

PAPER REUSABLE DEVICE

TopAccess Guide

e-STUDIO RD30

e-STUDIO RD301

Preface


Thank you for purchasing this TOSHIBA Paper Reusable Device.
This manual describes remote setup and remote management operated from the web based management utility TopAccess.
Read this manual carefully before using this equipment. Keep this manual within easy reach, and use it to configure an environment that makes best use of the equipment's functions.


Operations on some items are restricted depending on the privileges assigned to the TopAccess user.


■ 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.

□ Screens

In this guide, the Windows screens and operating procedures used as examples are for Windows 7. The displayed screens may vary depending on the installation status of optional equipment, as well as the operating system version and applications being used.

□ Defaults

- The default values mentioned in this guide are values for a standard operating environment. The default values may change depending on the installation environment.
- The default for the list item is shown underlined.

□ Trademarks

- 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, 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, 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.
- TopAccess is a trademark of Toshiba Tec Corporation.
- Other company names and product names displayed in this manual or software are the trademarks of their respective companies.

□ Security Precautions

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

CONTENTS

Preface.....	1
Chapter 1 Overview	
TopAccess Overview	6
Conditions for Using TopAccess	7
Accessing TopAccess	8
Accessing TopAccess by the Entering URL.....	8
TopAccess Screen Descriptions.....	9
Access Policy Mode	10
Chapter 2 [Device] Tab Page	
[Device] Item List.....	14
Chapter 3 [Logs] Tab Page	
[Logs] Tab Page Overview.....	16
[View Logs] Item List	16
[Export Logs] Item List.....	18
Chapter 4 [Registration] Tab Page	
[Registration] Tab Page Overview	20
[Template] Item List.....	20
[Remote Network Settings] Item List	24
[Registration] How to Set and How to Operate.....	27
Managing Templates.....	27
Chapter 5 [Counter] Tab Page	
[Counter] Tab Page Overview	30
[Total Counter] Item List.....	30
Chapter 6 [User Management] Tab Page	
[User Management] Tab Page Overview	36
[User Accounts] Item List.....	36
[Department Management] Item List	40
[Export/Import] Item List	43
Chapter 7 [Administration] Tab Page	
[Setup] Item List	46
General Settings.....	46
Network Settings	51
Management Scan Settings	68
Reuse Counter Settings	70
Judgement Settings.....	70
Off Device Customization Architecture Setting.....	71

Version	72
[Security] Item List	73
Authentication.....	73
Certificate Management Settings	77
Password Policy Settings	79
[Security] How to Set and How to Operate	82
Creating/Exporting a Self-signed Certificate.....	82
Creating a Client Certificate/Exporting	84
[Maintenance] Item List.....	86
Import	86
Export	87
Create Clone File.....	88
Install Clone File	89
Directory Service Settings	91
System Updates	93
Languages.....	94
Reboot Settings.....	94
Chapter 8 [My Account] Tab Page	
<hr/>	
[My Account] Tab Page Overview.....	96
[My Account] Item List	96
Chapter 9 APPENDIX	
<hr/>	
Installing Certificates for a Client PC	100
Index.....	109

Overview

This chapter provides an overview of the TopAccess functions.

TopAccess Overview	6
Conditions for Using TopAccess	7
Accessing TopAccess	8
Accessing TopAccess by the Entering URL	8
TopAccess Screen Descriptions.....	9
Access Policy Mode.....	10

TopAccess Overview

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

End-user mode


End users can:

- Display general device information including the status, and paper output information.
- Displaying job logs
- Viewing Counters

 P.8 "Accessing TopAccess"

Access policy mode

Operation privileges and displayed items vary depending on the user account you used to log in to TopAccess.

 P.10 "Access Policy Mode"

Conditions for Using TopAccess

Your equipment should be connected to the network and TCP/IP is correctly configured to operate TopAccess.

When TCP/IP is correctly configured, you can access TopAccess via a web browser.

1

Supported browsers

Windows

- Internet Explorer 9.0 or later
- Firefox 3.5 or later

Macintosh

- Safari 4.0 or later

UNIX


- Firefox 30.0 or later

Notes

- Because TopAccess uses cookies to store information on the user system, users must have cookies enabled in the browser.
- If TopAccess does not display the correct information in any pages, delete the cookies and try again.
- Make sure you disable your Web browser's pop-up blocker or allow pop-ups from TopAccess.

Accessing TopAccess

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

 P.8 “Accessing TopAccess by the Entering URL”

■ Accessing TopAccess by the Entering URL

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

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

Address	<code>http://10.10.70.120</code>
---------	----------------------------------

For example

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

`http://10.10.70.120`

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

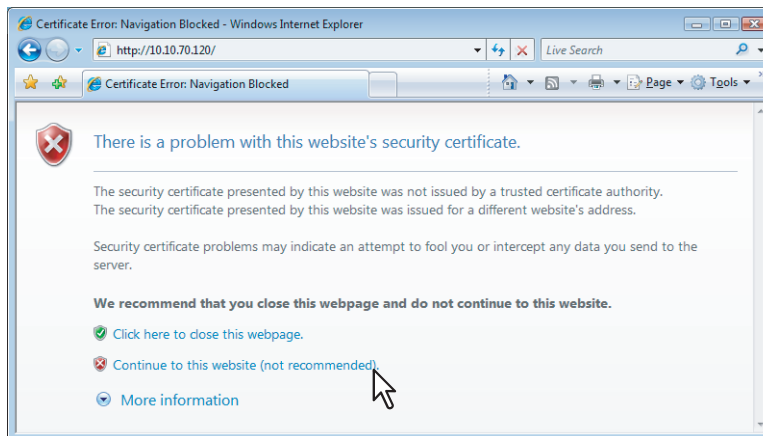
`3ffe-1-1-10-280-91ff-fe4c-4f54.ipv6-literal.net`

or

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

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.



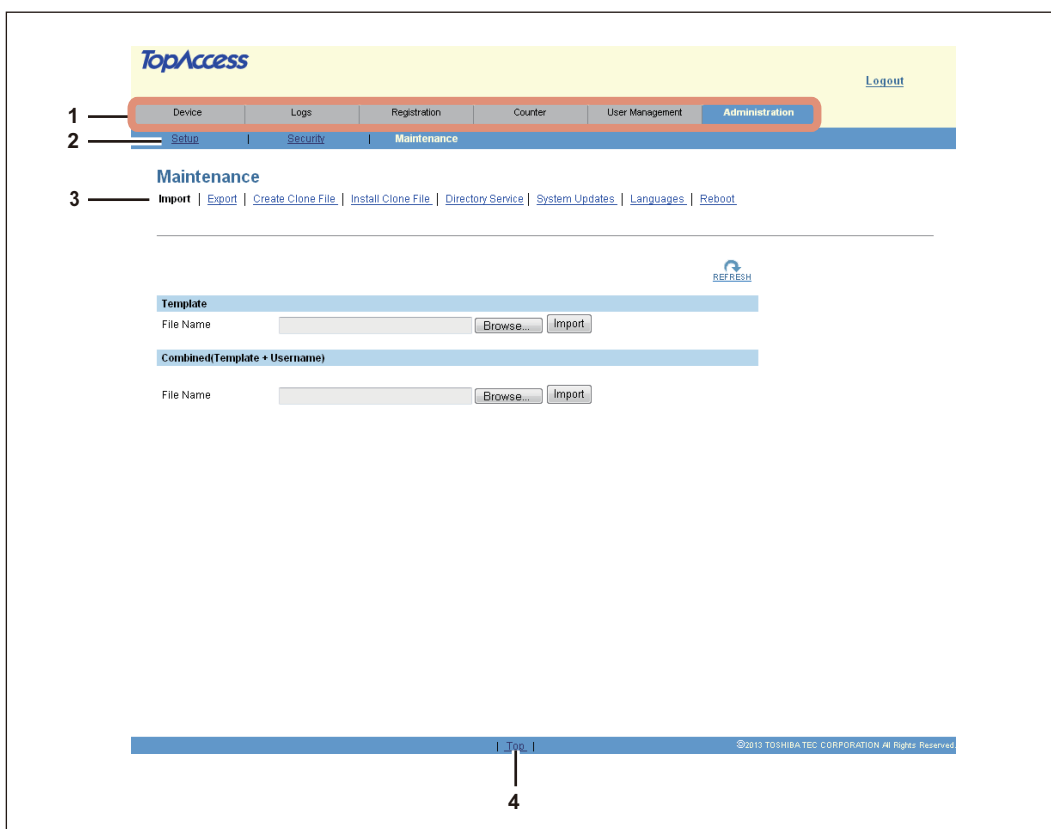
2 The TopAccess web page opens.

Device Information	
Status	Ready
Name	PRD10347993
Location	
Device Model	TOSHIBA e-STUDIO-RD301_Loops-RD301
Serial Number	■■■■■■■■■■
MAC Address	00:22:4d:86:6c:d9
Contact Information	
Phone Number	
Message	
Alerts	•

Drawer	Status
Upper Drawer	NOT FULL
Lower Drawer	NOT FULL

TopAccess Screen Descriptions

1




	Item name	Description
1	Function tab	Features are grouped under each tab. This provides access to the 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	Top link	Click this to display the top of the page that is currently displayed.

Access Policy Mode

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

The access policy mode controls details of operations and displays depending on the privileges assigned to the given user account.

1 Access TopAccess

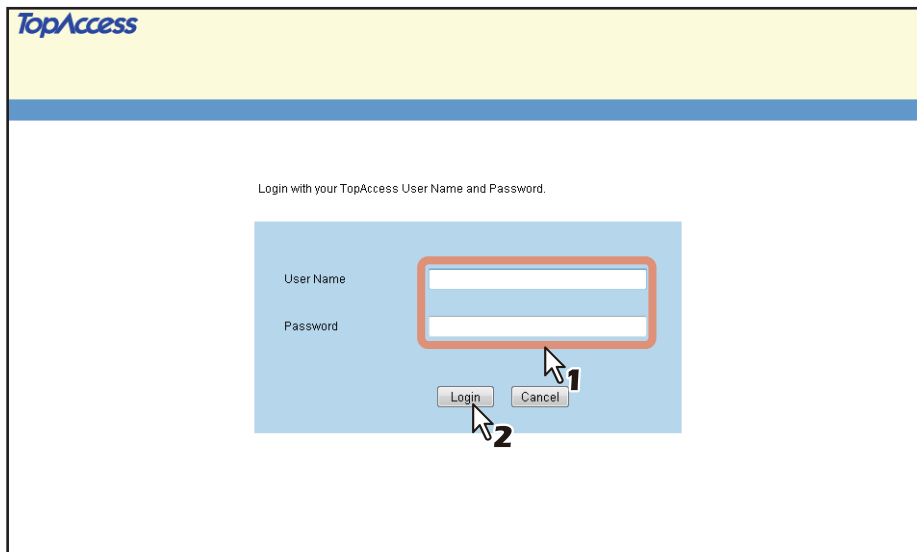
 P.8 "Accessing TopAccess"

2 Click [Login].



The login page is displayed.

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




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

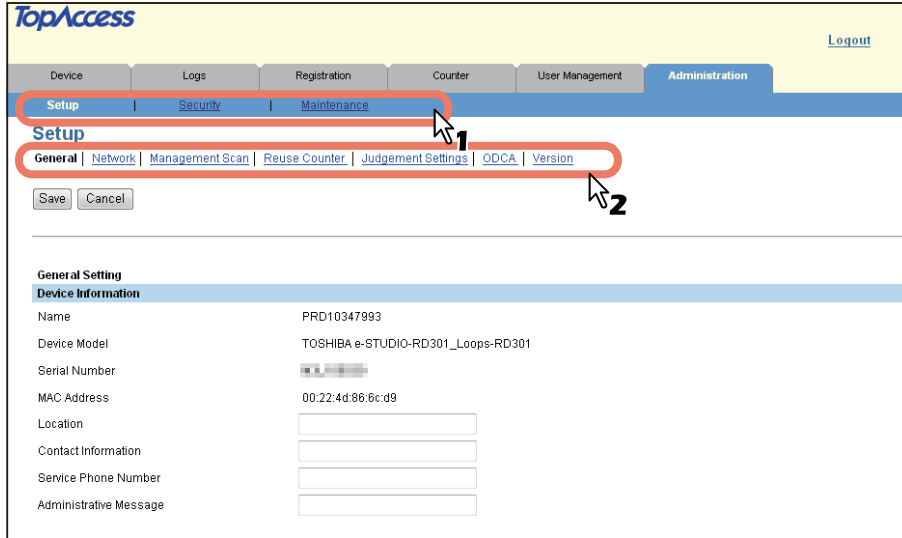
Notes

- Failing to enter the correct password for a number of times at login will be considered unauthorized access and you may not be able to log in for a certain period of time. If the messages "User account is locked" or "The User Name and Password are not recognized." are displayed and you cannot log in, contact your administrator.
- The password input is displayed in the blank symbols.
- After login, you will be automatically logged out when the time specified in the [Session Timer] elapses.

Tips

- Enter "admin" in User Name and "123456" in Password to log in for the first time.
- Lockout setting for user accounts can be set with [Administration] - [Security] - [Password Policy].
 P.79 "Password Policy Settings"
- The [Session Timer] can be set with [Administration] - [Setup] - [General] - [WEB General Setting].

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



The screenshot displays the TopAccess web interface. At the top, there is a navigation bar with tabs for Device, Logs, Registration, Counter, User Management, and Administration. Below this, a secondary menu shows Setup, Security, and Maintenance. The Setup menu is expanded, showing sub-items: General, Network, Management Scan, Reuse Counter, Judgement Settings, ODCA, and Version. A red circle highlights the Setup menu, and a red circle highlights the Version sub-item. A mouse cursor is positioned over the Version sub-item, with a '1' next to it. Another mouse cursor is positioned over the Version sub-item, with a '2' next to it. Below the navigation menu, there are Save and Cancel buttons. The main content area is titled 'General Setting' and 'Device Information'. It contains a table with the following data:

Device Information	
Name	PRD10347993
Device Model	TOSHIBA e-STUDIO-RD301_Loops-RD301
Serial Number	██████████
MAC Address	00:22:4d:86:6c:d9
Location	<input type="text"/>
Contact Information	<input type="text"/>
Service Phone Number	<input type="text"/>
Administrative Message	<input type="text"/>

Tip

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

[Device] Tab Page

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

[Device] Item List.....	14
-------------------------	----

[Device] Item List

The [Device] tab shows the following information about the device: At any time, the end-user may click REFRESH to update the TopAccess status information.

The screenshot shows the TopAccess web interface. At the top, there is a navigation bar with tabs for 'Device', 'Logs', and 'Counter'. Below this, the 'Device' section is active. It features a device image on the left, a 'Device Information' table on the right, a 'Drawer' table below it, and a 'Status' table at the bottom. A 'REFRESH' button is located in the top right corner of the device section. The 'Device Information' table lists various details such as Status, Name, Location, Device Model, Serial Number, MAC Address, Contact Information, Phone Number, Message, and Alerts. The 'Drawer' table shows the status of the Upper and Lower Drawers, both marked as 'NOT FULL'. The 'Status' table shows the availability of each cassette, also marked as 'NOT FULL'.

	Item name	Description
1	Device Information	The following information is displayed. <ul style="list-style-type: none"> • Status — Displays the equipment's status. • Name — Displays the equipment's name. • Location — Displays the equipment's location. • Device Model — Displays the equipment's model name. • Serial Number — Displays the equipment's serial number. • MAC Address — Displays the equipment's MAC address. • Contact Information — Displays the contact information of the person responsible for managing this equipment. • Phone Number — Displays the phone number of the person responsible for managing this equipment. • Message — Displays administrative messages. • Alerts — Displays alert messages.
2	Drawer	Displays a list of the drawers.
3	Status	Displays the availability of each cassette.

[Logs] Tab Page

This chapter explains the [Logs] tab page in TopAccess.

[Logs] Tab Page Overview	16
[View Logs] Item List	16
[Export Logs] Item List.....	18

[Logs] Tab Page Overview

You can check the job history.

Note

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


Tips

- Logs are recorded from the moment the equipment is turned on until it is shut down. Log recording continues even after entering the Energy Save mode.
- Up to 400 logs are displayed in chronological order, with the most recent first. You can check up to 1,000 logs in Job Log Export, and up to 2,000 logs in Messages Log Export by exporting them. The oldest logs are deleted when the number of logs exceeds the maximum limit.

 P.16 “[View Logs] Item List”

 P.18 “[Export Logs] Item List”

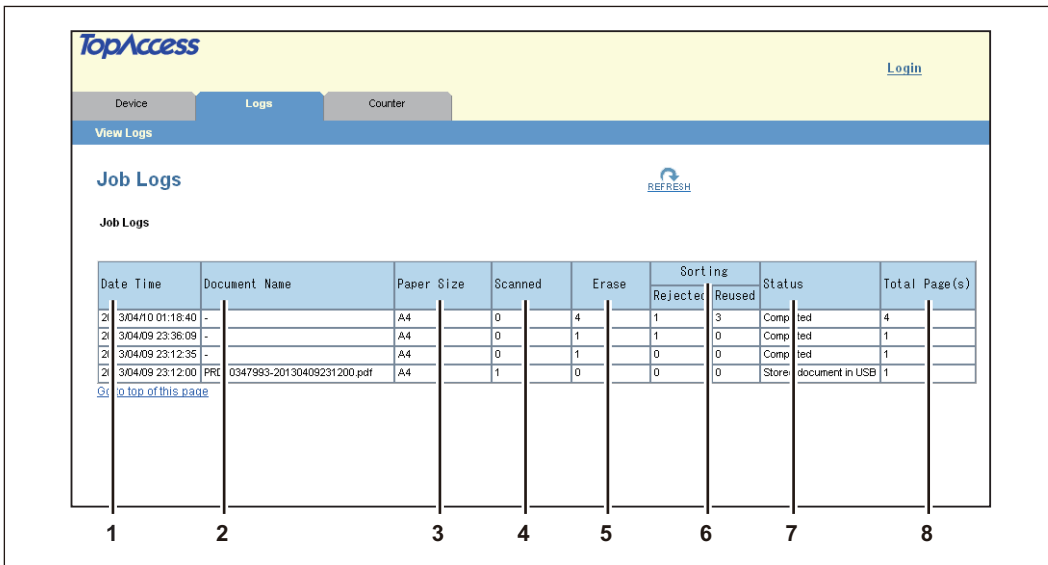
■ [View Logs] Item List

 P.16 “Job Logs”

 P.17 “Message Log”

□ Job Logs

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



	Date Time	Document Name	Paper Size	Scanned	Erase	Sorting		Status	Total Page(s)
						Rejecter	Reused		
21	3/04/10 01:18:40	-	A4	0	4	1	3	Completed	4
21	3/04/09 23:36:09	-	A4	0	1	1	0	Completed	1
21	3/04/09 23:12:35	-	A4	0	1	0	0	Completed	1
21	3/04/09 23:12:00	PRC 0347993-20130409231200.pdf	A4	1	0	0	0	Store document in USB	1

	Item name	Description
1	Date Time	Displays the date and time the job was performed.
2	Document Name	Displays the job's document name.
3	Paper Size	Displays the job's paper size.
4	Scanned	Displays the number of pages scanned in one job.
5	Erase	Displays the number of sheets erased in one job.
6	Sorting	Displays separately the number of rejected and reused sheets sorted in one job.
7	Status	Displays the completed job, or the results of the job.
8	Total Page(s)	Displays the number of sheets used in one job.

□ Message Log

The Message Log page displays errors which have occurred in the equipment.

Tip

Users who are granted administrator privileges in the access policy mode can access the Message Log page from the [Logs] tab.

See the following pages for how to access it:

P.10 “Access Policy Mode”

Date Time	Error Level	Message	Status	User Name	Domain Name/LDAP Server
2011/04/10 17:50:33	Information	Power On	711	---	
2011/04/10 04:13:10	Information	Power Off	711	---	
2011/04/10 02:38:12	Information	Power On	711	---	
2011/04/10 02:32:51	Information	Power Off	711	---	
2011/04/10 01:12:02	Information	Updated user information	628	Admin	
2011/04/10 01:11:51	Information	Updated user information	628	Admin	
2011/04/10 00:40:12	Information	Successfully exported Template	711	---	
2011/04/09 23:30:45	Information	Power On	711	---	
2011/04/09 23:14:33	Information	Power Off	711	---	
2011/04/09 23:09:36	Information	Power On	711	---	
2011/04/09 23:08:44	Information	Power Off	711	---	
2011/04/09 23:07:43	Information	Power On	711	---	


1 2 3 4 5 6

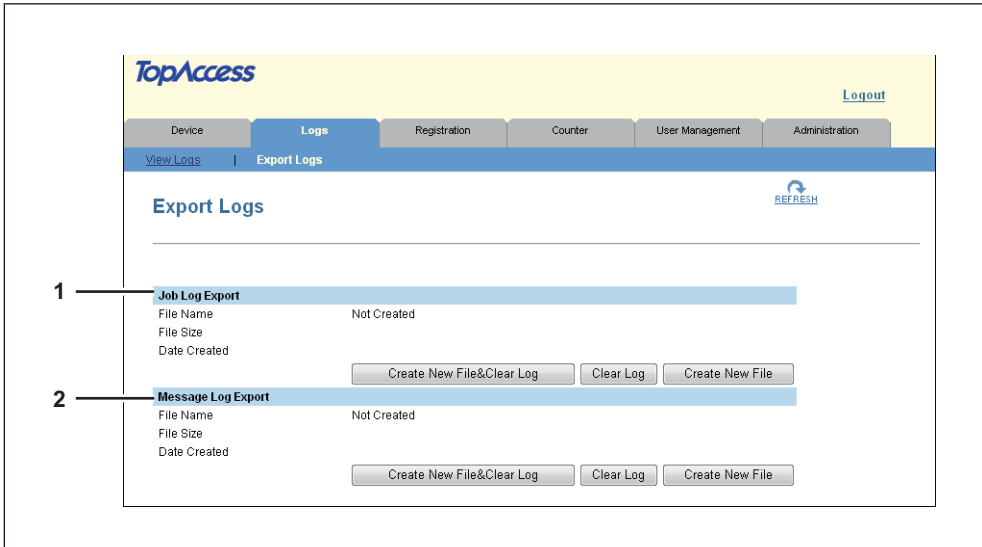
	Item name	Description
1	Date Time	Displays the date and time of the error.
2	Error level	Displays the error level. Error — Errors that cannot be handled by the end-user. Alerts — Errors that can be handled by the administrator. Information — Errors that can be handled by the end-user, or not errors.
3	Message	Displays the message if available.
4	Status	Displays the error code.
5	User Name	Displays the user account name related to the message.
6	Domain Name/LDAP Server	Displays the domain name or LDAP server of the user account related to the message.

