KONICA MINOLTA

bizhub 423/363/283/223

User's Guide [Network Administrator]

Table of contents

6   Sending and receiving network faxes

7   Using User Authentication

10 Managing

11 Registering

12 Configuring Settings for User Box Functions

13 Configuring Settings for Printer Function

14 Configuring Settings for Fax Functions

15   Appendix

16   Index

1 Introduction

1   Introduction

1.1   Welcome

Thank you for purchasing this machine.

This User's Guide describes the functions, operating instructions, precautions for correct operation, and simple troubleshooting guidelines of this machine. In order to obtain maximum performance from this product and use it effectively, please read this User's Guide as necessary.

1.1.1   User's guides

Printed manual	Overview
[Quick Guide Copy/Print/Fax/Scan/Box Operations]	This manual describes operating procedures and the functions that are most frequently used in order to enable you to begin using this machine immediately. This manual contains notes and precautions that should be followed to ensure safe usage of this machine. Please be sure to read this manual before using this machine.

User's guide CD manuals	Overview
[User's Guide Copy Operations]	This manual describes details on copy mode operations and the settings of this machine. • Specifications of originals and copy paper • Copy function • Maintaining this machine • Troubleshooting
[User's Guide Enlarge Display Operations]	This manual describes details on operating procedures of the enlarge display mode. • Copy function • Scanning function • G3 fax function • Network fax function
[User's Guide Print Operations]	This manual describes details on printer functions. • Printer function • Setting the printer driver
[User's Guide Box Operations]	This manual describes details on User Box functions. • Saving data in user boxes • Retrieving data from user boxes • Transferring and printing data from user boxes
[User's Guide Network Scan/Fax/Network Fax Operations]	This manual describes details on transmitting scanned data. • E-mail TX, FTP TX, SMB TX, Save in User Box, WebDAV TX, Web Services • G3 fax • IP Address Fax, Internet Fax
[User's Guide Fax Driver Operations]	This manual describes details on the fax driver function that transmits faxes directly from a computer. • PC-FAX
[User's Guide Network Administrator]	This manual describes details on setting methods for each function using the network connection. • Network settings • Settings using **PageScope Web Connection**

User's guide CD manuals	Overview
[User's Guide Advanced Function Operations]	This manual describes details on functions that become available by registering the optional license kit and by connecting to an application. • Web browser function • Image panel • PDF Processing Function • Searchable PDF • My panel and My address functions
[Trademarks/Copyrights]	This manual describes details on trademarks and copyrights. • Trademarks and copyrights

1.1.2   User's Guide

This User's Guide is intended for users ranging from those using this machine for the first time to administrators.

It describes basic operations, functions that enable more convenient operations, simple troubleshooting operations, and various setting methods of this machine.

Note that basic technical knowledge about the product is required to enable users to perform troubleshooting operation. Limit your troubleshooting operations to the areas explained in this manual.

Should you experience any problems, please contact our service representative.

1.2   Conventions used in this manual

1.2.1   Symbols used in this manual

Symbols are used in this manual to express various types of information.

The following describes each symbol related to correct and safe usage of this machine.

To use this machine safely

⚠ **WARNING**
● This symbol indicates that a failure to heed the instructions may lead to death or serious injury.

⚠ **CAUTION**
● This symbol indicates that negligence of the instructions may lead to mishandling that may cause injury or property damage.

NOTICE
This symbol indicates a risk that may result in damage to this machine or documents.
Follow the instructions to avoid property damage.

Procedural instruction

✔   This check mark indicates an option that is required in order to use conditions or functions that are prerequisite for a procedure.

1   This format number "1" represents the first step.

2   This format number represents the order of serial steps.
➜   This symbol indicates a supplementary explanation of a procedural instruction.

The operation procedures are described using illustrations.

➜   This symbol indicates transition of the **Control Panel** to access a desired menu item.
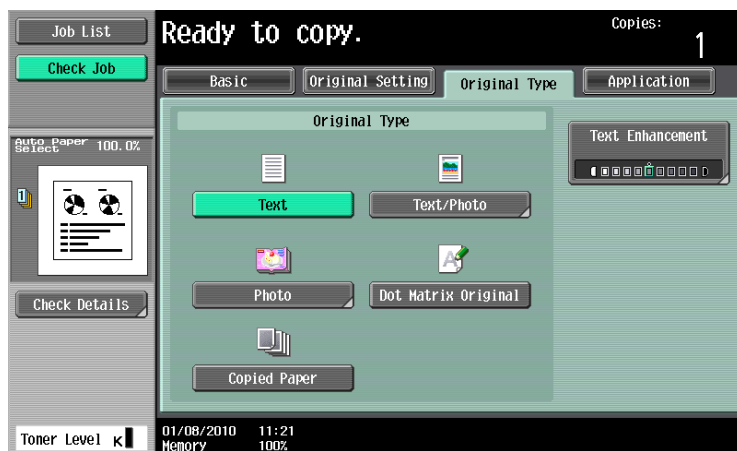
This symbol indicates a desired page.

📖 **Reference**

This symbol indicates a reference.

View the reference as required.

Key symbols

[ ]
Key names on the **Touch Panel** or computer screen, or a name of user's guide are indicated by these brackets.

Bold text
Key names, part names, product names and option names on the control panel are indicated in bold text.

1.2.2   Document and paper indications

Original and paper sizes

The following explains the indication for originals and paper described in this manual.
When indicating the original or paper size, the Y side represents the width and the X side the length.
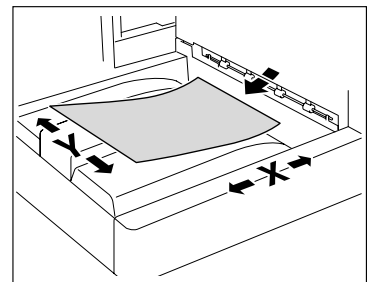
Original and paper indications

▭ indicates the paper size with the length (X) being longer than the width (Y).
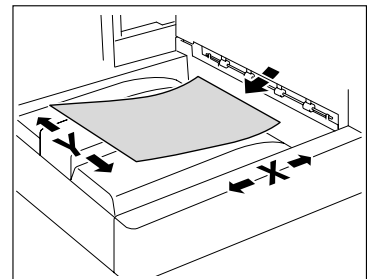
▯ indicates the paper size with the length (X) being shorter than the width (Y).
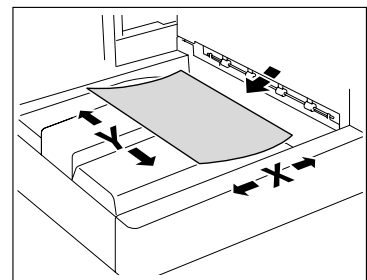
1.3   Display modes of PageScope Web Connection

The display modes of the **PageScope Web Connection** administrator modes are classified into two display modes: [Tab Function Display] and [List Function Display]. This manual shows an example where the [List Function Display] is set as the display mode.

This section provides an overview of each display mode. In either display mode, the available items are the same.

Reference

● For details on specifying the display mode, refer to page 3-7.

1.3.1   [Tab Function Display]

In the default setting, the screen is displayed in [Tab Function Display].

In [Tab Function Display], click the desired icon to change the menu.
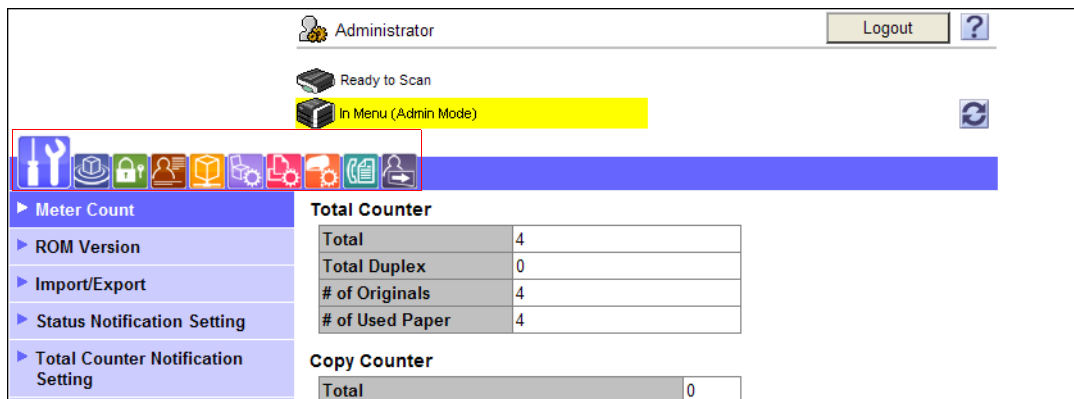
1.3.2   [List Function Display]

In [List Function Display], change the menu from the list box.

Select the desired menu in the drop-down list, click [Display].
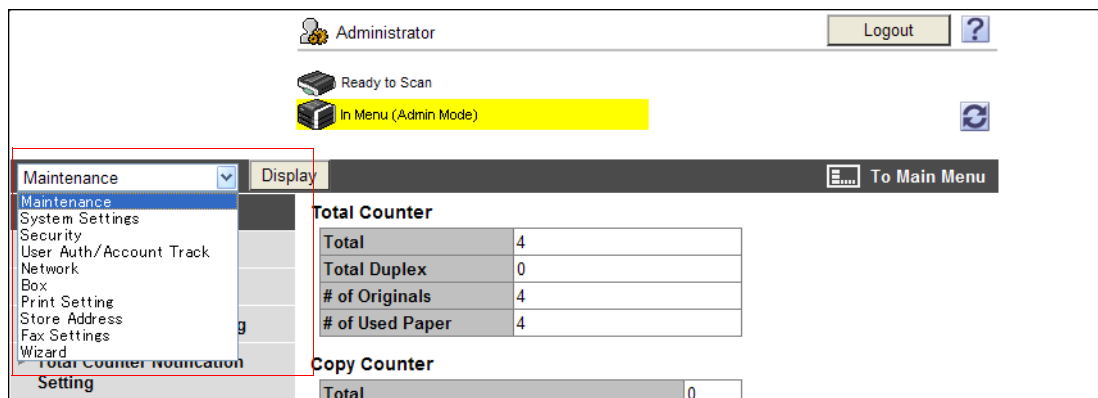
Main Menu

If you log in to the administrator mode while [List Function Display] is selected, the main menu appears first.

The main menu displays a list of all the menus in the administrator mode. Select the desired setting in the drop-down list, and click [Display] to display each setting screen.

Reference

- Click [To Main Menu] on each setting screen of the administrator mode to return to the main menu.
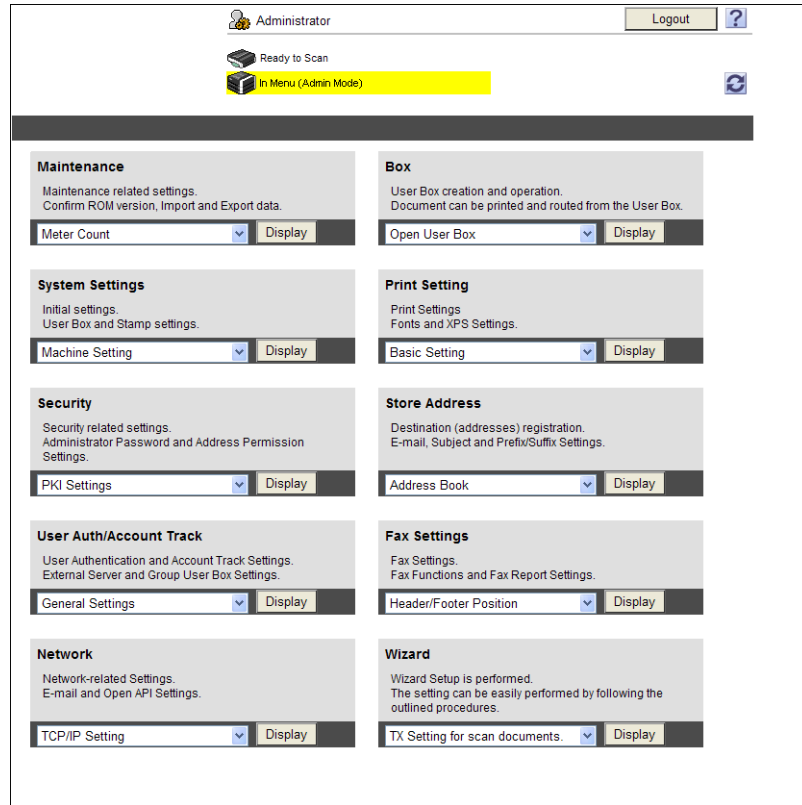
2 Connecting to network

2 Connecting to network

2.1 Basic settings for TCP/IP communication

Configure settings to use this machine in the TCP/IP network environment.

These settings are required before using this machine via the network.

NOTICE
To enable changed network settings, turn the main power of this machine off and on again.

To turn the main power switch off and on, first turn the main power off, and then turn it on after 10 or more seconds have elapsed. Not doing so may result in an operation failure.

[TCP/IP Settings]

In [Administrator Settings] on the **Control Panel**, select [Network Settings]▸▸[TCP/IP Settings].

📖 **Reference**
For details on how to go to the [Network Settings] screen, refer to page 15-3.

*For details on the menu structure of the [Network Settings] in the **Control Panel**, refer to page 15-5.*

For details on how to use this machine in the IPv6 environment, refer to page 2-5.
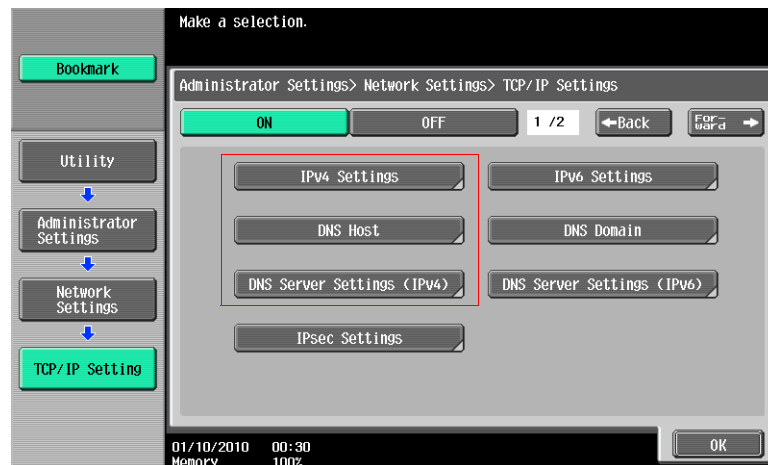
Item	Description	Prior check
[ON]/[OFF]	Select [ON].	

[IPv4 Settings]

Item	Description	Prior check
[IP Application Method]	Select whether to automatically obtain the IP address or directly specify it.	IP application method
[Auto Input]	To automatically obtain the IP address, select the automatic retrieval method.	
[IP Address]	To directly specify the IP address, enter the IP address of this machine.	IP address of this machine
[Subnet Mask]	When directly entering the IP address, configure the subnet mask of the network to be connected.	Subnet mask of this machine
[Default Gateway]	When directly entering the IP address, specify the default gateway of the network to be connected.	Default gateway of this machine

[DNS Host]

Item	Description	Prior check
[Dynamic DNS Settings]	Select [Enable] when automatically registering the host name specified in [DNS Host Name] with the DNS server that supports the Dynamic DNS function.	Is Dynamic DNS supported?
[DNS Host Name]	Specify the host name of this machine (up to 63 characters).	

[DNS Domain]

Item	Description	Prior check
[Domain Name Auto Retrieval]	Select whether to automatically obtain the domain name. This item is necessary when DHCP is enabled.	Can it be obtained automatically using DHCP?
[Search Domain Name Auto Retrieval]	Select whether to automatically obtain the search domain name. This item is necessary when DHCP is enabled.	Can it be obtained automatically using DHCP?
[Default DNS Domain Name]	When not automatically obtaining the domain name, specify the name of the domain that contains this machine (up to 255 characters, including the host name).	Default Domain Name
[DNS Search Domain Name 1] to [DNS Search Domain Name 3]	Specify the DNS search domain name (up to 253 characters).	

[DNS Server Settings (IPv4)]

Item	Description	Prior check
[DNS Server Auto Obtain]	Select whether to automatically obtain the DNS server address. This item is necessary when DHCP is enabled.	Can it be obtained automatically using DHCP?
[Priority DNS Server]	Enter the address of the primary DNS server if you do not obtain the DNS server address automatically.	Server address
[Secondary DNS Server 1] to [Secondary DNS Server 2]	Specify the addresses of the secondary DNS servers.	Server address

[Device Setting]

In [Administrator Settings] on the **Control Panel**, select [Network Settings]▶▶[Forward]▶▶[Detail Settings]▶▶[Device Setting].
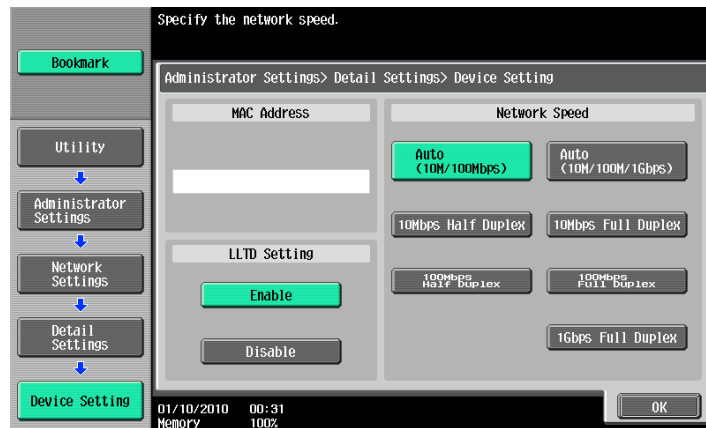
Item	Description	Prior check
[MAC Address]	Displays the MAC address of the network interface card of this machine.	
[Network Speed]	Specify the network speed.	

2.2   Communicating using IPv6

Configure settings for IPv6 communication.

These settings are required if you want use this machine with an IPv6 address assigned. You can use IPv6 together with IPv4, but you cannot use IPv6 alone.

When you use this machine in an IPv6 environment, the following restrictions apply.
- Printing with SMB is not supported (but it is allowed for the Direct Hosting service).
- No scanned data can be sent with SMB (but it is allowed for the Direct Hosting service).
- SMB browsing is not supported (available for Publication Service).
- NTLM authentication is not supported (but it is allowed for the Direct Hosting service).
- You cannot use the IP filtering function.
- You cannot use the installer of the printer driver (available for Windows Vista/Server 2008/7).
- You cannot display **PageScope Web Connection** in Flash.

Reference
For details on the Direct Hosting service, refer to the sections listed below.

"Sending scanned data to a computer on network" (p. 4-2)

"Print (SMB)" (p. 5-4)

"Restricting users of this machine (Windows domain or workgroup)" (p. 7-15)

[TCP/IP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [TCP/IP Setting] ►► [TCP/IP Setting].

Item	Description	Prior check
[TCP/IP Setting]	Select [ON].	
[IPv6]	Select [ON].	

Item	Description	Prior check
[Auto IPv6 Settings]	To obtain the IPv6 address automatically, select [ON].	Do you obtain the IPv6 address automatically?
[DHCPv6 Setting]	To use DHCPv6 to obtain the IPv6 address, select [ON].	Do you use DHCPv6?
[Link-Local Address]	Displays the link-local address generated from the MAC address.	
[Global Address]	If you do not obtain the IPv6 address automatically, enter the IPv6 global address.	IPv6 address
[Prefix Length]	If you do not obtain the IPv6 address automatically, enter the prefix length of the IPv6 global address.	Prefix Length
[Gateway Address]	If you do not obtain the IPv6 address automatically, enter the IPv6 gateway address.	Gateway Address
[DNS Server Setting (IPv6)]	Configure the DNS server settings as necessary.	
[DNS Server Auto Obtain]	Select whether to obtain the DNS server address automatically. This setting is required if DHCPv6 is enabled.	Can be obtained automatically with DHCPv6?
[Priority DNS Server]	Enter the address of the primary DNS server if you do not obtain the DNS server address automatically.	Server address
[Secondary DNS Server 1] to [Secondary DNS Server 2]	Specify the addresses of the secondary DNS servers.	Server address

3 Using PageScope Web Connection

3   Using PageScope Web Connection

3.1   Using PageScope Web Connection

Configure settings to use **PageScope Web Connection**.

