeout : 30
 CA Challenge :
 (note: If successful adds CA certificate automatically)

 CRL Verification
 Disable
 certurl.crt
☒ CRL file(PEM)
☐ CRL file(DER)

Note

A CA certificate is installed automatically as well as a user certificate for IEEE802.1X. If a CA certificate is already installed, delete the existing one by clicking [DELETE] of SCEP in [Certificate for IEEE802.1X]. Then click [Request] to install a new CA certificate.

6 Click [Save] on the Network submenu page.

7 Then you can enable IEEE802.1X for the following settings.

For instructions on how to enable the IEEE802.1X, refer to the following section in the *MFP Management Guide*.
 Chapter 2 "SETTING ITEMS (ADMIN)"

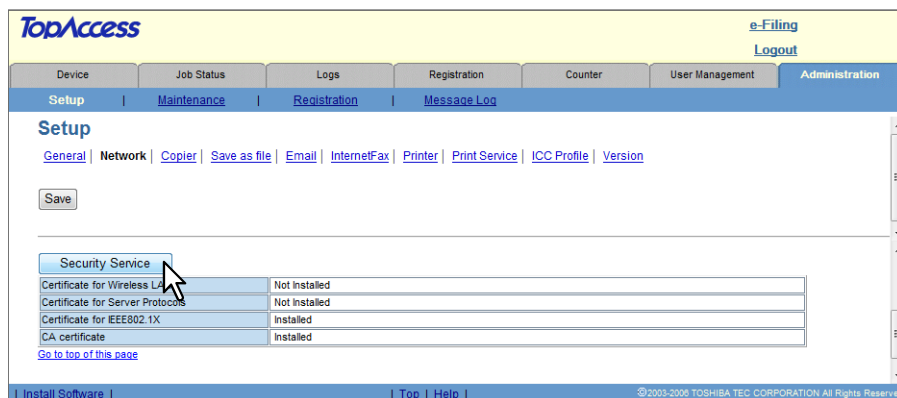
- "IEEE 802.1X Authentication Setting"

Deleting user certificate for IEEE802.1X installed automatically

Note

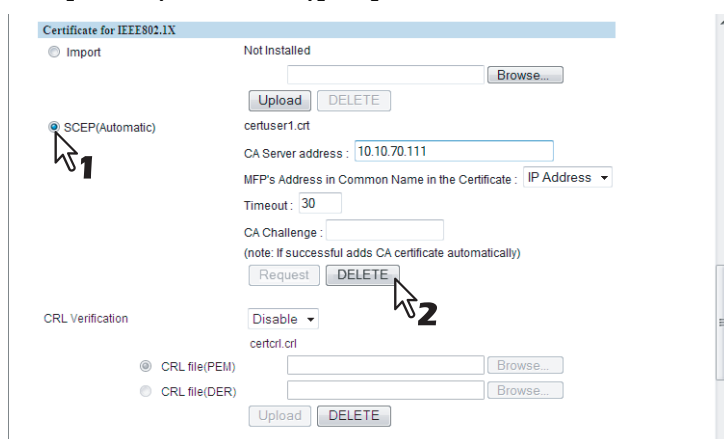
You cannot delete a user certificate for IEEE802.1X being used.

1 Click [Security Service].



The Security Service page is displayed.

2 Select [SCEP(Automatic)] in [Certificate for IEEE802.1X], and then click [DELETE].

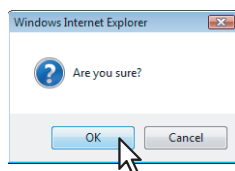


The confirmation dialog box appears.

Notes

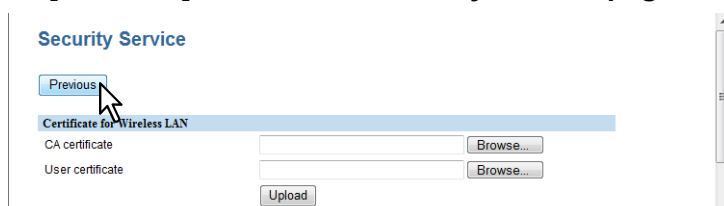
- A CA certificate already installed automatically will be deleted as well as the server certificate.
- Deleting is disabled when no server certificate has been installed automatically.

3 Click [OK].



The user certificate for IEEE802.1X is deleted.

4 Click [Previous] to close the Security Service page.



5 Click [Save] on the Network submenu page.

Installing CA certificate

When you want to enable SSL and verify with a CA certificate for the LDAP Session, SMTP Client, or POP3 Network Service, you must install the CA certificate.

You can install up to 10 CA certificates in this equipment.

📖 P.164 "Installing a CA certificate"

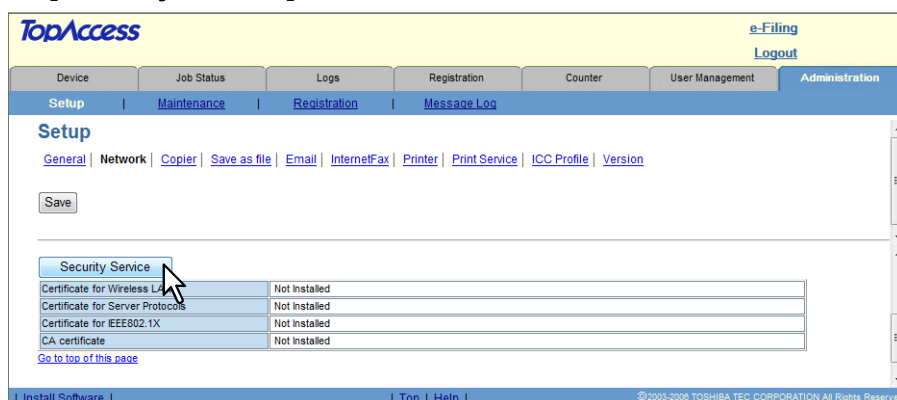
📖 P.165 "Deleting a CA certificate"

Tip

A CA certificate installed using SCEP for server certificates, IPsec certificates or IEEE802.1X certificates will not be counted into the number of registrations. They can be registered separately.

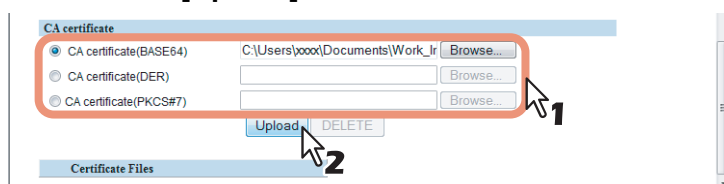
Installing a CA certificate

1 Click [Security Service].



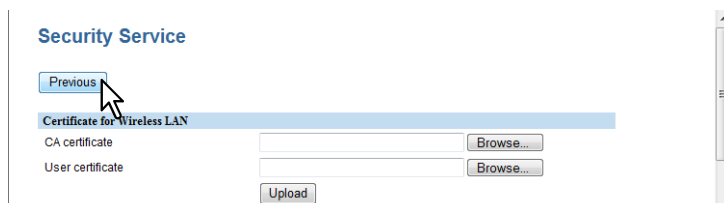
The Security Service page is displayed.

2 Select the encryption of the CA certificate and click [Browse] to select a CA certificate file. Then click [Upload].



The CA certificate is installed.

3 Click [Previous] to close the Security Service page.



4 Click [Save] on the Network submenu page.

5 Then you can enable SSL by selecting [Verify with imported cert] for the following network settings.

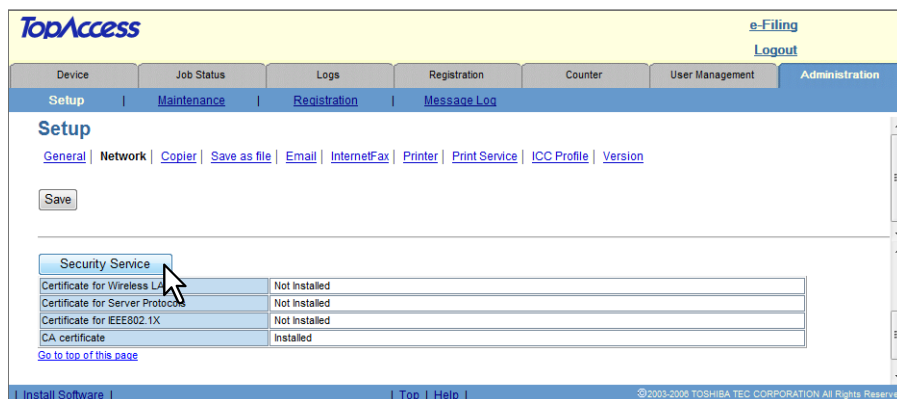
📖 P.126 "Setting up LDAP Session"

📖 P.134 "Setting up SMTP Client"

📖 P.137 "Setting up POP3 Network Service"

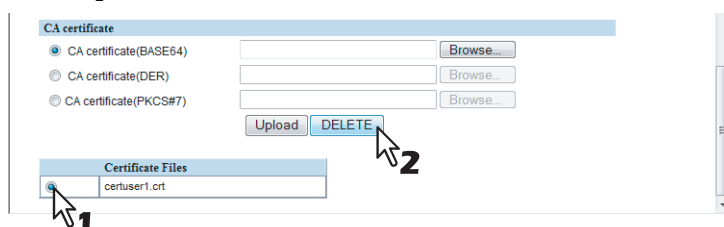
Deleting a CA certificate

1 Click [Security Service].



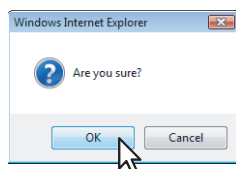
The Security Service page is displayed.

2 Select the CA certificate file that you want to delete in the [Certificate File] list, and click [DELETE].



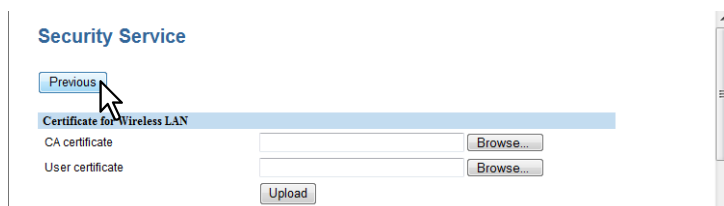
The confirmation dialog box appears.

3 Click [OK].



The self-signed certificate is deleted.

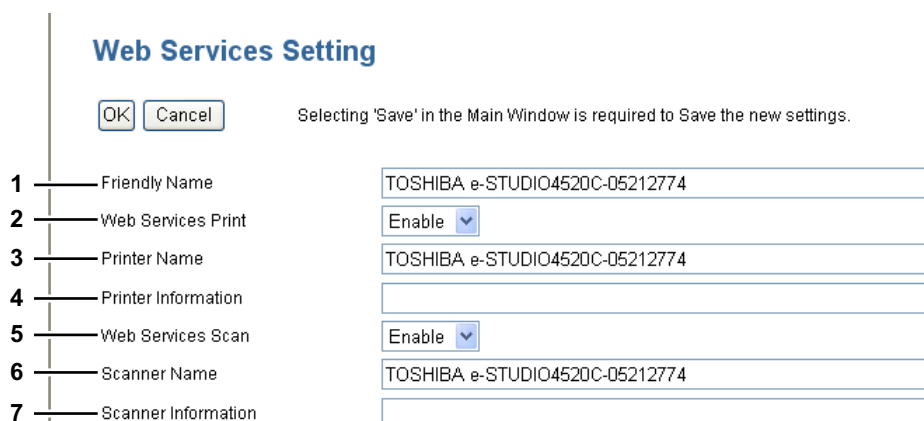
4 Click [Previous] to close the Security Service page.



5 Click [Save] on the Network submenu page.

❑ Setting up Web Services Setting

In Web Services Print and Web Services Scan, you can set the Web services Setting. The Web Services Print operations and Web Services Scan operations are performed on client computers with Windows Vista/Windows 7/Windows Server 2008 through a network.



1) Friendly Name

Assign the friendly name for this equipment.

2) Web Services Print

Select whether the Web Services Print is enabled or disabled.

- **Enable** — Select this to enable the Web Services Print.
- **Enable with web Security** — Select this to enable the Web Services Print using SSL communication.
- **Disable** — Select this to disable the Web Services Print.

Note

To enable Web Services Print using SSL, a certificate must be installed in this equipment or a client computer. For the details, see the following pages:

- 📖 P.146 “Setting up Security Service”
- 📖 P.362 “Installing Certificates for a Client PC”

3) Printer Name

Assign the printer name for this equipment.

4) Printer Information

Assign the printer information for this equipment.

5) Web Services Scan

Select whether the Web Services Scan is enabled or disabled.

6) Scanner Name

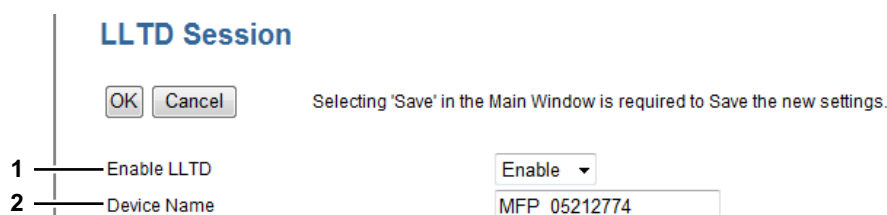
Assign the scanner name for this equipment.

7) Scanner Information

Assign the scanner information for this equipment.

❑ Setting up LLTD Setting

Enable this setting for confirming the device connection status, installing devices or accessing the TopAccess. This setting also allows you to discover the desired device over the local network and view device information such as location, IP address, MAC address or profile on the Network Map under the Windows Vista/Windows 7/Windows Server 2008 environment.



1) Enable LLTD

Select whether the LLTD setting is enabled or disabled.

- **Enable**: Enables the LLTD.

- **Disable:** Disables the LLTD.

2) Device Name

Enter a device name to be displayed on the Network Map. You can enter up to 16 characters for the device name.

□ Setting up Wake Up setting

This section describes how to set network access during the Super Sleep mode. Use this setting for a case such as when you want to recover this equipment from the Super Sleep mode by searching this equipment over a network.

Notes

- This setting is available only for the e-STUDIO455 Series and the e-STUDIO855 Series.
- This setting can be enabled only when [Enable] is selected for the Super Sleep mode setting. If not selected, the Wake Up setting is disabled because this equipment does not enter the Super Sleep mode.

Wake Up Setting

OK

Cancel

Selecting 'Save' in the Main Window is required to Save the new settings.

Please set the protocol for Wake up from Super Sleep mode.
Select up to 4 items.

1

Protocol
☒ ARP
☒ SNMP for IPv4
☐ SNMP for IPv6
☐ SMB
☐ Bonjour
☐ Neighbor Discovery(Link Local Address)
☐ Neighbor Discovery(Manual)
☐ LLMNR
☐ LLTD
☐ SLP
☐ Web Services for IPv4
☐ Web Services for IPv6

1) Protocol

Select protocols to be used for recovering this equipment from the Super Sleep mode. Up to 4 protocols can be selected.

- **ARP**
Select this to enable address resolution when this equipment is used under IPv4 environment.
- **SNMP for IPv4**
Select this to search this equipment over the network with SNMP protocol when Client Utilities is used under IPv4 environment.
- **SNMP for IPv6**
Select this to search this equipment over the network with SNMP protocol when Client Utilities is used under IPv6 environment.
- **SMB**
Select this to enable domain name resolution when NetBIOS name is used under IPv4 environment.
- **Bonjour**
Select this to search this equipment over the network with Bonjour protocol.
- **Neighbor Discovery (Link Local Address) / Neighbor Discovery (Manual)**
Select either of them to enable address resolution when this equipment is used under IPv6 environment.
- **LLMNR**
Select this to enable domain name resolution when NetBIOS name is used under IPv6 environment.
- **LLTD**
Select this to search this equipment over the network with Nmap display when Network Mapper is used.
- **SLP**
Select this to enable service discovery when SLP is used.

- Web Service for IPv4

Select this to search this equipment over the network with WS-Discovery under IPv4 environment.

- Web Service for IPv6

Select this to search this equipment over the network with WS-Discovery under IPv6 environment.

Notes

- The protocol selecting list of the Wake Up setting is made to select the desired protocols regardless of whether the selected protocol is enabled or disabled on each protocol setting. If the selected protocol is disabled on its protocol setting, however, the Wake Up setting is disabled either and therefore this equipment will not be recovered from the Super Sleep mode.
- When no response is returned from this equipment after you access the network even if a protocol selected on this setting is used, retry the access.

Tip

If any of the following protocols is selected, this equipment can be recovered from the Super Sleep mode even if the Wake Up setting is not set.

- IPP
- FTP
- HTTP
- SMTP
- RAW9100
- LPD
- WebService

■ Setting up Copier settings

In the [Copier] submenu in the [Setup] menu, an administrator can configure the copier settings that initially apply to copy operations.

Note

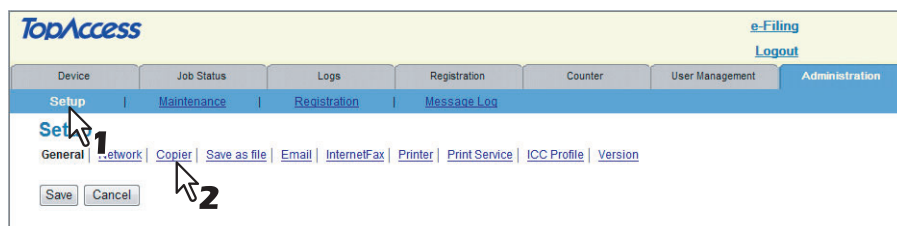
Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting the copier setting

1 Access TopAccess in the administrator mode.

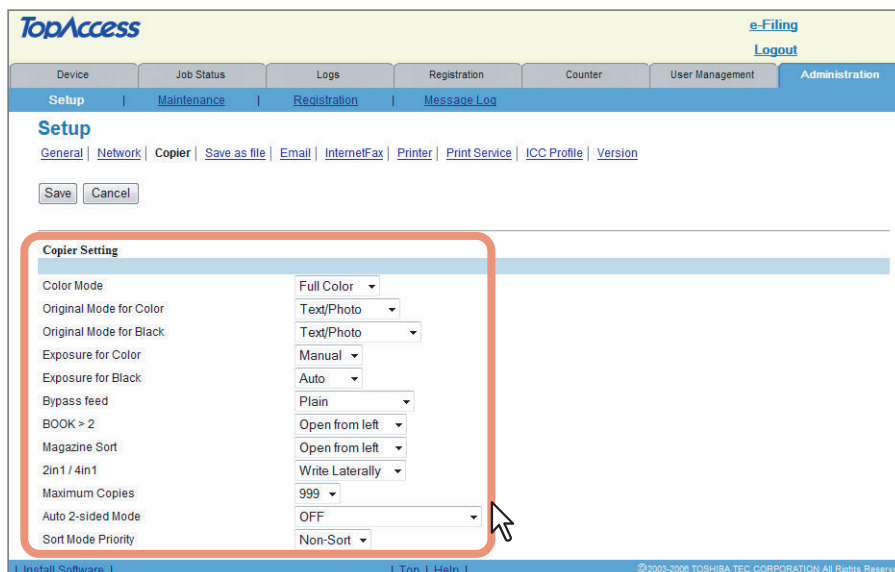
P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Setup] menu and [Copier] submenu.



The Copier submenu page is displayed.

3 In the Copier submenu page, set the copier settings as required.



To set the Copier Settings, see the following:

P.169 "Setting up Copier Setting"

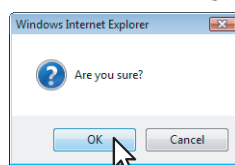
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Copier page immediately after changing the settings and clicking [Save]. If that happens, click the [Copier] submenu to refresh the page.

□ Setting up Copier Setting

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

For the e-STUDIO4520C Series and the e-STUDIO6530C Series

Copier Setting	
1 — Color Mode	Full Color
2 — Original Mode for Color	Text/Photo
3 — Original Mode for Black	Text/Photo
4 — Exposure for Color	Manual
5 — Exposure for Black	Auto
6 — Bypass feed	Plain
7 — BOOK > 2	Open from left
8 — Magazine Sort	Open from left
9 — 2in1 / 4in1	Write Laterally
10 — Maximum Copies	999
11 — Auto 2-sided Mode	OFF
12 — Sort Mode Priority	Non-Sort

For the e-STUDIO855 Series and the e-STUDIO455 Series

Copier Setting	
3 — Original Mode	Text/Photo ▾
5 — Exposure	Auto ▾
6 — Bypass feed	Plain ▾
7 — BOOK > 2	Open from left ▾
8 — Magazine Sort	Open from left ▾
9 — 2in1 / 4in1	Write Laterally ▾
10 — Maximum Copies	999 ▾
11 — Auto 2-sided Mode	OFF ▾
12 — Sort Mode Priority	Non-Sort ▾

1) Color Mode

Select the default color mode for copying.

Note

Only [Black] can be selected when the No Limit Black function is enabled. For the details of the No Limit Black function, refer to the **MFP Management Guide**.

Tip

This setting is available only for e-STUDIO4520C and e-STUDIO6530C Series.

2) Original Mode for Color

Select the default original mode for color originals.

Tip

This setting is available only for e-STUDIO4520C and e-STUDIO6530C Series.

3) Original Mode for Black

Select the default original mode for black and white originals.

Tip

[Original Mode for Black] is displayed as [Original Mode] on the TopAccess menu of the e-STUDIO855 Series and the e-STUDIO455 Series.

4) Exposure for Color

Select the type of image density for color copies.

- **Auto** — Select this to set the Auto mode as the default exposure for color copy. The Auto mode automatically detects the density of the original to make copies at the optimum exposure.
- **Manual** — Select this to set the Manual mode as the default exposure for color copy. The manual mode allows you to manually specify the density of the original.

Tip

This setting is available only for e-STUDIO4520C and e-STUDIO6530C Series.

5) Exposure for Black

Select the type of image density for black and white copies.

- **Auto** — Select this to set the Auto mode as the default exposure for black and white copies. The Auto mode automatically detects the density of the original to make copies at the optimum exposure.
- **Manual** — Select this to set the Manual mode as the default exposure for black and white copies. The manual mode allows you to manually specify the density of the original.

Tip

[Exposure for Black] is displayed as [Exposure] on the TopAccess menu of the e-STUDIO855 Series and the e-STUDIO455 Series.

6) Bypass feed

Select the default paper type for the Bypass Tray.

7) BOOK > 2

Select the default page arrangement of the book-type originals for Book to 2-sided copies.

- **Open from left** — Select this to copy the booklet originals that are read from a left page.
- **Open from right** — Select this to copy the booklet originals that are read from a right page.

8) Magazine Sort

Select the default page arrangement for magazine sort copies.

- **Open from left** — Select this to create a booklet that can be read from the left page.
- **Open from right** — Select this to create a booklet that can be read from the right page.

9) 2in1/4in1

Select the default page arrangement for 2in1/4in1 copies.

- **Write Laterally** — Select this to copy two pages or four pages from left to right or top to bottom. When the portrait originals are copied using 2in1 or 4in1, this equipment copies them from left to right. When the landscape originals are copied using 2in1 or 4in1, this equipment copies them from top to bottom.
- **Write Vertically** — Select this to copy each two pages or four pages from right to left or top to bottom. When the portrait originals are copied using 2in1 or 4in1, this equipment copies them from right to left. When the landscape originals are copied using 2in1 or 4in1, this equipment copies them from top to bottom.

10) Maximum Copies

Select the maximum numbers of pages that users can specify for copying. You can select either [9999]*, [999], [99], or [9] for the Maximum Copies.

11) Auto 2-sided Mode

Select how the 2-sided mode initially applies to copy settings when originals are set in the Automatic Document Feeder.

- **OFF** — Select this to initially apply [1->1 SIMPLEX] when originals are set in the Automatic Document Feeder.
- **One-sided/Double-sided** — Select this to initially apply [1->2 DUPLEX] when originals are set in the Automatic Document Feeder.
- **Double-sided/Double-sided** — Select this to initially apply [2->2 DUPLEX] when originals are set in the Automatic Document Feeder.
- **User Selection** — Select this to initially display the screen to select the 2-sided mode when originals are set in the Automatic Document Feeder.

12) Sorter Mode Priority

Select the default sort mode for copying.

* This feature is available only for the e-STUDIO6530C Series and the e-STUDIO855 Series.

■ Setting up Fax settings

In the [Fax] submenu in the [Setup] menu, an administrator can configure the fax device settings and the settings that initially apply to fax operations.

Notes

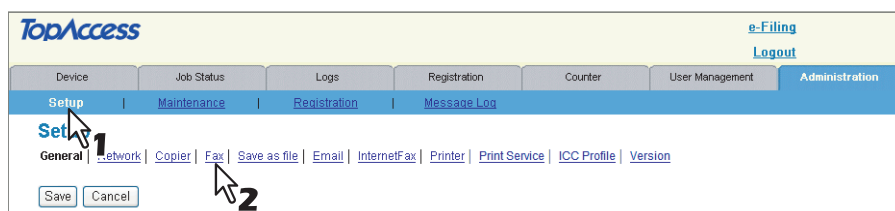
- Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.
- The [Fax] submenu in the [Setup] menu is available only when the optional Fax Unit is installed.

Setting the fax settings

1 Access TopAccess in the administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Setup] menu and [Fax] submenu.



The Fax submenu page is displayed.

3 In the Fax submenu page, set the fax settings as required.

To set the Fax Settings, see the following:

P.173 "Setting up Fax Setting"

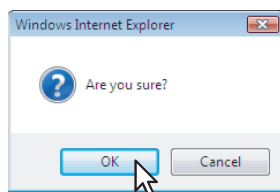
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Fax page immediately after changing the settings and clicking [Save]. If that happens, click the [Fax] submenu to refresh the page.

❑ Setting up Fax Setting

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

Fax Setting	
1 — Terminal ID	
2 — Fax Number	
3 — Line2 Number	
4 — Monitor Volume	0 ☐ ☐ ☐ ☐ ☒ ☐ ☐ ☐ 7
5 — Completion Tone Volume	0 ☐ ☐ ☐ ☐ ☒ ☐ ☐ ☐ 7
6 — Reception Mode	Auto ▼
7 — Dial Type	DP ▼
8 — Dial Type(Line 2)	DP ▼
9 — Line-2 Mode	Rx Only (Timer) ▼ START : END : Standard ▼
10 — Resolution	Text ▼
11 — Original Mode	☒ Auto ☐ ☐ ☐ ☐ ☐ [] ☐ ☐ ☐ ☐ ☒
12 — Exposure	ON ▼
13 — TTI	OFF ▼
14 — RTI	ON ▼
15 — ECM	ON ▼
16 — Discard	ON ▼
17 — Reduction	ON ▼
18 — Duplex Print	OFF ▼
19 — Rotate Sort	OFF ▼
20 — Recovery Transmit	OFF ▼
	Stored Time 6 ▼
21 — Journal Auto Print	ON ▼
22 — Memory Transmission Report	ON ERROR(Print 1st Page Image) ▼
23 — Multi Transmission Report	ON ERROR(Print 1st Page Image) ▼
24 — Polling Report	ON ERROR ▼
25 — Relay Originator	Always(Print 1st Page Image) ▼

- 1) **Terminal ID**
Enter the terminal ID name (company name) to identify this equipment. The name will be printed at the leading edge of all documents transmitted.
- 2) **Fax Number**
Enter the fax number of this equipment. This fax number will be printed at the leading edge of all documents transmitted from Line 1.
- 3) **Line2 Number**
Enter the fax number for Line 2 of this equipment, if installed. This fax number will be printed at the leading edge of all documents transmitted from Line 2.
- 4) **Monitor Volume**
Select the volume of the line monitor during transmission.
- 5) **Completion Tone Volume**
Select the volume of the line monitor when completing the print for received fax.
- 6) **Reception Mode**
Select how this equipment activates when a fax is received.
 - **Auto** — Select this to automatically receive incoming originals when the bell rings. Select this when the line is being used exclusively by the fax transmission.
 - **Manual** — Select this to manually receive incoming originals after pressing the [Start] button on the control panel.
- 7) **Dial Type**
Select the dial type for Line 1.
 - DP** — Select this to use the Dial Pulse type for Line 1.
 - MF** — Select this to use the Multi-frequency type for Line 1.

Note

Setting these items may not be required since they may not be displayed on the screen (it depends on your country or region).

8) Dial Type (Line 2)

Select the dial type for Line 2, if installed.

DP — Select this to use the Dial Pulse type for Line 2.

MF — Select this to use Multi-frequency type for Line 2.

Note

Setting these items may not be required since they may not be displayed on the screen (it depends on your country or region).

9) Line-2 Mode

Select how Line 2 is used, if installed.

- **Tx/Rx** — Select this to use Line 2 for sending and receiving a fax.
- **Rx Only (24 Hour)** — Select this to use Line 2 only for receiving a fax.
- **Rx Only (Timer)** — Select this to use Line 2 only for receiving a fax during specified time. When this is selected, enter the start time and end time that Line 2 is used for only receiving a fax.

10) Resolution

Select the default resolution for sending faxes.

- **Standard** — Select this to set the Standard mode as the default resolution appropriate for the originals in which the text is regular size.
- **Fine** — Select this to set the Fine mode as the default resolution appropriate for the originals in which the text is small or a detailed drawing is contained.
- **Ultra Fine** — Select this to set the Ultra-Fine mode as the default resolution appropriate for the originals in which the text is particularly small or a precision drawing is contained.

11) Original Mode

Select the default image quality mode for sending faxes.

- **Text** — Select this to set the Text mode as the default image quality mode appropriate for sending text originals.
- **Text/Photo** — Select this to set the Text/Photo mode as the default image quality mode appropriate for sending originals containing both text and photos.
- **Photo** — Select this to set the Photo mode as the default image quality mode appropriate for sending photo originals.

12) Exposure

Select the default exposure for sending faxes.

Select [Auto] to automatically apply the ideal contrast according to the original or select the contrast manually in 11 stages.

13) TTI

Select whether to print a transmission header (TTI) to identify the sender of received faxes.

14) RTI

Select whether to print a reception header (RTI) on received faxes to clearly identify the time, date, and page count of received faxes.

15) ECM

Select whether to enable or disable the ECM (Error Correction Mode) to automatically re-send any portion of the document affected by phone line noise or distortion.

16) Discard

Select whether to discard the lower portion of the received fax image if it is larger than the recording paper.

17) Reduction

Select whether to reduce the received fax image if it is larger than the effective printing area of the recording paper.

18) Duplex Print

Select whether to print the received fax images on both sides of the recording paper.

19) Rotate Sort

Select whether to rotate the output direction in the tray for each reception.

20) Recovery Transmit

Select whether to re-transmit a fax after failing the initially specified number of redial attempts. When this is enabled, select the stored time length from 1 to 24 hours.

21) Journal Auto Print

Select whether to automatically print a transmission and reception journal after every transmission completed.

22) Memory Transmission Report

Select how to print a result report after a memory transmission.

- **OFF** — Select this to not print a memory transmission report.
- **Always** — Select this to print a memory transmission report with all page images for each memory transmission completed.

- **ON ERROR** — Select this to print a memory transmission report with all page images only when the memory transmission is not successfully completed.
- **Always(Print 1st Page Image)** — Select this to print a memory transmission report with the 1st page image for each memory transmission completed.
- **ON ERROR(Print 1st Page Image)** — Select this to print a memory transmission report with the 1st page image only when the memory transmission is not successful.

23) Multi Transmission Report

Select how to print a result report after a multi-address transmission.

- **OFF** — Select this to not print a multi-address transmission report.
- **Always** — Select this to print a multi-address transmission report with all page images for each multi-address transmission completed.
- **ON ERROR** — Select this to print a multi-address transmission report with all page images only when the multi-address transmission is not successfully completed.
- **Always (Print 1st Page Image)** — Select this to print a multi-address transmission report with the 1st page image for each multi-address transmission completed.
- **ON ERROR (Print 1st Page Image)** — Select this to print a multi-address transmission report with the 1st page image only when the multi-address transmission is not successful.

24) Polling Report

Select how to print a result report after a multi-polling reception.

- **OFF** — Select this to not print a multi-polling report.
- **Always** — Select this to print a multi-polling report for each multi-polling reception.
- **ON ERROR** — Select this to print a multi-polling report only when the multi-polling reception is not successful.

25) Relay Originator

Select how to print a result report after a relay transmission.

- **OFF** — Select this to not print a relay station report.
- **Always** — Select this to print a relay station report with all page images for each relay transmission completed.
- **ON ERROR** — Select this to print a relay station report with all page images only when the relay transmission is not successful.
- **Always (Print 1st Page Image)** — Select this to print a relay station report with the 1st page image for each relay transmission completed.
- **ON ERROR (Print 1st Page Image)** — Select this to print a relay station report with the 1st page image only when the relay transmission is not successful.

■ Setting up Save as file settings

In the [Save as file] submenu in the [Setup] menu, an administrator can configure the Save as file settings that apply to the Save as file operations. An administrator also configures the Save as file settings that apply to the Save as file operation using the N/W-Fax driver.

Note

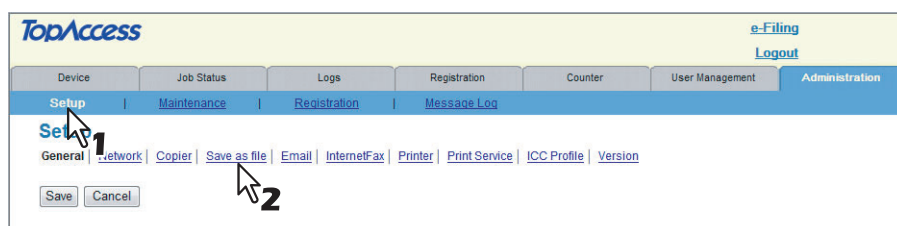
Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting the Save as file settings

1 Access TopAccess in the administrator mode.

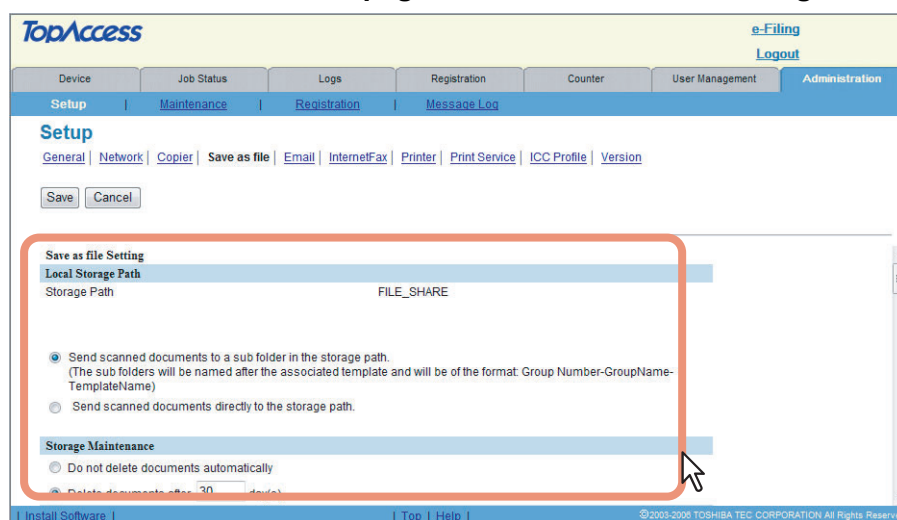
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [Save as file] submenu.



The Save as file submenu page is displayed.

3 In the Save as file submenu page, set the Save as file settings as required.



In the Save as file submenu page, you can set the following:

- P.177 “Setting up Local Storage Path”
- P.177 “Setting up Storage Maintenance”
- P.178 “Setting up Destination”
- P.178 “Setting up Folder Name”
- P.179 “Setting up Format”
- P.179 “Setting up Single Page Data Saving Directory”
- P.180 “Setting up File Composition”
- P.180 “Setting up User Name and Password at User Authentication for Save as File”
- P.180 “Setting up Searching Interval”
- P.181 “Setting up Remote 1 and Remote 2”
- P.182 “Setting up N/W-Fax Destination”
- P.182 “Setting up N/W-Fax Folder”

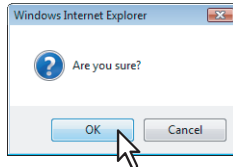
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Save as file page immediately after changing the settings and clicking [Save]. If that happens, click the [Save as file] submenu to refresh the page.

7

□ Setting up Local Storage Path

You can see the folder path where files are stored by the Save as file to local folder.

- Local Storage Path**
- 1 — Storage Path FILE_SHARE
 - 2 — ☒ Send scanned documents to a sub folder in the storage path.
(The sub folders will be named after the associated template and will be of the format: Group Number-GroupName-TemplateName)
 - 3 — ☐ Send scanned documents directly to the storage path.

1) Storage Path

This displays the local storage path where files are stored when files are saved to the local folder by the Save as file functions.

2) Send scanned documents to a sub folder in the storage path.

Select this to save the files in the sub folder that is named as "Group Number-Group Name-Template Name".

3) Send scanned documents directly to the storage path.

Select this to save the files directly in the storage path.

□ Setting up Storage Maintenance

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

Note

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

- Storage Maintenance**
- 1 — ☐ Do not delete documents automatically
 - 2 — ☒ Delete documents after day(s)

1) Do not delete documents automatically

Select this to delete files stored in the local folder manually.

2) Delete documents after [] day(s)

Select this to automatically delete files stored in the local folder after a specified number of days. When this is selected, enter the number of days that the files are to remain.

□ Setting up Destination

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

- Destination**
- 1 — ☐ Do not allow any network folder to be used as a destination
 - 2 — ☒ Use Network Folder Destination
 - 3 — Default file path Remote 1

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

When this is selected, users can only save a file in the local folder or USB media.

2) Use Network Folder Destination

When this is selected, set the Remote 1 and Remote 2 settings to specify how users can select the network folders for Save as file destinations.

Note

When you select [Use Network Folder Destination], make sure that both [Remote 1] and [Remote 2] are set properly. For example, even if you want to specify only Remote 1, you must select [Allow user to select network folder to be used as a destination] for Remote 2. When you select [Use Network Folder Destination], [Allow the following network folder to be used as a destination] is initially selected for both Remote 1 and Remote 2 and other boxes are left blank. If you do not change the settings, an error message asking you to enter the required items to complete the setup will be displayed.

3) Default file path

Select the destination that will be set as the default destination when performing Save as file from the touch panel.

□ Setting up Folder Name

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

- Folder Name**
- 1 — Folder Name Setting Disable

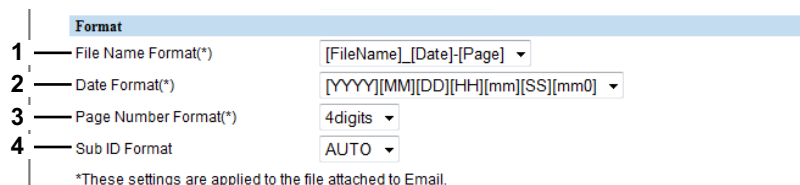
1) Folder Name Setting

Select additional information of the name of a folder created when you save files.

- **Disable** — Select this not to add any information.
- **Add MachineName** — Select this to add the NetBIOS name of this equipment.
- **Add UserName** — Select this to add a user name set in user authentication.

□ Setting up Format

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



Format

1 — File Name Format(*) [FileName]_[Date]-[Page] ▼

2 — Date Format(*) [YYYY][MM][DD][HH][mm][SS][mm0] ▼

3 — Page Number Format(*) 4digits ▼

4 — Sub ID Format AUTO ▼

*These settings are applied to the file attached to Email.

1) File Name Format

Select the format of the file name. Information such as file name, date and time or page number is added according to the selected format. The added information will also be applied to file names attached to Emails.

2) Date Format

Select how you add "date and time" of the file name selected in [File Name Format]. The added information will also be applied to file names attached to Emails.

- [YYYY][MM][DD][HH][mm][SS] — Year (4 digits), month, day, hour, minute and second are added.
- [YY][MM][DD][HH][mm][SS] — Year (2 digits), month, day, hour, minute and second are added.
- [YYYY][MM][DD] — Year (4 digits), month, and day are added.
- [YY][MM][DD] — Year (2 digits), month, and day are added.
- [HH][mm][SS] — Hour, minute and second are added.
- [YYYY][MM][DD][HH][mm][SS][mm0] — Year (4 digits), month, day, hour, minute, second and random number (2 digits and "0") are added.

3) Page Number Format

Select the number of digits of a page number applied to "Page" of the file name selected in [File Name Format] from 3 to 6. The added information will also be applied to file names attached to Emails.

4) Sub ID Format

This equipment automatically adds a sub ID (identification number) to the name of a file that you are saving the same file name exists. You can select the number of digits of this sub ID from 4 to 6 or [AUTO]. [AUTO] is selected by default. If [AUTO] is selected, a sub ID (4 to 6 digits, selected randomly) is added according to the status of the file name.

□ Setting up Single Page Data Saving Directory

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



Single Page Data Saving Directory

1 — ☒ Save under a subfolder

2 — ☐ Save without creating a subfolder

1) Save under a subfolder

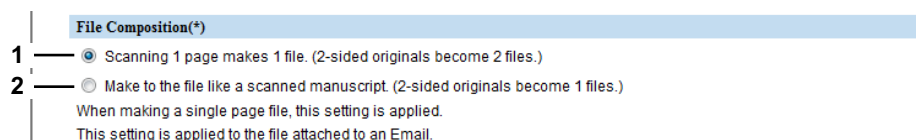
A subfolder is created in a specified directory and you can save the file into it.

2) Save without creating a subfolder

A subfolder is not created and the file is saved in a specified directory.

□ Setting up File Composition

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



File Composition(*)

1 — ☒ Scanning 1 page makes 1 file. (2-sided originals become 2 files.)

2 — ☐ Make to the file like a scanned manuscript. (2-sided originals become 1 files.)

When making a single page file, this setting is applied.
This setting is applied to the file attached to an Email.

1) Scanning 1 page makes 1 file. (2-sided originals become 2 files.)

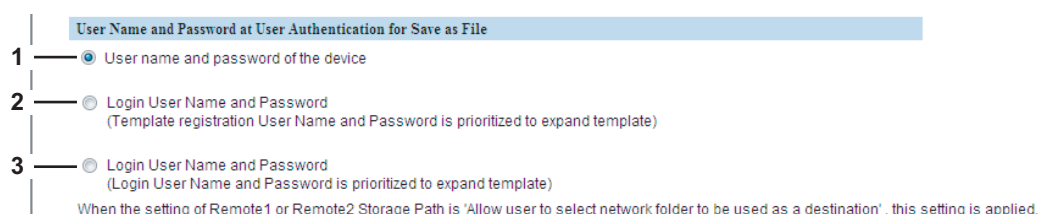
When 1 page of an original is scanned, the scanned data are saved as 1 file. When you scan 1 sheet of 2-sided original, for example, the data of its front side are saved as 1 file and those of its back side are also saved as 1 file.

2) Make to the file like a scanned manuscript. (2-sided originals become 1 files.)

When 1 page of an original is scanned, the scanned data are saved as 1 file. When you scan 1 sheet of 2-sided original, for example, the data of both front and back sides (= 2 pages) are saved as 1 file.

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

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



User Name and Password at User Authentication for Save as File

1 — ☒ User name and password of the device

2 — ☐ Login User Name and Password
(Template registration User Name and Password is prioritized to expand template)

3 — ☐ Login User Name and Password
(Login User Name and Password is prioritized to expand template)

When the setting of Remote1 or Remote2 Storage Path is 'Allow user to select network folder to be used as a destination', this setting is applied.

1) User name and password of the device

User names and passwords being logged in will not be applied. Enter [LOGIN USER NAME] and [PASSWORD] as required when scanning originals.

2) Login User Name and Password (Template registration User Name and Password is prioritized to expand template)

A user name and a password being logged in will be automatically applied. When a template is used, a user name and a password registered in this template will be automatically applied.

3) Login User Name and Password (Login User Name and Password is prioritized to expand template)

A user name and a password being logged in will be automatically applied. When a template is used, the user name and password being logged in will be applied.

□ Setting up Searching Interval

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



Searching Interval

1 — Deleting Expired File Hours(s)

This setting is applied to the e-Filing document.

1) Deleting Expired File [] Hours(s)

This equipment searches expired files every time a specified period of time has passed. The period can be selected from 1 to 24 hours. 12 hours is set by default.

Tip

You can set the expiration date of each file in the "FILE_SHARE" folder or whether to delete expired files or not using the items below.

 P.177 "Setting up Storage Maintenance"

□ Setting up Remote 1 and Remote 2

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

Note

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

Remote 1

- 1 — ☒ Allow the following network folder to be used as a destination
- 2 — Protocol ☒ SMB ☐ FTP ☐ NetWare IPX/SPX ☐ NetWare TCP/IP
- 3 — Server Name
- 4 — Port Number(Command)
- 5 — Network Path
- 6 — Login User Name
- 7 — Password Retype Password
- 8 —
- 9 — ☐ Allow user to select network folder to be used as a destination

1) Allow the following network folder to be used as a destination

Select this to restrict users to select only the network folder that you have specified. Otherwise, select [Allow user to select network folder to be used as a destination].

2) Protocol

Select the protocol to be used for uploading a file to the network folder.

- **SMB** — Select this to send a file to the network folder using the SMB protocol.
- **FTP** — Select this to send a file to the FTP server.
- **NetWare IPX/SPX** — Select this to send a file to the NetWare file server using the IPX/SPX protocol.
- **NetWare TCP/IP** — Select this to send a file to the NetWare file server using the TCP/IP protocol.

3) Server Name

When you select [FTP] as the protocol, enter the FTP server name or IP address where a scanned file will be sent. For example, to send a scanned file to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box. You can specify the directory in the [Network Path] box.

When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).

When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.

4) Port Number(Command)

If you select [FTP] as the protocol, enter the port number to be used for controls. Generally “-” is entered for the control port. When “-” is entered, the port number, that is set at [FTP Client] in the [Network] submenu of the [Setup] menu, will be used. Change this option if you want to use another port number.

5) Network Path

Enter the network path to store a file.

When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “user/scanned” folder in the computer named “Client01”, enter “\\Client01\users\scanned”.

When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “user/scanned”.

When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”.

6) Login User Name

Enter the login user name to access an SMB server, an FTP server or a NetWare file server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank.

7) Password

Enter the password to access an SMB server, an FTP server or a NetWare file server, if required. A space can be entered.

8) Retype Password

Enter the same password again for confirmation.

9) Allow user to select network folder to be used as a destination

Select this to allow users to specify a network folder as a destination. Otherwise, select [Allow the following network folder to be used as a destination].

Note

If you want to allow users to specify either Remote 1 or Remote 2, select the one that is not set for the network folder as a destination and select [Allow the following network folder to be used as a destination] of the selected folder.

□ Setting up N/W-Fax Destination

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

N/W-Fax Destination

- 1 — ☒ Do not allow any network folder to be used as a destination
- 2 — ☐ Use Network Folder Destination

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

Select this to not allow any network folders to be used as Save as file destinations for N/W-Faxes documents. When selected, users can only save an N/W-Fax document with the Save as file option enabled to local storage.

2) Use Network Folder Destination

Select this to allow network folders to be used as Save as file destinations for N/W-Fax documents. When selected, set the N/W-Fax Folder settings to specify which network folder to use.

□ Setting up N/W-Fax Folder

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

N/W-Fax Folder

- 1 — Protocol ☒ SMB ☐ FTP ☐ NetWare IPX/SPX ☐ NetWare TCP/IP
- 2 — Server Name
- 3 — Port Number(Command)
- 4 — Network Path
- 5 — Login User Name
- 6 — Password Retype Password
- 7 —

1) Protocol

Select the protocol for uploading an N/W-Fax document to a network folder.

- **SMB** — Select this to send an N/W-Fax document to the network folder using the SMB protocol.
- **FTP** — Select this to send a file to the FTP server.
- **NetWare IPX/SPX** — Select this to send a file to the NetWare file server using the IPX/SPX protocol.
- **NetWare TCP/IP** — Select this to send a file to the NetWare file server using the TCP/IP protocol.

2) Server Name

When you select [FTP] as the protocol, enter the FTP server name or IP address where an N/W-Fax document will be sent. For example, to send an N/W-Fax document to the “ftp://192.168.1.1/user/scanned” FTP folder in the FTP server, enter “192.168.1.1” in this box. You can specify the directory at the [Network Path] box.

When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).

When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.

3) Port Number(Command)

Enter the port number to be used for controls, if you select [FTP] as the protocol. Generally “-” is entered for the control port. When “-” is entered, the port number, that is set at [FTP Client] in the [Network] submenu of the [Setup] menu, will be used. Change this option if you want to use another port number.

4) Network Path

Enter the network path to store an N/W-Fax document.

When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the “users\nw-fax” folder in the computer named “Client01”, enter “\\Client01\users\nw-fax”.

When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the “ftp://192.168.1.1/user/nw-fax” FTP folder in the FTP server, enter “user/nw-fax”.

When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the “sys\scan” folder in the NetWare file server, enter “\sys\scan”.

5) Login User Name

Enter the login user name to access an SMB server, FTP server, or NetWare file server, if required. When you select [FTP] as the protocol, anonymous login is assumed if you leave this box blank.

6) Password

Enter the password to access an SMB server, FTP server, or NetWare file server, if required. The space can be entered.

7) Retype Password

Enter the same password again for a confirmation.

■ Setting up Email settings

In the [Email] submenu in the [Setup] menu, an administrator can configure the Email settings that are needed for Scan to Email operations.

Note

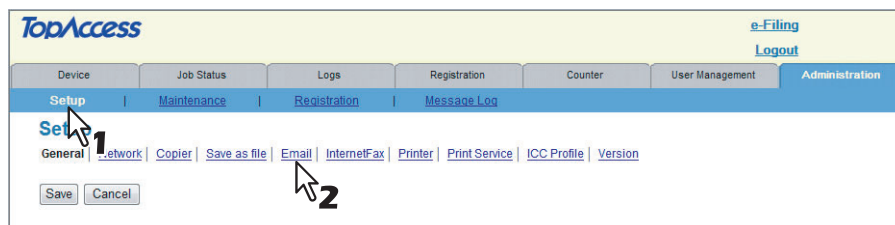
Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting the Email settings

1 Access TopAccess in the administrator mode.

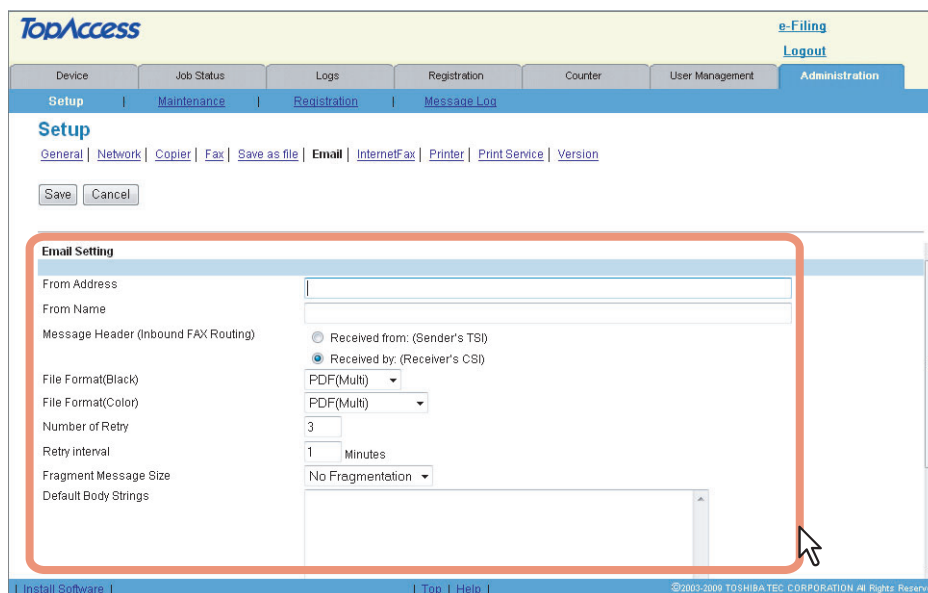
P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Setup] menu and [Email] submenu.



The Email submenu page is displayed.

3 In the Email submenu page, set the Email settings as required.



To set the Email settings, see the following:

P.184 "Setting up Email Setting"

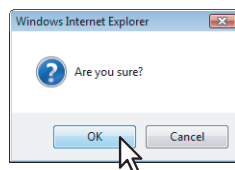
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Email page immediately after changing the settings and clicking [Save]. If that happens, click the [Email] submenu to refresh the page.

□ Setting up Email Setting

You can specify the sender's address, sender's name, subject, file format, fragment message size, and default body strings for the Scan to Email documents.

Email Setting	
1 — From Address	
2 — From Name	
3 — Message Header (Inbound FAX Routing)	☐ Received from: (Sender's TSI) ☒ Received by: (Receiver's CSI)
4 — File Format(Black)	PDF(Multi) v
5 — File Format(Color)	PDF(Multi) v
6 — Number of Retry	3 v
7 — Retry interval	1 Minutes v
8 — Fragment Message Size	No Fragmentation v
9 — Default Subject	☒ Factory Default ☐
10 — Add the date and time to the Subject	Enable v
11 — Subject Transmission	Enable v
12 — Editing of Subject	Enable v
13 — Default Body Strings	
14 — Body String Transmission	Enable v
15 — Address Specifying Method	To/Cc v
16 — Bcc Address Display	OFF v

*As for "File Name Format","Date Format","Page Number Format","File Composition" of the attached file, the setting of the "Save as file" is applied.

1) From Address

Enter the email address of this equipment.

Note

You must enter the email address in the [From Address] box to enable the Scan to Email unless the From Address is being determined automatically by the User Management Setting. For more information about User Management Setting, see the following section.

P.268 "Setting up User Management"

2) From Name

Enter the name of this equipment.

3) Message Header (Inbound FAX Routing)

Select the TTI as the subject for the Inbound Fax routing.

4) File Format (Black)

Select the file format of files to be sent when scanning in black mode.

- **TIFF(Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF(Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF(Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF(Single)** — Select this to save scanned images separately as Single-page PDF files.
- **XPS(Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS(Single)** — Select this to save scanned images separately as Single-page XPS files.

5) File Format (Color)

Select the file format of files to be sent when scanning in color mode.

- **TIFF(Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF(Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF(Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF(Single)** — Select this to save scanned images separately as Single-page PDF files.
- **Slim PDF(Multi)** — Select this to save scanned images as Multi-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image.
- **Slim PDF(Single)** — Select this to save scanned images separately as Single-page slim PDF files. Select this when you give priority to minimizing the file size over the quality of the image.
- **XPS(Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS(Single)** — Select this to save scanned images separately as Single-page XPS files.
- **JPEG** — Select this to save scanned images as JPEG files.

Note

Files saved in an XPS format can be used in Windows Vista/Windows 7/Windows Server 2008 SP1, or Windows XP SP2/Windows Server 2003 SP1 or later versions with Net Framework 3.0 installed.

6) Number of Retry

Enter the number of times to retry sending scanned images when it fails.

7) Retry interval

Enter the interval to retry sending scanned images when it fails.

Note

When the [Number of Retry] and [Retry interval] options are changed, the [Number of Retry] and [Retry interval] options in the Internet Fax settings are also changed.

📖 P.187 "Setting up InternetFax Setting"

8) Fragment Message Size

Select the size for the message fragmentation.

9) Default Subject

Select the subject set by default, or enter the desired one directly in the box, if required.

10) Add the date and time to the Subject

Select whether to add the date and time to the Email subject.

11) Subject Transmission

Select whether to send the Email subject.

12) Editing of Subject

Select whether to enable the editing of the Email subject.

If you select [Disable], users cannot edit the Email subject.

13) Default Body Strings

Enter the body text that will be automatically entered in the [Body] box when users operate Scan to Email from the touch panel. This sets only the default body text, so that it can be changed in each operation by users.

14) Body String Transmission

Select whether or not to send the body text of the Email.

15) Address Specifying Method

Select a method to specify e-mail addresses.

- **To/Cc**—"To" and "Cc" are used as destinations.
- **To/Bcc**—"To" and "Bcc" are used as destinations.

16) Bcc Address Display

Specify how to display the Bcc destination on the Scan Log list, the Scan Job list and the ITU Mailbox list when [To/Bcc] is selected for the [Address Specifying Method] setting above.

- **OFF**—Bcc addresses are not displayed but instead only [Bcc: Destination] is displayed.
- **ON**—Bcc addresses are displayed.

■ Setting up InternetFax settings

In the [InternetFax] submenu in the [Setup] menu, an administrator can configure the Internet Fax settings needed for Internet Fax transmissions.

Note

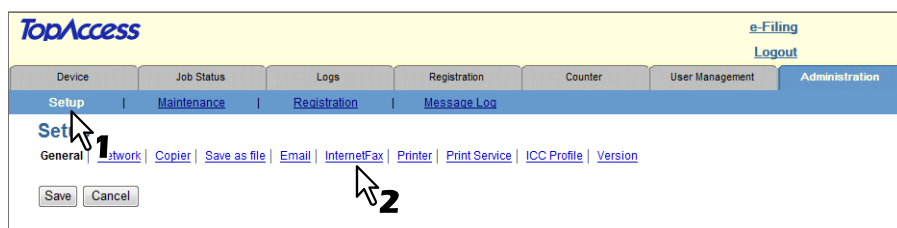
Some settings may not be reflected on the touch panel immediately after saving them. The settings will be updated by pressing the [FUNCTION CLEAR] button on the control panel or after an Auto Clear time period.