■ [Export Logs] Item List

You can erase logs or export them in a file.

Tips

- Users who are granted administrator privileges in access policy mode can access the Export Logs page from the [Logs] tab.
See the following pages for how to access it:
 P.10 "Access Policy Mode"
- Logs are exported in CSV format.
- You can export up to 1,000 job logs, and up to 2,000 message logs. The oldest logs are deleted when the number of logs exceeds the maximum limit.



	Item name	Description
1	Job Log Export	<p>You can erase job logs or export (download) them in a file.</p> <p>Create New File & Clear Log — Creates a file. Erases logs after a file has been created. You can display or download by clicking the created file.</p> <p>Clear Log — Erases logs.</p> <p>Create New File — Creates a file. You can display or download by clicking the created file.</p>
2	Messages Log Export	<p>You can erase message logs or export (download) them in a file.</p> <p>Create New File & Clear Log — Creates a file. Erases logs after a file has been created. You can display or download by clicking the created file.</p> <p>Clear Log — Erases logs.</p> <p>Create New File — Creates a file. You can display or download by clicking the created file.</p>

4

[Registration] Tab Page


This chapter describes how to register a template.

[Registration] Tab Page Overview	20
[Template] Item List	20
[Remote Network Settings] Item List	24
[Registration] How to Set and How to Operate	27
Managing Templates	27

[Registration] Tab Page Overview

You can register your own templates.

 P.20 “[Template] Item List”

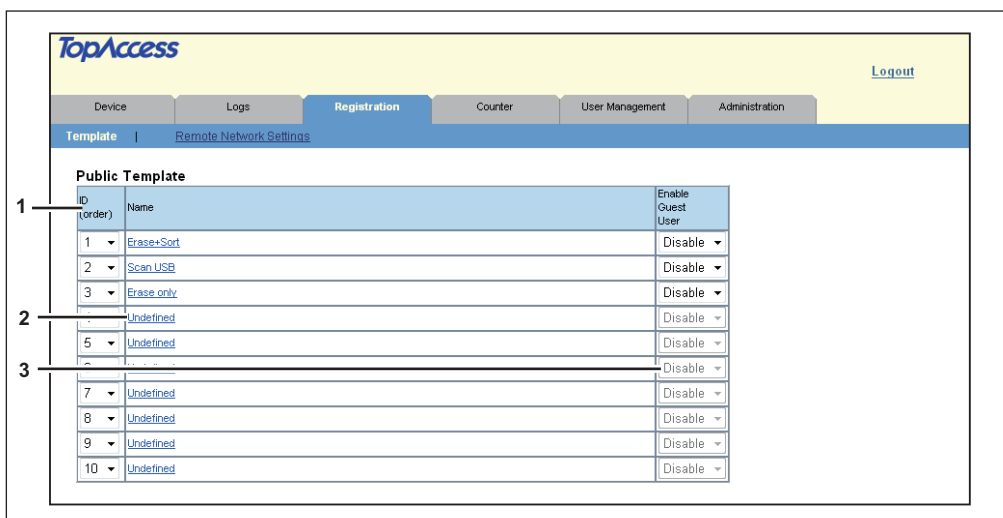
 P.24 “[Remote Network Settings] Item List”

■ [Template] Item List


□ [Public Template] Screen/[Private Template] Screen

When using this equipment from the control panel, you can combine settings for the erase, sort, and scan functions and register them as a template. You can then select that template when performing operations. This equipment can use up to ten public templates (3 preset templates), and up to ten private templates per user.



Public Templates



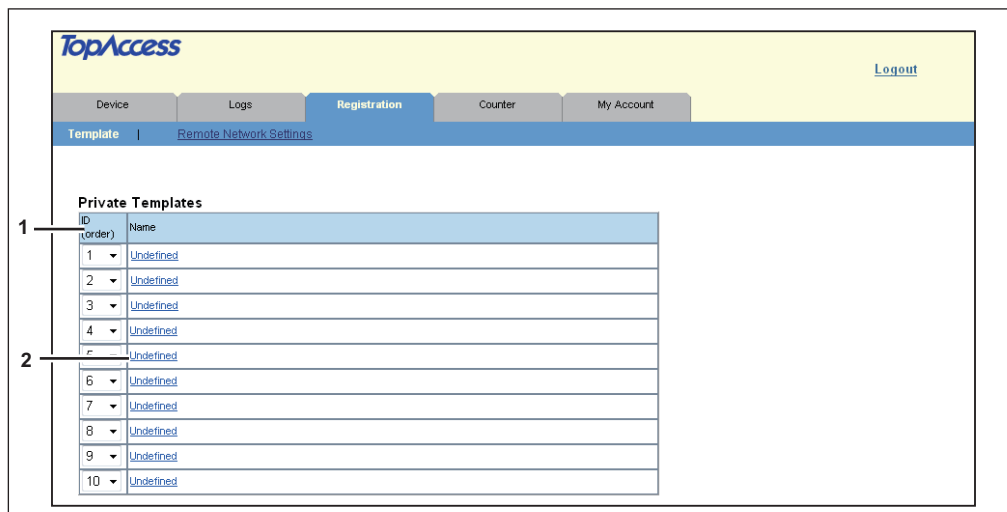
ID (order)	Name	Enable Guest User
1	Erase+Sort	Disable
2	Scan USB	Disable
3	Erase only	Disable
4	Undefined	Disable
5	Undefined	Disable
6	Undefined	Disable
7	Undefined	Disable
8	Undefined	Disable
9	Undefined	Disable
10	Undefined	Disable

	Item name	Description
1	ID (order)	Displays the template number. You can change the display order in the drop-down list on the LCD screen.
2	Name	Displays the template name.
3	Enable Guest User	When user authentication is enabled and operation by guest user allowed, the guest user can use templates set to "Enable" in the pull down list.  P.74 “Setting up User Authentication Setting”

Tips

- Public templates are created and managed by users who are granted administrator privileges in the access policy mode. See the following pages for how to access it:
 -  P.10 “Access Policy Mode”
- See the following descriptions for how to register public templates:
 -  P.27 “Registering or editing public templates”

Private Templates



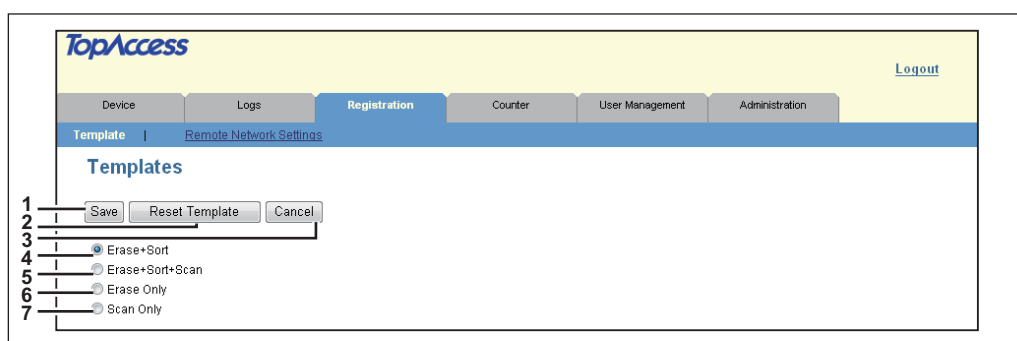
	Item name	Description
1	ID (order)	Displays the template number. You can change the display order in the drop-down list on the LCD screen.
2	Name	Displays the template name.

Tips

- Private templates are created and managed by users who are granted user privileges in the access policy mode. See the following pages for how to access it:
 P.10 “Access Policy Mode”
- See the following descriptions for how to register private templates:
 P.28 “Registering or editing private templates”

□ [Template] Screen

You can edit the template you are registering.



	Item name	Description
1	[Save] button	Saves the template settings.
2	[Reset Template] button	Resets registration of the public template.
3	[Cancel] button	The registration or editing process is canceled, and you are returned to the previous screen.
4	Erase+Sort	Creates the template for performing erasing and sorting.
5	Erase+Sort+Scan	Creates the template for performing erasing, sorting and scanning.

	Item name	Description
6	Erase Only	Creates the template for performing erasing.
	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Tip</div> [Erase Only] is not available if [Erase Only Mode] is disabled in the management scan function.	
7	Scan Only	Creates the template for performing scanning.

□ Panel Settings

Sets how the template is displayed on the equipment's LCD screen.

The screenshot shows a 'Panel Setting' window with three input fields:

- 1 Name: Undefined
- 2 User Name: admin
- 3 Paper Size: A4

	Item name	Description
1	Name	Sets the template name.
	<div style="border: 1px solid black; padding: 5px; margin-bottom: 5px;">Note</div> For names, you can use up to 30 alphanumeric characters. The following symbols (\ / : , ; * ? " < > ') are not allowed.	
2	User Name	Displays the template owner name.
3	Paper Size	Sets the paper size when creating a template.

□ Sorting Settings

Set the paper sorting method.

The screenshot shows a 'Sorting Settings' window with one dropdown menu:

- 1 Output Tray: Manual(Upper Drawer)

	Item name	Description
1	Output Tray	Set the paper sorting method and the output drawer after sorting. <ul style="list-style-type: none"> • Auto — Automatically identifies reusable paper and feeds the paper into the upper drawer. • Manual (Upper Drawer) — Feeds paper to the upper drawer without performing sorting. • Manual (Lower Drawer) — Feeds paper to the lower drawer without performing sorting.

□ Scan Settings

Sets how originals are scanned for the selected scan agent.

Item	Setting Name	Value
1	Color	Color
2	File Format	TIFF(Single)
3	Resolution	200dpi
4	Compression	Middle
5	Contrast	0
6	BRIGHTNESS	0
7	Background	0
8	Omit Blank Page	OFF
9	Single/Sided Scan	Duplex Book
10	Outside Erase	OFF
11	File Name Format(*)	[Device Name]-[Date]-[Page]
12	Folder Name Setting	None
13	Storage Path	USB

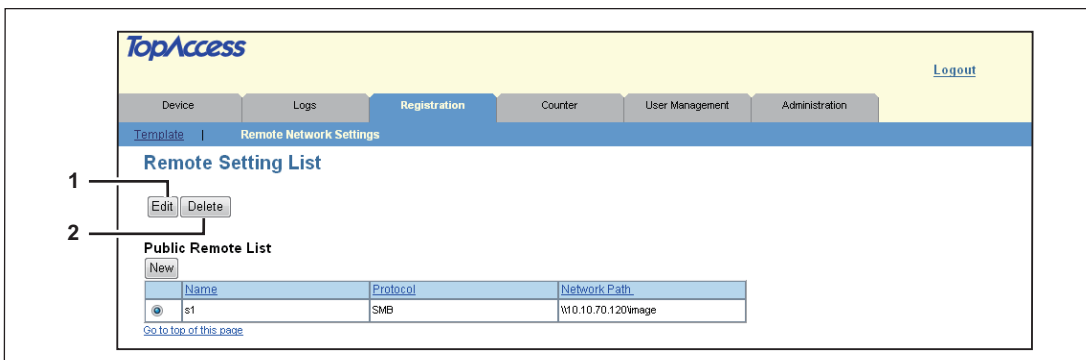
	Item name	Description
1	Color	Select the color mode for scanning.
	Tip	We recommend that you select "B&W (B&W(Blue))" when scanning paper printed in B&W on the e-STUDIO306LP/307LP.
2	File Format	Select the file format for the scanned file to be stored. <ul style="list-style-type: none"> • TIFF(Multi) — Select this to save scanned images as a Multi-page TIFF file. • TIFF(Single) — Select this to save scanned images separately as Single-page TIFF files. • PDF(Multi) — Select this to save scanned images as a Multi-page PDF file. • PDF(Single) — Select this to save scanned images separately as Single-page PDF files. • Slim PDF(Multi) — Select this to save scanned images as a Multi-page Slim PDF file. Use this format when you want to prioritize the smaller file size over the image quality. • SPDF(Single) — Select this to save scanned images as a Single-page Slim PDF file. Use this format when you want to prioritize the smaller file size over the image quality. • JPEG — Select this to save scanned images as JPEG files.
	Note	JPEG, Slim PDF(Multi) and SPDF(Single) are available when "Color" or "Gray" is selected for [Color].
3	Resolution	Select the resolution for scanning.
	Notes	<ul style="list-style-type: none"> • Selecting "300dpi" limits the maximum number of sheets usable in a job to 60. • When "Slim PDF(Multi)" or "SPDF(Single)" is selected for file format, "300dpi" and "200dpi" are available for resolution.
4	Compression	Select the compression for scanning.
	Tip	When "Slim PDF(Multi)" or "SPDF(Single)" is selected for file format, the compression cannot be changed.
5	Contrast	Select the contrast level of the scanned image. Contrast can be adjusted in 5 levels.

	Item name	Description
6	BRIGHTNESS	Select the brightness for scanning. Brightness can be adjusted in 5 levels.
7	Background	Select the density level of the background of the scanned image. Density can be adjusted in 5 levels.
8	Omit Blank Page	Select whether to automatically omit blank paper in the scanned image if it is included in originals.
9	Single/2-Sided Scan	Select whether to scan one side or both sides of an original. <ul style="list-style-type: none"> • Single — Select this to scan one side of an original. • Duplex Book — Select this to scan both sides of the 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 the originals with a vertical reversal to be bound along the horizontal side of the paper.
10	Outside Erase	Select whether to erase a shade that appears outside of the scanned image. The erased shade will be whitened.
11	File Name Format	You can set the file name by combining the following items. <ul style="list-style-type: none"> • Device Name • Date • Page
12	Folder Name Setting	Set whether or not the data are saved to a folder and the file name when saved. <ul style="list-style-type: none"> • None — Select this if you do not want to use a folder. • Add Device Name — Add the device name. • Add UserName — Add the user name.
13	Storage Path	Select the destination path. Saves the data to a USB media device or a network folder.

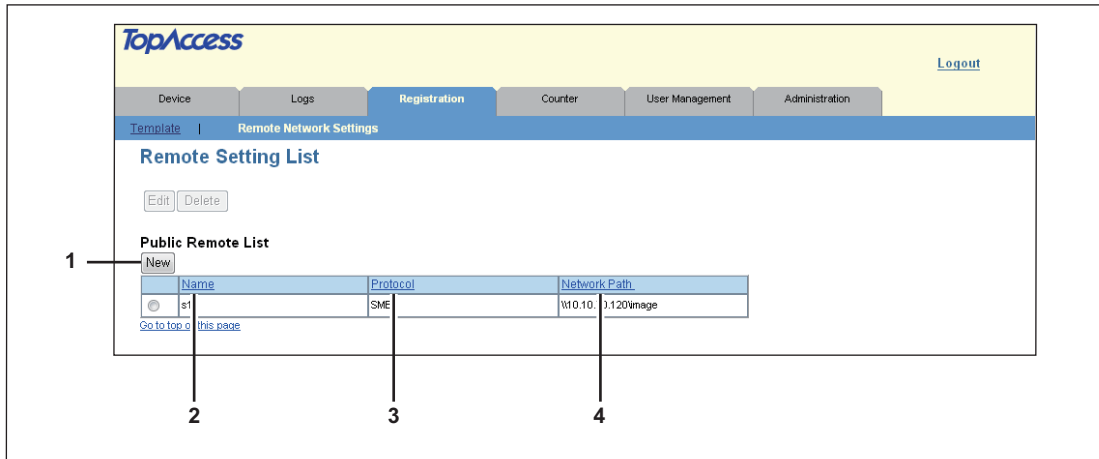
■ [Remote Network Settings] Item List

□ [Remote Setting List] screen

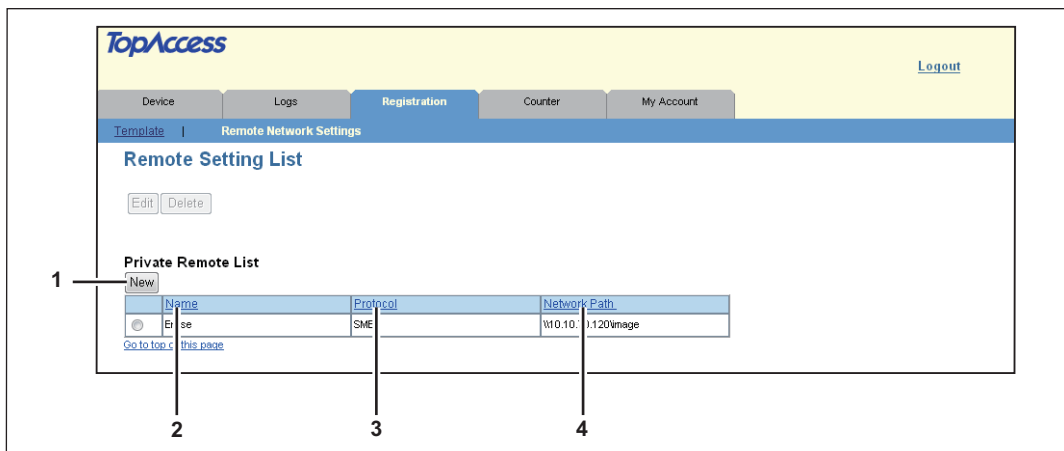
Displays the destination path list and allows you to create and edit a destination path.



	Item name	Description
1	[Edit] button	Edits the selected destination path.
2	[Delete] button	Deletes the selected destination path.

[Public Remote List] screen

	Item name	Description
1	[New] button	Allows you to add a new destination path. 📖 P.26 “[Remote Setting] screen”
2	Name	Displays the name of the destination path.
3	Protocol	Displays the protocol of the destination path.
4	Network Path	Displays the network path of the destination path.

[Private Remote List] screen

	Item name	Description
1	[New] button	Allows you to add a new destination path. 📖 P.26 “[Remote Setting] screen”
2	Name	Displays the name of the destination path.
3	Protocol	Displays the protocol of the destination path.
4	Network Path	Displays the network path of the destination path.

□ [Remote Setting] screen

Set the destination path for the scanned data.

The screenshot shows the 'Remote Setting' dialog box. On the left, a vertical list of numbers 1 through 10 is connected by lines to specific UI elements: 1 points to the 'Save' button, 2 to the 'Cancel' button, 3 to the 'Name' text box (containing 'Remote1'), 4 to the 'Protocol' radio buttons (SMB selected, WebDAV unselected), 5 to the 'Server Name' text box, 6 to the 'Port Number(Command)' text box, 7 to the 'Network Path' text box (containing '\\192.168.1.10\Scan'), 8 to the 'Login User Name' text box (containing 'User01'), 9 to the 'Password' text box (masked with dots), and 10 to the 'Retype Password' text box (masked with dots).

	Item name	Description
1	[Cancel] button	Cancels creating or editing the settings.
2	[Save] button	Saves the settings.
3	Name	Sets the name of the destination path.
	<div style="background-color: black; color: white; padding: 2px; display: inline-block;">Note</div> <p>For names, you can use up to 10 alphanumerical characters. The following symbols ([] * ? / \ " < > , ' ; : = + & %) and spaces are not allowed.</p>	
4	Protocol	Select the protocol. <ul style="list-style-type: none"> • SMB — Uses SMB as the protocol. • WebDAV — Uses WebDAV as the protocol.
5	Server Name	When WebDAV is selected as the protocol, enter the server name. You can enter up to 64 alphanumerical characters and symbols (- . / _ : %).
6	Port Number(Command)	When WebDAV is selected as the protocol, enter the port number. You can enter a value in the range from 0 to 65535 using numbers and hyphens (-). "-" is set as the default.
7	Network Path	Enter the network path for the destination path. You can enter up to 128 alphanumerical characters and symbols (excluding * ? " > < ;).
8	Login User Name	Enter the login user name to access the destination path if required. You can enter up to 32 alphanumerical characters and symbols (excluding : , ; * ? " < > ').
9	Password	Enter the password to access the destination path if required. You can enter up to 32 alphanumerical characters, symbols, and spaces. A single space only can also be entered.
10	Retype Password	Enter the same password again for confirmation.