PageScope Web Connection is a device management utility that is supported by the HTTP server built into this machine. Using a Web browser on a computer connected to the network, you can change machine settings and check the status of the machine. You can also handle some settings, which are to be configured on the **Control Panel** of this machine, through your computer.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
            ┌──────────────────────────┐
            │   [TCP/IP Settings]      │
            └──────────────────────────┘
                         │
            ┌──────────────────────────┐
            │   [PSWC Settings]        │
            └──────────────────────────┘
                         │
            ┌──────────────────────────┐
            │  [TCP Socket Settings]   │
            └──────────────────────────┘
                         │
            ┌──────────────────────────┐
            │ Do you use SSL communi-  │─────────┐
            │ cation?                  │         │
            └──────────────────────────┘         │
                   Yes                    No      │
            ┌──────────────────────────┐         │
            │ [Device Certificate      │         │
            │  Setting]                │         │
            └──────────────────────────┘         │
                         │                        │
            ┌──────────────────────────────────────┐
            │             Finish                    │
            └──────────────────────────────────────┘
```
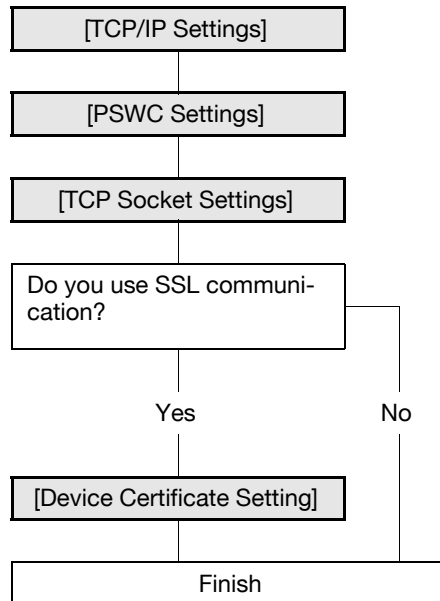
3.1.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

3.1.2 [PSWC Settings]

In [Administrator Settings] on the **Control Panel**, select [Network Settings]▸▸[HTTP Server Settings].

📖 **Reference**
For details on how to go to the [Network Settings] screen, refer to page 15-3.
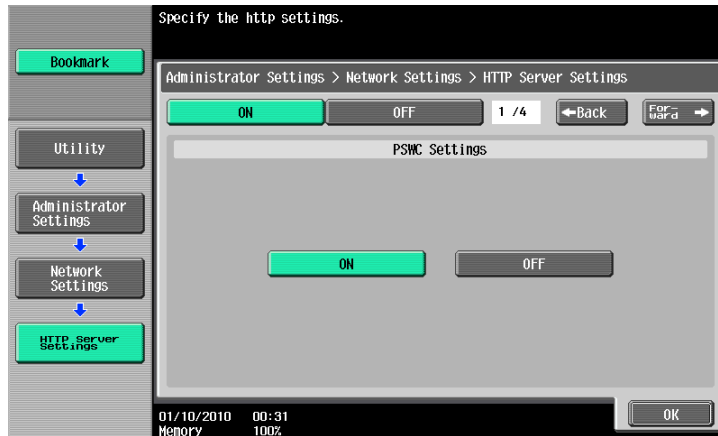
Item	Description	Prior check
[PSWC Settings]	Select [ON].	

3.1.3 [TCP Socket Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP Socket Settings].

📖 **Reference**
*For details on how to log in to the administrator mode of **PageScope Web Connection**, refer to page 3-5.*
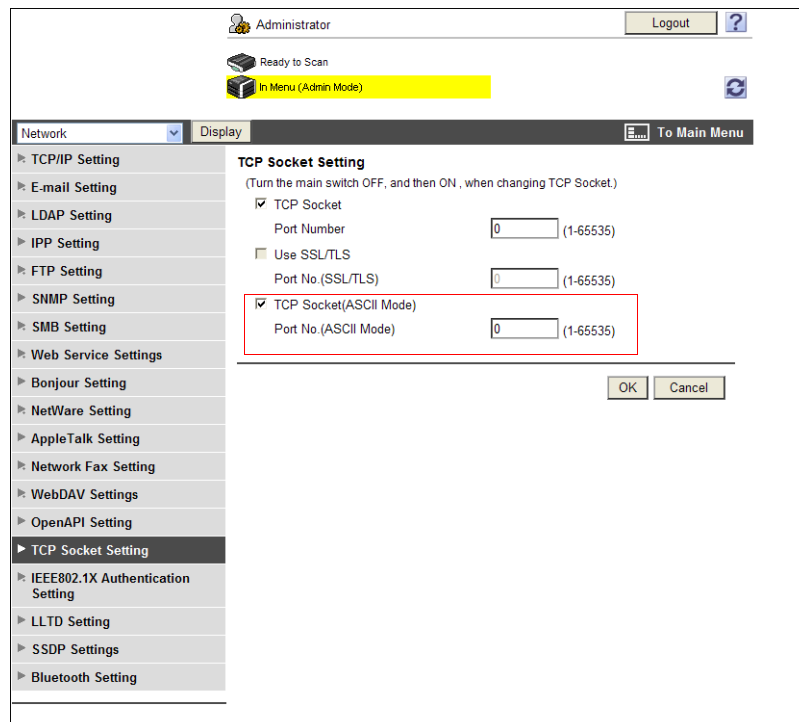
Item	Description	Prior check
[TCP Socket (ASCII Mode)]	Select this check box to use **PageScope Web Connection** in the flash format.	
[Port Number (ASCII Mode)]	Enter a port number.	

3.1.4   [Device Certificate Setting]

Configure settings for encrypting communication from a computer to this machine using SSL.

For details, refer to page 8-2.
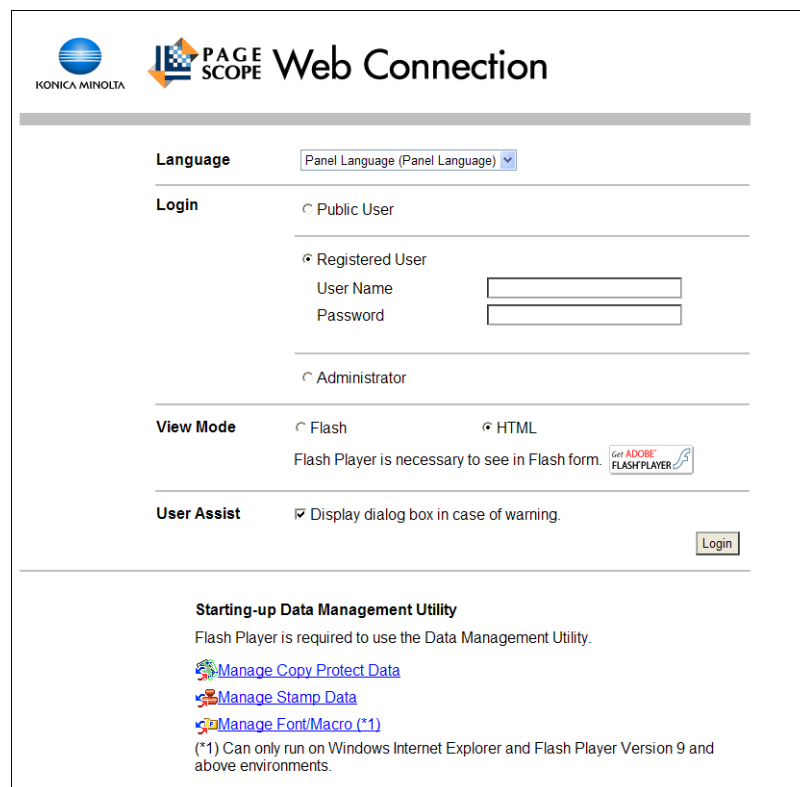
3.2 Logging in to the administrator mode

To configure this machine with **PageScope Web Connection**, log in to the administrator mode. The following shows a procedure to log in to the administrator mode.

Reference

- If you are already logging in to the administrator mode, you cannot use the **Control Panel** of this machine to perform operations.
- Depending on the status of this machine, you may not be able to log in to the administrator mode.
- If you access **PageScope Web Connection** while User Authentication or Account Track is not enabled, you will see the screen displayed when you logged in as the public user. To log in as an administrator, log out from the public user mode once.

1 In the login page, select [Administrator] and click [Login].
   ➜ If necessary, select the [Language] and [View Mode].
   ➜ The flash display can be restricted if necessary. For details on configuring the setting, refer to page 3-11.
   ➜ Selecting the [Display dialog box in case of warning] check box displays a dialog box when a warning has occurred during operation.

2 Enter the administrator password of this machine.
   ➜ If an incorrect password is entered the specified number of times while [Security Settings]▸▸[Security Details]▸▸[Prohibited Functions When Authentication Error] is set to [Mode 2] in [Administrator Settings] of the **Control Panel**, it will no longer be possible to log in to the administrator mode.

→ You can specify whether to use Popup Help in [Help Display Setting]. For details, refer to page 3-8.

3 Click [OK].

The administrator mode window appears.

3.3   Specifying the display mode of the administrator mode.

You can select the display mode of the **PageScope Web Connection** administrator mode from [Tab Function Display] or [List Function Display].

[Display Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings]▸▸[Display Setting].
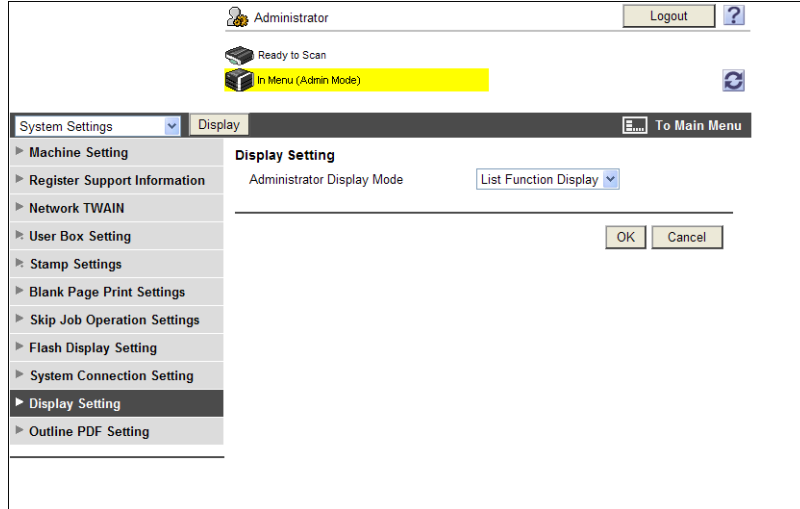
Item	Description
[Administrator Display Mode]	Select the display mode of the administrator mode.

[Tab Function display]
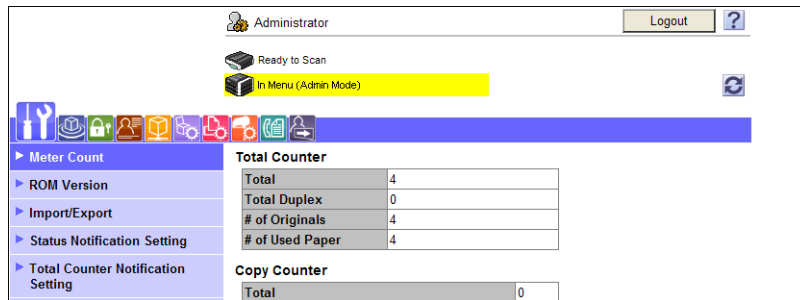
[List Function display]
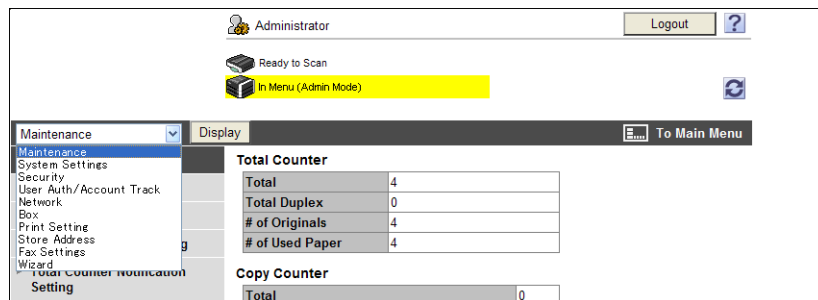
Reference
- This manual shows an example where the [List Function Display] is set as the display mode.

3.4 Using Popup Help

You can use Popup Help on the [Network] page of **PageScope Web Connection**.

Selecting a specific item in a page using On-Mouse or On-Focus (click) displays the explanation of the item in a popup window, so you can specify each item while checking its meaning.

Reference
- Help can be displayed only for network settings.
- Popup help can be displayed using two methods: On-Mouse and On-Focus (click). Whether to use On-Mouse or On-Focus can be specified individually.

[Help Display Setting]
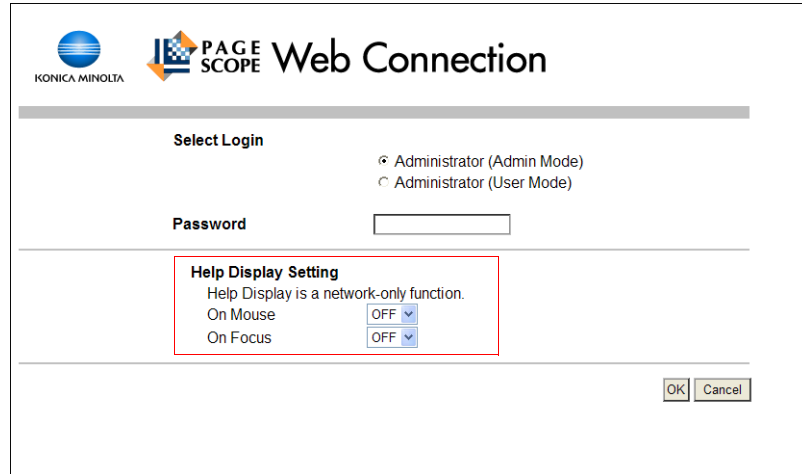
Item	Description
[On Mouse]	Select whether to display popup help using On-Mouse. To use On-Mouse, place the mouse over the desired setting item; its explanation appears on the right of the page.
[On Focus]	Select whether to display popup help using On-Focus. To use On-Focus, click the desired setting item entry area or option; its explanation appears on the right of the page.

Popup Help Display Example
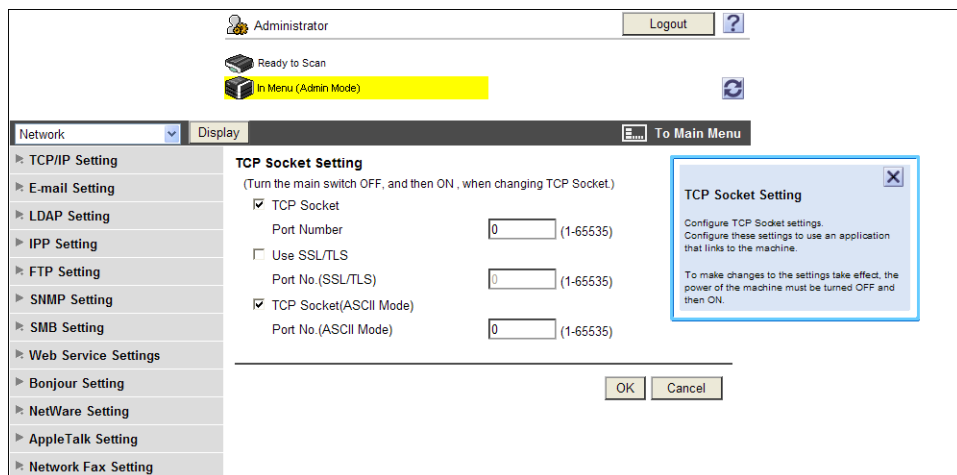
3.5   Configuring Settings for each Purpose via Wizard

[Wizard] allows you to easily configure settings for using the following functions according to the instructions shown by a wizard.

[TX Setting for scan documents.]
- [Transmit the scanned data via E-mail]
- [Transmit the scanned data via E-mail (attach Digital Signature)]
- [Transmit the scanned data via E-mail (Public Key Encryption)]

[Network print settings.]
- [LPR Print]
- [Print using RAW port]
- [Print using SMB]

[Restrict users from using this device.]
- [Do Not Authenticate]
- [User Authentication Only]
- [Account Track Only]
- [User Authentication & Account Track]
- [External Authentication Server]

3.5.1   Screen Components

The [Wizard] page has the following components.
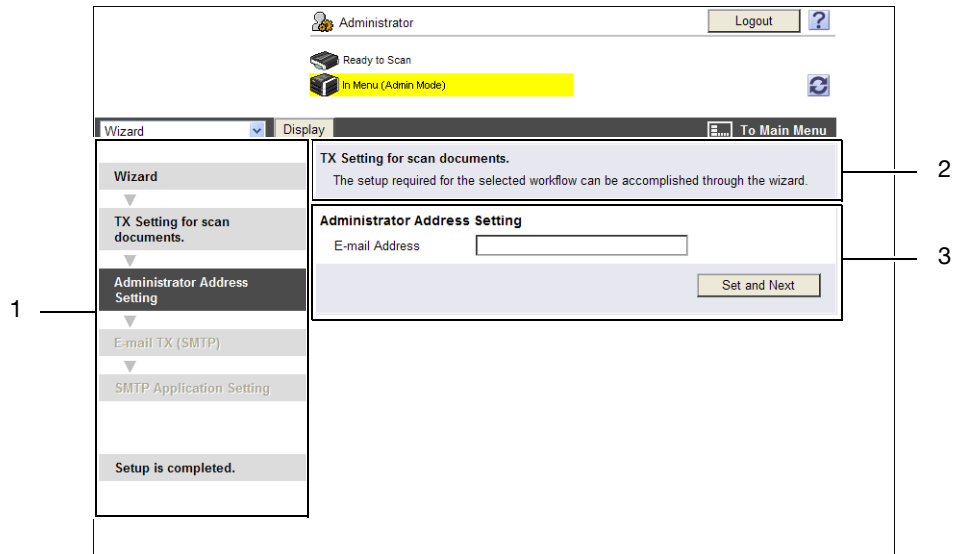
No.	Item	Description
1	Flow	Displays a setting flow to use the desired function. The currently enabled items are displayed in dark gray.
2	View Purpose	Displays the selected purpose.
3	View Settings	Displays settings.

3.5.2   [Wizard]

In the administrator mode of **PageScope Web Connection**, select [Wizard]. Select the desired purpose, and configure its setting according to the instructions shown by the wizard.
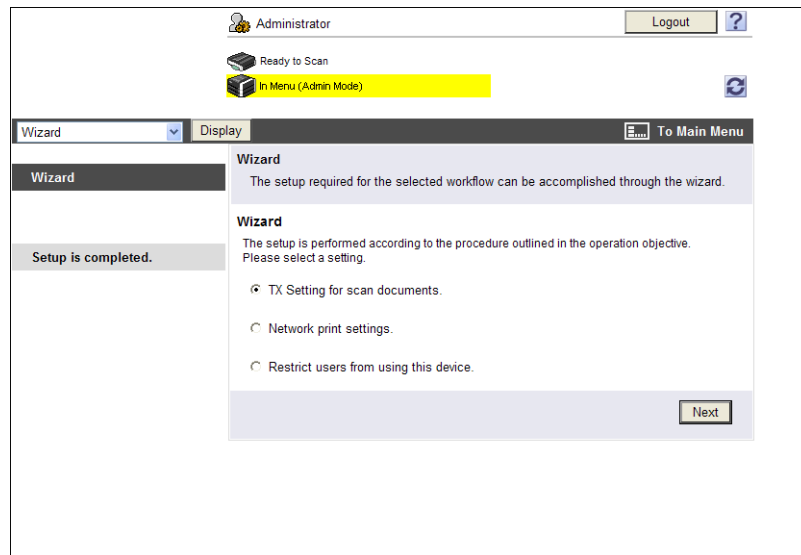
Reference

- To return to the previous setting item during the setting procedure, click the desired setting item using Flow. If you return to the previous item, perform re-configuration from its settings.
- To end the setting procedure, click [Setup is completed.] in Flow.

3.6   Disabling Flash View

You can disable the flash view in **PageScope Web Connection**.

Reference
- Disabling the flash view fixes the view mode to the HTML format.
- Disabling the flash view invalidates Data Management Utility.

[Flash Display Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings]▶▶[Flash Display Setting].
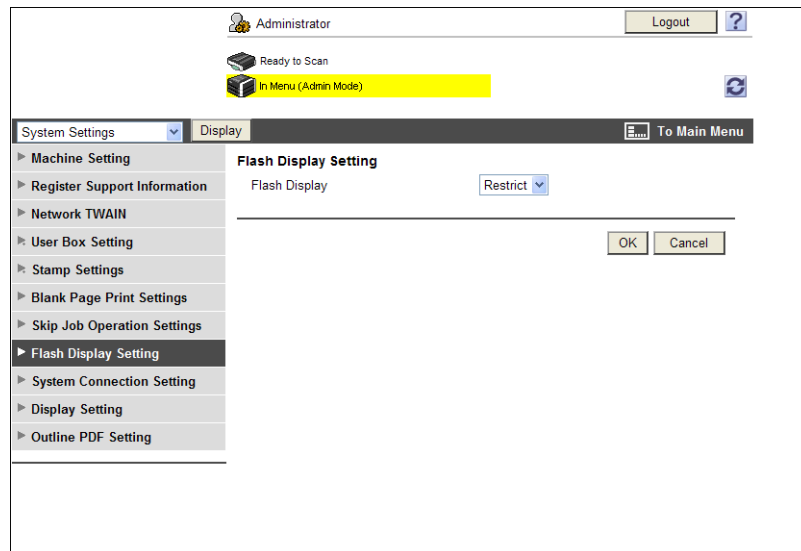
Item	Description
[Flash Display]	To disable the flash view, select [Restrict].

3.7   Specifying the Automatic Logout Time

Configure time before auto logout from the administrator or user mode of **PageScope Web Connection**.

If no operation is performed for a predefined length of time, the user will automatically be logged out.

[Auto Logout]

In the administrator mode of **PageScope Web Connection**, select [Security] ▸▸ [Auto Logout].
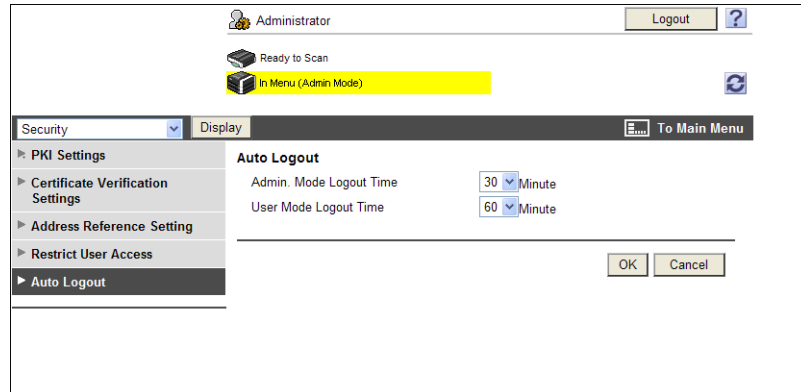
Item	Description
[Admin. Mode Logout Time]	Select the time period before the user will automatically be logged out when no operations have been performed in the administrator mode.
[User Mode Logout Time]	Select the time period before the user will automatically be logged out when no operations have been performed in the user mode.

4 Scanning

4   Scanning

4.1   Sending scanned data to a computer on network

Configure settings to send scanned data to a computer on network (SMB transmission).

Before SMB transmission, configure settings to share files in Windows using the computer that receives data.

If Samba is installed, data can be transmitted to a computer that is equipped with a non-Windows OS. SMB transmission is also available for the CIFS service (TCP/IP) that is running on the NetWare server.

To specify a computer over a router using the Windows name (NetBIOS name), use the WINS server.

To perform SMB sending in the IPv6 environment, enable the direct hosting service. Enabling the direct hosting service allows you to specify the destination with the IPv6 address or computer name (host name). When specify the destination with the computer name (host name), use the DNS server to obtain the IPv6 address.

To send data to a computer with Windows Vista/Server 2008/7 installed, you can perform name resolution using the LLMNR function even if DNS server is not present. To perform the name resolution especially in the IPv6-only communication environment under Windows Vista/Server 2008/7, it will be convenient to enable the LLMNR function.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                          ┌────────────────────┐
                          │  [TCP/IP Settings]  │
                          └────────────────────┘
                          ┌────────────────────┐
                          │  [Client Setting]   │
                          └────────────────────┘
                          ┌────────────────────┐
                          │  IPv6 environment?  │
                          └────────────────────┘
              No                                        Yes

  ┌──────────────────────────┐                ┌────────────────────────┐
  │ Do you use the WINS       │                │ [Direct Hosting Setting]│
  │ server?                   │                └────────────────────────┘
  └──────────────────────────┘
       Yes              No

  ┌────────────────────┐
  │   [WINS Setting]    │
  └────────────────────┘
                          ┌────────────────────┐
                          │ Do you send data to │
                          │ Windows Vista/Server│
                          │ 2008/7?             │
                          └────────────────────┘
              No                    Yes
                          ┌────────────────────┐
                          │   [LLMNR Setting]   │
                          └────────────────────┘
                          ┌────────────────────┐
                          │       Finish        │
                          └────────────────────┘
```
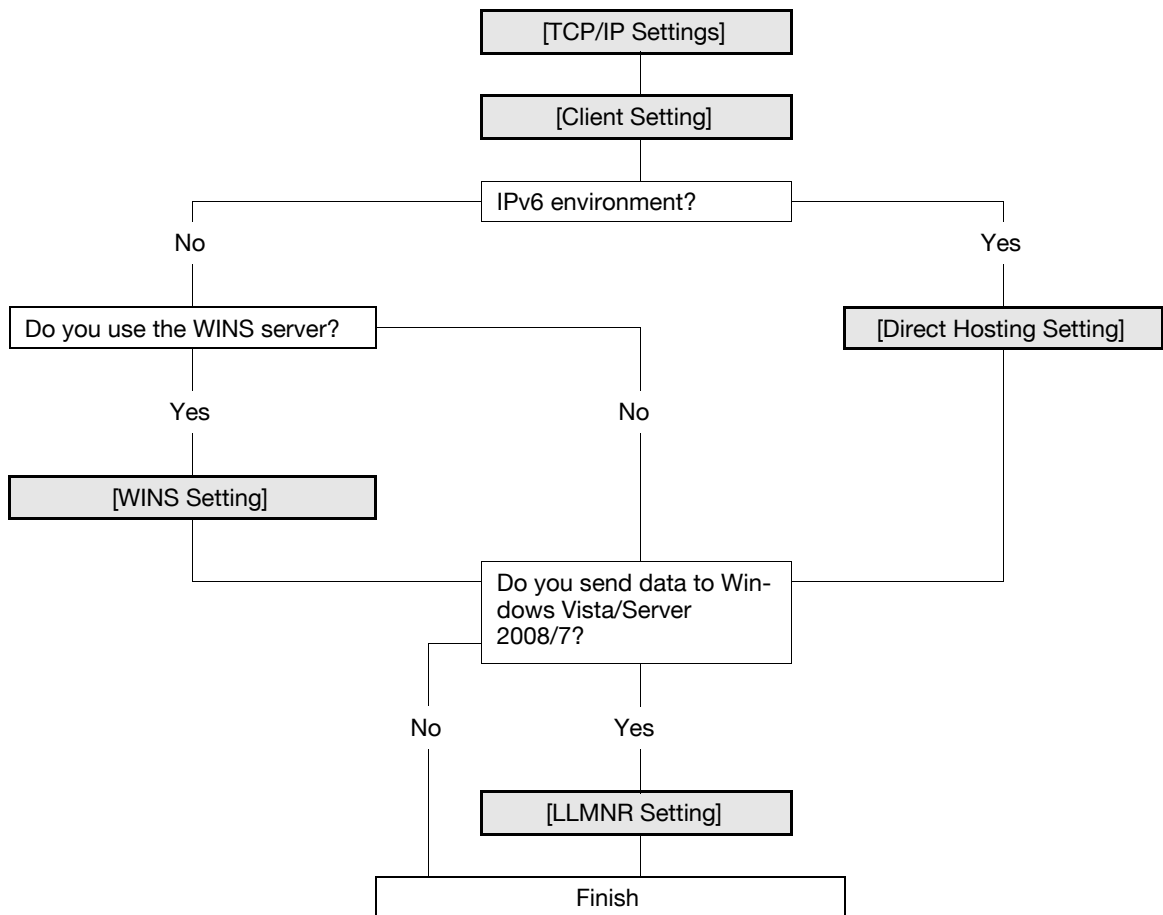
📖 **Reference**
For details on how to register the SMB address, refer to page 11-7.