Setting the InternetFax settings

1 Access TopAccess in the administrator mode.

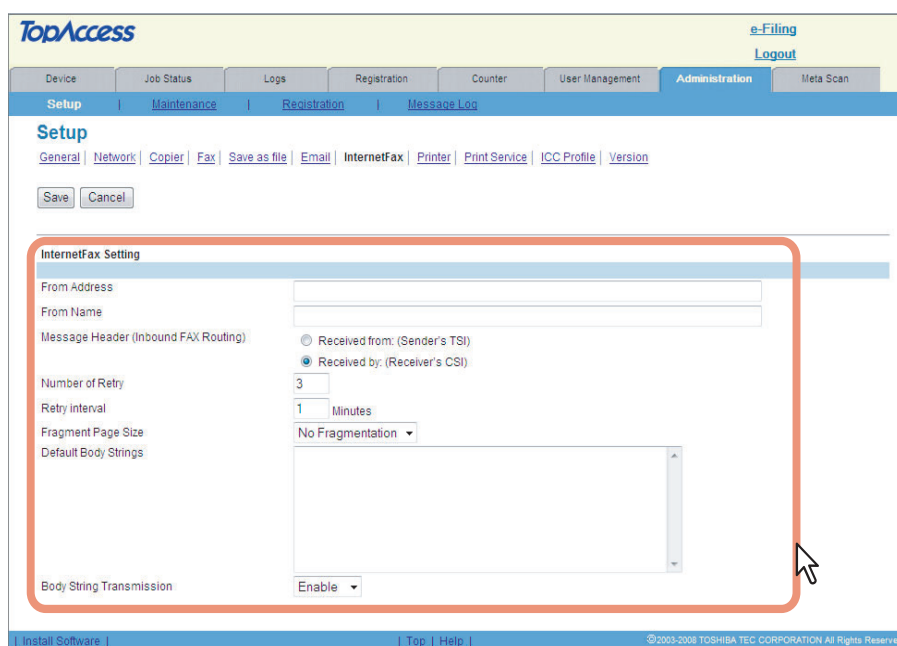
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [InternetFax] submenu.



The InternetFax submenu page is displayed.

3 In the InternetFax submenu page, set the Internet Fax settings as required.



To set the InternetFax Setting, see the following:

P.187 “Setting up InternetFax Setting”

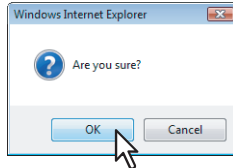
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Internet Fax page immediately after changing the settings and clicking [Save]. If that happens, click the [InternetFax] submenu to refresh the page.

□ Setting up InternetFax Setting

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

InternetFax Setting	
1 — From Address	mfp-04998820@ifax.com
2 — From Name	mfp-04998820
3 — Message Header (Inbound FAX Routing)	☐ Received from: (Sender's TSI) ☒ Received by: (Receiver's CSI)
4 — Number of Retry	3
5 — Retry interval	1 Minutes
6 — Fragment Page Size	No Fragmentation
7 — Default Body Strings	
8 — Body String Transmission	Enable

1) From Address

Enter the email address of this equipment.

Note

You must enter the email address in the [From Address] box to enable the Internet Fax unless the From Address is being determined automatically by the User Management Setting. For more information about User Management Setting, see the following section.

📖 P.268 "Setting up User Management"

2) From Name

Enter the name of this equipment.

3) Message Header (Inbound FAX Routing)

Select TTI to be used as a subject when the received InternetFax is forwarded.

4) Number of Retry

Enter the number of times to retry sending the Internet Faxes when it fails.

5) Retry interval

Enter the interval to retry sending the Internet Faxes when it fails.

Note

When the [Number of Retry] and [Retry interval] options are changed, the [Number of Retry] and [Retry interval] options in the Email settings are also changed.

📖 P.184 "Setting up Email Setting"

6) Fragment Page Size

Select the size for the message fragmentation.

7) 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.

8) Body Strings Transmission

Select whether the body strings will be sent or not.

■ Setting up Printer settings

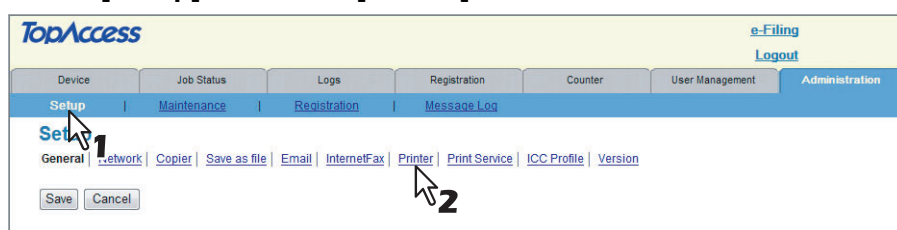
In the [Printer] submenu in the [Setup] menu, an administrator can configure how the printer works and the printer options needed for the raw print jobs.

Setting the printer settings

1 Access TopAccess in the administrator mode.

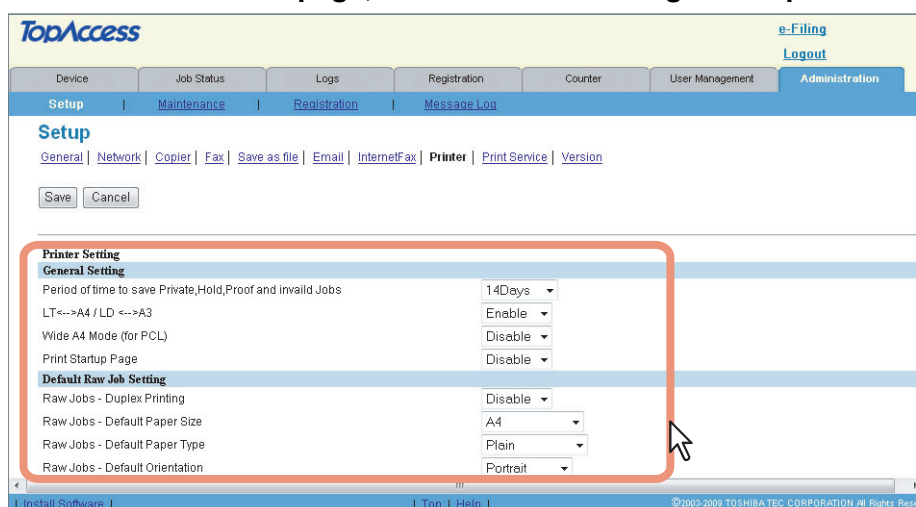
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [Printer] submenu.



The Printer submenu page is displayed.

3 In the Printer submenu page, set the Printer settings as required.



To set the Printer Settings, see the following:

P.189 “Setting up General Setting”

P.190 “Setting up Default Raw Job Setting”

P.191 “Setting up Raw Job Setting”

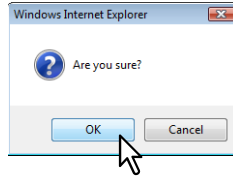
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Printer page immediately after changing the settings and clicking [Save]. If that happens, click the [Printer] submenu to refresh the page.

□ Setting up General Setting

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

General Setting	
1 — Period of time to save Private, Hold, Proof and invalid Jobs	14Days ▾
2 — LT<-->A4 / LD <-->A3	Enable ▾
3 — Wide A4 Mode (for PCL)	Disable ▾
4 — Print Startup Page	Disable ▾

1) Retention period of Private, Hold, Proof and Invalid Jobs

Select a period of time that this equipment retains print jobs in the Private, Hold, Proof, or Invalid queue from 1 hour to 12 hours or from 1 day to 30 days. Select [Indefinite] to retain all jobs in the queues until a user manually deletes them.

2) LT<-->A4 / LD <-->A3

Select whether printing a document intended for one paper size can be printed on paper of a different size. For example, you can print a document set up for Letter size on A4 paper. When disabled, this equipment will prompt users for the correct paper size.

3) Wide A4 Mode (for PCL)

Select whether the width of the printable area of copy paper is widened or not when you are printing PCL print job on A4 paper.
Select [Enable] to widen it for approx. 3.5 mm / 0.14 inch (when in a portrait direction) and approx. 1.5 mm / 0.06 inch (when in a landscape direction). Thus more data can be printed for each line.

4) Print Startup Page

Select whether printing the startup page every time this equipment is powered on. The startup page is the NIC Configuration page. You can also print the startup page from the touch panel manually.

□ Setting up Default Raw Job Setting

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

Tip

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

📖 P.191 “Setting up Raw Job Setting”

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

1) Raw jobs - Duplex Printing

Select whether a raw job will be printed on both sides of the paper.

Note

The [Raw jobs - Duplex Printing] option is available only when the Automatic Duplexer Unit is installed.

2) Raw jobs - Default Paper Size

Select the default paper size that applies to a raw job.

3) Raw jobs - Default Paper Type

Select the default paper type that applies to a raw job.

4) Raw jobs - Default Orientation

Select the default orientation that applies to a raw job.

5) Raw jobs - Default Stapling

Select whether a raw job will be stapled.

6) Raw jobs - Default Output Tray

Select the default output tray that applies to a raw job. A banner page that is created by NetWare, UNIX, and Windows operating systems also will be outputted to the tray set here.

7) PCL Form Line

Enter the number of lines printed per page.

8) PCL Font Pitch

Enter the font pitch when the selected font number represents a fixed pitch scalable font. Pitch is measured by characters per inch, so a 10-pitch is ten characters per inch.

9) PCL Font Point Size

Enter the font size when the selected font number represents a proportionally spaced scalable font. The Font Size option allows you to determine the point size (height) of the default font.

10) PCL Font Number

Enter the font number of the internal PCL font to be used as the default font for printing. You can check the font numbers and internal PCL fonts in the Internal PCL Font List. Refer to the **Printing Guide** for the font number of internal PCL fonts.

11) PCL Line Termination

Select the type of the line termination.

12) Symbol set

Select the symbol set that applies to a raw job.

13) Paper Source

Select the paper source that applies to a raw job.

14) Do not Print Blank Pages

Select whether blank pages are printed or not.

Note

When printing is performed using the UNIX filters or CUPS, this setting is not reflected.

If you do not want to print blank pages in these printings, enable [Do not Print Blank Pages] in the UNIX filter command or CUPS setting.

For the setting instructions, refer to the **Software Installation Guide** or **Printing Guide**.

15) Letterhead Print Mode

Select whether the last page (odd page number) is printed on the same side as the other odd-number pages when printing both sides of a Raw print job whose total page number is odd.

Select [Enable] to print the last page on the same side (back) as the other odd-number pages.

Select [Disable] to print it on the same side (front) as even-number pages.

Note

The Letterhead Print mode is available only for the e-STUDIO455 Series, e-STUDIO4520C Series and e-STUDIO6530C Series.

□ Setting up Raw Job Setting

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

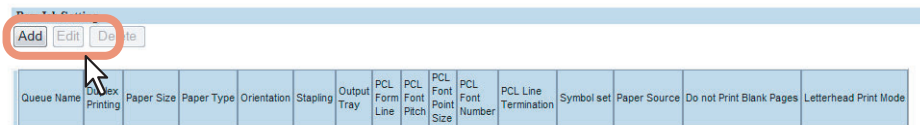
You can add, edit, or delete an LPR queue.

📖 P.191 "Adding or editing an LPR queue"

📖 P.193 "Deleting an LPR queue"

Adding or editing an LPR queue

- 1** To add a new LPR queue, click [Add] in Raw Job Setting.
To edit an existing LPR queue, select a radio button of a queue that you want to edit and click [Edit].



The Add New LPR Queue page is displayed.

2 Enter the following items as required.

Add New LPR Queue

Save Cancel

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

Queue Name — Enter the queue name using up to 31 alphanumeric characters. The queue name is case sensitive so that “Queue1” and “queue1” will be added as different queues.

Duplex Printing — Select whether a raw job will be printed on both sides of the paper.

Paper Size — Select the default paper size that applies to a raw job.

Paper Type — Select the default paper type that applies to a raw job.

Orientation — Select the default orientation that applies to a raw job.

Stapling — Select whether a raw job will be stapled.

Output Tray — Select the default output tray that applies to a raw job. A banner page that is created by NetWare, UNIX, and Windows operating systems also will be outputted to the tray set here.

PCL Form Line — Enter the number of lines printed per page.

PCL Font Pitch — Enter the font pitch when the selected font number represents a fixed pitch scalable font. Pitch is measured by characters per inch, so a 10-pitch is ten characters per inch.

PCL Font Point Size — Enter the font size when the selected font number represents a proportionally spaced scalable font. The Font Size option allows you to determine the point size (height) of the default font.

PCL Font Number — Enter the font number of the internal PCL font to be used as the default font for printing. You can check the font numbers and internal PCL fonts in the Internal PCL Font List. Refer to the **Printing Guide** for the font number of internal PCL fonts.

PCL Line Termination — Select the type of the line termination.

Symbol set — Select the symbol set that applies to a raw job.

Paper Source — Select the paper source that applies to a raw job.

Do not Print Blank Pages — Select whether blank pages are printed or not.

Note

When printing is performed using the UNIX filters or CUPS, this setting is not reflected.

If you do not want to print blank pages in these printings, enable [Do not Print Blank Pages] in the UNIX filter command or CUPS setting.

For the setting instructions, refer to the **Software Installation Guide** or **Printing Guide**.

Letterhead Print Mode — Select whether the last page (odd page number) is printed on the same side as the other odd-number pages when printing both sides of a Raw print job whose total page number is odd. Select [Enable] to print the last page on the same side (back) as the other odd-number pages. Select [Disable] to print it on the same side (front) as even-number pages.

Note

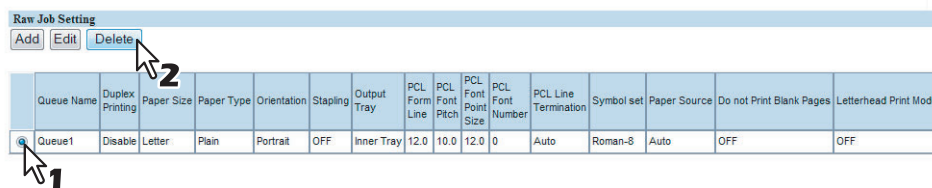
The Letterhead Print mode is available only for the e-STUDIO455 Series, e-STUDIO4520C Series and e-STUDIO6530C Series.

3 Click [Save].

The queue name is added to the list.

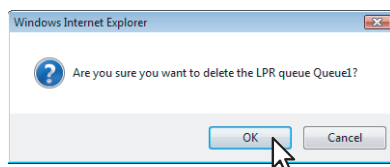
Deleting an LPR queue

- 1 Select a radio button of a queue that you want to delete and click [Delete].



The confirmation dialog box appears.

- 2 Click [OK].



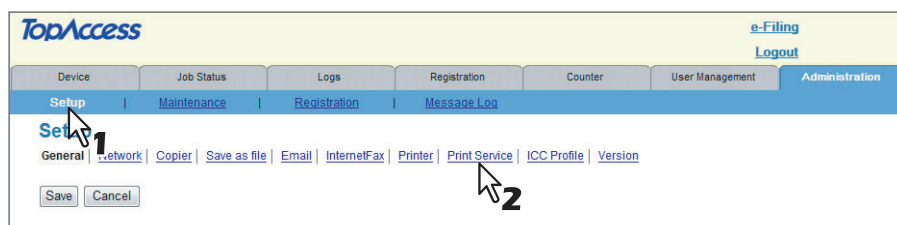
The selected queue is deleted.

Setting up Print Service settings

In the [Print Service] submenu in the [Setup] menu, an administrator can configure such print services as Raw TCP Print, LPD Print, IPP Print, FTP Print, NetWare Print, and Email Print.

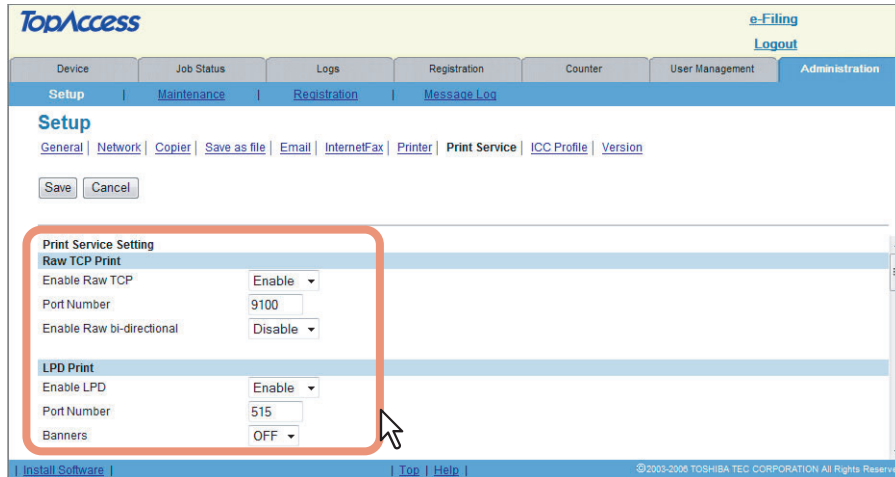
Setting the Print Service settings

- 1 Access TopAccess in the administrator mode.
P.106 "Accessing TopAccess Administrator Mode"
- 2 Click the [Setup] menu and [Print Service] submenu.



The Print Service submenu page is displayed.

3 In the Print Service submenu page, set the Print Service settings as required.



In the Print Service submenu page, you can set the following:

- 📖 P.195 "Setting up Raw TCP Print"
- 📖 P.195 "Setting up LPD Print"
- 📖 P.196 "Setting up IPP Print"
- 📖 P.197 "Setting up FTP Print"
- 📖 P.198 "Setting up NetWare Print"
- 📖 P.198 "Setting up Email Print"

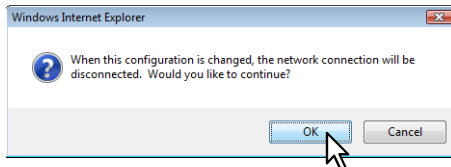
4 Click [Save].

The confirmation dialog box appears.

Tip

If you want to restore the current settings without saving the changes, click [Cancel]. Clicking [Cancel] cannot restore the defaults. This can only clear the changes and restore the current settings before saving the changes.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the Print Service page immediately after changing the settings and clicking [Save]. If that happens, click the [Print Service] submenu to refresh the page.

□ Setting up Raw TCP Print

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

Raw TCP Print		
1	Enable Raw TCP	Enable ▾
2	Port Number	9100
3	Enable Raw bi-directional	Disable ▾

1) Enable Raw TCP

Enable or disable Raw TCP print service.

2) Port Number

If enabling the Raw TCP, enter the Raw TCP port number for the Raw TCP print. Generally “9100” is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

3) Enable Raw bi-directional

Enable or disable Raw bi-directional communication.

7

□ Setting up LPD Print

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

LPD Print		
1	Enable LPD	Enable ▾
2	Port Number	515
3	Banners	OFF ▾

1) Enable LPD

Enable or disable LPD print service.

2) Port Number

If enabling the LPD, enter the LPD port number. Generally “515” is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

3) Banners

Select whether to print a banner page for each print job using LPR printing.

□ Setting up IPP Print

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

IPP Print	
1 — Enable IPP	Enable ▼
2 — Port80 Enable	Enable ▼
3 — Port Number	631
4 — URL	http://10.10.70.120:631/Print
5 — Enable SSL	Disable ▼
6 — SSL Port Number	443
7 — SSL URL	https://10.10.70.120:443/Print
8 — Administrator's Name	admin
9 — Administrator's Password	••••••
10 — Authentication	Disable ▼
11 — User Name	user
12 — Password	••••••••

1) Enable IPP

Enable or disable the IPP print service.

2) Port80 Enable

Enable or disable Port80 for IPP printing. Port631 is usually used for IPP access so users must specify the IPP port to the URL, i.e. "http://<IP address or DNS name>:631/Print", for the IPP port. When this is enabled, this equipment allows IPP access through the Port80, which is the default port for the HTTP access so users do not have to specify the port number in the IPP port, i.e. "http://<IP address or DNS name>/Print".

3) Port Number

If enabling the IPP, enter the IPP port number. Generally "631" is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

4) URL

Display the URL for IPP printing. You cannot change the URL for IPP printing. This URL should be set as the print port when users set up the printer driver for IPP printing.

5) Enable SSL

Enable or disable SSL for IPP printing.

Notes

- To enable SSL, you must create a self-signed certificate or import a server certificate in Security Service. If the self-signed certificate is not created or a server certificate is not imported, the SSL will not work correctly.
[P.146 "Setting up Security Service"](#)
- When the SLL is enabled, users can print to the IPP print port using the SSL. To print to the IPP print port using the SSL, specify the following URL for the IPP print port.
`https://<IP Address>:<SSL Port Number>/Print`
- Not all operating systems support SSL for all protocols.

6) SSL Port Number

Enter the port number for SSL. Generally "443" is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

7) SSL URL

Display the SSL URL for IPP printing. You cannot change the SSL URL for IPP printing. This SSL URL should be set as the print port when users set up the printer driver for IPP printing if the SSL for IPP printing is enabled.

8) Administrator's Name

Enter the user name of the administrator's client computer. When logging in to the client computer using this administrator's name, an administrator can delete all jobs in the IPP queue by selecting [Cancel All Documents] command in the [File] menu of printer queue dialog box on Windows.

9) Administrator's Password

Enter the password of user to be allowed to perform the [Cancel All Documents] function.

10) Authentication

Enable or disable the authentication for creating the IPP queue on the client computers. When this is enabled, the dialog box to enter a user name and password will be displayed when a user creates the IPP print port.

- **Disable** — Select this to disable the authentication.
- **Basic** — Select this to enable the authentication.

Note

When IPP printing is used for printing from a Macintosh computer, do not enable the authentication. The Mac OS does not support the authentication for IPP printing.

11) User Name

Enter the user name when the Authentication option is enabled. Users must enter this user name to create an IPP queue on the client computers.

12) Password

Enter the password when the Authentication option is enabled. Users must enter this password to create an IPP queue on the client computers. "password" has been set as the default.

7**□ Setting up FTP Print**

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

FTP Print	
1 — Enable FTP Printing	Enable ▾
2 — Port Number	21
3 — Print User Name	Print
4 — Print Password	

1) Enable FTP Printing

Enable or disable FTP print service.

2) Port Number

Enter the FTP port number for FTP printing. Generally "21" is used.

Note

When the same port number as the secondary one in the HTTP setting (SSL port number when SSL 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 control panel of the equipment to change the HTTP setting and enter the correct port number.

3) Print User Name

Enter the user name who attempts FTP printing. If you leave this box blank, the default user name "Print" is used.

4) Print Password

Enter the password if you want to request the login password of users who attempts FTP printing.

□ Setting up NetWare Print

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

NetWare Print	
1 — Login Name	MFP_04998820
2 — Password	
3 — Print Queue Scan Rate	5

1) Login Name

Enter the print server name that is created in the NetWare file server.

2) Password

Enter the password that is set to the print server, if required.

3) Print Queue Scan Rate

Enter how frequently to scan the print queues for print jobs. This should be entered in seconds. You can enter between 1 to 255.

□ Setting up Email Print

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

Email Print	
1 — Enable Print Header	Disable ▾
2 — Enable Print Message Body	Enable ▾
3 — Maximum Email Body Print	5
4 — Enable Print Email Error	Enable ▾
5 — Enable Email Error Forward	Disable ▾
6 — Email Error Transfer Address	
7 — Enable Partial Email	Enable ▾
8 — Partial Wait time	24
9 — MDN Reply	Disable ▾

1) Enable Print Header

Select whether to print the Email header when receiving Email print jobs.

2) Enable Print Message Body

Select whether to print the body message when receiving Email print jobs.

3) Maximum Email Body Print

Enter the maximum number of pages to print the body strings of the received Email print job. You can enter between 1 to 99.

4) Enable Print Email Error

Select whether to print the report when an error occurs for Email printing.

5) Enable Email Error Forward

Select whether to send an error message to an administrative Email address when Email printing cannot be completed.

6) Email Error Transfer Address

If enabling the Email Error Forward, enter an administrative Email address where the error message is sent.

7) Enable Partial Email

Select whether to print Email jobs that are partially received.

8) Partial Wait Time

Enter how long this equipment should wait before printing a partial Email job. This should be entered in hour.

9) MDN Reply

Select whether to send an MDN message reply or not when the equipment receives an Email print job with an MDN request.

■ Setting up ICC Profile settings

The administrator can set up profiles used in printing functions from the [ICC Profile] submenu of the [Setup] menu on the [Administration] tab.

Tip

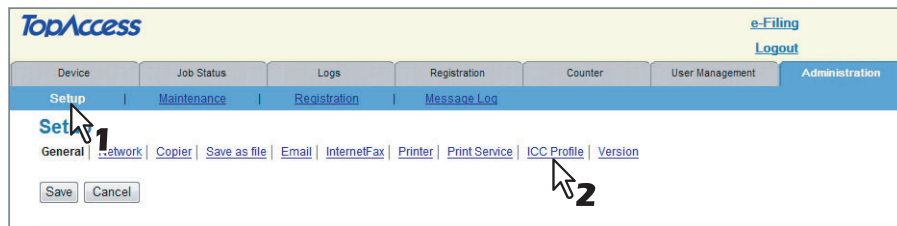
This feature is available only for the e-STUDIO4520C Series and the e-STUDIO6530C Series.

Setting the ICC Profile settings

1 Access TopAccess in the administrator mode.

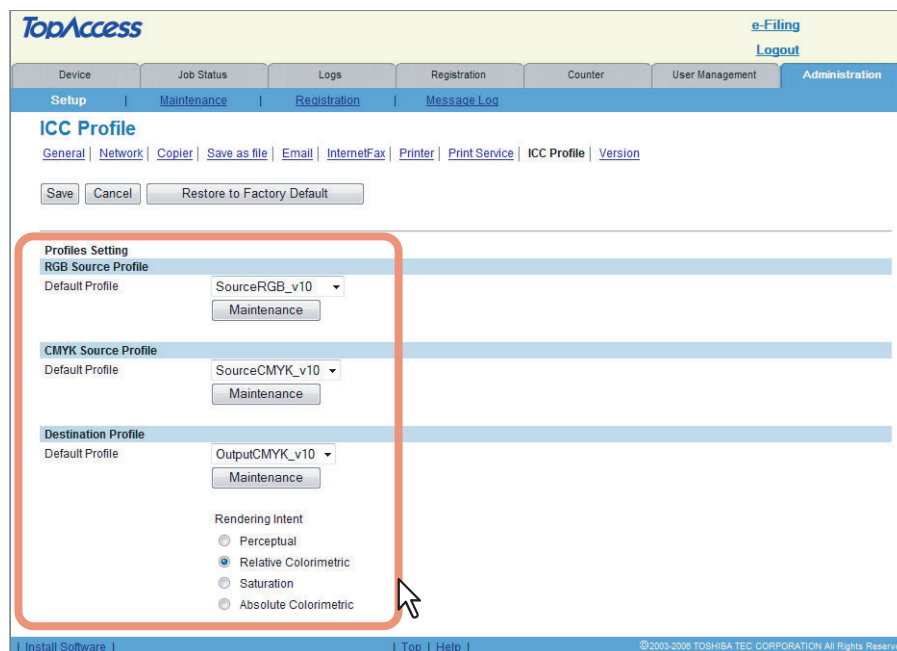
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [ICC Profile] submenu.



The ICC Profile submenu page is displayed.

3 In the ICC Profile submenu page, set the ICC Profile settings as required.



In the ICC Profile submenu page, you can set the following:

- 📖 P.200 “Setting up RGB Source Profile”
- 📖 P.204 “Setting up CMYK Source Profile”
- 📖 P.205 “Setting up Destination Profile”

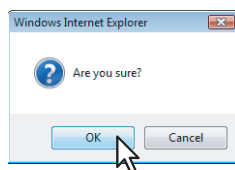
4 Click [Save].

The confirmation dialog box appears.

Tips

- When you click [Cancel] before saving the setting changes, the changes will not be saved and they will return to the current settings. Note that they will not return to the factory default by clicking [Cancel]. Click this to clear all the changes made and return the setting to the current one.
- Click [Restore to Factory Default] to return the settings to the factory default.

5 Click [OK] to apply the changes.



Note

When using Internet Explorer, the changes may not be reflected on the ICC Profile page immediately after changing the settings and clicking [Save]. If that happens, click the [ICC Profile] submenu to refresh the page.

□ Setting up RGB Source Profile

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



1) Default Profile

Select an RGB source profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among the RGB source profiles already registered in this equipment.

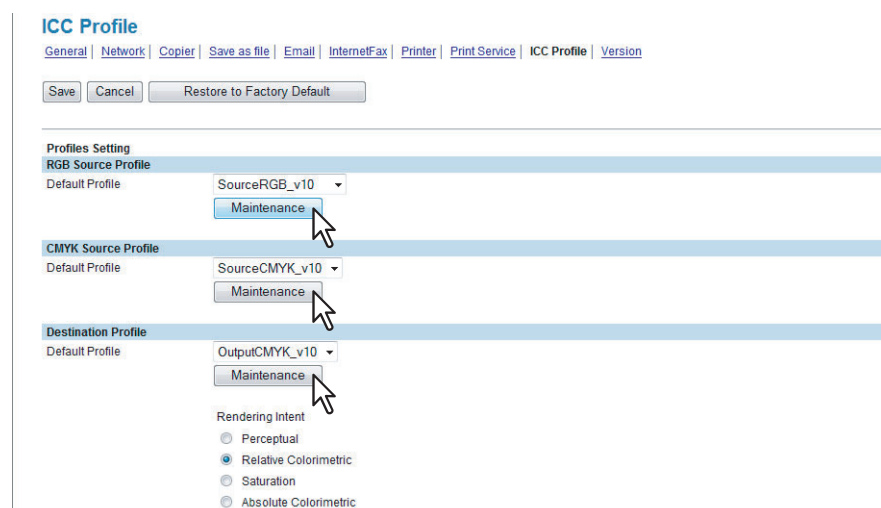
2) [Maintenance]

Click this to perform maintenance of RGB source profiles. The Maintenance RGB Source Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. For the details, see the following:

- 📖 P.200 "Importing profiles"
- 📖 P.201 "Exporting profiles"
- 📖 P.203 "Deleting profiles"

Importing profiles

1 Click [Maintenance] of the desired profile.



The Maintenance Profile page of the selected profile is displayed.

- Click [Browse] in [Import new Profile] to select the file of the selected profile, and then click [Import].

Maintenance RGB Source Profiles

[Previous](#)

	Description	File Name
Default Profile	SourceRGB_v10	TTEC_SourceRGB_A00.icc

Import new Profile

File Name [Browse...](#) [Import](#)

Current Profiles

[Delete](#) [Export](#)

	Description	File Name
☐	SourceRGB_v10	TTEC_SourceRGB_A00.icc
☐	Adobe RGB (1998)	AdobeRGB1998.icc
☐	Apple RGB	AppleRGB.icc

Importing starts.

- The profile is imported. Click [Previous] to close the Maintenance Profile page.

Maintenance RGB Source Profiles

[Previous](#)

	Description	File Name
Default Profile	SourceRGB_v10	TTEC_SourceRGB_A00.icc

Import new Profile

File Name [Browse...](#) [Import](#)

Current Profiles

[Delete](#) [Export](#)

	Description	File Name
☐	SourceRGB_v10	TTEC_SourceRGB_A00.icc
☐	Adobe RGB (1998)	AdobeRGB1998.icc
☐	Apple RGB	AppleRGB.icc
☐	Wide Gamut RGB	Profile1.icc

The imported profile is added to the [Current Profiles] list.

Exporting profiles

- Click [Maintenance] of the desired profile.

ICC Profile

[General](#) | [Network](#) | [Copier](#) | [Save as file](#) | [Email](#) | [InternetFax](#) | [Printer](#) | [Print Service](#) | [ICC Profile](#) | [Version](#)

[Save](#) [Cancel](#) [Restore to Factory Default](#)

Profiles Setting

RGB Source Profile

Default Profile [Maintenance](#)

CMYK Source Profile

Default Profile [Maintenance](#)

Destination Profile

Default Profile [Maintenance](#)

Rendering Intent

☐ Perceptual

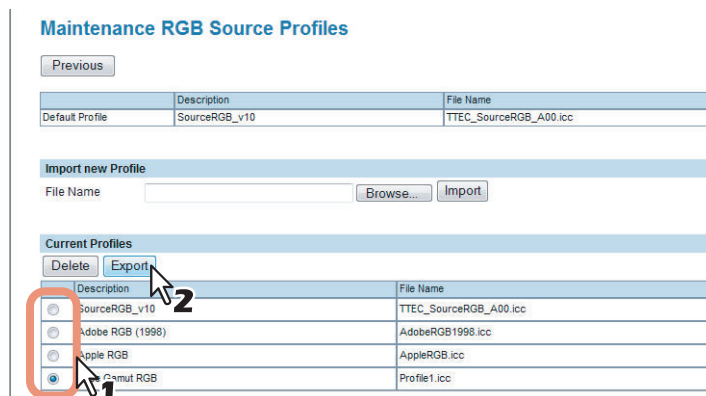
☒ Relative Colorimetric

☐ Saturation

☐ Absolute Colorimetric

The Maintenance Profile page of the selected profile is displayed.

2 Select the desired profile in the [Current Profiles] list, and then click [Export].

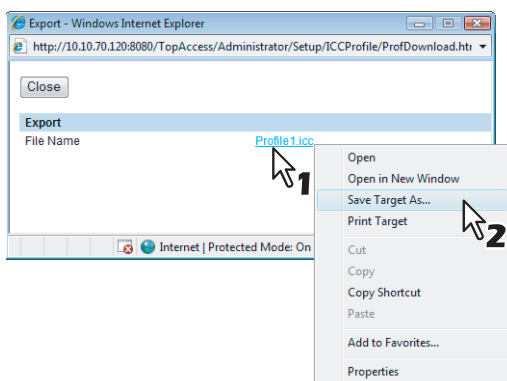


The Export page is displayed.

Note

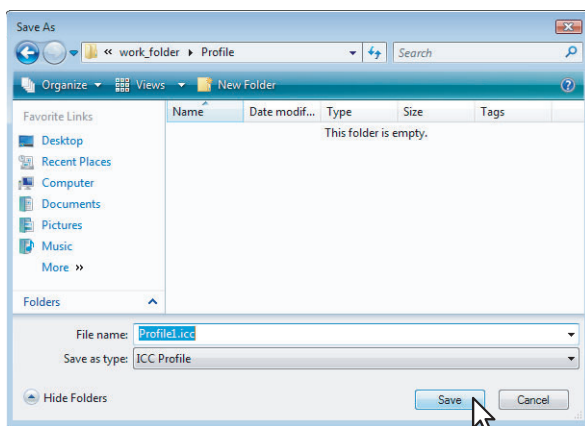
Profiles registered as a factory default cannot be exported.

3 Right-click the [File Name] link of a profile to be exported, and select [Save Target As].

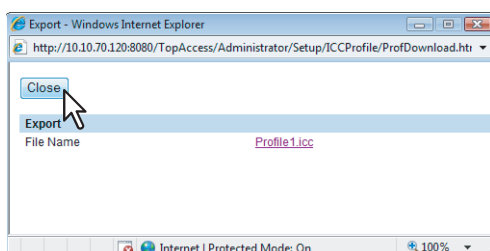


The [Save As] dialog box appears.

4 Select the file location and click [OK].



5 Click [Close] to close the Export page.



6 Click [Previous] to close the Maintenance Profile page.

Maintenance RGB Source Profiles

[Previous](#)

	Description	File Name
Default Profile	SourceRGB_v10	TTEC_SourceRGB_A00.icc

Import new Profile

File Name [Browse...](#) [Import](#)

Current Profiles

[Delete](#) [Export](#)

	Description	File Name
☐	SourceRGB_v10	TTEC_SourceRGB_A00.icc
☐	Adobe RGB (1998)	AdobeRGB1998.icc
☐	Apple RGB	AppleRGB.icc
☒	Wide Gamut RGB	Profile1.icc

Deleting profiles

1 Click [Maintenance] of the desired profile.

ICC Profile

[General](#) | [Network](#) | [Copier](#) | [Save as file](#) | [Email](#) | [InternetFax](#) | [Printer](#) | [Print Service](#) | [ICC Profile](#) | [Version](#)

[Save](#) [Cancel](#) [Restore to Factory Default](#)

Profiles Setting

RGB Source Profile

Default Profile [SourceRGB_v10](#) [Maintenance](#)

CMYK Source Profile

Default Profile [SourceCMYK_v10](#) [Maintenance](#)

Destination Profile

Default Profile [OutputCMYK_v10](#) [Maintenance](#)

Rendering Intent

☐ Perceptual

☒ Relative Colorimetric

☐ Saturation

☐ Absolute Colorimetric

The Maintenance Profile page of the selected profile is displayed.

2 Select the desired profile in the [Current Profiles] list, and then click [Delete].

Maintenance RGB Source Profiles

[Previous](#)

	Description	File Name
Default Profile	SourceRGB_v10	TTEC_SourceRGB_A00.icc

Import new Profile

File Name [Browse...](#) [Import](#)

Current Profiles

[Delete](#) [Export](#)

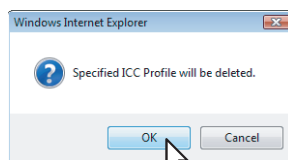
	Description	File Name
☒	SourceRGB_v10	TTEC_SourceRGB_A00.icc
☐	Adobe RGB (1998)	AdobeRGB1998.icc
☐	Apple RGB	AppleRGB.icc
☐	Wide Gamut RGB	Profile1.icc

The confirmation dialog box appears.

Note

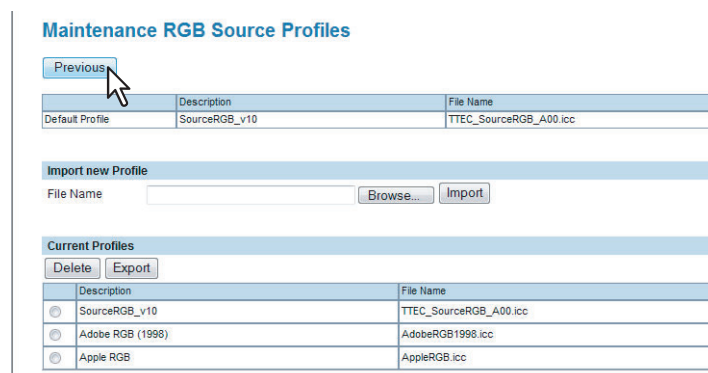
Profiles registered as a factory default cannot be deleted.

3 Click [OK].



The Profile is deleted.

4 Click [Previous] to close the Maintenance Profile page.



The profile is deleted from the [Current Profiles] list.

□ Setting up CMYK Source Profile

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



1) Default Profile

Select an CMYK source profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among CMYK source profiles already registered in this equipment.

2) [Maintenance]

Click this to perform maintenance of CMYK source profiles. The Maintenance CMYK Source Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. For the details, see the following:

- 📖 P.200 "Importing profiles"
- 📖 P.201 "Exporting profiles"
- 📖 P.203 "Deleting profiles"

□ Setting up Destination Profile

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

The screenshot shows a settings window titled 'Destination Profile'. It is divided into three numbered sections:

- 1** Default Profile: A dropdown menu currently showing 'OutputCMYK_v10'.
- 2** Maintenance: A button labeled 'Maintenance'.
- 3** Rendering Intent: Four radio button options:
 - Perceptual
 - Relative Colorimetric** (selected)
 - Saturation
 - Absolute Colorimetric

1) Default Profile

Select a destination profile to be displayed as a default setting of the color profile setting of a printer driver. You can select among destination profiles already registered in this equipment.

2) [Maintenance]

Click this to perform maintenance of destination profiles. The Maintenance Destination Profile page is displayed as you click this. You can import profiles into this equipment, or export or delete the registered profiles. For the details, see the following:

- 📖 P.200 "Importing profiles"
- 📖 P.201 "Exporting profiles"
- 📖 P.203 "Deleting profiles"

3) Rendering Intent

Select how you perform color space conversion when you print images.

- **Perceptual** — This is recommended for photo images.
- **Relative Colorimetric** — More original colors can be retained than those when you select [Perceptual].
- **Saturation** — This is recommended when the vividness of colors are more important than their correct reproduction. It is useful for graphic charts.
- **Absolute Colorimetric** — Original colors can be retained even on colored paper.

■ Displaying version information

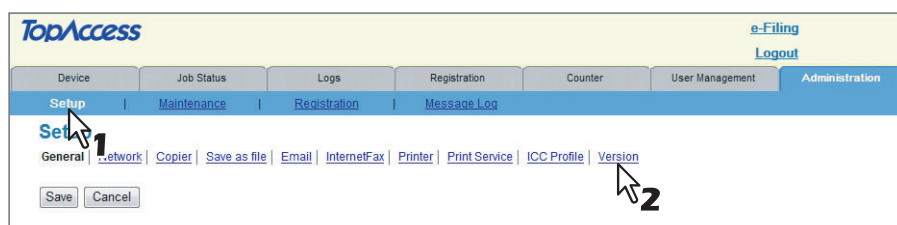
An administrator can display the system software version information of this equipment.
The version information can be displayed from the [Setup] menu.

Displaying the version information

1 Access TopAccess in the administrator mode.

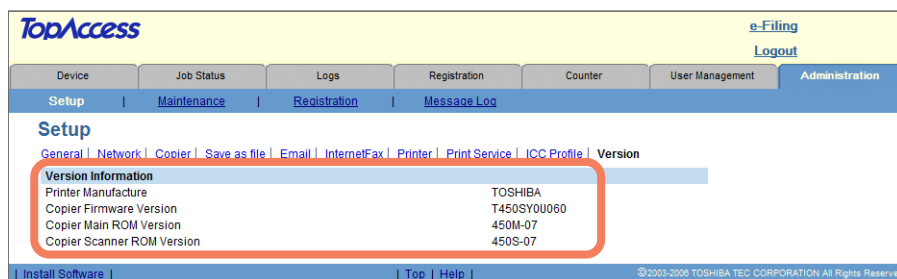
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Setup] menu and [Version] submenu.



The Version submenu page is displayed.

3 In the Version submenu page, you can confirm the version information of the system software.



Maintenance From TopAccess

This section details procedures for maintaining this equipment. It covers backing up and restoring files, deleting files stored on this equipment, and updating the software on TopAccess.

- 📖 P.207 “About the maintenance functions”
- 📖 P.208 “Uploading the software”
- 📖 P.209 “Removing the client software”
- 📖 P.210 “Backing up data”
- 📖 P.213 “Restoring data from backup file”
- 📖 P.215 “Deleting the data from local folder”
- 📖 P.216 “Managing directory service”
- 📖 P.218 “Setting up notification”
- 📖 P.223 “Importing and exporting the Address Book”
- 📖 P.228 “Importing and exporting the department code”
- 📖 P.231 “Exporting the logs, journals, and counters”
- 📖 P.233 “Clearing the logs and journals”
- 📖 P.235 “Rebooting the equipment”

■ About the maintenance functions

In the [Maintenance] menu of the TopAccess administrator mode, an administrator can perform the following maintenance:

Uploading client software in TopAccess

An administrator can upload client software that allows users to download to their computers from TopAccess. This maintenance feature is used to upload new versions of software in TopAccess.

- 📖 P.208 “Uploading the software”

Removing client software from TopAccess

An administrator can remove client software that restricts users from downloading software from TopAccess. This maintenance feature is used to disable specific software in TopAccess.

- 📖 P.209 “Removing the client software”

Backing up data in the hard disk

An administrator can create backup files of address book, mailboxes, and templates in the hard disk. This maintenance feature is used to create the backup files before updating the system software or hard disk replacement, etc.

- 📖 P.210 “Backing up data”

Restoring data from the backup files

An administrator can restore the address book, mailboxes, and templates data from the backup files. This maintenance feature is used to restore the data after updating the system software or hard disk replacement, etc.

- 📖 P.213 “Restoring data from backup file”

Deleting files stored in the hard disk

An administrator can delete scanned data, transmission data, and reception data in the hard disk. This maintenance feature must be operated periodically to maintain the hard disk space for future operation.

- 📖 P.215 “Deleting the data from local folder”

Registering directory service

An administrator can register the directory service properties of the LDAP (Lightweight Directory Access Protocol) server.

- 📖 P.216 “Managing directory service”

Setting up notifications

An administrator can enable the notifications by Emails and specify the events causing the notifications.

- 📖 P.218 “Setting up notification”

Importing or exporting address book data

This equipment allows you to import and export address book data in CSV format.

- 📖 P.223 “Importing and exporting the Address Book”

Importing or exporting department code

An administrator can import and export department code data in CSV format.

- 📖 P.228 “Importing and exporting the department code”

Exporting logs and journals

An administrator can export logs and journals as CSV files. This feature is used to save the logs and journals as files before clearing them, if you want to maintain them.

📖 P.231 “Exporting the logs, journals, and counters”

Clearing logs and journals

An administrator can clear logs and journals in this equipment. This maintenance feature must be operated periodically to maintain the hard disk space for future operation.

📖 P.233 “Clearing the logs and journals”

Rebooting the equipment

An administrator can reboot the equipment.

📖 P.235 “Rebooting the equipment”

■ Uploading the software

You can upload client software to this equipment so end-users can download the software to their computers from TopAccess.

You can upload the following components:

- Installer (Setup files) for Client Utilities CD-ROM
- Macintosh PPD Files
- UNIX Filters
- Printer Driver files for Point and Print

Note

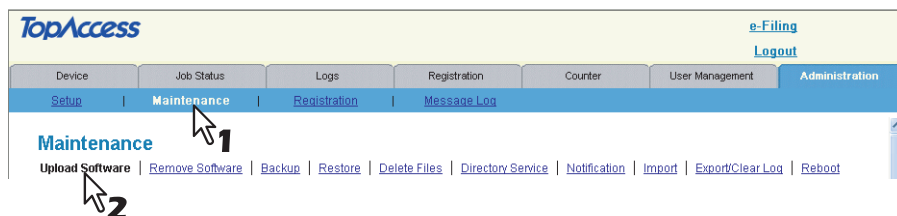
Uploading new software overwrites the old version of software that had been uploaded.

Uploading new versions of client software in TopAccess

1 Access TopAccess in the administrator mode.

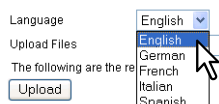
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Maintenance] menu and [Upload Software] submenu.

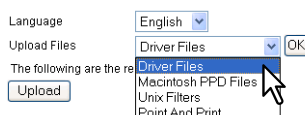


The Upload Software submenu page is displayed.

3 Select the language of the software that you are going to upload in the [Language] box.



4 Select the software that you are going to upload in the [Upload Files] box.



Driver Files — Select this to upload the setup files.

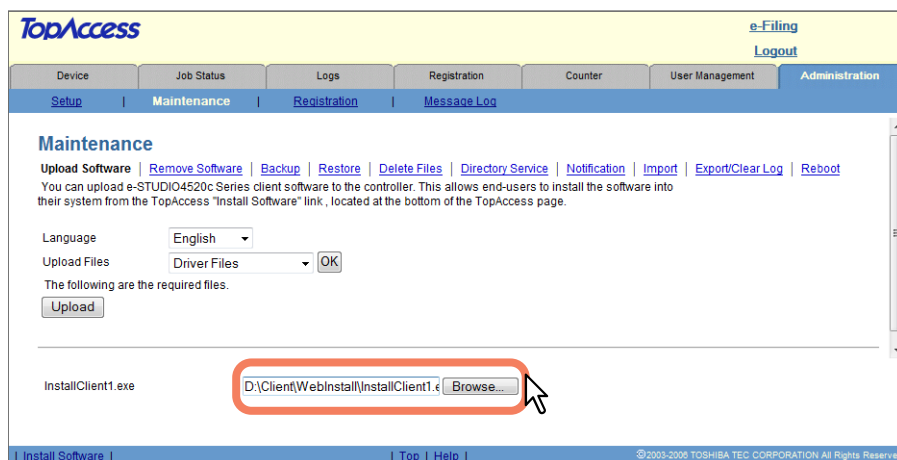
Macintosh PPD Files — Select this to upload the self-extracting files that contain the Macintosh PPD files for Mac OS X 10.2.4 to 10.3.x and Mac OS X 10.4 or later. In addition, select this to upload the plug-in files used for Mac OS X 10.4 or later.

Unix Filters — Select this to upload the tar files that contain filters for each UNIX workstation.

Point And Print — Select this to upload the printer driver files for the Point and Print installation.

5 Click [OK].

The bottom section in the page will be changed for selected software.

6 In each box displayed, click [Browse] to locate the setup files to be uploaded.**Note**

At the left of each box, the file name will be displayed. Be sure to specify the same file for each box.

Tip

The files for uploading are provided for each client software.

Driver Files — Contact your dealer for information about obtaining these files.

Macintosh PPD Files — Provided in the following sub folders in the “MacPPD” folder of the Client Utilities CD-ROM.

- \OSX\10_2-10_3
- \OSX\10_4-

Unix Filters — Provided in the Client Utilities CD-ROM.

Point And Print — Contact your dealer for information about obtaining these files.

7 Click [Upload].

Specified files are uploaded in this equipment.

■ Removing the client software

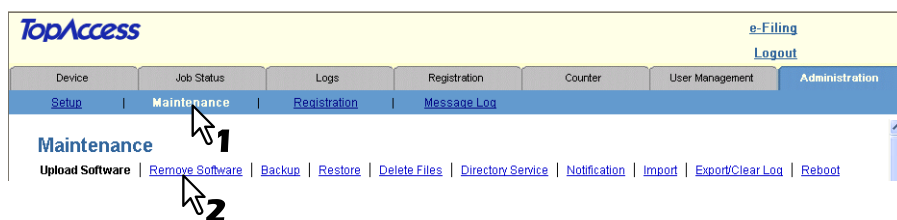
You can remove client software from TopAccess so that it can no longer be installed from TopAccess.

Note

The printer drivers for Point and Print that had been uploaded cannot be deleted. However, you can upload new printer drivers to overwrite them.

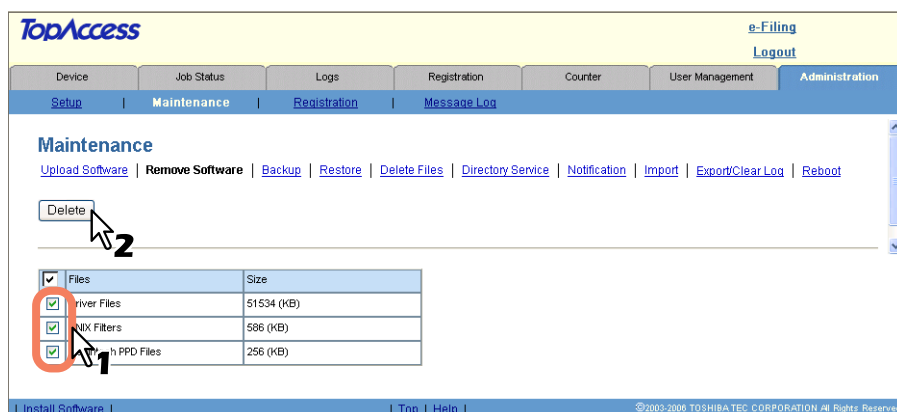
Removing the software from TopAccess**1 Access TopAccess in the administrator mode.**

P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Maintenance] menu and [Remove Software] submenu.

The Remove Software submenu page is displayed.

3 Select the box of the software which you are going to remove and click [Delete].



The selected software is deleted from this equipment.

■ Backing up data

The administrator can create backup files of the address book, mailboxes and templates that are stored in the hard disk of this equipment. These data must be backed up in the cases such as the updating of system software or the replacement of the hard disk. The created backup file can be used to restore these data or upload them to other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO855 Series or e-STUDIO455 Series.

Tip

The address book, mailbox, and template data are stored in the hard disk. Periodically back up data in the hard disk to secure the data from hard disk collapse.

Backing up data as files

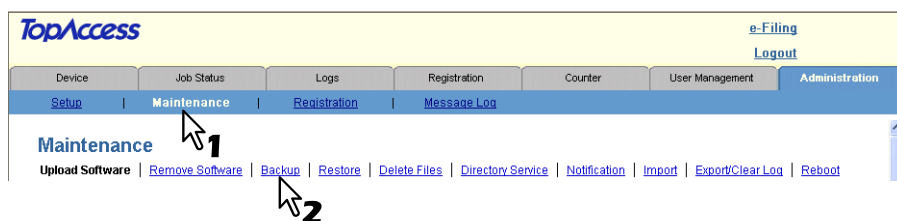
Notes

- Before backing up the data, confirm that there is no print job, no scan job, and no fax job. The backup files cannot be created if there are any jobs that have been processed. If backing up the data takes a long time, perform backing up the data after the equipment turns into the Sleep/Auto Shut Off mode.
- The password for the template will be displayed as texts in the backup file. Keep the backup file carefully when backing up the template data.

1 Access TopAccess in the administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Backup] submenu.

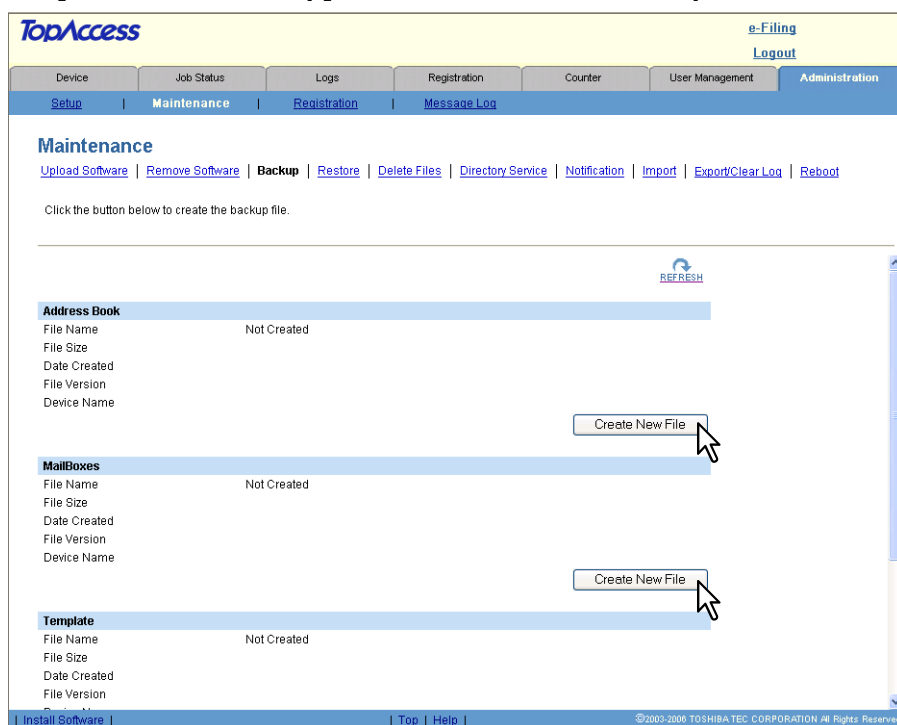


The Backup submenu page is displayed.

Tip

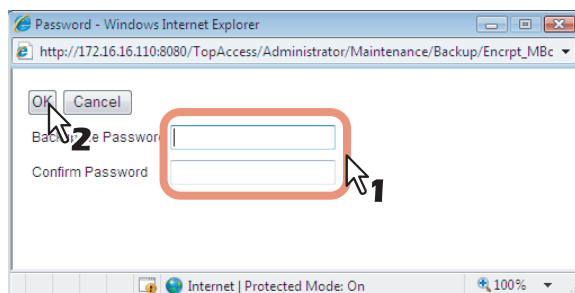
If you previously created a backup file, the backup file link and information are displayed in each area. You can click the link to save the previous backup file.

- 3** Click [Create New File] for the data that you want to back up, or click [Create New File] in the [Combined Backup] section to create a backup file of all data.



The Password dialog box appears.

- 4** Enter the password of the backup file.



The backup file will be created and the backup file name and file size will be displayed.

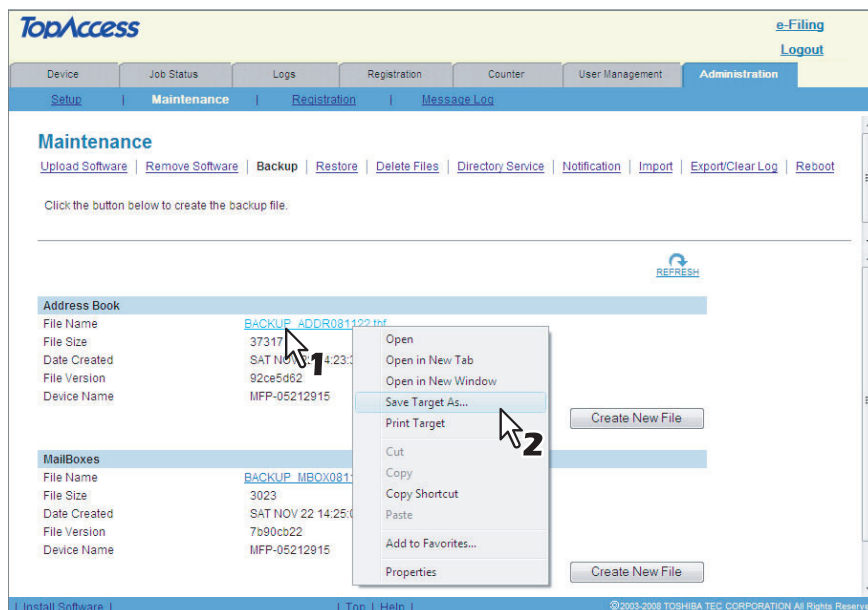
Tip

Passwords must be from 1 to 128 one-byte alphanumeric characters.