[Registration] How to Set and How to Operate

■ Managing Templates

- 📖 P.27 “Registering or editing public templates”
- 📖 P.28 “Registering or editing private templates”

□ Registering or editing public templates

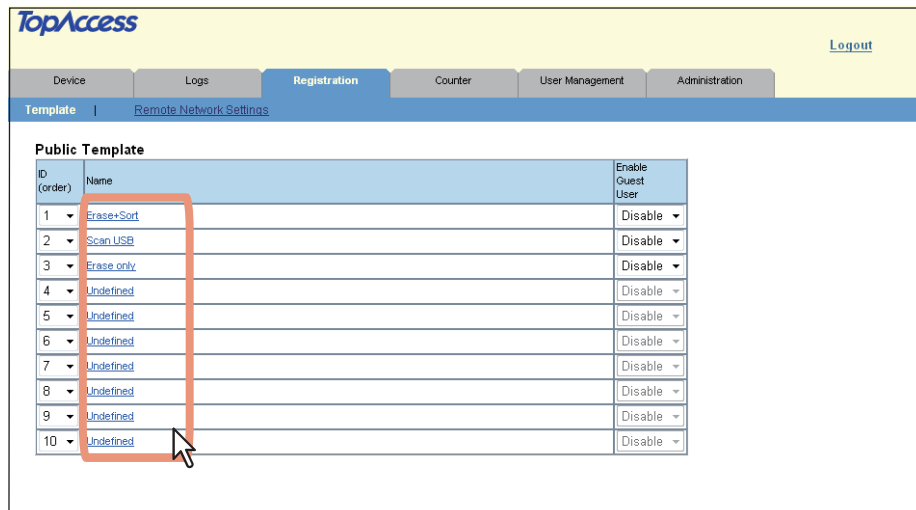
To define the public template, specify the public template name that will be displayed on the control panel and the agent settings.

Tip

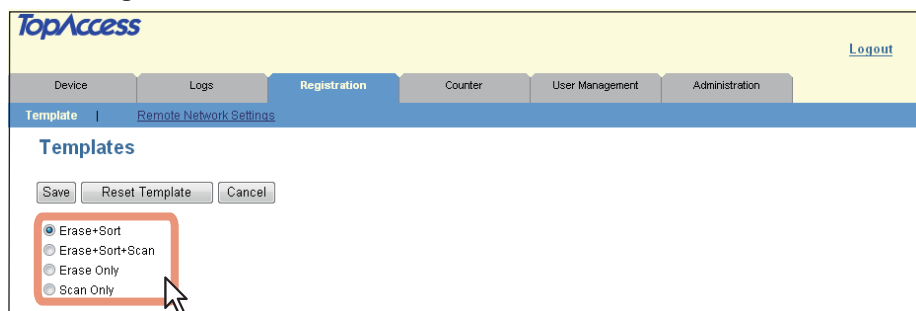
Public templates are created and managed by users who are granted administrator privileges in the access policy mode. See the following pages for how to access it:

- 📖 P.10 “Access Policy Mode”

- 1** Click the **[Registration]** tab.
The public template page is displayed.
- 2** Click the name of the public template you want to register or edit.



- 3** Enter the following items as required.
 - Select the agent.



On this page, you can set the following:

- 📖 P.20 “[Public Template] Screen/[Private Template] Screen”

- 4** Click **[Save]**.
- 5** Click **[OK]**.

□ Registering or editing private templates

To define the private template, specify the private template name that will be displayed on the control panel and the agent settings.

Tip

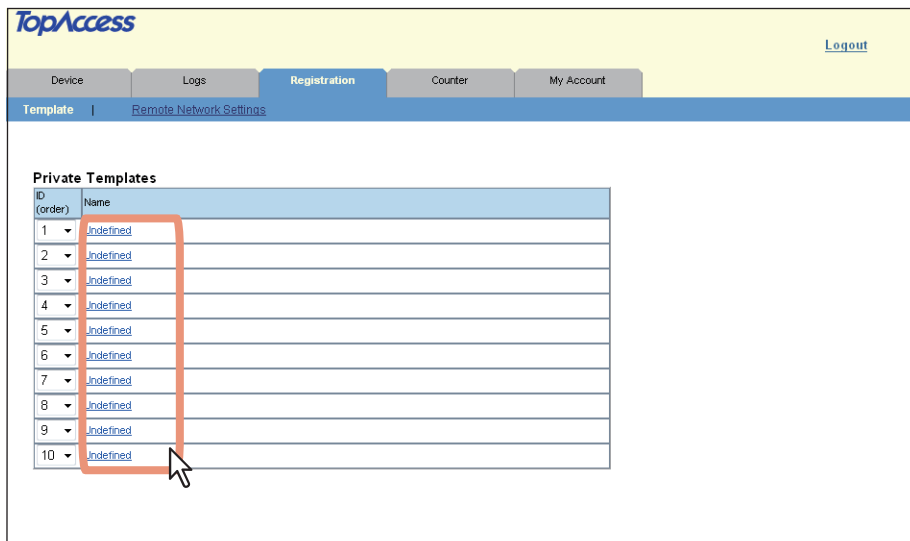
Private templates are created and managed by users who are granted user privileges in the access policy mode. See the following pages for how to access it:

📖 P.10 “Access Policy Mode”

1 Click the [Registration] tab.

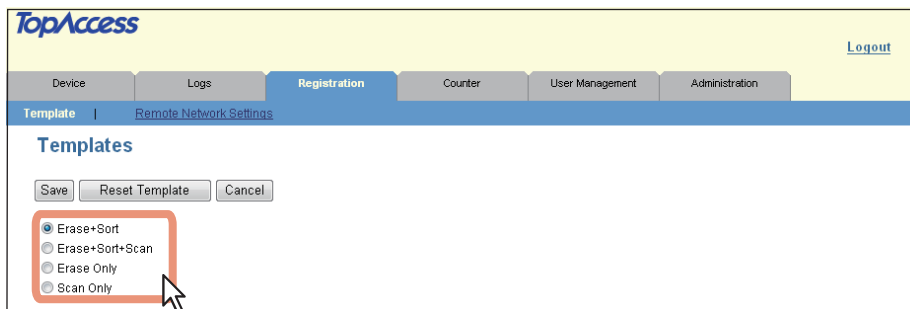
The private template page is displayed.

2 Click the name of the private template you want to register or edit.



3 Enter the following items as required.

- Select the agent.



On this page, you can set the following:

📖 P.20 “[Public Template] Screen/[Private Template] Screen”

4 Click [Save].

5 Click [OK].

[Counter] Tab Page

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

[Counter] Tab Page Overview	30
[Total Counter] Item List.....	30


[Counter] Tab Page Overview

You can export confirmation of the number of pages erased, scanned, and sorted (rejected or reused), as well as the counters in the [Counter] tab page.

 P.30 “[Total Counter] Item List”

■ [Total Counter] Item List

 P.30 “General”

 P.33 “Export”


□ General

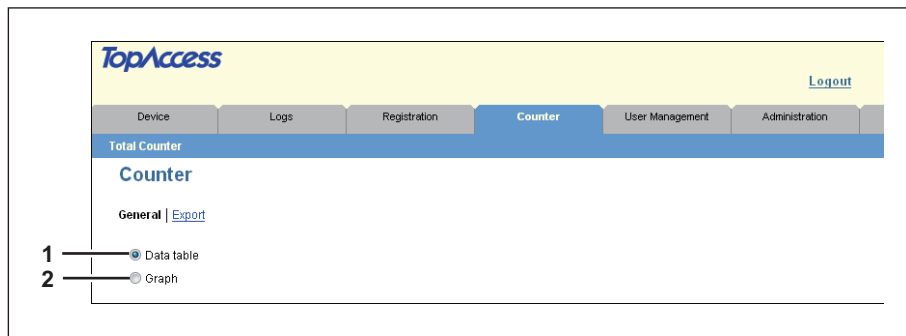
You can check counters in table or graph format.

Tip

When users who are granted administrator privileges in the access policy mode access this function, the total counter for the equipment is displayed. When guest users access this function, the total counter for the guest user is displayed.

See the following pages for how to access it:

 P.10 “Access Policy Mode”




	Item name	Description
1	Data table	Displays the counter in table format.
2	Graph	Displays the counter in graph format.

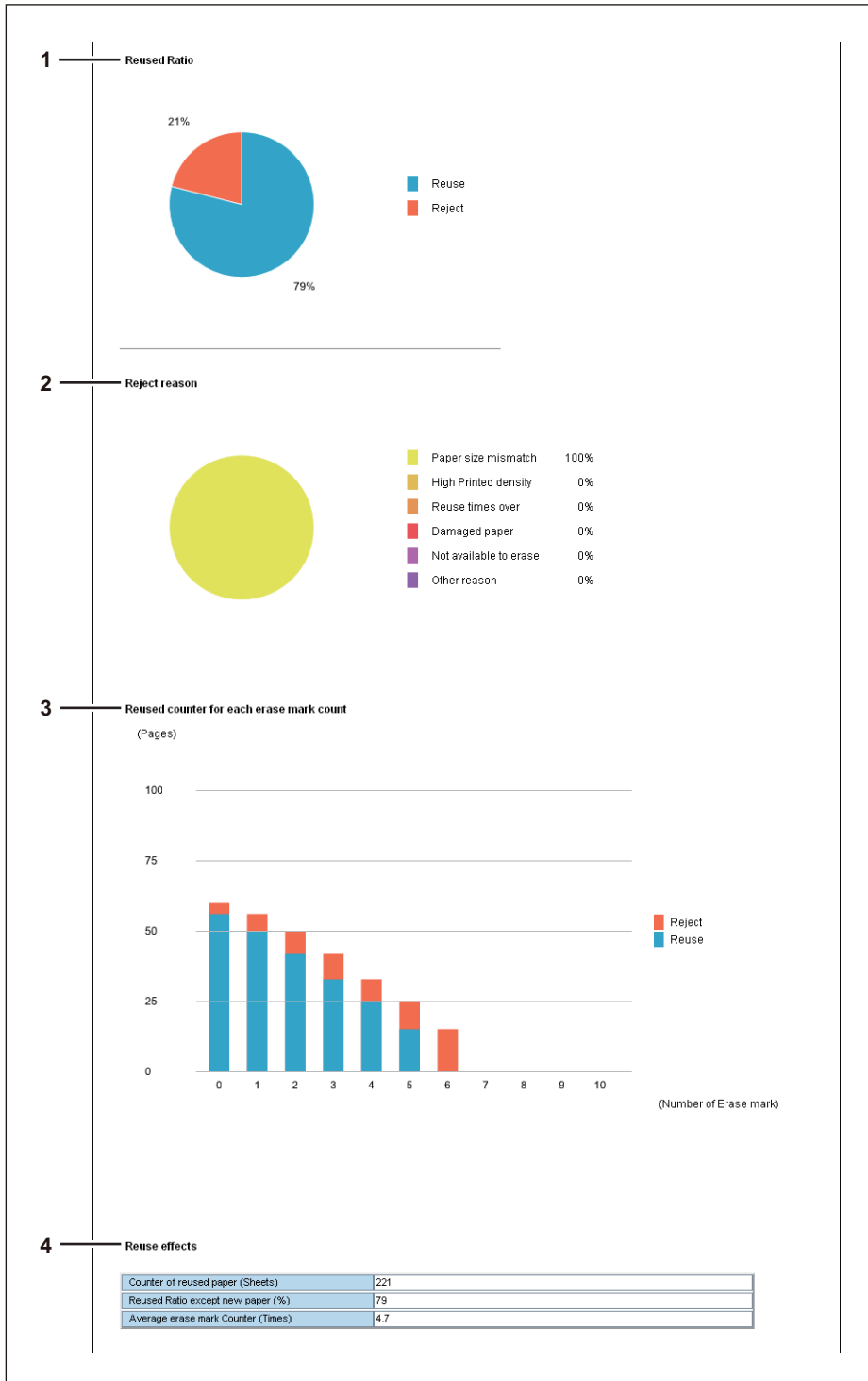
Data table

1	Erase Counter	Erase	281
2	Reuse counter	Reuse	221
3	Reject counter	Paper size mismatch	60
		High Printed density	0
		Reuse times over	0
		Damaged paper	0
		Not available to erase	0
		Other reason	0
		Total	60
4	Scan Counter	Scan	100
5	Reuse effects	Counter of reused paper (Sheets)	221
		Reused Ratio except new paper (%)	79
		Average erase mark Counter (Times)	4.7


5

	Item name	Description
1	Erase Counter	Displays the number of erased pages.
2	Reuse counter	Displays the number of pages that the sorter has determined can be reused.
3	Reject counter	Displays the number of pages that the sorter has determined cannot be reused.
4	Scan Counter	Displays the number of scanned pages.
5	Reuse effects	Displays the reuse effects.
	Note	To display the Reuse effects, you need to install ink cartridges and enable the Reuse Counter.  P.70 "Reuse Counter Settings"

Graph




	Item name	Description
1	Reused Ratio	Displays the reused ratio for paper as a pie chart.
2	Reject reason	Displays the reject reason for paper as a pie chart.
3	Reused counter for each erase mark count	Displays the number of rejected sheets of paper stamped with the reuse mark.
	Note	To display the number of rejected sheets of paper according to the reuse number, you need to install ink cartridges and enable the Reuse Counter. 📖 P.70 "Reuse Counter Settings"

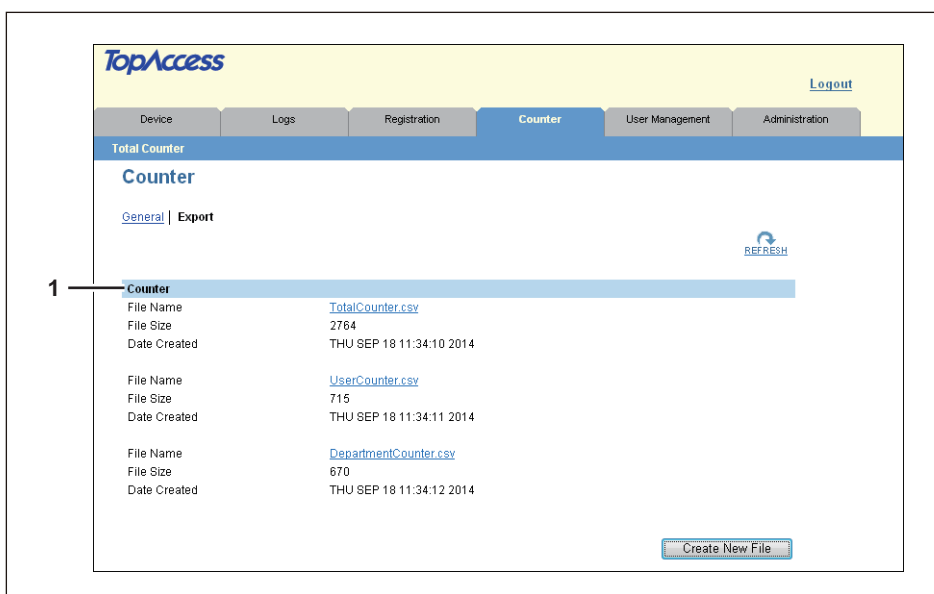
	Item name	Description
4	Reuse effects	Displays the reuse effects.
	<div style="background-color: #333; color: white; padding: 2px; display: inline-block;">Note</div> To display the Reuse effects, you need to install ink cartridges and enable the Reuse Counter.  P.70 "Reuse Counter Settings"	

❑ Export

You can export the counter as a file.

Tips

- Users who are granted administrator privileges in the access policy mode can access the counter export page from the [Counter] tab.
See the following pages for how to access it:
 P.10 "Access Policy Mode"
- Data is exported in CSV format.






	Item name	Description
1	Counter	You can export (download) the counter as a file. Create New File — Creates a file. You can display or download by clicking the created file.

[User Management] Tab Page

This chapter describes how to manage users in TopAccess.





[User Management] Tab Page Overview	36
[User Accounts] Item List.....	36
[Department Management] Item List	40
[Export/Import] Item List	43

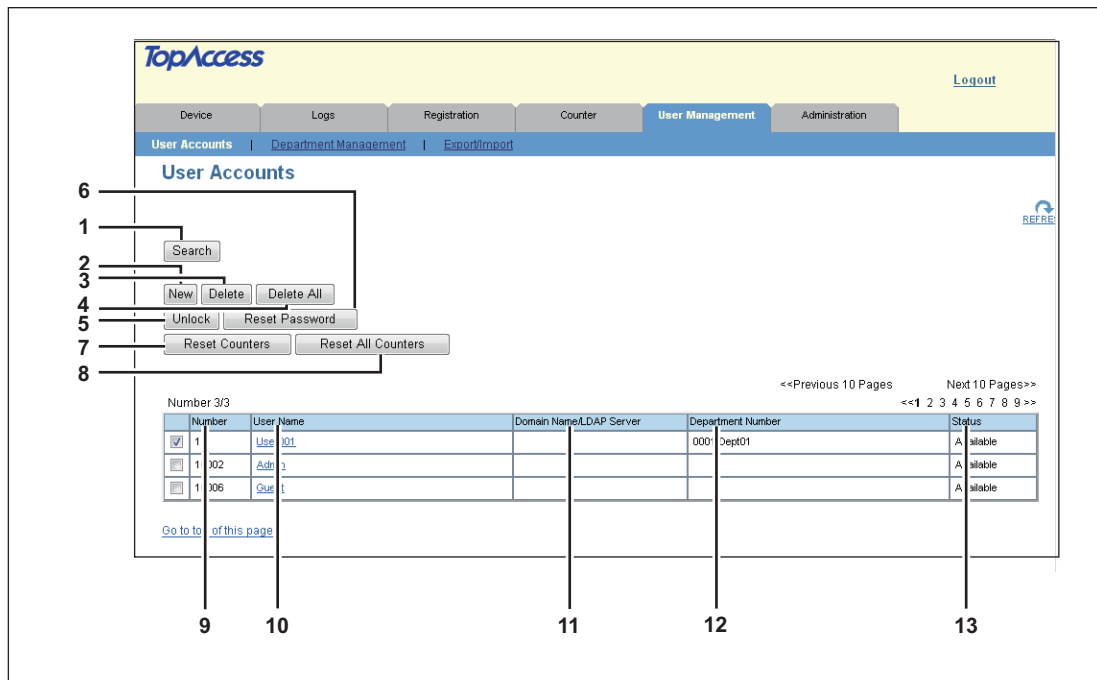
[User Management] Tab Page Overview





-  P.36 “[User Accounts] Item List”
-  P.40 “[Department Management] Item List”
-  P.43 “[Export/Import] Item List”

■ [User Accounts] Item List

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

-  P.37 “[Search User Account] screen”
-  P.37 “[Create User Information] screen”
-  P.38 “[Enter Password] screen”
-  P.39 “[User Information] screen”



	Item name	Description
1	[Search] button	Searches registered users.  P.37 “[Search User Account] screen”
2	[New] button	Registers new users.  P.37 “[Create User Information] screen”
3	[Delete] button	Deletes the user selected in the user account list. However, you cannot delete the default users.
4	[Delete All] button	Deletes all registered users. (Except default users)
5	[Unlock] button	Unlocks a locked user selected in the user account list.
6	[Reset Password] button	Resets the password of the user selected in the user account list.  P.38 “[Enter Password] screen”
7	[Reset Counters] button	Resets counters for the user selected in the user account list.
8	[Reset All Counters] button	Resets counters for all departments.
9	Number	Displays the registration number of the user. 10002 and 10006 are assigned to default users.
10	User Name	Displays the user name. Admin is the default user. You can check the user information by clicking the user name.  P.39 “[User Information] screen”
11	Domain Name/LDAP Server	Displays the domain name or LDAP server registered in the user information.
12	Department Number	Displays the department number registered in the user information.

	Item name	Description
13	Status	Displays the user status.

□ [Search User Account] screen

You can search registered users.



Select items to be searched and enter or select the search conditions.

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

□ [Create User Information] screen

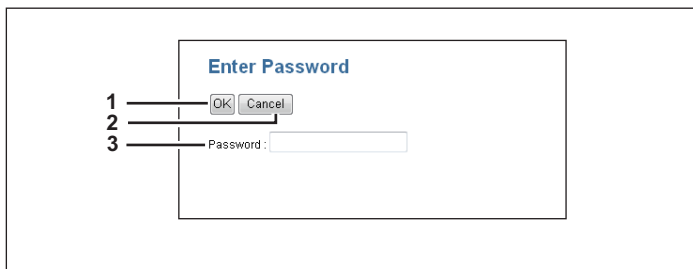
You can register new user information.

	Item name	Description
1	[Save] button	Saves the entered user information.
2	[Cancel] button	Cancels creating user information.
3	User Name	Enter the user name. You can enter up to 128 alphanumerical characters and symbols (! # \$ % & - , @ ^ _).

	Item name	Description
4	Domain Name/LDAP Server	Select the domain name or LDAP server.
5	Authentication Method	Select the user authentication method. <ul style="list-style-type: none"> • MFP Local Authentication — Use MFP local authentication on the equipment. • Windows Domain Authentication — Use network authentication managed by the Windows domain. • LDAP Authentication — Use network authentication managed by LDAP.
6	Password	Enter the password. You can enter up to 64 alphanumeric characters and symbols (! # () * + , - . / : ; = ? @ ^ _ ` { } ~).
	<div style="border: 1px solid gray; padding: 2px; width: fit-content;">Tip</div> <p>For MFP Local Authentication, the authentication method can also use symbols "\".</p>	
7	[Generate Pin] button	Generates a PIN code automatically.
	<div style="border: 1px solid gray; padding: 2px; width: fit-content;">Notes</div> <ul style="list-style-type: none"> • The PIN code is a number of up to 32 digits (0 to 9). The number of digits for the PIN code can be set with [Administration] - [Security] - [Password Policy].  P.79 “Setting up PIN Authentication” • When you use the PIN code for the Windows domain authentication or LDAP authentication, the unique PIN code should be assigned for all users. 	
8	Role Assignment	Select the user role.
9	Department Number	Select from the registered departments.  P.40 “[Department Management] Item List”

□ [Enter Password] screen

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



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

□ [User Information] screen

You can update registered user information.