For details on SMB file sending, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.1.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.
● To specify the destination computer with the computer name (host name) for SMB transmission in IPv6 environment, prepare a DNS server and configure DNS settings in this machine.

For details, refer to page 2-2.

4.1.2 [Client Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [SMB Setting] ▶▶ [Client Setting].

Item	Description	Prior check
[SMB TX Setting]	Select [ON].	
[NTLM Setting]	Specify the NTLM version. To perform SMB transmission for Windows sharing (Mac OSX) or Samba (Linux/Unix), select [v1]. To perform SMB transmission for Windows 98SE or Windows Me, select [v1/v2] or [v1].	OS of destination computer
[DFS Setting]	To perform SMB transmission in a DFS (Distributed File System) environment, select [Enable].	DFS environment?

4.1.3 [WINS Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [SMB Setting] ►► [WINS Setting].

Item	Description	Prior check
[WINS]	To use the WINS server, select [ON].	
[Auto Obtain Setting]	To automatically obtain the WINS server address, select [Enable]. This item is necessary when DHCP is enabled.	Can it be obtained automatically using DHCP?
[WINS Server Address1] to [WINS Server Address2]	Enter the WINS server address. Format: *.*.*.* (Asterisk * can be 0 to 255)	Server address
[Node Type Setting]	Specify the name resolution method. • [B Node]: Query by broadcast • [P Node]: Query the WINS server • [M Node]: Query by broadcast, and then query the WINS server • [H Node]: Query the WINS server, and then query by broadcast	

4.1.4   [Direct Hosting Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [SMB Setting] ►► [Direct Hosting Setting].

Item	Description	Prior check
[Direct Hosting Setting]	To use IPv6 addresses for communication, select [ON].	IPv6 environment?

4.1.5   [LLMNR Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [TCP/IP Setting] ►► [TCP/IP Setting].

Item	Description	Prior check
[LLMNR Setting]	To perform name resolution to send data to a computer with Windows Vista/Server 2008/7 installed in the environment where the DNS server is not running, select [Enable]. To perform the name resolution especially in the IPv6-only communication environment, enable this setting.	• Is the computer Windows Vista/Server 2008/7? • Is the DNS server not used?

4.2   Sending scanned data to your computer (Scan to Home)

Configure settings to send scanned data to your computer.

This function is available when the user's Home folder position is registered after user authentication has been performed with Active Directory.

If the Home folder of the user who logged in is registered in Active Directory, [Home] is displayed in the address book. Specify [Home] for a destination to enable you to easily send data to your Home folder.

To authenticate the user to send data to the Home folder, use the [User Name] and [Password] that were used in Active Directory authentication when you logged in to this machine.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                        ┌─────────────────────────┐
                        │     [TCP/IP Settings]    │
                        └─────────────────────────┘
                                     │
                        ┌─────────────────────────┐
                        │ User authentication (Ac- │
                        │     tive Directory)      │
                        └─────────────────────────┘
                                     │
                        ┌─────────────────────────┐
                        │  [Scan to Home Settings] │
                        └─────────────────────────┘
                                     │
                        ┌─────────────────────────┐
                        │      [Client Setting]    │
                        └─────────────────────────┘
                                     │
                  ┌──────────────────────────────────┐
        No        │         IPv6 environment?         │        Yes
     ┌────────────┤                                   ├────────────┐
     │            └──────────────────────────────────┘            │
     │                                                            │
┌──────────────────────────┐                         ┌─────────────────────────┐
│ Do you use the WINS server? ├──────────────┐       │ [Direct Hosting Setting]│
└──────────────────────────┘               │         └─────────────────────────┘
     Yes                                    No                     │
      │                                     │                      │
┌──────────────────┐                        │                      │
│  [WINS Setting]  │                        │                      │
└──────────────────┘                        │                      │
      │                  ┌──────────────────────────────┐          │
      └──────────────────┤ Do you send data to Win-     ├──────────┘
                         │ dows Vista/Server            │
                         │ 2008/7?                      │
                         └──────────────────────────────┘
                            No              Yes
                             │               │
                             │      ┌──────────────────┐
                             │      │  [LLMNR Setting] │
                             │      └──────────────────┘
                             │               │
                          ┌──────────────────────────┐
                          │          Finish           │
                          └──────────────────────────┘
```
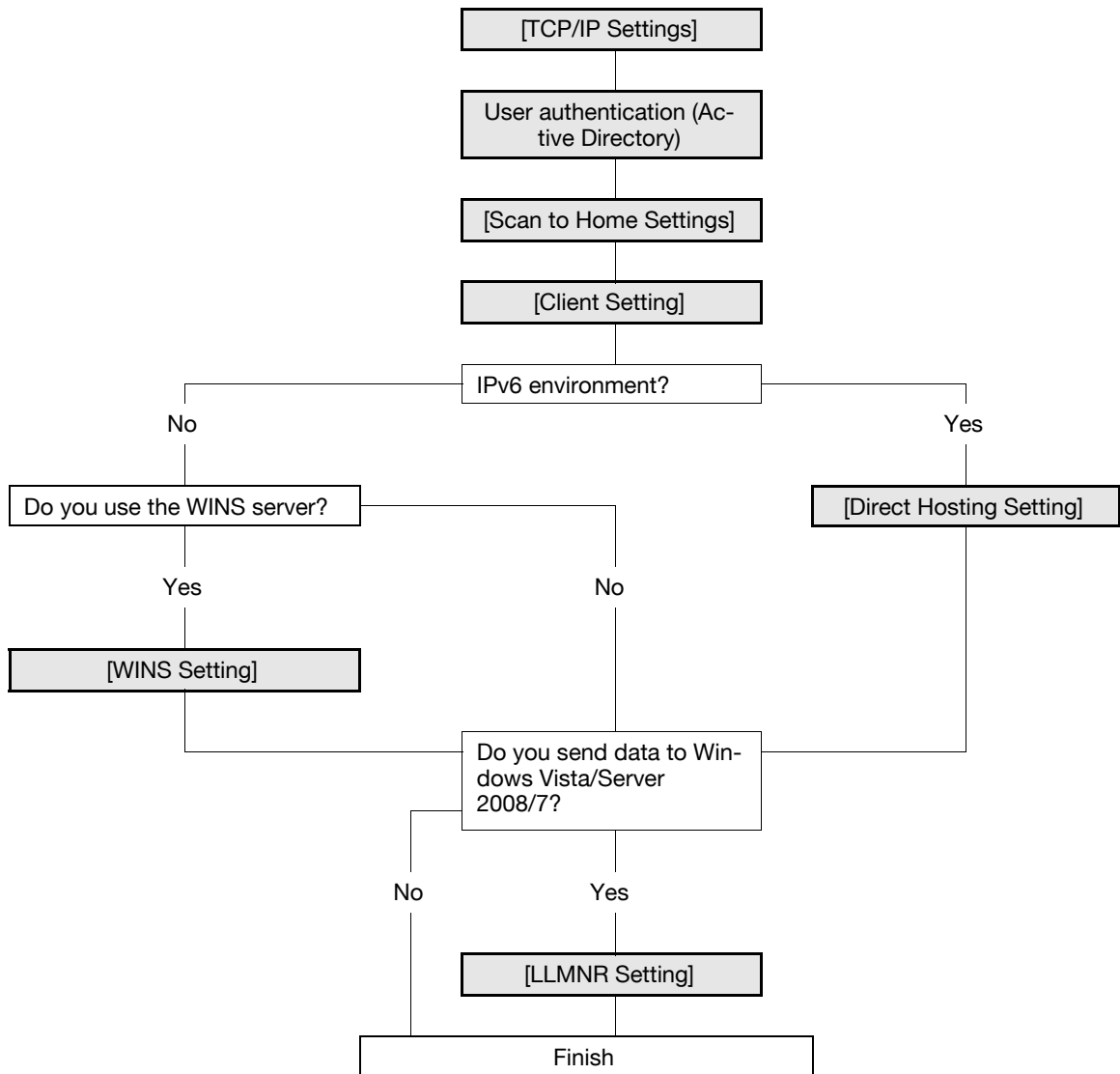
Reference

- To use the Scan to Home function, the Home folder of the user must be registered in Active Directory. Also, the user's E-mail address or fax number must be registered.
- When you register the location of the Home folder in Active Directory, use uppercase letters to specify a computer that has the Home folder using the NetBIOS name.
- For details on how to send a file to the Home folder using SMB, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.2.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

- To specify the destination computer with the computer name (host name) for SMB transmission in IPv6 environment, prepare a DNS server and configure DNS settings in this machine.

For details, refer to page 2-2.

4.2.2 User authentication (Active Directory)

Configure settings to restrict users who use this machine with Active Directory.

For details, refer to page 7-10.

4.2.3 [Scan to Home Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [Scan to Home Settings].
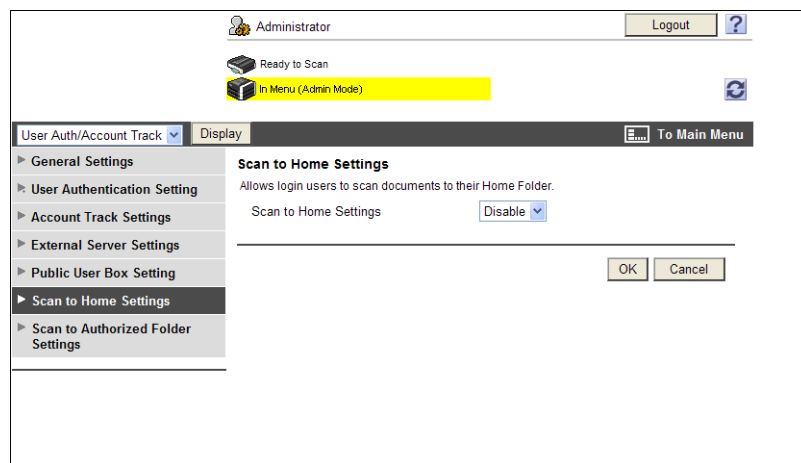
Item	Description	Prior check
[Scan to Home Settings]	Select [Enable].	

4.2.4 [Client Setting]

Configure SMB client settings.

For details, refer to page 4-3.

4.2.5 [WINS Setting]

To perform SMB transmission via routers, configure the WINS server settings.

For details, refer to page 4-4.

4.2.6 [Direct Hosting Setting]

To perform SMB transmission in an IPv6 environment, enable the Direct Hosting service.

For details, refer to page 4-5.

4.2.7 [LLMNR Setting]

To perform name resolution in the environment configured to communicate with Windows Vista/Server 2008/7, and where the DNS server is not running, enable the LLMNR function.

For details, refer to page 4-5.

4.3   Sending scanned data by E-mail

Configure settings to send scanned data to the specified E-mail address as an attachment file.

These settings are available when the SMTP server supports SMTP over SSL or Start TLS. SSL/TLS enables data encryption, assuring a secure communication between this machine and the SMTP server.

If SMTP authentication is requested from the SMTP server, configure its settings.

If POP before SMTP authentication is requested from the SMTP server, configure its settings. These settings can be combined when the POP server supports POP over SSL or APOP authentication.

Use the following flowchart to configure settings.

```
                        [TCP/IP Settings]

                        E-mail Transmis-
                             sion

  Do you have an          SMTP authenti-        POP before SMTP?
  SSL/TLS communi-          cation?
  cation with the
  SMTP server?

     Yes      No         Yes        No          Yes              No

  SMTP over             SMTP Authenti-         POP before SMTP
  SSL/Start TLS            cation

                                               (1) POP over SSL?
                                               (2) APOP?