Note

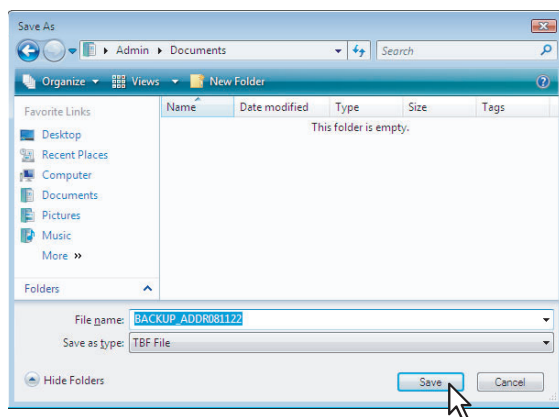
Creating the backup file may takes a few minutes depending on the file size.

5 Right-click the [File Name] link and select [Save Target As].



The [Save As] dialog box appears.

6 Select the file location and select [All Files] in the [Save as type] box.



Note

It is recommended to save the backup file as it is named. If you change the file name, the equipment cannot restore the data from the backup files. The file name of each backup data must be the following name:

- Address Book: BACKUP_ADDR<date>.tbf
- MailBoxes: BACKUP_MBOX<date>.enc
- Template: BACKUP_TEMP<date>.enc
- Combined Backup: BACKUP_ALL<date>.enc

7 Click [Save].

The backup file is saved in the selected location.

Restoring data from backup file

An administrator can restore the address book, mailboxes, and templates data using the backup files. This maintenance feature is used to restore data from backup files after updating the system software or hard disk replacement, etc., to recover the original environments. Also you can upload the data in different equipment using this Function.

Note

When restoring the data from the backup file, the same template number settings and mailbox settings are overwritten.

Restoring data from backup files

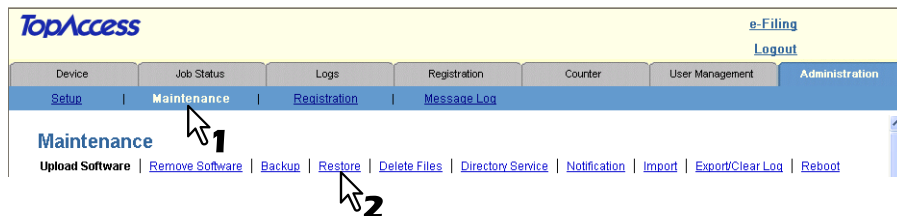
Note

Before restoring the data from backup files, confirm that there is no print job, no scan job, and no fax job. The backup files cannot be restored if there are any jobs that have been processed. If restoring the data takes a long time, restore the data after the equipment turns into the Sleep/Auto Shut Off mode.

1 Access TopAccess in the administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Restore] submenu.

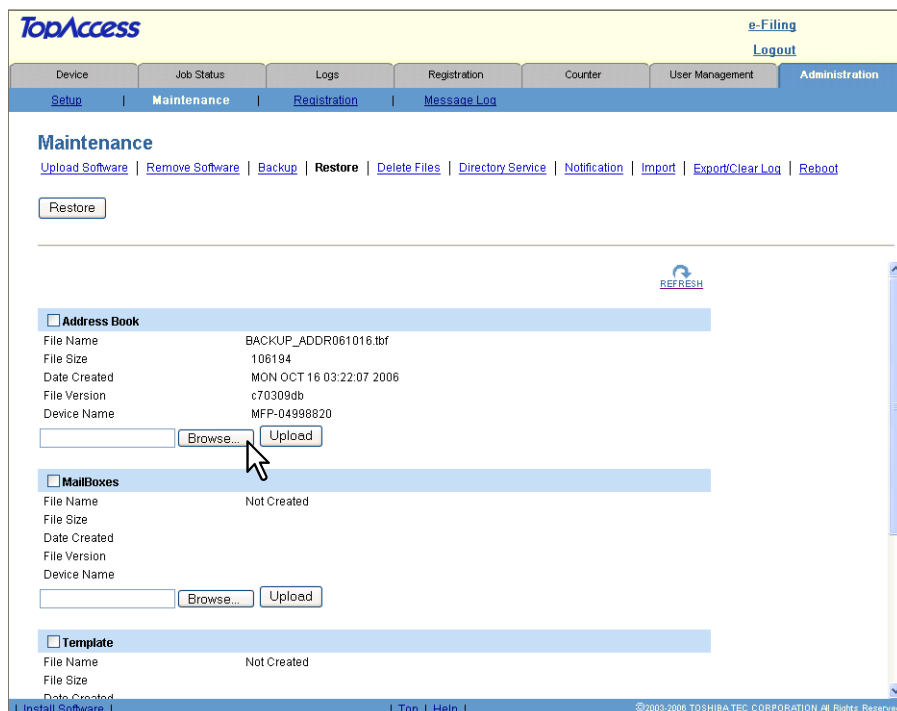


The Restore submenu page is displayed.

3 Click [Browse] in the data section that you want to restore, or click [Browse] in the [Combined Restore] section to restore all data from a backup file of all data.

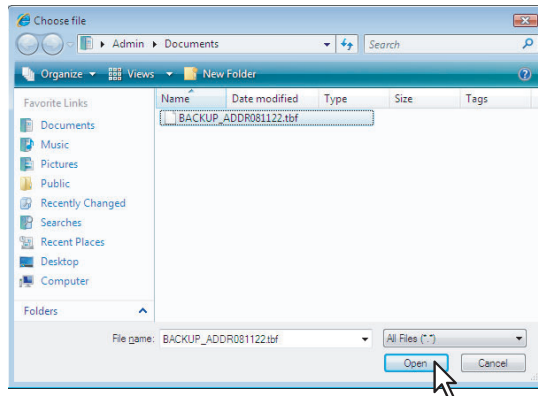
Note

You cannot restore several backup files at a time.



The Choose file dialog box appears.

4 Select a backup file and click [Open].



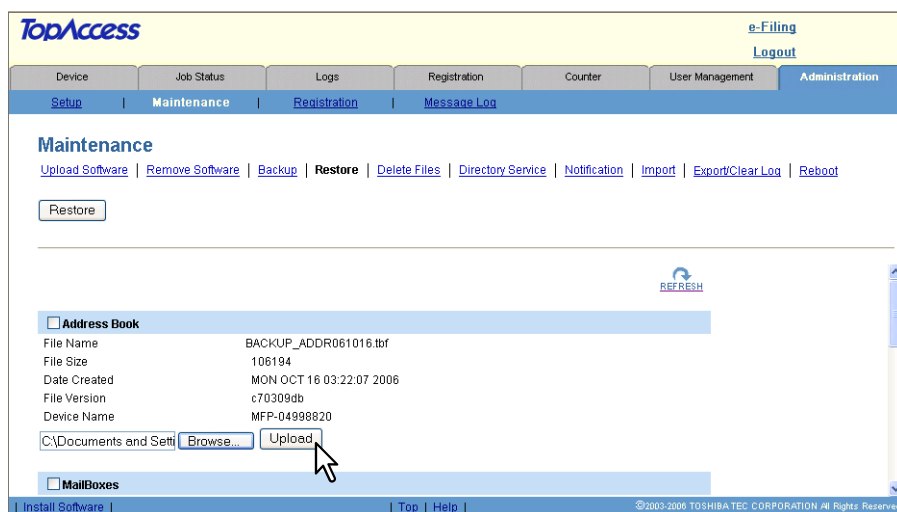
The file version and device name of the selected backup file will be displayed.

Note

If the backup file name is not the name as shown below, the equipment cannot restore the data from the backup files.

- Address Book: BACKUP_ADDR<date>.tbf
- MailBoxes: BACKUP_MBOX<date>.enc
- Template: BACKUP_TEMP<date>.enc
- Combined Backup: BACKUP_ALL<date>.enc

5 Click [Upload].



The Restore screen displays the backup file information.

6 Select the check box of data that you uploaded a backup file and click [Restore].



The restore process begins. This procedure may take several minutes.

Deleting the data from local folder

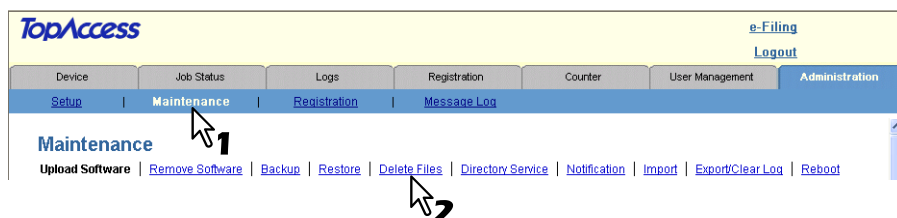
An administrator can delete information such as scanned data, transmission data, and reception data that are stored in the local folder using the Save as file function. It is recommended to delete the stored data periodically to maintain the hard disk.

Deleting data

1 Access TopAccess in the administrator mode.

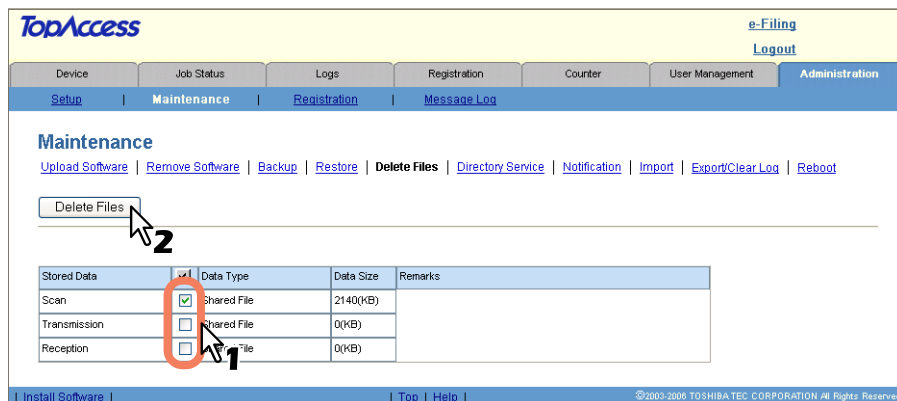
📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Delete Files] submenu.



The Delete Files submenu page is displayed.

3 Select the check box of data that you want to delete and click [Delete Files].



Scan — The data in the "SCAN" folder within the "FILE_SHARE" folder of this equipment, that are stored by Scan to File operations, will be deleted.

Transmission — The data in the "TXFAX" folder within the "FILE_SHARE" folder of this equipment, that are stored by Fax to File operations, will be deleted.

Reception — The data in the "RXFAX" folder within the "FILE_SHARE" folder of this equipment, that are stored by Save as file mailbox and Save as file Fax Received Forward or Internet Fax Received Forward.

■ Managing directory service

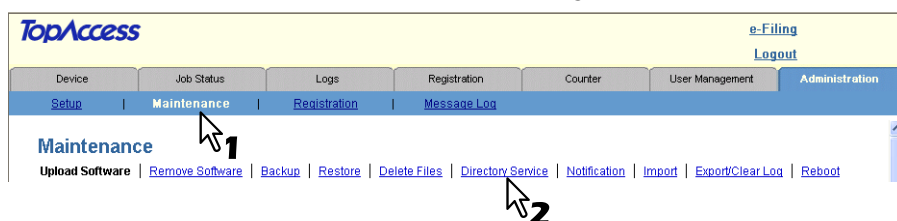
You can use TopAccess to register the Directory Service properties of the LDAP (Lightweight Directory Access Protocol) server and add a new directory service that allows users to search for Email addresses in the LDAP server.

Setting up the directory service

1 Access TopAccess in the administrator mode.

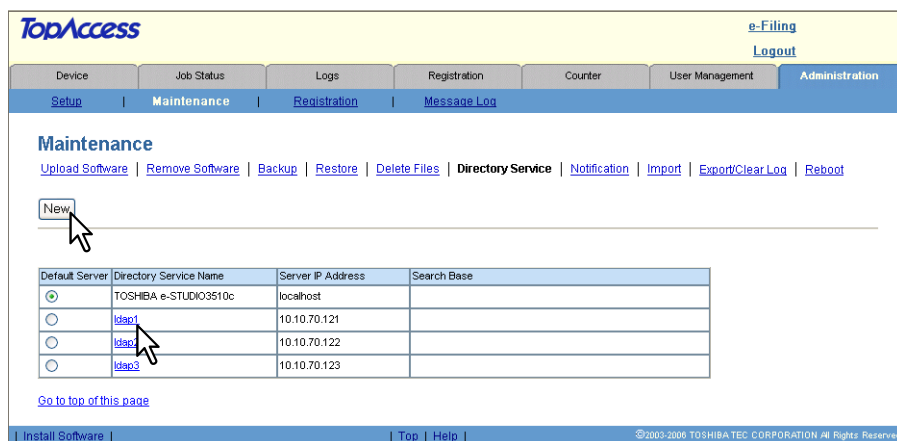
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Maintenance] menu and [Directory Service] submenu.



The Directory Service submenu page is displayed.

3 Click [New] to add a new Directory Service, or click the Directory Service name link to edit the Directory Service properties.



The Directory Service Properties page is displayed.

4 Enter the following items as required.

Directory Service Name — Enter the directory service name that identifies the directory service.

Server IP Address — Enter the IP address or FQDN of the LDAP server.

Port Number — Enter the port number to access the LDAP server. Generally the “389” port is used to access the LDAP server without SSL. When the SSL is required, generally the “636” port is used to access the LDAP server.

Authentication — Select the authentication type for SASL. If you do not know the authentication type, select [Auto].

- **Auto** — Select this to access the LDAP server using the appropriate authentication that this equipment detects.
- **Kerberos** — Select this to access the LDAP server using the Kerberos authentication.
- **Digest-MD5** — Select this to access the LDAP server using the Digest-MD5 authentication.
- **CRAM-MD5** — Select this to access the LDAP server using the CRAM-MD5 authentication.
- **Login** — Select this to access the LDAP server using the login authentication.
- **Plain** — Select this to access the LDAP server using the plain authentication.
- **Simple Bind** — Select this to access the LDAP server using the Simple Bind authentication.

Search Base — Enter the search root suffix. When you configure the Active Directory in Windows server, make sure to enter this option.

User Name — Enter the user name to access the LDAP server, if required.

Password — Enter the password to access the LDAP server, if required.

Search Timeout — Select the time interval to quit the communication when the LDAP server does not respond.

Notes

- If you use FQDN to specify the LDAP server, you must configure the DNS server and enable the DNS in the DNS Session.
- When you configure the Active Directory in Windows server and Role Based Access Control will be enabled for the User Management Setting, specify the domain administrator or account operator for the user name.
- When you configure the Active Directory in Windows server, make sure to enter the Search Base.

Tips

- You can clear the entered values by clicking [Reset].
- You can delete the Directory Service by clicking [Delete] when you edit the Directory Service.

5 Click [OK].

The entered Service Directory is added to the Directory Service List.

6 Select a radio button of the directory service that you want to set as default server.

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Setup Maintenance Registration Message Log

Maintenance

Upload Software Remove Software Backup Restore Delete Files Directory Service Notification Import Export/Clear Log Reboot

New

Default Server	Directory Service Name	Server IP Address	Search Base
☐	TOSHIBA e-STUDIO4520C	localhost	
☒	ldap1	10.10.70.121	
☐	ldap2	10.10.70.122	
☐	ldap3	10.10.70.123	

[Go to top of this page](#)

Install Software Top Help ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

Tip

The default server will be used for an LDAP search from the control panel. If you select this equipment as the default server, no default server will be set.

Setting up notification

As administrator, you can configure notification settings and receive Email notification of system errors.

Note

To enable the Email notification, the Email settings in the [Setup] menu page must be configured correctly.

📖 P.183 "Setting up Email settings"

Setting up the notifications of system errors and events

1 Access TopAccess in the administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Notification] submenu.

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Setup Maintenance Registration Message Log

Maintenance

Upload Software Remove Software Backup Restore Delete Files Directory Service Notification Import Export/Clear Log Reboot

The Notification submenu page is displayed.

3 In Email Setting, select the check box [Notify administrator at Email Address 1 to 3] to enable the notifications, and enter the administrator's Email address where the notifications are to be sent.

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter User Management Administration

Setup Maintenance Registration Message Log

Maintenance

Upload Software Remove Software Backup Restore Delete Files Directory Service Notification Import Export/Clear Log Reboot

Save

Notification Setting

Email Setting

☒ Notify administrator at Email Address 1

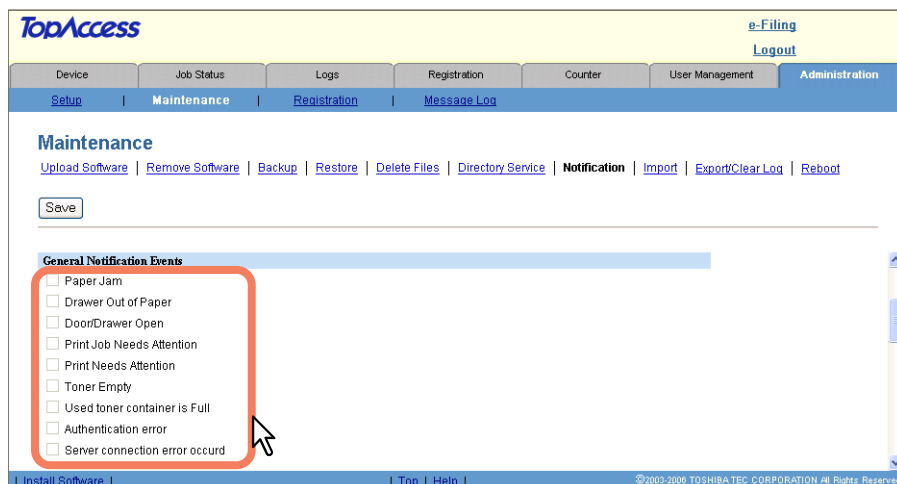
☒ Notify administrator at Email Address 2

☐ Notify administrator at Email Address 3

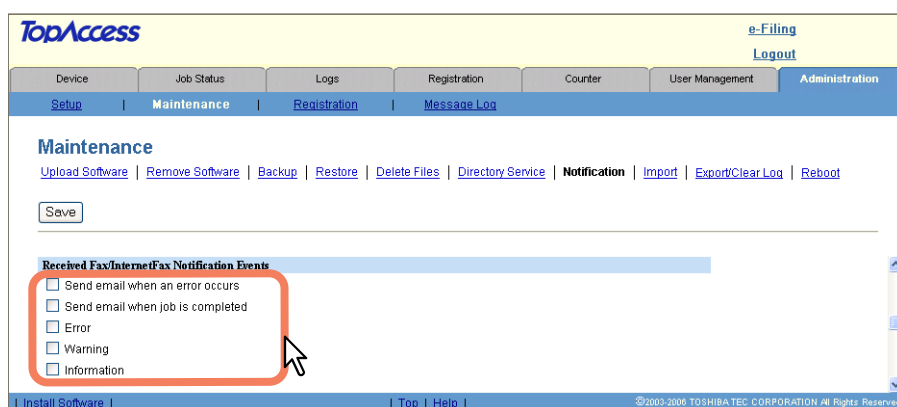
administrator@ifax.com

user01@ifax.com

4 In General Notification Events, select the check boxes for general events to be notified.



5 In Received Fax/Internet Fax Notification Events, select the check boxes for the events and status to be notified.



Tip

When these are enabled, the following events will be notified.

When [Send email when an error occurs] is enabled:

- Failed to print or store the received fax or Internet Fax jobs.

When [Error] is enabled:

- Failed to receive the Internet Fax jobs from the POP3 server.

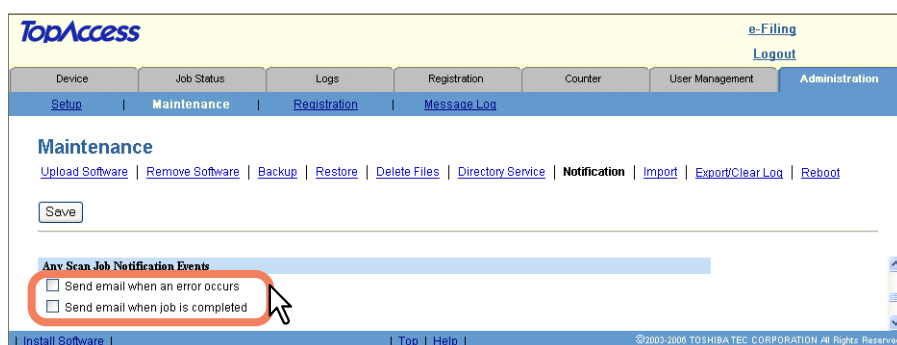
When [Warning] is enabled:

- Deleting files automatically by Storage Maintenance is successfully done.

When [Information] is enabled:

- Deleting manually by the Delete Files function in the [Maintenance] menu is successfully done.

6 In Any Scan Notification Events, select the check boxes for scanning status to be notified.

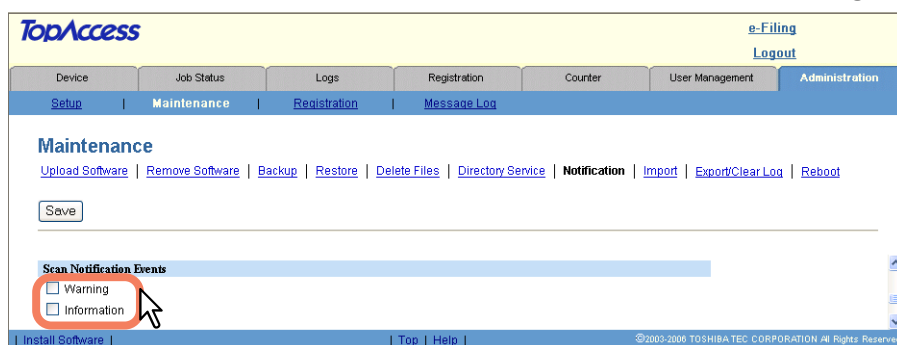


Tip

When [Send email when an error occurs] is enabled, the following events will be notified.

- Failed to acquire resource.
- Failed to delete files automatically by Storage Maintenance.

7 In Scan Notification Events, select the check boxes for scanning status to be notified.



Tip

When these are enabled, the following events will be notified.

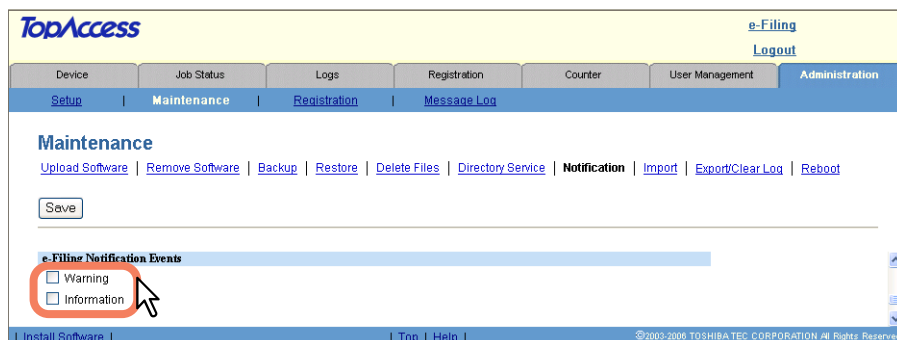
When [Warning] is enabled:

- Deleting files automatically by Storage Maintenance is successfully done.

When [Information] is enabled:

- Deleting manually by the Delete Files function in the [Maintenance] menu is successfully done.

8 In e-Filing Notification Events, select the check boxes for the status to be notified.



Tip

When these are enabled, the following events will be notified.

When [Warning] is enabled:

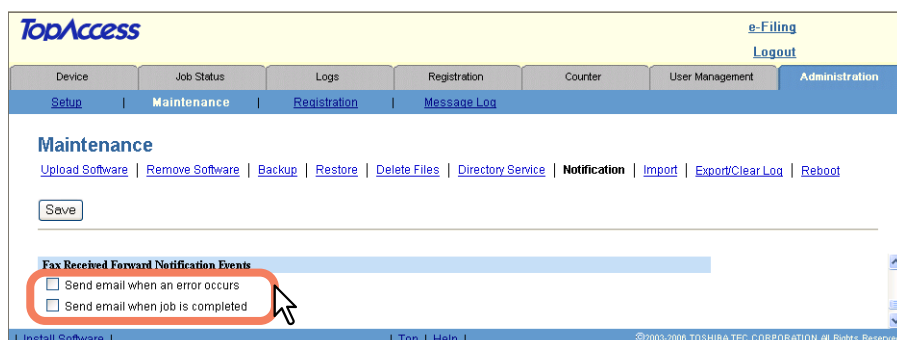
- Hard Disk space for Electronic Filing is nearly full.
- Document(s) will expire in a few days.

When [Information] is enabled:

- Initialize e-Filing Box.

In order to notify whether the e-Filing operations are successfully performed, set the notification settings in the box properties using the e-Filing web utility. For instructions on how to set the notification settings in the box properties using the e-Filing web utility, refer to the **e-Filing Guide**.

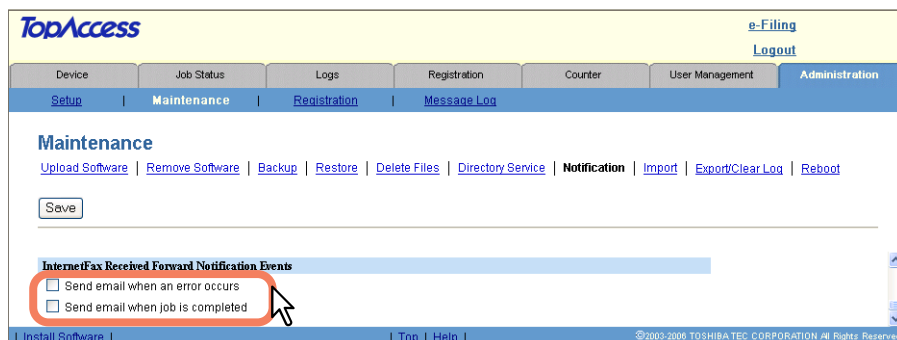
9 In Fax Received Forward Notification Events, select the check boxes for the events to be notified.



Note

Even if you select the items in the Fax Received Forward Notification Events, Emails are sent only when the optional Fax Unit is installed.

10 In Internet Fax Received Forward Notification Events, select the check boxes for the events to be notified.



11 In Firmware/Network Setting Change Notification Events, select the check boxes for the events to be notified.

Tip

When Firmware/Network Setting Change Notification Events are enabled, CSV files are created or updated to be downloaded.

A CSV file once created can be downloaded even if this setting is disabled.

12 Click [Save].

■ Importing and exporting the Address Book

This equipment allows you to import and export address book data in CSV format.

📖 P.223 "Importing the address book data"

📖 P.225 "Exporting the address book data"

□ Importing the address book data

The address book data exported in a CSV format from the address book or a different address book program in other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO4511 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series can be imported to this equipment.

The importing method of address book data is either adding imported data to the address book already registered in this equipment or deleting all the address book data already registered and replacing them with the imported data.

Data to be imported must be a comma-delimited file in a CSV format. Create address book data in any of the formats below.

```
"First Name","Last Name","Email Address","Tel Number","Company","Department"
"User01","User","user01@ifax.com","00000000001","12345 COMPANY","Dept01"
"User02","User","user02@ifax.com","00000000002","12345 COMPANY","Dept01"
"User03","User","user03@ifax.com","00000000003","12345 COMPANY","Dept01"
```

Note

If the address data of any entry items exceed the number of characters as described below, the address data will not be imported.

- First Name: 32 characters
- Last Name: 32 characters
- Email Address: 192 characters
- Tel Number: 128 characters
- Company: 64 characters
- Department: 64 characters

Tip

The group data are not included in the imported address book data.

Importing the address book data from a CSV file

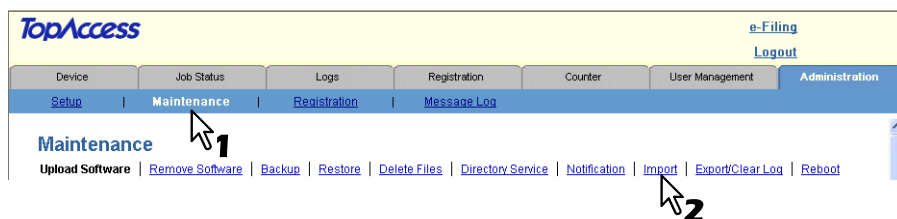
Note

Before importing the address book data, confirm that there is no print job, no scan job, and no fax job. The address book data cannot be imported if there are any jobs that have been processed. If importing the address book data takes a long time, restore the data after the equipment turns into the Sleep/Auto Shut Off mode.

1 Access TopAccess in the administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Import] submenu.



The Import submenu page is displayed.

3 If you want to change the importing method, click [Import Method].

The importing method currently set is displayed on [Current Import Method] in the Address Book area. If not changing, go to step 5.

The screenshot shows the TopAccess Maintenance page. At the top, there's a navigation bar with tabs: Device, Job Status, Logs, Registration, Counter, User Management, and Administration. Below this is a sub-navigation bar with links: Setup, Maintenance, Registration, and Message Log. The main content area is titled 'Maintenance' and contains several links: Upload Software, Remove Software, Backup, Restore, Delete Files, Directory Service, Notification, Import, Export/Clear Log, and Reboot. A button labeled 'Import Method' is highlighted with a mouse cursor. Below this button, there's a text prompt: 'Please enter file name. Importing address book may take time.' and a 'REFRESH' button. Further down, there are two sections: 'Address Book' and 'Department Code'. Each section has a 'Current Import Method' dropdown set to 'Addition', a 'File Name' input field, a 'Browse...' button, and an 'Import' button. The footer contains links for 'Install Software', 'Top', and 'Help', along with a copyright notice: '©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved'.

The Import Method page is displayed.

4 Select the desired import method, and then click [Save].

The screenshot shows the 'Import Method' dialog box. It has a title bar 'Import Method' and two buttons: 'Save' and 'Cancel'. Below the buttons is a section labeled 'Address' with two radio buttons: 'Addition' (which is selected and circled in red with a '2' next to it) and 'Overwrite' (which is circled in red with a '1' next to it). The background shows a blurred view of the Maintenance page.

Addition — Select this to add the imported address book data into the address book already registered in this equipment.

Overwrite — Select this to delete all the address book data registered in this equipment and replace them with the imported address book data.

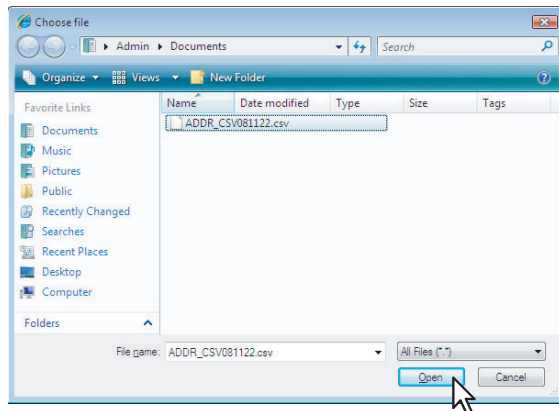
The Import Method page is closed.

5 Click [Browse] in the Address Book area.

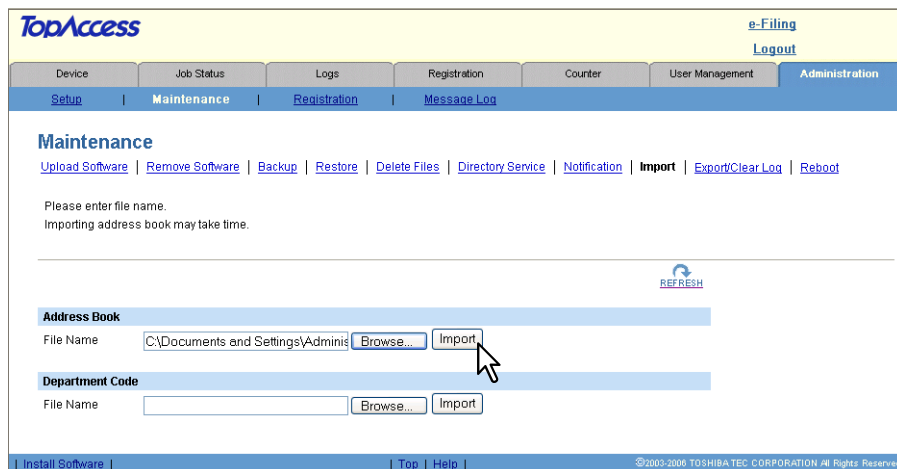
The screenshot shows the TopAccess Maintenance page, similar to the first one. In the 'Address Book' section, the 'File Name' input field is active, and the 'Browse...' button is highlighted with a mouse cursor. The 'Import' button is also visible. The 'Department Code' section below it also has a 'File Name' input field, a 'Browse...' button, and an 'Import' button. The footer is the same as the previous screenshot.

The Choose File dialog box appears.

6 Select the CSV file that contains address book data and click [Open].



7 Click [Import].



The data is imported to the address book.

□ Exporting the address book data

You can export address information for use in another TopAccess address book or another address book program.

Tip

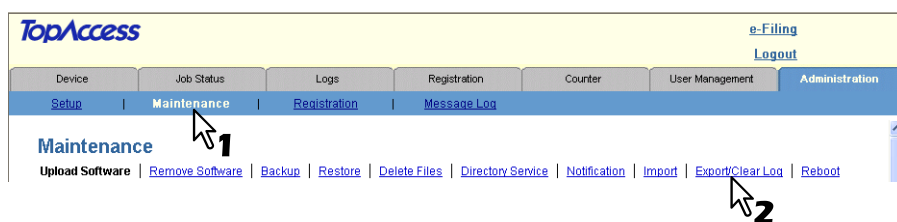
The group data are not included in the exported address book data.

Exporting the address book data as a CSV file

1 Access TopAccess in the administrator mode.

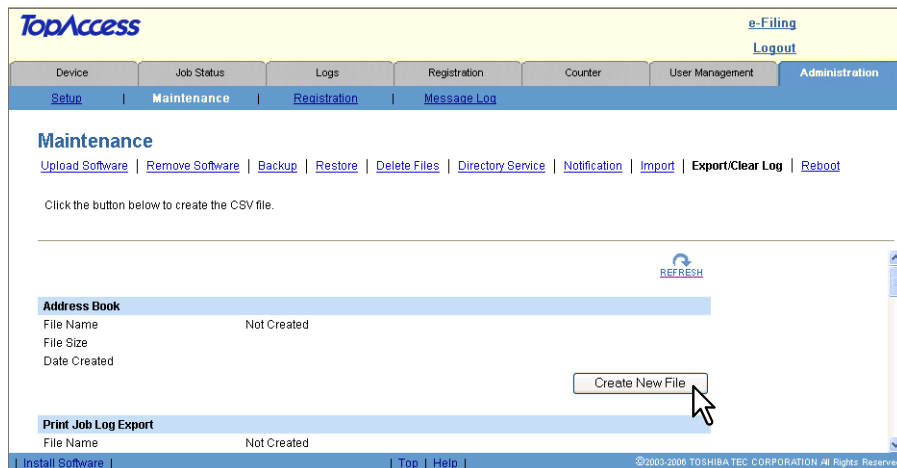
📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Export/Clear Log] submenu.



The Export/Clear Log submenu page is displayed.

3 Click [Create New File] in the Address Book area.

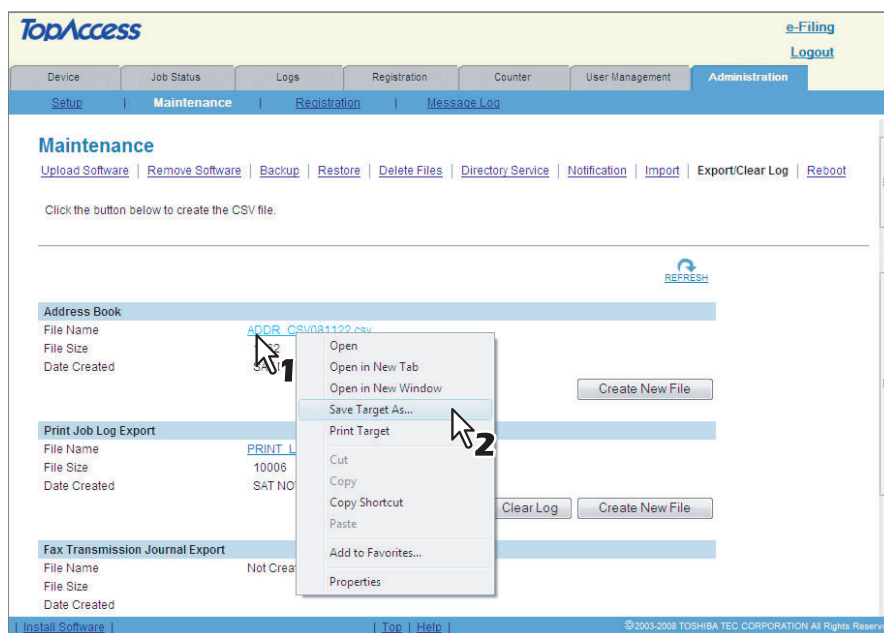


The CSV file name will be displayed.

Tip

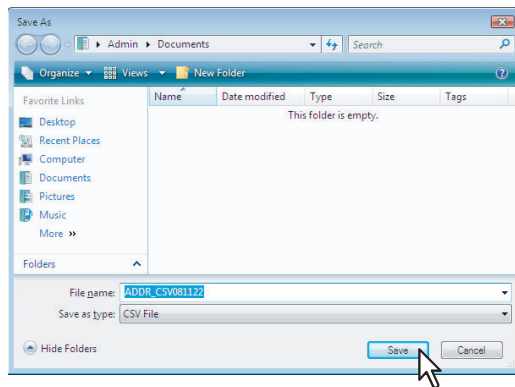
If you previously exported address book data, the exported file link and information are displayed in the Address Book area. You can click the link to save the previously exported file.

4 Right-click the [File Name] link and select [Save Target As].



The [Save As] dialog box appears.

5 Select the file location and select [All Files] or [.csv Document] in the [Save as type] box.



6 Click [Save]

The CSV file that contains the address book data is saved in the selected location.

■ Importing and exporting the department code

An administrator can import and export department code data in CSV format.

📖 P.228 “Importing the department code data”

📖 P.229 “Exporting the department code data”

□ Importing the department code data

The department code data exported in a CSV format from other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO4511 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series can be imported to this equipment. When the department code data are imported, the existing department code data are overwritten with the imported one.

The imported file must be a comma delimited CSV file and created in a suitable format for the department code data.

Importing the department code data from a CSV file

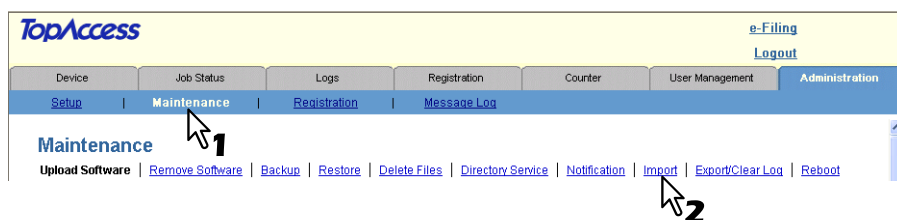
Note

Before importing the department code data, confirm that there is no print job, no scan job, and no fax job. The department code data cannot be imported if there are any jobs that have been processed. If importing the department code data takes a long time, restore the data after the equipment turns into the Sleep/Auto Shut Off mode.

1 Access TopAccess in the administrator mode.

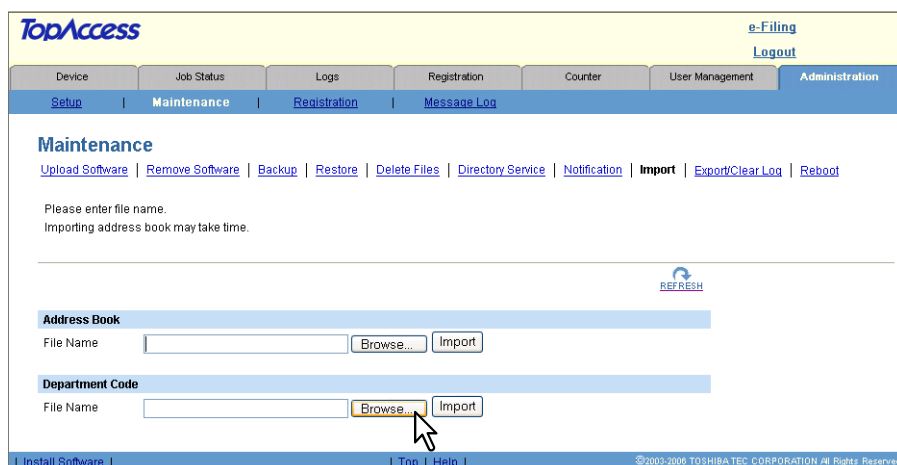
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Maintenance] menu and [Import] submenu.



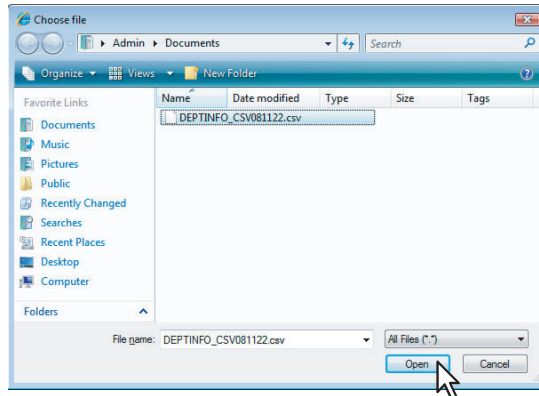
The Import submenu page is displayed.

3 Click [Browse] in the Department Code area.

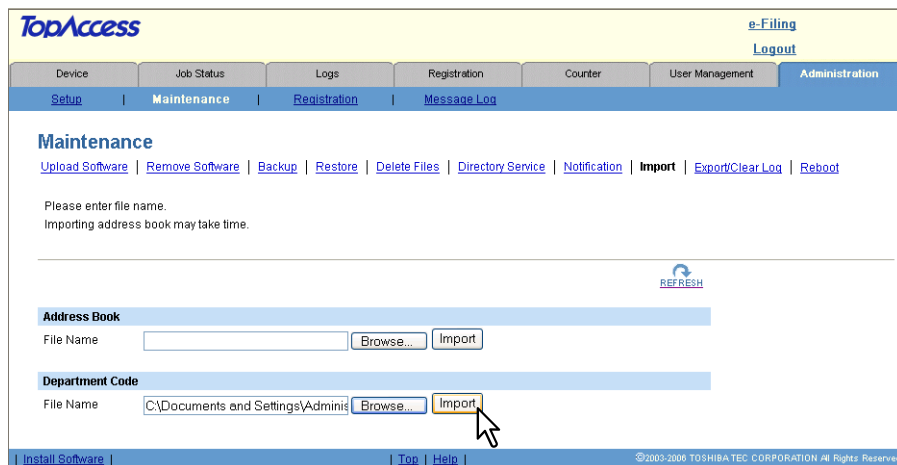


The Choose File dialog box appears.

4 Select the CSV file that contains department code data and click [Open].



5 Click [Import].



The data are imported to the department code information.

□ Exporting the department code data

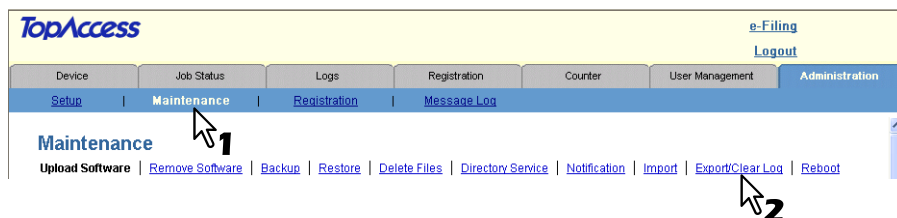
You can export department code information for use in other equipment.

Exporting the department code data as a CSV file

1 Access TopAccess in the administrator mode.

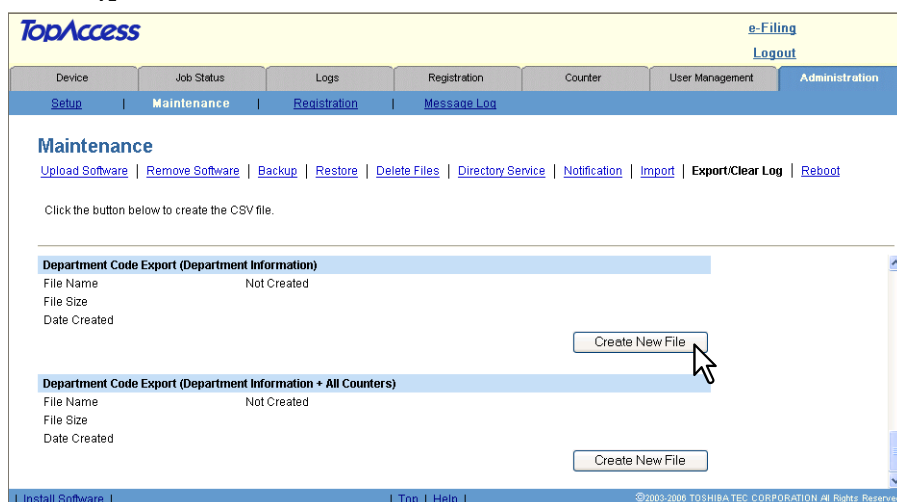
📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Export/Clear Log] submenu.



The Export/Clear Log submenu page is displayed.

- 3** When you want to export only department code information, click **[Create New File]** in the **[Department Code Export (Department Information)]** area.
When you want to export department code information with counter information, click **[Create New File]** in the **[Department Code Export (Department Information + All Counters)]** area.

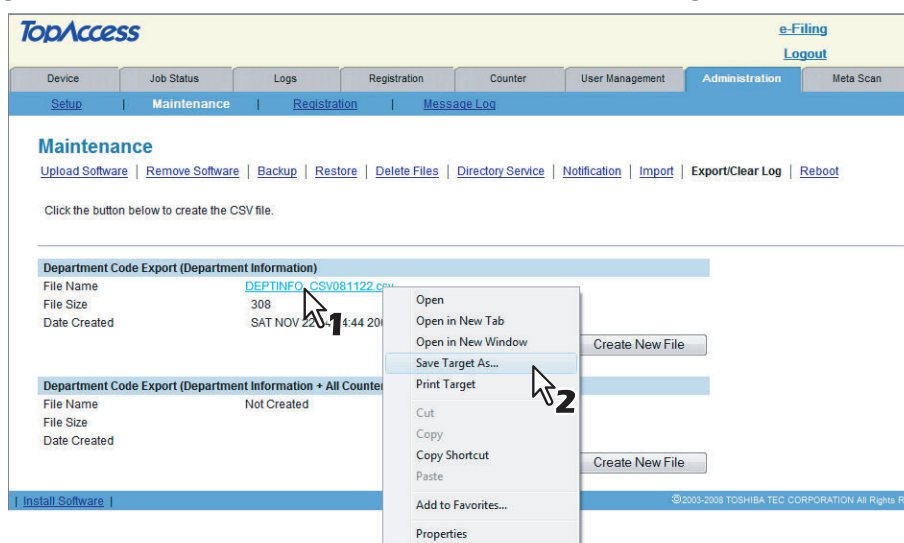


The CSV file name will be displayed.

Tip

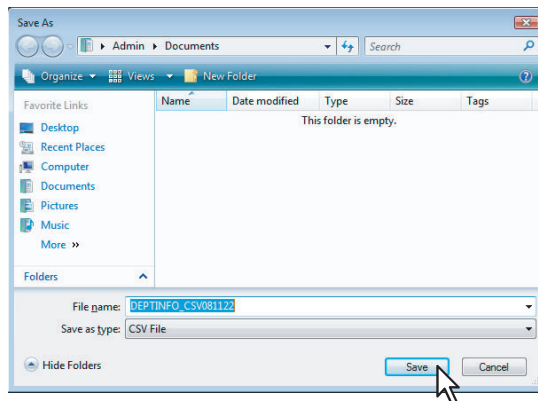
If you previously exported department code data, the exported file link and information are displayed in the Department Code Export area. You can click the link to save the previously exported file.

- 4** Right-click the **[File Name]** link and select **[Save Target As]**.



The **[Save As]** dialog box appears.

5 Select the file location and select [All Files] or [.csv Document] in the [Save as type] box.



6 Click [Save].

The CSV file that contains the department code data is saved in the selected location.

Exporting the logs, journals, and counters

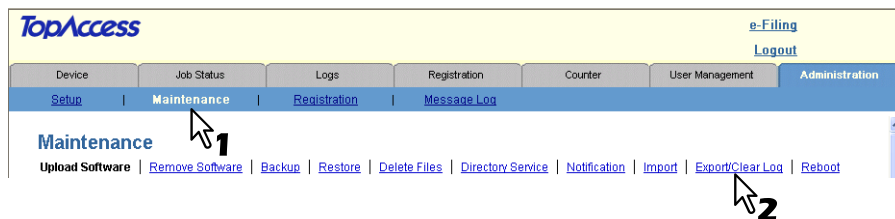
An administrator can export logs and journals in this equipment as CSV files. Before clearing them, you can save the logs, journals, and counters as files.

Exporting the logs, journals, and counters as a CSV file

1 Access TopAccess in the administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Maintenance] menu and [Export/Clear Log] submenu.

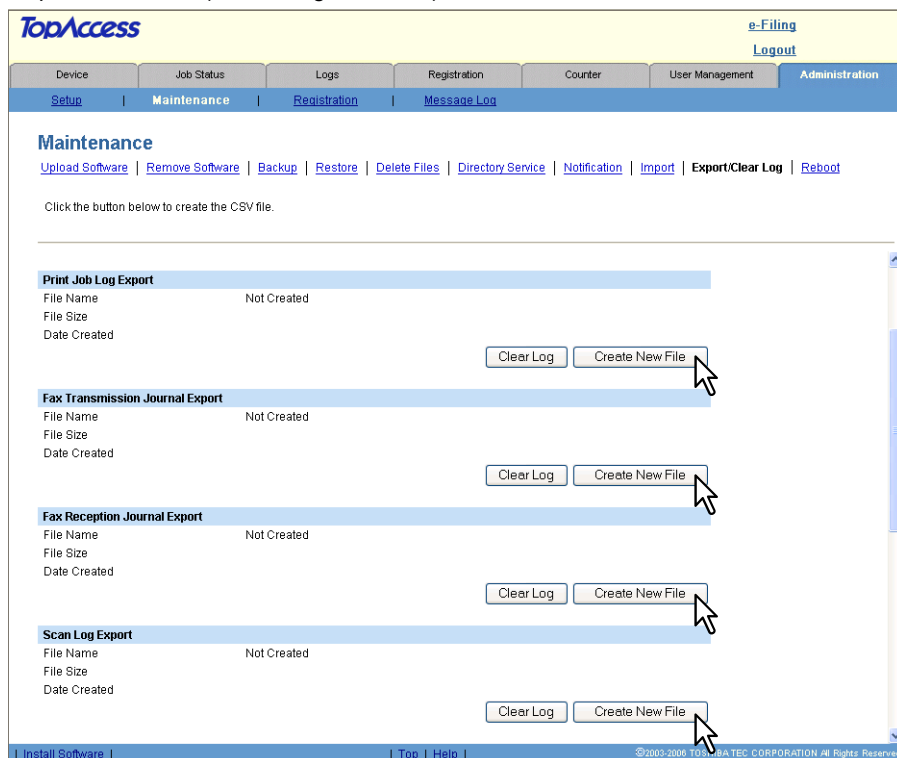


The Export/Clear Log submenu page is displayed.

3 Click [Create New File] in the area of logs or journals that you want to export.

You can export the following logs and journals.

- Print Job Log
- Fax Transmission Journal
- Fax Reception Journal
- Scan Log
- Message Log
- Department Code (Small/Large Counter)

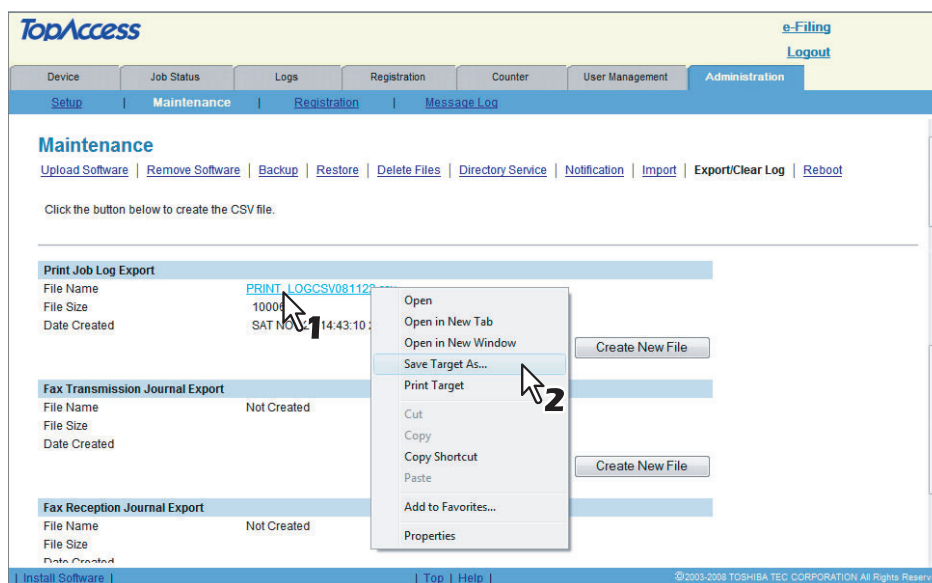


The CSV file name will be displayed.

Tip

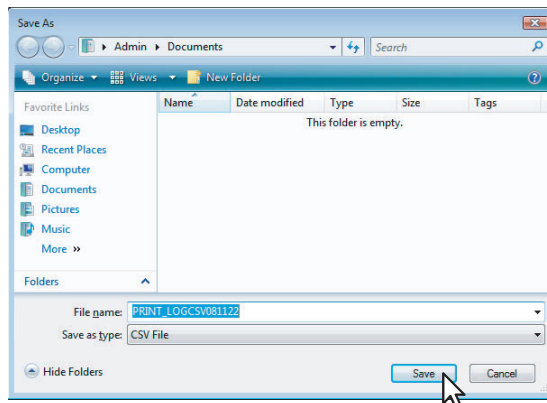
If you previously exported data, the exported file link and information are displayed in each area. You can click the link to save the previously exported file.

4 Right-click the [File Name] link and select [Save Target As].



The [Save As] dialog box appears.

- 5** Select the file location and select [All Files] or [.csv Document] in the [Save as type] box.



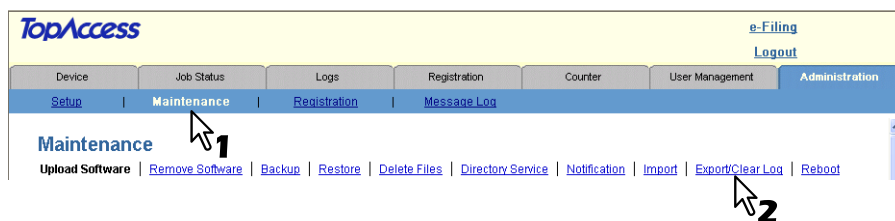
- 6** Click [Save].
The CSV file that contains the logs or journals data is saved in the selected location.

■ Clearing the logs and journals

An administrator can clear logs and journals in this equipment. This maintenance procedure is recommended periodically to maintain the hard disk.

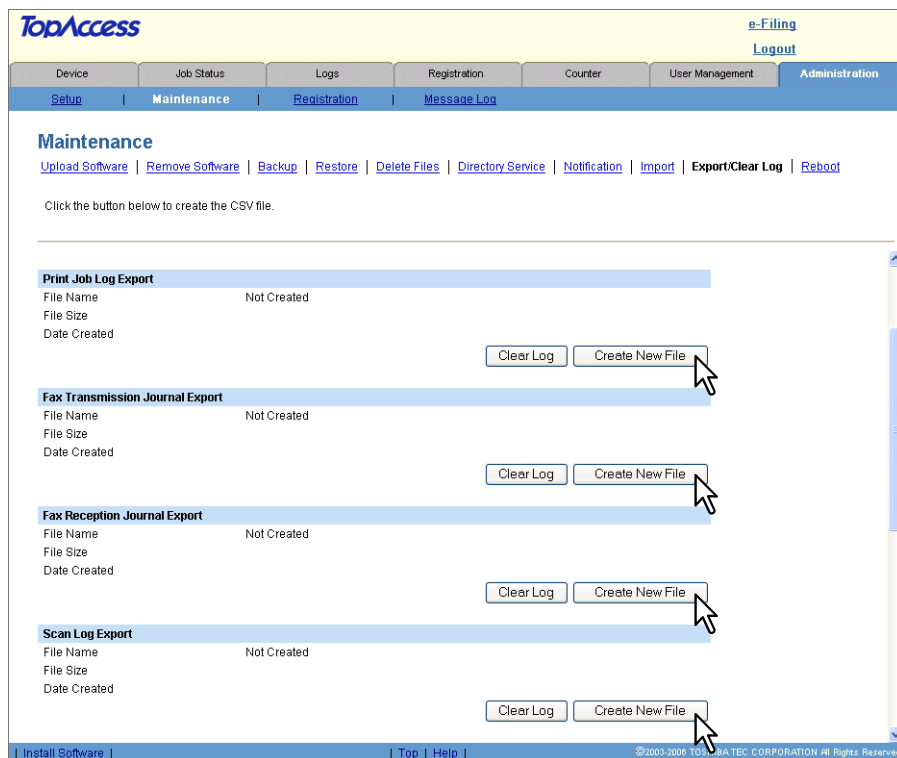
Clearing the logs and journals

- 1** Access TopAccess in the administrator mode.
P.106 "Accessing TopAccess Administrator Mode"
- 2** Click the [Maintenance] menu and [Export/Clear Log] submenu.