The screenshot shows the 'User Information' screen with the following elements and callouts:


- 1**: Title bar 'User Information'
- 2**: [Save] button
- 3**: [Cancel] button
- 4**: [Delete] button
- 4**: [Reset Counters] button
- 5**: User Name field (displaying 'User001')
- 6**: Domain Name/LDAP Server dropdown
- 7**: Authentication Method dropdown (displaying 'MFP Local Authentication')
- 8**: Password field (displaying masked characters)
- 9**: [Generate Pin] button
- 10**: Role Assignment dropdown (displaying 'User')
- 11**: Department Number dropdown
- 12**: Erase Counter field (displaying '0')
- 13**: Reuse counter field (displaying '0')
- 14**: Reject counter table with rows: Paper size mismatch (0), High Printed density (0), Reuse times over (0), Damaged paper (0), Not available to erase (0), Other reason (0), Total (0)
- 15**: Scan Counter field (displaying '0')

	Item name	Description
1	[Save] button	Saves the entered user information.
2	[Cancel] button	Cancels changing user information.
3	[Delete] button	Deletes the displayed user from the user account.
4	[Reset Counters] button	Resets counters.
5	User Name	Displays the user name.
	Note	If you change any settings, the changes will be reflected from the next time you log in.
6	Domain Name/LDAP Server	Displays the registered domain name or LDAP server. Select this item if you want to change. You can select this item only when the authentication method is [Windows Domain Authentication] or [LDAP Authentication].
7	Authentication Method	Displays the user authentication method. <ul style="list-style-type: none"> • MFP Local Authentication — Use MFP local authentication in the equipment. • Windows Domain Authentication — Use network authentication managed by the Windows domain. • LDAP Authentication — Use network authentication managed by LDAP.
8	Password	Changes the password.
	Note	If you change any settings, the changes will be reflected from the next time you log in.
9	[Generate Pin] button	Generates a pin code automatically.
10	Role Assignment	Select the user role.
11	Department Number	Displays the registered departments. Select this item if you want to change. P.40 “[Department Management] Item List”

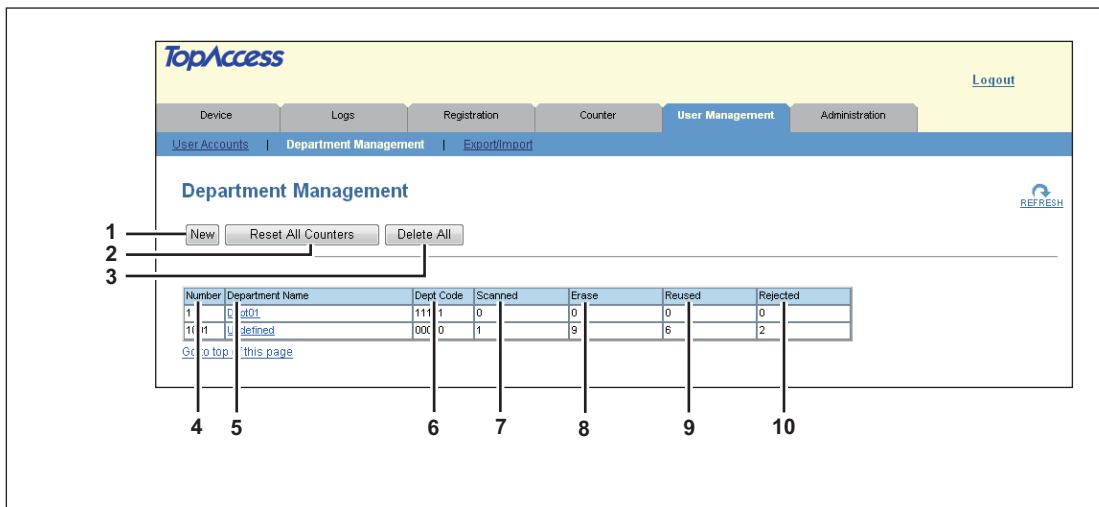
	Item name	Description
12	Erase Counter	Displays the number of erased pages.
13	Reuse counter	Displays the number of pages that the sorter has determined can be reused.
14	Reject counter	Displays the number of pages that the sorter has determined cannot be reused.
15	Scan Counter	Displays the number of scanned pages.



■ [Department Management] Item List

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

 P.41 “[Department Information] screen”

 P.41 “[Department Information] (Edit) screen”



	Item name	Description
1	[New] button	Allows you to add a new department.  P.41 “[Department Information] screen”
2	[Reset All Counters] button	Resets counters for all departments.
3	[Delete All] button	Deletes the registered department.
4	Number	Displays the registration number of the department.
5	Department Name	Displays the department name. Click a department name link to check the department management information.  P.41 “[Department Information] (Edit) screen”
6	Dept Code	Displays the department code.
7	Scanned	Displays the number of scanned sheets of the department.
8	Erase	Displays the number of erased sheets of the department.
9	Reused	Displays the number of reused sheets of the department.
10	Rejected	Displays the number of rejected sheets of the department.

□ [Department Information] screen

You can register a new department.

	Item name	Description
1	[Save] button	Saves the entered department information.
2	[Cancel] button	Cancels creating the department.
3	Department Name	Enter the department name. You can enter up to 20 characters.
4	Department Code	Enter the department code. You can enter up to 63 characters.

6

□ [Department Information] (Edit) screen

You can confirm and edit department information.

	Item name	Description
1	[Save] button	Saves the entered department information.
2	[Cancel] button	Cancels editing the department.
3	[Reset Counters] button	Resets counters.
4	[Delete] button	Deletes the displayed department.
5	Department Number	Displays the registration number of the department.
6	Department Name	Enter if changing the department name. You can enter up to 20 characters and symbols (! # \$ % & - . @ ^ _ ' () ` { } ~).
7	Department Code	Enter if changing the department code. You can enter up to 63 characters.

	Item name	Description
8	Erase Counter	Displays the number of erased pages.
9	Reuse counter	Displays the number of pages that the sorter has determined can be reused.
10	Reject counter	Displays the number of pages that the sorter has determined cannot be reused.
11	Scan Counter	Displays the number of scanned pages.

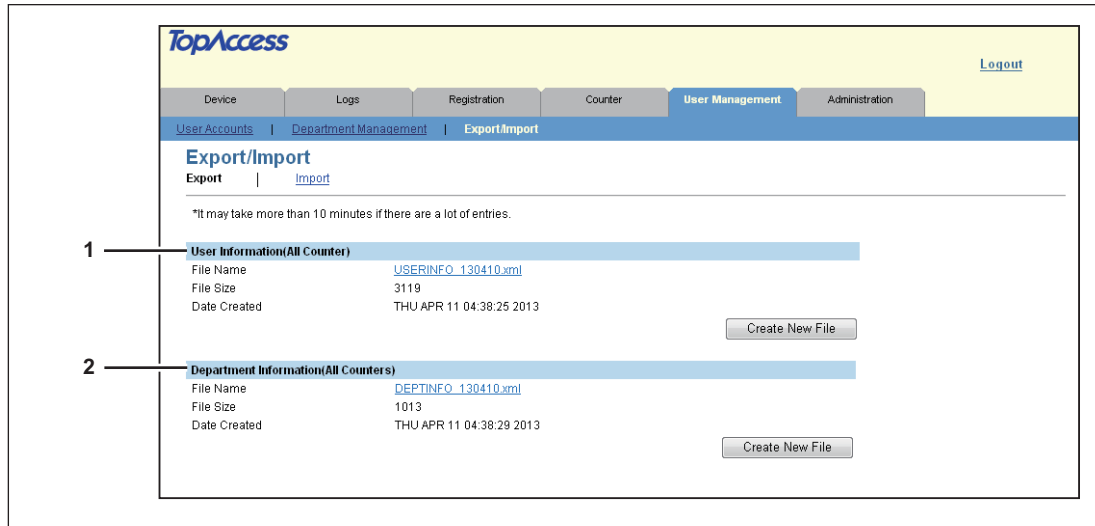
■ [Export/Import] Item List

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

📖 P.43 “Export”

📖 P.44 “Import”

☐ Export



	Item name	Description
1	User Information(All Counter)	You can create an export file for User Information(All Counter). Click the [Create New File] button to create the file. The file name, file size, and created date are displayed if you have already created a file. Click the file name and follow the displayed dialog messages when exporting.
2	Department Information(All Counters)	You can create an export file for Department Information(All Counters). Click the [Create New File] button to create the file. The file name, file size, and created date are displayed if you have already created a file. Click the file name and follow the displayed dialog messages when exporting.
	<div style="border: 1px solid gray; padding: 2px; width: fit-content;">Tip</div> <p>You can use exported files to import "Department Code" and "Department Counter" using [Import] - [Department Information(All Counters)].</p> <p>📖 P.44 “Import”</p>	

□ Import

1 → **User Information(All Counter)**

File Name

2 → **Department Information(All Counters)**

Import Method: Overwrite Addition Addition and Clear Counter

File Name

*Counters of all departments will be cleared if you select "Addition and ClearCounter" and import.

	Item name	Description
1	User Information(All Counter)	You can import user information from a file. Click the [Browse...] button to select the file to import and click [Open]. Check the file name and click the [Import] button.
2	Department Information(All Counters)	You can import department code from a file. Click the [Browse...] button to select the file to import and click [Open]. Select the import method among [Overwrite], [Addition] or [Overwrite and Clear Counter], and then click the [Import] button.

[Administration] Tab Page

This chapter describes how to use administration functions to make device settings and network settings from the TopAccess access policy mode.









[Setup] Item List	46
General Settings.....	46
Network Settings	51
Management Scan Settings	68
Reuse Counter Settings	70
Judgement Settings.....	70
Off Device Customization Architecture Setting.....	71
Version	72
[Security] Item List	73
Authentication.....	73
Certificate Management Settings	77
Password Policy Settings	79
[Security] How to Set and How to Operate	82
Creating/Exporting a Self-signed Certificate	82
Creating a Client Certificate/Exporting	84
[Maintenance] Item List	86
Import	86
Export	87
Create Clone File	88
Install Clone File.....	89
Directory Service Settings	91
System Updates	93
Languages.....	94
Reboot Settings	94

[Setup] Item List

Tip

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

See the following pages for how to access it:

-  P.10 "Access Policy Mode"
-  P.46 "General Settings"
-  P.51 "Network Settings"
-  P.68 "Management Scan Settings"
-  P.70 "Reuse Counter Settings"
-  P.70 "Judgement Settings"
-  P.71 "Off Device Customization Architecture Setting"
-  P.72 "Version"










■ General Settings

You can configure general settings such as Device Information, Energy Save, Date and Time, and Web General Setting.

Tip

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

See the following pages for how to access it and information on the [Setup] menu:

-  P.10 "Access Policy Mode"
-  P.46 "[Setup] Item List"
-  P.47 "Setting up Device Information"
-  P.47 "Setting up Functions"
-  P.48 "Setting up Energy Save"
-  P.48 "Setting up Date & Time"
-  P.48 "Setting up SNTP Service"
-  P.49 "Setting up Daylight Savings Time Setting"
-  P.50 "Setting up WEB General Setting"

□ Setting up Device Information

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

	Item name	Description
1	Name	Displays the device name of this equipment.
2	Device Model	Displays the model name of this equipment.
3	Serial Number	Displays the serial number of this equipment.
4	MAC Address	Displays the MAC Address of this equipment.
5	Location	Enter the installed location of this equipment. This information is displayed on the TopAccess [Device] tab page.
6	Contact Information	Enter the name of the person who is responsible for this equipment. This information is displayed on the TopAccess [Device] tab page.
7	Service Phone Number	Enter the telephone number of the person who is responsible for servicing this equipment. This information is displayed on the TopAccess [Device] tab page.
8	Administrative Message	Enter the message to the users about this equipment. This information is displayed on the TopAccess [Device] tab page.

□ Setting up Functions

You can set up the functions of this equipment.

	Item name	Description
1	Scan to USB	Select whether to enable or disable saving of scanned data to USB media.
2	Auto Job Resume	Select whether to automatically resume the job after an error.
3	Maximum scan pages for SlimPDF	Select the maximum number of sheets usable in a job when saving the scanned data to a Slim PDF. The default setting is 30 sheets.

□ Setting up Energy Save

You can set the Energy Save mode.

For the types of energy saving modes and procedures for entering each mode, refer to the *User's Guide*.

	Item name	Description
1	Auto Clear	Select how long this equipment remains inactive before the LCD screen returns to its default display.
2	Auto Power Save	Select how long this equipment remains inactive before it enters the Automatic Energy Save mode.

□ Setting up Date & Time

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

Tip


[Date & Time] settings are not available if the SNTP function is enabled.

	Item name	Description
1	Year/Month/Day/Hours/Minutes	Select the year and month in designated boxes. Also, enter the day/hours/minutes in the designated boxes.
2	Time Zone	Select the time zone where this equipment is located.

□ Setting up SNTP Service

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

	Item name	Description
1	Enable SNTP	Select whether to enable or disable SNTP (Simple Network Time Protocol). When this is enabled, the time settings of this equipment can be adjusted using the SNTP service.
	<p>Tip</p> <p>[Date & Time] settings are not available if enabled.</p>	
2	Primary SNTP Address	Enter the IP address or FQDN (Fully Qualified Domain Name) of the Primary SNTP Address when [Enable SNTP] is enabled.

	Item name	Description
3	Secondary SNTP Address	Enter the IP address or FQDN (Fully Qualified Domain Name) of the Secondary SNTP Address when [Enable SNTP] is enabled as required.
	<div style="background-color: #e0e0e0; padding: 2px;">Tip</div> <p>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> <p> P.52 "Setting up TCP/IP"</p>	
4	Scan Rate	Enter how often this equipment should access the SNTP server to check the time.
5	Port Number	Enter the port number for the SNTP service. Generally "123" is used.

□ Setting up Daylight Savings Time Setting

You can make the required settings for daylight savings time.

The screenshot shows the 'Daylight Savings Time Setting' configuration window. It includes the following elements:


- 1 Daylight Savings Time:** A dropdown menu set to 'Enable'.
- 2 Offset:** A dropdown menu set to '+1:00'.
- 3 Dates:** Two rows of fields for 'Start' and 'End'. Each row has dropdowns for 'Month' (Jan), 'Week' (1st), 'Day of Week' (Sun), and 'Time' (00:00).

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

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.

Notes

- Select the Start and the End dates and times based on the time set for the equipment.
 P.48 "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 session timer for TopAccess.

	Item name	Description
1	Session Timer	Enter how long you want this equipment to preserve the session data of TopAccess. You can enter any integer between 5 to 999. "10" is set as the default.

Tip


When logged in the access policy mode, you will be automatically logged out if the session timer elapses without any operation being performed.


■ Network Settings

You can configure the network settings for this equipment.

Tip

The [Network] submenu can be accessed from the [Setup] menu on the [Administration] tab. See the following pages for how to access it and information on the [Setup] menu:

 P.10 "Access Policy Mode"

 P.46 "[Setup] Item List"

 P.52 "Setting up TCP/IP"

 P.54 "Setting up Filtering"

 P.55 "Setting up IPv6"

 P.57 "Setting up Bonjour"


 P.57 "Setting up DNS"


 P.58 "Setting up DDNS"

 P.60 "Setting up SMB"

 P.61 "Setting up HTTP"

 P.63 "Setting up SNMP Network Service"

 P.66 "Setting up Proxy Setting"

 P.66 "Setting up Wake Up Setting"

□ Setting up TCP/IP

You can set the TCP/IP protocol to enable communication over TCP/IP.

	Item name	Description
1	Ethernet Speed Duplex Mode	Select the ethernet speed. [Auto] is set as the default.
	<p>Notes</p> <ul style="list-style-type: none"> When you select a specific ethernet speed, you must choose 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	Host Name	Assign the host name for this equipment. You can enter up to 63 alphanumerical characters including hyphens (-) and periods (.). You cannot use a "-" (hyphen) as the first and last character. The model name is set as the default.
3	Address Mode	<p>Select how to set the IP address.</p> <ul style="list-style-type: none"> Static IP — Select this to assign the static IP address manually. When this is selected, enter the static IP address in the [IP Address] box. Dynamic — Select this to assign the IP address using the DHCP with Auto-IP addressing enabled. The IP address, subnet mask, gateway address, primary WINS server address, and secondary WINS server address can be automatically acquired from the DHCP server if the network supports DHCP. However, use the AutoIP function to assign an IP address if the network does not support DHCP. No AutoIP — Select this to assign the IP address using the DHCP with Auto-IP addressing disabled. The IP address, subnet mask, gateway address, primary WINS server address, and secondary WINS server address can be automatically acquired from the DHCP server if the network supports DHCP. The previous IP address is used if the communication with the DHCP cannot be established.
4	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. [Enable] is set as the default.
	<p>Note</p> <p>When the DHCP server does not have a domain name, the data are left blank in the domain name even if you set the correct domain name manually in the DDNS Session. In that case, select [Disable] here and set the correct domain name in the DDNS Session.</p> <p> P.58 "Setting up DDNS"</p>	

	Item name	Description
5	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. [Enable] is set as the default.
	Note	When the DHCP server does not have 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 ones 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.57 "Setting up DNS"
6	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. [Enable] is set as the default.
	Note	When the DHCP server does not have 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 ones 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.60 "Setting up SMB"
7	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. [Disable] is set as the default.
	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 one 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.48 "Setting up SNTP Service"
8	IP Conflict Detect	Specify whether or not to detect IP address conflicts. Select [Enable] to display a message on the control panel when an IP address conflict is detected. [Enable] is set as the default.
9	IP Address	Enter the static IP address for the equipment when [Static IP] is selected in the [Address Mode] box. Specify within the range from 1 to 126 and 128 to 223 for the 1st octet, 0 to 255 for the 2nd to 4th octet.
	Note	If the IP address is "0.0.0.0" when it is set, an IP address conflict will occur. Specify a different IP address.
10	Subnet Mask	Enter the subnet mask if required when [Static IP] is selected in the [Address Mode] box. Specify within a range from 0.0.0.0 to 255.255.255.255. However, you cannot set 0.0.0.0 and 255.255.255.255.
11	Default Gateway	Enter the gateway address if required when [Static IP] is selected in the [Address Mode] box. Specify within a range from 0.0.0.0 to 255.255.255.255. However, you cannot set 0.0.0.0 and 255.255.255.255.

□ 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.

	Item name	Description
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 the conditions set in [IP Filtering Rule]. [Disable] is set as the default.
	Note	IP filtering is valid only in a network environment implemented with IPv4. It is not available in an IPv6 network environment. If you need to use IP address filtering under IPv6 environment, select MAC address filtering.
2	IP Filtering Rule	Select IP address filtering rules. <ul style="list-style-type: none"> • Permit — Select this to permit access from devices on a network to which the IP address (specified in [IP Filtering]) is set. • Deny — Select this to deny access from devices to which the specified IP address is set.
3	IP Filtering	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.

	Item name	Description
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 the conditions set in [MAC Address Filtering Rule]. [Disable] is set as the default.
5	MAC Address Filtering Rule	Select MAC address filtering rules. <ul style="list-style-type: none"> • Permit — Select this to permit access from devices on a network to which the MAC address (specified in [MAC Address Filtering]) is set. • Deny — Select this to deny access from devices to which the specified MAC address is set.
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.

	Item name	Description
1	Enable IPv6	Select whether the IPv6 protocol is enabled or disabled. [Disable] is set as the default.
2	Link Local Address	Displays the unique IP address generated automatically for use with IPv6.

	Item name	Description
3	Manual	<p>You assign the IPv6 address, prefix and default gateway manually. In this mode, you can assign one IPv6 address to this equipment.</p> <p>IP Address — Assign the IPv6 address for this equipment. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>Prefix Length — Assign the prefix length for the IPv6 address. Specify within a range from 0 to 128. "0" is set as the default.</p> <p>Gateway — Assign the default gateway address. Specify within the range from 1:0:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.</p> <p>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.</p>
	<p>Tips</p> <ul style="list-style-type: none"> • When [Manual] is selected, a stateful address cannot be set. • If the selected IPv6 address is already assigned, DAD (Duplicate Address Detection) detects it and notifies you on the LCD screen of this equipment. 	
4	Use Stateless Address	<p>Use the IPv6 addresses (Stateless addresses) issued from routers.</p> <ul style="list-style-type: none"> • Use DHCPv6 Server for IP Address(M flag) — Use the IPv6 address issued from the DHCPv6 server in the stateless network environment. • Use DHCPv6 Server for options(O flag) — Use the optional information (IPv6 address for the DNS server, etc.) issued from the DHCPv6 server in the stateless network environment. • FQDN Option — The FQDN option is available if Use DHCPv6 Server for IP Address acquisition is selected. Select [Server] or [Client] for [Update Method] if using the FQDN option. [Server] is set as the default. • IP Address — Stateless Addresses obtained from routers are displayed. Up to 7 IPv6 addresses can be retained.
	<p>Tip</p> <p>When this equipment receives a router advertisement (RA) from a router, of which the M flag configuration is "0", the DHCPv6 function is disabled. If you change the router advertisement (RA) M flag configuration from "0" to "1", it is necessary to reboot this equipment to enable the DHCPv6 function.</p>	
5	Use Stateful Address	<p>Use the Stateful address issued from DHCPv6 server.</p> <ul style="list-style-type: none"> • Use DHCPv6 Server for IP Address — Select whether or not the IPv6 address which is issued from the DHCPv6 server is used for this equipment. • Use DHCPv6 Server for options — Select whether or not the optional information (IPv6 address for the DNS server, etc.) except the IPv6 address for this equipment, which is issued from the DHCPv6 server is used on this equipment. • FQDN Option — The FQDN option is available if Use DHCPv6 Server for IP Address acquisition is selected. When FQDN Option is selected, select [Server] or [Client] as the [Update Method]. [Server] is set as the default. • IP Address — A stateful address, Prefix Length and Gateway obtained from DHCPv6 Server are displayed.

□ Setting up Bonjour

In Bonjour, you can enable or disable the Bonjour networking that is available for Mac OS X.