                                                  Yes        No

                                               (1) POP over SSL
                                               (2) APOP Authenti-
                                                      cation

                             Finish
```
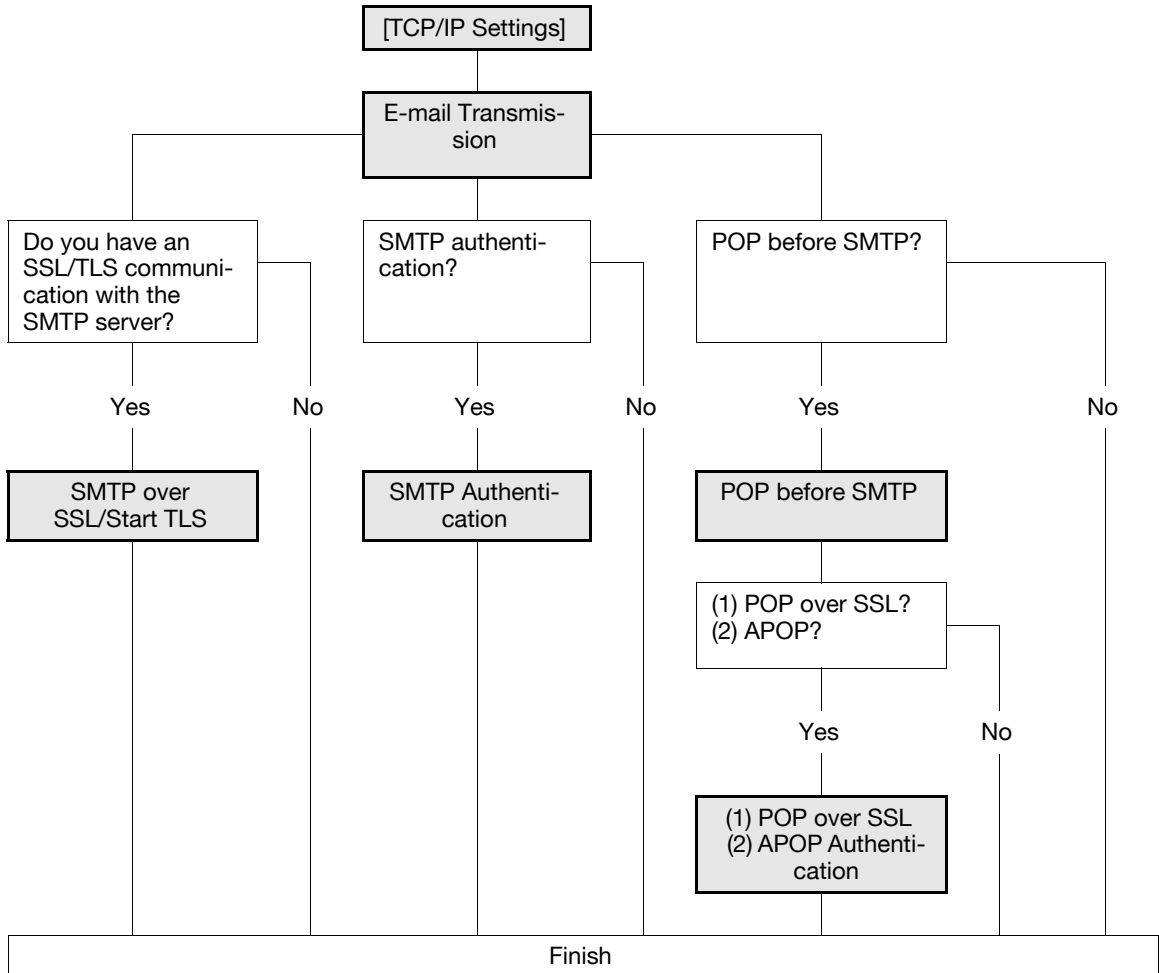
📖 **Reference**
For details on how to register E-mail addresses, refer to page 11-7.

For details on how to send a file by E-mail, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.3.2   E-mail Transmission

[E-mail TX (SMTP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail Transmission (SMTP)].

Item	Description	Prior check
[E-mail TX Setting]	Select the [E-mail TX (SMTP)] check box.	
[Scan to E-mail]	Select [ON].	
[SMTP Server Address]	Enter the SMTP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port Number]	Enter a port number. Default setting: 25	Server port number
[Connection Timeout]	Specify the timeout period for a communication with a server.	
[Max Mail Size]	Select whether to limit the size of an E-mail to be sent.	
[Server Capacity]	Enter the SMTP server capacity. A mail that exceeds the upper limit of the server capacity will be discarded. If an E-mail is divided, this setting is made invalid.	Server reception limit
[Admin. E-mail Address]	Displays the E-mail address of the administrator.	

Item	Description	Prior check
[Binary Division]	Select this check box to divide an E-mail. If the E-mail software that received an E-mail does not have a restoration function, you may not be able to read the E-mail.	Restoration function of E-mail software
[Divided Mail Size]	Enter the divided mail size to divide an E-mail.	Server reception limit

[Administrator E-Mail Address]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [Machine Setting].

Item	Description	Prior check
[E-mail Address]	Enter the administrator's E-mail address (up to 128 characters). If the administrator's E-mail address is omitted, you will not be able to send an E-mail. Usually, the administrator's E-mail address is set to the From address of the E-mail to be sent from this machine. To enable user authentication, the user's E-mail address is set to the From address. However, when the user's E-mail address is not registered or S/MIME is used to send an E-mail, the administrator's E-mail address is set to the From address. If [Security]►►[Restrict User Access]►►[Changing the "From" Address] is set to [Allow], the user can change the From address before sending an E-mail.	E-mail address of the administrator

4.3.3   SMTP over SSL/Start TLS

[E-mail TX (SMTP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail Transmission (SMTP)].

Item	Description	Prior check
[Use SSL/TLS]	To encrypt a communication between this machine and the SMTP server using SSL/TLS, select [SMTP over SSL] or [Start TLS].	Does the server support SSL or Start TLS?
[Port Number]	Enter a port number if [Start TLS] is selected. Default setting: 25	Server port number
[Port No.(SSL)]	Enter the port number to be used for SSL communication if [SMTP over SSL] is selected. Default setting: 465	Server port number

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	
[CN]	Select whether to check that the CN of the server certificate matches the server address.	
[Key Usage]	Select whether to check that the server certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the server certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	

Item	Description	Prior check
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

4.3.4   SMTP Authentication

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail TX (SMTP)].

Item	Description	Prior check
[SMTP Authentication]	Select this check box to perform SMTP authentication. For SMTP authentication, the authentication method with the highest strength that is supported by the SMTP server is automatically selected from Digest-MD5, CRAM-MD5, PLAIN, and LOGIN.	Is SMTP authentication requested by the server?
[User ID]	Enter the user ID for SMTP authentication (up to 255 bytes).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password for SMTP authentication (up to 128 bytes, excluding space and ").	
[Domain Name]	Enter the domain name (realm) for SMTP authentication (up to 255 characters). This setting is required when the authentication method is set to Digest-MD5. If there is only one user domain (realm), you do not need to enter this item because the domain name is reported from the SMTP server at initial communication, and with the domain name, a communication is established automatically. If there are two or more user domains (realm), specify the user domain name.	Authentication Method
[Authentication Setting]	For user authentication, select whether to synchronize SMTP authentication with user authentication. Selecting [User Authentication] uses the user name and password for user authentication as those for SMTP authentication. Selecting [Set Value] uses the values specified in [User ID] and [Password].	Synchronized with user authentication?

4.3.5 POP before SMTP

[POP before SMTP]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [E-mail Setting] ▸▸ [E-mail TX (SMTP)].

Item	Description	Prior check
[POP before SMTP]	Select [ON] to perform POP before SMTP authentication.	Is POP before SMTP authentication requested by the server?
[POP Before SMTP Time]	Enter the period from a time you log in to the POP server to a time you access the SMTP server. If the POP and SMTP servers are in different computers, it will take time to notify the SMTP server that you have logged in to the POP server. Therefore, if a too short time is specified, sending of E-mails may fail.	Are the POP and SMTP servers in different computers?

[E-mail RX (POP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [E-mail Setting] ▸▸ [E-mail RX (POP)].

Item	Description	Prior check
[E-mail RX Setting]	Select [ON] to perform POP before SMTP authentication.	
[POP Server Address]	Enter the POP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Login Name]	Enter the login name of the POP server (up to 63 characters).	

Item	Description	Prior check
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the POP server (up to 15 characters).	
[Connection Time-out]	Specify the timeout period for a communication with a server.	
[Port Number]	Enter a port number. Default setting: 110	Server port number

4.3.6   POP over SSL

[E-mail RX (POP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail RX (POP)].

Item	Description	Prior check
[Use SSL/TLS]	Select this check box to encrypt a communication between this machine and POP server.	Does the server support SSL?
[Port Number (SSL)]	Enter the port number to be used for SSL communication. Default setting: 995	Server port number
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	
[CN]	Select whether to check that the CN of the server certificate matches the server address.	
[Key Usage]	Select whether to check that the server certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the server certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

4.3.7 APOP Authentication

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail RX (POP)].

Item	Description	Prior check
[APOP Authentica-tion]	Select [ON] to encrypt the login name and password when logging in to the POP server. The password is encrypted with MD5 to log in to the POP server using APOP. Before you select [ON], check whether the POP server supports APOP. If the POP server does not support APOP, it results in an error, causing a communication failure.	Is APOP authentica-tion requested by the server?

4.4   Sending scanned data to the user's E-mail address (Scan to Me)

Configure settings to send scanned data to the user's E-mail address.

This function is available when user authentication is enabled and the E-mail address is registered as user information.

If the login user's E-mail address is registered, [Me] is displayed in the address book. Specify [Me] for the address to enable you to easily send data to your E-mail address.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                            [TCP/IP Settings]

                            User Authentica-
                                 tion

                            Scan to E-Mail

   Do you have an          SMTP authenti-          POP before
   SSL/TLS communi-        cation?                 SMTP?
   cation with the
   SMTP server?

      Yes      No          Yes       No            Yes            No

   SMTP over             SMTP Authenti-          POP before SMTP
   SSL/Start TLS         cation

                                                 (1) POP over SSL?
                                                 (2) APOP?

                                                   Yes        No

                                                 (1) POP over SSL
                                                 (2) APOP Authenti-
                                                     cation

                                 Finish
```
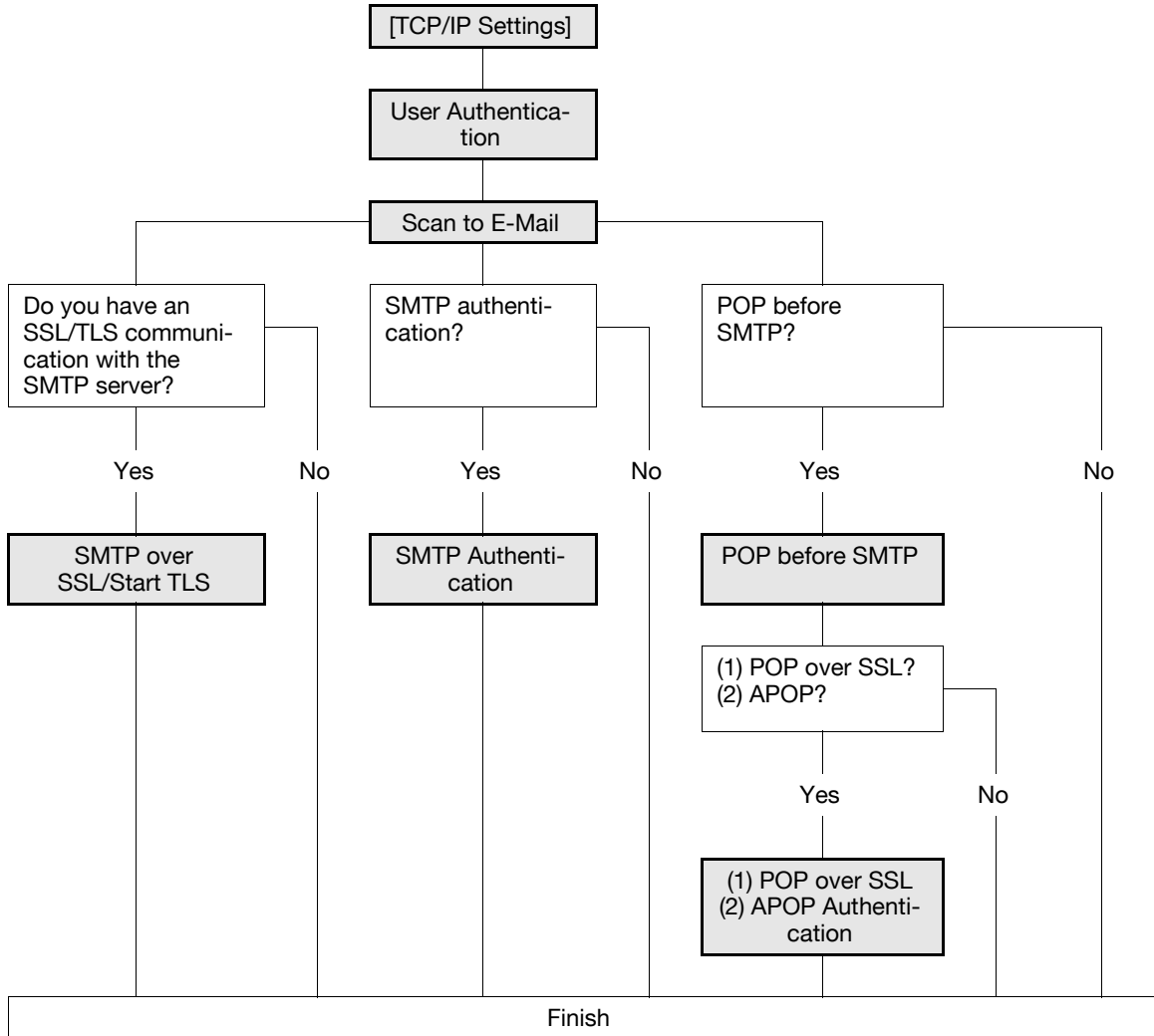
📖 **Reference**
For details on how to send a file to the user's own E-mail address, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.4.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.4.2   User Authentication

Configure settings to restrict users who use this machine.

When the MFP authentication is selected

When the MFP authentication is selected, do the following.
- Configure the settings required for the MFP authentication
- Register the E-mail address of each user when registering users

For details on the settings for the MFP authentication and user registration, refer to page 7-2.

When the Active Directory authentication is selected

When the Active Directory authentication is selected, do the following.
- Configure the settings required for the Active Directory authentication
- Register the E-mail address of each of the users from this machine with the server to enable this machine to obtain the address using the LDAP protocol

For details on Active Directory authentication settings, refer to page 7-10.

When the NTLM or NDS authentication is selected

When the NTLM or NDS authentication is selected, do the following.
- Configure the settings required for the NTLM or NDS authentication
- Register the E-mail address of each user in User Registration

For details on NTLM authentication settings, refer to page 7-15.

For details on NDS over IPX/SPX authentication settings, refer to page 7-19.

For details on NDS over TCP/IP authentication settings, refer to page 7-22.

4.4.3   Scan to E-Mail

Configure settings to send an E-mail.

For details, refer to page 4-9.

4.4.4   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

4.4.5   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

4.4.6   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

4.4.7   POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

4.4.8   APOP Authentication

Configure APOP authentication settings.

For details, refer to page 4-16.

4.5   Sending scanned data by E-mail (with digital signature)

Configure settings to send scanned data by E-mail with a digital signature.

Sending an E-mail with a digital signature enables you to prove that the E-mail has been sent from this machine and also to send a device certificate to the user. Using the obtained certificate (public key), the user can send an encrypted E-mail to this machine.

If necessary, you can combine POP before SMTP authentication, APOP authentication, SMTP authentication, and SSL/TLS encryption to have a communication.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference

● This function is available only when a **Hard Disk** is installed.
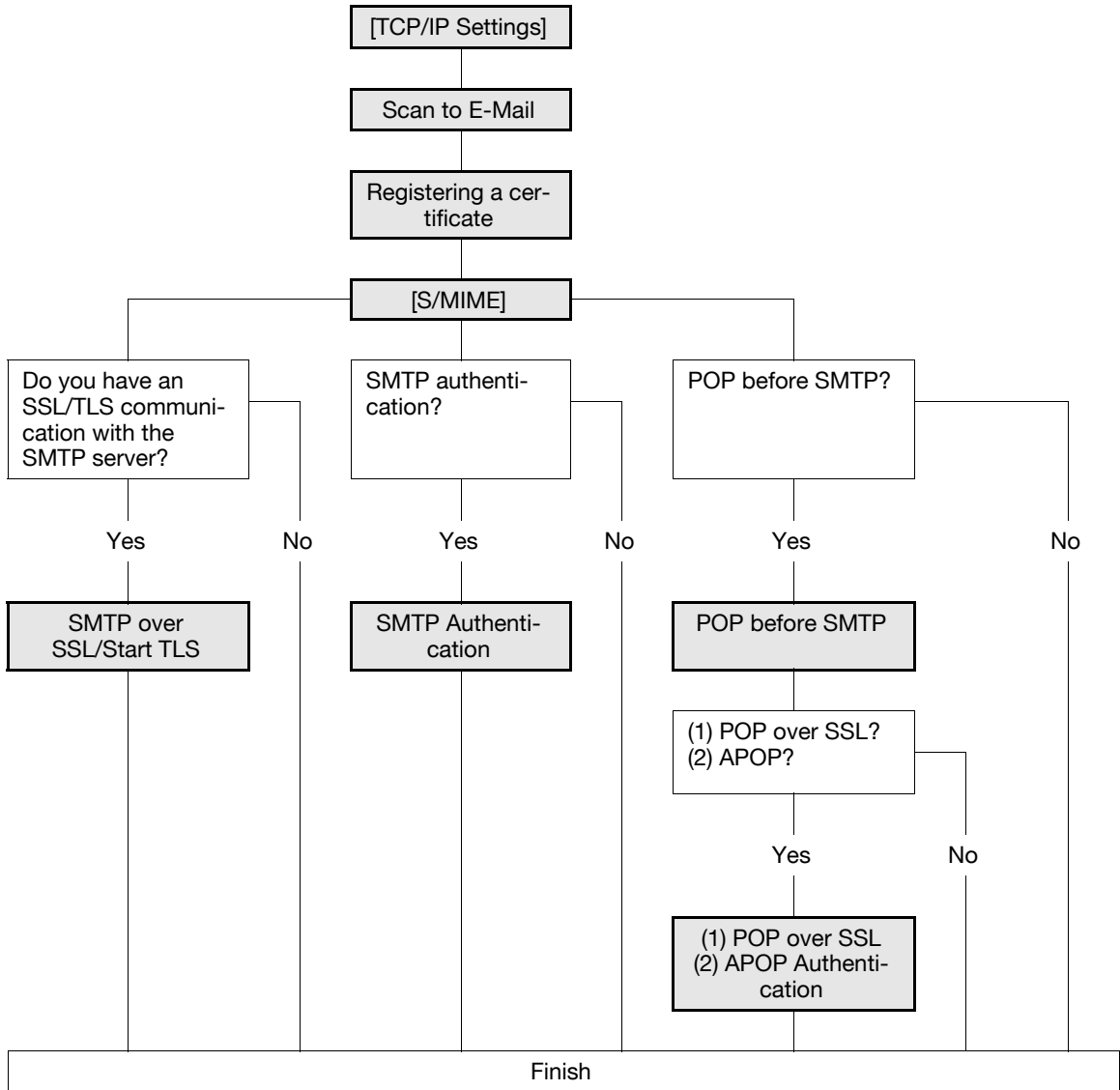
4.5.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.5.2   Scan to E-Mail

Configure settings to send an E-mail.

For details, refer to page 4-9.

4.5.3   Registering a certificate

Register a device certificate.

- You cannot send an E-mail if the administrator address of the device certificate used for digital signature does not match the From address of the E-mail.

For details, refer to page 8-2.

4.5.4   [S/MIME]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [S/MIME].
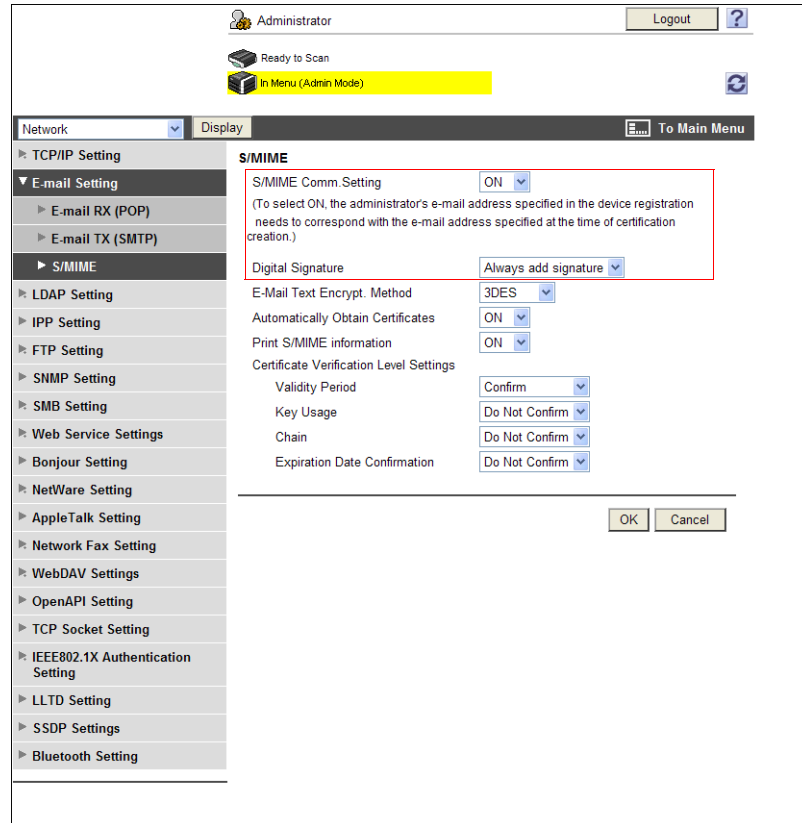
Item	Description	Prior check
[S/MIME Comm. Setting]	Select [ON].	
[Digital Signature]	Select [Always add signature] or [Select when sending].	