The Export/Clear Log submenu page is displayed.

3 Click [Clear Log] in the area of logs or journals that you want to clear.



The selected logs are cleared.

■ Rebooting the equipment

An administrator can reboot the equipment.

Note

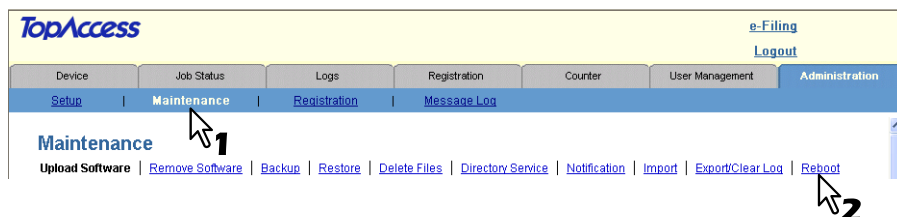
Rebooting the equipment cannot be performed when there are jobs in progress.

Rebooting the equipment

1 Access TopAccess in the administrator mode.

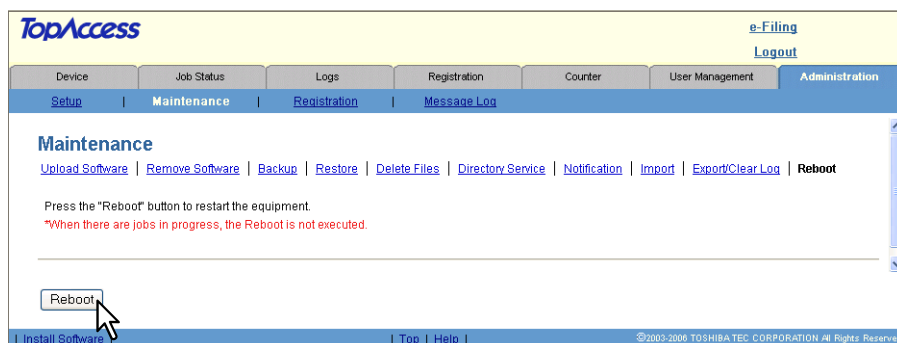
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Maintenance] menu and [Reboot] submenu.



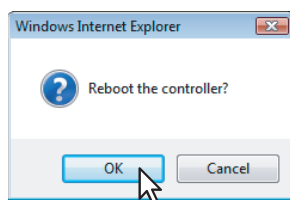
The Reboot submenu page is displayed.

3 Click [Reboot] to reboot the equipment.



The confirmation dialog box appears.

4 Click [OK].



The equipment is restarted.

Note

While the equipment is being restarted, the network will not be available. TopAccess will display “Please restart after waiting a few minutes.”. The touch panel will display “NETWORK INITIALIZING”. When this “NETWORK INITIALIZING” message disappears, TopAccess will once again be available.

Registering From TopAccess

In the [Registration] menu in the TopAccess administrator mode, an administrator can register the public Templates, and relay transmissions of received faxes/internet faxes.

Public Template

The administrator can create public templates that are held in a public template group available to everyone.

📖 P.236 “Registering public templates”

Fax Received Forward, Internet Fax Received Forward

An administrator can register the agent to which all received faxes/internet faxes are forwarded to enable the documents to be checked.

📖 P.245 “Registering Fax and Internet Fax received forward”

Note

The Fax Received Forward can be registered only when the optional Fax Unit is installed.

■ Registering public templates

Administrators create and maintain public templates and manage the public template group. Users can display and use public templates but cannot modify them.

The public group can contain up to 60 public templates. Typically, these are general-purpose templates available to all users.

TopAccess in the administrator mode allows the following operations for managing the public templates:

📖 P.236 “Creating or editing the public templates”

📖 P.242 “Resetting the public template”

□ Creating or editing the public templates

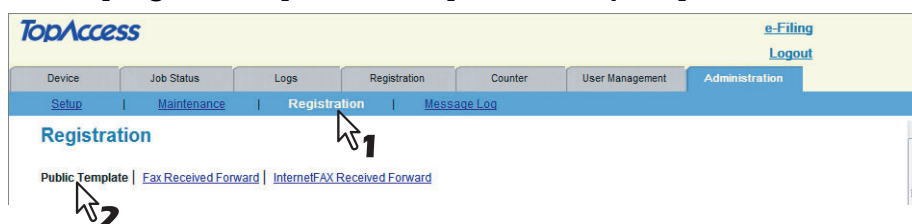
Use the Templates page to set up and modify templates.

Creating or editing the public templates

1 Access TopAccess in the administrator mode.

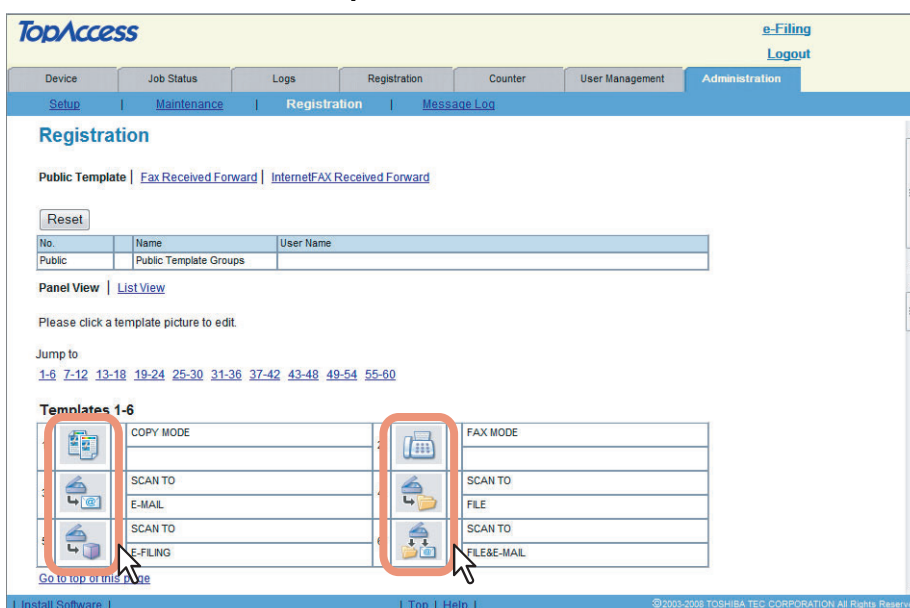
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Registration] menu and [Public Template] submenu.



The Public Template submenu page is displayed.

3 From the templates list, click the [Undefined] icon to register a new template, or click defined icon to edit the template.

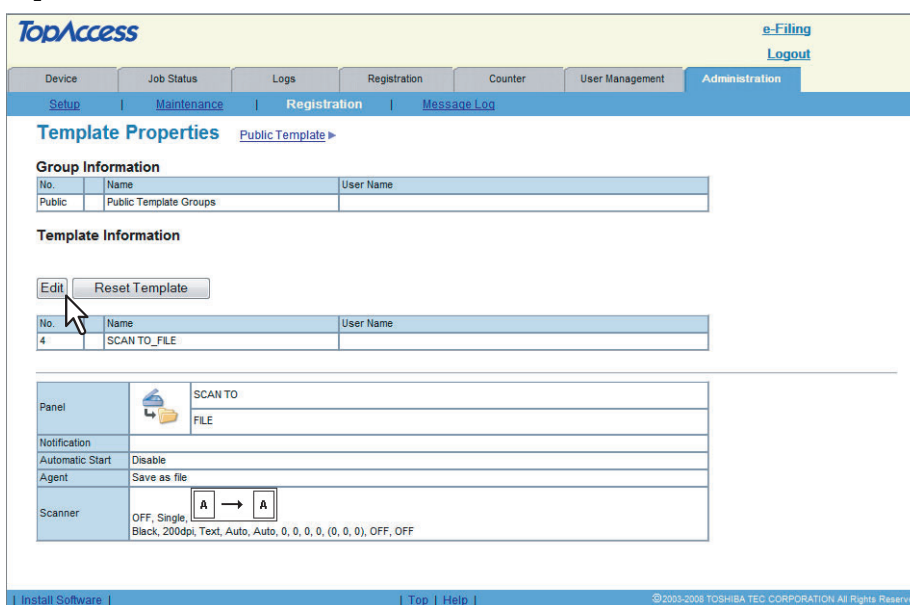


- If the templates list is displayed in the List View, click the [Undefined] template name to register a new template, or click a defined template name to edit the template.
- If you select a public template that has not been defined, the Template Properties page to select agents is displayed. Skip to step 5.
- If you select a defined private template, the Template Properties page is displayed. Go to the next step.

Tips

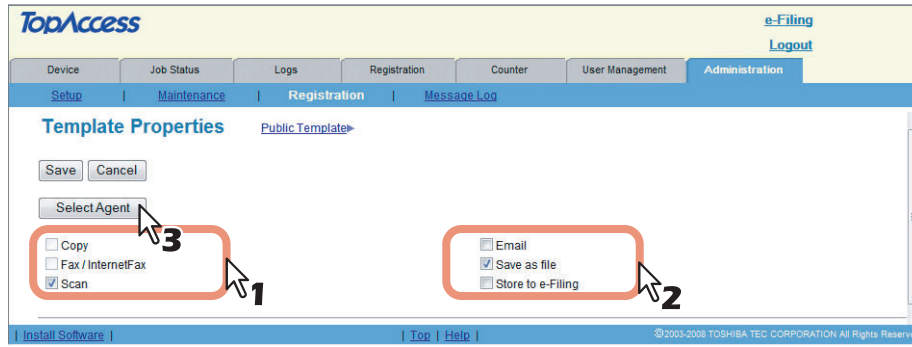
- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which public template you want to define or edit, click the number of the public template in the [Jump to] links.

4 When you edit an existing template, the following window will be displayed. Click [Edit].



The Template Properties page to select agents is displayed.

5 Select agents and click [Select Agent].



You can select one of the following templates:

Copy — Select this to create a copy template. Usually, this is selected to print copies as well as sending originals to other destinations. This agent can also be combined with the Save as file agent or Store to e-Filing agent.

Fax/InternetFax — Select this to create a fax and Internet Fax transmission template. This agent can be combined with the Save as file agent.

Scan — Select this to create a scan template combined with the Email, Save as file, and Store to e-Filing agents. When you select this, select the agent from [Email], [Save as file], or [Store to e-Filing]. You can specify up to two agents for a scan template.

6 Click each button displayed in the page to specify or edit the associated template properties.

[Panel Setting] — Click this to specify the icon settings for the template.

P.240 “Panel Setting (Public template)”

Panel Setting	
Picture	
Caption1	SCAN TO
Caption2	FILE
User Name	
Automatic Start	Disable
Notification	

[Destination Setting] — Click this to specify the document's destination. This can be set only when creating a Fax/Internet Fax agent or Email agent.

P.240 “Destination Setting (Public template)”

When Creating the Fax/Internet Fax agent:

Destination Setting	
Destination	

When Creating the Email agent:

To: Destination Setting	
To: Destination	

Cc: Destination Setting	
Cc: Destination	

Tip

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

P.183 “Setting up Email settings”

To: Destination Setting	
To: Destination	

Bcc: Destination Setting	
Bcc: Destination	

[InternetFax Setting] — Click this to specify how the document will be sent. This can be set only when creating a Fax/Internet Fax agent.

P.241 “InternetFax Setting (Public template)”

InternetFax Setting	
Subject	Scanned from (Device Name)(Template Name)(Date)(Time)
From Address	admin@fax.com
From Name	admin
Body	
File Format	TIFF-S
Fragment Page Size	No Fragmentation

[Fax Setting] — Click this to specify how the document will be sent. This can be set only when creating a Fax/Internet Fax agent.

P.241 “Fax Setting (Public template)”

Fax Setting	
Resolution	Standard
Original Mode	Text
Exposure	Auto
Transmission Type	
ECM	ON
Line Select	
Quality Transmit	
SUB/SEP	
Poling	
Delayed Transmit	00 00:00
Priority Transmit	OFF

[Email Setting] — Click this to specify how the document will be sent. This can be set only when creating an Email agent.

P.241 “Email Setting (Public template)”

Email Setting	
Subject	
From Address	mfp-00c67861@fax.com
From Name	MFP-00C67861
Body	
File Format	PDF(Multi)
File Name	DocMDDYY(MMDDYY is a date)
Fragment Message Size	No Fragmentation

[Save as file Setting] — Click this to specify how the document will be stored in the local hard disk or network folder. This can be set only when creating a Save as file agent.

P.241 “Save as file Setting (Public template)”

Save as file Setting	
File Format	TIFF(Mult)
Destination	\\MFP-04958820\FILE_SHARE\
File Name	DocMMDYY(MMDYY is a date)

[Box Setting] — Click this to specify how the document will be stored in the Box. This can be set only when creating a Store to e-Filing agent.

P.241 “Box Setting (Public template)”

Box Setting	
Destination	000
Folder Name	
Document Name	DocMMDYY(MMDYY is a date)

[Scan Setting] — Click this to specify how the document will be scanned. This can be set only when creating a Save as file agent, Email agent, or Store to e-Filing agent. This cannot be set when combining with a Fax/Internet Fax agent.

P.241 “Scan Setting (Public template)”

Scan Setting	
Preview	OFF
Single/2-Sided Scan	Single
Rotation	
Color Mode	Black
Resolution	600dpi
Compression	
Original Mode	Text
Exposure	Auto
Original Size	Auto
Background	0
Contrast	0
Sharpness	0
Saturation	0
RGB Adjustment	Red: 0 Green: 0 Blue: 0
Omt Blank Page	OFF
Outside Erase	OFF

7 After configuring the desired template properties, click [Save].

The template properties are registered.

Panel Setting (Public template)

In the Panel Setting page, specify how the icon for the template is displayed in the touch panel, and the notification settings for the template.

Instructions on how to set the Panel Setting for public templates are the same as for setting the Panel Setting for private templates.

P.51 “Panel Setting (Private template)”

Destination Setting (Public template)

In the Recipient List page, you can specify the destinations to which the fax, Internet Fax, or Scan to Email document will be sent.

When you are setting destinations for an Email agent, you can only specify the Email addresses for the destinations.

When you are setting destinations for a Fax/Internet Fax agent, you can specify both fax numbers and Email addresses for the destinations.

Note

However, the optional Fax Unit must be installed in this equipment to specify the fax numbers of the destinations.

You can specify the recipients by entering their Email addresses or fax numbers manually, selecting recipients from the address book, selecting recipient groups from the address book, or searching for recipients in the LDAP server.

Instructions on how to set the Destination settings for public templates are the same as for setting the Destination settings for private templates.

P.52 “Destination Setting (Private template)”

InternetFax Setting (Public template)

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

Instructions on how to set the Internet Fax settings for public templates are the same as for setting the Internet Fax settings for private templates.

 P.58 "InternetFax Setting (Private template)"

Fax Setting (Public template)

In the Fax Setting page, you can specify how the fax will be sent.

Instructions on how to set the Fax settings for public templates are the same as setting the Fax settings for private templates.

 P.59 "Fax Setting (Private template)"

Email Setting (Public template)

In the Email Setting page, you can specify the content of the Scan to Email document to be sent.

Instructions on how to set the Email settings for public templates are the same as for setting the Email settings for private templates.

 P.61 "Email Setting (Private template)"

Save as file Setting (Public template)

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

Instructions on how to set the Save as file settings for public templates are the same as for setting the Save as file settings for private templates.

 P.63 "Save as file Setting (Private template)"

Box Setting (Public template)

In the Box Setting page, you can specify how scanned images will be stored in the Box.

Instructions on how to set the Box settings for public templates are the same as for setting the Box settings for private templates.

 P.66 "Box Setting (Private template)"

Scan Setting (Public template)

In the Scan Setting page, you can specify how originals are scanned for the Save as file, Email, and Store to e-Filing agent.

Instructions on how to set the Scan settings for public templates are the same as for setting the Scan settings for private templates.

 P.67 "Scan Setting (Private template)"

❑ Resetting the public template

You can reset a public template that you have registered.

You can reset a public template that you selected, or you can reset all public templates that are registered in the Public Template Group.

📖 P.242 “Resetting a public template”

📖 P.244 “Resetting all public templates”

Resetting a public template

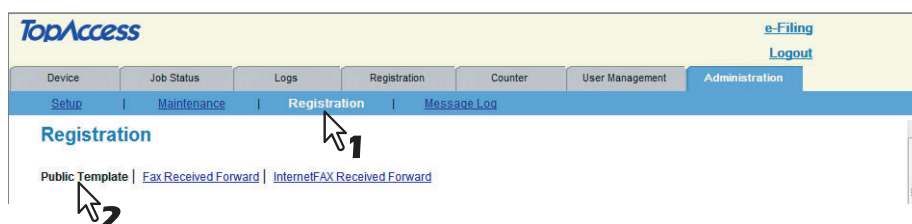
To reset an unnecessary public template, perform the following procedure.

Resetting a public template

1 Access TopAccess in the administrator mode.

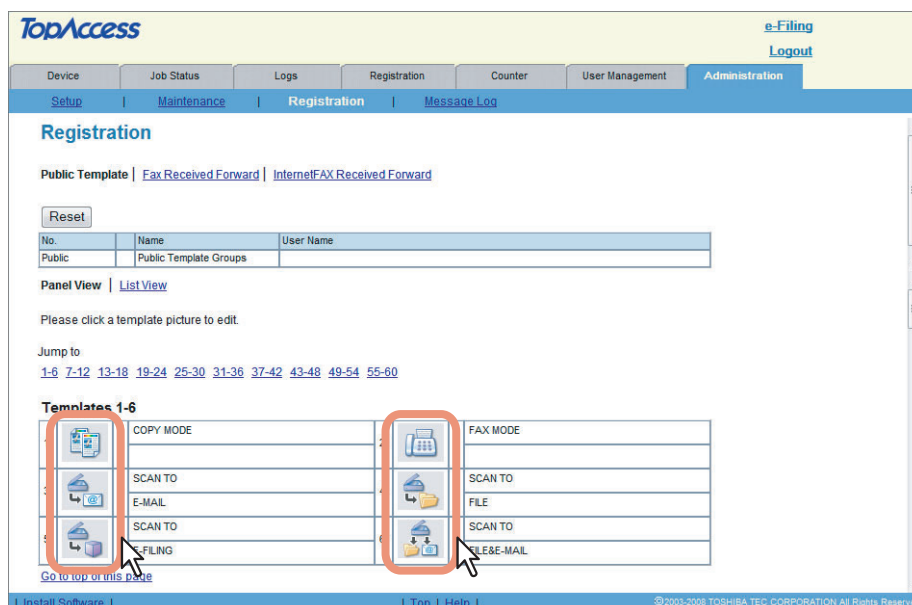
📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Registration] menu and [Public Template] submenu.



The Public Template submenu page is displayed.

3 From the templates list, click the template icon that you want to reset.



- If the templates list is displayed in the List view, click the template name that you want to reset.
- The Template Properties page is displayed.

Tips

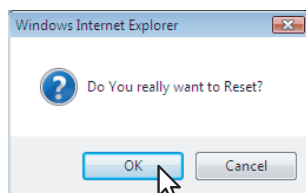
- You can change the template list view by clicking on either [Panel View] or [List View].
- If you know which public template you want to reset, click the number of the public template in the [Jump to] links.

4 Click [Reset Template].

The screenshot shows the 'Template Properties' page in the TopAccess Administrator. The page has a navigation bar with tabs: Setup, Maintenance, Registration, and Message Log. The 'Registration' tab is active. Below the navigation bar, there are sections for 'Group Information' and 'Template Information'. The 'Template Information' section contains a table with columns 'No.', 'Name', and 'User Name'. The first row shows '4' in the 'No.' column and 'SCAN TO_FILE' in the 'Name' column. Below this table, there are several configuration options: 'Panel' (SCAN TO, FILE), 'Notification' (Disable), 'Automatic Start' (Save as file), and 'Scanner' (OFF, Single, Black, 200dpi, Text, Auto, Auto, 0, 0, 0, 0, 0, 0, 0, 0, OFF, OFF). The 'Reset Template' button is highlighted with a mouse cursor.

The confirmation dialog box appears.

5 Click [OK].



The selected template is cleared.

Resetting all public templates

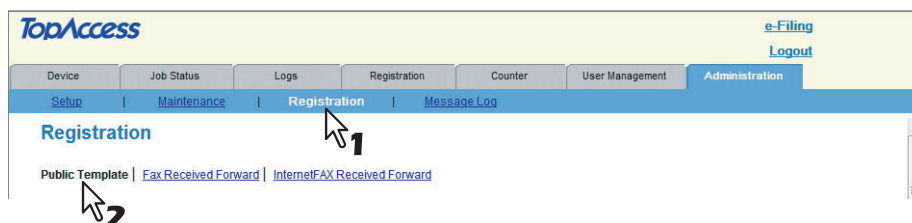
To reset all public templates, perform the following procedure.

Resetting all public templates

1 Access TopAccess in the administrator mode.

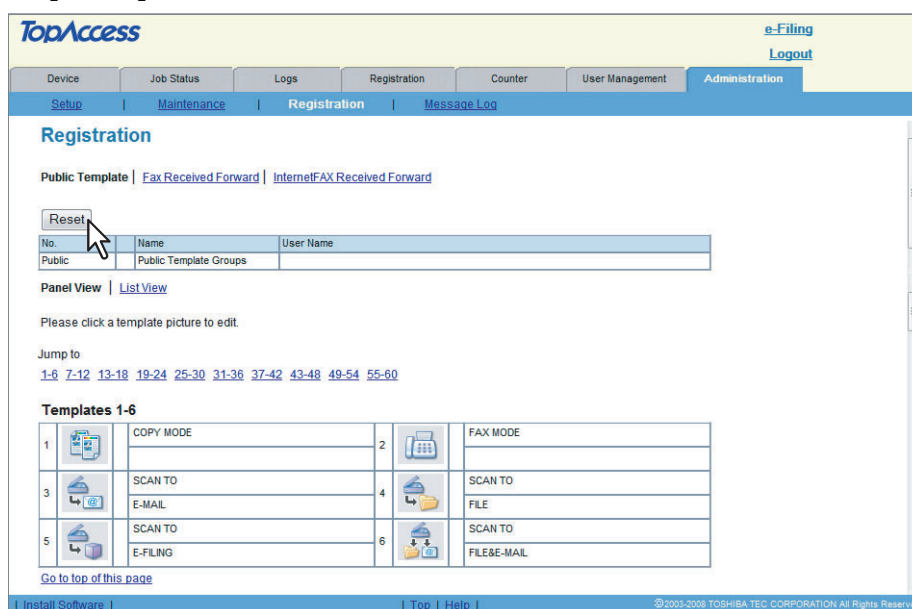
P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Registration] menu and [Public Template] submenu.



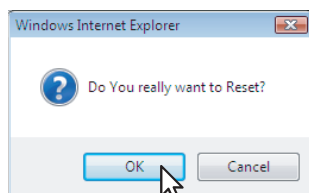
The Public Template submenu page is displayed.

3 Click [Reset].



The confirmation dialog box appears.

4 Click [OK].



The group information is cleared.

■ Registering Fax and Internet Fax received forward

The Fax Received Forward and Internet Fax Received Forward allow you to transmit received fax or Internet Faxes to specific destinations — to check all fax and Internet Faxes received.

Notes

- The Fax Received Forward can be registered only when the optional Fax Unit is installed.
- When the 2nd line board is installed, the received faxes are forwarded to the specified destinations according to the Fax Received Forward setting regardless of whether the faxes are received through line 1 or line 2.

The received fax and Internet Faxes can be transmitted to the following destinations:

- Other Internet Fax devices
- Local folder in this equipment or network folders
- Email addresses
- Box in this equipment

Registering the Fax or Internet Fax received forward

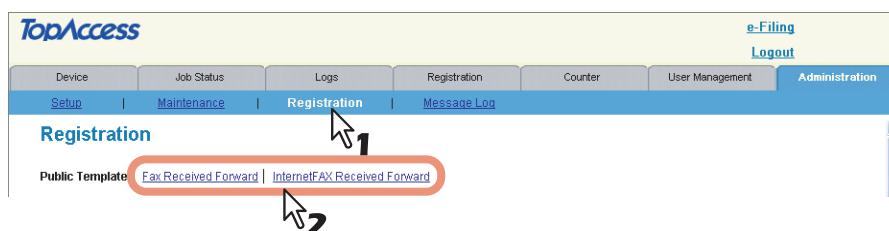
Tip

The procedures to register the Fax Received Forward and Internet Fax Received Forward are almost the same.

1 Access TopAccess in the administrator mode.

📖 P.106 “Accessing TopAccess Administrator Mode”

2 Click the [Registration] menu and [Fax Received Forward] submenu to register the Fax Received Forward, or click the [InternetFax Received Forward] submenu to register the Internet Fax Received Forward.



- When you click the [Fax Received Forward] submenu, the Fax Received Forward submenu page is displayed.
- When you click the [InternetFax Received Forward] submenu, the Internet Fax Received Forward submenu page is displayed.

3 Select the [Forward] check box and select the desired agents and click [Select Agent].

Tip

To disable the Fax Received Forward or Internet Fax Received Forward, clear the [Forward] check box and click [Select Agent], and then click [Save].

InternetFax — Select this to transmit received fax or Internet Faxes to other Internet Fax devices. This agent can be combined with the Save as file agent or Store to e-Filing agent.

Save as file — Select this to transmit received fax or Internet Faxes to local folder in this equipment or to network folders. This agent can be combined with another agent.

Email — Select this to transmit received fax or Internet Faxes to Email addresses. This agent can be combined with the Save as file agent or Store to e-Filing agent.

Store to e-Filing — Select this to transmit received fax or Internet Faxes to e-Filing. This agent can be combined with another agent.

Note

The image quality of the file that is stored by Save as file, Email, and Store to e-Filing is different from the output of the received fax when it is printed.

4 Use the [Document Print] box to select when the Fax or InternetFax Received Forward document will be printed.

Always — Select this to always print a forwarded document.

ON ERROR — Select this to print a forwarded document when the document will not be sent for all destinations due to errors.

5 Click each button displayed in the page to specify or edit the associated properties.

[Destination Setting] — Click this to specify the destinations of documents sent. This can be set only when registering the Internet Fax, or Email agent.

P.248 “Destination Setting (Fax/Internet Fax received forward)”

When Registering the Internet Fax agent:

Destination Setting	
Destination	

When Registering the Email agent:

To: Destination Setting	
To: Destination	

Cc: Destination Setting	
Cc: Destination	

Tip

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

P.183 “Setting up Email settings”

To: Destination Setting	
To: Destination	

Bcc: Destination Setting	
Bcc: Destination	

[InternetFax Setting] — Click this to specify how the document will be sent. This can be set only when registering the Internet Fax agent.

P.252 “InternetFax Setting (Fax/Internet Fax Received Forward)”

InternetFax Setting	
Subject	Scanned from (Device Name)\(Template Name)\(Date)\(Time)
From Address	admin@fax.com
From Name	admin
Body	
File Format	TIFF-S
Fragment Page Size	No Fragmentation

[Email Setting] — Click this to specify how the document will be sent. This can be set only when registering the Email agent.

P.253 “Email Setting (Fax/Internet Fax received forward)”

Email Setting	
Subject	Scanned from (Device Name)\(Template Name)\(Date)\(Time)
From Address	mfp-00c67861@fax.com
From Name	MFP-00C67861
Body	
File Format	PDF(Multi)
Encryption	Disable
File Name	(Sender)-NNN (NNN is a sequential number)
Fragment Message Size	No Fragmentation

[Save as file Setting] — Click this to specify how the document will be stored in the local hard disk or network folder. This can be set only when registering the Received to File agent.

P.255 “Save as file Setting (Fax/Internet Fax received forward)”

Save as file Setting	
File Format	TIFF(Multi)
Encryption	Disable
Destination	\\MFP-05212774\FILE_SHARE\
File Name	(Sender)-NNN (NNN is a sequential number)

[Box Setting] — Click this to specify how the document will be stored in e-Filing. This can be set only when registering the Store to e-Filing agent.

P.258 “Box Setting (Fax/Internet Fax received forward)”

Box Setting	
Destination	000
Folder Name	
Document Name	(Sender)-NNN (NNN is a sequential number)

6 After configuring the desired properties, click [Save].

The Fax or Internet Fax Received Forward properties are registered.

❑ Setting up Fax or Internet Fax received forward properties

This section describes how to set items in each agent's properties.

Destination Setting (Fax/Internet Fax received forward)

In the Recipient List page, you can specify the destinations to which the received faxes or Internet Faxes will be transmitted.

You can specify the recipients by entering Email addresses manually, selecting recipients from the address book, selecting recipient groups from the address book, or searching for recipients in the LDAP server.

📖 P.248 "Entering the recipients manually"

📖 P.249 "Selecting the recipients from the address book"

📖 P.250 "Selecting the groups from the address book"

📖 P.251 "Searching for recipients in the LDAP server"

📖 P.252 "Removing the contacts from the recipient list"

Entering the recipients manually

Using this method, you can add a recipient manually to the Recipient List.

- 1 Click [Destination Setting] to open the Recipient List page.**
- 2 Click [New].**

The Contact Property page is displayed.

- 3 Enter the Email address of the recipient, in the [Destination] box.**

- 4 Click [OK].**
Entered recipient is added to the Recipient List page.
- 5 Repeat step 2 to 4 to add all recipients you require.**

Tip

You can remove contacts that you have added to the recipient list before saving the destination settings.

📖 P.252 "Removing the contacts from the recipient list"

- 6 Click [Save].**

The contacts are added as destinations.

Selecting the recipients from the address book

By this method, you can select recipients from the address book.

- 1 Click [Destination Setting] to open the Recipient List page.
- 2 Click [Address Book].

Recipient List

☒	Name	Destination

The Address Book page is displayed.

- 3 Select the [Email] check boxes of users you want to add as the recipients.**

Address Book

Group: All Groups

Add Cancel

Email	Name	Email Address
☒	User99 User	user99@fzax.com
☒	User98 User	user98@fzax.com
☒	User97 User	user97@fzax.com
☒	User96 User	user96@fzax.com
☒	User95 User	user95@fzax.com
☐	User94 User	user94@fzax.com
☐	User93 User	user93@fzax.com
☐	User92 User	user92@fzax.com
☐	User91 User	user91@fzax.com
☐	User90 User	user90@fzax.com
☐	User89 User	user89@fzax.com

Note

If you want to sort the recipient list by a specific group, select the desired group name in the [Group] box.

- 4 Click [Add].**
The selected recipients are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before saving the destination settings.

 P.252 “Removing the contacts from the recipient list”

- 5 Click [Save].**

Recipient List

☒	▼ Add	Destination
☐	User99 User	user99@ifax.com
☐	User98 User	user98@ifax.com
☐	User97 User	user97@ifax.com
☐	User96 User	user96@ifax.com
☐	User95 User	user95@ifax.com

The contacts are added as destinations.

Selecting the groups from the address book

By this method, you can select groups from the address book.

1 Click [Destination Setting] to open the Recipient List page.

2 Click [Address Group].



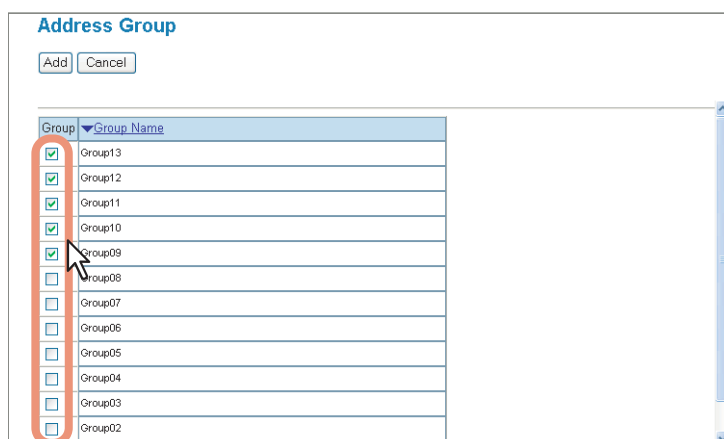
Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐		

The Address Group page is displayed.

3 Select the [Group] check boxes that contain the desired recipients.



Address Group

Add Cancel

Group	Group Name
☒	Group13
☒	Group12
☒	Group11
☒	Group10
☒	Group09
☐	Group08
☐	Group07
☐	Group06
☐	Group05
☐	Group04
☐	Group03
☐	Group02

4 Click [Add].

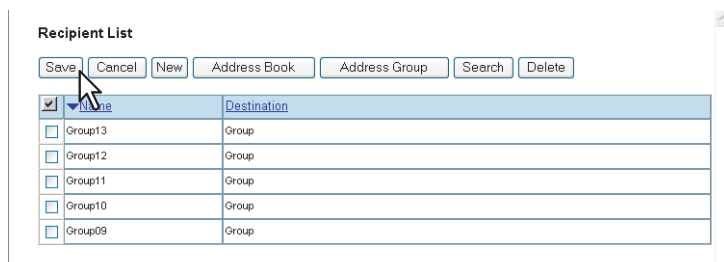
All recipients in the selected groups are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before saving the destination settings.

 P.252 "Removing the contacts from the recipient list"

5 Click [Save].



Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐	Group13	Group
☐	Group12	Group
☐	Group11	Group
☐	Group10	Group
☐	Group09	Group

The contacts are added as destinations.

Searching for recipients in the LDAP server

By this method, you can search for recipients in the registered LDAP server and in the address book.

1 Click [Destination Setting] to open the Recipient List page.

2 Click [Search].

The Search Contact page is displayed.

3 Select the directory service name that you want to search for in the [Directory Service Name] box, and enter the search terms in the boxes that you want to search.

Tips

- If you select the model name of this equipment at the [Directory Service Name] box, you can search for recipients in the address book of this equipment.
- TopAccess will search for recipients who match the entries.
- Leaving the box blank allows wild card searching. (However, you must specify at least one.)

4 Click [Search].

TopAccess will start searching for recipients in the LDAP server and the Search Address List page will display the results.

5 Select the [Email] check boxes of users you want to add.

	Name	company	department	Email Address
☒	User09 User	abcdef	ghijklmn	user09@fax.com

Note

The value of [company] and [department] will depend on the settings determined by the administrator.

6 Click [Add].

The selected recipients are added to the Recipient List page.

Tip

You can remove contacts that you have added to the recipient list before saving the destination settings.

P.252 “Removing the contacts from the recipient list”

7 Click [Save].

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☐		user99@ifax.com
☐		user98@ifax.com
☐		user97@ifax.com
☐		user96@ifax.com
☐		user95@ifax.com

The contacts are added as destinations.

Removing the contacts from the recipient list

1 Select the check boxes of the contacts that you want to remove from the recipient list, and click [Delete].

Recipient List

Save Cancel New Address Book Address Group Search Delete

☒	Name	Destination
☒		user99@ifax.com
☒		user98@ifax.com
☒		user97@ifax.com
☒		user96@ifax.com
☐		user95@ifax.com

The selected contacts are removed from the recipient list.

2 Click [Save].

InternetFax Setting (Fax/Internet Fax Received Forward)

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

Instructions on how to set the Internet Fax settings for the Fax or Internet Fax Received Forward are the same as for setting the Internet Fax settings for private templates.

P.58 “InternetFax Setting (Private template)”

Email Setting (Fax/Internet Fax received forward)

In the Email Setting page, you can specify the content of the Email document to be sent.

The screenshot shows the 'Email Setting' form with the following fields and options:

- 1 Subject:** Includes radio buttons for 'Send data from (Device name) [(Template Name)]' (selected) and an empty text box. A checked checkbox 'Add the date and time to the subject' is also present.
- 2 *From Address:** An empty text input field.
- 3 From Name:** An empty text input field.
- 4 Body:** A large text area for the email body.
- 5 File Format:** A dropdown menu currently set to 'PDF(Multi)'.
- 6 Encryption:** A section containing:
 - ☒ Encryption
 - User Password and Retype Password fields (both masked with dots).
 - Master Password and Retype Password fields (both masked with dots).
 - Encryption Level dropdown set to '128-bit RC4'.
 - Authority section with checkboxes for:
 - ☐ Printing
 - ☐ Change of Documents
 - ☐ Content Copying or Extraction
 - ☐ Content Extraction for accessibility
- 7 File Name:** A text field with the value '(Sender)-NNNN (NNNN is a sequential number)'.
- 8 Fragment Message Size:** A dropdown menu set to 'No Fragmentation'.

1) Subject

This sets the subject of the Email documents. Select [Send data from (Device name) [(Template Name)]] set by default, or enter the desired subject in the box.

When you want to add the date and time to the subject, select the [Add the date and time to the subject] check box.

2) From Address

Enter the Email address of the sender. When the recipient replies, the message will be sent to this Email address.

3) From Name

Enter the sender name of the Email document.

4) Body

Enter the body message of the Email document. You can enter up to 1000 characters (including spaces).

5) File Format

Select the file format to which the received document will be converted.

- **TIFF (Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF (Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF (Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF (Single)** — Select this to save scanned images separately as Single-page PDF files.
- **XPS (Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS (Single)** — Select this to save scanned images separately as Single-page XPS files.

Tips

- If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, refer to the **MFP Management Guide**.
- Files saved in an XPS format can be used in Windows Vista/Windows 7/Windows Server 2008 SP1, or Windows XP SP2/Windows Server 2003 SP1 or later versions with Net Framework 3.0 installed.

6) Encryption

Set this to encrypt PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.

Encryption

Select this if you want to encrypt PDF files.

User Password

Enter a password for opening encrypted PDF files.

Master Password

Enter a password for changing the Encrypt PDF setting.

Tips

- If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, refer to the ***MFP Management Guide***.
- The user password and the master password are not set at the factory shipment.
- Passwords must be from 1 to 32 one-byte alphanumeric characters.
- The user password must differ from the master password.

Notes

- These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. Ask the administrator for resetting these passwords.
- For the details of the encryption setting, refer to the ***MFP Management Guide***.

Encryption Level

Select the desired encryption level.

- **40-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 3.0, PDF V1.1.
- **128-bit RC4** — Select this to set an encryption level to the one compatible with Acrobat 5.0, PDF V1.4.
- **128-bit AES** — Select this to set an encryption level to the one compatible with Acrobat 7.0, PDF V1.6.

Authority

Select the desired types of authority for Encrypt PDF.

- **Printing** — Select this to authorize users to print documents.
- **Change of Documents** — Select this to authorize users to change documents.
- **Content Copying or Extraction** — Select this to authorize users to copy and extract the contents of documents.
- **Content Extraction for accessibility** — Select this to enable the accessibility feature.

7) File Name

The file name will be "(From Name)-NNN". The file name cannot be changed.

8) Fragment Message Size

Select the size of the message fragmentation.

Save as file Setting (Fax/Internet Fax received forward)

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

The screenshot shows the 'Save as file Setting' dialog box. It has a title bar and two buttons: 'Save' and 'Cancel'. The dialog is divided into several sections. On the left, there is a vertical list of sections: 'File Format', 'Encryption', 'Destination', and 'File Name'. On the right, there are corresponding settings. The 'File Format' section has a dropdown menu set to 'PDF(Multi)'. The 'Encryption' section has a checked 'Encryption' checkbox, password fields for 'User Password' and 'Master Password' (each with a 'Retype Password' field), an 'Encryption Level' dropdown set to '128-bit RC4', and a list of permissions: 'Printing', 'Change of Documents', 'Content Copying or Extraction', and 'Content Extraction for accessibility'. The 'Destination' section has a 'Select following 2 items' checkbox, 'Use local folder' checked, and a 'Storage Path' field showing ':\MFP-04587704\FILE_SHARE\'. Below this are options for 'Remote 1' and 'Remote 2', each with 'Use Administrator Setting' and 'Use User Setting' radio buttons, and fields for 'Protocol', 'Network Path', 'Server Name', 'Port Number(Command)', 'Login User Name', 'Password', and 'Retype Password'. The 'File Name' section has a text field showing '(Sender)-NNNN (NNNN is a sequential number)'. Numbered annotations 1 through 6 point to specific parts of the dialog: 1 points to the 'File Format' dropdown, 2 points to the 'Encryption' section, 3 points to the 'Use local folder' checkbox, 4 points to the 'Storage Path' field, 5 points to the 'Remote 1' section, and 6 points to the 'File Name' field.

1) File Format

Select the file format to which the received document will be converted.

- **TIFF (Multi)** — Select this to save scanned images as a Multi-page TIFF file.
- **TIFF (Single)** — Select this to save scanned images separately as Single-page TIFF files.
- **PDF (Multi)** — Select this to save scanned images as a Multi-page PDF file.
- **PDF (Single)** — Select this to save scanned images separately as Single-page PDF files.
- **XPS (Multi)** — Select this to save scanned images as a Multi-page XPS file.
- **XPS (Single)** — Select this to save scanned images separately as Single-page XPS files.

Tips

- If the Forced Encryption setting is enabled, only the PDF (Multi) and the PDF (Single) are selectable for a file format. For the Forced Encryption function, refer to the **MFP Management Guide**.
- Files saved in an XPS format can be used in Windows Vista/Windows 7/Windows Server 2008 SP1, or Windows XP SP2/Windows Server 2003 SP1 or later versions with Net Framework 3.0 installed.

2) Encryption

Set this to encrypt PDF files if you have selected [PDF (Multi)] or [PDF (Single)] in the File Format setting.

Encryption

Select this if you want to encrypt PDF files.

User Password

Enter a password for opening encrypted PDF files.

Master Password

Enter a password for changing the Encrypt PDF setting.

Tips

- If the Forced Encryption setting is enabled, you cannot clear the [Encryption] check box. For the Forced Encryption function, refer to the *MFP Management Guide*.
- The user password and the master password are not set at the factory shipment.
- Passwords must be from 1 to 32 one-byte alphanumeric characters.
- The user password must differ from the master password.

Notes

- These passwords can be re-entered only by an authorized user. Users cannot change the settings of the [Encryption Level] box and the [Authority] box noted below if they are not authorized to change the master password. Ask the administrator to reset these passwords.
- For the details of the encryption setting, refer to the *MFP Management Guide*.

Encryption Level

Select the desired encryption level.

- **40-bit RC4** — Select this to set an encryption level to one compatible with Acrobat 3.0, PDF V1.1.
- **128-bit RC4** — Select this to set an encryption level to one compatible with Acrobat 5.0, PDF V1.4.
- **128-bit AES** — Select this to set an encryption level to one compatible with Acrobat 7.0, PDF V1.6.

Authority

Select the desired types of authority for Encrypt PDF.

- **Printing** — Press this to authorize users to print documents.
- **Change of Documents** — Press this to authorize users to change documents.
- **Content Copying or Extraction** — Press this to authorize users to copy and extract the contents of documents.
- **Content Extraction for accessibility** — Press this to enable the accessibility feature.

3) Destination — Use local folder

Select this to save a received document to the "FILE_SHARE" folder.

4) Destination — Remote 1

Select this check box to save a scanned file to Remote 1. How you can set this item depends on how your administrator configured the Save as file settings.

If Remote 1 does not allow you to specify a network folder, you can only select [Use Administrator Settings]. The protocol and the network path are displayed below this item.

If Remote 1 allows you to specify a network folder, you can select [Use User Settings] and specify the network folder settings by entering the following items:

Protocol

Select the protocol to be used for uploading a scanned file to the network folder.

- **SMB** — Select this to send a scanned file to the network folder using the SMB protocol.
- **FTP** — Select this to send a scanned file to the FTP server.
- **NetWare IPX/SPX** — Select this to send a scanned file to the NetWare file server using the IPX/SPX protocol.
- **NetWare TCP/IP** — Select this to send a scanned file to the NetWare file server using the TCP/IP protocol.

Server Name

When you select [FTP] as the protocol, enter the FTP server name or IP address to which a scanned file will be sent. For example, to send a scanned file to the "ftp://192.168.1.1/user/scanned" FTP folder in the FTP server, enter "192.168.1.1" in this box. You can specify the directory at the [Network Path] box.

When you select [NetWare IPX/SPX] as the protocol, enter the NetWare file server name or Tree/Context name (when NDS is available).

When you select [NetWare TCP/IP] as the protocol, enter the IP address of the NetWare file server.

Port Number (Command)

Enter the port number to be used for controls if you select [FTP] as the protocol. Generally "-" is entered for the control port. When "-" is entered, the default port number, that is set for FTP Client by an administrator, will be used. If you do not know the default port number for FTP Client, ask your administrator and change this option if you want to use another port number.

Network Path

Enter the network path to store a scanned file.

When you select [SMB] as the protocol, enter the network path to the network folder. For example, to specify the "users\scanned" folder in the computer named "Client01", enter "\\Client01\users\scanned".

When you select [FTP] as the protocol, enter the directory in the specified FTP server. For example, to specify the "ftp:/192.168.1.1/user/scanned" FTP folder in the FTP server, enter "user/scanned".

When you select [NetWare IPX/SPX] or [NetWare TCP/IP] as the protocol, enter the folder path in the NetWare file server. For example, to specify the "sys\scan" folder in the NetWare file server, enter "\sys\scan".

Login User Name

Enter the login user name to access an SMB server, an FTP server, or a NetWare file server, if required. When you select [FTP] as the protocol, an anonymous login is assumed if you leave this box blank.

Password

Enter the password to access an SMB server, an FTP server, or a NetWare file server, if required.

Retype Password

Enter the same password again for a confirmation.

5) Destination — Remote 2

Select this check box to save a received document to Remote 2. How you can set this item depends on how the 2nd Folder has been set up in the [Save as file] submenu in the [Setup] menu.

If Remote 2 does not allow you to specify a network folder, you can only select [Use Administrator Settings]. The protocol and the network path are displayed below this item.

If Remote 2 allows you to specify a network folder, you can select [Use User Settings] and specify the network folder settings. See the description of the Remote 1 option for each item.

6) File Name

Display how the a received document will be named. You cannot change the file name.

Tip

The display of the file name when setting Fax Received Forward or Internet Fax Received Forward differs depending on the setting conditions as follows:

- The name registered in the address book is displayed when the number registered in the address book and the recipient's number are the same.
- The recipient's number is displayed when the name is not registered in the address book and the recipient has registered its fax number.
- DOC and the date are displayed when the name is not registered and the recipient has not registered its fax number.

Note

Up to 999 files that are sent from the same sender can be stored in the same destination. If 999 files that are sent from the same sender have already been stored in the specified destination, this equipment will print the received document from the same sender instead of storing them as files.

Box Setting (Fax/Internet Fax received forward)

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

The screenshot shows the 'Box Setting' form. At the top left, there are 'Save' and 'Cancel' buttons. The form contains several fields: 'Box Number' (a dropdown menu showing '000 : Public Box'), 'Password' (a text box), and 'Retype Password' (a text box). Below these are 'Destination', 'Folder Name', and 'Document Name' fields. Three numbered annotations are present on the left side of the form: '1' points to the 'Destination' field, '2' points to the 'Folder Name' field, and '3' points to the 'Document Name' field. The 'Document Name' field has a placeholder text '(Sender)-NNNN (NNNN is a sequential number)'.

1) Destination

Specify the destination box number for e-Filing.

Box Number

Enter the Box number where a received document will be stored.

Password

Enter the password if the specified Box number requires a password.

Retype Password

Enter the password again if the specified Box number requires a password.

2) Folder Name

Enter the name of the folder where a received document will be stored.

3) Document Name

Display how the a received document will be named. You cannot change the document name.

Displaying Message Log

In the [Message Log] menu, you can display the system message logs such as job information, warnings, and errors. You can use this page to find out what happened and troubleshoot the problem.

Displaying the message logs

1 Access TopAccess in the administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

2 Click the [Message Log] menu.

The screenshot shows the TopAccess Administrator interface. The 'Message Log' menu item is highlighted in the top navigation bar. Below the navigation bar, the 'Message Log' page is displayed, showing a table of log entries.

Date Time	Error Level	Error Message	Error Code
10/16/2008 04:04:08	Information	The file has been imported	5C20
10/16/2008 03:51:12	Information	The file has been imported	5C20
10/16/2008 03:47:13	Information	The file has been imported	5C20
10/16/2008 03:31:42	Information	Scanned documents in shared folder deleted upon user's request.	2DA3
10/16/2008 03:22:07	Information	The file has been imported	5C20
10/16/2008 03:21:32	Information	The file has been imported	5C20
10/16/2008 03:17:34	Information	The file has been imported	5C20
10/15/2008 22:37:06	Information	POP3 Connection Error has occurred in the received mail.	3E10
10/15/2008 22:37:03	Information	POP3 Connection Error has occurred in the received mail.	3E10
10/15/2008 22:24:16	Information	The file has been imported	5C20
02/16/2008 03:22:08	Information	The file has been imported	5C20

Go to top of this page

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Message Log menu page is displayed.

Managing Department Code

In the [Department] menu at the [Counter] tab, an administrator can:

- Display the department list that contains the counter information for each department
- Display the department counter of a specific department
- Clear all department counters
- Clear the department counter of a specific department
- Register new department code settings
- Modify the department code settings
- Delete all department codes
- Delete a department code

To do this, you must know the administrator password.

Notes

- An [Undefined] department group is registered as the default. This department group is used to count Invalid jobs. You can view the counter for this department group, but cannot modify or delete this default department group.
- The department management function does not support Web Services Scan. Web Services Scan jobs performed while the department management is enabled are always counted as [Undefined] Department Names.

Tip

You can also manage the department code in the Department Management submenu page that can be displayed by clicking the [User Management] tab and [Department Management] submenu in the User Confirm/Create/Modify menu page.

■ Displaying the department list and counters

An administrator can display the department list registered in this equipment and the counter information for each department code.

Displaying the departments list

- 1 Click the [Counter] tab and the [Department] menu.**
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].**

The Department Management page is displayed.

- 3 The department list containing counter information is displayed.**

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

Displaying the department counters

- 1 Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code Enter

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Management page is displayed.

- 3 Click the department name link to display more details.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

Enter a department code to access department counters

Department Code Enter

New Reset All Counters Delete All

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

- 4 The Department Information page opens.

Department Information

Save Cancel Reset Counters Delete

Department Number 1

Department Name Dept01

Department Code 10001

Set Limitation of Full Color OFF

Maximum reached for Full Color output

Set Limitation of Black OFF

Maximum reached for Black output

Total Counter

	Full Color	Twin Color	Black	Total
Copy	0	0	0	0
Fax	-	-	0	0
Printer	0	0	0	0
List	-	-	0	0
Total	0	0	0	0

■ Clearing the department counters

An administrator can clear the counters for all departments at one time, or individually.

Clearing all department counters

- 1 Click the **[Counter]** tab and the **[Department]** menu.
The Department management page is displayed.
- 2 Enter the administrator password in the **[Department Code]** box and click **[Enter]**.

TopAccess e-Filing

Device Job Status Logs Registration **Counter** User Management Administration

Total Count | **Department**

Department management

Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code: [*****] Enter

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Management page is displayed.

- 3 Click **[Reset All Counters]**.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Total Count | **Department**

Department management

Enter a department code to access department counters

Department Code: [] Enter

New Reset All Counters Delete All

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The confirmation dialog box appears.

- 4 Click **[OK]**.

Windows Internet Explorer

Clear OK?

OK Cancel

The department counters for all departments are cleared.

Clearing the department counter for a department

- 1 Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].

TopAccess e-Filing

Device Job Status Logs Registration **Counter** User Management Administration

Total Count | **Department**

Department management

Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Management page is displayed.

- 3 Click the department name link whose counter you want to clear.

TopAccess e-Filing

Device Job Status Logs Registration **Counter** User Management Administration

Total Count | **Department**

Department management

Enter a department code to access department counters
Department Code

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Information page opens.

- 4 Click [Reset Counters].

Department Information

Department Number 1

Department Name Dept01

Department Code 10001

Set Limitation of Full Color OFF

Maximum reached for Full Color output

Set Limitation of Black OFF

Maximum reached for Black output

Total Counter	Full Color	Twin Color	Black	Total
Copy	0	0	0	0
Fax	-	-	0	0
Printer	0	0	0	0
List	-	-	0	0
Total	0	0	0	0

The confirmation dialog box appears.

- 5 Click [OK].

Windows Internet Explorer

Clear OK?

The department counters for the selected department are cleared.

■ Registering or modifying the department code

An administrator can register new department code or modify the department code settings.

Registering or modifying the department code setting

- 1 Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].

The Department Management page is displayed.

- 3 Click [New] to set up a new department code, or click the department name link that you want to edit in the departments list.

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

The Department Information page is displayed.

4 Enter the following items to specify the department information.

For the e-STUDIO4520C Series and the e-STUDIO6530C Series

Department Information

Save Cancel

Department Name

Department Code

Set Limitation of Full Color

Maximum reached for Full Color output

Set Limitation of Black

Maximum reached for Black output

For the e-STUDIO855 Series and the e-STUDIO455 Series

Department Information

Save Cancel

Department Name

Department Code

Set Limitation

Maximum reached

Department Name — Enter the department name to identify the department code. You can enter up to 20 characters.

Department Code — Enter a 5-digit department code.

Maximum reached of Full Color output — Select whether to enable the limitation for color outputs for this department code. When you select [ON], enter the maximum number of color outputs for this department code in the [Maximum reached for Full Color output] box.

Maximum reached for Full Color output — Enter the maximum number of color outputs for this department code when the [Set Limitation of Full Color] option is enabled.

Set Limitation of Black — Select whether to enable the limitation of black outputs for this department code. When you select [ON], enter the maximum number of black outputs for this department code in the [Maximum reached for Black output] box.

Maximum reached for Black output — Enter the maximum number of black outputs for this department code when the [Set Limitation of Black] option is enabled.

Tips

- [Set Limitation of Full Color] and [Maximum reached for Full Color output] are displayed only on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series. When the total count of color outputs in copying or printing reaches the maximum number, printing cannot be performed.
- On the TopAccess menu of the e-STUDIO855 Series and the e-STUDIO455 Series, [Set Limitation of Black] is displayed as [Set Limitation] and [Maximum reached for Black output] is displayed as [Maximum reached]. When the total count of black outputs in copying, printing, those in printing received faxes*1 or system page reaches the maximum number, printing cannot be performed.

*1 The number of outputs are only counted for received faxes, in which the department code needs to be entered, such as manual reception, polling reception or the printing of originals stored in the confidential mailbox and the bulletin mailbox.

Notes

- [Set Limitation of Black] and [Maximum reached for Black output] options cannot be set when the No Limit Black function is enabled.
- When the number of outputs exceeds the limitation while a job is being printed, a few copies exceeding the limitation are printed and counted because the equipment cannot stop the job immediately.

5 Click [Save].

The department code is added or edited.

■ Deleting the department code

An administrator can delete all department code settings at one time, or individually.

Deleting all department code settings

- 1 Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].

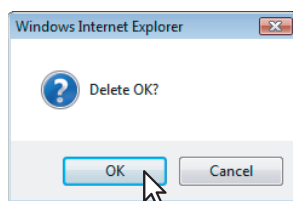
The Department Management page is displayed.

- 3 Click [Delete All].

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

The confirmation dialog box appears.

- 4 Click [OK].



All department code settings are deleted.

Deleting a department code setting

- 1 Click the [Counter] tab and the [Department] menu.
The Department management page is displayed.
- 2 Enter the administrator password in the [Department Code] box and click [Enter].

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

Enter a department code to access department counters
To confirm, create or modify the department information, enter the Administrator's password.

Department Code

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Management page is displayed.

- 3 Click the department name link that you want to delete.

TopAccess e-Filing

Device Job Status Logs Registration Counter User Management Administration

Total Count | Department

Department management

Enter a department code to access department counters

Department Code

Number	Department Name	Dept Code	Total Printing	Total Scanning	Fax Transmission	Fax Reception
1	Dept01	10001	0	0	0	0
2	Dept02	10002	0	0	0	0
3	Dept03	10003	0	0	0	0
4	Dept04	10004	0	0	0	0
5	Dept05	10005	0	0	0	0
6	Dept06	10006	0	0	0	0
7	Dept07	10007	0	0	0	0
8	Dept08	10008	0	0	0	0

Install Software | Top | Help | ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

The Department Information page opens.

- 4 Click [Delete].

Department Information

Department Number 1

Department Name Dept01

Department Code 10001

Set Limitation of Full Color OFF

Maximum reached for Full Color output

Set Limitation of Black OFF

Maximum reached for Black output

Total Counter	Full Color	Twin Color	Black	Total
Copy	0	0	0	0
Fax	-	-	0	0
Printer	0	0	0	0
List	-	-	0	0
Total	0	0	0	0

The confirmation dialog box appears.

- 5 Click [OK].

Windows Internet Explorer

Delete OK?

The selected department code is deleted.

Setting up User Management

In the [User Management] tab page, you can enable or disable the department management, configure the User Management Setting, and configure the User Authentication for Scan to E-mail.

📖 P.268 “Enabling department management”

📖 P.271 “Setting up User Management setting”

📖 P.301 “Setting role information”

📖 P.307 “Setting up User Authentication for Scan to Email”

■ Enabling department management

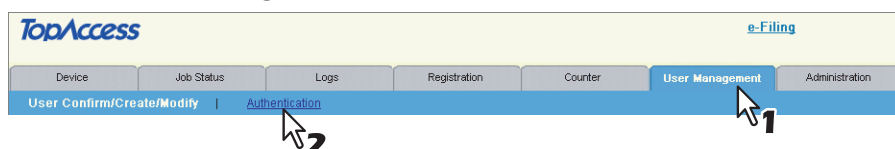
The department management is disabled as the default setting. When you want to manage the counters for every department, enable the department management. If the department management is enabled, the department code input screen will be displayed in the touch panel when you perform copying, scanning, faxing, internet faxing and e-Filing box operations to manage the operations separately every department. Printing can be also managed using the department codes.