	Item name	Description
1	Enable Bonjour	Select whether Bonjour is enabled or disabled. [Enable] is set as the default.
2	Link-Local Host Name	Enter the DNS host name of this equipment. You can enter up to 127 alphanumeric characters and symbols (excluding = ; # \).
3	Service Name	Enter the device name of this equipment that will be displayed in the Bonjour network. You can enter up to 63 alphanumeric characters and symbols (excluding = ; # \).

7

□ Setting up DNS

In a 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 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.58 “Setting up DDNS”

	Item name	Description
1	Enable DNS	Select whether the DNS server is enabled or not. [Enable] is set as the default.
2	Primary DNS Server Address	Specify the IP address of the primary DNS server when the DNS service is enabled. Specify within a range from 0.0.0.0 to 255.255.255.255.
3	Secondary DNS Server Address	Specify the IP address of the secondary DNS server when the DNS service is enabled, as you require. Specify within a range from 0.0.0.0 to 255.255.255.255.
4	Primary DNS Server Address (IPv6)	Specify the IP address of the primary DNS server when the DNS service is enabled in IPv6. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
5	Secondary DNS Server Address(IPv6)	Specify the IP address of the secondary DNS server when the DNS service is enabled in IPv6, as required. Specify within the range from 1:0:0:0:0:0:0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Tip

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

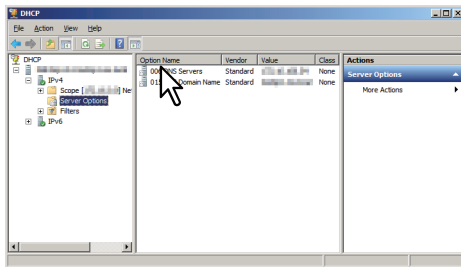
📖 P.52 "Setting up TCP/IP"

□ Setting up DDNS

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

Notes

- When using the security in DDNS, if the difference between the time set in the server, in which the 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 Scope Options or Server Options.

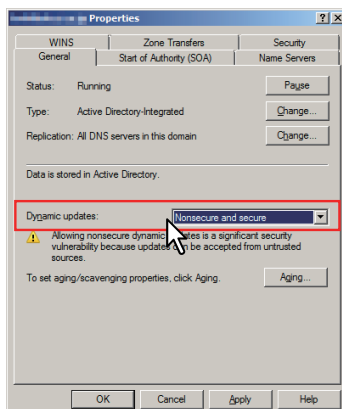


- When using DDNS, make sure the "Allow dynamic updates?" option is set to "Nonsecure and secure" (for Windows Server 2003/Windows 2008) for the Forward Lookup Zones and Reversed Lookup Zones.

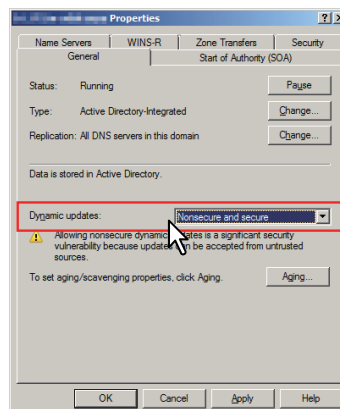
If the setting of Windows Server 2003/Windows Server 2008 is "Nonsecure and secure" for this DDNS function, you need to set the correct primary and secondary "login name" and "password" to update the DNS server using DDNS.

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 host name manually in the Forward and Reversed Lookup Zone.

Forward Lookup Zones
(Windows 2008 Server)



Reversed Lookup Zones
(Windows 2008 Server)



	Item name	Description
1	Enable DDNS	Select whether the dynamic DNS service is enabled or disabled. [Enable] is set as the default.
2	Domain Name	Enter the domain name that will be added to the DNS server using DDNS. You can enter up to 96 alphanumeric characters and symbols (excluding = ; # \).
	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.52 "Setting up TCP/IP"
3	Security Method	Enter the security method. <ul style="list-style-type: none"> • None Performs a nonsecure DDNS update. • 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 not uploaded, the security setting will be disabled. • SIG(0) Select this to perform a secure DDNS session using SIG(0). To select this, you must upload a key file and a private key file. If any of them is not uploaded, the security setting will be disabled.
4	Primary Login Name	Enter the primary login name if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumeric characters and symbols (excluding = ; # \).
5	Primary Password	Enter the primary password if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumeric characters and symbols (excluding = ; # \).
6	Secondary Login Name	Enter the secondary login name if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumeric characters and symbols (excluding = ; # \).

	Item name	Description
7	Secondary Password	Enter the secondary password if the security method selected in the above setting is GSS-TSIG. You can enter up to 128 alphanumerical characters and symbols (excluding = ; # \).
8	TSIG/SIG(0) Key file	Use this setting to upload or delete a key file to be used for TSIG and SIG (0). To upload it, click [Browse..] and specify a private key file to be uploaded, and then click [Upload]. To delete it, click [DELETE].
9	TSIG/SIG(0) Private Key file	Use this setting to upload or delete a private key file to be used for TSIG and SIG(0). To upload it, click [Browse..] and specify a private key file to be uploaded, and then click [Upload]. To delete it, click [DELETE].

□ Setting up SMB

In an SMB Session, access to this equipment through a Microsoft Windows Network is enabled. You can also specify the WINS server when it is used to enable Windows file sharing services between the different subnets.

	Item name	Description
1	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.52 "Setting up TCP/IP"
2	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.52 "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.

	Item name	Description
3	SMB Signing of SMB Client	<p>Select whether SMB Signing is enabled or disabled when this equipment accesses the clients using SMB, such as when this equipment stores the scanned data in the network folder using SMB.</p> <ul style="list-style-type: none"> • If server agrees, digital signature is done for the communication. — Select this to use the digital signature to secure the communication to an SMB server only when the SMB Signing of SMB Server that this equipment accesses is enabled. If the SMB Signing of SMB Server is disabled in an SMB server, communication is performed without the digital signature. • Digital signature is always done for the communication on the client side. — Select this to make this equipment always access an SMB server with a digital signature. When the SMB Signing of SMB Server is disabled in an SMB server, communication is not allowed. • Digital signature isn't done for the communication for the client. — Select this to communicate to an SMB server without the digital signature. If the SMB Signing of SMB Server is always enabled in an SMB server, communication is not allowed.
	<p>Notes</p> <ul style="list-style-type: none"> • If you do not know whether the SMB Signing of SMB Server is enabled or disabled in the SMB servers, it is recommended to select [If server agrees, digital signature is done for the communication.]. If this is set incorrectly, SMB communication may become unavailable. • A digital signature is always used for communication on the server side as the default on Windows Server 2003/Windows Server 2008. Therefore specify "If server agrees, digital signature is done for the communication." or "Digital signature is always done for communication on the client side." for SMB communications with a Windows Server 2003/Windows Server 2008. 	

□ Setting up HTTP

In the HTTP Network Service, you can enable or disable Web-based services such as TopAccess.

Note

When "Enable HTTP Server" or "Enable SSL" are set to [Disable], you cannot start TopAccess. Also if the port numbers for "Primary Port Number", "Secondary Port Number", and "SSL Port Number" are not recognized after they have been changed, you cannot start TopAccess. In this situation, contact your service representative, or see the **User's Guide** to reset the equipment to its factory defaults.

	Item name	Description
1	Enable HTTP Server	Select to enable Web-based services such as TopAccess. [Enable] is set as the default.
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. [Disable] is set as the default.
	<p>Note</p> <p>Not all operating systems support SSL for all protocols.</p>	

	Item name	Description
3	Primary Port Number	Enter the port number for the NIC HTTP server. You can enter a value in the range from 1 to 65535. Generally, the default value "80" is used.
4	Secondary Port Number	Enter the port number for the TopAccess. You can enter a value in the range from 1 to 65535. Generally, the default value "8080" is used.
5	SSL Port Number	Enter the port number for the SSL. You can enter a value in the range from 1 to 65535. Generally, the default value "10443" is used.

□ 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.

	Item name	Description
1	Enable SNMP V1/V2	Select whether the SNMP V1/V2 monitoring with MIB is enabled or disabled. [Enable] is set as the default.
2	Read Community	Enter the SNMP read community name for the SNMP access. You can enter up to 31 alphanumerical characters and symbols (excluding = ; # \). "public" is set as the default.
	Notes	<ul style="list-style-type: none"> It is recommended to change the default Read Community name for security reasons. If changing the Read Community name, match the setting with the applications in use. Otherwise, applications that use MIB (TopAccess) will become unavailable. When you leave the [Read Write Community] option blank, the SNMP communication between the SNMP Browser of the Client computer and this equipment will be disabled.
3	Read Write Community	Enter the SNMP Read Write community name for the SNMP access. You can enter up to 31 alphanumerical characters and symbols other than =, ; (semicolon), #, and \ (backslash). "private" is set as the default.
	Notes	<ul style="list-style-type: none"> It is recommended to change the default Read Write Community name for security reasons. If changing the Read Write Community name, match the setting with the applications in use. Otherwise, applications that use MIB (TopAccess) will become unavailable.
4	Enable SNMP V3	Select whether SNMP V3 monitoring with MIB is enabled or disabled. [Disable] is set as the default.
5	Create SNMP V3 User Information	SNMP V3 user information registered into this equipment is displayed in a list. SNMP V3 user information can be registered, edited, deleted.

	Item name	Description
6	Enable SNMP V3 Trap	Select whether SNMP V3 Trap is sent or not. [Disable] is set as the default.
7	SNMP V3 Trap User Name	Enter an SNMP V3 Trap User Name. You can enter up to 31 alphanumerical characters and symbols.
8	SNMP V3 Trap Authentication Protocol	Select an authentication protocol. <ul style="list-style-type: none"> • HMAC-MD5 — Select this to use HMAC-MD5. • HMAC-SHA — Select this to use HMAC-SHA.
9	SNMP V3 Trap Authentication Password	Enter an authentication password. You can enter up to 31 alphanumerical characters and symbols.
10	SNMP V3 Trap Privacy Protocol	Select a protocol for data encryption. <ul style="list-style-type: none"> • None — Select this not to encrypt data. • CBC-DES — Select this to use CBC-DES. • CFB-AES-128 — Select this to use AES-128 (CFB mode).
11	SNMP V3 Trap Privacy Password	Enter a privacy password. You can enter up to 31 alphanumerical characters and symbols.
12	Enable Authentication Trap	Select whether to send SNMP Traps when this equipment is accessed using SNMP V1/V2 from a different read community. [Enable] is set as the default.
13	Enable Alerts Trap	Select whether to send SNMP V1/V2 Traps when an alert condition occurs. [Enable] is set as the default.
14	IP Trap Address 1 to 10	Enter the IP address where the SNMP Traps will be sent. You can specify up to 10 addresses. Specify within the range from 0 0 0 0 to 255 255 255 255.
15	IP Trap Community	Enter the trap community name for the IP Traps. You can enter up to 31 alphanumerical characters and symbols. "public" is set as the default.

[Create SNMP V3 User Information] screen

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

Tip

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

	Item name	Description
1	Context Name	Displays the context name.
2	User Name	Enter the user name. You can enter up to 31 alphanumeric characters and symbols.
3	Authentication Protocol	Select an authentication protocol. <ul style="list-style-type: none"> • HMAC-MD5 — Select this to use HMAC-MD5. • HMAC-SHA — Select this to use HMAC-SHA.
4	Authentication Password	Enter the password when the Authentication option is enabled. You can enter up to 31 characters.
5	Privacy Protocol	Select a protocol for data encryption. <ul style="list-style-type: none"> • None — Select this not to encrypt data. • CBC-DES — Select this to use CBC-DES. • CFB-AES-128 — Select this to use AES-128 (CFB mode).
6	Privacy Password	Enter the password for the user information. You can enter up to 31 alphanumeric characters and symbols.
7	Permissions Level	Select the access permission level of the SNMP V3 user. <ul style="list-style-type: none"> • General User — Select this to permit only the reading of data. • Administrator — Select this to permit both the reading and writing of data.

□ Setting up Proxy Setting

You can make settings for proxy.

	Item name	Description
1	Enable Proxy	Select whether the proxy service is enabled or disabled. [Disable] is set as the default.
2	Proxy Server Address	When [Enable Proxy] is enabled, enter the address for the proxy server. You can enter alphanumerical characters and symbols (excluding - / _ : %).
3	Port Number	Enter the port number for the proxy server. The port number depends on the port setting in the proxy server. You can enter a value in a range of 1 to 65535.
4	Enable Authentication	Select whether connecting to the proxy server is enabled or disabled. [Disable] is set as the default.
5	User Name	Enter the user name to access the proxy server if proxy authentication is enabled. You can enter up to 16 alphanumerical characters and symbols (excluding / \ ; , * ? " < >).
6	Password	Enter the password to access the proxy server if proxy server authentication is enabled. You can enter up to 16 characters.

□ Setting up Wake Up Setting


This section describes how to set network access during the Energy Save mode.

Use this setting for situations such as when you want to wake this equipment from the Energy Save mode by searching for it this equipment over a network.

Note

This setting can only be enabled when "Enable" is selected as the Energy Save setting. If this is not selected, the Wake Up setting is disabled because this equipment does not enter the Energy Save mode.

P.48 "Setting up Energy Save"

	Item name	Description
1	Wake Up Conditions	Select protocols to be used for recovering this equipment from the Energy Save mode. Up to 4 protocols can be selected. <ul style="list-style-type: none"> • ARP • HTTP/ODCA • Wake on Magic Packet • IPv6 settings
	<p>Note</p> <p>For [IPv6 settings], select items in compliance with the [IPv6] settings.  P.55 "Setting up IPv6"</p>	

Note

When no response is returned from this equipment after you access the network even if a protocol selected on this setting is used, reattempt the access.

■ Management Scan Settings

The Management Scan function allows you to scan paper for all jobs regardless of the template settings.

□ Management Scan

You can configure the Management Scan function.

	Item name	Description
1	Enable Management Scan	Select this to use the Management Scan function.
	Note	Selecting [Enable Management Scan] disables [Erase Only Mode].
2	Erase Only Mode	Set whether or not to allow erasing only. [Enable] is set as the default.

□ Folder Name

You can set the name of the folder in which scanned data are saved.

	Item name	Description
1	Folder Name Setting	Set whether or not the data are saved to a folder and the file name when saved. <ul style="list-style-type: none"> • None — Select this if you do not want to use a folder. • Add Device Name — Add the device name. • Add UserName — Add the user name.

□ Format

You can set the file name and the file format.

	Item name	Description
1	File Name Format	You can set the file name by combining the following items. <ul style="list-style-type: none"> • Device Name • Date • Page

□ Save as file Setting

You can set the destination path.

Note

When the scan function defined in a template is used, setting items from [Color] onwards are disabled.

	Item name	Description
1	Protocol	Select the protocol. <ul style="list-style-type: none"> SMB — Uses SMB as the protocol. WebDAV — Uses WebDAV as the protocol.
2	Server Name	When WebDAV is selected as the protocol, enter the server name. You can enter up to 64 alphanumerical characters and symbols (- . / _ : %).
3	Port Number(Command)	When WebDAV is selected as the protocol, enter the port number. You can enter a value in the range from 0 to 65535 using numbers and hyphens (-). "-" is set as the default.
4	Network Path	Enter the network path for the destination path. You can enter up to 128 alphanumerical characters and symbols (excluding ; * ? " < >).
5	Login User Name	Enter the login user name to access the destination path if required. You can enter up to 32 alphanumerical characters and symbols (excluding : ; * ? " < > ').
6	Password	Enter the password to access the destination path if required. You can enter up to 32 alphanumerical characters, symbols, and spaces. You can also enter a single space only.
7	Retype Password	Enter the same password again for a confirmation.
8	Color	Select the color mode for scanning. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Tip</p> <p>We recommend that you select "B&W (blue)" when scanning paper printed in B&W on the e-STUDIO306LP/307LP.</p> </div>
9	File Format	Select the file format to which the received document will be converted. <ul style="list-style-type: none"> TIFF (Single) — Select this to save scanned images separately as Single-page TIFF files. PDF (Single) — Select this to save scanned images separately as Single-page PDF files. JPEG — Select this to save scanned images as JPEG files. <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>JPEG is available when "Color" or "Gray" is selected for [Color].</p> </div>
10	Resolution	Select the resolution for scanning.
11	Compression	Select the compression for scanning.

	Item name	Description
12	Single/2-Sided Scan	In management scan, only "Duplex Book" is available.

■ Reuse Counter Settings

You can make settings for the reuse counter function.

	Item name	Description
1	Mark Count Option	Set whether or not to use the reuse counter function. Reuse counter is a function that prints a reuse counter mark to be read by this equipment on a corner of the paper (lower left or upper right corner for A4/LT in landscape orientation) when it is reused. The paper is automatically rejected when it has been reused for a certain number of times (6 by default). [Disable] is set as the default. When this is enabled, install ink cartridges. See the User's Guide for information on supported ink cartridges.
	Notes	<ul style="list-style-type: none"> The reuse counter function can be used in templates including the erase and sort functions. You can only print a reuse counter mark on A4 (For North America: LT) size paper.
2	Mark Count	Set the maximum number (from 3 to 10) of reuse counter marks printed on the paper. "6" is set as the default.
3	Erase count mark position	Set the position of the paper where to print the reuse counter mark. Set this item when the reuse counter mark overlaps with the printing by e-STUDIO306LP/307LP, or a part of the reuse counter mark is missing because it falls outside the paper.

■ Judgement Settings

You can set the standards for rejecting paper when performing sorting.

	Item name	Description
1	Print density	Select the stain density to reject paper from 3 levels.
2	Printed dot size	Select the stain size to reject paper from 3 levels.
3	Broken size of paper	Select the folded or torn status to reject paper from 3 levels.

■ Off Device Customization Architecture Setting


You can set ODCA (Off Device Customization Architecture) when you are linking external application software to services provided by this equipment.

For details, refer to the application software manual.

Tip

The [ODCA] submenu can be accessed from the [Setup] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Setup] menu:

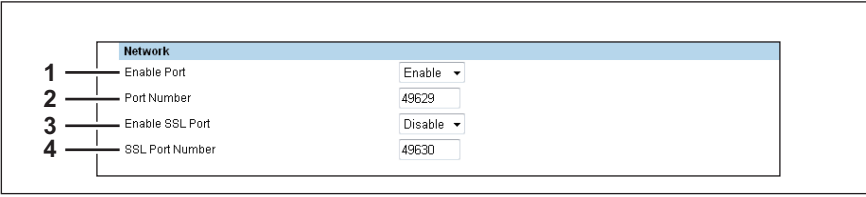
 P.10 "Access Policy Mode"

 P.46 "[Setup] Item List"

 P.71 "Network"

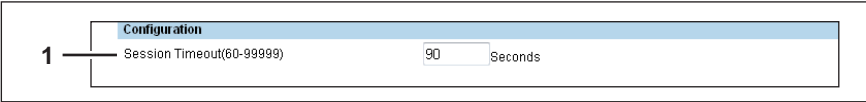
 P.71 "Configuration"

□ Network



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

□ Configuration




	Item name	Description
1	Session Timeout	Specify the duration to maintain the connection.


Version

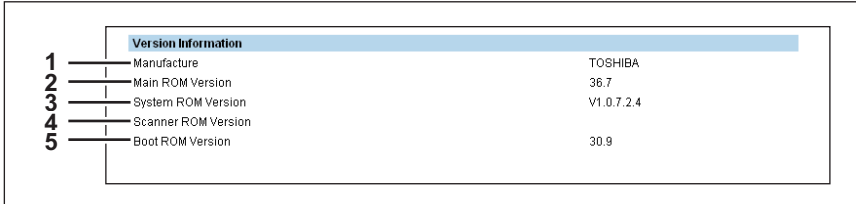
Displays version information of this equipment.

Tip

The [Version] submenu can be accessed from the [Setup] menu on the [Administration] tab. See the following pages for how to access it and information on the [Setup] menu:

 P.10 "Access Policy Mode"

 P.46 "[Setup] Item List"



Version Information	
1	Manufacture TOSHIBA
2	Main ROM Version 36.7
3	System ROM Version V1.0.7.2.4
4	Scanner ROM Version
5	Boot ROM Version 30.9


	Item name	Description
1	Manufacture	Displays the manufacturer name of this equipment.
2	Main ROM Version	Displays the main ROM version information of this equipment.
3	System ROM Version	Displays the system ROM version information of this equipment.
4	Scanner ROM Version	Displays the scanner ROM version information of this equipment.
5	Boot ROM Version	Displays the boot ROM version information of this equipment.

[Security] Item List

Tip

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

See the following pages for how to access it:

 P.10 "Access Policy Mode"

 P.73 "Authentication"

 P.77 "Certificate Management Settings"

 P.79 "Password Policy Settings"


■ Authentication


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


Tip

The [Authentication] submenu can be accessed from the [Security] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Security] menu:

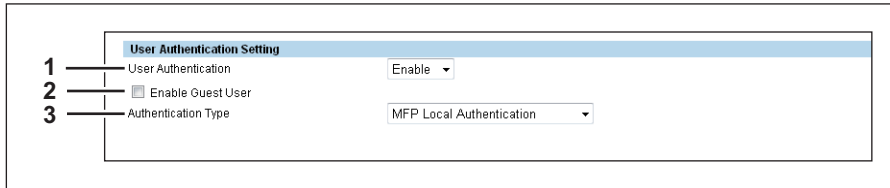
 P.10 "Access Policy Mode"

 P.73 "[Security] Item List"

 P.74 "Setting up User Authentication Setting"

□ Setting up User Authentication Setting

You can configure user authentication to access this equipment.