4.5.5   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

4.5.6   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

4.5.7   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

4.5.8 POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

4.5.9 APOP Authentication

Configure APOP authentication settings.

For details, refer to page 4-16.

4.6   Sending scanned data by E-mail (Encryption by public key)

Configure settings to encrypt an E-mail using the user certificate (public key) registered in this machine when sending scanned data by E-mail.

Sending an encrypted E-mail prevents information from being leaked to the third party on the transmission route. Combining a digital signature with an E-mail also enables you to perform the authentication of this machine and message. For details on settings for attaching a digital signature to an E-mail, refer to page 4-20.

If necessary, you can combine POP before SMTP authentication, APOP authentication, SMTP authentication, and SSL/TLS encryption to have a communication.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference

● This function is available only when a **Hard Disk** is installed.
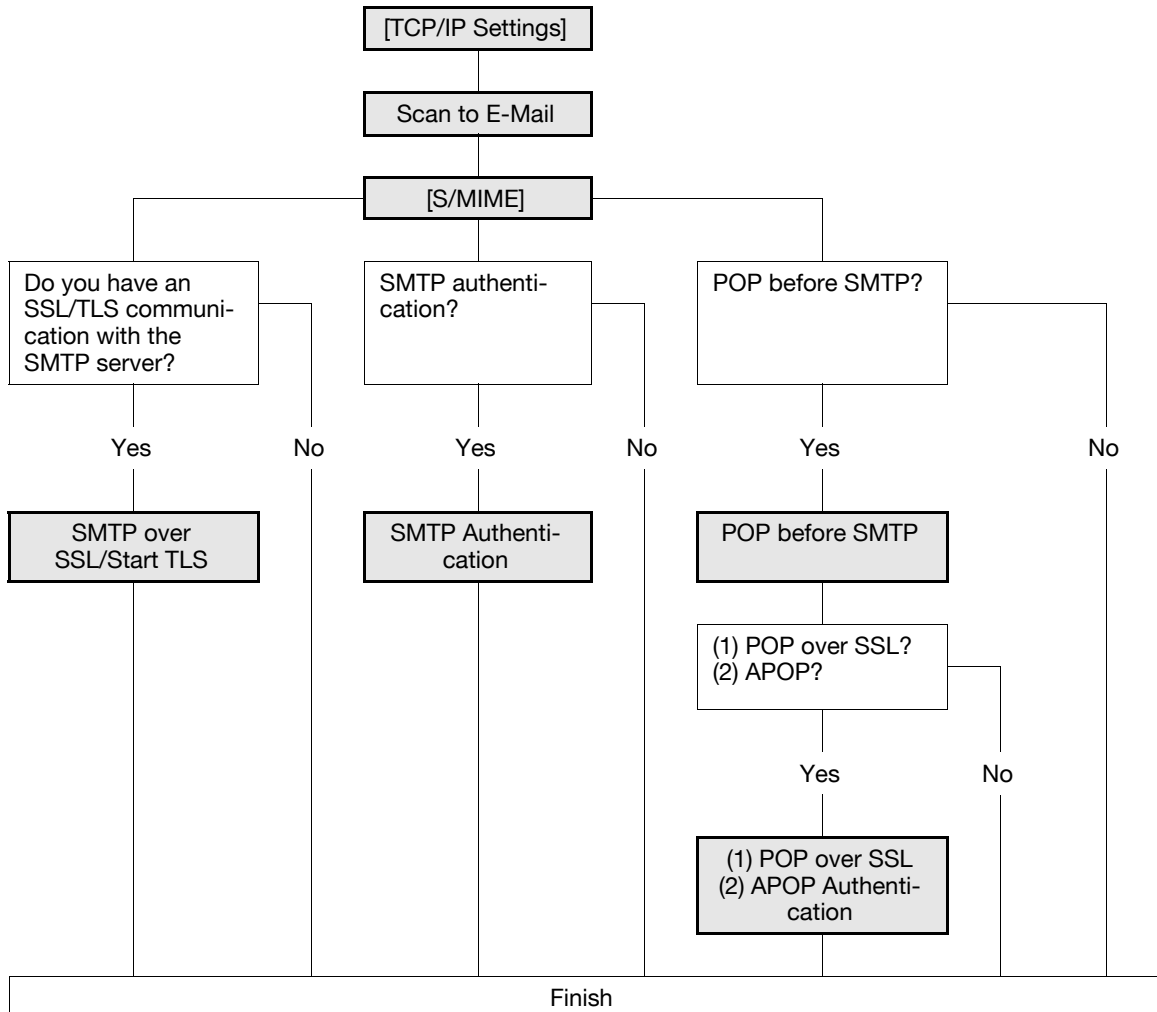
📖 **Reference**
You cannot select an address with no certificate registered. To send an encrypted E-mail, pre-register the user certificate in this machine. For details, refer to page 8-13.

4.6.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.6.2   Scan to E-Mail

Configure settings to send an E-mail.

For details, refer to page 4-9.

4.6.3   [S/MIME]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [S/MIME].

Item	Description	Prior check
[S/MIME Comm. Setting]	Select [ON].	
[E-Mail Text Encrypt. Method]	Specify the E-mail text encryption format.	

4.6.4   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

4.6.5   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

4.6.6   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

4.6.7   POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

4.6.8   APOP Authentication

Configure APOP authentication settings.

For details, refer to page 4-16.

4.7 Sending scanned data to the FTP server

Configure settings to send scanned data to the FTP server.

You can send scanned data to the specified folder in the FTP server via the network, which contains the FTP server. This allows you to download the data sent to the FTP server from a computer via the network. This function is suitable to send a large amount of data such as high-resolution data.

If a proxy server is in network environment, you can configure settings to access the FTP server on Internet via the proxy server.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
┌─────────────────────────────┐
│      [TCP/IP Settings]      │
└─────────────────────────────┘
              │
┌─────────────────────────────┐
│      [FTP TX Setting]       │
└─────────────────────────────┘
              │
┌─────────────────────────────┐
│           Finish            │
└─────────────────────────────┘
```
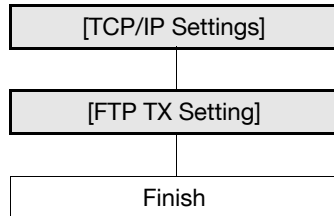
📖 **Reference**

For details on how to register the FTP address, refer to page 11-7.

For details on FTP file sending, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.7.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.7.2 [FTP TX Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [FTP Setting] ►► [FTP TX Setting].

Item	Description	Prior check
[FTP TX]	Select [ON].	
[Proxy Server Address]	To perform transmissions via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[Connection Timeout]	Enter the timeout period for a communication with a server.	
[Port Number]	Enter a port number. Default setting: 21	Server port number

4.8   Sending scanned data to the WebDAV server

Configure settings to send scanned data to the WebDAV server.

You can send scanned data to the specified folder in the WebDAV server via the network, which contains the WebDAV server. This allows you to download the data sent to the WebDAV server from a computer via the network.

WebDAV, which is an extension to the HTTP specification, provides the same security technologies as HTTP. Use SSL to encrypt a communication with the WebDAV server; you can send a file more securely.

If a proxy server is in network environment, you can configure settings to access the WebDAV server on Internet via the proxy server.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
              ┌─────────────────────┐
              │   [TCP/IP Settings]  │
              └──────────┬──────────┘
                         │
              ┌─────────────────────────┐
              │ [WebDAV Client Settings] │
              └──────────┬──────────────┘
                         │
              ┌───────────────────────────┐
              │ Do you have an SSL com-    ├──────────┐
              │ munication with the Web-   │          │
              │ DAV server?                │          │
              └──────────┬────────────────┘          │
                    Yes  │                      No    │
              ┌───────────────────────────┐          │
              │      WebDAV over SSL       │          │
              └──────────┬────────────────┘          │
              ┌───────────────────────────────────────┤
              │                Finish                  │
              └───────────────────────────────────────┘
```
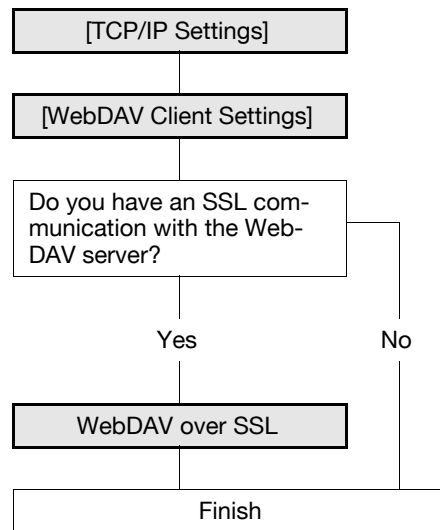
📖 **Reference**
For details on how to register the WebDAV address, refer to page 11-7.

When registering the address, specify whether to send a file encrypted with SSL. For details, refer to page 11-7.

For details on WebDAV file sending, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.8.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.8.2 [WebDAV Client Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [WebDAV Settings] ►► [WebDAV Client Settings].

Item	Description	Prior check
[WebDAV TX Setting]	Select [ON].	
[Proxy Server Address]	To perform transmissions via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Chunk Transmission]	Select whether to enable chunk TX (batch transmission) or non-chunk TX (split transmission) when sending data to the WebDAV server. By default, it is set to [Non-Chunk Transmission]. Change the setting to fit the target WebDAV server.	Method supported by the server
[Connection Timeout]	Enter the timeout period for a communication with a server.	
[Server Authentication Character Code]	Select a character code to perform the authentication under the WebDAV server. You can use this setting when [Japanese] is specified for the language to be displayed on the **Control Panel**.	

4.8.3   WebDAV over SSL

[Certificate Verification Level Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [WebDAV Settings] ►► [Web-DAV Client Settings].

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	
[CN]	Select whether to check that the CN of the server certificate matches the server address.	
[Key Usage]	Select whether to check that the server certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the server certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	

Item	Description	Prior check
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

4.9   Importing images by TWAIN scan

Configure settings to use this machine as a scanner.

Using the TWAIN driver enables you to use this machine as a scanner. This function controls this machine from a computer via the network, and imports scanned data to application on network.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
        ┌──────────────────────┐
        │   [TCP/IP Settings]  │
        └──────────────────────┘
                   │
        ┌──────────────────────┐
        │    [SLP Setting]     │
        └──────────────────────┘
                   │
        ┌──────────────────────┐
        │ [TCP Socket Setting] │
        └──────────────────────┘
                   │
        ┌──────────────────────┐
        │   [Network TWAIN]    │
        └──────────────────────┘
                   │
        ┌──────────────────────┐
        │        Finish        │
        └──────────────────────┘
```
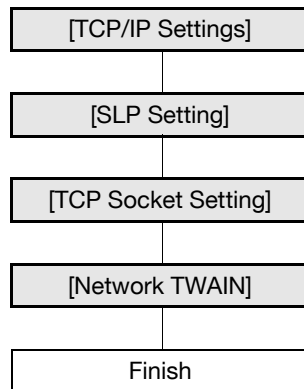
📖 **Reference**

For details on how to install the TWAIN driver, refer to the TWAIN driver manual in the Driver CD-ROM.

4.9.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.9.2   [SLP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [TCP/IP Setting].

Item	Description	Prior check
[SLP]	Select [Enable] to search for this machine using TWAIN.	

4.9.3 [TCP Socket Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [TCP Socket Setting].

Item	Description	Prior check
[TCP Socket]	Select this check box to use the TWAIN driver.	
[Port Number]	Enter a port number.	

4.9.4 [Network TWAIN]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [Network TWAIN].

Item	Description	Prior check
[TWAIN Lock Time]	Enter the time to automatically release the operation lock using the TWAIN scan function.	

4.10   Using the WS scan function

Configure the following settings when you scan data using the Web services function of Windows Vista/Server 2008/7.

The Web services function can automatically detect this network-connected machine and install it as a WS scanner. When you select this machine (installed as the WS scanner), you can use the HTTP for communication and scan data.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
      [TCP/IP Settings]
             |
 [Web Service Common Set-
          tings]
             |
     [Scanner Settings]
             |
          Finish
```
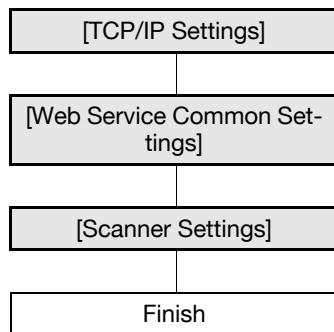
📖 **Reference**
For details on the WS scan functions, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

4.10.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

4.10.2   [Web Service Common Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [Web Service Settings] ▸▸ [Web Service Common Settings].

Item	Description	Prior check
[Friendly Name]	Enter a Friendly Name (up to 62 characters).	
[Publication Serv-ice]	If you use this machine in an environment where NetBIOS is disabled or only the IPv6 protocol communication is used by the Windows Vista/Server 2008/7 system, set this item to [Enable]. The Publication Service function can detect up to 512 destinations, including those detected with the NetBIOS service.	

4.10.3   [Scanner Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [Web Service Settings] ▸▸ [Scanner Settings].
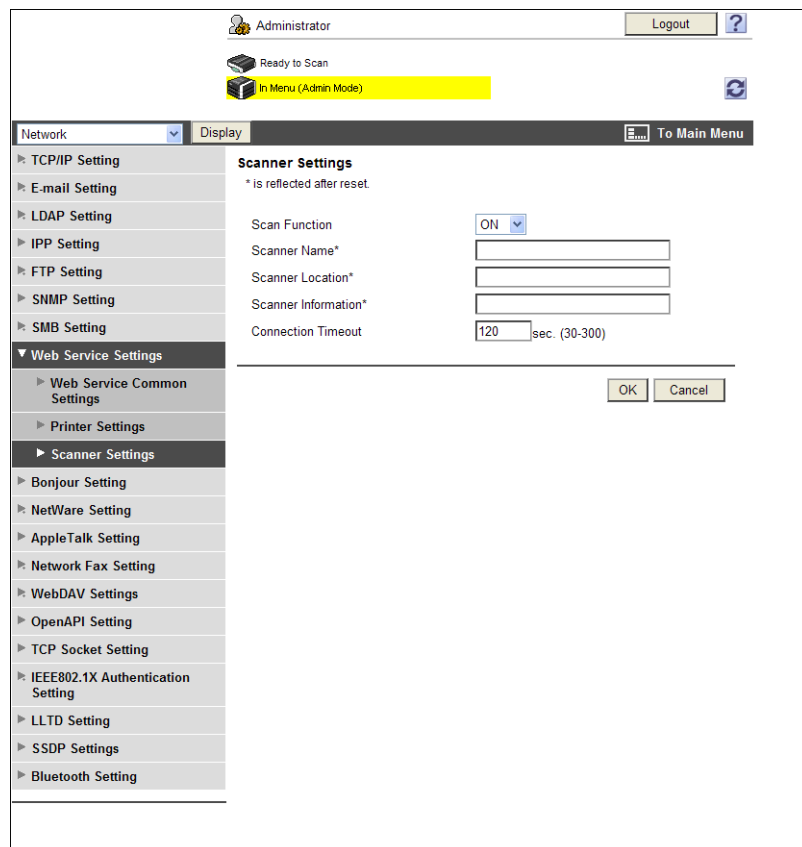
Item	Description	Prior check
[Scan Function]	Select [ON].	
[Scanner Name]	Enter a scanner name (up to 63 characters).	
[Scanner Location]	Enter a scanner location (up to 63 characters).	
[Scanner Informa-tion]	Enter scanner information (up to 63 characters).	
[Connection Time-out]	Enter a connection timeout.	

5 Printing

5 Printing

5.1 Printing (LPR/Port9100)

Configure settings for LPR or Port9100 printing.

LPR printing is performed via the network using the LPR protocol. It is mainly used in UNIX-based operating systems.

Port9100 printing is performed via the network by directly specifying the RAW port (Port9100) of this machine connected to the TCP/IP network as a destination printer.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
              ┌────────────────────────┐
              │    [TCP/IP Settings]    │
              └────────────────────────┘
              ┌────────────────────────┐
              │ (1) LPR printing        │
              │ (2) Port9100 printing   │
              └────────────────────────┘
       (1)                                    (2)
┌────────────────────┐             ┌────────────────────┐
│   [LPD Setting]    │             │  [RAW Port Number] │
└────────────────────┘             └────────────────────┘
┌──────────────────────────────────────────────────────┐
│                        Finish                          │
└──────────────────────────────────────────────────────┘
```
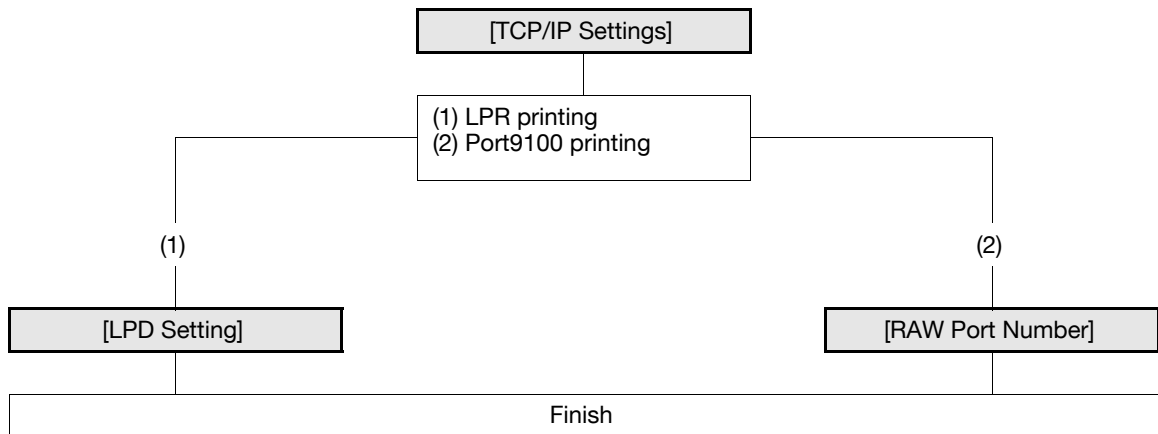
📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide [Print Operations]].

5.1.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

5.1.2 [LPD Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [TCP/IP Setting].

Item	Description	Prior check
[LPD]	Select [Enable].	

5.1.3   [RAW Port Number]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [TCP/IP Setting] ►► [TCP/IP Setting].

Item	Description	Prior check
[RAW Port Number]	Select the check box of the required port, and enter the RAW port number.	

Reference

● If you select [OK] after changing multiple port numbers together in **PageScope Web Connection** or on the **Control Panel**, a port number duplication error may be displayed. When this error is displayed, first change one port number and select [OK]. Then change another one and select [OK].

5.2   Print (SMB)

Configure settings for SMB printing.

A printer can be shared on the Windows network using the SMB protocol. The SMB printing allows a computer to directly specify this machine running on the Windows network to print information.

To use SMB printing in the IPv6 environment, you must enable the direct hosting service.

To perform the SMB printing from a computer with Windows Vista/Server 2008/7 installed, you can perform the name resolution using the LLMNR function even if DNS server is not present. To perform the name resolution especially in the IPv6-only communication environment under Windows Vista/Server 2008/7, it will be convenient to enable the LLMNR function.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                        [TCP/IP Settings]

                        [Print Setting]

                        IPv6 environment?
        No                                              Yes

  Do you use the WINS server?                    [Direct Hosting Setting]

        Yes                      No

   [WINS Setting]        Do you send data to
                         Windows Vista/Server
                         2008/7?

                    No              Yes

                            [LLMNR Setting]

                            Finish
```
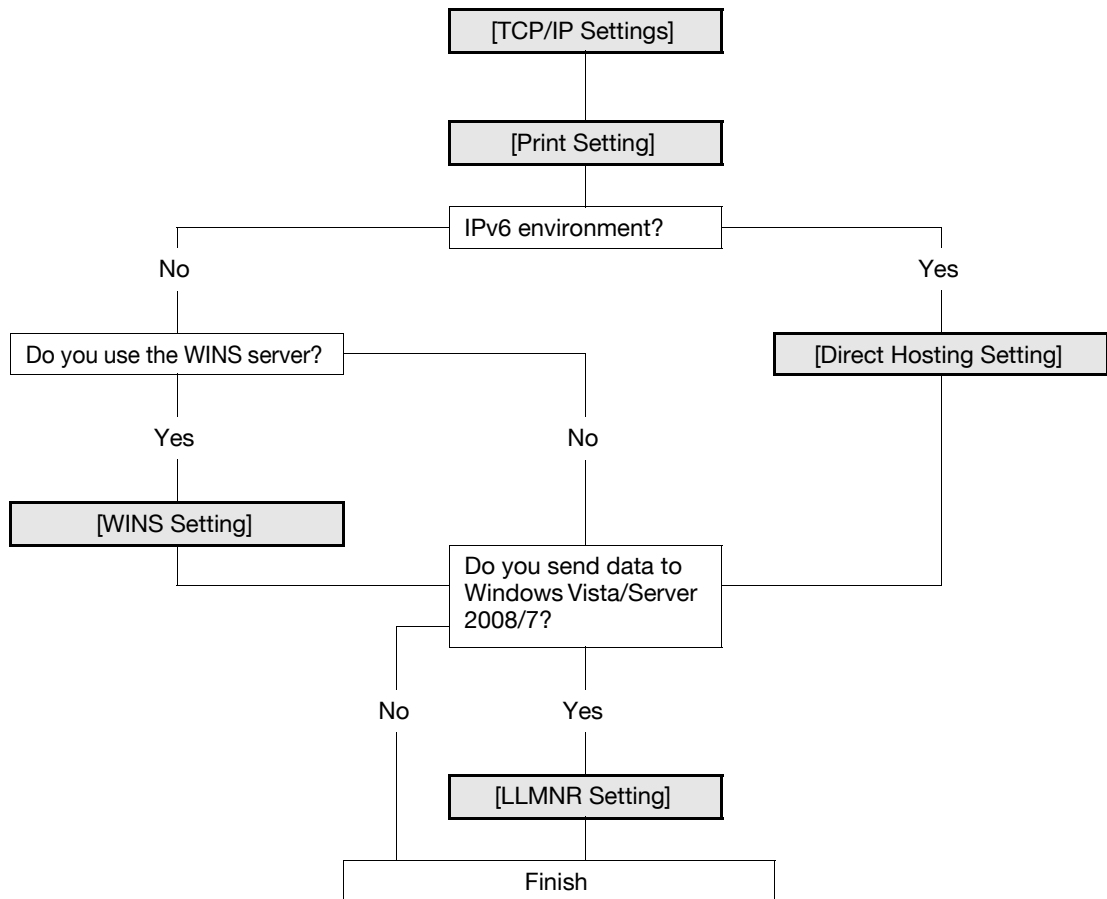
📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide [Print Operations]].