Notes

- To enable the department management, at least one department code must be registered. Before enabling the department management, register the department code that you require.
📖 P.264 “Registering or modifying the department code”
- Department management will not be enabled automatically even if the User Authentication is enabled. When you configure the User Authentication, you will not need to register more than one department code. However, if you want to enable [Create User Information Automatically], you must enable the department management with more than one department code registered.
- Enabling or disabling the department management can be operated in the [General] submenu in the [Setup] menu.
📖 P.110 “Setting up Device Information”
- Enabling or disabling the department management can be operated using the control panel. For instructions using the control panel, refer to the **MFP Management Guide**.
- The department management function does not support Web Services Scan.
Web Services Scan jobs performed while the department management is enabled are always counted as [Undefined] Department Names.

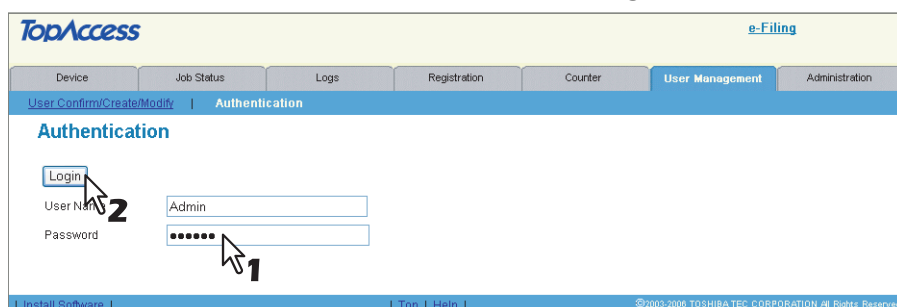
Enabling the department management

1 Click the [User Management] tab and the [Authentication] menu.



The login page is displayed.

2 Enter the administrator password and click [Login].



The Authentication page is displayed.

3 Click [Department Setting].

TopAccess

Device Job Status Logs Registration Counter **User Management** Administration Meta Scan

User Confirm/Create/Modify Authentication

Authentication

Department Setting

Current Setting	
Department Code	Enable
Department Code Enforcement	ON
Department Management (Copy)	Enable
Department Management (FAX)	Enable
Department Management (Print)	Enable
Department Management (Scan)	Enable
Department Management (List)	Enable

User Management Setting

Current Setting	
User Authentication	Disable
User Authentication Enforcement	Disable

User Authentication for Scan to Email

Current Setting	
Method	Disable

The Department Setting page opens.

4 Specify the following items and click [Finish].

Department Setting

Cancel Finish

Department Code Enable

Department Code Enforcement ON

Department Management (Copy) Enable

Department Management (FAX) Enable

Department Management (Print) Enable

Department Management (Scan) Enable

Department Management (List) Enable

*Department Code Enforcement Select whether invalid jobs, which a department code is not specified or invalid department code is specified, are printed or stored in the invalid job list when the department code is enabled.
 ON: Select this to not print the invalid jobs and store them in the invalid job list.
 Print: Select this to print the invalid jobs.
 Delete: Select this to delete the invalid jobs
 *If the Department Code Enforcement is set to ON and the SNMP communication is enabled in the printer driver, the user will be prompted to enter the correct department code if an invalid department code was entered in the printer driver.

- **Department Code**
Select whether the department management is enabled or disabled.
- **Department Code Enforcement**
Select whether invalid jobs, for which a department code is not specified or an invalid department code is specified, are printed or stored in the invalid job list when the department code is enabled.
ON — Select this to not print the invalid jobs and store them in the invalid job list.
Print — Select this to print the invalid jobs.
Delete — Select this to delete the invalid jobs without storing them in the invalid job list.

Notes

- If the Department Code Enforcement is set to ON and the SNMP communication is enabled in the printer driver, the user will be prompted to enter the correct department code if an invalid department code was entered in the printer driver.
- The Department Code Enforcement setting is not applied when the User Management Setting is enabled.
- **Department Management (Copy)**
When this function is enabled, the following counters are managed in each department.
 - Number of copied sheets of paper
 - Number of originals scanned when copying is performed.
- **Department Management (FAX)**
When this function is enabled, the following counters are managed in each department.
 - Number of sent faxes
 - Number of originals scanned when faxes are sent
 - Number of received faxes
 - Number of outputs in printing received faxes*¹

*¹ The number of outputs are only counted for received faxes, in which the department code needs to be entered, such as manual reception, polling reception or the printing of originals stored in the confidential mailbox and the bulletin mailbox.

-
- **Department Management (Print)**
When this function is enabled, the number of outputs in printing (for printing, received Email and InternetFax) is managed in each department.
 - **Department Management (Scan)**
When this function is enabled, the number of originals scanned such as when they are stored in the shared folder is managed in each department.
 - **Department Management (List)**
When this function is enabled, the number of system page outputs is managed in each department.

■ Setting up User Management setting

When the User Management setting is enabled, users must enter the user name and password before operating this equipment. Therefore, you can secure the equipment from the unexpected users.

When the User Management Setting is enabled, the following functions will be available.

- The counters for each user can be managed.
- The limitations for each user can be set.
- Up to 10000 users can be registered.
- The user name and password will be required to operate the [COPY], [SCAN], [e-FILING], [FAX], [TEMPLATE], [USER FUNCTIONS], and [JOB STATUS] buttons.
- The user name and password will be required to operate the e-Filing web utility.
- The print jobs can be accepted only from the computer of which the login user name can be attested. (When the Windows Domain Authentication or LDAP Authentication is used, the computer must also join the domain.)
- When the Windows Domain or LDAP Authentication is used, the user information will be registered automatically in the equipment when a user enters the user name and password in the User Authentication screen and then enters the department code.

The following table shows which function will use the User Management Setting.

Operation		Authentication	Remarks
Control Panel	COPY	Yes	
	SCAN	Yes	
	e-FILING	Yes	
	FAX/Internet Fax	Yes	
	EXTENSION	No	
	JOB STATUS	Yes	
	ACCESS	No	
	INTERRUPT	Yes	
	TEMPLATE	Yes	
	USER FUNCTIONS	Yes	
Web	TopAccess	No	
	e-Filing	Yes	
Client Software	Printer Driver N/W-Fax Driver	Yes (User Name Only)	The computer must login the domain.
	TopAccessDocMon	No	
	File Downloader	No	
	TWAIN Driver	No	
	Backup/Restore	No	
	Address Book Viewer	No	
	Remote Scan	No	
	Web Services Scan	No	

Note

Remember the following limitations and considerations for the User Management Setting.

- The jobs cannot be printed or deleted from TopAccess. When you want to print or delete the jobs, perform the operation from the [JOB STATUS] on the touch panel.
- When the Windows Domain or LDAP Authentication is enabled, the password setting in the User Information will not be used for the authentication. Do not specify a password for User Information when Windows Domain or LDAP Authentication is used.
- When the user's jobs are in progress or the user is currently logged in to the touch panel, user information cannot be deleted and you cannot reset the user's counters.
- To manage counter data for each user, the department management function must be enabled in advance.
 P.268 "Enabling department management"

Before registering the user information, enable the User Management Setting.

 P.272 "Enabling User Management setting"

After you enable the User Management Setting, register the user information.

 P.286 "Managing user information"

□ Enabling User Management setting

This equipment supports the following methods for the User Management Setting.

- **Windows Domain Authentication**

When your network manages the network users using the Windows Domain, this equipment can be managed using the Windows Domain Authentication.

When this is configured, users must enter the user name and password that is registered in the Windows Domain to perform any operations on the control panel of this equipment.

📖 P.272 “Enabling Windows Domain Authentication”

- **LDAP Authentication**

When your network manages the network users using the LDAP, this equipment can be managed using the LDAP Authentication.

When this is configured, users must enter the user name and password that is registered in the LDAP server to perform any operations on the control panel of this equipment.

📖 P.278 “Enabling LDAP Authentication”

- **MFP Local Authentication**

When you do not have any network authentication systems in your network, you can use the MFP Local Authentication.

When this is configured, users must enter the user name and password that is registered in the MFP to perform any operations on the control panel of this equipment.

📖 P.283 “Enabling MFP Local Authentication”

Note

If you want to change the authentication method, change the domain name and password settings of the User Information as required. It is easy to change the settings of the User Information using the Export/Import function.

📖 P.294 “Exporting user information and counters”

📖 P.296 “Importing user information”

Enabling Windows Domain Authentication

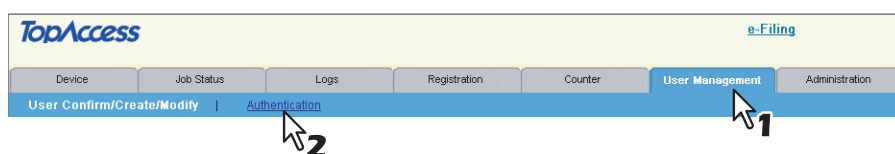
To use the Windows Domain Authentication, you must have Windows Domain Authentication system in your network.

Note

When the Windows Domain Authentication is enabled, the SNMP Communication must be enabled for printing.

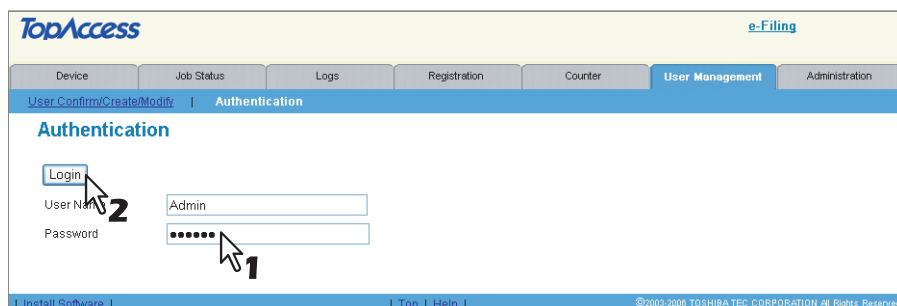
Enabling Windows Domain Authentication

1 Click the [User Management] tab and the [Authentication] menu.



The login page is displayed.

2 Enter the administrator password and click [Login].



The Authentication page is displayed.

3 Click [User Management Setting].

The screenshot shows the TopAccess Administrator interface. The 'Authentication' tab is active. Under 'User Management Setting', the 'User Authentication' is set to 'Disable' and 'User Authentication Enforcement' is set to 'Disable'. A mouse cursor is pointing at the 'User Management Setting' tab.

The User Management Setting page opens.

4 Select [Windows Domain Authentication].

The screenshot shows the 'User Management Setting' dialog box. The 'User Authentication' dropdown menu is open, and 'Windows Domain Authentication' is selected. The 'User Authentication Enforcement' dropdown is also open, showing 'Disable' and 'Windows Domain Authentication'. The 'Create User Information Automatically' checkbox is unchecked, and the 'Enable Guest User' checkbox is checked.

Note

You can disable the User Management Setting by selecting [Disable] and clicking [Next].

5 Select how to process a print job whose user authentication has failed in the [User Authentication Enforcement] box, and then click [Next].

The screenshot shows the 'User Management Setting' dialog box. The 'User Authentication Enforcement' dropdown menu is open, and 'Delete' is selected. The 'Create User Information Automatically' checkbox is unchecked, and the 'Enable Guest User' checkbox is checked.

In the [User Authentication Enforcement] box, select whether invalid jobs, for which authentication has failed, are printed or stored in the invalid job list.

- **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
- **Print** — Select this to print the invalid jobs.
- **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tips

- If you want to automatically register user information entered in the authentication screen on the touch panel, TopAccess, or e-Filing Web Utility into this equipment, enable the department management and then select the [Create User Information Automatically] check box.
- If you want to enable the guest user operations, select the [Enable Guest User] check box.

6 Enter domain names for the network in the [Domain Name 1], [Domain Name 2] and [Domain Name 3] boxes, and then click [Detail Setting].

Note

You can specify up to 3 domain names. You must specify at least one domain name to enable the Windows Domain Authentication.

7 Select the [Use NT Domain Server] check box, and enter the following items. Then click [Next].

Domain Name — The domain name entered in Step 6 is displayed.

PDC — Enter the server name or IP address of the Primary Domain Controller.

BDC — Enter the server name or IP address of the Backup Domain Controller as required.

Connection Timeout — Enter timeout period for quitting communication when no response is received from PDC or BDC server in 1 to 180 seconds.

Note

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. In that case, correct the primary or backup domain controller setting after the beep sounds and the alert message will be displayed on the touch panel.

8 Specify the following items and click [Next].

User Management Setting

Cancel Next

Role Based Access 2

Role Based Access: Disable

LDAP Server: ldap1 1

Role Based Access — Select whether the Role Based Access Control is enabled or not.

LDAP Server — Select the LDAP server that manages the Role Based Access Control.

Tips

- To enable Role Based Access, you must first export a role based data setting file embedded in this equipment or other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series. Then edit this file into the form required for LDAP server setting, and then import it to the equipment. For instructions on how to edit the role based data setting file, see P.303 “Exporting Role Information” and P.305 “Importing role information”.
- The LDAP server to be used for the authentication must be configured in the [Directory Service] submenu in the [Maintenance] menu. When you configure the Active Directory in Windows server, specify the domain administrator or account operator for the user name.
P.216 “Managing directory service”
- If you selected the [Enable Guest User] check box in Step 5, the Guest ACL Settings page is displayed. Go to the next step. If you did not select it, go to Step 10.

9 Select the items you want to allow for guest user operations and click [Next].

User Management Setting

Cancel Next

Guest ACL Settings 2

☐ Enable Copy

☐ Enable Email

☐ Enable File Share

☐ Enable Internet Fax

☐ Enable Print

☐ Enable e-Filing Box

☐ Enable Fax

☐ Enable Remote Scan

☐ Permit Guest User's authority for all registered users. 1

Enable Copy — Select this to enable copying.

Enable Email — Select this to enable Emailing.

Enable File Share — Select this to enable the file saving operation

Enable Internet Fax — Select this to enable the Internet Fax function.

Enable Print — Select this to enable printing when the color mode is [Black].

Enable e-Filing Box — Select this to enable the e-Filing function.

Enable Fax — Select this to enable the Fax function.

Enable Color Output — Select this to enable color printing when the color mode is [Full Color] or [Auto Color].

* This feature is available only for the e-STUDIO4520C Series and the e-STUDIO6530C Series.

Enable Remote Scan — Select this to enable the remote scan function.

Permit Guest User's authority for all registered users. — Select this to grant guest privileges set in the User Management setting to all users.

10 Specify how the From Address is set for Scan to Email.

User Authentication for Scan to Email

Cancel Finish

Setting method of From Address field.

☒ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☐ Setting Address is searching from 'User Name' of LDAP.

[...More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

☐ From Address is acquired from Email setting.

**From Address registered by what Email Setting is used.*

☒ From Address cannot be edited in Scan to Email.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, where “User Name” is the user name that is entered on the touch panel for authentication, and “Mail Domain Name” is the domain name that is entered in the [Mail Domain Name] box. When this is selected, enter the domain name in the [Mail Domain Name] box.

Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address found in the LDAP server. Specify the LDAP server name found in the [LDAP Server] box, the schema of an email address to set as the email address in the [Attribute type of 'E-mail Address'] box, the schema to search for the user name in the [Attribute type of 'User Name'] box or the domain name that is used when the user name is not found in the [Mail Domain Name] box.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'E-mail Address']: Select this to specify the schema to set as the email address when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema specified in [Attribute type of 'User Name'] in the specified LDAP server. If the user name is not found in the specified schema, the email address is set as “User Name@Mail Domain Name”. The user name entered on the touch panel for authentication is used for “User Name”.

[Mail Domain Name]: Select this to use the domain name entered in the [Mail Domain Name] box if the schema specified in [Attribute type of 'User Name'] is not found.

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Name field].

From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.

From Address cannot be edited in Scan to Email — Select this check box if you do not want to allow users to edit the From Address.

11 Specify how the From Name is set for Scan to Email.

Setting method of From Name field

☐ Setting Name is 'Account Name of From Address + From Name of Email Setting'

[More Information](#)

☐ Setting Name is searching from 'User Name' of LDAP.

LDAP Server

Attribute type of 'From Name'

Attribute type of 'User Name'

☒ From Name is acquired from Email setting.

*From Name registered by what Email Setting is used.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Name is 'Account Name of From Address + From Name of Email Setting' — Select this check box to set the name of an email sender in a format 'Account Name + (space) + From Name of Email Setting'. The character string before "@" in the sender's address (From Address) comes at 'Account Name'. The name displayed in [From Name] of the [Email] submenu of the [Setup] menu on the [Administration] tab page comes at 'From Name of Email Setting'.

Setting Name is searching from 'User Name' of LDAP.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'From Name']: Select this to specify the schema to set as the sender name when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema in [Attribute type of 'User Name'] in the specified LDAP server.

If the entered user name is not found in the specified schema, the From Name is set the same as [Setting Name is 'Account Name of From Address + From Name of Email Setting'].

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Address field].

From Name is acquired from Email setting. — Select this to set the sender name specified in the email setting.

12 Click [Finish].

The Windows Domain Authentication is enabled.

Enabling LDAP Authentication

To enable the LDAP Authentication, you must have LDAP directory service in your network.

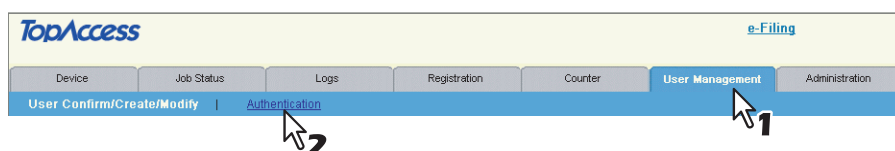
Note

To enable LDAP with SSL, see the following section.

📖 P.126 “Setting up LDAP Session”

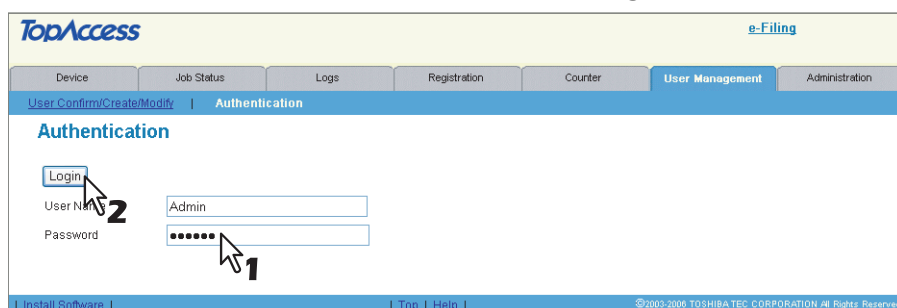
Enabling LDAP Authentication

- 1 Click the [User Management] tab and the [Authentication] menu.



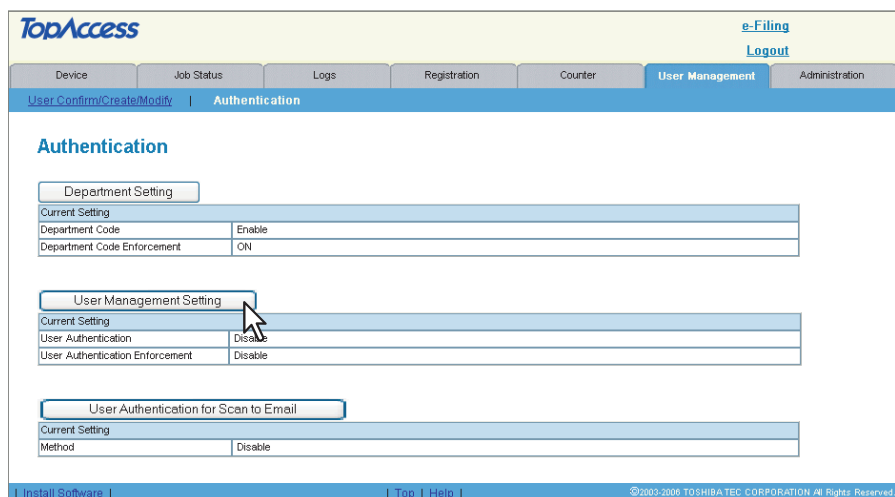
The login page is displayed.

- 2 Enter the administrator password and click [Login].



The Authentication page is displayed.

- 3 Click [User Management Setting].



The User Management Setting page opens.

4 Select [LDAP Authentication].

Note

You can disable the User Management Setting by selecting [Disable] and clicking [Next].

5 Select how to process a print job whose user authentication has failed in the [User Authentication Enforcement] box, and then click [Next].

In the [User Authentication Enforcement] box, select whether invalid jobs, in which authentication has failed, are printed or stored in the invalid job list.

- **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
- **Print** — Select this to print the invalid jobs.
- **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tips

- If you want to automatically register user information entered in the authentication screen on the touch panel, TopAccess, or e-Filing Web Utility into this equipment, enable the department management and then select the [Create User Information Automatically] check box.
- If you want to enable the guest user operations, select the [Enable Guest User] check box.

6 Select the LDAP server to be used for the authentication and select the type of the LDAP server. Then click [Detail Setting].

Windows Server — Select this when LDAP is running on a Windows server.

LDAP Server (Other than Windows Server) — Select this when the LDAP is running on a server other than a Windows server. When this is selected, you have to specify the attribute type of 'User Name'.

Tip

The LDAP server to be used for authentication must be configured in the [Directory Service] submenu in the [Maintenance] menu.

📖 P.216 “Managing directory service”

7 Specify the following items and click [Next].

The screenshot shows the 'User Management Setting' dialog box. At the top, there are 'Cancel' and 'Next' buttons. Below them is a progress bar with '2' indicating the current step. The 'Role Based Access' section is highlighted with a red box. It contains two dropdown menus: 'Role Based Access' set to 'Disable' and 'LDAP Server' set to 'ldap1'. A mouse cursor is pointing at the 'Next' button.

Role Based Access — Select whether the Role Based Access Control is enabled or not.

LDAP Server — Select the LDAP server that manages the Role Based Access Control.

Tips

- To enable Role Based Access, you must first export a role based data setting file embedded in this equipment or other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series. Then edit this file into the form required for LDAP server setting, and then import it to the equipment. For instructions on how to edit the role based data setting file, see P.303 “Exporting Role Information” and P.305 “Importing role information”.
- The LDAP server to be used for the authentication must be configured in the [Directory Service] submenu in the [Maintenance] menu. When you configure the Active Directory in Windows server, specify the domain administrator or account operator for the user name.
P.216 “Managing directory service”
- If you selected the [Enable Guest User] check box in Step 5, the Guest ACL Settings page is displayed. Go to the next step. If you did not select it, go to Step 9.

8 Select the items you want to allow for guest user operations and click [Next].

The screenshot shows the 'User Management Setting' dialog box. At the top, there are 'Cancel' and 'Next' buttons. Below them is a progress bar with '2' indicating the current step. The 'Guest ACL Settings' section is highlighted with a red box. It contains several checkboxes: 'Enable Copy', 'Enable Email', 'Enable File Share', 'Enable Internet Fax', 'Enable Print', 'Enable e-Filing Box', 'Enable Fax', 'Enable Remote Scan', and 'Permit Guest User's authority for all registered users.' A mouse cursor is pointing at the 'Next' button.

Enable Copy — Select this to enable copying.

Enable Email — Select this to enable Emailing.

Enable File Share — Select this to enable the file saving operation

Enable Internet Fax — Select this to enable the Internet Fax function.

Enable Print — Select this to enable printing when the color mode is [Black].

Enable e-Filing Box — Select this to enable the e-Filing function.

Enable Fax — Select this to enable the Fax function.

Enable Color Output — Select this to enable color printing when the color mode is [Full Color] or [Auto Color].

* This feature is available only for the e-STUDIO4520C Series and the e-STUDIO6530C Series.

Enable Remote Scan — Select this to enable the remote scan function.

Permit Guest User's authority for all registered users. — Select this to grant guest privileges set in the User Management setting to all users.

9 Specify how the From Address is set for Scan to Email.

User Authentication for Scan to Email

Cancel Finish

Setting method of From Address field.

☒ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☐ Setting Address is searching from 'User Name' of LDAP.

[...More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

☐ From Address is acquired from Email setting.

**From Address registered by what Email Setting is used.*

☒ From Address cannot be edited in Scan to Email.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, where “User Name” is the user name that is entered on the touch panel for authentication, and “Mail Domain Name” is the domain name that is entered in the [Mail Domain Name] box. When this is selected, enter the domain name in the [Mail Domain Name] box.

Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address found in the LDAP server. Specify the LDAP server name found in the [LDAP Server] box, the schema of an email address to set as the email address in the [Attribute type of 'E-mail Address'] box, the schema to search for the user name in the [Attribute type of 'User Name'] box or the domain name that is used when the user name is not found in the [Mail Domain Name] box.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'E-mail Address']: Select this to specify the schema to set as the email address when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema specified in [Attribute type of 'User Name'] in the specified LDAP server. If the user name is not found in the specified schema, the email address is set as “User Name@Mail Domain Name”. The user name entered on the touch panel for authentication is used for “User Name”.

[Mail Domain Name]: Select this to use the domain name entered in the [Mail Domain Name] box if the schema specified in [Attribute type of 'User Name'] is not found.

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Name field].

From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.

From Address cannot be edited in Scan to Email — Select this check box if you do not want to allow users to edit the From Address.

10 Specify how the From Name is set for Scan to Email.

Setting method of From Name field

☐ Setting Name is 'Account Name of From Address + From Name of Email Setting'

[More Information](#)

☐ Setting Name is searching from 'User Name' of LDAP.

LDAP Server

Attribute type of 'From Name'

Attribute type of 'User Name'

☒ From Name is acquired from Email setting.

*From Name registered by what Email Setting is used.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Name is 'Account Name of From Address + From Name of Email Setting' — Select this check box to set the name of an email sender in a format 'Account Name + (space) + From Name of Email Setting'. The character string before "@" in the sender's address (From Address) comes at 'Account Name'. The name displayed in [From Name] of the [Email] submenu of the [Setup] menu on the [Administration] tab page comes at 'From Name of Email Setting'.

Setting Name is searching from 'User Name' of LDAP.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'From Name']: Select this to specify the schema to set as the sender name when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema in [Attribute type of 'User Name'] in the specified LDAP server.

If the entered user name is not found in the specified schema, the From Name is set the same as [Setting Name is 'Account Name of From Address + From Name of Email Setting'].

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Address field].

From Name is acquired from Email setting. — Select this to set the sender name specified in the email setting.

11 Click [Finish].

The LDAP Authentication is enabled.

Enabling MFP Local Authentication

When no network authentication system is configured in your network, you can enable MFP Local Authentication. MFP Local Authentication uses the account information that is registered in this equipment for authentication. Therefore, you must register the user account information first before enabling MFP Local Authentication. This equipment also manages the counters for each user if MFP Local Authentication is enabled.

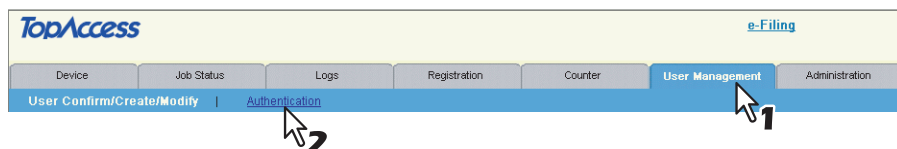
📖 P.286 “Creating or modifying user information”

After you register the user information, enable MFP Local Authentication.

📖 P.283 “Enabling MFP Local Authentication”

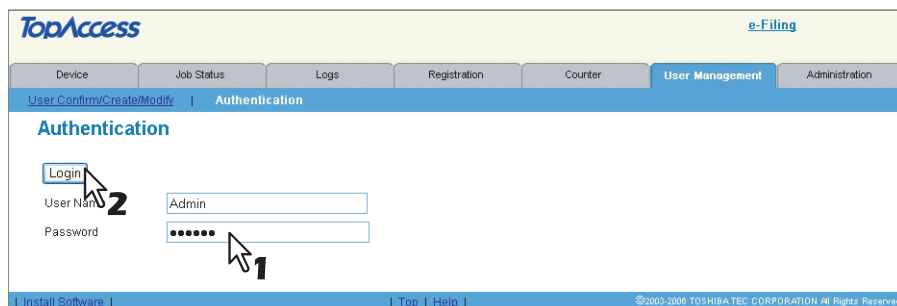
Enabling MFP Local Authentication

- 1 Click the [User Management] tab and the [Authentication] menu.



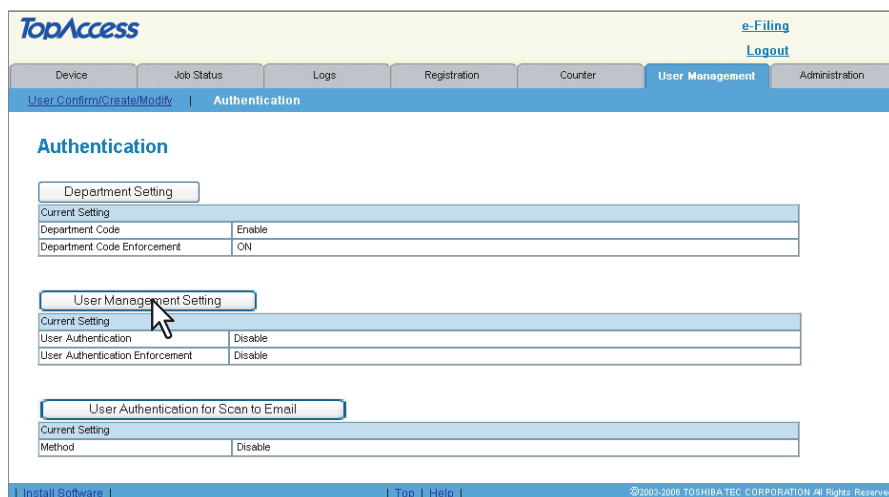
The login page is displayed.

- 2 Enter the administrator password and click [Login].



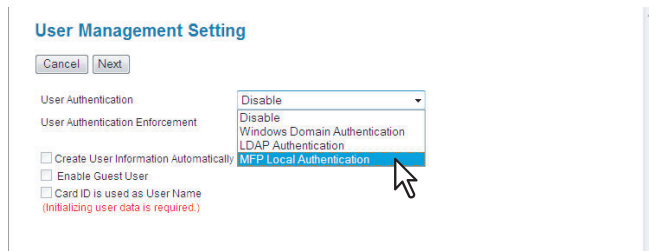
The Authentication page is displayed.

- 3 Click [User Management Setting].



The User Management Setting page opens.

4 Select the [MFP Local Authentication] box, and select how invalid jobs are processed in the [User Authentication Enforcement] box. Then click [Next].

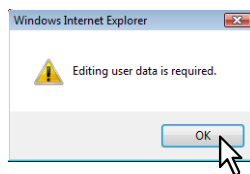


The confirmation dialog box appears.

Tip

If you want to enable guest user operations, select the [Enable Guest User] check box. Go to the next step.

5 Click [OK].



6 Select the [MFP Local Authentication] box, and select how invalid jobs are processed in the [User Authentication Enforcement] box. Then click [Next].



In the [User Authentication Enforcement] box, select whether invalid jobs, for which authentication has failed, are printed or stored in the invalid job list.

- **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
- **Print** — Select this to print the invalid jobs.
- **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tips

- You can disable the User Management Setting by selecting [Disable] and click [Next].
- If you use your Card ID as a user name, select the [Use Card ID for User Name] check box. This check box is displayed only when the card was authenticated.

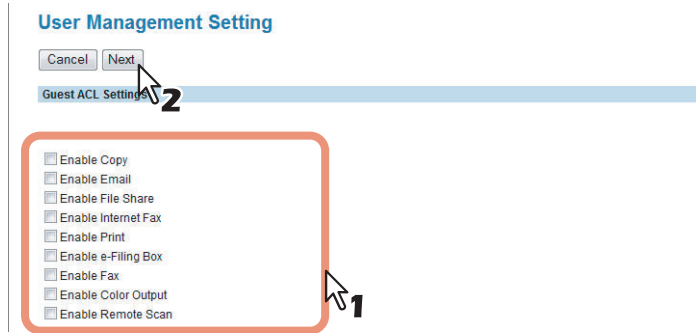
Note

If you changed the setting, you must register the new user information. To register new user information, delete all the user information on the [User Management] tab page and then register the new user information.

📖 P.290 “Deleting all user information”

📖 P.296 “Importing user information”

7 Select the items you want to allow for guest user operations and click [Next].



Enable Copy — Select this to enable copying.

Enable Email — Select this to enable Emailing.

Enable File Share — Select this to enable the file saving operation

Enable Internet Fax — Select this to enable the Internet Fax function.

Enable Print — Select this to enable printing when the color mode is [Black].

Enable e-Filing Box — Select this to enable the e-Filing function.

Enable Fax — Select this to enable the Fax function.

Enable Color Output — Select this to enable color printing when the color mode is [Full Color] or [Auto Color].

* This feature is available only for the e-STUDIO4520C Series and the e-STUDIO6530C Series.

Enable Remote Scan — Select this to enable the remote scan function.

❏ Managing user information

After enabling the User Management Setting, you must register the user information in the User Confirm/Create/Modify page.

In this page, you can do:

- 📖 P.286 “Creating or modifying user information”
- 📖 P.289 “Deleting user information”
- 📖 P.290 “Deleting all user information”
- 📖 P.291 “Resetting the counters for specific users”
- 📖 P.293 “Resetting the counters for all users”
- 📖 P.294 “Exporting user information and counters”
- 📖 P.296 “Importing user information”

The registered users can view the own user information in the User Confirm/Create/Modify page. Users can also change the own password (only when the Local MFP Authentication is enabled).

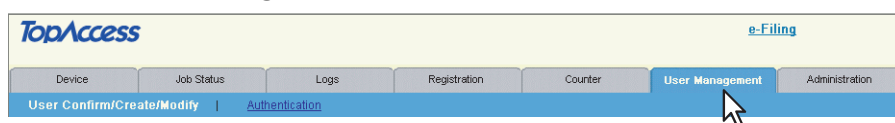
- 📖 P.298 “Viewing the own user information by a user”
- 📖 P.299 “Changing a password by a user (Local MFP Authentication only)”

Notes

- When the Windows Domain or LDAP Authentication is used and the [Create User Information Automatically] option is enabled when enabling the User Management Setting, the user information can be registered automatically in the equipment when a user enters the user name and password in the User Authentication screen and then enters the department code.
- There is “Undefined” user information that is registered as the default. This user information is used to count the Invalid jobs. You can view the counter information of this user information, but cannot modify or delete this default user information.

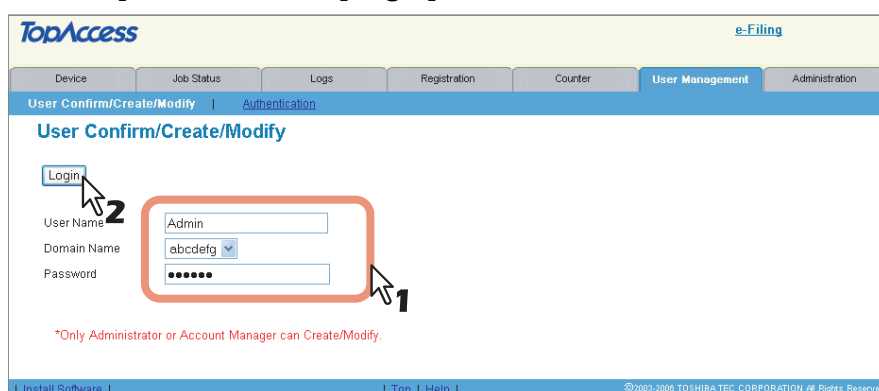
Creating or modifying user information

1 Click the [User Management] tab.



The login page is displayed.

2 Enter “Admin” in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

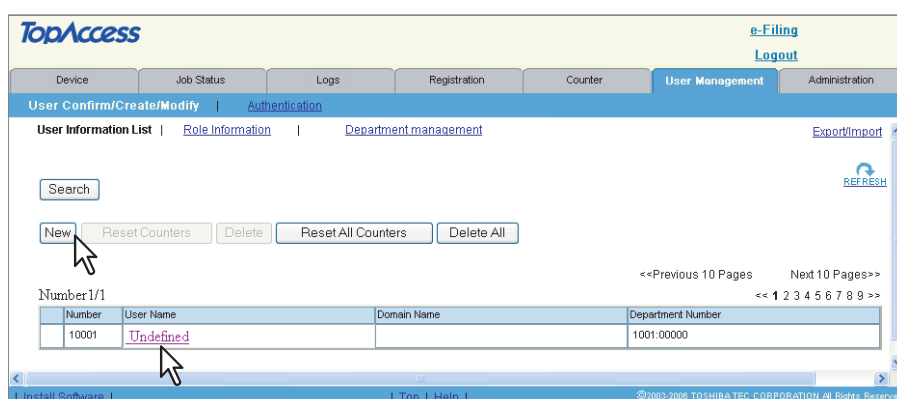


The User Information List submenu page is displayed.

Tips

- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [New] to create a new user or click a user name link to modify the existing user information.



The User Information page is opened.

4 Enter the following items and press [Save].

Create User Information

Save Cancel

User Name **2**

Domain Name

Password

Department Number

Account Manager

Set Limitation of Full Color

Maximum reached for Full Color output

Set Limitation of Black

Maximum reached for Black output

user01

abcdefg

.....

0001:Dept01

Disable

OFF

OFF

1

User Name — Enter a login user name. You can enter up to 128 characters.

Domain Name — Select the domain name that this user will login. The domain name that is set while enabling the Windows Domain authentication is used for the authentication.

Password — Enter a login password. You can enter up to 64 characters. You do not have to specify this when the Windows Domain or LDAP authentication is used.

Department Number — Select the department code that the user belongs. The jobs that are performed by the user are counted as the specified department code.

Account Manager — Select whether this user is registered as the Account Manager. Users who are registered as the Account Manager can log in to the User Information List submenu page.

Set Limitation of Full Color — Select whether to enable the limitation for color outputs for this user. When you select [ON], enter the maximum number of color outputs for this user in the [Maximum reached for Full Color output] box.

Maximum reached for Full Color output — Enter the maximum number of color outputs for this user when the [Set Limitation of Full Color] option is enabled.

Set Limitation of Black — Select whether to enable the limitation of black outputs for this user. When you select [ON], enter the maximum number of black outputs for this user in the [Maximum reached for Black output] box.

Maximum reached for Black output — Enter the maximum number of black outputs for this user when the [Set Limitation of Black] option is enabled.

Tips

- You can also delete the user information by clicking [Delete].
- You can also reset the counter for this user by clicking [Reset Counters].
- When you are editing the existing user information, the counter information of the user is displayed in the page.
- [Set Limitation of Full Color] and [Maximum reached for Full Color output] are displayed only on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series.
When the total count of color outputs in copying or printing reaches the maximum number, printing cannot be performed.
- On the TopAccess menu of the e-STUDIO855 Series and the e-STUDIO455 Series, [Set Limitation of Black] is displayed as [Set Limitation] and [Maximum reached for Black output] is displayed as [Maximum reached].
When the total count of black outputs in copying, printing, those in printing received faxes*1 or system page reaches the maximum number, printing cannot be performed.

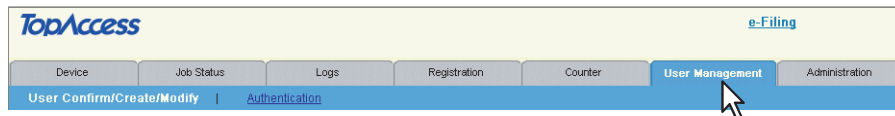
*1 The number of outputs are only counted for received faxes, in which the department code needs to be entered, such as manual reception, polling reception or the printing of originals stored in the confidential mailbox and the bulletin mailbox.

Deleting user information

Notes

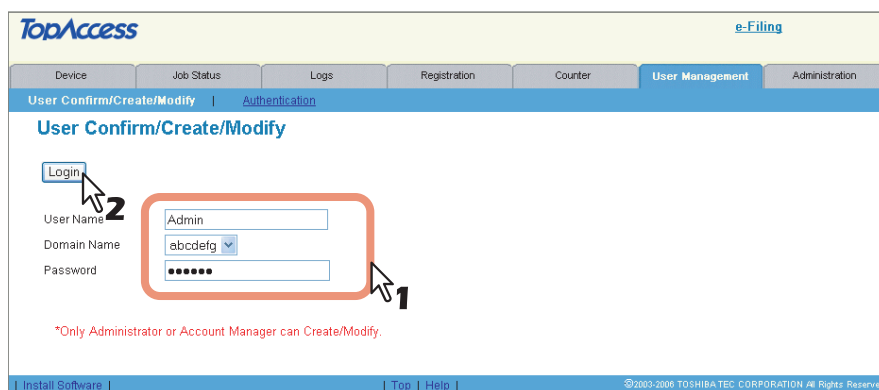
- When the user's jobs are in progress or the user is currently logged in to touch panel, the user information cannot be deleted.
- The [Undefined] user information cannot be deleted.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

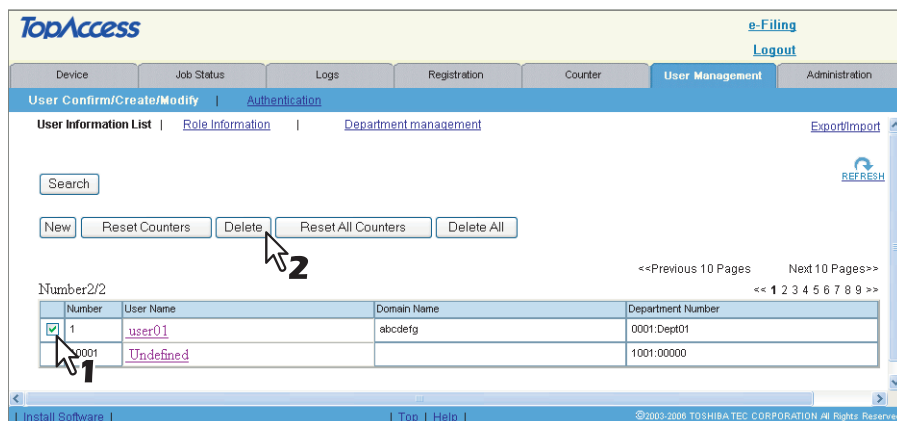


The User Information List submenu page is displayed.

Tips

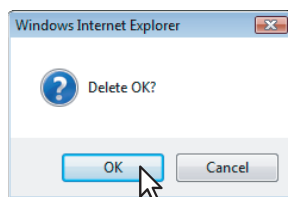
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Select the check boxes of users that you want to delete and click [Delete].



The confirmation dialog box appears.

4 Click [OK] to delete the user information.



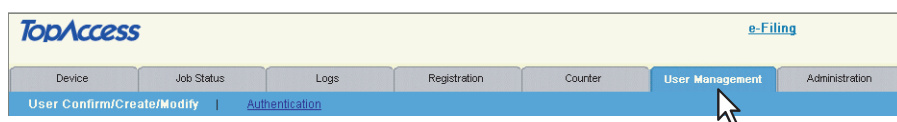
The selected users are deleted.

Deleting all user information

Notes

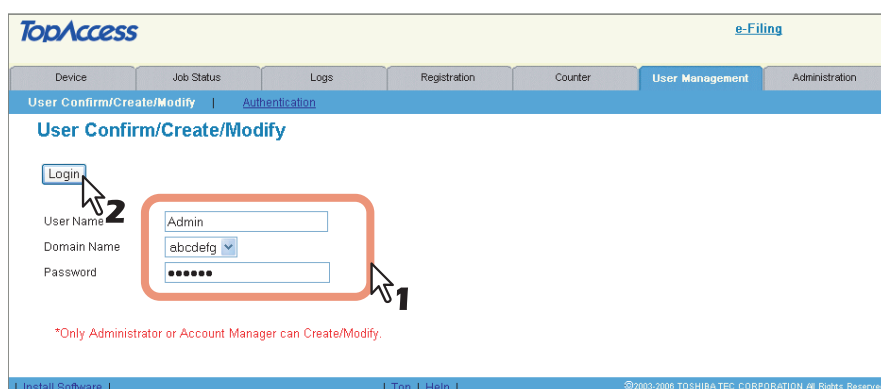
- When the user's jobs are in progress or the user is currently logged in the touch panel, user information cannot be deleted.
- The [Undefined] user information cannot be deleted.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

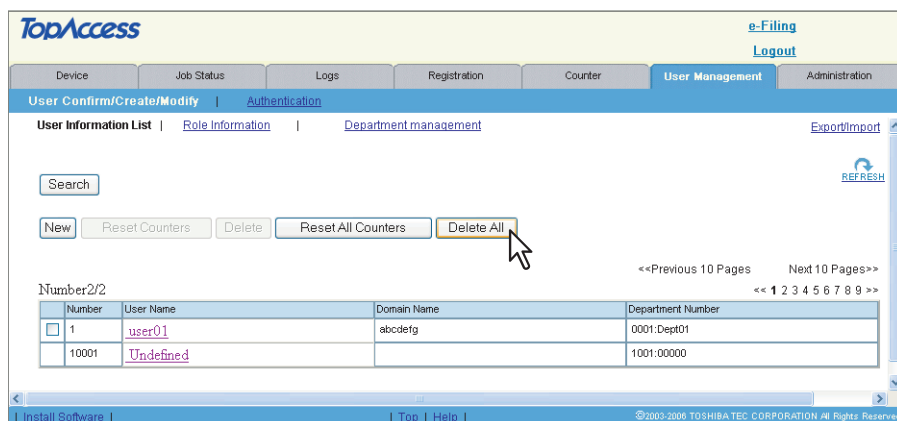


The User Information List submenu page is displayed.

Tips

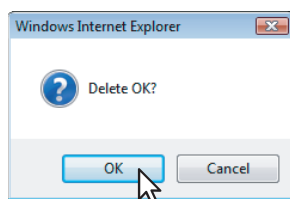
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [Delete All].



The confirmation dialog box appears.

4 Click [OK] to delete all user information.



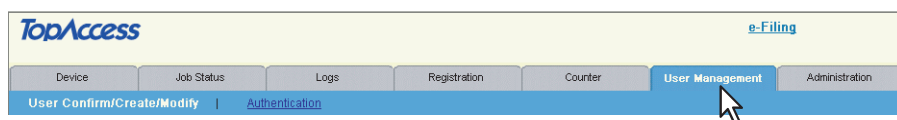
All user information is deleted.

Resetting the counters for specific users

Note

When the user's jobs are in progress or the user is currently logged in the touch panel, you cannot reset the user's counters.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter “Admin” in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

TopAccess e-Filing

Device Job Status Logs Registration Counter **User Management** Administration

User Confirm/Create/Modify Authentication

User Confirm/Create/Modify

Login

User Name Admin

Domain Name abcdefg

Password

*Only Administrator or Account Manager can Create/Modify.

Install Software Top Help ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The User Information List submenu page is displayed.

Tips

- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Select the check boxes of users whose counters are to be reset and click [Reset Counters].

TopAccess e-Filing

Device Job Status Logs Registration Counter **User Management** Administration

User Confirm/Create/Modify Authentication

User Information List Role Information Department management

Search

New Reset Counters Delete Reset All Counters Delete All

Number 2/2

<<Previous 10 Pages Next 10 Pages>>

<< 1 2 3 4 5 6 7 8 9 >>

Number	User Name	Domain Name	Department Number
1	user01	abcdefg	0001:Dept01
10001	Undefined		1001:00000

Install Software Top Help ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The confirmation dialog box appears.

4 Click [OK] to reset the counters.

Windows Internet Explorer

Clear OK?

OK Cancel

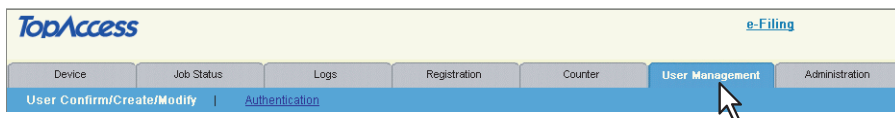
The counters of selected users are cleared.

Resetting the counters for all users

Note

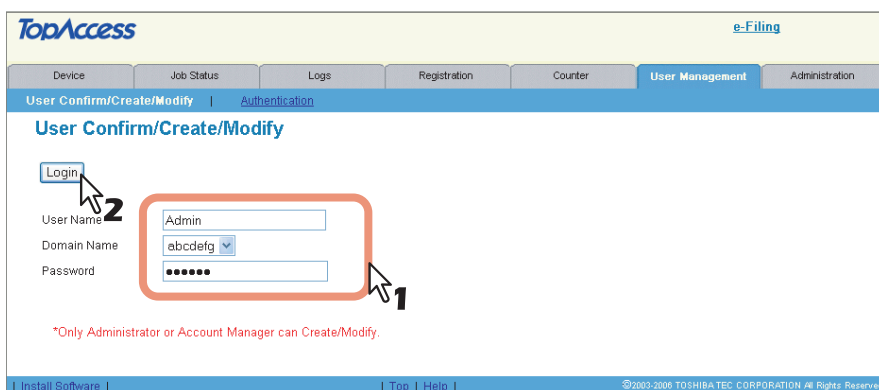
When the user's jobs are in progress or the user is currently logged in the touch panel, you cannot reset the user's counters.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

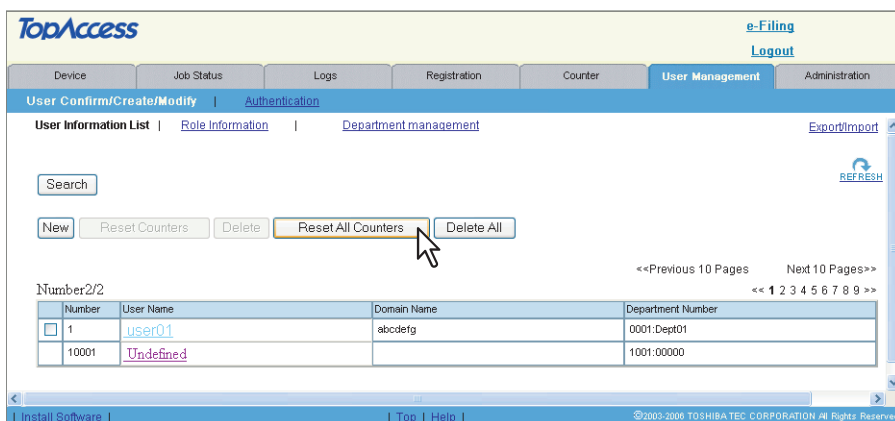


The User Information List submenu page is displayed.

Tips

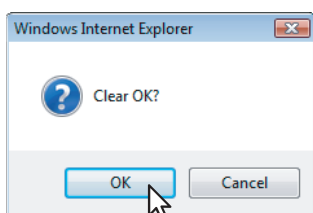
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [Reset All Counters].



The confirmation dialog box appears.

4 Click [OK] to reset all counters.



All user information counters are reset.

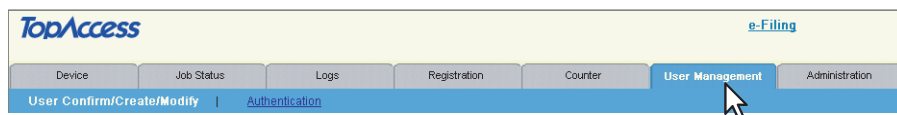
Exporting user information and counters

The user information can be exported as a CSV file for use in other equipment.

Note

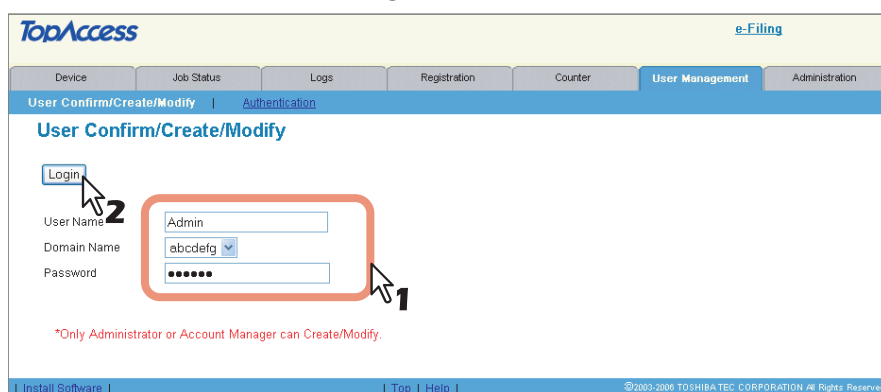
Before exporting the user information, confirm that there are not any jobs in process, private print jobs, hold print jobs, scheduled print jobs or proof print jobs. If such jobs exist, the user information cannot be exported. If it takes long to export the user information, retry after this equipment enters the Sleep mode. It may take a relatively long time to export it when there are many user information items or when the user information includes long user names or domain names.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

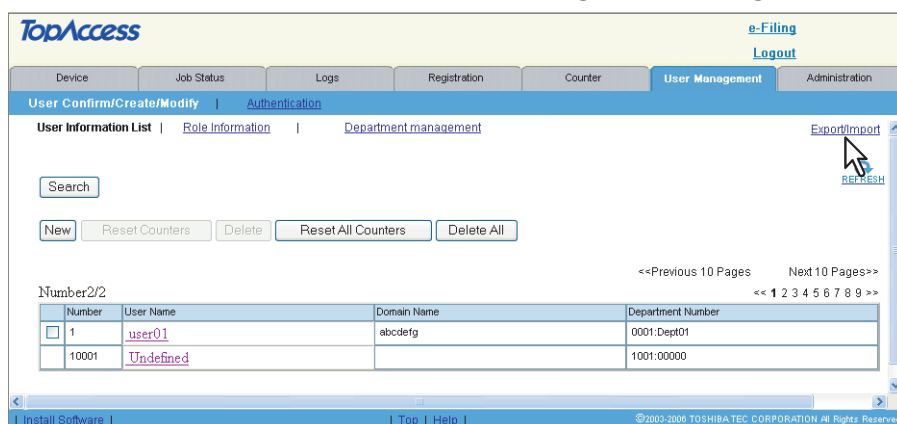


The User Information List submenu page is displayed.

Tips

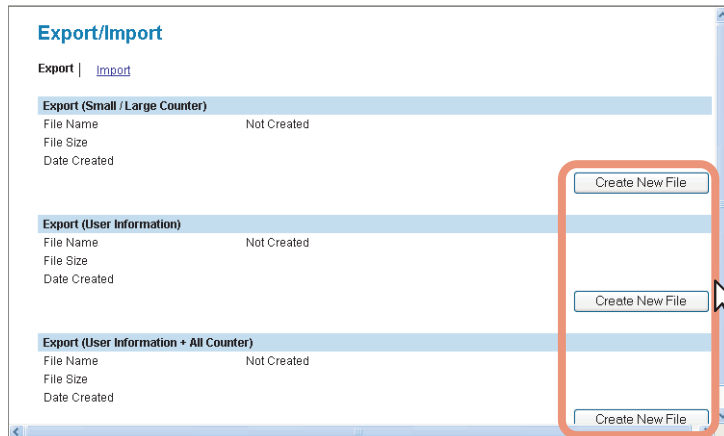
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click the [Export/Import] link at the upper right of the page.



The Export/Import window appears.

4 Click [Create New File] under the file to be exported.



Export (Small/Large Counter) — Click [Create New File] here to export the counter information only.

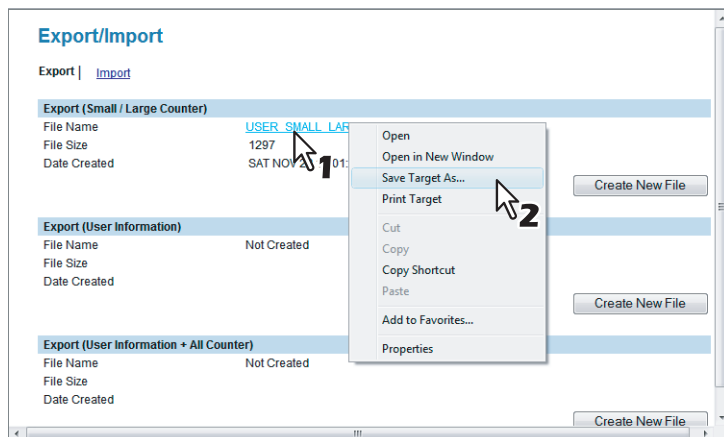
Export (User Information) — Click [Create New File] here to export the user information only.

Export (User Information + All Counter) — Click [Create New File] here to export the counter information and user information.

Tip

If you have previously exported user information data, the exported file link and information are displayed on the page. You can click the link to save the previously exported file.

5 Right-click the [File Name] link and select [Save Target As].

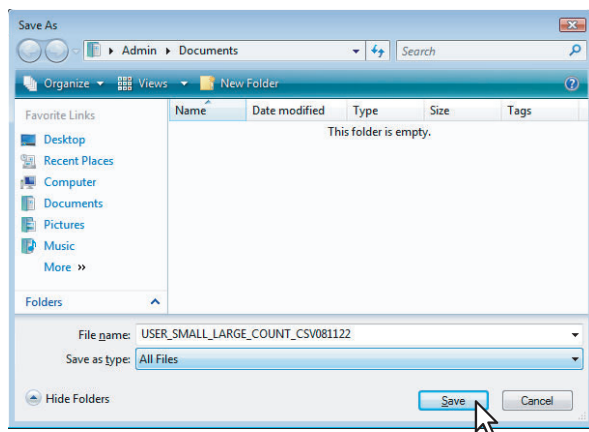


The [Save As] dialog box appears.