	Item name	Description
1	User Authentication	Select whether or not to enable user authentication. [Disable] is set as the default.
2	Enable Guest User	Enables operations by the guest user.
3	Authentication Type	<p>Select the authentication method.</p> <ul style="list-style-type: none"> <u>MFP Local Authentication</u> You can manage network users with the MFP local authentication of the equipment when you do not have a user authentication system in your environment. When MFP local authentication is enabled, users must enter the PIN code that is registered in the equipment to operate the control panel. <u>Windows Domain Authentication</u> You can manage network users with Windows domain authentication when you already manage your network using Windows domains. When Windows domain authentication is enabled and a card reader installed in the equipment, touching the card reader with the authentication card enables the user to perform operations from the control panel. For information on the card reader, contact your service representative. ⓘ P.75 “Windows Domain Authentication” <u>LDAP Authentication</u> You can manage network users with LDAP authentication when you already manage your network using LDAP. When LDAP authentication is enabled and a card reader installed in the equipment, touching the card reader with the authentication card enables the user to perform operations from the control panel. For information on the card reader, contact your service representative. ⓘ P.75 “LDAP Authentication”

Windows Domain Authentication

User Authentication Setting

User Authentication: Enable

Enable Guest User:

Authentication Type: Windows Domain Authentication

Windows Domain Authentication

Use NT Domain Server:

Primary	Domain Name	PDC	BDC
<input type="radio"/> Domain1			
<input type="radio"/> Domain2			
<input type="radio"/> Domain3			

Connection Timeout: PDC(1-180) _____ Seconds
*Reboot is necessary to reflect Connection Timeout.

	Item name	Description
1	Use NT Domain Server	Select this check box if you are managing the domain using the NT domain controller.
2	Domain 1 - Domain 3	Specify the domain you want to use for Windows domain authentication. Click one of the domains and specify the following items in the displayed screen to register the domain. Domain Name — Enter the domain name. PDC — Enter the server name or IP address of the Primary Domain Controller (PDC). You can enter up to 128 alphanumerical characters and symbols. BDC — Enter the server name or IP address of the Backup Domain Controller (BDC) as required. You can enter up to 128 alphanumerical characters and symbols.
3	Connection Timeout	Enter the timeout period for quitting communication when no response is received from the PDC or BDC server. Specify within the range from 1 to 180 seconds.

LDAP Authentication

User Authentication Setting

User Authentication: Enable

Enable Guest User:

Authentication Type: LDAP Authentication

Use NT Domain Server:

Primary	LDAP Server	Type	Attribute type of 'User Name'
<input type="radio"/> LDAP Server1			
<input type="radio"/> LDAP Server2			
<input type="radio"/> LDAP Server3			

Connection Timeout: PDC(1-180) _____ Seconds
*Reboot is necessary to reflect Connection Timeout.

	Item name	Description
1	LDAP Server1 - LDAP Server3	Select the LDAP server you want to use for LDAP authentication. Click one of the LDAP servers and specify the following items in the displayed screen to register the LDAP server. Windows Server — Select this when LDAP is running on a Windows server. LDAP Server (Other than Windows Server) — Select this when the LDAP is running on a server other than a Windows one. When this is selected, you have to specify the attribute type of 'User Name'.

□ PIN Authentication Setting

You can select the LDAP server you want to use for PIN authentication when "Windows Domain Authentication" or "LDAP Authentication" is selected for "Authentication Type" in "User Authentication Setting".

Primary	LDAP Server	Type	Attribute type of 'User Name'	Attribute type of 'PIN'
<input type="radio"/>	LDAP Server1			
<input type="radio"/>	LDAP Server2			
<input type="radio"/>	LDAP Server3			

	Item name	Description
1	LDAP Server1 - LDAP Server3	<p>Click one of the LDAP servers and specify the following items in the displayed screen to register the LDAP server.</p> <p>Windows Server — Select this when LDAP is running on a Windows server. Enter the attribute type of 'PIN' registered in LDAP.</p> <p>LDAP Server (Other than Windows Server) — Select this when the LDAP is running on a server other than a Windows one. When this is selected, enter the attribute type of 'User Name' or 'PIN' registered in LDAP.</p>

■ Certificate Management Settings

You can manage device certificates and client certificates.

Tip

The [Certificate Management] submenu can be accessed from the [Security] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Security] menu:

P.10 “Access Policy Mode”

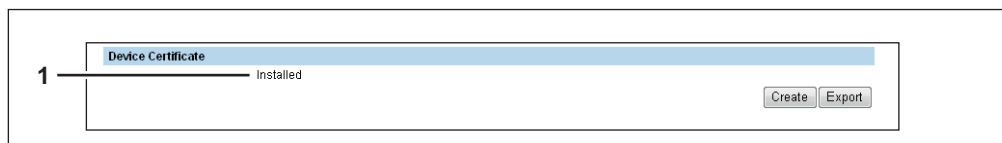
P.73 “[Security] Item List”

P.77 “Setting up Device Certificate”

P.78 “Setting up Client Certificate”

□ Setting up Device Certificate

You can configure the device certificate for encrypted communications using SSL.



	Item name	Description
1	Device Certificate	Creates a certificate for encrypted communications using SSL on this equipment. [Create] button — Displays the [Create self-signed certificate] screen. Specify items necessary for the certificate to create the self-signed certificate. P.77 “[Create Self-signed Certificate] Screen” [Export] button — Exports the created self-signed certificate.

[Create Self-signed Certificate] Screen

	Item name	Description
1	[Save] button	Saves the self-signed certificate.
2	[Cancel] button	Cancels creating the certificate.
3	Country/Region Name	Enter the country or region code using two alphabetical characters. (Example: JP)
4	State or Province Name	Enter the state or province name using alphanumerical characters or symbols. You can enter up to 128 characters.
5	Locality Name	Enter the locality name using alphanumerical characters or symbols. You can enter up to 128 characters.
6	Organization Name	Enter the organization name using alphanumerical characters or symbols. You can enter up to 64 characters.

	Item name	Description
7	Organizational Unit Name	Enter the organizational unit name using alphanumerical characters or symbols. You can enter up to 64 characters.
8	Common Name	Enter the FQDN or IP address of this equipment using alphanumerical characters or symbols. You can enter up to 64 characters.
9	Email Address	Enter the email address using alphanumerical characters or symbols. You can enter up to 64 characters.
10	Validity Period	Enter the validity period of the self-signed certificate.

□ Setting up Client Certificate

	Item name	Description
1	Client Certificate	Creates the client certificate. [Create] button — Displays the [Create client certificate] screen. Specify items necessary for the certificate to create the client certificate. 📖 P.78 “[Create Client Certificate] Screen”

[Create Client Certificate] Screen

	Item name	Description
1	[Save] button	Saves the client certificate.
2	[Cancel] button	Cancels creating the certificate.
3	Country/Region Name	Enter the country or region code using two alphabetical characters. (Example: JP)
4	State or Province Name	Enter the state or province name using alphanumerical characters or symbols. You can enter up to 128 characters.
5	Locality Name	Enter the locality name using alphanumerical characters or symbols. You can enter up to 128 characters.
6	Organization Name	Enter the organization name using alphanumerical characters or symbols. You can enter up to 64 characters.
7	Organizational Unit Name	Enter the organizational unit name using alphanumerical characters or symbols. You can enter up to 64 characters.
8	Common Name	Enter the FQDN or IP address of a client computer using alphanumerical characters or symbols. You can enter up to 64 characters.
9	Validity Period	Enter the validity period of the self-signed certificate.
10	Password	Enter the certificate's password using alphanumerical characters or symbols. You can enter up to 64 characters.

■ Password Policy Settings

You can configure policies for the password to register.

Tip

The [Password Policy] submenu can be accessed from the [Security] menu on the [Administration] tab. See the following pages for how to access it and information on [Security] menu:

P.10 "Access Policy Mode"

P.73 "[Security] Item List"

P.79 "Setting up Policy for Users"

P.80 "Setting up Policy for Administrator"

P.81 "Setting up Policy for SNMPv3"

□ Setting up PIN Authentication

You can configure the number of digits for the PIN code.

	Item name	Description
1	Select the limit for the PIN	Specify the number of digits for the automatically generated PIN code. Specify within the range from 1 to 32. "4" is set as the default.

□ Setting up Policy for Users

You can configure policies for user registration.

	Item name	Description
1	Minimum Password Length	Specify the minimum number of digits for the password. Specify within the range from 0 to 64. "0" is set as the default.
2	Requirements to Apply	Select [Enable] to set restrictions on the character strings that can be used in passwords. [Disable] is set as the default. Restrictions <ul style="list-style-type: none"> • The user name and password cannot be the same. • The same password cannot be used again. • A password consisting of sequences of the same characters cannot be used. • A password containing the characters entered in the restricted character text box cannot be used.

	Item name	Description
3	Lockout Setting	Specify whether or not to enable the lockout setting when the user failed to supply the correct password. [Enable] is set as the default. Number of Retry — Specify the number of retries before lockout. Specify within the range from 1 to 30 times. “10” is set as the default. Lockout Time — Specify the duration to lock out the user. Specify within the range from 1 to 1440 minutes. “1” is set as the default.
4	Available Period	Select [Enable] to specify how long the password is valid before its expiry. [Disable] is set as the default. Expiration day(s) — Specify how long the password is valid before its expiry. Specify within the range from 1 to 999 days. “180” is set as the default.
	Tip	When the number of days set in [Expiration day(s)] elapses, a screen that prompts the user to change the password will appear the next time the user logs in.

❑ Setting up Policy for Administrator

You can configure policies for administrator.

	Item name	Description
1	Minimum Password Length	Specify the minimum number of digits for the password. Specify within the range from 6 to 64. “6” is set as the default.
2	Requirements to Apply	Select [Enable] to set restrictions on the character strings that can be used in passwords. [Disable] is set as the default. Restrictions <ul style="list-style-type: none"> • The user name and password cannot be the same. • The same password cannot be used again. • A password consisting of sequences of the same characters cannot be used. • A password containing the characters entered in the restricted character text box cannot be used.
3	Lockout Setting	Specify whether or not to enable the lockout setting when the user failed to supply the correct password. [Enable] is set as the default. Number of Retry — Specify the number of retries before lockout. Specify within the range from 1 to 30 times. “10” is set as the default. Lockout Time — Specify the duration to lock out the user. Specify within the range from 1 to 1440 minutes. “1” is set as the default.
	Tip	Save the settings to reflect the change in the number of retry times. Due to a change in the number of retry times, a user may lock out in the next login. The history of lockouts is registered in the log.

	Item name	Description
4	Available Period	Select [Enable] to specify how long the password is valid before its expiry. [Disable] is set as the default. Expiration day(s) — Specify how long the password is valid before its expiry. Specify within the range from 1 to 999 days. "180" is set as the default.
	<div style="border: 1px solid gray; padding: 2px; width: fit-content;">Tip</div> <p>When the number of days set in [Expiration day(s)] elapses, a screen that prompts the user to change the password will appear the next time the user logs in.</p>	

□ Setting up Policy for SNMPv3

Setting up Password Policy for SNMPv3.

	Item name	Description
1	Minimum Password Length	Specify the minimum number of digits for the password. Specify within the range from 1 to 20. "1" is set as the default.

[Security] How to Set and How to Operate

When using SSL for the security settings, you can create and export the necessary self-signed certificate.

📖 P.82 “Creating/Exporting a Self-signed Certificate”

📖 P.84 “Creating a Client Certificate/Exporting”

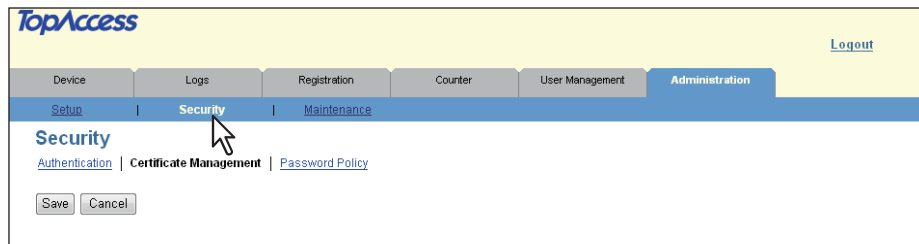
■ Creating/Exporting a Self-signed Certificate

1 Start TopAccess access policy mode.

📖 P.10 “Access Policy Mode”

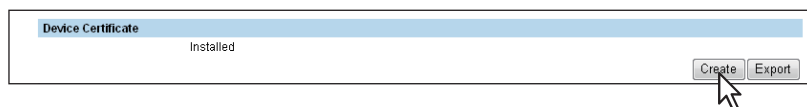
2 Click the [Administrator] tab.

3 Click [Security] > [Certificate Management].



The Certificate Management page is displayed.

4 Click [Create] from [Device Certificate].



The Create self-signed certificate page is displayed.

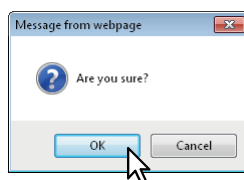
5 Enter the following items and click [Save].

Field	Value
Country Name	JP
State or Province Name	Tokyo
Locality Name	abcdefghijklmn
Organization Name	ABCDEFGH CORPORATION
Organizational Unit Name	ABCDEFGH Dept.
Common Name	PRD08919363
Email Address	User01@example.com
Validity Period	36 month(s)(1-99)

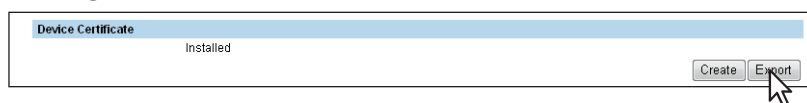
You can set the following in this page.

📖 P.77 “[Create Self-signed Certificate] Screen”

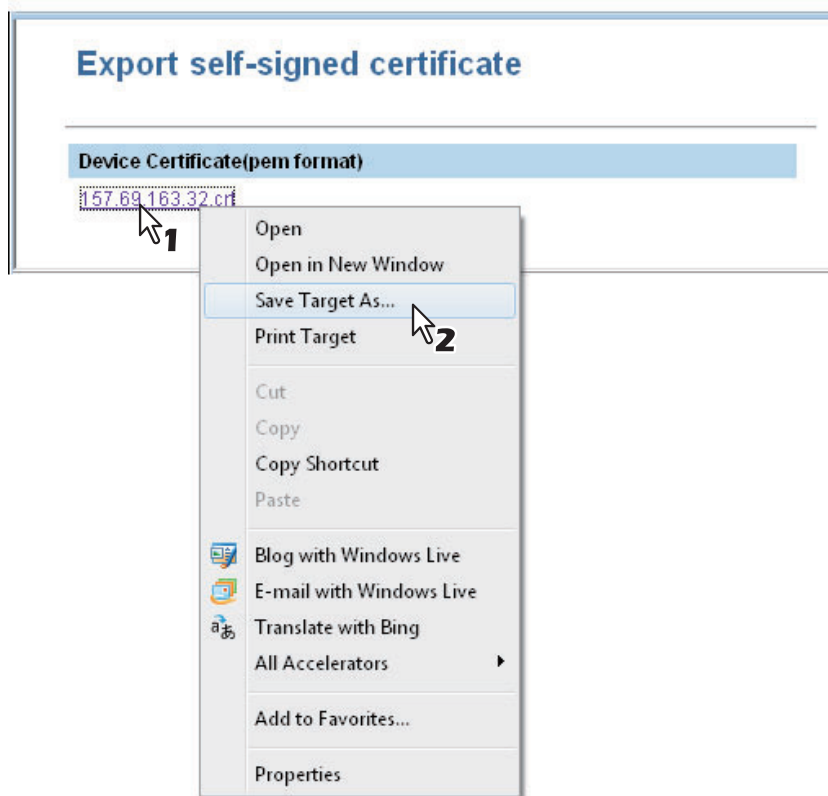
6 Click [OK].



7 A self-signed certificate is created. Click the [Export] button if you are exporting.

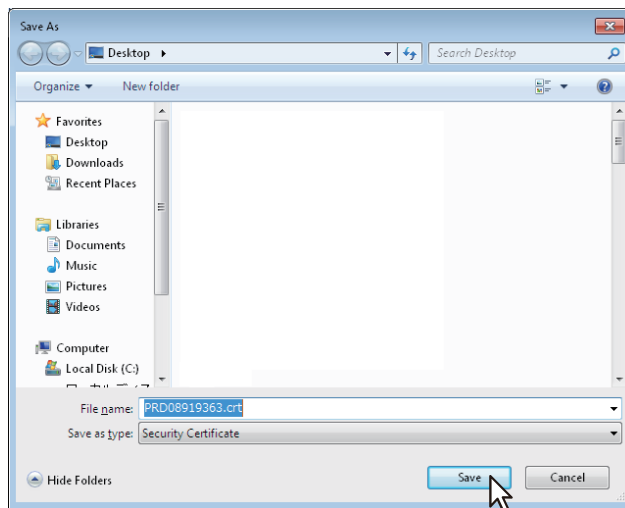


- 8** Right-click the [File Name] link of the certificate to be exported, and select [Save Target As].



The [Save As] dialog box appears.

- 9** Specify a directory to which the certificate is to be saved and then click [Save].



- 10** Click [Save] on the [Certificate Management] submenu page.

Tip

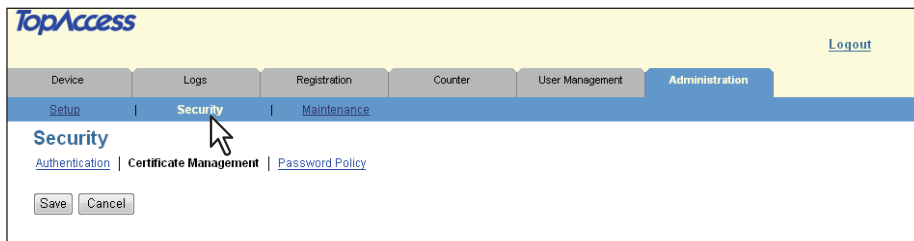
You can upgrade the security level of a client computer by installing the exported certificate into the computer.

- 11** Then you can enable SSL for the following network settings.

- 📖 P.61 "Setting up HTTP"
- 📖 P.71 "Off Device Customization Architecture Setting"

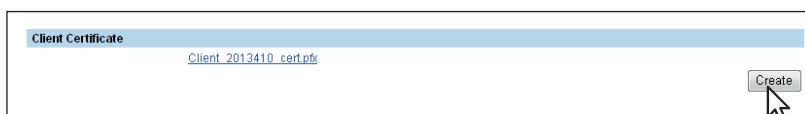
■ Creating a Client Certificate/Exporting

- 1 Start TopAccess access policy mode.
 ① P.10 “Access Policy Mode”
- 2 Click the [Administrator] tab.
- 3 Click [Security] > [Certificate Management].



The Certificate Management page is displayed.

- 4 Click [Create] from [Client Certificate].



The Create Client Certificate page is displayed.

- 5 Enter the following items and click [Save].

 A screenshot of the 'Create Client Certificate' form. The form has a 'Save' button and a 'Cancel' button at the top left. The following fields are filled out:

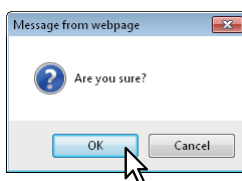
Country Name	JP
State or Province Name	Tokyo
Locality Name	abcdefghijklmn
Organization Name	ABCDEFGH CORPORATION
Organizational Unit Name	ABCDEFGH Dept.
Common Name	PRD08919363
Validity Period	36 month(s)(1-99)
Password	

 A red box highlights the input fields, and a mouse cursor points to the 'Save' button.

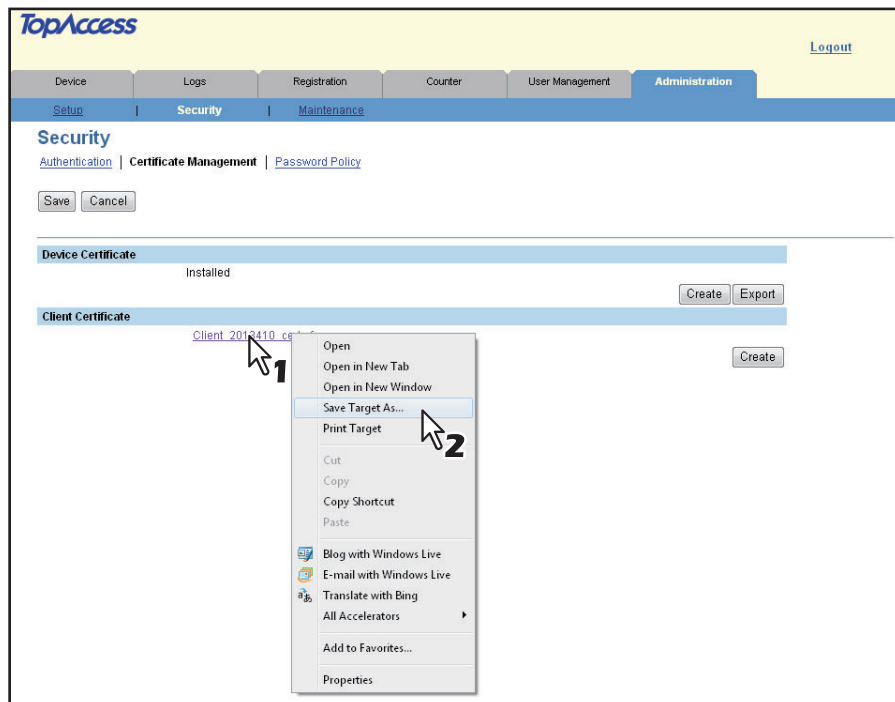
You can set the following in this page.

① P.78 “[Create Client Certificate] Screen”

- 6 Click [OK].