5.2.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

5.2.2   [Print Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [SMB Setting] ►► [Print Setting].
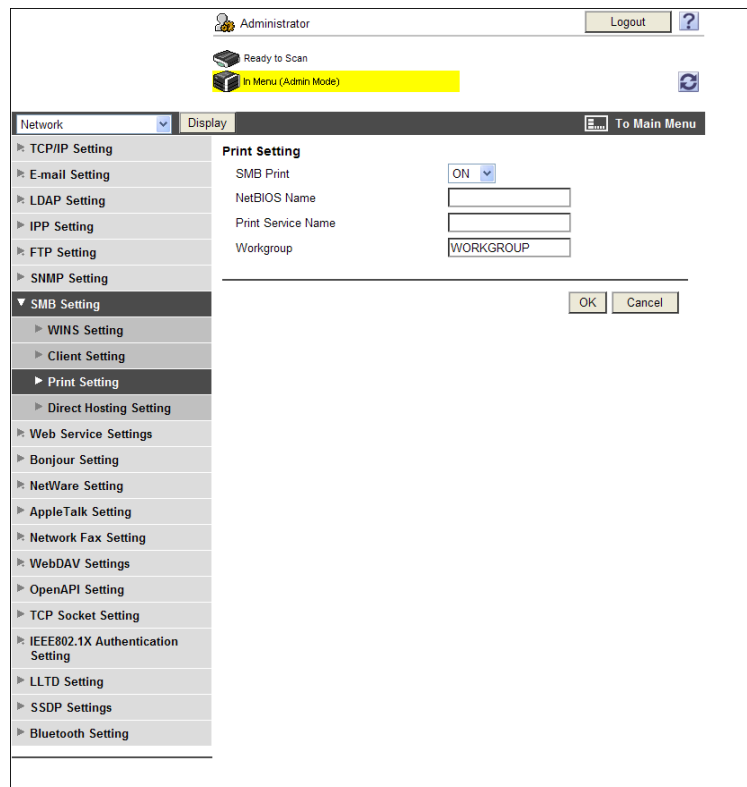
Item	Description	Prior check
[Print Setting]	Select [ON].	
[NetBIOS Name]	Enter the NetBIOS name in uppercase letters (up to 15 characters, the only symbol allowed is a hyphen (-)).	
[Print Service Name]	Enter a print service name in uppercase letters (up to 12 characters, excluding / and \).	
[Workgroup]	Enter a workgroup name in uppercase letters (up to 15 characters, excluding " \ :; , * < > | + = ?).	The workgroup this machine belongs to

5.2.3   [WINS Setting]

When you start SMB printing via the router, you must set up the WINS server.

For details, refer to page 4-4.

5.2.4   [Direct Hosting Setting]

To use SMB printing in the IPv6 environment, enable the direct hosting service.

For details, refer to page 4-5.

5.2.5   [LLMNR Setting]

To perform name resolution in the environment configured to communicate with Windows Vista/Server 2008/7, and where the DNS server is not running, enable the LLMNR function.

For details, refer to page 4-5.

5.3   Print (IPP)

Configure settings for IPP printing.

IPP printing uses the Internet Printing Protocol (IPP) and prints information via the network. Because the IPP printing allows the print data to be transferred to a network printer using HTTP protocol, you can also output the data to a remote printer via the Internet.

If you have set the authentication for IPP printing, you can prevent illegal access by a third party.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
            ┌────────────────────────┐
            │    [TCP/IP Settings]    │
            └────────────────────────┘
                         │
            ┌────────────────────────┐
            │     [IPP Setting]       │
            └────────────────────────┘
                         │
            ┌────────────────────────┐
            │  Do you authorize?      │──────────┐
            └────────────────────────┘          │
                         │                       │
                        Yes                      No
                         │                       │
            ┌────────────────────────┐          │
            │  [IPP Authentication Set-│          │
            │        tings]           │          │
            └────────────────────────┘          │
                         │                       │
            ┌────────────────────────────────────┘
            │        Finish          │
            └────────────────────────┘
```
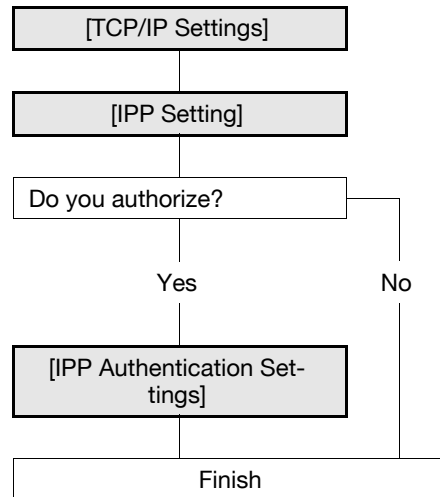
📖 Reference
For details on how to install the printer driver, refer to the [User's Guide [Print Operations]].

5.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

5.3.2 [IPP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [IPP Setting].

Item	Description	Prior check
[IPP Setting]	Select [ON].	
[Accept IPP job]	Select [ON].	
[Printer Name]	Enter a printer name (up to 127 characters).	
[Printer Location]	Enter a printer location (up to 127 characters).	
[Printer Information]	Enter printer information (up to 127 characters).	
[Print URI]	Displays the URI of the printer that can print data using the IPP.	
[Support Information]	Select the check box of each job to be executed using the IPP.	
[Print Job]	Select whether to allow a print job. Select this check box to enable IPP printing.	
[Valid Job]	Select whether to allow confirmation of a valid job.	
[Cancel Job]	Select whether to allow canceling the job.	
[Open Job Attributes]	Select whether to obtain job attributes.	
[Open Job]	Select whether to obtain a list of job attributes.	
[Open Printer Attributes]	Select whether to obtain printer attributes.	

5.3.3   [IPP Authentication Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [IPP Setting].

Item	Description	Prior check
[IPP Authentication Setting]	Select this check box to force an authentication for IPP printing.	
[Authentication Method]	Select an authentication method.	
[User Name]	Enter a user name (up to 20 characters, excluding a colon (:)). This entry is required if you have selected [basic] or [digest] for the [Authentication Method].	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password (up to 20 characters). This entry is required if you have selected [basic] or [digest] for the [Authentication Method].	
[realm]	Enter realm (up to 127 characters). This entry is required if you have selected [digest] for the [Authentication Method].	

5.4   Print (IPPS)

Configure settings for IPPS printing.

When this machine starts IPP printing, the communication between the computer and this machine is encrypted using the SSL. The encryption using the SSL can enhance the security during IPP printing.

To use IPPS printing on the Windows Vista/Server 2008/7 system, check the following points.
- Enter "https://host-name.domain-name/ipp". These host-name and domain-name must be the [DNS Host Name] and [Default DNS Domain Name] that you have set for the [TCP/IP Settings].
- Your computer must be able to resolve the name of this machine using the DNS. Register this machine in the DNS server and configure the DNS settings in your computer in advance.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the device certificate in [Trusted Root Certification Authorities] of the local computer.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
              ┌─────────────────────────┐
              │     [TCP/IP Settings]    │
              └─────────────────────────┘
                           │
              ┌─────────────────────────┐
              │       [IPP Setting]      │
              └─────────────────────────┘
                           │
              ┌─────────────────────────┐
              │ [Device Certificate Setting] │
              └─────────────────────────┘
                           │
              ┌─────────────────────────┐
              │      Do you authorize?   │────────────┐
              └─────────────────────────┘            │
                           │                          │
                          Yes                        No
                           │                          │
              ┌─────────────────────────┐            │
              │ [IPP Authentication Setting] │        │
              └─────────────────────────┘            │
                           │                          │
              ┌─────────────────────────────────────┐
              │               Finish                 │
              └─────────────────────────────────────┘
```

📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide [Print Operations]].

5.4.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.
- To use IPPS printing in Windows Vista/Server 2008/7, correctly set the [DNS Host Name] and [Default DNS Domain Name] in [TCP/IP Settings] before creating its certificate. If their settings are incorrect, you cannot connect to this machine using IPPS.

For details, refer to page 2-2.

5.4.2   [IPP Setting]

Configure settings for IPP printing.

For details, refer to page 5-7.

5.4.3   [Device Certificate Setting]

Configure settings for SSL communication.

For details, refer to page 8-2.

5.4.4   [IPP Authentication Setting]

Configure these settings to force an authentication for IPP printing.

For details, refer to page 5-8.

5.5   Printing (Bonjour)

Configure these settings when you connect this machine to a Macintosh computer using the Bonjour protocol for printing.

Before starting Bonjour protocol communication between this machine and a Macintosh computer, configure the Bonjour protocol for this machine.

📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide Print Operations].

[Bonjour Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [Bonjour Setting].
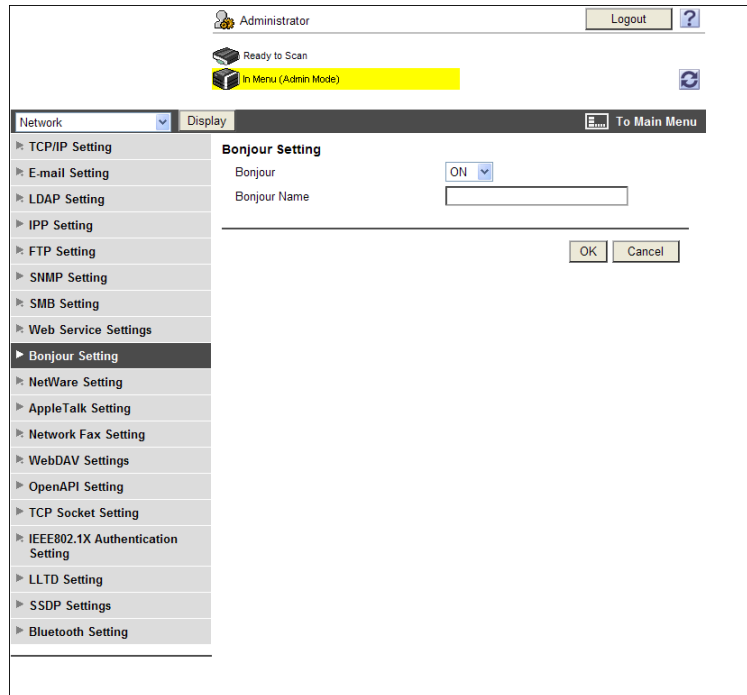
Item	Description	Prior check
[Bonjour]	Select [ON].	
[Bonjour Name]	Enter a Bonjour name that is displayed as the name of connected device (up to 63 characters).	

5.6   Printing (AppleTalk)

Configure these settings when you connect this machine to a Macintosh computer using the AppleTalk protocol for printing.

Before starting AppleTalk protocol communication between this machine and a Macintosh computer, set the AppleTalk protocol for this machine.

Reference

- AppleTalk connection supports Mac OS X 10.2/10.3/10.4/10.5 only.

📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide Print Operations].

[AppleTalk Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [AppleTalk Setting].

Item	Description	Prior check
[AppleTalk]	Select [ON].	
[Printer Name]	Enter a printer name to be displayed on the selector (up to 31 characters, excluding = and ~).	
[Zone Name]	Enter a name of zone this machine belongs to (up to 31 characters).	
[Current Zone]	The current zone name is displayed.	

5.7   Printing (Netware)

Configure settings for printing in a NetWare environment.

Before you start printing in a NetWare environment, you must set the NetWare file system on this machine.

📖 **Reference**

For details on how to install the printer driver, refer to the [User's Guide Print Operations].

5.7.1   [NetWare Settings]

In the administrator mode of **PageScope Web Connection**, select [Network]▸▸[NetWare Settings]▸▸[NetWare Settings].

The required items depend on your operating environment. Set the items by referring to the following figure.

In Remote Printer mode using the NetWare 4.x Bindery Emulation

✔ When you use the Bindery Emulation, make sure that the Bindery Emulation has been enabled on the NetWare server.

1 From the client, log in the NetWare file system as Bindery with the administrator authority.

2 Start Pconsole.

3 Select [Quick Setup] from [Available Options] list box, and press the Enter key.

4 Fill in [Print Server Name], [Printer Name], and [Print Queue Name]. Set the [Type] of the printer to [Other/Unknown], and save them.

5 Terminate Pconsole by pressing the Esc key.

6 Load the PSERVER.NLM file on the NetWare Server console.

Then, configure the following settings in [NetWare Setting].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type
[NetWare Print Mode]	Select [Nprinter/Rprinter].	
[Print Server Name]	Enter a print server name to be operated as the Nprinter/Rprinter (up to 63 characters, excluding / \ :; , * [ ] < > | + = ? .).	The print server name specified in Step 4
[Printer Number]	Enter the Nprinter/Rprinter number.	

In Print Server mode using the NetWare 4.x Bindery Emulation

✔ When you use the Bindery Emulation, make sure that the Bindery Emulation has been enabled on the NetWare server.

✔ When you select the Print Server mode, the IPX protocol must already be loaded on the NetWare server.

1 From the client, log in the NetWare file system as Bindery with the administrator authority.

2 Start Pconsole.

3 Select [Quick Setup] from [Available Options] list box, and press the Enter key.

4 Fill in [Print Server Name], [Printer Name], and [Print Queue Name]. Set the [Type] of the printer to [Other/Unknown], and save them.

5 Terminate Pconsole by pressing the Esc key.

Then, configure the following settings in [NetWare Setting].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type
[NetWare Print Mode]	Select [PServer].	
[Print Server Name]	Enter a print server name to be operated as Pserver (up to 63 characters, excluding / \ :; , * [ ] < > | + = ? .).	The print server name specified in Step 4
[Print Server Password]	Enter a print server password if necessary (up to 63 characters).	
[Polling Interval]	Set a job inquiry interval.	
[Bindery/NDS Setting]	Select [NDS/Bindery Setting].	
[File Server Name]	Enter the priority file server name to be used in the Bindery emulation mode (up to 47 characters, excluding ∧ :; , * [ ] < > | + = ? .).	

In NetWare 4.x Remote Printer mode (NDS)

1 From the client, log in the NetWare file system with administrator authority.

2 Start NWAdmin.

3 Select an organization or department container for the print service, and select [Print Services Quick Setup] from the Tools menu.

4 Fill in [Print Server Name], [Printer Name], [Print Queue Name], and [Print Queue Volume]. Then, set the [Type] of the printer to [Other/Unknown] and save them.

5 Load the PSERVER.NLM file on the NetWare Server console.

Then, configure the following settings in [NetWare Setting].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type
[NetWare Print Mode]	Select [Nprinter/Rprinter].	
[Print Server Name]	Enter a print server name to be operated as the Nprinter/Rprinter (up to 63 characters, excluding / \ :; , * [ ] < > | + = ? .).	The print server name specified in Step 4
[Printer Number]	Enter the Nprinter/Rprinter number.	

In the NetWare 4.x/5.x/6 Print Server mode (NDS)

✔ When you select the Print Server mode, the IPX protocol must already be loaded on the NetWare server.

1 From the client, log in the NetWare file system with administrator authority.

2 Start NWAdmin.

3 Select an organization or department container for the print service, and select [Print Services Quick Setup (non-NDPS)] from the Tools menu.

4 Fill in [Print Server Name], [Printer Name], [Print Queue Name], and [Print Queue Volume]. Then, set the [Type] of the printer to [Other/Unknown] and click [Create].

Then, configure the following settings in [NetWare Setting].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type
[NetWare Print Mode]	Select [PServer].	
[Print Server Name]	Enter a print server name to be operated as Pserver (up to 63 characters, excluding / \ :; , * [ ] < > | + = ? .).	The print server name specified in Step 4
[Print Server Password]	Enter a print server password if necessary (up to 63 characters).	
[Polling Interval]	Set a job inquiry interval.	
[Bindery/NDS Setting]	Select [NDS].	
[NDS Context Name]	Enter an NDS context name for print server connection (up to 191 characters, excluding / \ :; , * [ ] < > | + = ?).	
[NDS Tree Name]	Enter an NDS tree name for print server connection (up to 63 characters, excluding / \ :; , * [ ] < > | + = ? .).	
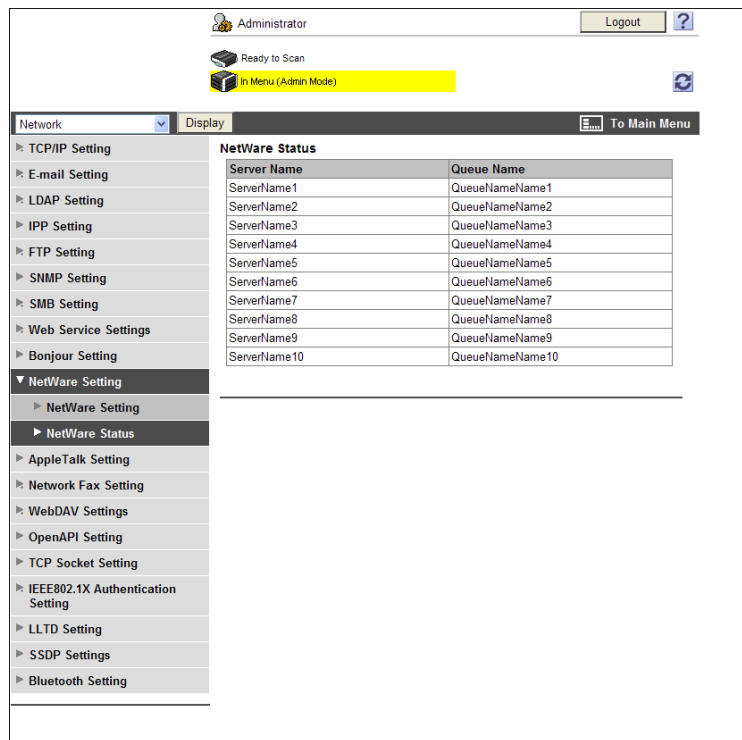
For NetWare 5.x/6 Novell Distributed Print Service (NDPS)

✔   Before starting the NDPS setting, make sure that an NDPS broker and NDPS manager have already been created and loaded.