Notes

- If the [File Name] link is not displayed or not updated, close the window and try again. Creating a new file may take a few minutes.
- Importing of the Small/Large Counter data in a CSV format is not available.

6 Select the file location and select [All Files] in the [Save as type] box. Then click [Save].



The CSV file that contains the user information data is saved in the selected location.

Importing user information

You can import user information that is exported from other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series to this equipment in a CSV format. The imported file must be a comma delimited CSV file and created in a suitable format for the user information data.

Notes

- When the user information data is imported, the old data will be cleared and overwritten with the new data.
- Before importing the user information, confirm that there are not any jobs in process, private print jobs, hold print jobs, scheduled print jobs or proof print jobs. If such jobs exist, the user information cannot be imported. If it takes long to import the user information, retry after this equipment enters the Sleep mode. It may take a relatively long time to import it when there are many user information items or when the user information includes long user names or domain names.
- Before importing the CSV file, confirm that all required data for each item is entered in the CSV file. The required items vary depending on the authentication type.

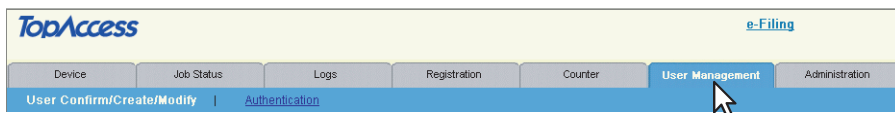
* Yes = Required, No = Not Required

Items	Windows Domain	LDAP	Local	Supplements
UserId	Yes	Yes	Yes	
Username	Yes	Yes	Yes	
Password	No	No	Yes	The value must be deleted for Windows Domain or LDAP.
Domainname	Yes	No	No	The value must be deleted for LDAP or Local.
Department Code	Yes	Yes	Yes	
Access Manager	No	No	No	When the value is blank, the value is set to "0". 0 = Disable, 1 = Enable
Rolebase	No	No	No	When the value is blank, the value is set to "0". 0 = Disable, 1 = Enable
Set limitation of full color	No	No	No	When the value is blank or invalid value is entered, the value is set to [OFF].
Maximum reached for Full Color output	No	No	No	
Set Limitation of Black	No	No	No	When the value is blank or invalid value is entered, the value is set to [OFF].
Maximum reached for Black output	No	No	No	

* [Set Limitation of Full Color] and [Maximum reached for Full Color output] are displayed only on the TopAccess menu of the e-STUDIO4520C Series and the e-STUDIO6530C Series.

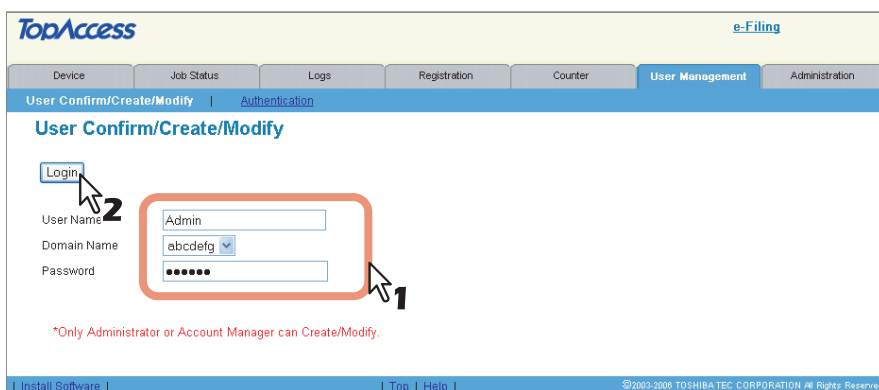
- Be sure that any of the user ID and the user name (information entered in the "UserId" and "Username" fields above) is not overlapped in a CSV file to be imported. If they are overlapped, the correct user information will not be registered even if the CSV file was imported.
- When a user sends a print job while importing user information, an alert message will be displayed to say that the equipment cannot receive the print job. When this equipment receives a fax while importing user information, this equipment cannot start receiving the fax, so that it continues ringing.

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

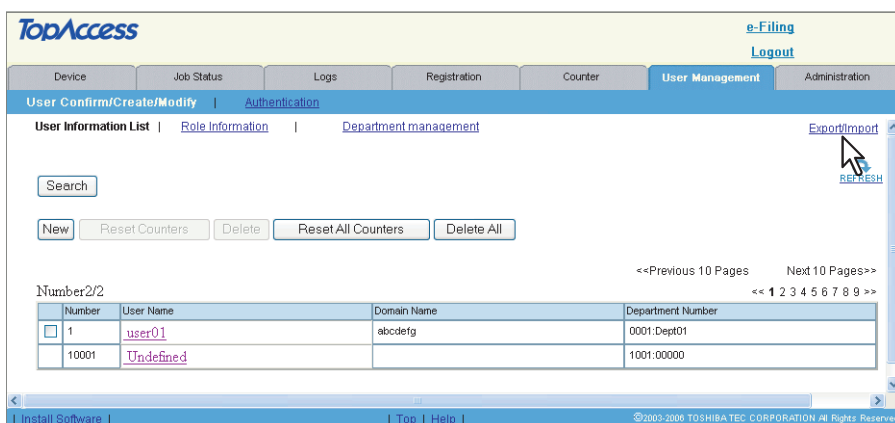


The User Information List submenu page is displayed.

Tips

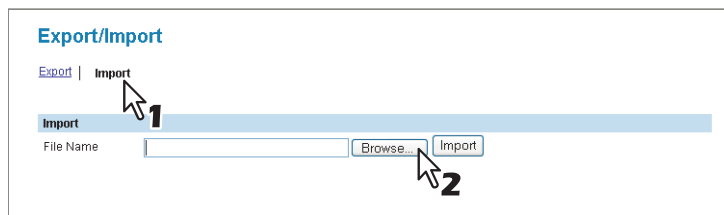
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click the [Export/Import] link at the upper right of the page.



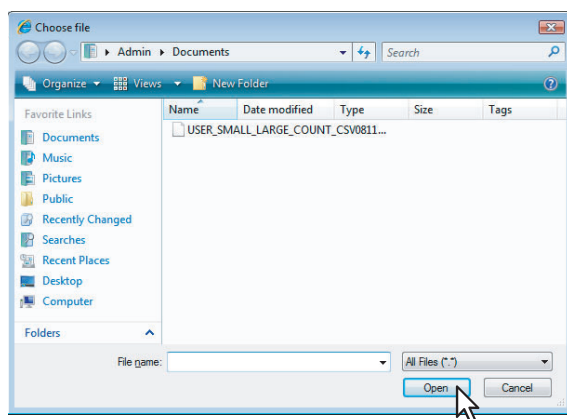
The Export/Import window appears.

4 Click [Import] menu and click [Browse].



The Choose file dialog box appears.

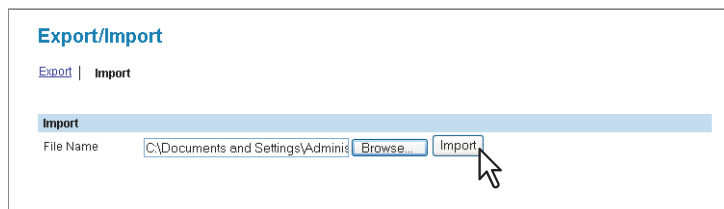
5 Select the CSV file that contains the user information data and click [Open].



Note

Importing of the Small/Large Counter data in a CSV format is not available.

6 Click [Import].

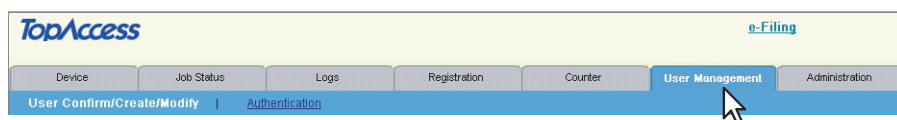


The data is imported to the User Information list page.

Viewing the own user information by a user

Users can view their own user information by logging in to the User Confirm/Create/Modify page. When the Role Based Access Control is enabled, users can also confirm the functions to be allowed.

1 Click the [User Management] tab.



The login page is displayed.

- 2 Enter your user name in the [User Name] box, select a domain name (required only when Windows Domain Authentication is enabled), enter your password in the [Password] box, and click [Login].

TopAccess e-Filing

Device Job Status Logs Registration Counter **User Management** Administration

User Confirm/Create/Modify Authentication

User Confirm/Create/Modify

Login

User Name user01

Domain Name abcdefg

Password

*Only Administrator or Account Manager can Create/Modify.

Install Software Top Help ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

- 3 The User Information page is displayed.

TopAccess e-Filing Logout

Device Job Status Logs Registration Counter **User Management** Administration

User Confirm/Create/Modify Authentication

User Information

User Name	user01
Domain Name	abcdefg
Department Number	0001_Dept01
Account Manager	Disable
Set Limitation of Full Color	OFF
Maximum reached for Full Color output	
Set Limitation of Black	OFF
Maximum reached for Black output	

Role Information

Registration/Settings	ON
Copy	ON
Email	ON
File Share	ON
InternetFax	ON
Print	ON
e-Filing	ON
Fax	ON

Change Password

Install Software Top Help ©2003-2006 TOSHIBA TEC CORPORATION All Rights Reserved

Changing a password by a user (Local MFP Authentication only)

When the Local MFP Authentication is enabled, not only an administrator or account managers but also each registered user can change the password himself.

- 1 Click the [User Management] tab.

TopAccess e-Filing

Device Job Status Logs Registration Counter **User Management** Administration

User Confirm/Create/Modify Authentication

The login page is displayed.

- 2** Enter your user name in the [User Name] box, enter your password in the [Password] box, and click [Login].

The User Information page is displayed.

- 3** Click [Change Password].

The Change Password window appears.

- 4** Enter the following items and click [Save].

Old Password — Enter your login password.

New Password — Enter a new login password. You can enter up to 64 characters.

Retype Password — Enter the new login password again.

- 5** Click [OK].

The password is changed.

■ Setting role information

Role information is stored in this equipment in the XML format. The role information can be exported as a CSV file for use in other equipment.

You can import user information that is exported from other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO3510C Series, e-STUDIO451C Series, e-STUDIO855 Series, e-STUDIO850 Series, e-STUDIO455 Series, e-STUDIO452 Series or e-STUDIO282 Series to this equipment in an XML format.

Files to be imported must be in an XML format that complies with the TopAccess role information format.

Tip

To edit the role information, refer to the information described in the exported role information configuration file.

Note

Web Services Scanning is not given any restrictions by the user management setting.

□ Confirming role information

You can confirm the set functions for role information on the User Confirm/Create/Modify page.

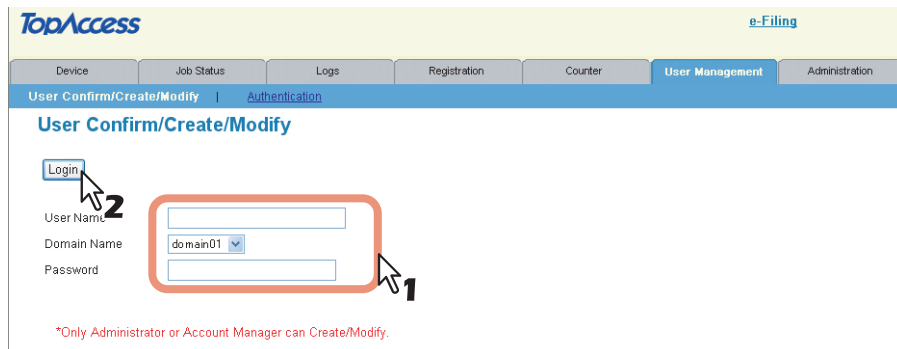
Confirming role information

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

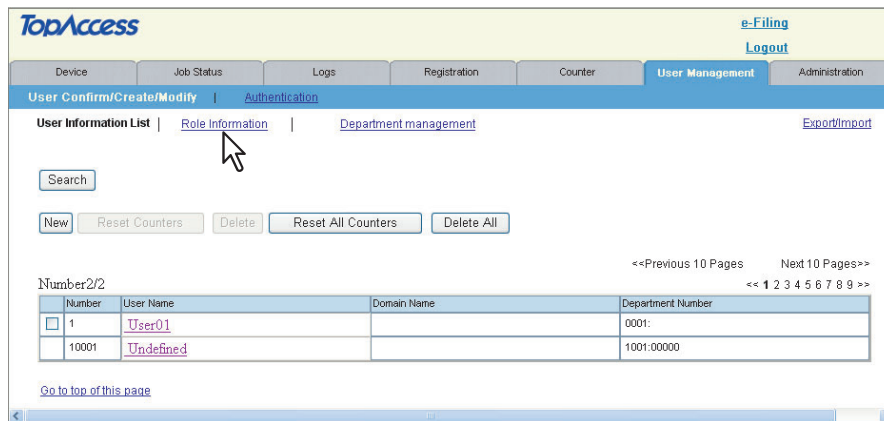


The User Information List submenu page is displayed.

Tips

- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [Role Information].

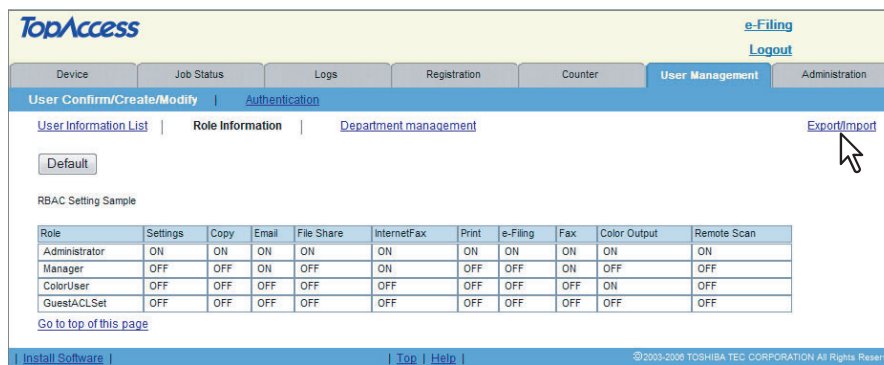


The screenshot shows the TopAccess Administrator interface. The 'User Management' tab is active, and the 'Role Information' sub-tab is selected. The page displays a table with user information. A mouse cursor is pointing at the 'Role Information' link.

Number	User Name	Domain Name	Department Number
1	User01		0001:
10001	Undefined		1001:00000

The Role Information page is displayed.

4 Click the [Export/Import] link at the upper right of the page.



The screenshot shows the 'RBAC Setting Sample' page. The 'Export/Import' link is highlighted in the top right corner. The page contains a table with role settings.

Role	Settings	Copy	Email	File Share	InternetFax	Print	e-Filing	Fax	Color Output	Remote Scan
Administrator	ON	ON	ON	ON	ON	ON	ON	ON	ON	ON
Manager	OFF	OFF	ON	OFF	ON	OFF	OFF	ON	OFF	OFF
ColorUser	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	ON	OFF
GuestACLSet	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF	OFF

The Export/Import window appears.

❑ Exporting/Importing role information

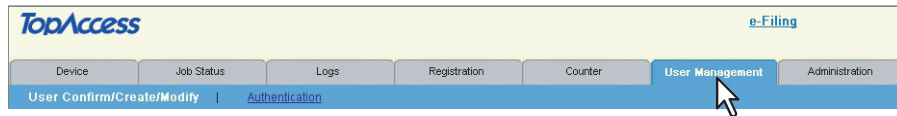
Export or import role information on the User Confirm/Create/Modify page.

📖 P.303 “Exporting Role Information”

📖 P.305 “Importing role information”

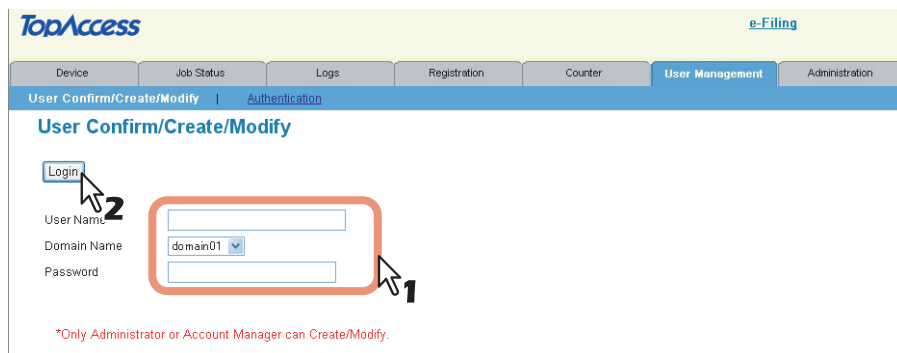
Exporting Role Information

1 Click the [User Management] tab.



The login page is displayed.

2 Enter “Admin” in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

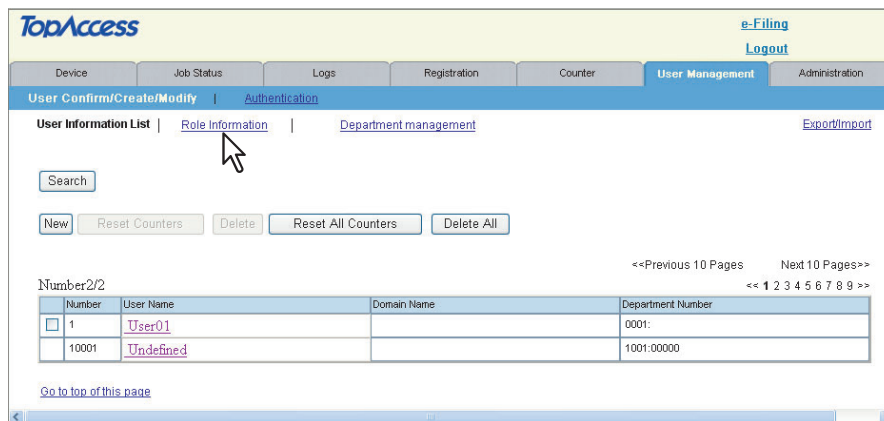


The User Information List submenu page is displayed.

Tips

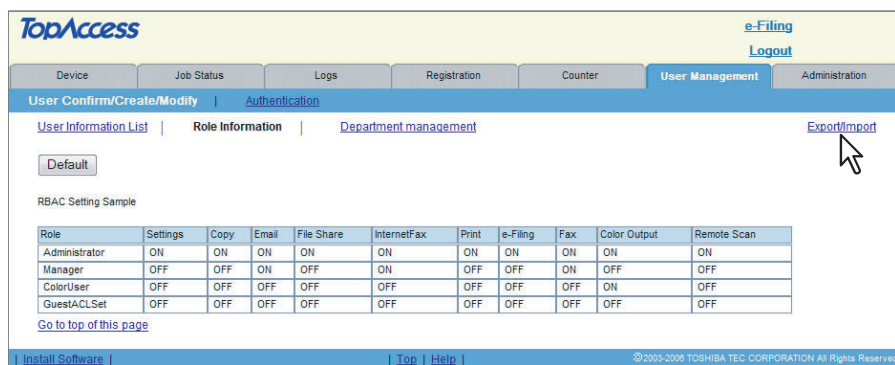
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [Role Information].



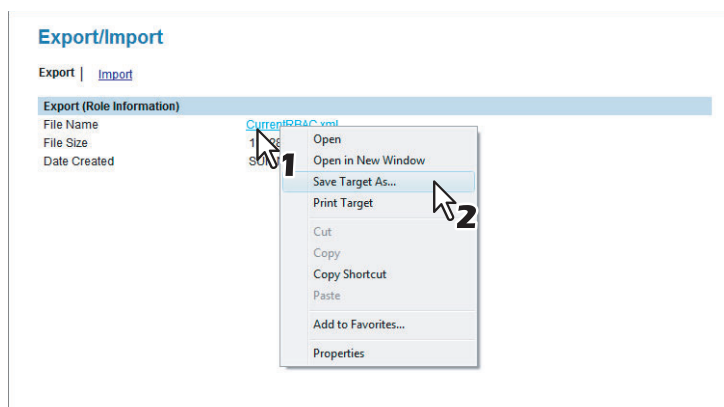
The Role Information page is displayed.

4 Click the [Export/Import] link at the upper right of the page.



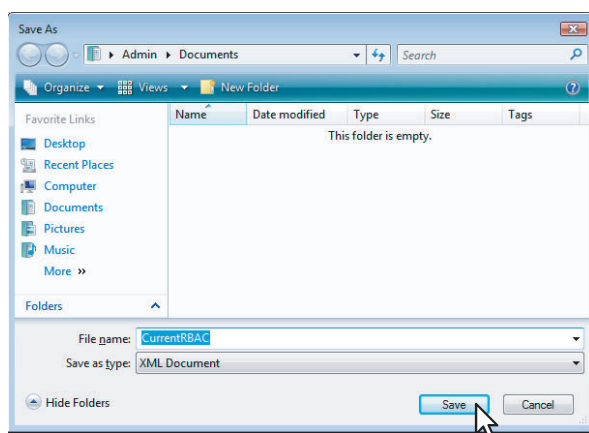
The Export/Import window appears.

5 Right-click the [File Name] link and select [Save Target As].



The [Save As] dialog box appears.

6 Select the file location and select [XML Document] in the [Save as type] box. Then click [Save].



The XML file that contains the role information data is saved in the selected location.

Importing role information

1 Click the [User Management] tab.



The login page is displayed.

2 Enter "Admin" in the [User Name] box, enter the administrator password in the [Password] box, and click [Login].

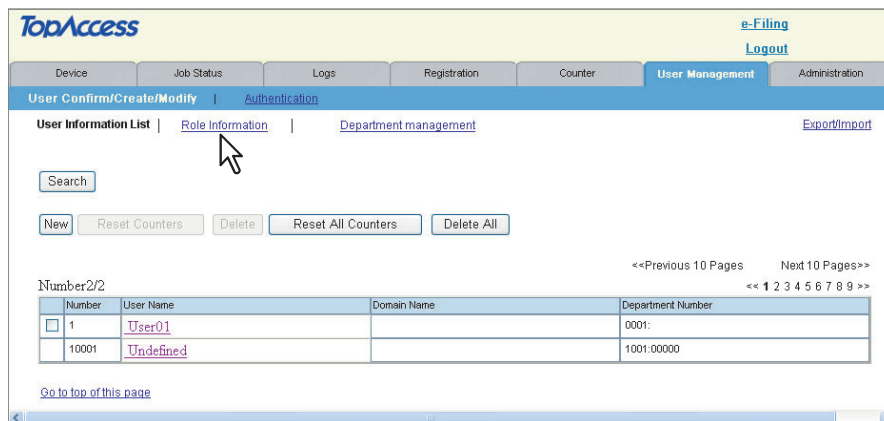


The User Information List submenu page is displayed.

Tips

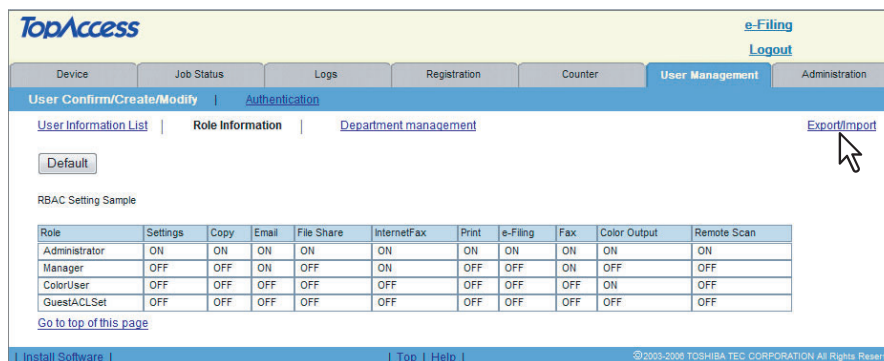
- Users can also log in using a user name, domain name (required only when Windows Domain Authentication is enabled), and password that have been set as Account Manager in User Information.
- You do not have to select the [Domain Name] box when you log in as the Administrator.

3 Click [Role Information].



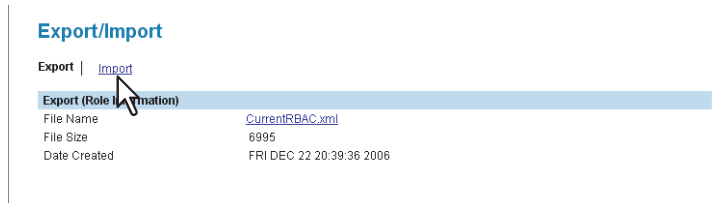
The Role Information window appears.

4 Click the [Export/Import] link at the upper right of the page.



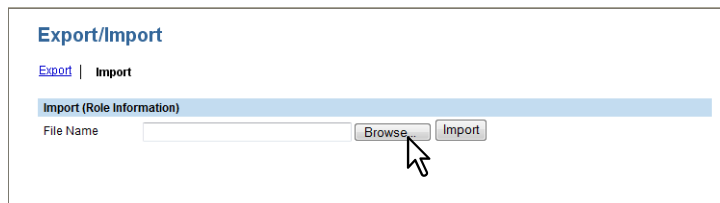
The Export/Import window appears.

5 Click [Import] menu.



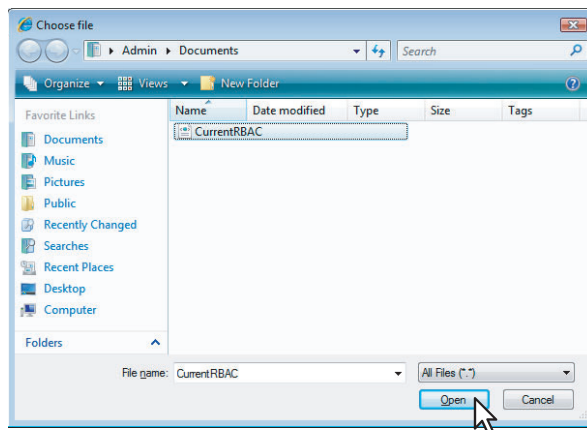
The Import page appears

6 Click [Browse].

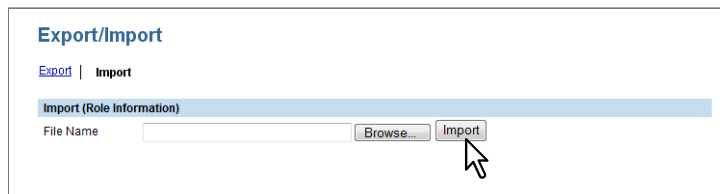


The Choose file dialog box appears.

7 Select the XML file that contains the user information data and click [Open].



8 Click [Import].



The data is imported to Role Information.

■ Setting up User Authentication for Scan to Email

When the User Authentication for Scan to Email is enabled, users must enter the user name and password before performing Scan to Email.

You can select either the SMTP or LDAP for User Authentication for Scan to Email.

- SMTP Authentication

This equipment can be managed using the SMTP Authentication.

When this is configured, users must enter the user name and password that is registered in the SMTP server to perform Scan to Email on the control panel of this equipment.

P.307 “Enabling User Authentication for Scan to Email (SMTP)”

- LDAP Authentication

When your network manages the network users using the LDAP, this equipment can be managed using the LDAP Authentication.

When this is configured, users must enter the user name and password that is registered in the LDAP server to perform Scan to Email on the control panel of this equipment.

P.310 “Enabling User Authentication for Scan to Email (LDAP)”

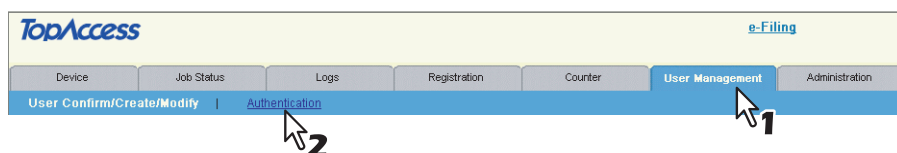
Note

When the User Authentication for Scan to Email is enabled, the Email Notification may not be sent to the administrator. Make sure to set the login name and password in the SMTP Client settings.

P.134 “Setting up SMTP Client”

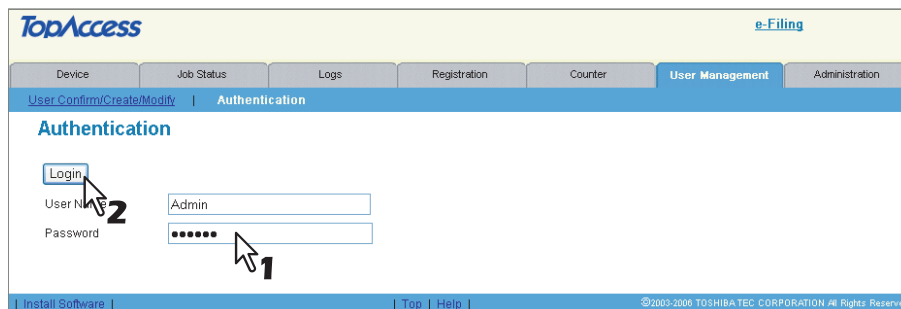
Enabling User Authentication for Scan to Email (SMTP)

1 Click the [User Management] tab and the [Authentication] menu.



The login page is displayed.

2 Enter the administrator password and click [Login].



The Authentication page is displayed.

3 Click [User Authentication for Scan to Email].

The screenshot shows the TopAccess Administrator interface. The top navigation bar includes links for e-Filing, Logout, and various system settings. The main content area is titled 'Authentication' and contains three sections: 'Department Setting', 'User Management Setting', and 'User Authentication for Scan to Email'. The 'User Authentication for Scan to Email' section is highlighted with a mouse cursor, indicating it is the next step in the process.

The User Authentication for Scan to Email page opens.

4 Select [SMTP] in the [Method] box and click [Next].

The screenshot shows the 'User Authentication for Scan to Email' configuration page. It includes 'Cancel' and 'Next' buttons. Below them, the 'Select Authentication Method' section shows 'Method' set to 'SMTP' and 'Internet Fax Not Allowed' checked. Arrows and numbers indicate the next steps: clicking 'Next' (1) and selecting 'SMTP' (2).

Tips

- This equipment can set authentication for Scan to Email, but cannot set authentication for Internet Fax transmission. If you do not want to allow users to perform the Internet Fax transmission, select the [Internet Fax Not Allowed] check box. When you select this check box, users can no longer perform Internet Fax transmissions.
- When you want to disable the User Authentication for Scan to Email, select [Disable] in the [Method] and click [Next].

5 Enter the IP address or FQDN (Fully Qualified Domain Name) of the SMTP server and select the authentication type in the [Authentication] box. Then click [Next].

The screenshot shows the 'User Authentication for Scan to Email' configuration page. It includes 'Cancel' and 'Next' buttons. Below them, the 'SMTP Authentication Setting' section shows 'SMTP Server Address' set to '10.10.20.14' and 'Authentication' set to 'Plain'. Arrows and numbers indicate the next steps: clicking 'Next' (1) and selecting 'Plain' (2).

Tip

If you have set the SMTP Client settings in the Network setup page, the setting values of the SMTP Client settings in the Network setup page are reflected in these settings.

6 Specify how the From Address is set for Scan to Email.

User Authentication for Scan to Email

Cancel Finish

Setting method of From Address field.

☒ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☐ Setting Address is searching from 'User Name' of LDAP.

[More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

☐ From Address is acquired from Email setting.

*From Address registered by what Email Setting is used.

☒ From Address cannot be edited in Scan to Email.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, where “User Name” is the user name that is entered on the touch panel for authentication, and “Mail Domain Name” is the domain name that is entered in the [Mail Domain Name] box. When this is selected, enter the domain name in the [Mail Domain Name] box.

Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address found in the LDAP server. Specify the LDAP server name found in the [LDAP Server] box, the schema of an email address to set as the email address in the [Attribute type of 'E-mail Address'] box, the schema to search for the user name in the [Attribute type of 'User Name'] box or the domain name that is used when the user name is not found in the [Mail Domain Name] box.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'E-mail Address']: Select this to specify the schema to set as the email address when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema specified in [Attribute type of 'User Name'] in the specified LDAP server. If the user name is not found in the specified schema, the email address is set as “User Name@Mail Domain Name”. The user name entered on the touch panel for authentication is used for “User Name”.

[Mail Domain Name]: Select this to use the domain name entered in the [Mail Domain Name] box if the schema specified in [Attribute type of 'User Name'] is not found.

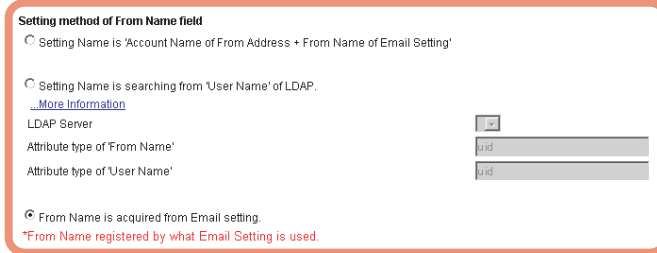
Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Name field].

From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.

From Address cannot be edited in Scan to Email — Select this check box if you do not want to allow users to edit the From Address.

7 Specify how the From Name is set for Scan to Email.



Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Name is 'Account Name of From Address + From Name of Email Setting' — Select this check box to set the name of an email sender in a format 'Account Name + (space) + From Name of Email Setting'. The character string before "@" in the sender's address (From Address) comes at 'Account Name'. The name displayed in [From Name] of the [Email] submenu of the [Setup] menu on the [Administration] tab page comes at 'From Name of Email Setting'.

Setting Name is searching from 'User Name' of LDAP.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'From Name']: Select this to specify the schema to set as the sender name when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema in [Attribute type of 'User Name'] in the specified LDAP server.

If the entered user name is not found in the specified schema, the From Name is set the same as [Setting Name is 'Account Name of From Address + From Name of Email Setting'].

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Address field].

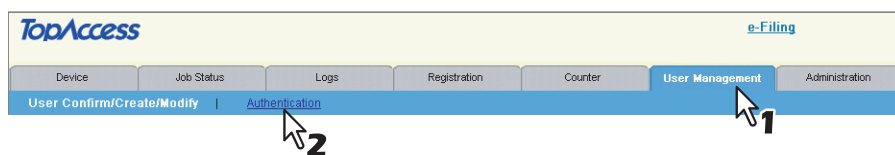
From Name is acquired from Email setting. — Select this to set the sender name specified in the email setting.

8 Click [Finish].

The User Authentication for Scan to Email is enabled.

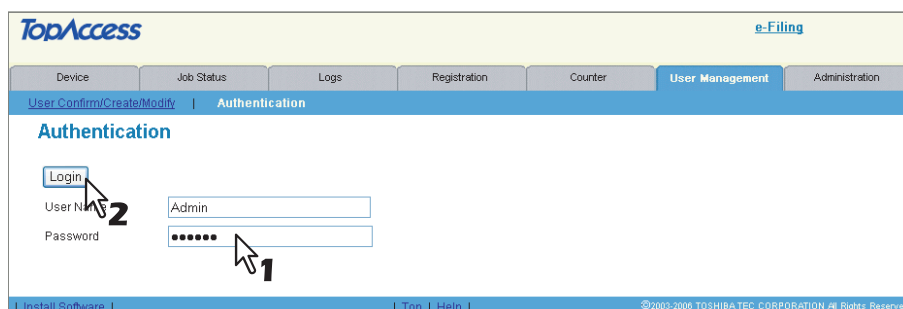
Enabling User Authentication for Scan to Email (LDAP)

1 Click the [User Management] tab and the [Authentication] menu.



The login page is displayed.

2 Enter the administrator password and click [Login].



The Authentication page is displayed.

3 Click [User Authentication for Scan to Email].

The screenshot shows the TopAccess Administrator interface. The 'Authentication' tab is selected. Under 'User Authentication for Scan to Email', the 'Method' dropdown is set to 'Disable'. A red box highlights this section, and a mouse cursor points to the 'Method' dropdown.

The User Authentication for Scan to Email page opens.

4 Select [LDAP] in the [Method] box and click [Next].

The screenshot shows the 'User Authentication for Scan to Email' dialog box. The 'Method' dropdown is set to 'LDAP'. The 'Internet Fax Not Allowed' checkbox is checked. A red box highlights the 'Method' dropdown and the 'Next' button.

Tips

- This equipment can set authentication for Scan to Email, but cannot set authentication for Internet Fax transmission. If you do not want to allow users to perform the Internet Fax transmission, select the [Internet Fax Not Allowed] check box. When you select this box, users can no longer perform Internet Fax transmissions.
- When you want to disable the User Authentication for Scan to Email, select [Disable] in the [Method] and click [Next].

5 Select the LDAP server to be used for authentication and select the type of the LDAP server. Then click [Next].

The screenshot shows the 'User Authentication for Scan to Email' dialog box. The 'LDAP Authentication' section is expanded. The 'LDAP Server' dropdown is set to 'Idap1'. The 'Windows Server' radio button is selected. A red box highlights the 'LDAP Server' dropdown and the 'Windows Server' radio button.

Windows Server — Select this when LDAP is running on a Windows server.

LDAP Server (Other than Windows Server) — Select this when the LDAP is on running the server other than a Windows server. When this is selected, you have to specify the attribute type of 'User Name'.

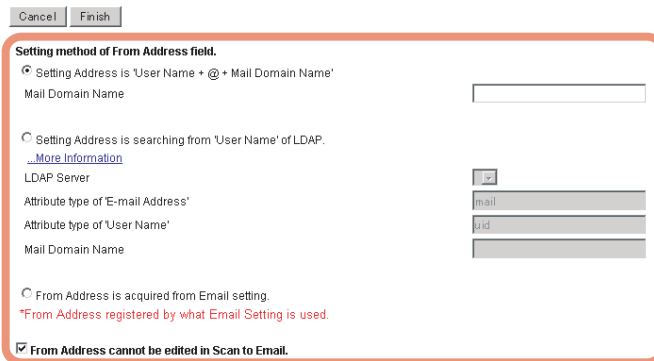
Tip

The LDAP server to be used for authentication must be configured in the [Directory Service] submenu in the [Maintenance] menu.

📖 P.216 “Managing directory service”

6 Specify how the From Address is set for Scan to Email.

User Authentication for Scan to Email



Cancel Finish

Setting method of From Address field.

☒ Setting Address is 'User Name + @ + Mail Domain Name'

Mail Domain Name

☐ Setting Address is searching from 'User Name' of LDAP.

[More Information](#)

LDAP Server

Attribute type of 'E-mail Address'

Attribute type of 'User Name'

Mail Domain Name

☐ From Address is acquired from Email setting.

*From Address registered by what Email Setting is used.

☒ From Address cannot be edited in Scan to Email.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, where “User Name” is the user name that is entered on the touch panel for authentication, and “Mail Domain Name” is the domain name that is entered in the [Mail Domain Name] box. When this is selected, enter the domain name in the [Mail Domain Name] box.

Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address found in the LDAP server. Specify the LDAP server name found in the [LDAP Server] box, the schema of an email address to set as the email address in the [Attribute type of 'E-mail Address'] box, the schema to search for the user name in the [Attribute type of 'User Name'] box or the domain name that is used when the user name is not found in the [Mail Domain Name] box.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'E-mail Address']: Select this to specify the schema to set as the email address when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema specified in [Attribute type of 'User Name'] in the specified LDAP server. If the user name is not found in the specified schema, the email address is set as “User Name@Mail Domain Name”. The user name entered on the touch panel for authentication is used for “User Name”.

[Mail Domain Name]: Select this to use the domain name entered in the [Mail Domain Name] box if the schema specified in [Attribute type of 'User Name'] is not found.

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Name field].

From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.

From Address cannot be edited in Scan to Email — Select this check box if you do not want to allow users to edit the From Address.

7 Specify how the From Name is set for Scan to Email.

Setting method of From Name field

☐ Setting Name is 'Account Name of From Address + From Name of Email Setting'

☐ Setting Name is searching from 'User Name' of LDAP.
[..More Information](#)

LDAP Server

Attribute type of 'From Name'

Attribute type of 'User Name'

☒ From Name is acquired from Email setting.
 *From Name registered by what Email Setting is used.

Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Name is 'Account Name of From Address + From Name of Email Setting' — Select this check box to set the name of an email sender in a format 'Account Name + (space) + From Name of Email Setting'. The character string before "@" in the sender's address (From Address) comes at 'Account Name'. The name displayed in [From Name] of the [Email] submenu of the [Setup] menu on the [Administration] tab page comes at 'From Name of Email Setting'.

Setting Name is searching from 'User Name' of LDAP.

[LDAP Server]: Select this to set the LDAP server to search for the sender name.

[Attribute type of 'From Name']: Select this to specify the schema to set as the sender name when the schema specified in [Attribute type of 'User Name'] is found.

[Attribute type of 'User Name']: Select this to search for the user name, which is entered on the touch panel for authentication, from the schema in [Attribute type of 'User Name'] in the specified LDAP server.

If the entered user name is not found in the specified schema, the From Name is set the same as [Setting Name is 'Account Name of From Address + From Name of Email Setting'].

Note

For [LDAP Server] and [Attribute type of 'User Name'], select the same items as for [LDAP Server] and [Attribute type of 'User Name'] in [Setting method of From Address field].

From Name is acquired from Email setting. — Select this to set the sender name specified in the email setting.

8 Click [Finish].

User Authentication for Scan to Email is enabled.

OPTION SETUPS

This section describes how to set up options from the TopAccess menus.

About Option Setups	316
Setting up IP Security Function	317
Setting up IPsec	318
Registering policies	319
Installing IPsec certificate	326
Flushing out IPsec sessions	332
Setting up Meta Scan Function	333
Registering/Editing Meta Scan templates	333
Maintaining Meta Scan templates	349
Maintaining XML format files	355

About Option Setups

You can set up the functions of the options below from the TopAccess menus if the options below are installable to this equipment.

IPsec Enabler (GP-1080)

With this option, you can enable data encryption using IPsec (IP Security Protocol) on this equipment. On the TopAccess menus, you can switch whether to enable or disable the IPsec function, or set the registration, modification or deletion of filters, IKE keys, profiles and policies used for IPsec.

 P.317 “Setting up IP Security Function”

Meta Scan Enabler (GS-1010)

With this option, you can enable the “Meta Scan function”. Using this function, you can send emails with meta data (XML format files) attached, together with the image data attachment that you scanned with this equipment. You can operate meta data which define the processing method of the scanned data and a workflow system which circulates or manages data together, so that, for example, you can configure a document solution environment that automatically processes image data scanned with this equipment in a workflow.

On the TopAccess menus, you can register templates for the Meta Scan function or import XML format files defining the contents of meta data.

 P.333 “Setting up Meta Scan Function”

External Interface Enabler (GS-1020)

With this option, you can enable the “EWB (Embedded Web Browser) function” which displays web pages on the touch panel of this equipment, or “Web Service Interface function” which allows you to remotely control jobs or data viewing.

On the TopAccess menu, you can set the default page of the EWB (Embedded Web Browser) function, and also register or delete a server for sending user information that was authenticated on this equipment. For the details of the EWB function, contact your service technician.

Notes

- Option setup menus on the TopAccess menu are displayed only when the corresponding option is installed.
- Only the administrator can set up these options.

Setting up IP Security Function

With the IP security function, you can enable data encryption communication using IPsec (IP Security Protocol). On the IP security setup menu, you can switch whether to enable or disable the IPsec function, or set the registration, modification or deletion of filters, IKE keys, profiles and policies used for IPsec.

 P.318 “Setup procedure of IP security function”

Notes

- The IPsec Enabler GP-1080 (optional) is required to enable the IP security function.
- IP security setup menus on the TopAccess menu are displayed only when the IP security function is available. ([Administration] tab > [Setup] menu > [Network] submenu > [IP Security])
- Only the administrator can set up IP security function.
- The normal filtering settings are given priority over IP security filtering.
- If [Enable] is selected for [Enable IPsec] of [IP Security], this equipment does not enter the Super Sleep mode.

 P.112 “Setting up Energy Save”

Tip

A fallback function is embedded in the IP security function of this equipment. Fallback occurs automatically from IKEv2 to IKEv1 when this equipment receives a notification message “INVALID_MAJOR_VERSION 5” in a notification payload in IKEv2 communication.

■ Setting up IPsec

The administrator can set up the IP security function on the following TopAccess menu:
[Setup] menu > [Network] submenu > [IP Security]

Setup procedure of IP security function

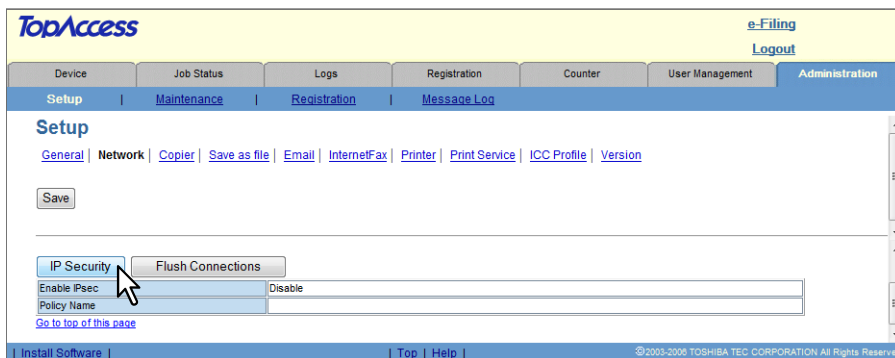
1 Access the TopAccess administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

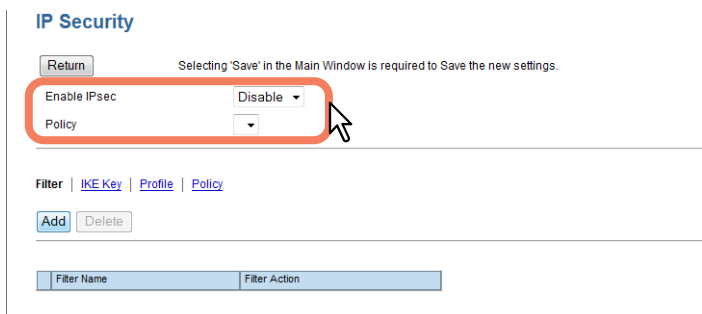
2 Click [Setup], and then [Network].

P.118 "Setting up Network settings"

3 Click a link on the [Network] submenu or scroll down the menu and click [IP Security].



The IP Security setting page is displayed.



On the IP Security setting page, you can set up the items below.

Enable IPsec — Selects whether to enable or disable IPsec.

- **Enable** — Select this to enable IPsec.
- **Disable** — Select this to disable IPsec.

Policy — Selects a policy to be used for IPsec.

Tip

You must select a policy to enable IPsec. Policies must be set according to the IPsec environment that you use and must be registered into this equipment in advance. For instructions on how to register policies, see the following page:

P.319 "Registering policies"

IPsec menu — Select this to access each menu for setting the detailed functions of the IPsec. When you select this menu, the registration contents of each menu are displayed in a list. These contents can be modified or deleted. For instructions on how to operate with each menu, see the following page:

P.319 "Registering policies"

4 Click [Return] after you complete the setting.

The IP Security Setting page is closed.

5 Click [Save].

The confirmation dialog box appears.

6 Click [OK] to apply the change.

Note

During the initialization of a network interface card, the use of a network is not available. During the initialization “Please restart after waiting a few minutes.” appears on the TopAccess menu and also “NETWORK INITIALIZING” appears on the touch panel of this equipment. The TopAccess will be available again when these messages disappear.

Tips

- When you use a certificate for IKE authentication to enable IPsec communication, an IPsec Certificate must be installed in this equipment. For details, see the following page:
[P.326 “Installing IPsec certificate”](#)
- If the keys for IPsec communication are leaked out or any security violation occurs, you can manually delete (flush) the current session with a flush connection function and start a new session. When you want to delete the information of SAD (Security Association Database) for any reason, you can delete it in the same way. For details, see the following page:
[P.332 “Flushing out IPsec sessions”](#)

■ Registering policies

To enable data encryption communication using IPsec, you need to create IPsec policies first according to your system environment. You can create policies by combining IKE key exchange process setting, filtering setting for registration of addresses from which you permit or block access, and ESP or AH settings to be used as a security protocol.

[P.319 “Registering or modifying policies”](#)

[P.325 “Deleting policies”](#)

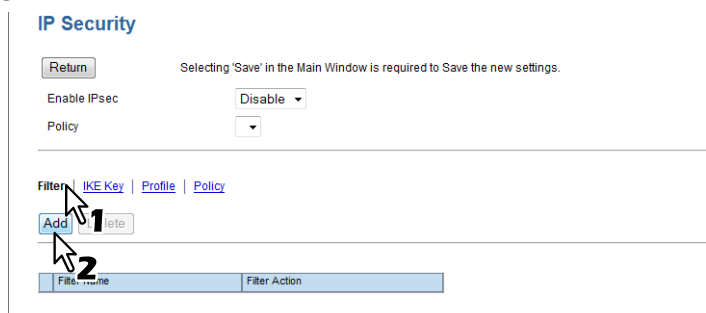
8

□ Registering or modifying policies

Define policies required for IPsec. First create a filter and an IKE key according to your IPsec environment, and then create profiles by combining them. Then select a specific profile among those you have created and make a “policy” from the profile.

Registering or modifying IPsec policies

- 1 Select [Filter] on the IPsec menu, and then click [Add]. To modify a filter already registered, click the link for the desired filter name in the list.



The Add Filter / Modify Filter page is displayed.

2 Select the items below, and then click [OK].

Filter Name — Enter the filter name. You can enter up to 63 alphanumeric characters and symbols other than #, %, &, +, ; (semicolon) and , (comma).

Internet Protocol Version — Selects the IP version for the IP security function.

- **IPv4** — Select this to use IPsec under the IPv4 environment.
- **IPv6** — Select this to use IPsec under the IPv6 environment.

Source Address — The IP address of this equipment is automatically set for this item as a sender address for communication to which filtering is applied. [My IP Address] is displayed in this box. This item is not changeable.

Destination Address — Sets a communication address to which the filter is applied.

- **Specific IP Address** — Sets a specific IP address. Enter the IP address in the address entry box.
- **Subnet/Prefix** — Sets the destination with its IP address and subnet mask. Enter the IP address and the prefix of the subnet mask directly in the address entry box.
- **FQDN** — Sets FQDN for the destination. Enter FQDN in the address entry box.
- **Any IP Address** — Sets the desired IP address.

Protocol Type — Selects a protocol to be used for the filter.

- **Any** — Sets the desired protocol.
- **TCP** — Select this to use TCP only.
- **UDP** — Select this to use UDP only.
- **ICMP** — Select this to use ICMP only.

Source Port — Sets the port number of the sender. This setting is available only if you selected TCP or UDP in the protocol type setting.

- **Any** — Sets the desired source port.
- **Port Number** — Sets the port number of the sender. Key in the port number in the port number entry box.

Destination Port — Sets the port number of the destination. This setting is available only if you selected TCP or UDP in the protocol type setting.

- **Any** — Sets the desired destination port.
- **Port Number** — Sets the port number of the destination. Key in the port number in the port number entry box.

Filter Action — Sets the operation of the filter.

- **Permit** — Select this to permit access from the specified destination.
- **Block** — Select this to block access from the specified destination.
- **Negotiate Security** — IPsec communication is performed with the specified destination. When this item is set, you must select the security protocol type to be used from the following:
 - **ESP** — Select this to use ESP (Encapsulating Security Payload).
 - **AH** — Select this to use AH (Authentication Header).

The Add Filter / Modify Filter page is closed and the filter newly created in the list is registered.

Tips

- The entered content will be deleted when you click [Reset].
- Up to 60 filters can be created.

Note

The normal filtering settings are given priority over IP security filtering.

3 Select [IKE Key] on the IPsec menu, and then click [Add]. To modify an IKE key setting already registered, click the link for the desired key name on the list.

IP Security

[Return](#) Selecting 'Save' in the Main Window is required to Save the new settings.

Enable IPsec Disable

Policy

[Filter](#) | [IKE Key](#) | [Profile](#) | [Policy](#)

[Add](#) [Delete](#)

Key Name	IKE Type

The Add IKE / Modify IKE page is displayed.

4 Select the items below, and then click [OK].

Add IKE

[OK](#) [Cancel](#) [Reset](#) Selecting 'Save' in the Main Window is required to Save the new settings.

IKE Name

IKE Type

IKE Version

☒ IKEv1(Main Mode) [Note: This selection will be applicable for all IKEv1 settings]

Authentication Method

☒ Certificate

☐ Preshared Key

☐ IKEv2

Authentication Method

☐ Certificate

☐ Preshared Key

Local ID IP Address

Remote ID IP Address

Session Key Settings

Generate a new key after /Seconds ☒ Enable PFS

IKE Transforms

Integrity

☒ SHA1 ☐ MD5

Encryption

☐ AES-256-CBC ☐ AES-192-CBC ☒ AES-128-CBC ☒ 3DES-CBC ☐ DES-CBC

Diffie-Hellman algorithm MODP 1024 (Group 2)

IKE Key Name — Enter IKE key name. You can enter up to 63 alphanumeric characters and symbols other than #, %, &, +, ; (semicolon) and , (comma).

IKE Type:

IKEv1 (Main Mode) — Select this to use IKEv1.

- **Certificate** — Select this to use an electronic certificate. To select this, IPsec certificate must be installed in this equipment in advance. For details, see the following page:
[P.326 "Installing IPsec certificate"](#)
- **Preshared Key** — Select this to perform authentication by sharing key information with the recipient of the communication in advance. Enter key information to be shared in the entry box. You can enter up to 128 alphanumeric characters and symbols other than ", &, <, \, ` (back quote), {, }, = and a space.

Note

If you register more than one Preshared Key for IKEv1, only the one that you registered last will be valid.

IKEv2 — Select this to use IKEv2.

- **Certificate** — Select this to use an electronic certificate. To select this, IPsec certificate must be installed in this equipment in advance. For details, see the following page:
[P.326 “Installing IPsec certificate”](#)
- **Preshared Key** — Select this to perform authentication by sharing key information with the recipient of the communication in advance. Enter key information to be shared in the entry box. You can enter up to 128 alphanumeric characters and symbols other than ", &, <, \, ` (back quote), {, }, = and a space.
 - **Local ID**—Select among IP address, FQDN, Email and Key-ID. If Key-ID is selected, enter a value corresponding to Key-ID. You can enter up to 128 alphanumeric characters and symbols other than ", &, <, \, ` (back quote), {, }, = and a space.
 - **Remote ID**—Select among IP address, FQDN, Email and Key-ID. When you selected FQDN, Email or Key-ID, enter a value corresponding to the item you selected. You can enter up to 128 alphanumeric characters and symbols other than ", &, <, \, ` (back quote), {, }, = and a space.

Session Key Settings:

Generate a new key after [] / Seconds — Enter an interval in seconds for regenerating key information of IPsec communication. Set the interval period for regenerating key information for IPsec communication from 60 seconds to 604,800 seconds (7 days).

Enable PFS — Select this check box to use PFS (Perfect Forward Secrecy) in IKE.

IKE Transforms:

Integrity — Selects the authentication algorithm to be used in IKE.

- **SHA1** — Select this to use SHA1.
- **MD5** — Select this to use MD5.

Encryption — Selects the encryption algorithm to be used in IKE.

- **AES-256-CBC** — Select this to use AES-CBC (256 bits).
- **AES-192-CBC** — Select this to use AES-CBC (192 bits).
- **AES-128-CBC** — Select this to use AES-CBC (128 bits).
- **3DES-CBC** — Select this to use 3DES-CBC.
- **DES-CBC** — Select this to use DES-CBC.

Diffie-Hellman algorithm — Selects the Diffie-Hellman group to be used in IKE.

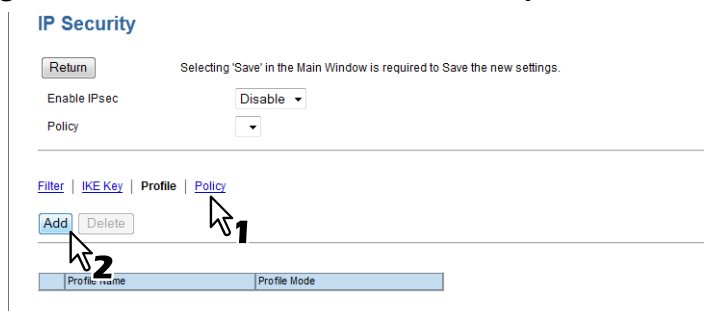
- **MODP 768 (Group 1)** — Select this to use the MODP group in 768 bits.
- **MODP 1024 (Group 2)** — Select this to use the MODP group in 1024 bits.
- **MODP 2048 (Group 14)** — Select this to use the MODP group in 2048 bits.

The Add IKE / Modify IKE page is closed and a key newly created in the list is registered.

Tips

- The entered contents will be deleted when you click [Reset].
- Up to 30 IKE keys can be created.

5 Select [Profile] on the IPsec menu, and then click [Add]. To modify a profile already registered, click the link for the desired profile name on the list.



The Add Profile / Modify Profile page is displayed.

6 Select the items below, and then click [OK].

Add Profile

OK Cancel Reset Selecting 'Save' in the Main Window is required to Save the new settings.