7 Right-click the [File Name] link of the certificate to be exported, and select [Save Target As].

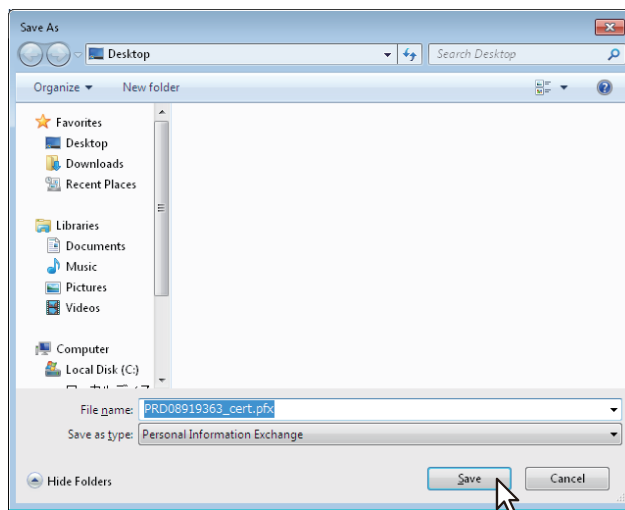


The [Save As] dialog box appears.

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.

8 Specify a directory to which the certificate is to be saved and then click [Save].



9 Click [Save] on the [Certificate Management] submenu page.

Tip

You can upgrade the security level of a client computer by installing the exported certificate into the computer.

[Maintenance] Item List

Tip

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

See the following pages for how to access it:

P.10 “Access Policy Mode”

- P.86 “Import”
- P.87 “Export”
- P.88 “Create Clone File”
- P.89 “Install Clone File”
- P.91 “Directory Service Settings”
- P.93 “System Updates”
- P.94 “Languages”
- P.94 “Reboot Settings”

■ Import

You can import templates exported from other equipment.

Tip

The [Import] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Maintenance] menu:

P.10 “Access Policy Mode”

P.86 “[Maintenance] Item List”

- P.86 “Template”
- P.86 “Combined(Template + Username)”

Note

Before importing data, check that there are no jobs being processed. You cannot import data if there are jobs being processed. If the import is taking too long, try importing data after the equipment has entered the Energy Save mode.

□ Template

You can import public templates.

	Item name	Description
1	File Name	Select the template file to be imported. [Browse] button — Allows you to select the template file. [Import] button — Imports the selected template file.

□ Combined(Template + Username)

You can import private templates.

	Item name	Description
1	File Name	Select the template file to be imported. [Browse] button — Allows you to select the template file. [Import] button — Imports the selected template file.

■ Export

You can export the selected template.

Tip

The [Export] submenu can be accessed from the [Maintenance] menu on the [Administration] tab. See the following pages for how to access it and information on the [Maintenance] menu:

📖 P.10 “Access Policy Mode”

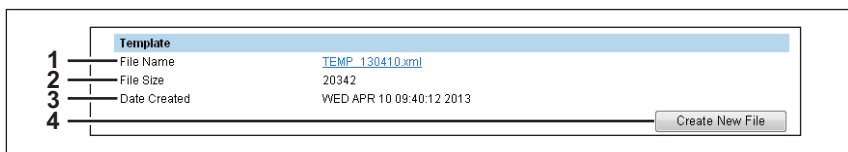
📖 P.86 “[Maintenance] Item List”

📖 P.87 “Template”

📖 P.86 “Combined(Template + Username)”

□ Template

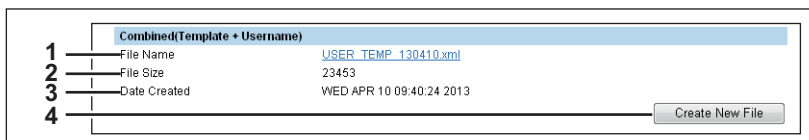
You can export public templates.



	Item name	Description
1	File Name	Displays the file name of the created export files. Click the file name you want to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the date the export files were created.
4	[Create New File] button	Creates the export file.

□ Combined(Template + Username)

You can export private templates.



	Item name	Description
1	File Name	Displays the file name of the created export files. Click the file name you want to download.
2	File Size	Displays the file size of the created export files.
3	Date Created	Displays the date the export files were created.
4	[Create New File] button	Creates the export file.


■ Create Clone File

Creates a clone file of the operating environment of this equipment.
You can implement a cloned environment by installing the created clone file on other equipment.

Tip

The [Create Clone File] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.

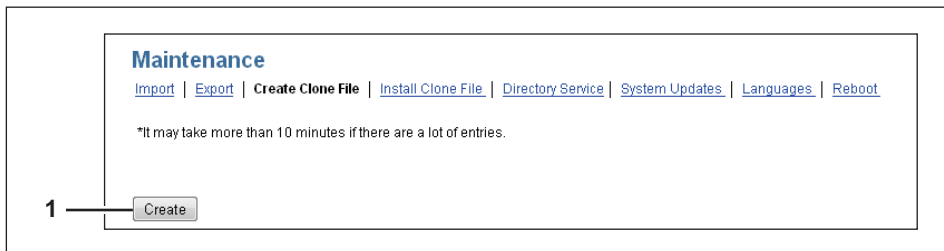
See the following pages for how to access it and information on the [Maintenance] menu:

 P.10 "Access Policy Mode"

 P.86 "[Maintenance] Item List"

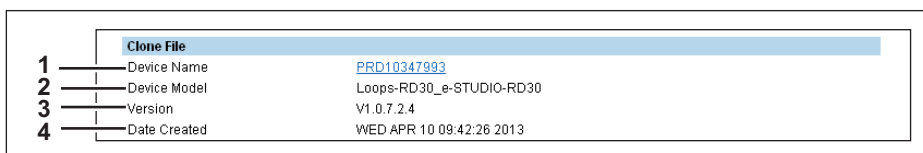
 P.88 "Clone File"

 P.89 "Category Setting"



	Item name	Description
1	[Create] button	Creates the clone file of the category selected in the category setting. When you click this button, a screen is displayed to set a password on the clone file.
	Note	The PIN code is a number of up to 32 digits (0 to 9).

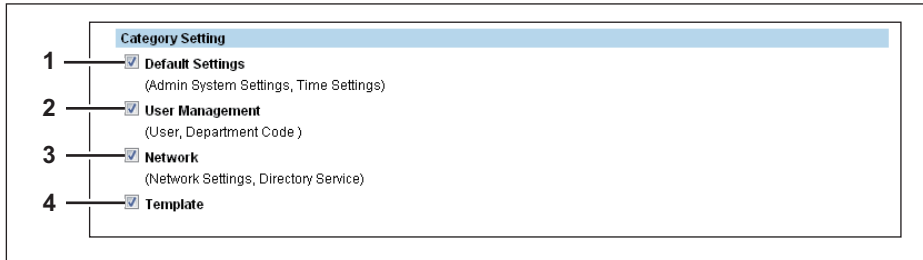
□ Clone File



	Item name	Description
1	Device Name	Displays the device name of the created clone file. Click the device name to download the clone file.
2	Device Model	Displays the device model of the created clone file.
3	Version	Displays the system ROM version of the created clone file.
4	Date Created	Displays the date the clone file was created.

□ Category Setting

Select the category for the clone file.



	Item name	Description
1	Default Settings	Includes the admin system and time settings in the clone file.
2	User Management	Includes the user and department code settings in the clone file.
3	Network	Includes the network settings and Directory Service settings in the clone file.
4	Template	Includes the public template and private template in the clone file.

7

■ Install Clone File

You can install the created clone file.

You can implement a cloned environment by installing a clone file created on another equipment.

Note

When creating and installing a clone file, make sure the source and target are running the same software version.

See the following pages for how to check the software version and update.

📖 P.72 “Version”

📖 P.93 “System Updates”

Tip

The [Install Clone File] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Maintenance] menu:

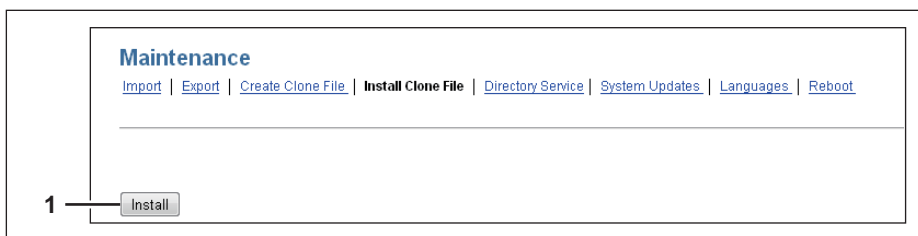
📖 P.10 “Access Policy Mode”

📖 P.86 “[Maintenance] Item List”

📖 P.90 “File Upload”

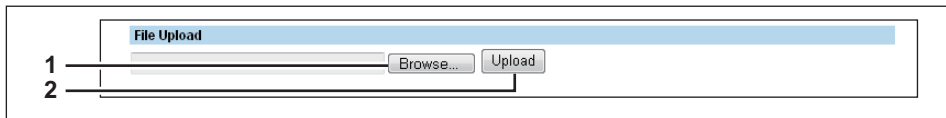
📖 P.90 “Clone File Information”

📖 P.90 “Setting Data Included in Clone File”



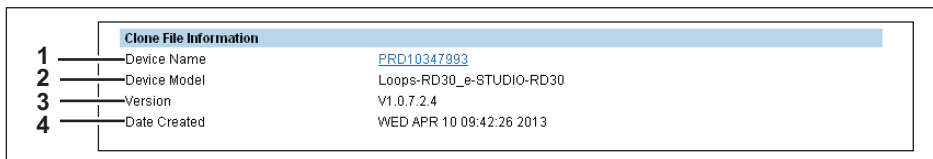
	Item name	Description
1	[Install] button	Installs the selected clone file. When you click this button, a dialog box is displayed to prompt you to enter the password you specified when creating the clone file.

□ File Upload



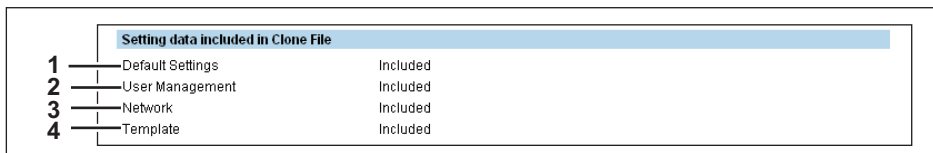
	Item name	Description
1	[Browse] button	Select a clone file.
2	[Upload] button	Displays information on the selected clone file and what is included in the clone file.

□ Clone File Information



	Item name	Description
1	Device Name	Displays the device name of the created clone file.
2	Device Model	Displays the device model of the created clone file.
3	Version	Displays the system ROM version of the created clone file.
4	Date Created	Displays the created date of the clone file.

□ Setting Data Included in Clone File



	Item name	Description
1	Default Settings	Displays if the admin system and time settings are included.
2	User Management	Displays if the user and department code settings are included.
3	Network	Displays if the network and directory service settings are included.
4	Template	Displays if the public template and private template are included.

■ Directory Service Settings

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

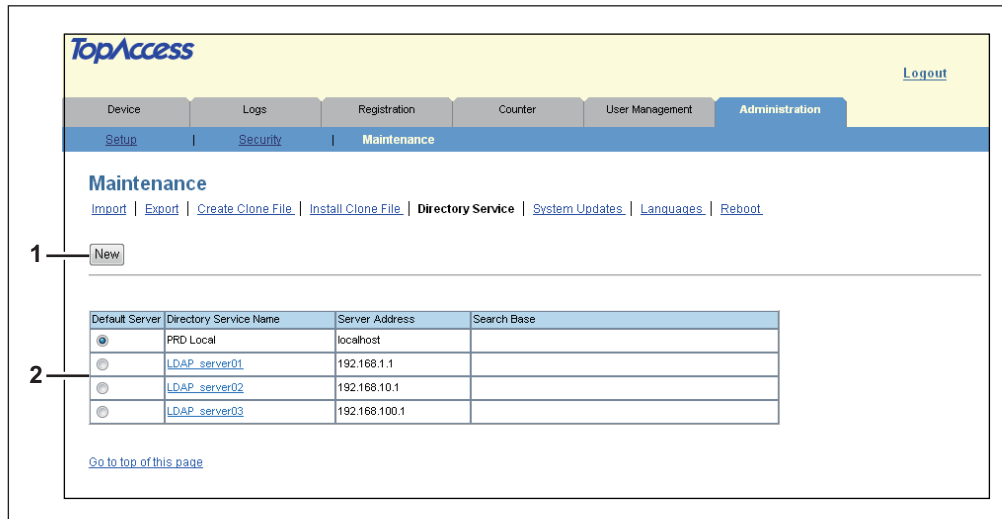
Tip

The [Directory Service] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Maintenance] menu:

📖 P.10 “Access Policy Mode”

📖 P.86 “[Maintenance] Item List”



	Item name	Description
1	[New] button	Registers the LDAP server that provides a directory service. 📖 P.91 “[Directory Service Properties] Screen”
2	Directory Service List	Displays a list of registered LDAP servers. You can edit the registered details by clicking a directory service name. 📖 P.91 “[Directory Service Properties] Screen”

□ [Directory Service Properties] Screen

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

The screenshot shows the 'Directory Service Properties' screen. The fields are as follows:

- 1: *Directory Service Name (LDAP_server02)
- 2: *Server Address (192.168.10.1)
- 3: *Port Number (389)
- 4: Authentication (Auto)
- 5: Search Base
- 6: User Name
- 7: Password
- 8: Search Timeout (1)
- 9: Enable SSL (Disable)
- 10: SSL Port Number (636)

	Item name	Description
1	Directory Service Name	Enter the directory service name to identify the directory service. You can enter up to 64 alphanumerical characters and symbols (excluding = ; # \).

	Item name	Description
2	Server Address	Enter the IP address or FQDN of the LDAP server. You can enter up to 128 alphanumerical characters and symbols.
3	Port Number	Enter the port number to access the LDAP server. You can enter a value in the range from 1 to 65535. Generally the default value "389" is used to access the LDAP server without SSL. When the SSL is required, generally the "636" port is used to access the LDAP server.
4	Authentication	Select the SASL authentication protocol. If you do not know the authentication type, select [Auto]. <ul style="list-style-type: none"> • Auto — Select this to access the LDAP server using the appropriate authentication that this equipment detects. • Kerberos — Select this to access the LDAP server using the Kerberos authentication. • Digest-MD5 — Select this to access the LDAP server using the Digest-MD5 authentication. • Simple Bind — Select this to access the LDAP server using the Simple Bind authentication.
5	Search Base	Enter the search base. When you configure the Active Directory in Windows server, make sure to enter this option. You can enter up to 256 alphanumerical characters and symbols (excluding ; # \).
6	User Name	Enter the login user name if a user name is required to access the directory service. You can enter up to 256 alphanumerical characters and symbols.
7	Password	Enter the password if required to access the directory service. You can enter up to 32 alphanumerical characters and symbols.
8	Search Timeout	Select the timeout period for quitting communication when no response is received from the LDAP server. Specify within the range from 1 to 5. "1" is set as the default.
9	Enable SSL	Select whether the SSL (Secure Sockets Layer) is enabled or disabled for communicating the LDAP directory service. <ul style="list-style-type: none"> • Disable — Select this to disable the SSL for communicating the LDAP directory service. • Accept all certificates without CA — Select this to enable the SSL without using imported CA certificate.
	<p>Notes</p> <ul style="list-style-type: none"> • 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. • Not all operating systems support SSL for all protocols. 	
10	SSL Port Number	Enter the port number to access the LDAP server using SSL. You can enter a value in the range from 1 to 65535. Generally, the default value "636" is used.

■ System Updates

You can update the system on your equipment.

Tip

The [System Updates] submenu can be accessed from the [Maintenance] menu on the [Administration] tab.

See the following pages for how to access it and information on the [Maintenance] menu:

📖 P.10 “Access Policy Mode”

📖 P.86 “[Maintenance] Item List”

📖 P.93 “Install Software Package”

□ Install Software Package

	Item name	Description
1	File Name	Select the software pack file to be installed. [Browse] button — Allows you to select the software pack file. [Install] button — Installs the selected software pack file.

□ Network Software Update

You can update the software on this equipment using a network update file.

	Item name	Description
1	[Save] button	Click to update the software after checking the values entered for network path, login user name, password, and confirm password.
2	Network Path	Specify the path to where the update file is stored. You can enter alphanumerical characters and symbols (excluding : , ; * ? " < > ').
3	Login User Name	Enter the login user name to access a network folder that is using SMB protocol. You can enter up to 32 alphanumerical characters and symbols.
4	Password	Enter the password to access a network folder that is using SMB protocol. You can enter up to 32 alphanumerical characters, symbols, and spaces.
5	Retype Password	Enter the same password again for confirmation.

■ Languages

You can specify the language for the LCD panel of this equipment.

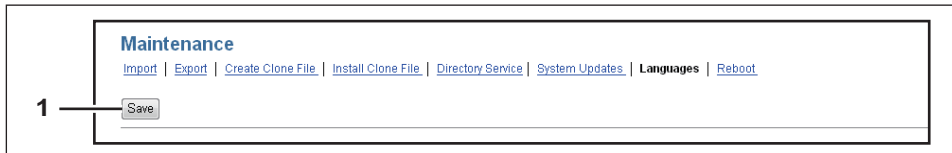
Tip

The [Languages] submenu can be accessed from the [Maintenance] menu on the [Administration] tab. See the following pages for how to access it and information on the [Maintenance] menu:

📖 P.10 “Access Policy Mode”

📖 P.86 “[Maintenance] Item List”

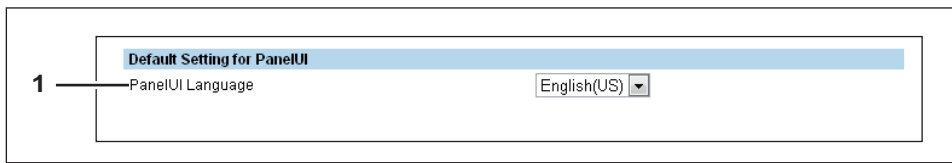
📖 P.94 “Default Setting for PanelUI”



	Item name	Description
1	[Save] button	Saves the registered language.

□ Default Setting for PanelUI

Select the display language for the LCD panel.



	Item name	Description
1	PanelUI language	Select the display language for the LCD panel.

■ Reboot Settings

You can reboot the equipment.

Tip

The [Reboot] submenu can be accessed from the [Maintenance] menu on the [Administration] tab. See the following pages for how to access it and information on the [Maintenance] menu:

📖 P.10 “Access Policy Mode”

📖 P.86 “[Maintenance] Item List”

[My Account] Tab Page

This chapter explains the [My Account] tab page in TopAccess.

[My Account] Tab Page Overview	96
[My Account] Item List	96

[My Account] Tab Page Overview

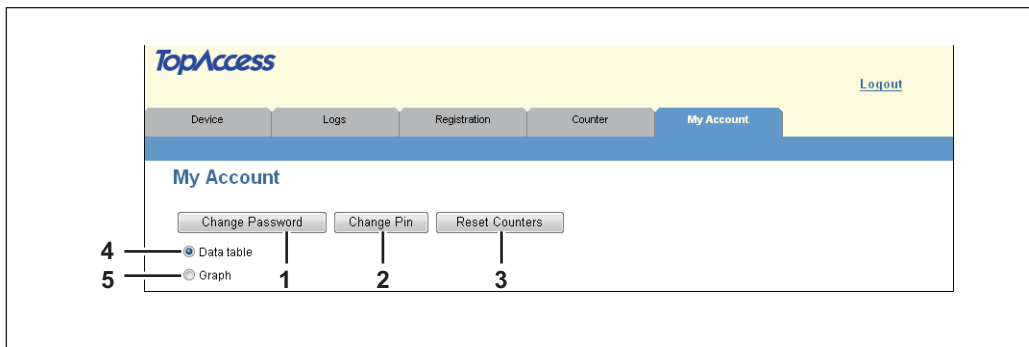
The [My Account] tab is displayed when [User Authentication] is enabled in the [Administrator] tab - [Security] - [Authentication] - [User Authentication Setting].

The [My Account] tab displays the account information of the user accessing the equipment.