✔   Make sure that the TCP/IP protocol has been set on the NetWare server, an IP address of this machine has been set, and this machine has already been started.

1   From the client, log in the NetWare file system with administrator authority.

2   Start NWAdmin.

3   Right-click the [Organization] and [Organization unit] containers for printer agent creation, and select [NDPS Printer] from Create.

4   Enter a [NDPS Printer Name] in the [Printer Name] field.

5   Select [Create a New Printer Agent] in the [Printer Agent Source] field, and click [Create].

6   Confirm the printer agent name, and browse and register the NDPS manager in the [NDPS Manager Name] field.

7   Set the [Gateway Types] to [Novell Printer Gateway], and register it.

8   In the [Configure Novell NDPS for Printer Agent] window, set the Printer to [(None)] and the port hander to [Novell Port Handler], and register the settings.

9   Set the [Connection type] to [Remote (LPR on IP)] and register the setting.

10   For the host address, enter the IP address of this machine you have configured. Enter [Print] for the printer name, and then press [Finish] to register the settings.

11   When printer driver registration windows appear, select [None] for each OS and finish the registration.

5.7.2 [NetWare Status]

In the administrator mode of **PageScope Web Connection**, select [Network]▶▶[NetWare Settings]▶▶[NetWare Status].

The current NetWare connection can be checked if necessary.

5.8 Using the WS print function

Configure the following settings when you print data using the Web services function of Windows Vista/Server 2008/7.

The Web services function can automatically detect this network-connected machine and install it as a WS printer. When you select this machine (installed as the WS printer), you can use the HTTP for communication and print data.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
      ┌─────────────────────────────┐
      │      [TCP/IP Settings]        │
      └─────────────────────────────┘
                    │
      ┌─────────────────────────────┐
      │  [Web Service Common Set-    │
      │          tings]              │
      └─────────────────────────────┘
                    │
      ┌─────────────────────────────┐
      │      [Printer Settings]       │
      └─────────────────────────────┘
                    │
      ┌─────────────────────────────┐
      │           Finish             │
      └─────────────────────────────┘
```
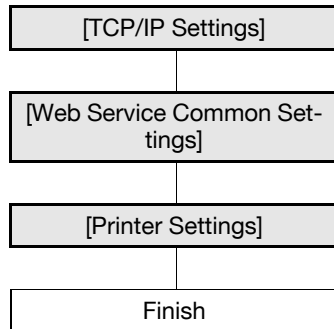
📖 **Reference**
For details on how to install the printer driver, refer to the [User's Guide [Print Operations]].

5.8.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

5.8.2 [Web Service Common Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Web Service Settings] ►► [Web Service Common Settings].

Item	Description	Prior check
[Friendly Name]	Enter a Friendly Name (up to 62 characters).	
[Publication Service]	If you use this machine in an environment where NetBIOS is disabled or only the IPv6 protocol communication is used by the Windows Vista/Server 2008/7 system, set this item to [Enable].	

5.8.3   [Printer Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Web Service Settings] ►► [Printer Settings].

Item	Description	Prior check
[Print Function]	Select [ON].	
[Printer Name]	Enter a printer name (up to 63 characters, excluding ! \ and ,).	
[Printer Location]	Enter a printer location (up to 63 characters).	
[Printer Information]	Enter printer information (up to 63 characters).	

5.9 Using Data Saved in a Cellular Phone or PDA

Configure settings to wirelessly connect this machine to a cellular phone or PDA with the Bluetooth function installed and to use data stored in such a terminal.

You can print data saved in a cellular phone or PDA or save data in a User Box of this machine. Once data is saved in a User Box, it can be sent to an external device if necessary.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference
● To use this function, install the optional **Local Interface Kit EK-605** in this machine.
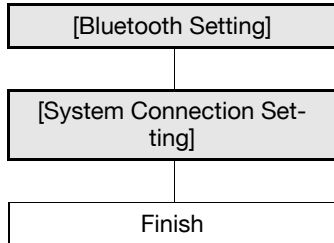
📖 **Reference**
For details on printing data saved in a cellular phone or PDA or saving data in a User Box of this machine, refer to the [User's Guide Print Operations]. For details on using the saved data in User Boxes of this machine, refer to the [User's Guide Box Operations].

5.9.1 [Bluetooth Setting]

In the administrator mode of **PageScope Web Connection**, select [Network]▶▶[Bluetooth Setting].
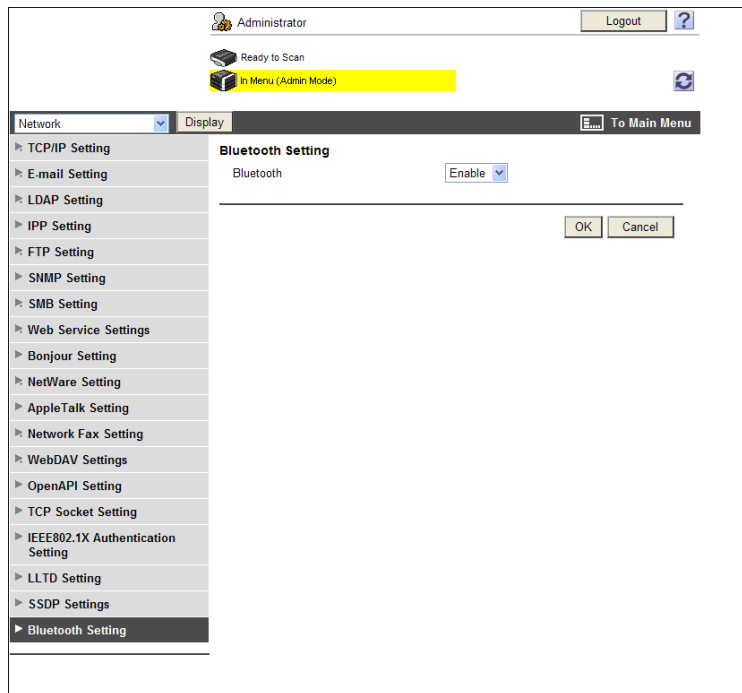
Item	Description	Prior check
[Bluetooth]	Select [Enable].	

5.9.2 [System Connection Setting]

In the administrator mode of **PageScope Web Connection**, select[System Settings]▶▶[System Connection Setting].
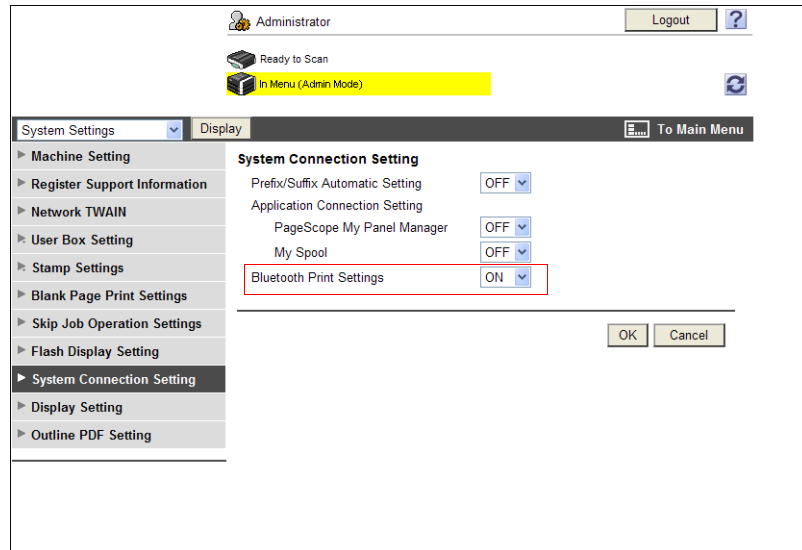
Item	Description	Prior check
[Bluetooth Print Settings]	Select [ON]. This item is not displayed when [Bluetooth] is set to [Disable].	

6 Sending and receiving network faxes

6   Sending and receiving network faxes

Reference
- This function is available only when a **Hard Disk** is installed.

6.1   Sending Internet faxes

Configure settings to send Internet fax.

Internet faxing sends and receives the read original as an E-mail attachment file (TIFF format) via Intranet or Internet. It also allows you to send a colored original.

The Internet fax function establishes a communication via Intranet or Internet; therefore, you can reduce the communication cost compared with a general Fax communication when frequently handling remote or over-seas communications.

If necessary, you can combine POP before SMTP authentication, APOP authentication, SMTP authentication, and SSL/TLS encryption to have a communication.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                          ┌─────────────────────┐
                          │  [TCP/IP Settings]  │
                          └─────────────────────┘
                                    │
                          ┌─────────────────────┐
                          │   [Network Fax      │
                          │  Function Settings] │
                          └─────────────────────┘
                                    │
                          ┌─────────────────────┐
                          │  [Machine Setting]  │
                          └─────────────────────┘
                                    │
                          ┌─────────────────────┐
                          │  [Header Informa-   │
                          │       tion]         │
                          └─────────────────────┘
                                    │
                          ┌─────────────────────┐
                          │  Scan to E-Mail     │
                          └─────────────────────┘
                                    │
                          ┌─────────────────────┐
                          │  [Network Fax Set-  │
                          │       ting]         │
                          └─────────────────────┘
```

Do you have an SSL/TLS communication with the SMTP server?	Do you use SMTP authentication?	POP before SMTP?
Yes No	Yes No	Yes No
SMTP over SSL/Start TLS	SMTP Authentication	POP before SMTP

(1) POP over SSL?
(2) APOP?

No   Yes

(1) POP over SSL
(2) APOP Authentication

Finish
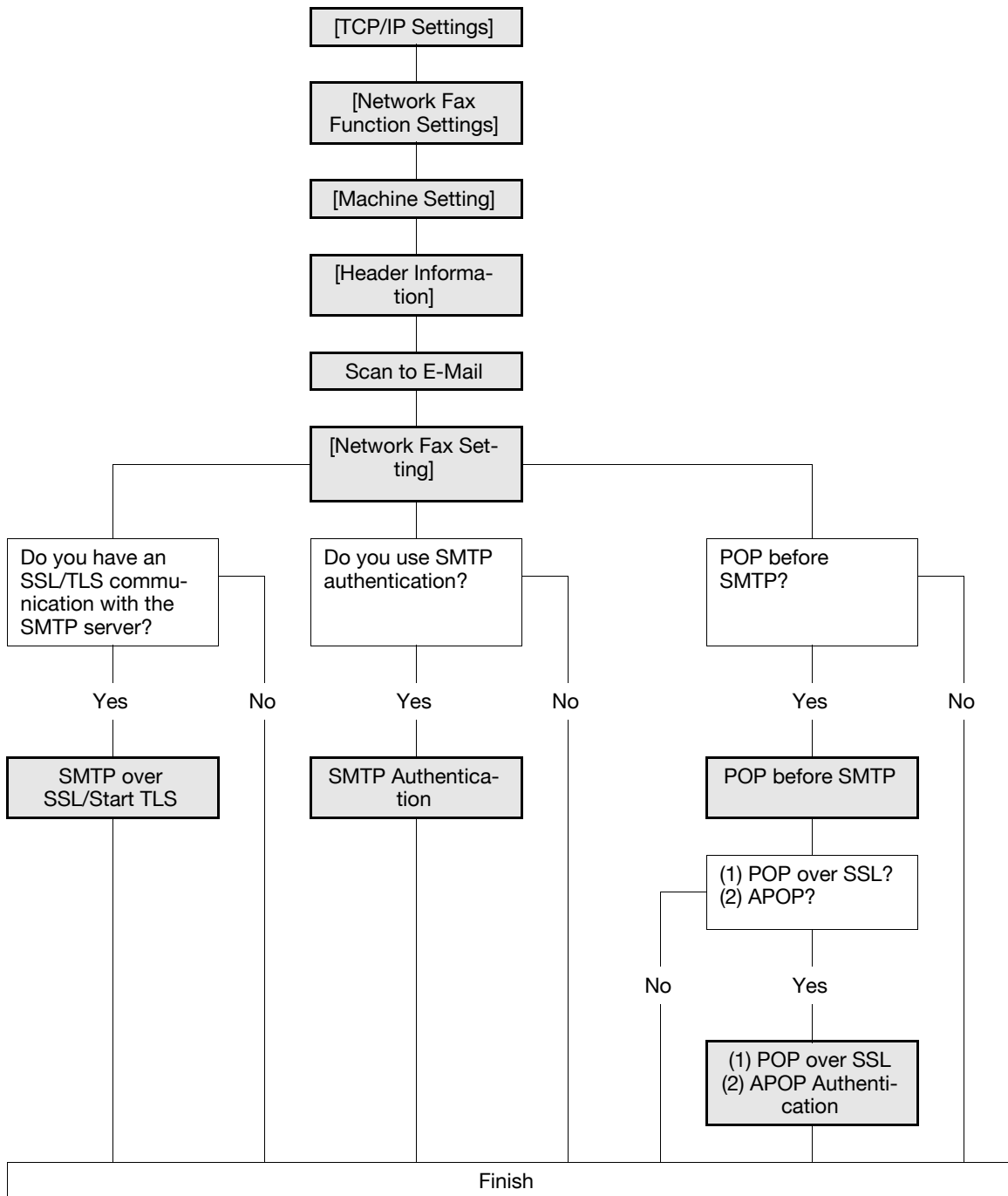
Reference
- To use the Internet fax function, ask your service representative to configure settings. For details, contact your service representative.
- For details on how to register Internet fax destinations, refer to page 11-7.
- For details on the Internet fax function, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

6.1.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

6.1.2 [Network Fax Function Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Network Fax Setting] ►► [Network Fax Function Settings].
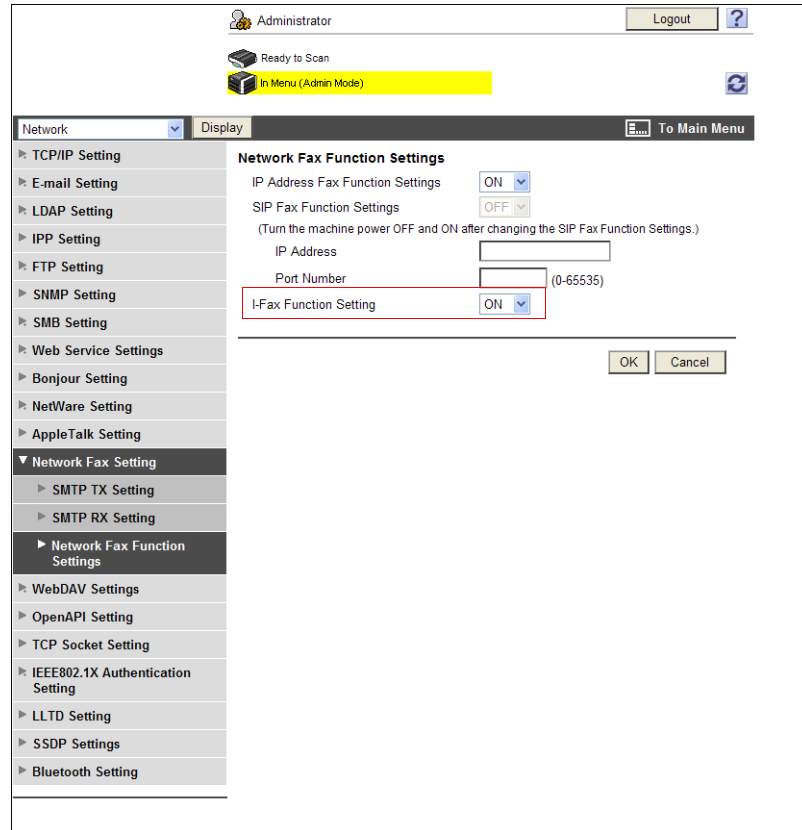
Item	Description	Prior check
[I-Fax Function Setting]	Select [ON].	

6.1.3   [Machine Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▸▸ [Machine Setting].

Item	Description	Prior check
[Device Name]	Enter the device name (up to 80 characters). This name is used as a part of an Internet fax subject name.	
[E-mail Address]	Enter the E-mail address of this machine (up to 320 characters). This setting is required when sending Internet faxes.	E-mail Address

6.1.4   [Header Information]

Register sender information for fax sending.

For details, refer to page 14-20.

6.1.5   Scan to E-Mail

Configure settings to send an E-mail.

For details, refer to page 4-9.

6.1.6   [Network Fax Setting]

(This menu item will not be displayed if the Network Fax function is not available.)

[I-Fax Advanced Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▶▶ [Network Fax Setting] ▶▶ [I-Fax Advanced Setting].

(This menu item will not be displayed if the Internet Fax function is not available.)

Item	Description	Prior check
[MDN Request]	Select [ON]. You can receive an MDN response when an Internet fax is printed in the receiver side. By receiving an MDN response, you can obtain information on the reception capability of the remote machine. When an MDN response is received from a remote machine that is already registered in the address book, the information on the reception capability that has been obtained will be overwritten.	
[DSN Request]	Select [ON]. You can receive a DSN response when an Internet fax arrives in the mail server of the receiver side. The DSN request is not issued when MDN is set to [ON].	
[MDN/DSN Response Monitoring Setting]	Select this check box to specify the MDN/DSN response monitoring time.	
[Monitoring Time]	Enter the MDN/DSN response receiving wait time. An MDN/DSN response is ignored if it does not reach within this wait time.	
[Maximum Resolution]	Select the highest resolution of read or transfer logs.	
[Add Content-Type Information]	Select whether to add Content-Type information to the MIME header.	

[Black Compression Level]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▸▸ [Network Fax Setting] ▸▸ [Black Compression Level].

Item	Description	Prior check
[Black Compression Level]	Select the default setting of the black compression level in the black and white sending mode.	

[Color/Grayscale Multi-Value Compression Method]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▸▸ [Network Fax Setting] ▸▸ [Color/Grayscale Multi-Value Compression Method].

Item	Description	Prior check
[Color/Grayscale Multi-Value Compression Method]	Select the default setting of the color/grayscale multi-value compression method in the color sending mode.	

6.1.7   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

6.1.8   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

6.1.9   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

6.1.10   POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

6.1.11   APOP Authentication

Configure APOP authentication settings.

For details, refer to page 4-16.

6.2 Receiving Internet faxes

Configure settings to receive Internet faxes.

To use the Internet fax function, ask your service representative to configure settings. For details, contact your service representative.

Internet faxing sends and receives the read original as an E-mail attachment file (TIFF format) via Intranet or Internet. It also allows you to send a colored original.

The Internet fax function establishes a communication via Intranet or Internet; therefore, you can reduce the communication cost compared with a general Fax communication when frequently handling remote or over-seas communications.