Profile Name:

Tunnel Settings

Tunnel mode: No

IPv4/IPv6 Address:

Key Selection

Key: 001(IKEv1)

Proposals

ESP Transforms

Integrity: ☒ SHA1 ☐ MD5

Encryption: ☐ AES-256-CBC ☐ AES-192-CBC ☒ AES-128-CBC ☒ 3DES-CBC ☐ DES-CBC ☐ None

☐ IPCOMP Transform

AH Transforms

Integrity: ☒ SHA1 ☐ MD5

Session Key Settings

Generate a new key after: 3600 /Seconds

Generate a new key after: 100000 /KBytes

IP Filter

Move Up Move Down

Move	Filter Name	Filter Action	Destination Address
☐	001	Negotiate Security	Any IP Address

Profile Name — Enter the profile name. You can enter up to 63 alphanumeric characters and symbols other than #, %, &, +, ; (semicolon) and , (comma).

Tunnel Settings:

Tunnel mode — Selects whether to use the tunnel mode for IPsec communication or not.

- **Yes** — Select this to use the tunnel mode.
- **No** — Select this not to use the tunnel mode. (The transport mode will be used instead.)

IPv4/IPv6 Address — Enter the gateway IP address for encrypting or decrypting data in the tunnel mode.

Key Selection:

Key — Selects an IKE key to be applied to a profile. IKE keys already registered in this equipment are displayed.

Proposals:

ESP Transforms - Sets the transform to be applied to ESP.

- **Integrity** — Selects the authentication algorithm to be used in ESP.
 - **SHA1** — Select this to use SHA1.
 - **MD5** — Select this to use MD5.
- **Encryption** — Selects the encryption algorithm to be used in ESP.
 - **AES-256-CBC** — Select this to use AES-CBC (256 bits).
 - **AES-192-CBC** — Select this to use AES-CBC (192 bits).
 - **AES-128-CBC** — Select this to use AES-CBC (128 bits).
 - **3DES-CBC** — Select this to use 3DES-CBC.
 - **DES-CBC** — Select this to use DES-CBC.
 - **None** — Select this not to perform data encryption.

AH Transforms — Sets the transform to be applied to AH.

- **Integrity** — Selects the authentication algorithm to be used in AH.
 - **SHA1** — Select this to use SHA1.
 - **MD5** — Select this to use MD5.

Session Key Settings — Sets the session key to be used in IPsec communication.

- **Session Key Settings** — Sets an interval for regenerating the session key. The interval can be set in time or the amount of data. Select the desired check box and then key in the value in the entry box.
 - **Generate a new key after [] / Seconds** — Set an interval in time (seconds) for regenerating key information from 180 seconds to 86,400 seconds (24 hours).
 - **Generate a new key after [] / KBytes** — Set an interval in the amount of data (kilobytes) for regenerating key information from 20,480 KB to 214,783,647 KB.

IPCOMP Transform —Select this to use IPCOMP Transform.

IP Filter:

IP Filter — Filter settings already registered in this equipment are displayed in a list. Select the check box for the filter to be applied to the profile. If more than one filter is registered, you can change their order in the list. Click [Move] for the desired filter, and then click [Move Up] or [Move Down] to move the filter.

The Add Profile / Modify Profile page is closed and the profile newly created in the list is registered.

Tip

Up to 30 profiles can be created.

7 Select [Policy] on the IPsec menu, and then click [Add]. To modify a policy already registered, click the link for the desired policy name on the list.

The screenshot shows the 'IP Security' configuration page. At the top, there are tabs for 'Filter', 'IKE Key', 'Profile', and 'Policy'. The 'Policy' tab is selected and highlighted with a red circle and a mouse cursor labeled '1'. Below the tabs, there are buttons for 'Add' and 'Delete'. The 'Add' button is highlighted with a red circle and a mouse cursor labeled '2'. Below these buttons is a table with a header 'Policy Name' and one row with a blank space for input.

The Add Policy / Modify Policy page is displayed.

8 Select the items below, and then click [OK].

The screenshot shows the 'Add Policy' configuration page. At the top, there are buttons for 'OK' and 'Cancel'. Below these buttons is a text input field for 'Policy Name' with the value 'Policy1'. Below this field is a table with a header 'Profile Name' and one row with a checked checkbox and the value 'Profile1'. The 'Policy Name' field and the table are both highlighted with red circles and mouse cursors labeled '2' and '1' respectively.

Policy Name — Enter the policy name. You can enter up to 63 alphanumeric characters and symbols other than #, %, &, +, ; (semicolon) and , (comma).

Profile Name — Profile settings already registered in this equipment are displayed in a list. Select the check box for a profile to be applied to the policy.

The Add Policy / Modify Policy page is closed and a policy newly created in the list is registered.

Tips

- Up to 10 policies can be created.
- You can select a registered policy in [Policy] on the IP Security Setting page.

P.318 "Setup procedure of IP security function"

❑ Deleting policies

You can delete policies no longer needed.

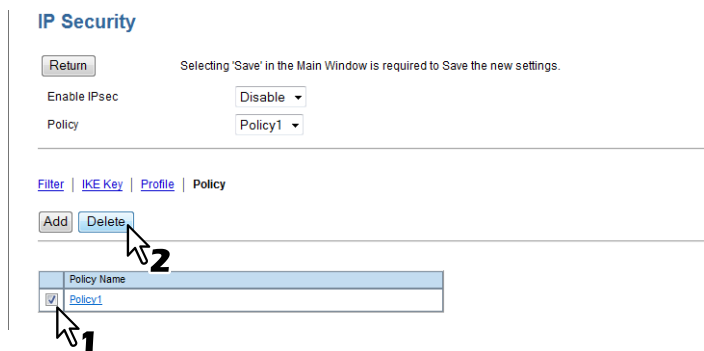
Deleting IPsec policies

Tips

- Filters, IKE keys and profiles can be deleted in the same procedure as that of policies. Apply the procedure below to the item that you want to delete.
- Even if an IPsec policy is deleted, the contents of filters, IKE keys or profiles registered in the IPsec policy will not be deleted. If you want to delete the contents of filters, IKE keys or profiles, you need to do this individually.
- If you want to delete all policies, set [Enable IPsec] to [Disable] and then delete them.

📖 P.318 “Setting up IPsec”

- 1** Select [Policy] on the IPsec menu and select the check box of the desired policy. Then click [Delete].



The selected policy is deleted from this equipment.

■ Installing IPsec certificate

You must install an IPsec certificate when you want to use it for IKE authentication of data encryption communication with this equipment. Install it from an authentication agency or CA server. You can also install it automatically from CA server using SCEP.

Notes

- This equipment supports CA certificate and User certificate that are in the following encoding formats.
 - CA Certificate: DER, BASE64, PKCS#7
 - User Certificate: PKCS#12
- This equipment supports md5RSA and sha1RSA certificate. Make sure to use the certificate in these algorithms.
- When enabling IPsec communication with this equipment, the IPsec Enabler GP-1080 (optional) is required.
- IPsec Certificate setup menus on the TopAccess menu are displayed only when the IPsec function is available. ([Administration] tab > [Setup] menu > [Network] submenu > [Security Service] > [Certificate for IP SEC])
- When you install the User Certificate in this equipment, it is recommended to connect this equipment and a client computer using a crossing cable for ensuring security.

📖 P.326 "Installing an imported IPsec certificate"

📖 P.328 "Deleting an imported IPsec certificate"

📖 P.329 "Installing IPsec certificate automatically"

📖 P.330 "Deleting IPsec certificate installed automatically"

Installing an imported IPsec certificate

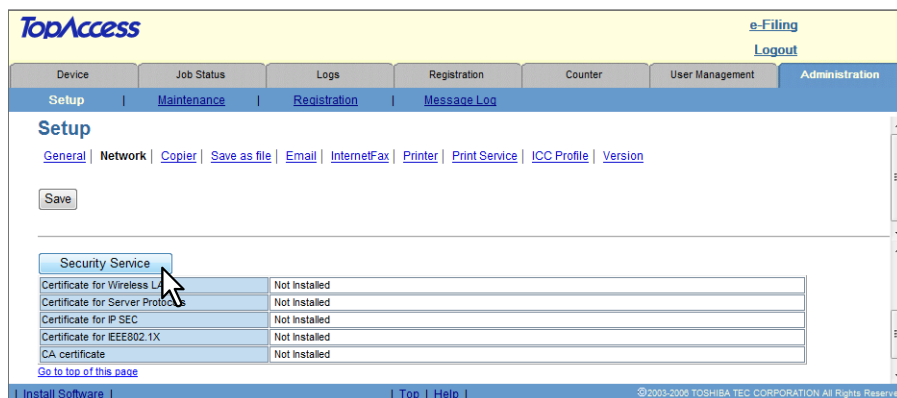
1 Access the TopAccess administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click [Setup], and then [Network].

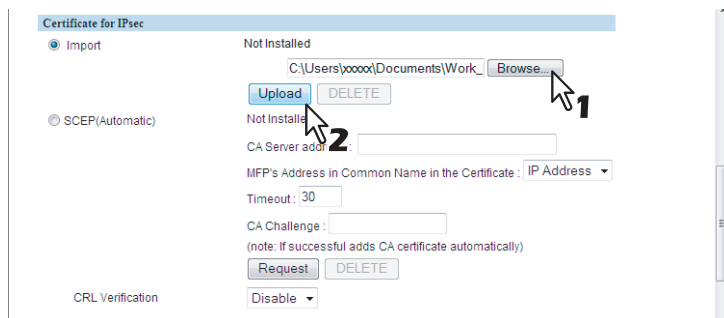
📖 P.118 "Setting up Network settings"

3 Click a link on the [Network] submenu or scroll down the menu and click [Security Service].



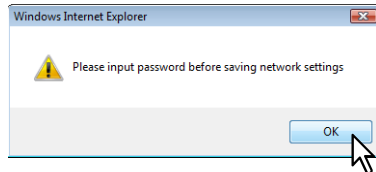
The Security Service page is displayed.

4 Click [Browse] of [Import] in [Certificate for IP SEC] to select an IPsec certificate file, and then click [Upload].



The alert message dialog box appears.

5 Click [OK].



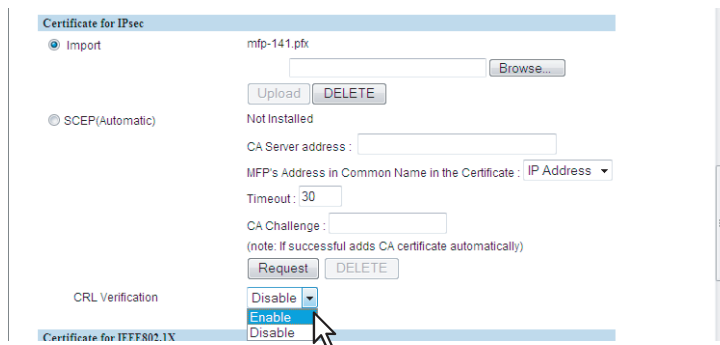
The IPsec certificate is imported.

If you want to enable CRL Verification, go to the next step. If not, go to step 7.

Tip

This alert message shows that you must enter a password on the control panel of this equipment after you installed the IPsec certificate. The certificate cannot be used unless you enter a password.

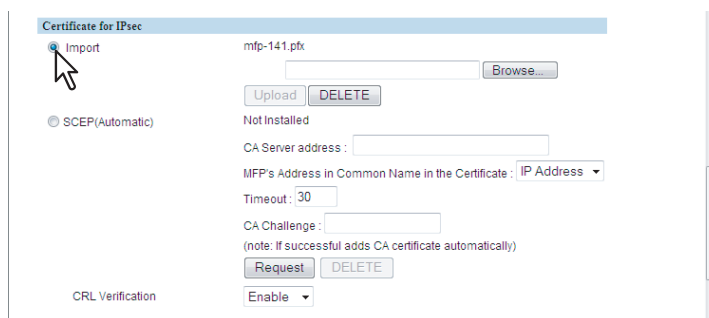
6 Select [Enable] of [CRL Verification].



Notes

- The authentication will fail if the installation of the CRL file failed due to network disconnection or other reasons.
- If you switched the [CRL Verification] setting, save the setting and then turn the power of this equipment OFF and then back ON.

7 Select [Import], and then click [Previous] to close the Security Service page.



8 Click [Save] on the Network submenu page.

9 You must enter a password for IPsec certificate on the control panel of this equipment before setting up the IPsec.

For instructions on how to input the password, refer to the following section in the *MFP Management Guide*.

Chapter 2 "SETTING ITEMS (ADMIN)"

- "Setting Network Functions"
- "Decrypting the user certificate"

10 Then you can enable IPsec for the following settings.

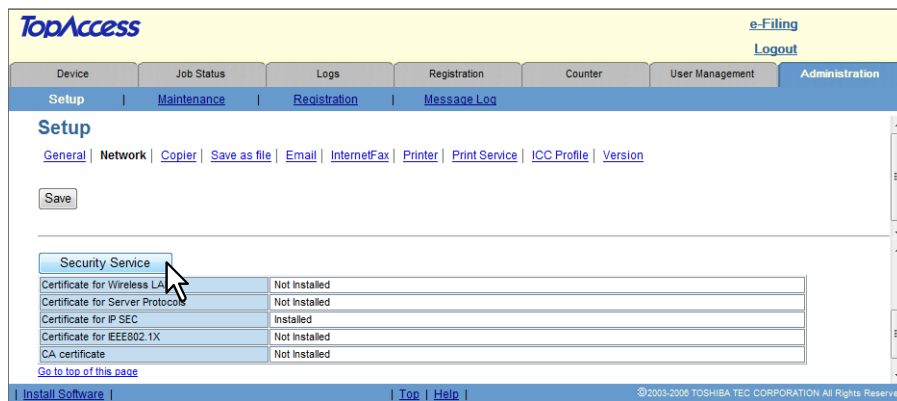
📖 P.317 "Setting up IP Security Function"

Deleting an imported IPsec certificate

Note

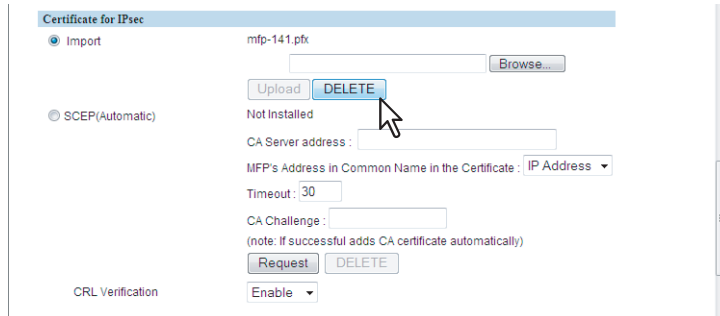
You cannot delete an IPsec certificate being used.

- 1 Access the TopAccess administrator mode.**
 P.106 "Accessing TopAccess Administrator Mode"
- 2 Click [Setup], and then [Network].**
 P.118 "Setting up Network settings"
- 3 Click a link on the [Network] submenu or scroll down the menu and click [Security Service].**



The Security Service page is displayed.

- 4 Click [DELETE] of [Import] in [Certificate for IP SEC].**

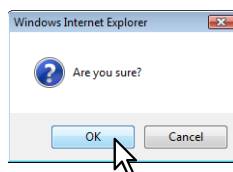


The confirmation dialog box appears.

Note

If the IPsec certificate has not been imported, you cannot delete the IPsec certificate.

- 5 Click [OK].**



The IPsec certificate is deleted.

6 Click [Previous] to close the Security Service page.

7 Click [Save] on the Network submenu page.

Installing IPsec certificate automatically

1 Access the TopAccess administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

2 Click [Setup], and then [Network].

P.118 "Setting up Network settings"

3 Click a link on the [Network] submenu or scroll down the menu and click [Security Service].

The Security Service page is displayed.

4 Enter the items below, and then click [Request] in [Certificate for IP SEC].

CA Server address — Enter the IP address or FQDN of CA server within 128 characters.

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.

Timeout — Enter timeout period for quitting communication when no response is received from CA server.

CA Challenge — Enter the CA challenge.

Notes

- If FQDN is used in [CA Server address], you need to configure DNS server and enable DNS settings.
- If [FQDN] is selected in [MFP's Address in Common Name in the Certificate], the IP address of this equipment must be registered into DNS server.

A server certificate is installed.

If you want to enable CRL Verification, go to the next step. If not, go to step 6.

5 Select [Enable] of [CRL Verification].

The screenshot shows the 'Certificate for IPsec' configuration page. The 'SCEP(Automatic)' option is selected. The 'CRL Verification' dropdown menu is open, showing 'Disable', 'Enable', and 'Disable' options. A mouse cursor is pointing at the 'Enable' option.

Notes

- The authentication will fail if the installation of the CRL file failed due to network disconnection or other reasons.
- If you switched the [CRL Verification] setting, save the setting and then turn the power of this equipment OFF and then back ON.

6 Select [SCEP(Automatic)] in [Certificate for IP SEC], and then click [Previous] to close the Security Service page.

The screenshot shows the 'Certificate for IPsec' configuration page. The 'SCEP(Automatic)' option is selected. The 'CRL Verification' dropdown menu is set to 'Enable'.

Note

A CA certificate is installed automatically as well as an IPsec certificate. If a CA certificate is already installed, delete the existing one by clicking [DELETE] of SCEP in [Certificate for IP SEC]. Then click [Request] to install a new CA certificate.

7 Click [Save] on the Network submenu page.

8 Then you can enable IPsec for the following settings.

📖 P.317 "Setting up IP Security Function"

Deleting IPsec certificate installed automatically

Note

You cannot delete an IPsec certificate being used.

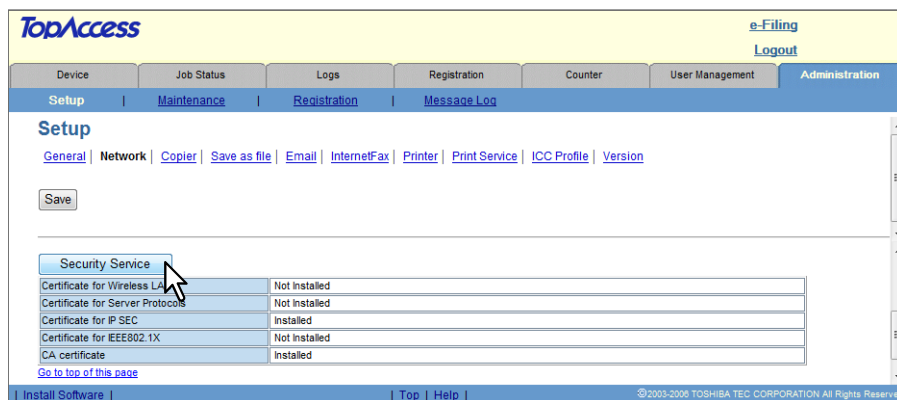
1 Access the TopAccess administrator mode.

📖 P.106 "Accessing TopAccess Administrator Mode"

2 Click [Setup], and then [Network].

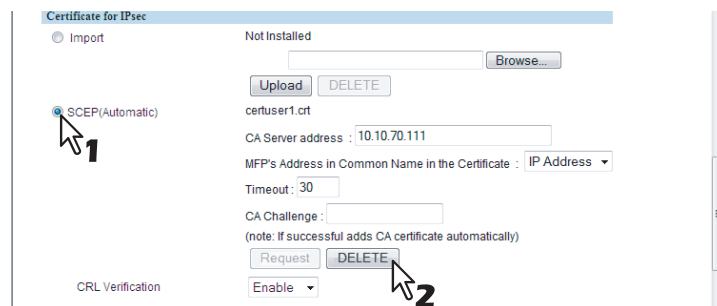
📖 P.118 "Setting up Network settings"

3 Click a link on the [Network] submenu or scroll down the menu and click [Security Service].



The Security Service page is displayed.

4 Select [SCEP(Automatic)] in [Certificate for IP SEC], and then click [DELETE].

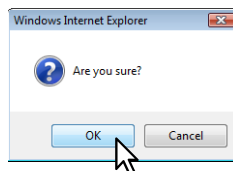


The confirmation dialog box appears.

Notes

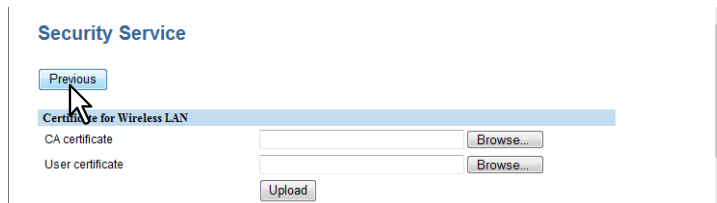
- A CA certificate already installed automatically will be deleted as well as the server certificate.
- Deleting is disabled when no server certificate has been installed automatically.

5 Click [OK].



The IPsec certificate is deleted.

6 Click [Previous] to close the Security Service page.



7 Click [Save] on the Network submenu page.

■ Flushing out IPsec sessions

If the keys for IPsec communication are leaked out or any security violation occurs, you can manually delete (flush) the current session with a flush connection function and start a new session. When you want to delete the information of SAD (Security Association Database) for any reason, you can do it in the same way.

Flushing out IPsec sessions

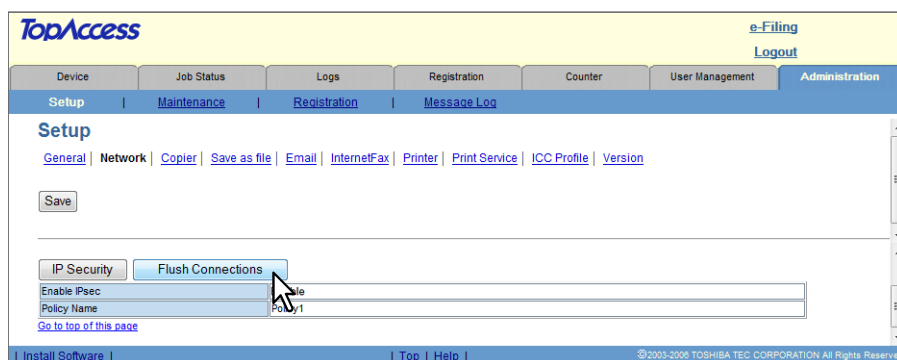
1 Access the TopAccess administrator mode.

P.106 "Accessing TopAccess Administrator Mode"

2 Click [Setup], and then [Network].

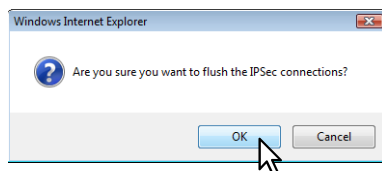
P.118 "Setting up Network settings"

3 Click a link on the [Network] submenu or scroll down the menu and click [Flush Connections].



The confirmation dialog box appears.

4 Click [OK].



The IPsec session is flushed out. The confirmation dialog box appears after you flush out the session. Click [OK].

Setting up Meta Scan Function

With the Meta Scan function, you can attach the scanned image together with meta data onto an Email and send it to a workflow server using the [Scan to Email] or [Save as file] function of the scanning functions of this equipment.

Meta data must be in an XML format file. When data are scanned, the data corresponding to each field (variable) are stored in an XML format file so that the meta data in an XML format will be attached to an Email. There are “extended fields” which enable the customization of the data that the administrator stored, in addition to the fields for storing the already specified information.

On the Meta Scan settings, you can register, import or export Meta Scan templates (templates exclusively for sending meta data), or importing and deleting of XML format files, and register extended fields.

📖 P.333 “Registering/Editing Meta Scan templates”

📖 P.349 “Maintaining Meta Scan templates”

📖 P.355 “Maintaining XML format files”

Notes

- The Meta Scan Enabler GS-1010 (optional) is required for enabling the Meta Scan function.
- The [Meta Scan] tab menu is displayed on the TopAccess menu only when the Meta Scan function is available.
- Only the administrator can set up the Meta Scan function.

■ Registering/Editing Meta Scan templates

To enable the Meta Scan function, you must register templates exclusive to the Meta Scan function first. You can set agents for [Scan to Email] and [Save as file] in the Meta Scan templates. If you want to include extended fields in meta data, you must register the properties of the extended fields.

Meta Scan templates and the properties of extended fields are managed for each group. You can create up to 100 groups and up to 24 templates per group.

When you create a template or a group for the first time, you should decide how you wish to sort the templates into each group. When you created groups, register necessary templates or extended field properties.

📖 P.333 “Registering Meta Scan template groups”

📖 P.337 “Registering Meta Scan templates”

📖 P.344 “Registering extended field properties”

Tip

Meta Scan template groups, templates and extended field properties are created and managed on the TopAccess menus by the administrator, but the created templates can be used by users by their selecting on the touch panel. For instructions on how to use Meta Scan templates on the touch panel, refer to the **Scanning Guide**.

□ Registering Meta Scan template groups

Before you create templates, you must define Meta Scan template groups to manage these templates. You can sort templates into Meta Scan template groups created for each department, user or purpose.

📖 P.334 “Registering or editing Meta Scan template groups”

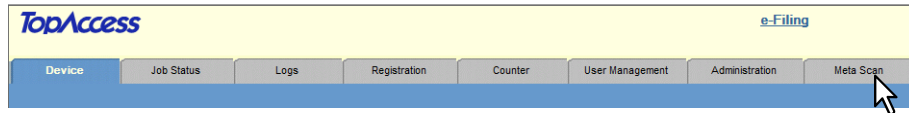
📖 P.336 “Resetting Meta Scan template group information”

Registering or editing Meta Scan template groups

Up to 100 Meta Scan template groups can be created. To create a new group, you must define a group name, an owner, Email notification setting and XML format files to be used.

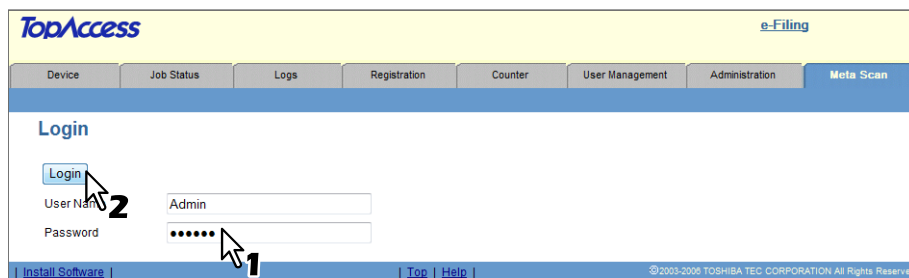
Registering or editing Meta Scan template groups

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

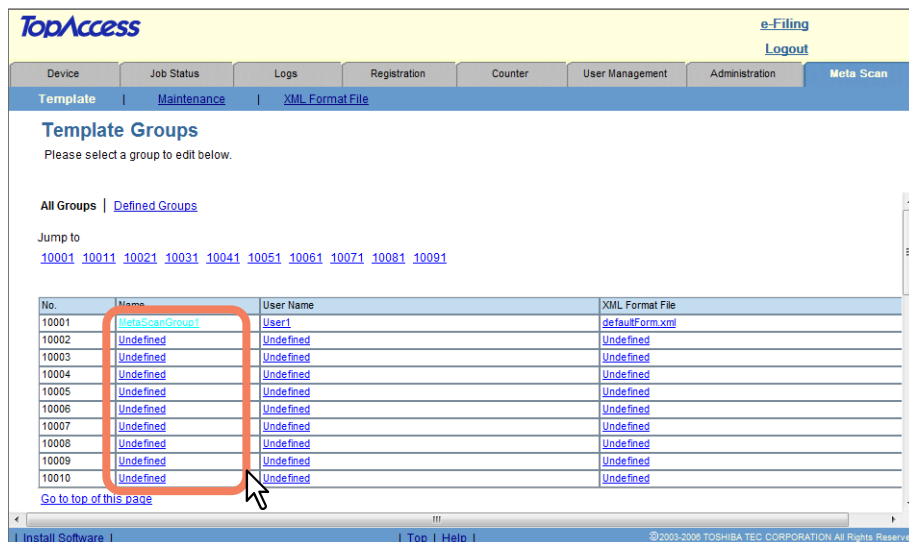


- You cannot change the name in the [User Name] box. It always must be “Admin” to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at “123456” by factory default.

3 Click the [Undefined] name link for an undefined group to create a Meta Scan template group. Click the name link of an defined group to edit the group information.



- If you select an undefined group, the Group Properties page is displayed. Skip to step 5.
- If you select an already defined group, the Meta Scan Template Group list for the selected group appears. Go to the next step.

Tips

- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

4 Click [Edit] to define or edit the group information.

TopAccess e-Filing
Logout

Device Job Status Logs Registration Counter User Management Administration Meta Scan

Template Maintenance XML Format File

Meta Scan Template Template Groups

Group Information

Edit Reset

No.	Name	User Name	XML Format File
10001	MetaScanGroup1	User1	defaultForm.xml

The Group Properties page is displayed.

5 Enter the items below as required.

TopAccess e-Filing
Logout

Device Job Status Logs Registration Counter User Management Administration Meta Scan

Template Maintenance XML Format File

Group Properties

Group Information

No.	Name	User Name	XML Format File
10001	MetaScanGroup1	User1	defaultForm.xml

Save Cancel

*Required

Number 10001

*Name MetaScanGroup1

User Name User1

Notification This email address is used as default recipient each for template.
Email to

XML Format File defaultForm.xml

Number — Key in the number of a Meta Scan template group.

Name — Enter the name of a Meta Scan template group.

User Name — Enter the owner of the Meta Scan template group.

Notification — Enter an Email address be displayed as the default name of the notification mail recipient. You can select whether notification will be sent or not for each template.

XML Format File — Select an XML format file to be used as the format of the meta data attached to the scanned data.

Note

Select an XML format file among the files already registered in this equipment. For instructions on how to register them, see the following page:

📖 P.355 "Importing XML format files"

6 Click [Save] to apply the change.

7 Set extended field properties as required.

📖 P.344 "Registering extended field properties"

Resetting Meta Scan template group information

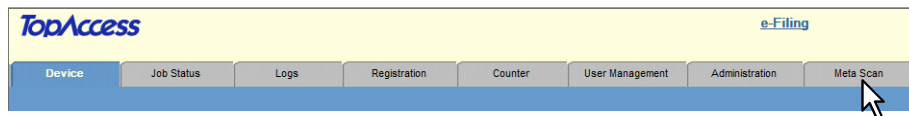
You can reset Meta Scan template groups no longer needed and return them to the undefined groups.

Note

When you reset a Meta Scan template group, all the templates registered in this group will be deleted.

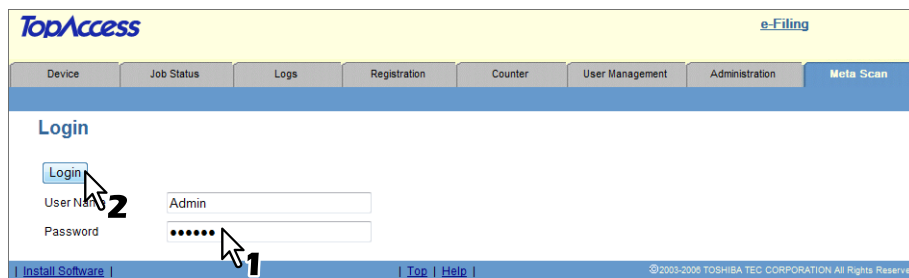
Resetting Meta Scan template group information

1 Click the [Meta Scan] tab.



The Login page is displayed

2 Enter the administrator password in the [Password] box, and then click [Login].

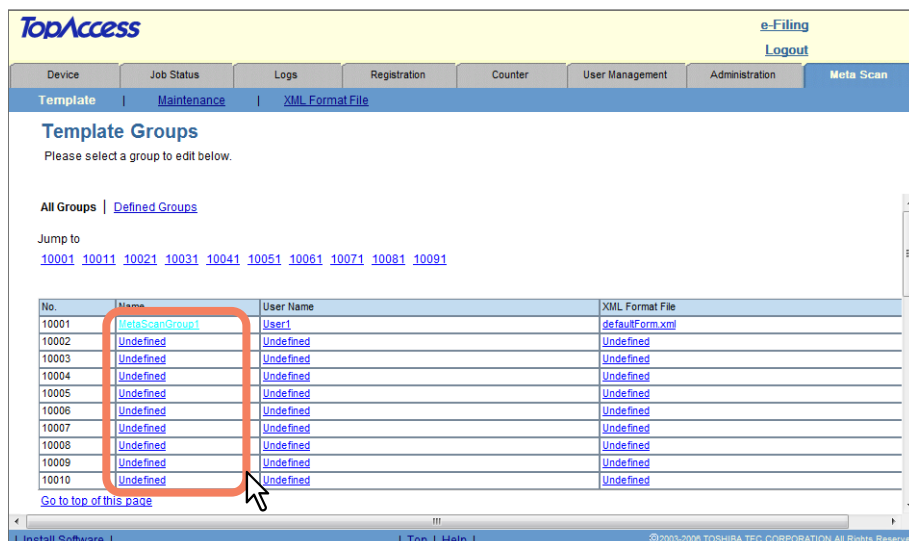


- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click the name link of the defined group whose information is to be reset.

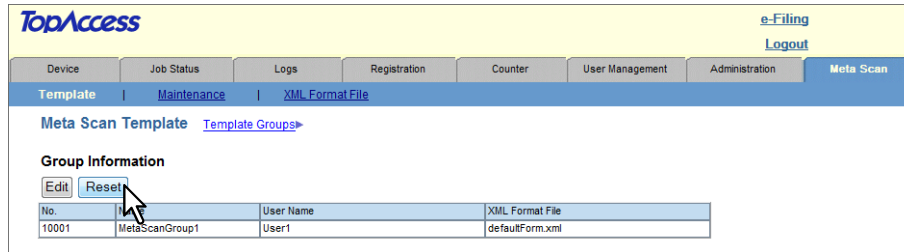


The Meta Scan Template page is displayed.

Tips

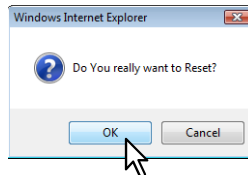
- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

4 Click [Reset].



The confirmation dialog box appears.

5 Click [OK].



The information of the Meta Scan template group is reset and the group will be returned to an undefined one.

□ Registering Meta Scan templates

Up to 24 templates can be created for each Meta Scan template group. You can set names and agents to be displayed on the touch panel of this equipment.

📖 P.337 "Registering or editing Meta Scan templates"

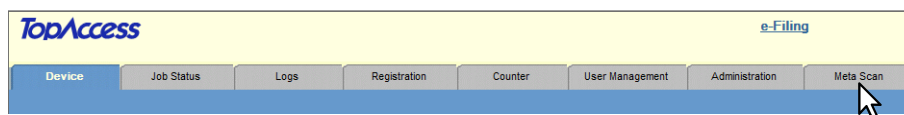
📖 P.342 "Resetting Meta Scan template information"

Registering or editing Meta Scan templates

You can set [Save as file] and [Scan to Email] in the Meta Scan template registration.

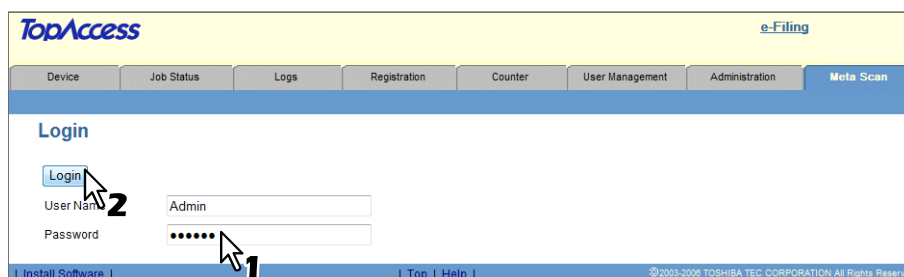
Registering or editing Meta Scan templates

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

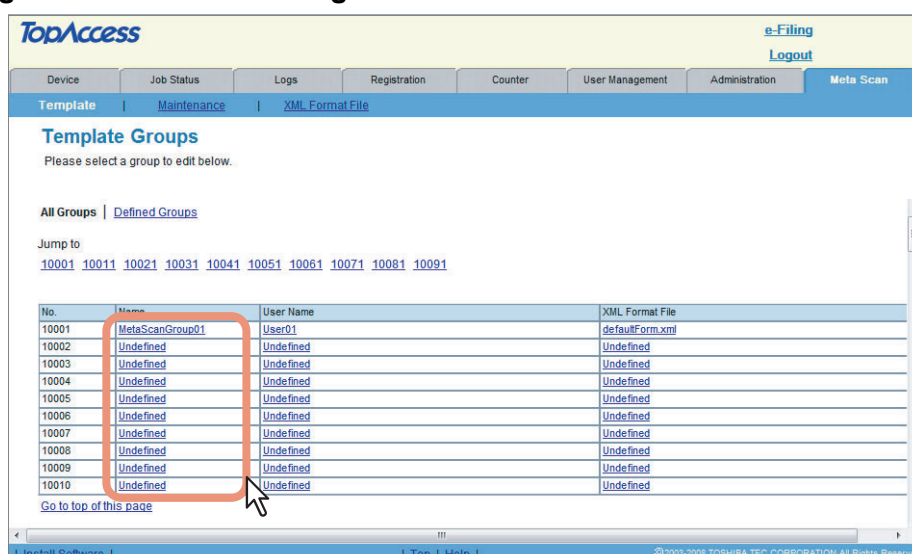


- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click the name link for the defined group to which the Meta Scan template to be registered or edited belongs.

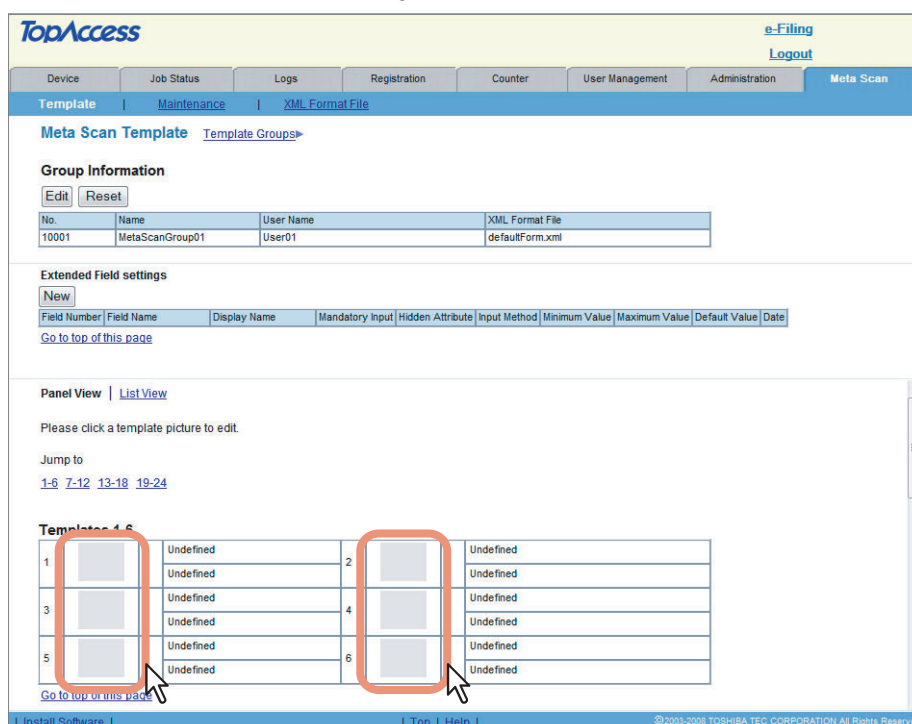


The Meta Scan Template page is displayed.

Tips

- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

4 Click the [Undefined] icon on the template list to create a new template. Click the [Defined] icon to edit an already defined template.



- If you clicked the [Undefined] icon, the Template Properties page to select agents is displayed. Skip to step 6.
- If you select the [Defined] icon, the Template Properties page is displayed. Go to the next step.

Tips

- You can change the template list view by clicking either [Panel View] or [List View].
- If you have a Meta Scan template number, click the [Jump to] link to immediately display the desired template.

5 Click [Edit] to define or edit the template properties.

TopAccess e-Filing Logout

Device | Job Status | Logs | Registration | Counter | User Management | Administration | **Meta Scan**

Template | Maintenance | XML Format File

Template Properties Template Groups> Enhanced Scan Template>

Group Information

No.	Name	User Name
10001	MetaScanGroup01	User01

Template Information

No.	Name	User Name
1	SCAN_TO_FILE&E-MAIL	

Edit Reset Template

Panel SCAN TO
FILE&E-MAIL

Notification

Automatic Start Disable

Agent Email & Save as file

Scanner OFF, Single
Black, 200dpi, Text, Auto, Auto, 0, 0, 0, 0, 0, 0, 0, 0, OFF, OFF

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

The Template Properties page is displayed.

6 Select the desired agent and click [Select Agent].

TopAccess e-Filing Logout

Device | Job Status | Logs | Registration | Counter | User Management | Administration | **Meta Scan**

Template | Maintenance | XML Format File

Template Properties Template Groups> Enhanced Scan Template>

Save Cancel

Select Agent

☐ Scan to Email
☐ Scan to File

Install Software | Top | Help | ©2003-2008 TOSHIBA TEC CORPORATION All Rights Reserved

Select either [Scan to Email] or [Scan to File]. You can also combine 2 agents for them.

7 Click each button displayed on the page to specify or edit the associated template properties

[Panel Setting] — Click this to specify the icon settings for the template.

P.341 “Panel setting (Meta Scan template)”

Panel Setting	
Picture	
Caption1	SCAN TO
Caption2	FILE&E-MAIL
User Name	
Automatic Start	Disable
Notification	

[Destination Setting] — Click this to specify the document's destination. This can be set only when you create a [Scan to Email] agent.

P.341 “Destination setting (Meta Scan template)”

To: Destination Setting	
To: Destination	

Cc: Destination Setting	
Cc: Destination	

Tip

When [To/Bcc] is selected for the [Address Specifying Method] setting, [To: Destination] and [Bcc: Destination] are displayed.

When the setting above is changed from [To/Bcc] to [To/Cc], an e-mail address entered in [Bcc: Destination] will be treated as Cc destination. When the setting is changed from [To/Cc] to [To/Bcc], an e-mail address entered in [Cc: Destination] will be treated as Bcc destination.

P.184 “Setting up Email Setting”

To: Destination Setting	
To: Destination	

Bcc: Destination Setting	
Bcc: Destination	

[Email Setting] — Click this to specify how the document will be sent. This can be set only when you create a [Scan to Email] agent.

P.341 “Email setting (Meta Scan template)”

Email Setting	
Subject	Scanned from (Device Name){(Template Name)}(Date)(Time)
From Address	
From Name	
Body	
File Format	PDF (Multi)
Encryption	Disable
File Name	DocMMDDYY(MMDDYY is a date)
Fragment Message Size	No Fragmentation

[Save as file Setting] — Click this to specify how the document will be stored in the “FILE_SHARE” folder of this equipment, a network folder or USB media. This can be set only when you create a [Save as file] agent.

P.341 “Save as file setting (Meta Scan template)”

Save as file Setting	
File Format	TIF (Multi)
Encryption	Disable
Destination	\\MFP-05212774\\FILE_SHARE\\
File Name	DocMMDDYY(MMDDYY is a date)

Tip

When the data were scanned using a Meta Scan template to which a Save as file agent is set, a new folder with the same name as that of the Meta Scan template is created in a specified directory. The scanned data and the meta data are stored together in this folder. They are saved with the file name specified in [Format] of [Save as file].

[Scan Setting] — Click this to specify how the document will be scanned.

P.341 “Scan setting (Meta Scan template)”

Scan Setting	
Preview	OFF
Single/2-Sided Scan	Single
Rotation	
Color Mode	Black
Resolution	600dpi
Compression	
Original Mode	Text
Exposure	Auto
Original Size	Auto
Background	0
Contrast	0
Sharpness	0
Saturation	0
RGB Adjustment	Red: 0 Green: 0 Blue: 0
Omit Blank Page	OFF
Outside Erase	OFF

[Extended Field Settings] — Click this to set the default value of extended fields. Set this as required when you use extended fields.

P.342 “Extended field setting (Meta Scan template)”

Extended Field settings	
ExField1	

8 Click **[Save]** after you complete the template properties settings.

The set properties are registered.

8

Panel setting (Meta Scan template)

In the Panel Setting page, you can specify how icons for templates are displayed in the touch panel and how you set up notification Emails for templates. The setup procedure is the same as that of the registration of private templates.

P.51 “Panel Setting (Private template)”

Destination setting (Meta Scan template)

In the Recipient List page, you can specify the Email addresses to which the [Scan to Email] document will be sent. When you specify destinations, you can enter the Email address of the destination manually or select the user name or group name in the address book. Or you can select it by searching with LDAP service.

The setup procedure is the same as that for the registration of private templates.

P.52 “Destination Setting (Private template)”

Email setting (Meta Scan template)

In the Email Setting page, you can specify the properties of Emails to be sent. The setup procedure is the same as that for the registration of private templates.

P.61 “Email Setting (Private template)”

Save as file setting (Meta Scan template)

In the Save as file Setting page, you can specify the storing method for [Save as file] and a directory in which the file is to be stored. The setup procedure is the same as that for the registration of private templates.

P.63 “Save as file Setting (Private template)”

Tip

When the data were scanned using a Meta Scan template to which a Save as file agent is set, a new folder with the same name as that of the Meta Scan template is created in a specified directory. The scanned data and the meta data are stored together in this folder. They are saved with the file name specified in [Format] of [Save as file].

Scan setting (Meta Scan template)

In the Scan Setting page, you can specify how originals are scanned. The setup procedure is the same as that for the registration of private templates.

P.67 “Scan Setting (Private template)”

Extended field setting (Meta Scan template)

In the Extended Field Properties page, you can enter the default value of each extended field registered in each group. For details, see the following page:

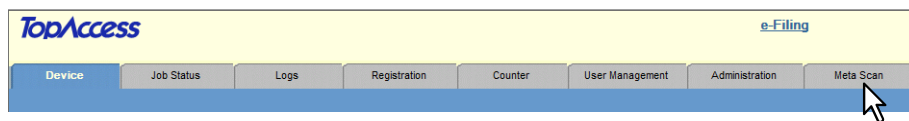
📖 P.344 “Registering or editing extended fields”

Resetting Meta Scan template information

You can reset Meta Scan templates no longer needed and return them to the undefined templates.

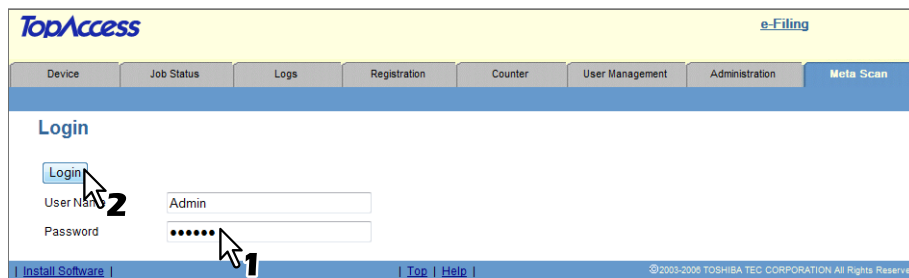
Resetting Meta Scan template information

- 1 Click the [Meta Scan] tab.



The Login page is displayed

- 2 Enter the administrator password in the [Password] box, and then click [Login].

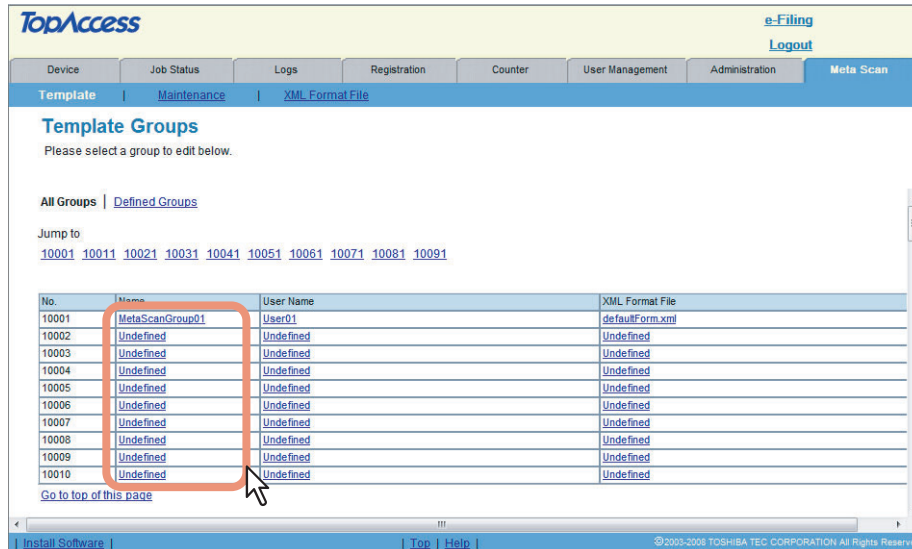


- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at “123456” by factory default.

3 Click the name link of a group to which the desired template belongs.



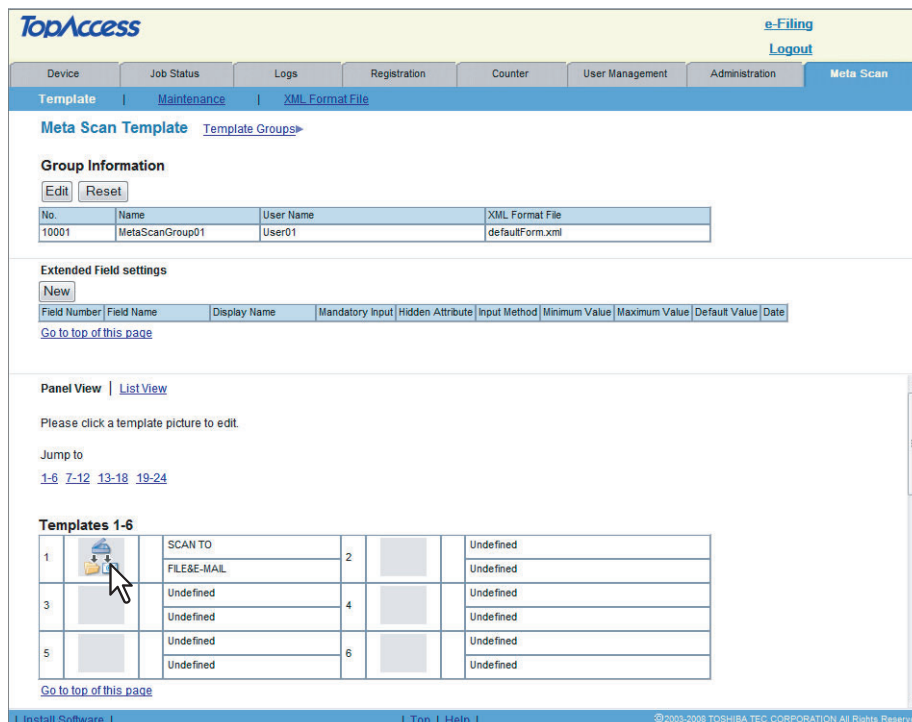
The Meta Scan Template page is displayed.

Tips

- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

8

4 Click the icon of the desired template.



If the templates list is displayed in the list view, click the desired template name.

Tips

- You can change the template list view by clicking either [Panel View] or [List View].
- If you have a Meta Scan template number, click the [Jump to] link to immediately display the desired template.

5 Click [Reset Template].

TopAccess

[e-Filing](#)
[Logout](#)

Device

Job Status

Logs

Registration

Counter

User Management

Administration

Meta Scan

Template

Maintenance

XMI_Format File

Template Properties

[Template Groups](#) > [Enhanced Scan Template](#) >

Group Information

No.	Name	User Name
10001	MetaScanGroup01	User01

Template Information

No.	Name	User Name
1	SCAN_TO_FILE&E-MAIL	

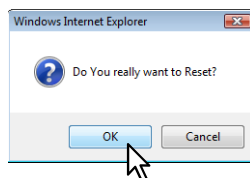
Edit

Reset Template

Panel	 SCAN TO FILE&E-MAIL
Notification	
Automatic Start	Disable
Agent	Email & Save as file
Scanner	A → A OFF, Single, Black, 200dpi, Text, Auto, Auto, 0, 0, 0, 0, (0, 0, 0), OFF, OFF

The confirmation dialog box appears.

6 Click [OK].



The information of the Meta Scan template is reset and the template will be returned to an undefined one.

❑ Registering extended field properties

Extended fields enable the customization of data stored by the administrator, in addition to fields for storing already specified information. The administrator can define the types of extended fields and values to be stored in them.

Extended fields can be created for each Meta Scan template group. Up to 25 extended fields can be created. The created extended fields will be applied to all the templates registered in a group.

 P.344 “Registering or editing extended fields”

 P.347 “Deleting extended field properties”

Registering or editing extended fields

The types of extended fields and values to be stored in them can be defined.

Registering or editing extended fields

1 Click the [Meta Scan] tab.


[e-Filing](#)

[Device](#)
[Job Status](#)
[Logs](#)
[Registration](#)
[Counter](#)
[User Management](#)
[Administration](#)
[Meta Scan](#)

The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click the name link for the defined group to which the Meta Scan template to be registered or edited belongs.

The Meta Scan Template page is displayed.

Tips

- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

4 Click [New] to create a new extended field. Click the name link for the defined field to edit the existing extended field.

The Extended Field Properties page is displayed.

5 Select the items below, and click [OK].

Extended Field Properties

Save Cancel

Field Name

Name

*Display

☐ Mandatory Input ☐ Hidden Attribute

Input Method

☒ Numerical ☐ Decimal ☐ Text ☐ List ☐ Address ☐ Password ☐ Date

List Items

Move Up Move Down Delete

Name

Value Add

Minimum Length

Maximum Length

*Minimum Value

*Maximum Value

Default Value Delete

Password

Date

Year Month Date

*Required

Field Number — Displays the field number of the extended field setting selected only when you edit the existing extended fields. The field number will not be displayed when you create a new extended field. A field number is automatically assigned when you register a new extended field into this equipment.

Note

A field number displayed on the extended field setting list and that of an extended field described in an XML format file are combined together. For example, information defined to the field number “1” will be stored in the extended field “1” (<!--\$VALUE1\$-->) of an XML format file. Information will not be stored if an extended field having the same number as the field number is not described in the XML format file.

Field Name — Displays the field name of the extended field.

Note

A string of characters entered in this field will be stored in a variable corresponding to each field number. (e.g. <!--\$FIELDNAME1\$-->, <!--\$FIELDNAME2\$-->)

Display — Sets how to display extended fields on the touch panel.

- **Name** — Enter the name of an extended field to be displayed on the touch panel within 256 characters.
- **Mandatory Input** — Select this check box when you create an extended field which requires mandatory input of information.
- **Hidden Attribute** — Select this check box when you create an extended field not to be displayed on the touch panel.

Input Method — Selects the types of an extended field.

- **Numerical** — Select this to create an extended field to key in integer numbers.
- **Decimal** — Select this to create an extended field to key in decimal numbers
- **Text** — Select this to create an extended field to enter a character string.
- **List** — Select this to create an extended field to select values from a list.
- **Address** — Select this to create an extended field to enter an address.
- **Password** — Select this to create an extended field to enter a password.
- **Date** — Select this to create an extended field to enter a date.

Tip

The types of the extended fields selected in [Input Method] above and setting items are shown below. (*) is displayed before a mandatory setting item.

Input Method (Types of extended fields)	Mandatory setting items	Optional setting items
Numerical	[Maximum Value], [Minimum Value] * Acceptable value: -999,999,999,999 to 999,999,999,999	[Default Value]
Decimal	[Maximum Value], [Minimum Value] * Acceptable value: -999,999,999,999.999999 to 999,999,999,999.999999	[Default Value]
Text	[Maximum Length], [Minimum Length] * Acceptable value: 0 to 128	[Default Value]
List	[List Items]	[Default Value] * Select among the registered setting items.
Address	None	[Default Value]
Password	None	[Password]
Date	None	[Date]

List Items — Sets the items to select in the extended fields of the list. The registered list items are displayed in [List Items]. When you register items in the extended field, enter in [Name] and [Value], and then click [Add]. If you click [Move Up], the selected item moves up in the list. If you click [Move Down], it moves down. When you delete items no longer needed in the extended field, select the desired ones and click [Delete].

- **Name** — Enter the name of the item.
- **Value** — Enter digits or text to be applied for the selected item.

Notes

- The maximum total number of characters that can be displayed in a List Items extended field is 127.
- Semicolon cannot be entered in [Name] and [Value].

Tip

[Move Up] and [Move Down] are displayed only on the TopAccess menu of the e-STUDIO455 Series and the e-STUDIO855 Series.

Minimum Length — Sets the minimum number of characters that can be entered in an extended field.

Maximum Length — Sets the maximum number of characters that can be entered in an extended field.

Minimum Value — Sets the minimum value that can be entered in an extended field.

Maximum Value — Sets the maximum value that can be entered in an extended field.

Default Value — Sets a default value to be set in an extended field.

Password — Sets a default value to be set in the password extended field.

Date — Sets a default value to be set in the date extended field.

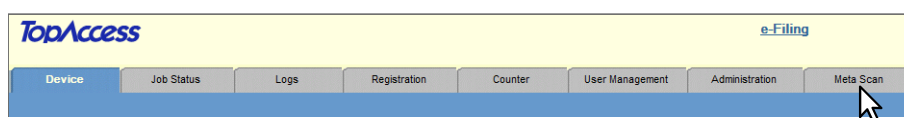
The Extended Field Properties page is closed and the extended field newly created in the list is registered.

Deleting extended field properties

You can delete extended field properties no longer needed.

Deleting extended field properties

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click the name link for a group to which an extended field to be deleted belongs.