P.96 “[My Account] Item List”

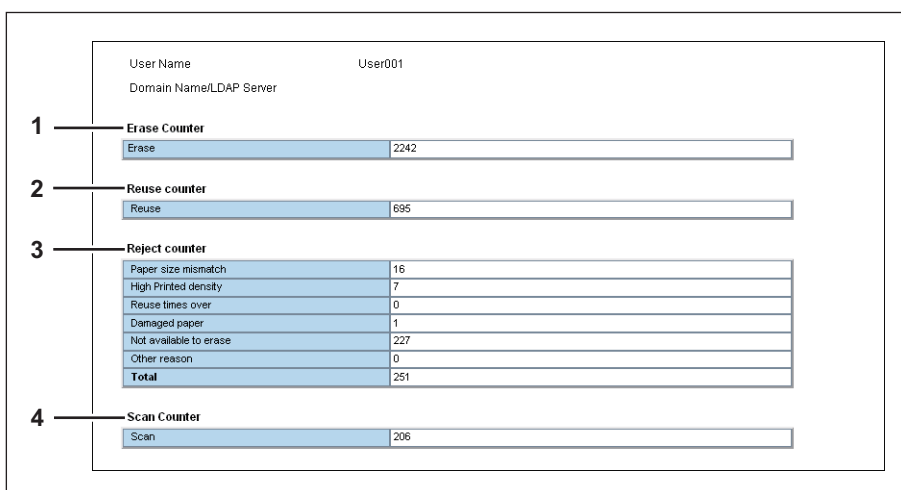
■ [My Account] Item List

P.97 “[Change Password] screen”



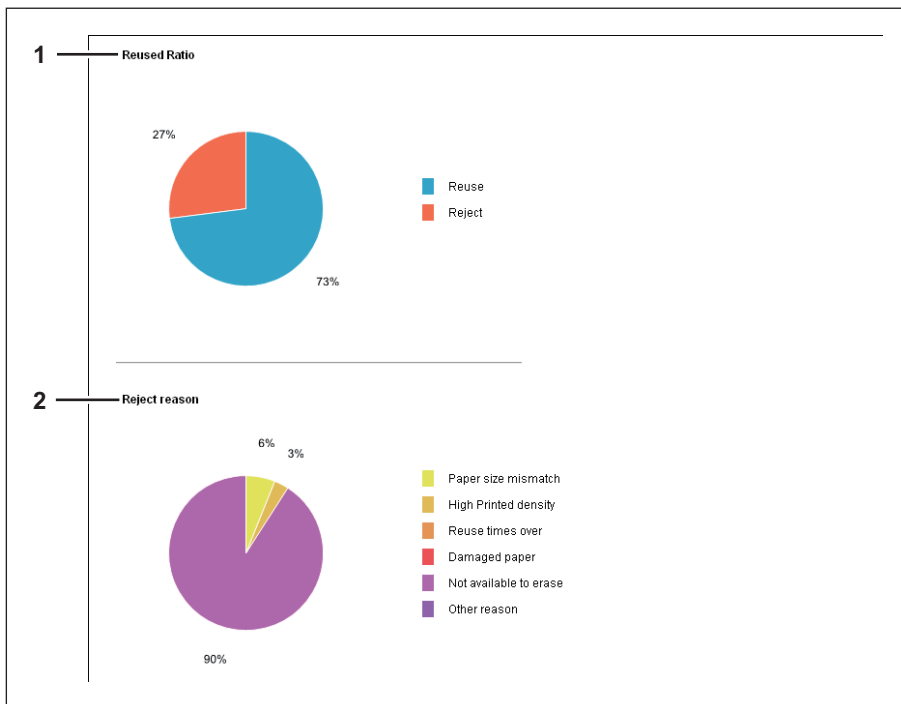
	Item name	Description
1	[Change Password] button	Changes the password of the user accessing the equipment (for TopAccess).
2	[Change Pin] button	Changes the PIN code of the user accessing the equipment (for the control panel).
3	[Reset Counters] button	Resets the counter of the user accessing the equipment.
4	Data table	Displays the counter in table format.
5	Graph	Displays the counter in graph format.

□ Data table



	Item name	Description
1	Erase Counter	Displays the number of erased pages.
2	Reuse counter	Displays the number of pages that the sorter has determined can be reused.
3	Reject counter	Displays the number of pages that the sorter has determined cannot be reused.
4	Scan Counter	Displays the number of scanned pages.

□ Graph



8

	Item name	Description
1	Reused Ratio	Displays the reused ratio for paper as a pie chart.
2	Reject reason	Displays the reject reason for paper as a pie chart.

□ [Change Password] screen

Changes the password of the user accessing the equipment (for TopAccess).

Change Password

1 — [Save] [Cancel]

2 — [Save] button

3 — Old Password

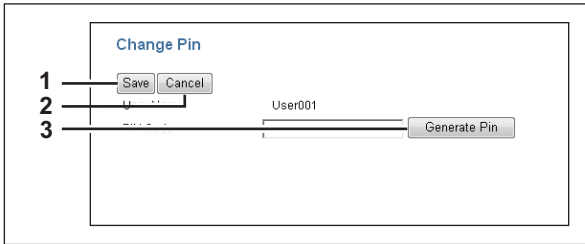
4 — New Password

5 — Retype Password

	Item name	Description
1	[Save] button	Saves the password changes.
2	[Cancel] button	Cancels the operation.
3	Old password	Enter the current password.
4	New password	Enter the new password.
5	Retype Password	Enter the new password again to confirm.

□ [Change Pin] screen

Changes the PIN code of the user accessing the equipment (for the control panel).



	Item name	Description
1	[Save] button	Saves the pin code changes.
2	[Cancel] button	Cancel the operation.
3	[Generate Pin] button	Generates a pin code automatically.
	<p>Note</p> <p>The PIN code is a number of up to 32 digits (0 to 9). The number of digits for the PIN code can be set with [Administration] - [Security] - [Password Policy].</p> <p>📖 P.79 "Setting up PIN Authentication"</p>	

APPENDIX

This chapter contains the following contents.

Installing Certificates for a Client PC	100
--	------------

Installing Certificates for a Client PC

Configuring the Microsoft Management Console

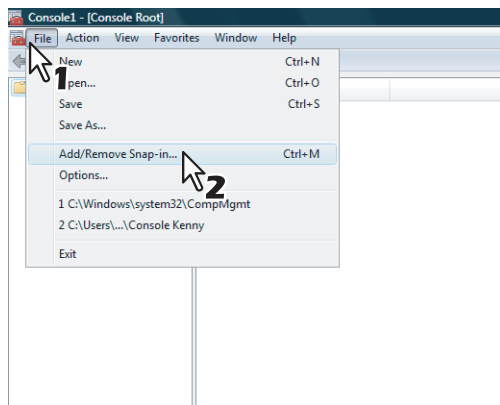
The following describes a configuration on Windows Vista.

- 1 Open the command prompt, type "mmc" and press the Enter key.

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

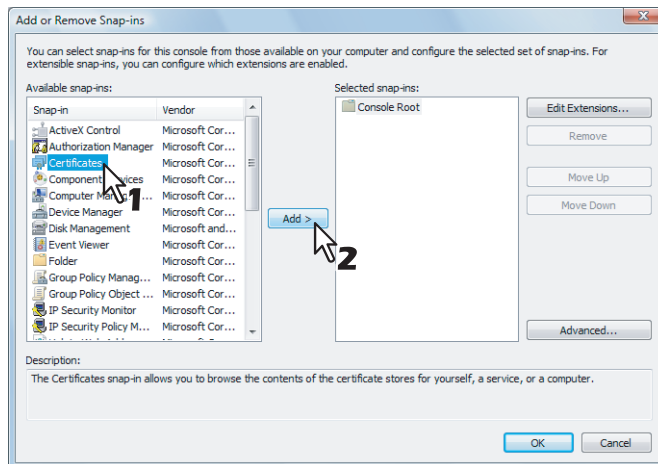
C:\Users\user-001>mmc_
```

- 2 From the [File] or [Console] menu of the window that appears, select [Add/Remove Snap-in]



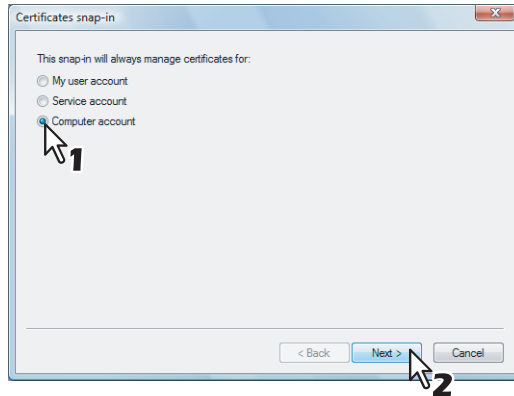
The Add or Remove Snap-ins dialog box appears.

- 3 From the list of [Available snap-ins:], select [Certificates] and click [Add].



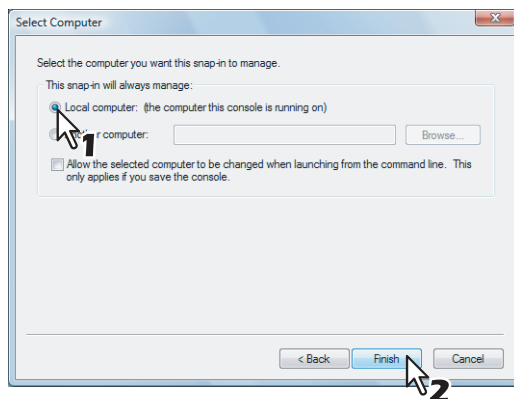
The [Certificates snap-in] dialog box appears.

4 Select [Computer account] and click [Next].



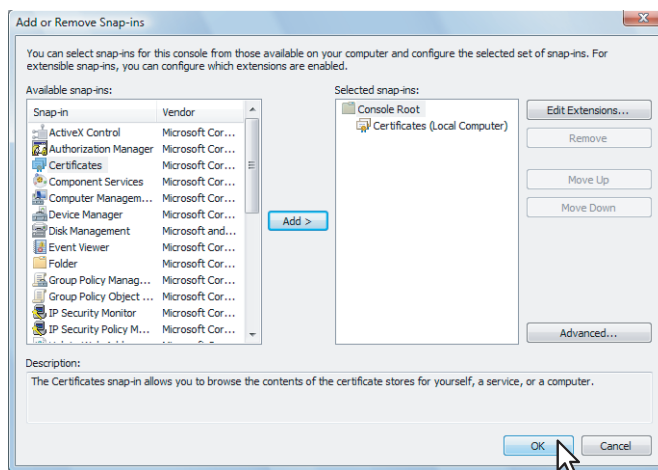
The [Select Computer] dialog box appears.

5 Select [Local computer: (the computer this console is running on)] and click [Finish].

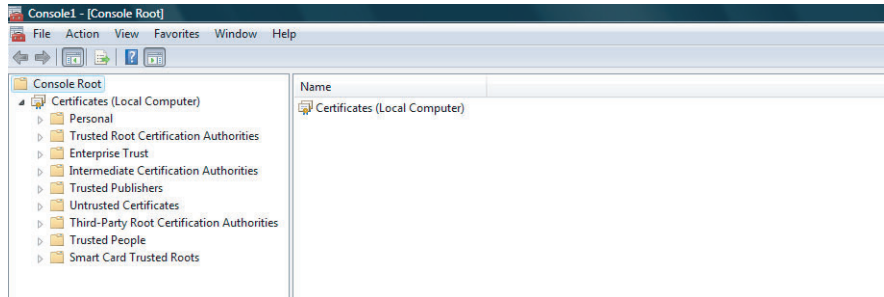


The [Select Computer] dialog box is closed.

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

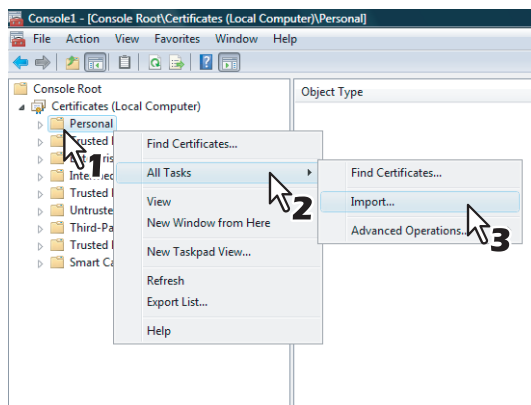
The following describes an import on Windows Vista.

Notes

- 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:

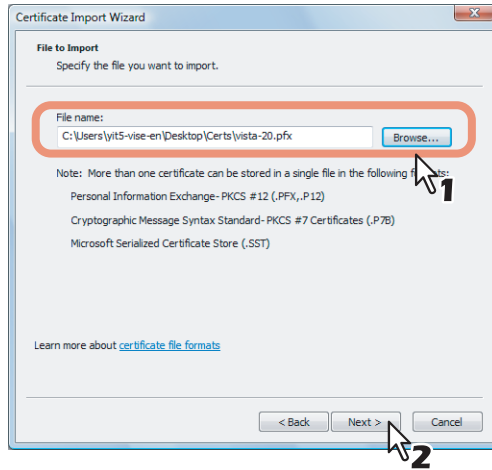
- **Self-signed certificate (.crt):** Console Root > Certificates (Local Computer) > Trusted Root Certification Authorities
 - **Client certificate (.pfx):** Console Root > Certificates (Local Computer) > Personal
- The Certificate Import Wizard appears.

- 2 On the Certificate Import Wizard, click [Next].

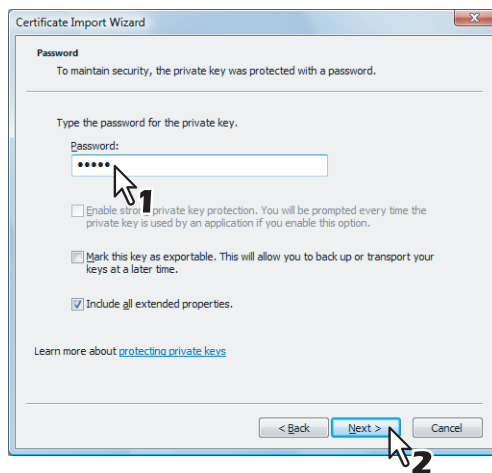


For importing a client certificate, proceed to the next step. Otherwise, skip to step 5.

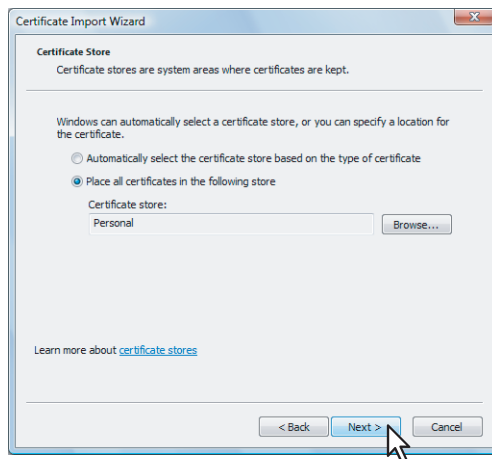
3 From [Browse], select the certificate to install, and click [Next].



4 Enter the password for the private key and click [Next].



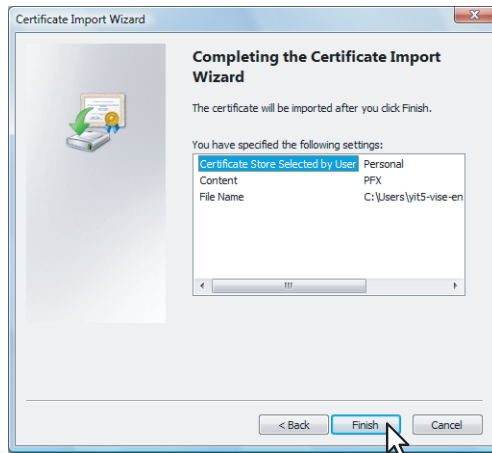
5 Click [Next].



Note

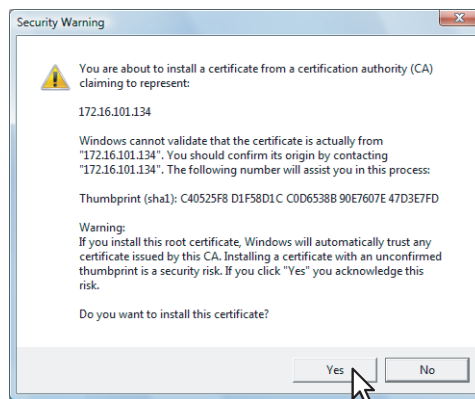
Do not change the certificate store using [Browse].

6 Click [Finish].

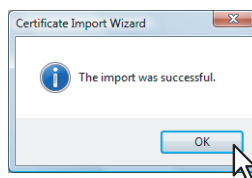


Tip

If the following security warning message appears, click [Yes].



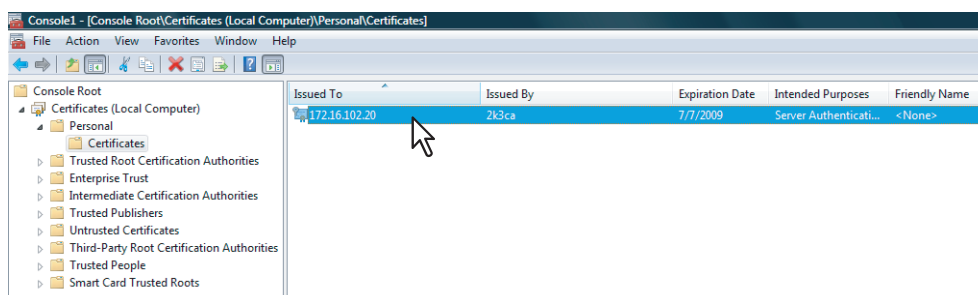
7 Click [OK] to complete the import.



If you are importing a client certificate (.pfx) to a Windows Vista PC, proceed to the next step. Otherwise, the installation is complete.

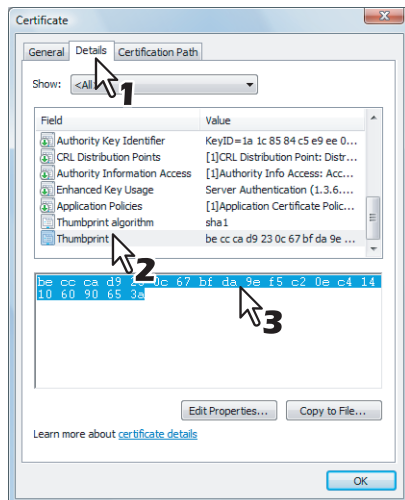
If you need to install another certificate, repeat the steps from the beginning.

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=becccad923
0c67bfd9ef5c20ec414106090653aappid={00112233-4455-6677-8899-AABBCCDDEEFF}

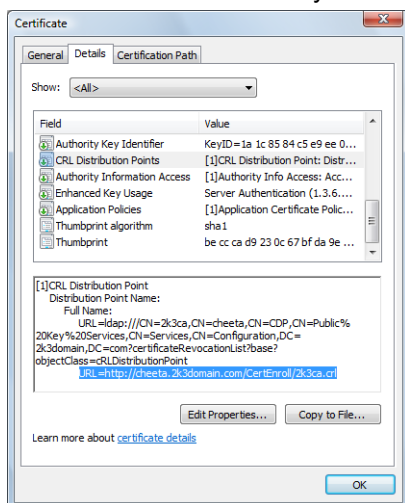
SSL Certificate successfully added

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.

Note

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

A	
Access Policy Mode	10
Access policy mode	6
Accessing TopAccess	8
Accessing TopAccess by the Entering URL	8
Authentication	73
C	
Category Setting	89
Certificate Management Settings	77
Change Password	97
Change Pin	98
Clone File	88
Clone File Information	90
Combined(Template + Username)	86, 87
Conditions for Using TopAccess	7
Configuration	71
Counter Tab Page Overview	30
Create Client Certificate	78
Create Clone File	88
Create Self-signed Certificate	77
Create SNMP V3 User Information	65
Create User Information	37
Creating a Client Certificate/Exporting	84
Creating/Exporting a Self-signed Certificate	82
D	
Data table	96
Default Setting for PanelUI	94
Department Information	41
Department Information (Edit)	41
Department Management Item List	40
Device Item List	14
Directory Service Properties	91
Directory Service Settings	91
E	
End-user mode	6
Enter Password	38
Export	33, 43, 87
Export Logs Item List	18
Export/Import Item List	43
F	
File Upload	90
Folder Name	68
Format	68
G	
General	30
General Settings	46
Graph	97
I	
Import	44, 86
Install Clone File	89
Install Software Package	93
J	
Job Logs	16
Judgement Settings	70
L	
Languages	94
LDAP Authentication	75
Logs Tab Page Overview	16
M	
Maintenance Item List	86
Management Scan	68
Management Scan Settings	68
Managing Templates	27
Message Log	17
My Account Item List	96
My Account Tab Page Overview	96
N	
Network	71
Network Settings	51
Network Software Update	93
O	
Off Device Customization Architecture Setting	71
P	
Panel Settings	22
Password Policy Settings	79
PIN Authentication Setting	76
Private Template Screen	20
Private Templates	21
Public Remote List	25
Public Template Screen	20
Public Templates	20
R	
Reboot Settings	94
Registering or editing private templates	28
Registering or editing public templates	27
Registration How to Set and How to Operate	27
Registration Tab Page Overview	20
Remote Network Settings Item List	24
Remote Setting	26
Remote Setting List	24
Reuse Counter Settings	70
S	
Save as file Setting	69
Scan Settings	23
Search User Account	37
Security How to Set and How to Operate	82
Security Item List	73
Setting Data Included in Clone File	90
Setting up Bonjour	57
Setting up Client Certificate	78
Setting up Date & Time	48
Setting up Daylight Savings Time Setting	49
Setting up DDNS	58
Setting up Device Certificate	77
Setting up Device Information	47
Setting up DNS	57
Setting up Energy Save	48
Setting up Filtering	54
Setting up Funcations	47
Setting up HTTP	61
Setting up IPv6	55
Setting up PIN Authentication	79
Setting up Policy for Administrator	80
Setting up Policy for SNMPv3	81
Setting up Policy for Users	79
Setting up Proxy Setting	66
Setting up SMB	60
Setting up SNMP Network Service	63
Setting up SNTP Service	48
Setting up TCP/IP	52

Setting up User Authentication Setting	74
Setting up Wake Up Setting	66
Setting up WEB General Setting	50
Setup Item List	46
Sorting Settings	22
Supported browsers	7
System Updates	93
T	
Template	21, 86, 87
Template Item List	20
TopAccess Overview	6
TopAccess Screen Descriptions	9
Total Counter Item List	30
U	
User Accounts Item List	36
User Information	39
User Management Tab	35
User Management Tab Page Overview	36
V	
Version	72
View Logs Item List	16
W	
Windows Domain Authentication	75

PAPER REUSABLE DEVICE

TopAccess Guide

The logo for e-STUDIO RD30 features a green square with a white lowercase 'e' on the left. To its right, the word 'STUDIO' is written in a bold, black, sans-serif font. Further right, 'RD' is in a thin, black, outlined font, and '30' is in a large, bold, black, sans-serif font.

The logo for e-STUDIO RD301 features a green square with a white lowercase 'e' on the left. To its right, the word 'STUDIO' is written in a bold, black, sans-serif font. Further right, 'RD' is in a thin, black, outlined font, and '301' is in a large, bold, black, sans-serif font.

TOSHIBA TEC CORPORATION

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