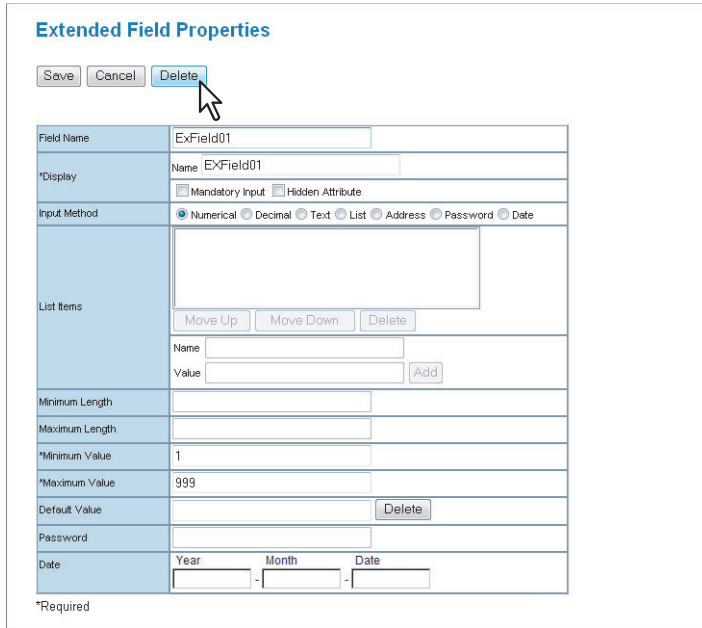
The Meta Scan Template page is displayed.

Tips

- The page displays all the 100 Meta Scan template groups in the initial page view. Click the [Defined Groups] link to display only the defined Meta Scan template groups.
- If you have a Meta Scan template group number, click the [Jump to] link for the desired group.

4 Click the name link of the desired extended field.

5 Click [Delete].



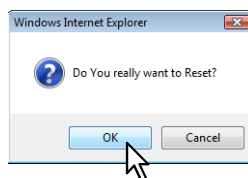
The 'Extended Field Properties' dialog box is shown. At the top, there are three buttons: 'Save', 'Cancel', and 'Delete'. A mouse cursor is pointing at the 'Delete' button. Below the buttons, the dialog contains several fields and sections:

- Field Name:** ExField01
- Name:** EXField01
- *Display:** ☐ Mandatory Input ☐ Hidden Attribute
- Input Method:** ☒ Numerical ☐ Decimal ☐ Text ☐ List ☐ Address ☐ Password ☐ Date
- List Items:** A large empty text area with buttons 'Move Up', 'Move Down', and 'Delete' below it.
- Name:** **Value:** **Add**
- Minimum Length:**
- Maximum Length:**
- *Minimum Value:** 1
- *Maximum Value:** 999
- Default Value:** **Delete**
- Password:**
- Date:** Year - Month - Date

*Required

The confirmation dialog box appears.

6 Click [OK].



The extended field is deleted.

Note

A field number displayed on the extended field setting list and an extended field number described in an XML format file are combined together for use. For example, information defined to the field number "1" will be stored in the extended field "1" (<!--\$VALUE1\$-->) of an XML format file. Information will not be stored if an extended field having the same number as the field number is not described in the XML format file.

■ Maintaining Meta Scan templates

You can import or export Meta Scan templates, Meta Scan template groups or extended field properties in an XML format.

📖 P.349 "Exporting Meta Scan templates"

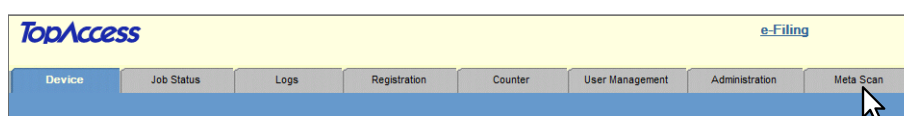
📖 P.351 "Importing Meta Scan templates"

❑ Exporting Meta Scan templates

The administrator can export Meta Scan templates registered in this equipment in an XML format.

Exporting Meta Scan templates and extended field properties

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click [Maintenance].

The Maintenance page is displayed.

4 Click [Create New File] in the Template Exporting area.

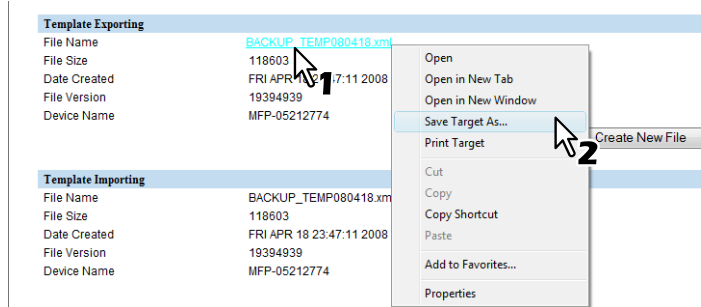
The information of exported files is displayed.

Tip

If you have created, exported or imported a new template data file in the past, the link and data of the file created in the latest operation are displayed in the Template Exporting area. When you click the link, you can save the file created in the latest operation.

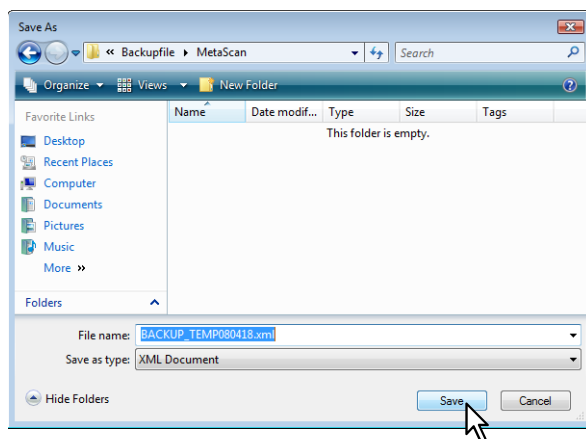
If you want to delete all these data, click [Restore] on the right bottom of the [Maintenance] menu.

5 Right-click the link for the [File Name], and then select [Save Target As].



The [Save As] dialog box appears.

6 Select a directory to which the file is saved, and then click [Save].



The XML file of Meta Scan template data is saved in the selected directory.

□ Importing Meta Scan templates

You can import Meta Scan template data or template data that are created in an XML format by the administrator from other equipment of the e-STUDIO6530C Series, e-STUDIO4520C Series, e-STUDIO855 Series or e-STUDIO455 Series. There are two methods for importing Meta Scan templates; one is to add the imported template data to the templates already registered in this equipment, and the other is to delete the already registered templates and replace them. Template data to be imported must be XML files in a tag format, complying with the TopAccess Meta Scan template data format. For details, ask the administrator.

Note

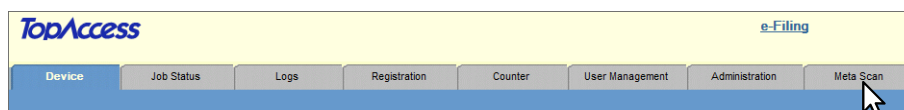
When you import a Meta Scan template using an XML file that is not registered in this equipment, you need to register this XML file in this equipment in advance. If the registration was not done before importing a Meta Scan template, a default XML file will be assigned to this template.

Importing Meta Scan templates and extended fields properties

Note

Before you start importing template data, make sure that there is no private print job, scheduled print job, proof print job or other job in process. If there is any, template data cannot be imported. When the import takes an extremely long time even if there are no such jobs, try again when this equipment has entered the Auto Shut Off mode.

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

3 Click [Maintenance].

The Maintenance page is displayed.

4 Select [Import Method] in the Template Importing area.

Addition — Adds the imported template data to the Meta Scan templates already registered in this equipment.

Overwrite — Deletes all the Meta Scan templates already registered in this equipment and replaces them with the imported template data.

Tip

If you have created, exported or imported a new template data file in the past, the link and data of the file created in the latest operation are displayed in the Template Importing area. When you click the link, you can save the file created in the latest operation.

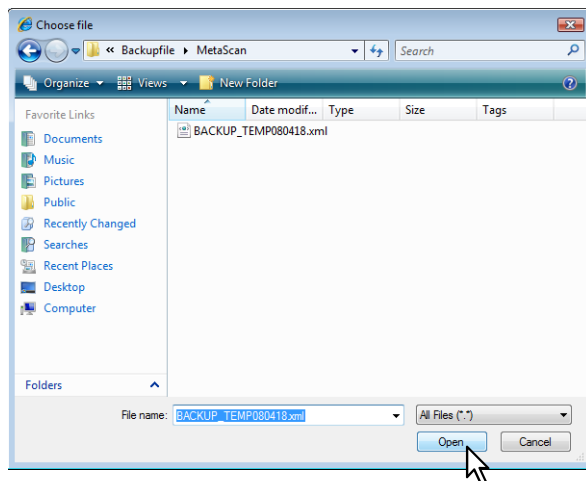
If you want to delete all these data, click [Restore] on the right bottom of the [Maintenance] menu.

5 Click [Browse].

The screenshot shows the TopAccess web interface. The 'Maintenance' tab is selected, and the 'Template Importing' section is active. The 'File Name' field is empty and labeled 'Not Created'. Below the field are buttons for 'Browse...' and 'Upload'. A mouse cursor is pointing at the 'Browse...' button. The 'Import Method' section has radio buttons for 'Addition' and 'Overwrite', with 'Overwrite' selected. There is also a 'Restore' button.

The [Choose File] dialog box appears.

6 Select the XML file that contains the desired template, and click [Open].



7 Click [Upload].

The screenshot shows the TopAccess web interface. At the top, there's a yellow header with 'TopAccess' and links for 'e-Filing' and 'Logout'. Below this is a navigation bar with tabs: Device, Job Status, Logs, Registration, Counter, User Management, Administration, and Meta Scan. The 'Maintenance' tab is selected, and within it, the 'Template' sub-tab is active. The main content area is titled 'Maintenance' and contains a section for 'Import/Export for Templates and Enhanced Settings'. This section has two main parts: 'Template Exporting' and 'Template Importing'. Both sections show fields for File Name, File Size, Date Created, File Version, and Device Name, all with a 'Not Created' status. The 'Template Importing' section also includes an 'Import Method' section with radio buttons for 'Addition' and 'Overwrite' (which is selected). Below this, there's a file path 'C:\Users\yooxoo\Docume' followed by a 'Browse...' button and an 'Upload' button. A mouse cursor is pointing at the 'Upload' button. There is also a 'Restore' button at the bottom right of the form area. The footer contains links for 'Install Software', 'Top', and 'Help', along with a copyright notice for Toshiba TEC Corporation.

The Meta Scan template data are imported into this equipment.

■ Maintaining XML format files

You can import XML format files to be used as a meta data format, or delete the registered XML format files. In the Meta Scan operation, this equipment stores information corresponding to the variable of each field described in the XML format file and attaches these data to an Email as meta data in an XML format.

📖 P.355 “Importing XML format files”

📖 P.357 “Deleting XML format files”

XML files must be in a UTF-8 XML format. For the samples and variables of XML format file, see the following pages:

📖 P.359 “Default XML format file”

📖 P.360 “Variables of XML format files”

Tips

- The name of an XML meta data file attached to the scanned data will be the same as that of the scanned data. If a single-page format (e.g. TIFF (SINGLE)) is selected as a file format for the scanned data, however, the file name of the XML meta data file will differ depending on the setting as follows:
 - When [Save under a subfolder] is selected for [Single Page Data Saving Directory] on the [Save as file] submenu - The name of the XML meta data file will be the same as that of the subfolder.
 - When [Save without creating a subfolder] is selected for [Single Page Data Saving Directory] on the [Save as file] submenu - The name of the XML meta data file will be the file name of the scanned data without a page number.

For the Save as file setting, see the following page:

📖 P.179 “Setting up Single Page Data Saving Directory”

- A variable for XML format files can be used for the file name of meta data in an XML format attached to the scanned data. Enter the desired variable in the file name entry box of [File Name] of [Save as file setting] or [Email setting]. If “TODAY_IS_<!--\$DAY\$-->” is entered, the file name will be “TODAY_IS_XX” (the day that the data were scanned comes at “XX”). Note that a variable of file names “<!--\$FILE\$-->” and file paths “<!--\$PATH\$-->” cannot be entered.

8

□ Importing XML format files

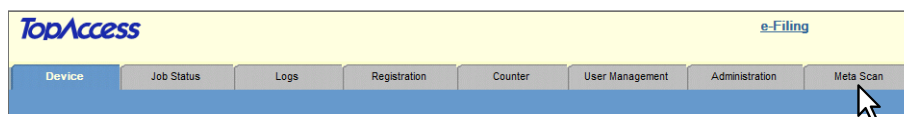
You can import XML format files to be used as a format of meta data attached to the scanned data. Up to 99 XML format files can be imported into this equipment.

Importing XML format files

Note

Before you start importing XML format files, make sure that there is no private print job, scheduled print job, proof print job or other job in process. If there is any, XML format files cannot be imported. When the import takes an extremely long time even if there are no such jobs, try again when this equipment has entered the Auto Shut Off mode.

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

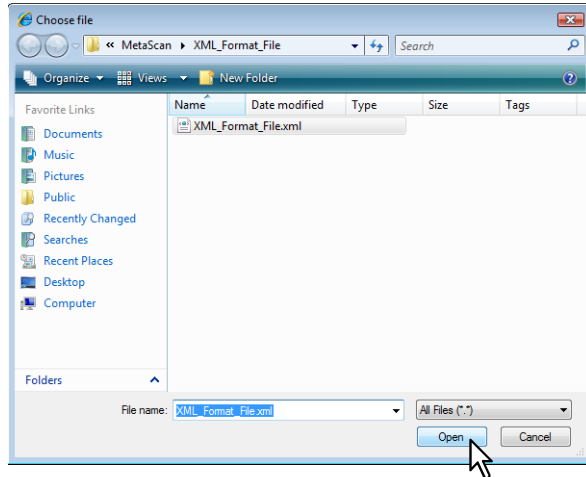
3 Click [XML Format File].

The XML Format File page is displayed.

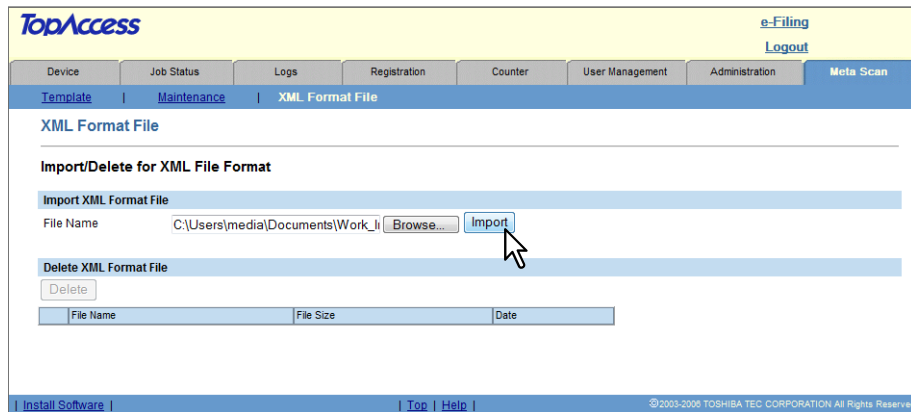
4 Click [Browse] in the Import XML Format File area.

The [Choose File] dialog box appears.

5 Select the desired XML format file, and click [Open].



6 Click [Import].



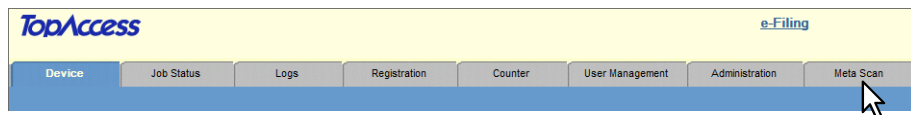
The XML format file is imported into this equipment and the imported file is registered on the list of XML format files.

□ Deleting XML format files

You can delete XML format files no longer needed.

Deleting XML format files

1 Click the [Meta Scan] tab.



The Login page is displayed.

2 Enter the administrator password in the [Password] box, and then click [Login].

- You cannot change the name in the [User Name] box. It always must be "Admin" to log in to TopAccess in the administrator mode.
- The Template Groups page is displayed.

Tip

The administrator password is set at "123456" by factory default.

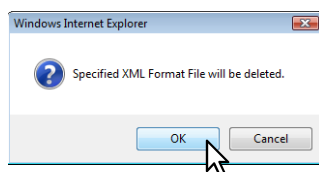
3 Click [XML Format File].

The XML Format File page is displayed.

4 Select the desired XML format file from the list in the Delete XML Format File area, and then click [Delete].

The confirmation dialog box appears.

5 Click [OK].



The XML format file is deleted.

□ Default XML format file

XML format files registered in this equipment by default are shown below. XML format files must be in a UTF-8 XML format. In the Meta Scan operation, this equipment stores information corresponding to the variable of each field described in the XML format file and attaches these data to an Email as meta data in an XML format.

Tip

You can decide the composition of the XML format file or tag names as you desired, according to your system environment. In this case, see the following page for the name of variables ("xxxx" in <!--\$ xxxx \$-->) or data stored in each variable in the Meta Scan operation:

📖 P.360 "Variables of XML format files"

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Sample XML format file version 1.0.0 -->
<mfp_metadata>
  <device_info>
    <ip_address><!--$IP$--></ip_address>
    <host_name><!--$HOST$--></host_name>
    <location><!--$LOCATION$--></location>
    <contact_tel><!--$CONTACTTEL$--></contact_tel>
    <FW_version><!--$FWVER$--></FW_version>
    <manufacture><!--$MANUFACT$--></manufacture>
    <model><!--$MODEL$--></model>
    <serial><!--$SERIAL$--></serial>
    <tempt_file_ver><!--$TEMPVER$--></tempt_file_ver>
  </device_info>
  <scan_info>
    <scanned_date><!--$YEAR$--><!--$MONTH$--><!--$DAY$--></scanned_date>
    <scanned_time><!--$DATE$-->T<!--$TIME$--></scanned_time>
    <color_mode><!--$COLORMODE$--></color_mode>
    <resolution><!--$RESOLUTION$--></resolution>
    <file_format><!--$FILEFORMAT$--></file_format>
    <no_of_files><!--$NUMFILE$--></no_of_files>
    <no_of_pages><!--$PAGES$--></no_of_pages>
    <workflow><!--$WORKFLOW$--></workflow>
  </scan_info>
  <user_info>
    <user_id><!--$USER$--></user_id>
    <dept_code><!--$DEPTCODE$--></dept_code>
    <user_email><!--$MYEMAIL$--></user_email>
  </user_info>
  <user_input>
    <field1 name="<!--$FIELDNAME1$-->"><!--$VALUE1$--></field1>
    <field2 name="<!--$FIELDNAME2$-->"><!--$VALUE2$--></field2>
    <field3 name="<!--$FIELDNAME3$-->"><!--$VALUE3$--></field3>
    <field4 name="<!--$FIELDNAME4$-->"><!--$VALUE4$--></field4>
    <field5 name="<!--$FIELDNAME5$-->"><!--$VALUE5$--></field5>
    <field6 name="<!--$FIELDNAME6$-->"><!--$VALUE6$--></field6>
    <field7 name="<!--$FIELDNAME7$-->"><!--$VALUE7$--></field7>
    <field8 name="<!--$FIELDNAME8$-->"><!--$VALUE8$--></field8>
    <field9 name="<!--$FIELDNAME9$-->"><!--$VALUE9$--></field9>
    <field10 name="<!--$FIELDNAME10$-->"><!--$VALUE10$--></field10>
    <field11 name="<!--$FIELDNAME11$-->"><!--$VALUE11$--></field11>
    <field12 name="<!--$FIELDNAME12$-->"><!--$VALUE12$--></field12>
    <field13 name="<!--$FIELDNAME13$-->"><!--$VALUE13$--></field13>
    <field14 name="<!--$FIELDNAME14$-->"><!--$VALUE14$--></field14>
    <field15 name="<!--$FIELDNAME15$-->"><!--$VALUE15$--></field15>
    <field16 name="<!--$FIELDNAME16$-->"><!--$VALUE16$--></field16>
    <field17 name="<!--$FIELDNAME17$-->"><!--$VALUE17$--></field17>
    <field18 name="<!--$FIELDNAME18$-->"><!--$VALUE18$--></field18>
    <field19 name="<!--$FIELDNAME19$-->"><!--$VALUE19$--></field19>
    <field20 name="<!--$FIELDNAME20$-->"><!--$VALUE20$--></field20>
    <field21 name="<!--$FIELDNAME21$-->"><!--$VALUE21$--></field21>
    <field22 name="<!--$FIELDNAME22$-->"><!--$VALUE22$--></field22>
```

```

    <field23 name="<!--$FIELDNAME23$-->"><!--$VALUE23$--></field23>
    <field24 name="<!--$FIELDNAME24$-->"><!--$VALUE24$--></field24>
    <field25 name="<!--$FIELDNAME25$-->"><!--$VALUE25$--></field25>
  </user_input>
</mfp_metadata>

```

□ Variables of XML format files

Variables that can be defined to XML format files are shown below. Data corresponding to these variables are stored in the Meta Scan operation.

Variable	Data to be stored	Value
<!--\$IP\$-->	IP address	string
<!--\$HOST\$-->	Host name	string
<!--\$LOCATION\$-->	Location	string
<!--\$CONTACT\$-->	Contact information	string
<!--\$CONTACTTEL\$-->	Contact telephone number	string
<!--\$YEAR\$-->	Year	string
<!--\$MONTH\$-->	Month	string
<!--\$DAY\$-->	Day	string
<!--\$TIME\$-->	Time	string
<!--\$USER\$-->	User name in user authentication	string
<!--\$MYEMAIL\$-->	Authenticated user's Email address	string
<!--\$DEPTCODE\$-->	Department code	string
<!--\$WORKFLOW\$-->	Name of workflow process	string
<!--\$FWVER\$-->	Firmware version	string
<!--\$MODEL\$-->	Model name	string
<!--\$SERIAL\$-->	Serial number	string
<!--\$MANUFACT\$-->	Manufacturer name	string
<!--\$TEMPVER\$-->	Template setup file version	string
<!--\$NUMFILE\$-->	The number of image files	string
<!--\$RESOLUTION\$-->	Scan resolution	string
<!--\$PAGES\$-->	Scanned pages	string
<!--\$FILEFORMAT\$-->	File format	MultipleTIFF singleTIFF MultiplePDF singlePDF MultipleSLIMPDF singleSLIMPDF MultipleXPS singleXPS JPEG
<!--\$COLORMODE\$-->	Color mode	BLACK GRAY FULLCOLOR AUTOCOLOR
<!--\$VALUEn\$-->	Extended field "n" * A field number (from 1 to 25) comes at "n".	string
<!--\$FIELDNAMEn\$-->	Extended field name "n" * A field number (from 1 to 25) comes at "n".	string

Tip

The administrator can customize data to be stored in an extended field in the Meta Scan operation. For the definition of extended fields, see the following page:

📖 P.344 "Registering extended field properties"

APPENDIX

This chapter contains the following contents.

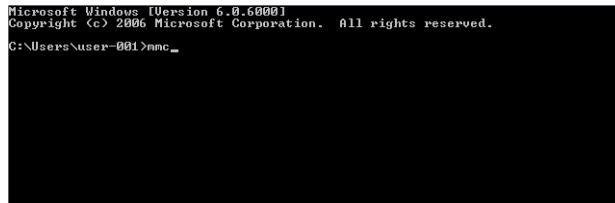
Installing Certificates for a Client PC	362

Installing Certificates for a Client PC

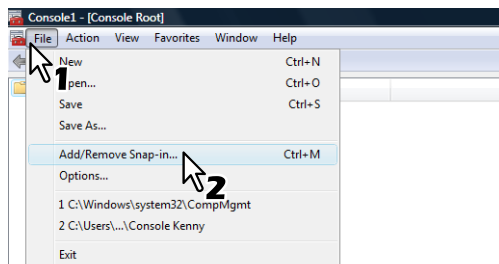
Configuring the Microsoft Management Console

The following describes a configuration on Windows Vista. The procedure is the same when Windows XP or Windows 2000 is used.

- 1 Open the command prompt, type “mmc” and press the Enter key.

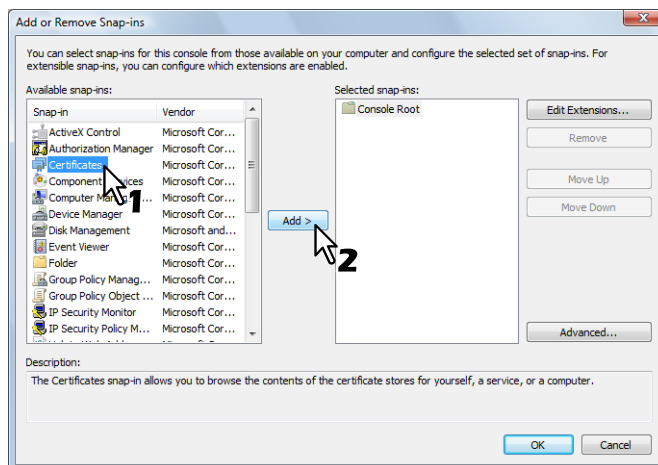


- 2 From the [File] or [Console] menu of the window that appears, select [Add/Remove Snap-in]



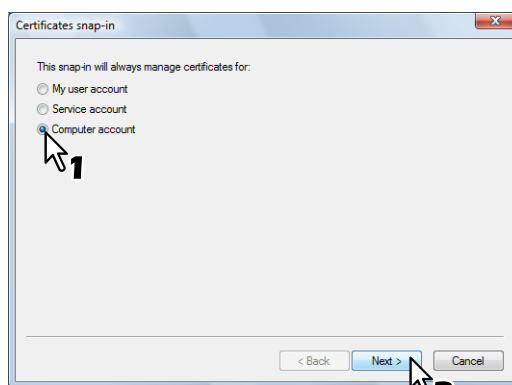
The Add or Remove Snap-ins dialog box appears.

- 3 From the list of [Available snap-ins:], select [Certificates] and click [Add].



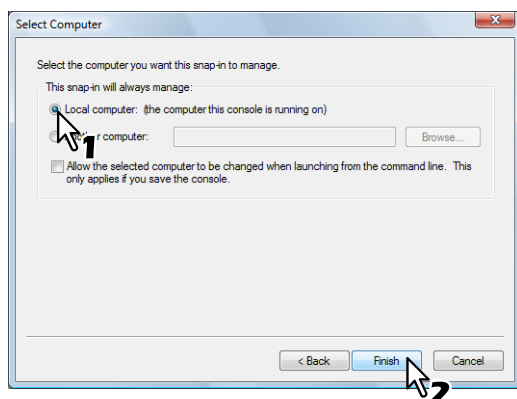
For Windows XP/2000, click [Add] to display the list and then select [Certificates.] The [Certificates snap-in] dialog box appears.

- 4 Select [Computer account] and click [Next].



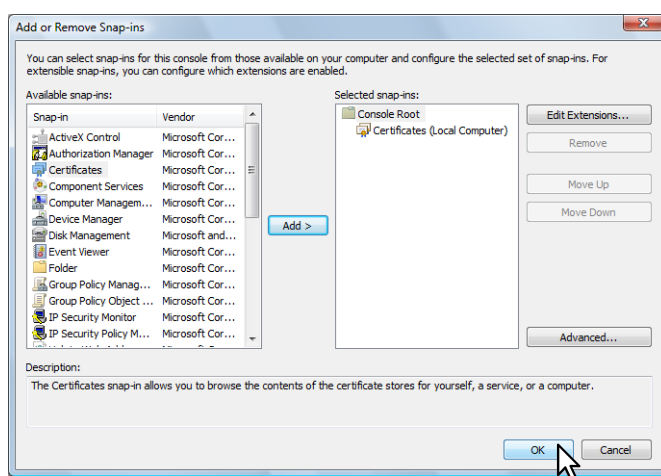
The [Select Computer] dialog box appears.

5 Select [Local computer: (the computer this console is running on)] and click [Finish].

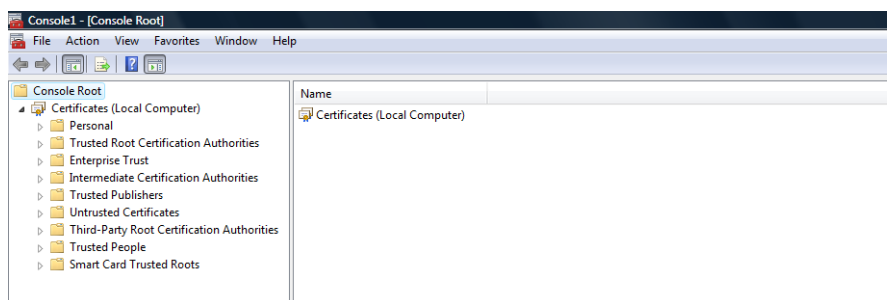


The [Select Computer] dialog box is closed.

6 Make sure that "Certificates (Local computer)" is added under the Console Root Folder; click [OK].



7 Save the setting.

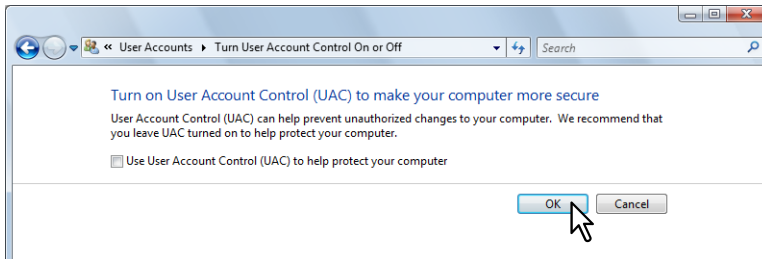


Importing certificates to a client PC

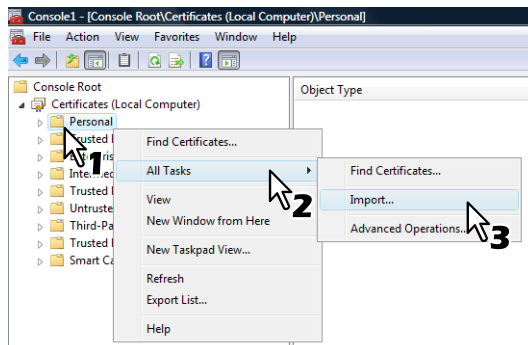
The following describes an import on Windows Vista. The procedure is the same when Windows XP or Windows 2000 is used.

Note

For Windows Vista, you must log in to Windows as a user who has the “Administrators” privilege. Before importing certificates, make sure that User Account Control (UAC) is turned off. From Control Panel > User Accounts > Turn User Account Control On or Off, clear the check box for the [Use User Account Control (UAC) to help protect your computer] option and click [OK].



- 1 On the MMC, select and right-click on the appropriate folder to store the certificate and select [All Tasks] > [Import]



Select the appropriate folder according to the type of your certificate:

Self-signed certificate (.crt): Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities

Client certificate (.pfx): Console Root > Certificates (Local Computer) > Personal

CA certificate (.cer): Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities

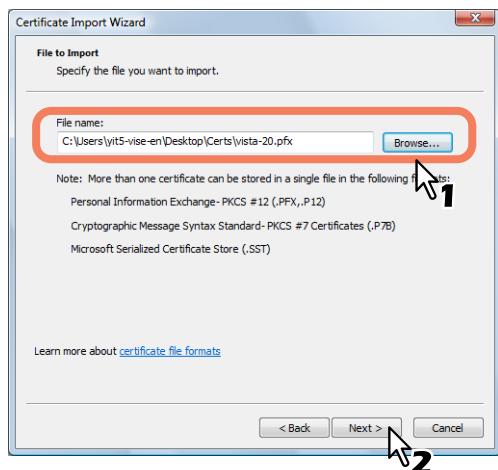
The Certificate Import Wizard appears.

- 2 On the Certificate Import Wizard, click [Next].

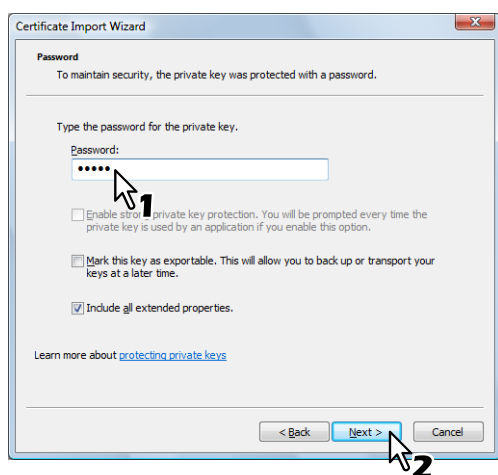


For importing a client certificate, proceed to the next step. Otherwise, skip to step 5.

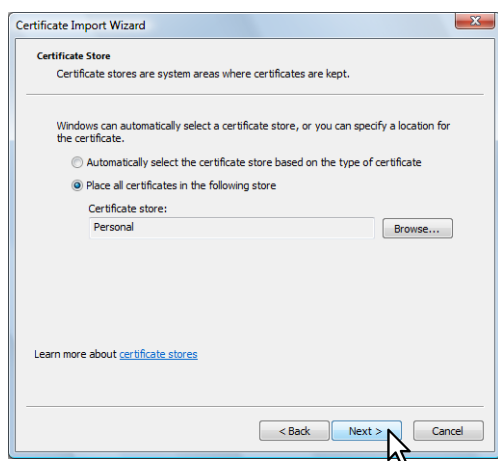
3 From [Browse], select the certificate to install, and click [Next].



4 Enter the password for the private key and click [Next].



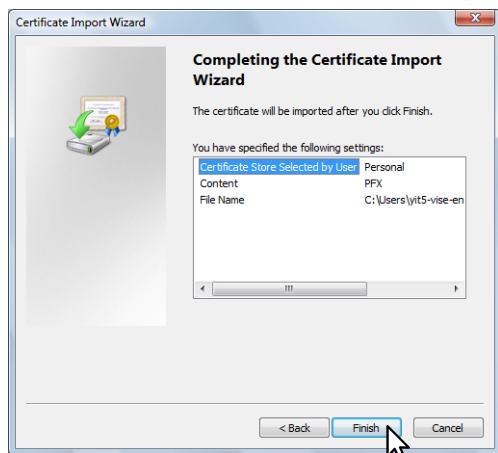
5 Click [Next].



Note

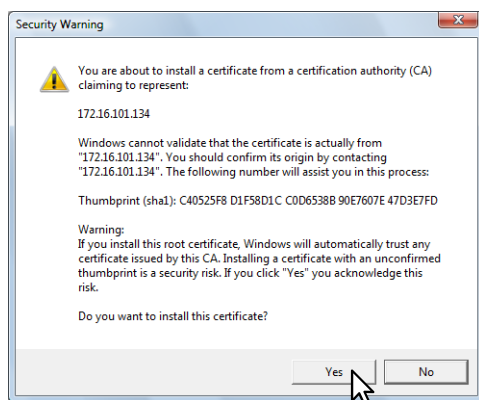
Do not change the certificate store using [Browse].

6 Click [Finish].

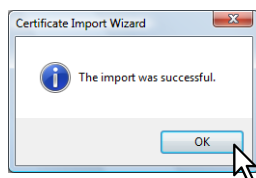


Tip

If the following security warning message appears, click [Yes].



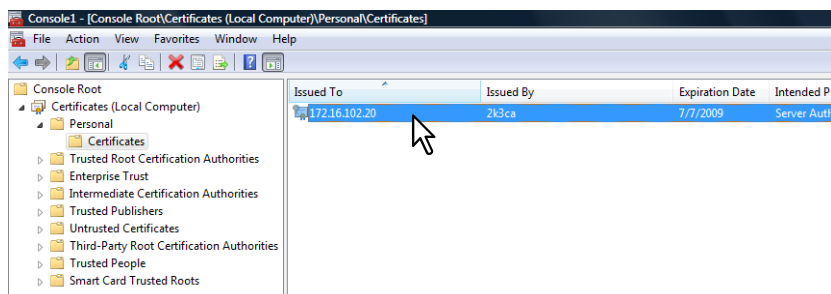
7 Click [OK] to complete the import.



If you are importing a client certificate (.pfx) to a Windows Vista PC, proceed to the next step. Otherwise, the installation is complete.

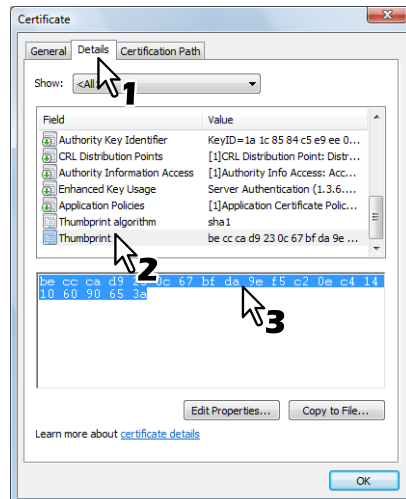
If you need to install another certificate, repeat the steps from the beginning.

8 Double-click the imported client certificate.



The Certificate window appears.

9 Click the [Details] tab and select [Thumbprint] to check the 40-digit thumbprint.



10 Open the command prompt and execute the “netsh” command as shown below.

Tip

If you log in to Windows Vista as a user without the administrator privilege, open the command prompt by right-clicking the icon and selecting [Run as administrator.] This way, you can temporarily have the administrator privilege to execute the command.

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\user-001>netsh http add sslcert ipport=0.0.0.0:5358 certhash=beccad923
0c67bfda9ef5c20ec414106090653a appid={00112233-4455-6677-8899-AABBCCDDEEFF}

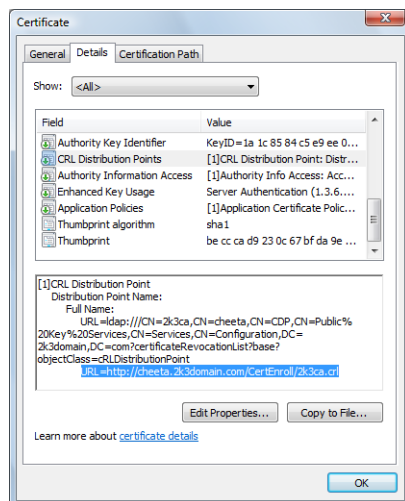
SSL Certificate successfully added

C:\Users\user-001>_
```

- Using the thumbprint obtained in Step 9, type the following command:
netsh http add sslcert ipport=0.0.0.0:5358 certhash=(your 40-digit thumbprint) appid={00112233-4455-6677-8899-AABBCCDDEEFF}
- When inputting the thumbprint, exclude the spaces.

Tip

When your client certificate is created with Certificate Revocation List (CRL), you need to check if the CA server is accessible by FQDN (See the following figure).



If no FQDN connection is established, ask your administrator to perform either of the following options:

- In the “hosts” file accessible from the following folder path, add the IP address and the host name:
C:\WINNT\system32\drivers\etc
- Configure the DNS server to handle the name-to-address resolution.

INDEX

Numerics

2in1/4in1	171
2nd Fax Number	79

A

Accessing TopAccess	
Administrator Mode	106
End-User Mode	9
Account Manager	288
Account Name	138
Actual Frame	124
Add Address	78
Add the date and time to the Subject	185
Address Book	53
Address Group	55
Address Mode	120
Address Specifying Method	185
Administrative Message	111
Administrator's Name	197
Administrator's Password	111, 197
AH Transforms	323
Alerts	19
Allow the following network folder to be used as a destination	181
Allow user to select network folder to be used as a destination	181
AppleTalk	125
Attribute 1	126
Attribute 2	126
Authentication	135, 137, 197, 217
Authentication Password	143
Authority	62, 64, 254, 256
Auto 2-sided Mode	171
Auto Clear	112
Auto Power Save	112
Automatic Start	52

B

Background	69
Backup	210
Backup Domain Controller	131
Banners	195
Bcc Address Display	185
BDC	274
Body	58, 61, 253
Body String Transmission	185
Body Strings Transmission	188
Bonjour	125
BOOK > 2	171
Box Number	66, 90
Box Setting	
Fax/Internet Fax Received Forward	258
Mailbox	90
Private template	50, 66
Public template	241
Bulletin Board	88
Bulletin Board mailbox	86
Bypass feed	170

C

Capacity	20
Caption1	51
Caption2	51
CBC-DES	142
Clearing Logs and Journals	233
CMYK Source Profile	204

Color Mode	68, 170
Comment	90
Common Name	148
Company	79
Completion Volume	173
Compression	68
Confidential	88
Confidential mailbox	86
Confirm Password	112
Contact	
Adding	78
Deleting	81
Contact Information	19, 111
Context	132
Context Name	143
Contrast	69
Controller Type	19
Copier Model	110
Copier Settings	169
Copier settings	168
Copy agent	48, 238
Country/Region Code	148
Create SNMP User Information	142

D

Date Format	114
Dates	114
Daylight Savings Time	114
DDNS Session	128
Default Body Strings	185, 188
Default file path	178
Default Gateway	122
Default Page	115
Default Port Number	139
Default Profile	200, 204, 205
Default Raw Job Setting	190
Default Subject	185
Delayed Transmit	60
Delete documents after [] day(s)	177
Delete Files	215
Department	79
Department Code	
Clearing Counters	262, 263
Deleting	266, 267
Department management	269
Device Information	110
Displaying Counters	98, 261
Displaying Department List	260
Modifying	264
Registering	264
Department Code Enforcement	110, 269
Department Counter	98
Department Management	
Copy	111, 269
FAX	111, 269
List	111, 270
Print	111, 270
Scan	111, 270
Department Name	265
Department Number	288
Desired Zone	125
Destination	64, 66, 256, 258
Destination Address	320
Destination Port	320
Destination Profile	205

Destination Setting		Enable LDAP	126
Fax/Internet Fax received forward	248	Enable LPD	195
Mailbox	89, 91	Enable MAC Address Filtering	123
Meta Scan template	340, 341	Enable NDS	132
Private template	49, 52	Enable OffRamp	136
Public template	240	Enable Partial Email	198
Device Information	19, 110	Enable PFS	322
Device Name	125	Enable POP3 Client	137
Device settings	108	Enable Print	275, 280, 285
Dial Type	173	Enable Print Email Error	198
Dial Type (Line 2)	174	Enable Print Header	198
Diffie-Hellman algorithm	322	Enable Print Message Body	198
Direct Transmit	59	Enable Raw bi-directional	195
Directory Service	216	Enable Raw TCP	195
Directory Service Name	217	Enable Remote Scan	275, 280, 285
Discard	174	Enable SLP	140
DNS Session	127	Enable SMTP Client	134
Do not allow any network folder		Enable SMTP Server	136
to be used as a destination	178, 182	Enable SNMP V1/V2	141
Do not delete documents automatically	177	Enable SNMP V3	141
Do not Print Blank Pages	191, 192	Enable SNMP V3 Trap	142
Document Name	66, 258	Enable SNTP	138
Document Print	91, 246	Enable SSL	126, 133, 134, 137, 139
Domain	130	Encryption	62, 64, 253, 256, 322, 323
Domain Name	129, 274	Encryption Level	62, 64, 254, 256
Drawer	20	Energy Save	112
Duplex Print	174	ESP Transforms	323
Duplex Printing	192	Ethernet Speed Duplex Mode	120
E		EWB Setting	115
ECM	59, 80, 174	Export/Clear Log	225, 229, 231, 233
Editing of Subject	185	Exporting	
e-Filing Notification Events	112	Address Book Data	225
Email Address	79, 91, 136	Department Code	229
Email agent	86, 88, 246	Journals	231
Email Error Transfer Address	198	Logs	231
Email Setting		Exposure	59, 69, 174
Fax/Internet Fax Received Forward	253	Exposure for Black	170
Mailbox	89, 92	Exposure for Color	170
Meta Scan template	340, 341	Extended field	344
Private template	50, 61	Extended Field Settings	341, 342
Public template	241	F	
Email Settings	183, 184	Fax	20
Email to	52	Fax Number	79, 173
Enable Alerts Trap	142	Fax Number (Security)	60
Enable Apple Talk	125	Fax Reception Space Available	19, 110
Enable Authentication Trap	142	Fax Setting	
Enable Bindery	132	Address Book	79
Enable Bonjour	125	Private template	49, 59
Enable Color Output	275, 280, 285	Public template	241
Enable Copy	275, 280, 285	Fax Settings	173
Enable DDNS	129	Fax settings	171
Enable DNS	127	Fax Transmission Jobs	
Enable e-Filing Box	275, 280, 285	Deleting	28
Enable Email	275, 280, 285	Displaying	27
Enable Email Error Forward	198	Fax Transmission Space Available	19, 110
Enable Fax	275, 280, 285	Fax/Internet Fax agent	48, 238
Enable File Share	275, 280, 285	File Format	58, 61, 63, 253, 255
Enable FTP Printing	197	File Format (Black)	185
Enable FTP Server	139	File Format (Color)	185
Enable HTTP Server	133	File Name	62, 65, 254, 257
Enable Internet Fax	275, 280, 285	Filter Action	320
Enable IP Filtering	122	Filter Name	320
Enable IPP	196	Filtering	122
Enable IPsec	318	Fine	59
Enable IPX/SPX	123, 124	Finisher	20

First Name	79
Folder Name	66, 258
Forward	88, 246
Forward mailbox	86
Fragment Message Size	62, 185, 254
Fragment Page Size	58, 187
Frame Type	124
From Address	58, 61, 184, 187, 253
From Name	58, 61, 184, 187, 253
FTP Client	139
FTP MODE	139
FTP Server	139
Function tab	15

G

General	
Daylight Savings Time	114
Device Information	110
e-Filing Notification Events	112
Energy Save	112
Time Stamp	114
Web General Setting	115
General Setting	189
Group	
Adding	83
Deleting	85
Editing	83
Group Name	84
GSS-TSIG	129

H

Help link	15
HMAC-MD5	142
HMAC-SHA	142
Hole Punch Unit	20
Host Name	129
HTTP Network Service	133

I

ICC Profile settings	199
IKE Key Name	321
IKE Transforms	322
IKE Type	321
IKEv1 (Main Mode)	321
IKEv2	322
Import	223, 228
Importing	
Address Book Data	223
Department Code	228
Inbound Fax Routing	90
Insertter	20
Install Software link	15
Integrity	322
Internet Fax agent	246
Internet Fax Settings	
Fax/Internet Fax Received Forward	252
Mailbox	89, 91
Private template	49, 58
Public template	241
Internet Protocol Version	130, 320
Internet/Fax (Relay) agent	86
Internet/Fax(Relay)	88
InternetFax Setting	187
InternetFax Settings	186
IP Address	122
IP Conflict Detect	122

IP Filter	324
IP Filtering	122
IP Filtering Rule	122
IP Trap Address 1-10	142
IP Trap Community	142
IPCOMP Transform	323
IPsec	317
IPsec menu	318
IPv4/IPv6 Address	323
IPv6	123
IPX Trap Address	142
IPX/SPX	124
ITU-T	86

J

Journal Auto Print	174

K

Key Selection	323
Keyword	79

L

Last Name	79
LDAP Authentication	272
LDAP server	56, 82
LDAP Session	126
Letterhead Print Mode	191, 192
Line 2 Number	173
Line Select	59, 80
Line-2 Mode	174
Link Local Address	123
Link-Local Host Name	125
LLMNR	123
LLTD	166
Locality Name	148
Location	19, 111
Login Name	135, 198
Login page	106
Login User Name	65, 181, 182, 257
Logon User Name	131
LT<-->A4/LD<-->A3	189

M

MAC Address Filtering	123
MAC Address Filtering Rule	123
Magazine Sort	171
MailBox Setting	89, 90
Main Memory Size	19
Maintenance	
Backup	210
Delete Files	215
Directory Service	216
Export/Clear Log	225, 229, 231, 233
Import	223, 228
Notification	218
Reboot	235
Remove Software	209
Restore	213
Upload Software	208
Maintenance from TopAccess	104
Maintenance Functions	207

Managing		Obtain a SMTP Server Address automatically	121
Address Book	78	Obtain a SNTP Server Address automatically	121
Counters	95	Obtain a WINS Server Address automatically	121
Fax/Internet Fax Jobs	27	OffRamp Print	136
Mailboxes	86	OffRamp Security	136
Print Jobs	24	Offset	114
Scan Jobs	29	Omit Blank Page	70
Manual	123	Open Mailbox	
Master Password	62, 64, 253, 256	Deleting	93
Maximum Copies	171	Setting up	87
Maximum Email / Internet Fax Size	135	Optional Function kit	20
Maximum Email Body Print	198	Options	20
Maximum reached for Black output	265, 288	Organization Name	148
Maximum reached for Full Color output	265, 288	Organizational Unit Name	148
Maximum reached of Full Color output	265	Orientation	192
MDN Reply	198	Original Mode	59, 69, 174
Memory Transmission Report	174	Original Mode for Black	170
Memory Transmit	59	Original Mode for Color	170
Menu bar	15	Original Size	69
Message	19	Output Tray	192
Message Header (Inbound FAX Routing)	184, 187	Outside Erase	70
Message Log	259		
Meta Scan	333	P	
Meta Scan template	333	Page Memory Size	19
Meta Scan template group	333	Panel Setting	
MFP Local Authentication	272	Meta Scan template	340, 341
Monitor Volume	173	Private template	49, 51
Multi Transmission Report	175	Public template	240
N		Paper	20
Name	19, 40	Paper Size	192
NetBIOS Name	130	Paper Source	190, 192
NetWare Session	132	Paper Type	192
Network		Partial Wait Time	198
AppleTalk	125	Password	
Bonjour	125	Box Setting	66, 258
DDNS Session	128	Directory Service Properties	217
DNS Session	127	Fax Setting	60
Filtering	122	IPP Print	197
FTP Client	139	MailBox Setting	90
FTP Server	139	N/W-Fax Folder	183
HTTP Network Service	133	NetWare Print	198
IP Security	318	POP3 Network Service	138
IPv6	123	Remote1 and Remote 2	181
IPX/SPX	124	Save as file Setting	65, 257
LDAP Session	126	SMB Session	131
LLTD	166	SMTP Client	135
NetWare Session	132	PCL Font Number	190, 192
POP3 Network Service	137	PCL Font Pitch	190, 192
Security Service	146	PCL Font Point Size	190, 192
SMB Session	130	PCL Form Line	190, 192
SMTP Client	134	PCL Line Termination	190, 192
SMTP Server	136	PDC	274
SNMP Network Service	141	Permissions Level	143
SNTP Service	138	Permit Guest User's authority	
TCP/IP	120	for all registered users.	275, 280
Web Services Setting	166	Phone Number	19
Network Path	65, 181, 182, 257	Picture	51
Network settings	118	Policy	318
Notification	40, 52, 91, 218	Policy Name	324
Number of Retry	185, 187	Polling Report	175
O		POP Before SMTP	135
Obtain a Domain Name automatically	121	POP3 Client Connection Timeout	138
Obtain a Domain Server Address automatically	121	POP3 Network Service	137
Obtain a POP3 Server Address automatically	121	POP3 Server Address	137

Port Number		Read Write Community	141
Directory Service Properties	217	Reboot	235
FTP Client	139	Reception Journals	34
FTP Print	197	Reception Mode	173
IPP Print	196	Recovery Transmit	174
LPD Print	195	Reduction	174
POP3 Network Service	138	Registration	
Raw TCP Print	195	Fax Received Forward	245
SMTP Client	135	Internet Fax Received Forward	245
SMTP Server	136	Public Template	236
SNTP Service	138	Registration from TopAccess	104
Port Number (Command)	65, 181, 182, 256	Relay End Terminal Report	89, 92
Port80 Enable	196	Relay Originator	175
Preview	68	Remote 1	65, 256
Primary DNS Server Address	127	Remote 2	65, 257
Primary Domain Controller	131	Remove Software	209
Primary Login Name	129	Rendering Intent	205
Primary Password	129	Reset All Counters	262
Primary Port Number	133	Reset Counters	263
Primary SNTP Address	138	Resolution	59, 68, 174
Primary WINS Server	131	Restore	213
Print Job Logs	32	Retention period of Private, On-hold, Proof and Invalid Jobs	189
Print Jobs		Retry interval	185, 187
Deleting	25	Retype Password	65, 66, 181, 183, 257
Displaying	24	RGB Adjustment	69
Releasing	26	RGB Source Profile	200
Print Password	197	Role Based Access	275, 280
Print Queue Scan Rate	198	Rotate Sort	174
Print Service		Rotation	68
Email Print	198	RTI	174
FTP Print	197		
IPP Print	196	S	
LPD Imaging	195	Saturation	69
NetWare Imaging	198	Save as file	
Raw TCP Print	195	Destination	178
Print Service settings	193	File Composition	180
Print Startup Page	189	Folder Name	178
Print User Name	197	Format	179
Printer settings	188	Local Storage Path	177
Priority Transmit	60	N/W-Fax Destination	182
Privacy Password	143	N/W-Fax Folder	182
Privacy Protocol	143	Remote 1 and Remote 2	181
Private Template Groups	38	Searching Interval	180
Profile Name	323, 324	Single Page Data Saving Directory	179
Proposals	323	Storage Maintenance	177
Protocol	65, 181, 182, 256	User Name and Password at User Authentication	
Protocol Type	320	for Save as File	180
Public Template		Save as file agent	86, 88, 246
Creating	236	Save as file Setting	
Editing	236	Fax/Internet Fax Received Forward	255
PWD	80	Mailbox	89, 92
Q		Meta Scan template	340, 341
Quality Transmit	60, 80	Private template	50, 63
Queue Name	192	Public template	241
Queue name	111	Save as file settings	176
R		Save as File Space Available	19, 110
Raw Job Setting	191	Save to USB Media	64
Raw jobs - Default Orientation	190	Scan agent	48, 238
Raw jobs - Default Output Tray	190	Scan Job Logs	35
Raw jobs - Default Paper Size	190	Scan Jobs	
Raw jobs - Default Paper Type	190	Deleting	30
Raw jobs - Default Stapling	190	Displaying	29
Raw jobs - Duplex Printing	190	Scan Rate	138
Read Community	141		

Scan Setting		SNMP V3 Trap Privacy Protocol	142
Meta Scan template	341	SNMP V3 Trap User Name	142
Private template	50, 67	SNTP Service	138
Public template	241	Sorter Mode Priority	171
Scope	140	Source Address	320
Search	56, 82	Source Port	320
Search Base	217	SSL Port Number	138, 139
Search Method	126	SSL URL	196
Search root	133	SSL/TLS	134
Search Timeout	217	Standard	59
Secondary DNS Server Address	127	Stapling	192
Secondary Login Name	129	State or Province Name	148
Secondary Password	129	Status	19, 20
Secondary Port Number	133	Storage Path	177
Secondary SNTP Address	138	Store to e-Filing agent	86, 88, 246
Secondary WINS Server	131	Store to e-Filing Space Available	19, 110
Security Method	129	SUB	60, 80
Security Service	146	Subject	58, 61, 253
Select Agent	238, 246	Subject Transmission	185
self-signed certificate	148	Submenu Bar	15
Send email when an error occurs	52, 91	Subnet mask	122
Send email when job is completed	52, 91	Super Sleep	112
SEP	60, 80	Symbol set	190, 192
Serial Number	19, 110		
Server IP Address	217	T	
Server Name	65, 181, 182, 256	Tab	
Server Registration	115	[Administration]	106
Service Name	125	[Counter]	96, 98
Service Phone Number	111	[Device]	18
Session Key Settings	322, 323	[Job Status]	24, 27, 29
Session Timer	115	[Logs]	32, 33, 34, 35
Set Limitation of Black	265, 288	[Meta Scan]	334
Set Limitation of Full Color	288	[Registration]	38, 78, 87
Setup		[User Management]	268
Copier	168	TCP/IP	120
Email	183	Templates	
Fax	171	Editing	45, 78
General	108	Managing	38
ICC Profile	199	Registering	45, 337
InternetFax	186	Terminal ID	173
Network	118	Time Stamp	114
Print Service	193	Top link	15
Printer	188	Total Counter	96
Save as file	176	Transmission Journals	33
Version	206	Transmission Type	59, 80
Setup from TopAccess	103	Tree	133
Sharpness	69	TSIG	129
SID	80	TSIG/SIG (0) Key file	129
SID/PWD	60	TSIG/SIG (0) Private Key file	129
SIG (0)	129	TTI	174
Single/2-Sided Scan	68	TTL	140
Size	20	Tunnel mode	323
Sleep Timer	112	Tunnel Settings	323
SLP	140	Type	20
SMB Server Protocol	130	Type POP3 Login	137
SMB Session	130		
SMB Signing of SMB Client	132	U	
SMB Signing of SMB Server	131	Ultra Fine	59
SMTP Client	134	Upload Software	208
SMTP Client Connection Timeout	135	URL	196
SMTP Server	136	Use local folder	64, 256
SMTP Server Address	134	Use Network Folder Destination	178, 182
SNMP Network Service	141	Use Stateful Address	124
SNMP V3 Trap Authentication Password	142	Use Stateless Address	124
SNMP V3 Trap Authentication Protocol	142	User Authentication Enforcement	284
SNMP V3 Trap Privacy Password	142	User Authentication for Scan to Email	308, 311

User Management Setting	273, 278, 283
User Name	40, 51, 90, 143, 217
User Password	62, 64, 253, 256

W

Wake Up setting	167
Web General Setting	115
WEB Language	115
Web Services Setting	166
Wide A4 Mode (for PCL)	189
Windows Domain Authentication	272
Work Space Available	19, 110
Workgroup	130

X

XML Format File	335, 355

FC-5520C/6520C/6530C
FC-2020C/2330C/2820C/2830C/3520C/3530C/4520C
DP-2090/2520/3000/3570/4570
DP-5550/6550/7550/8550
OME080020F0

MULTIFUNCTIONAL DIGITAL SYSTEMS

TopAccess Guide

TOSHIBA TEC CORPORATION

2-17-2, HIGASHIGOTANDA, SHINAGAWA-KU, TOKYO, 141-8664, JAPAN