This function performs SSL/TLS encryption or APOP authentication when receiving Internet faxes, assuring more secure communications.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    ┌─────────────────────┐
                    │  [TCP/IP Settings]  │
                    └─────────────────────┘
                              │
                    ┌─────────────────────┐
                    │ [Network Fax Func-  │
                    │  tion Settings]     │
                    └─────────────────────┘
                              │
                    ┌─────────────────────┐
                    │  [E-mail RX (POP)]  │
                    └─────────────────────┘
                              │
          ┌───────────[Network Fax Setting]───────────┐
          │                                           │
┌─────────────────────┐                   ┌─────────────────────┐
│ Do you have an SSL  │                   │ APOP?               │
│ communication with  │                   │                     │
│ the POP server?     │                   │                     │
└─────────────────────┘                   └─────────────────────┘
     │           │                             │           │
    Yes          No                           Yes          No
     │           │                             │           │
┌──────────┐     │                        ┌──────────────────┐  │
│POP over  │     │                        │APOP              │  │
│SSL       │     │                        │Authentication    │  │
└──────────┘     │                        └──────────────────┘  │
     │           │                             │                 │
     └───────────┴──────── Finish ────────────┴─────────────────┘
```
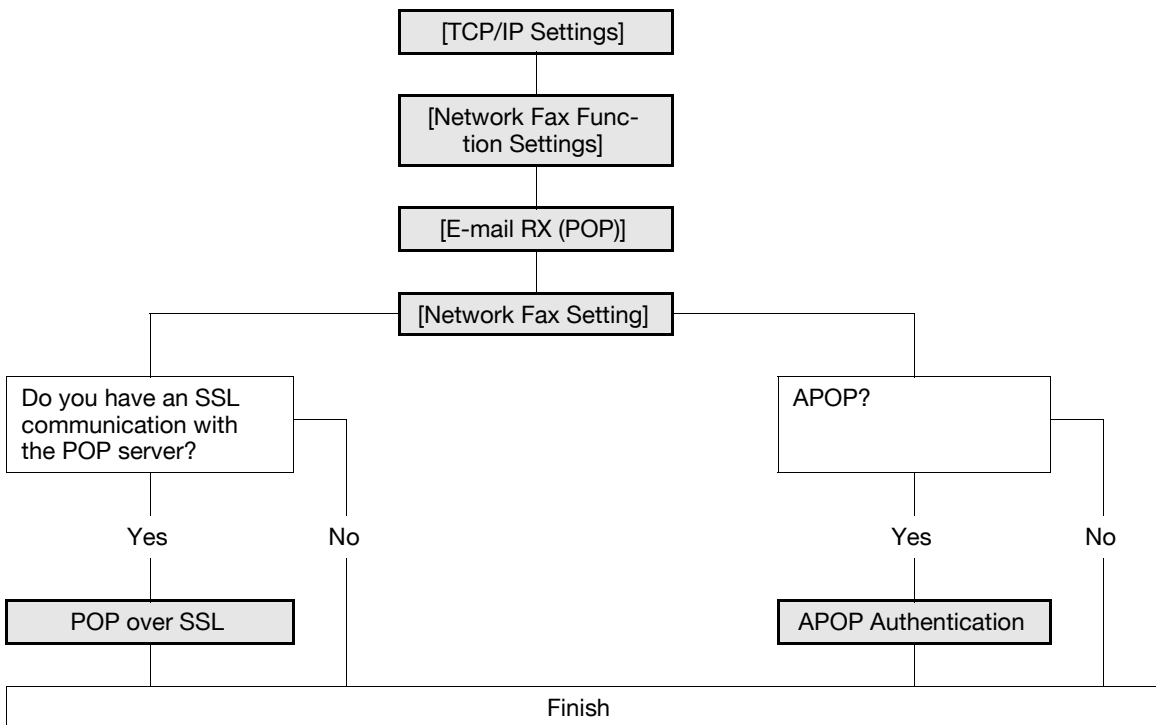
📖 **Reference**
For details on the Internet fax function, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

6.2.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

6.2.2 [Network Fax Function Settings]

Enables the Internet fax function of this machine.

For details, refer to page 6-4.

6.2.3 [E-mail RX (POP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [E-mail Setting] ▸▸ [E-mail RX (POP)].

Item	Description	Prior check
[E-mail RX Setting]	Select [ON].	
[POP Server Address]	Enter the POP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Login Name]	Enter the login name of the POP server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the POP server (up to 15 characters).	
[Connection Timeout]	Specify the timeout period for a communication with a server.	
[Port Number]	Enter a port number. Default setting: 110	Server port number
[Check for New Messages]	Select this check box to automatically receive an E-mail. To manually receive an E-mail, press [Receive I-Fax] in the Fax/Scan mode.	
[Polling Interval]	Enter the interval to check the arrival by automatically connecting to the POP server.	

6.2.4 [Network Fax Setting]

(This menu item will not be displayed if the Network Fax function is not available.)

[I-Fax Advanced Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▸▸ [Network Fax Setting] ▸▸ [I-Fax Advanced Setting].

(This menu item will not be displayed if the Internet Fax function is not available.)
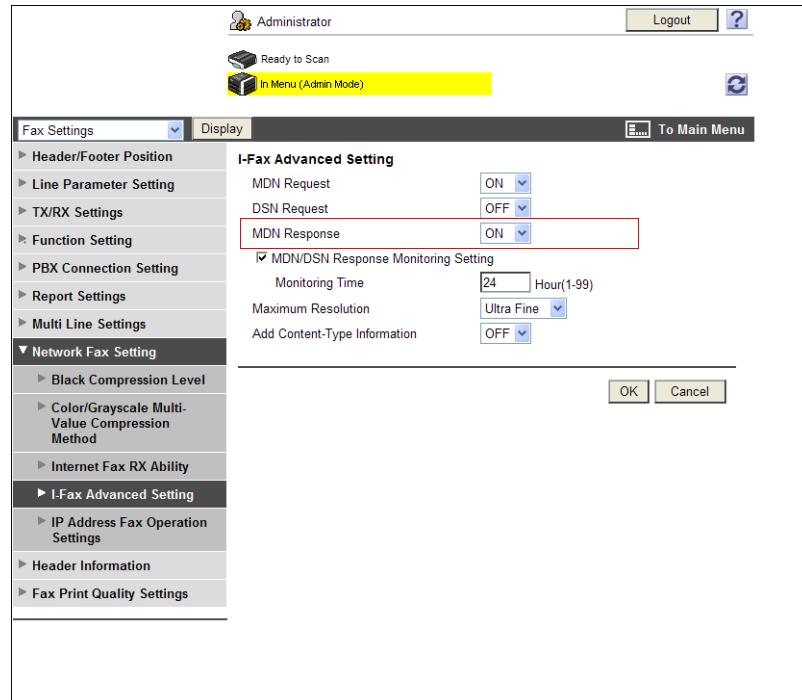
Item	Description	Prior check
[MDN Response]	Select [ON] to respond to an MDN request (reception confirmation request) from the remote side.	

[Internet Fax RX Ability]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▶▶ [Network Fax Setting] ▶▶ [Internet Fax RX Ability].

(This menu item will not be displayed if the Internet Fax function is not available.)

Reference

- The recipient is notified of the RX Ability specified here when this machine sends an MDN response. To enable the RX Ability, set [MDN Response] to [ON] in [I-Fax Advanced Setting].
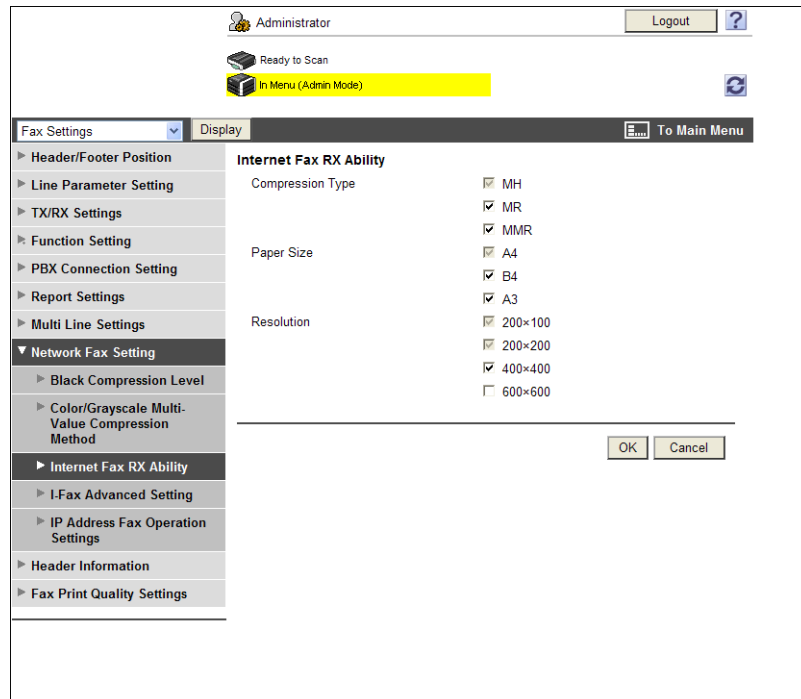
Item	Description	Prior check
[Compression Type]	Select the check box of the compression format that is available for this machine to receive Internet fax. All the compression formats available for this machine are selected in Initial Setting.	
[Paper Size]	Select the check box of the paper size that is available for this machine to receive Internet faxes. All the paper sizes available for this machine are selected by default.	
[Resolution]	Select the check box of the resolution that is available for this machine to receive Internet faxes.	

6.2.5 POP over SSL

Configure the settings for POP over SSL.

6.2.6 APOP Authentication

Configure APOP authentication settings.

6.3   Sending and receiving IP address faxes

Configure settings to send and receive IP address faxes.

IP Address Fax means FAX that is available on the IP network. To send a fax, specify the IP address, host name, or E-mail address of the remote machine.

The SMTP protocol is used to send and receive IP address faxes. Because the SMTP server function of this machine sends and receives data, no server is required when sending or receiving a fax by specifying the IP address of the remote machine. (However, the DNS server is required to send or receive a fax by specifying the host name or E-mail address.)

This machine supports the following two IP address fax operation modes. Switch the operation mode according to your environment.

- [Mode 1]: This mode allows communication between Konica Minolta models capable of transmitting IP address faxes, and between models compatible with the Direct SMTP standard defined by CIAJ (Communications and Information Network Association of Japan). However, because a unique method developed by Konica Minolta is used to send a color fax, only the Konica Minolta models can receive such a color fax.
- [Mode 2]: This mode allows communication between Konica Minolta models capable of transmitting IP address faxes, and between models compatible with the Direct SMTP standard defined by CIAJ (Communications and Information Network Association of Japan). The method compatible with the Direct SMTP standard (Profile-C format) is used to send a color fax.

To use the IP Address Fax function, check the following.

- Install the optional **Fax Kit FK-508** in this machine.
- To use the IP Address Fax function, ask your service representative to configure settings. For details, contact your service representative.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
┌──────────────────────────────┐
│      [TCP/IP Settings]        │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│  [Network Fax Function Settings] │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│      [SMTP TX Setting]        │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│      [SMTP RX Setting]        │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│     [Network Fax Setting]     │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│     [Header Information]       │
└──────────────────────────────┘
                │
┌──────────────────────────────┐
│           Finish              │
└──────────────────────────────┘
```
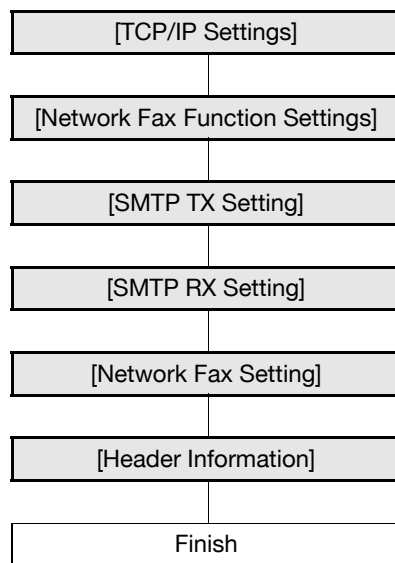
📖 **Reference**
For details on how to register IP address fax destinations refer to page 11-7.

For details on IP Address Fax, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

6.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

6.3.2 [Network Fax Function Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Network Fax Setting] ►► [Network Fax Function Settings].

Item	Description	Prior check
[IP Address Fax Function Settings]	Select [ON].	

6.3.3 [SMTP TX Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [Network Fax Setting] ▶▶ [SMTP TX Setting].

Item	Description	Prior check
[Port Number]	Enter a port number. Default setting: 25	Required port number
[Connection Time-out]	Enter the timeout period for a communication with a server.	

6.3.4   [SMTP RX Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Network Fax Setting] ►► [SMTP RX Setting].
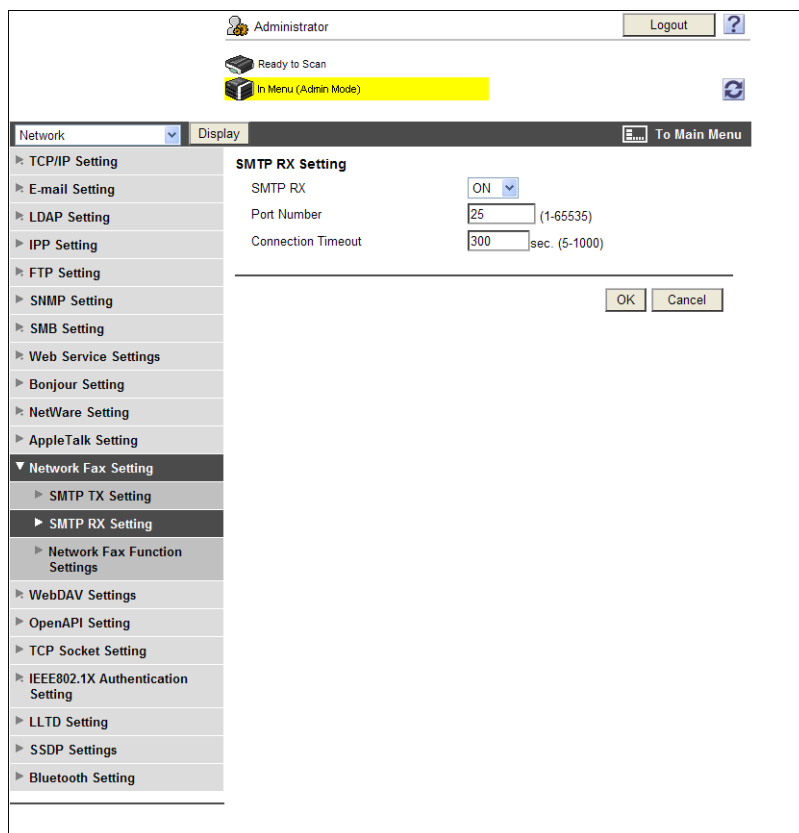
Item	Description	Prior check
[SMTP RX]	Select [ON].	
[Port Number]	Enter a port number. Default setting: 25	Required port number
[Connection Time-out]	Enter the timeout period for a communication with a server.	

6.3.5 [Network Fax Setting]

(This menu item will not be displayed if the Network Fax function is not available.)

[Black Compression Level]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Network Fax Setting] ►► [Black Compression Level].

Item	Description	Prior check
[Black Compression Level]	Select the default setting of the black compression level in the black and white sending mode.	

[Color/Grayscale Multi-Value Compression Method]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Network Fax Setting] ►► [Color/Grayscale Multi-Value Compression Method].

Item	Description	Prior check
[Color/Grayscale Multi-Value Compression Method]	Select the default setting of the color/grayscale multi-value compression method in the color sending mode.	

[IP Address Fax Operation Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings]▶▶[Network Fax Setting]▶▶[IP Address Fax Operation Settings].
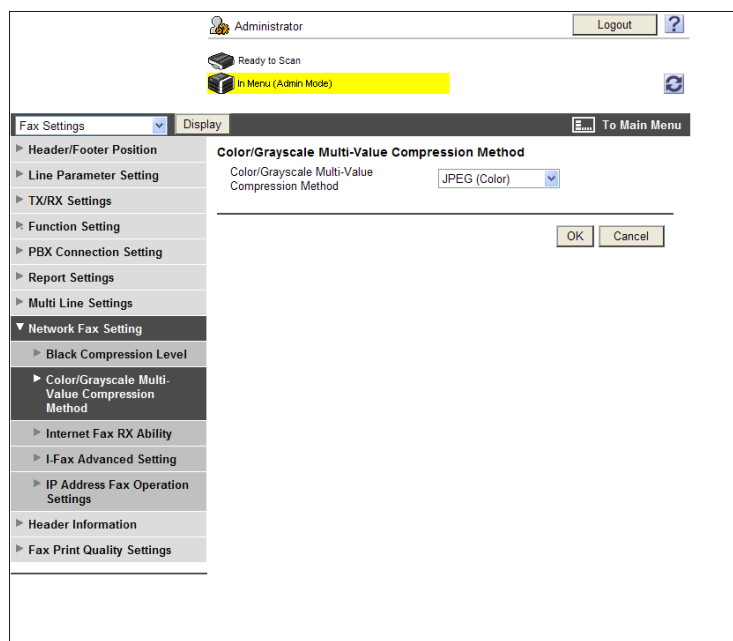

Item	Description	Prior check
[Operating Mode]	Select the operation mode for IP address fax according to your environment. • [Mode 1]: This mode allows communication between Konica Minolta models capable of transmitting IP address faxes, and between models compatible with the Direct SMTP standard defined by CIAJ (Communications and Information Network Association of Japan). However, because a unique method developed by Konica Minolta is used to send a color fax, only the Konica Minolta models can receive such a color fax. • [Mode 2]: This mode allows communication between Konica Minolta models capable of transmitting IP address faxes, and between models compatible with the Direct SMTP standard defined by CIAJ (Communications and Information Network Association of Japan). The method compatible with the Direct SMTP standard (Profile-C format) is used to send a color fax.	
[Sending Colored Documents]	Select whether or not to accept sending of colored originals when selecting [Mode 2] for [Operating Mode]. If you select [Restrict], color originals are converted to black and white before sending. To send a fax to a machine that does not support color reception based on the Direct SMTP standard, select [Restrict].	Can the recipient machine receive a color fax using the Direct SMTP standard?

6.3.6   [Header Information]

Register sender information for fax sending.

For details, refer to page 14-20.

7 Using User Authentication

7   Using User Authentication

7.1   Restricting users of this machine (MFP authentication)

Configure settings to restrict users who can use this machine by MFP authentication.

You can configure the user authentication and account track settings to restrict use of this machine. Specify user authentication when managing individual users, and specify account track when managing a group or multiple users.

You can use a combination of user authentication and account track for management of each user for each department. You can use this function to assign the counter to both the department and user counters, and to aggregate the resulting values of both counters.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

7.1.1 [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (MFP)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Account Track]	To enable account track, select [ON].	Do you use the account track function?
[Account Track Input Method]	To use the account track function, select its authentication method. This setting is required when you only use the account track function.	
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track and manage users for each account track, select [Synchronize]. Once you specify the account name of the user at user registration, you will be bale to log in by entering only the user name. If you have omitted the account name, the user must specify the account name when logging in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user.	Do you synchronize user authentication with account track?
[Number of Counters Assigned for Users]	Enter a number of user counters to be assigned if user authentication and account track are enabled. You can aggregate the counter by user or account track, and assign up to 1,000 counters to users and account tracks. For example, if the number of user counters to be assigned is set to 950, you can register up to 50 account tracks.	

Item	Description	Prior check
[When Number of Jobs Reach Maximum Skip Job Stop Job]	Select the operation that is performed when the job count of each user or department has reached its limit. This limit must be set during user registration or account track registration.	

Reference

- If [Enhanced Security Mode] is enabled, you cannot select [OFF] in [General Settings]▸▸[User Authentication]. Also, you cannot allow the public user access.
- If a **Hard Disk** is not installed in this machine, the upper limit is set to 99 in [Number of Counters Assigned for Users].

7.1.2 [Administrative Setting]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track]▸▸[General Settings]▸▸[Administrative Setting].

(This menu item will not be displayed if user authentication is disabled.)

Reference

- This function is available only when a **Hard Disk** is installed.

Item	Description	Prior check
[ID & Print]	Select whether to process all print jobs requested from a registered user as ID & print jobs. If you select [ON], all print jobs requested from a registered user are processed as ID & print jobs even when [ID & Print] is not enabled on the printer driver. If you select [OFF], print jobs are processed as ID & print jobs only when [ID & Print] is enabled on the printer driver. A print job requested from a registered user is processed as a normal one if [ID & Print] is not enabled on the printer driver.	Do you want to process all print jobs requested from a registered user as ID & Print jobs?
[Public User]	Select the operation required when receiving a job without authentication information (a job for which printing is instructed while user authentication or account track is not enabled on the printer driver) or receiving a public user's job. If you select [Print Immediately], the received job is printed as it is. If you select [Save], the received job is saved in the ID & Print User Box.	

Item	Description	Prior check
[ID & Print Operation Settings]	Select the operating mode when using the ID & Print function on an optional Authentication Unit. This item is displayed when the optional Authentication Unit is installed. Select [Print All Jobs] to print all jobs of the target user that are saved in the ID & Print User Box by one authentication operation. Select [Print Each Job] to print one job of the target user that is saved in the ID & Print User Box by one authentication operation.	
[Default Operation Selection]	Select the default operation you want to apply after Authentication has been completed on the authentication unit (success in login). If you select [Begin Printing], ID & print jobs are executed after authentication has been completed. If you select [Print & Access], ID & print jobs are executed after authentication has been completed, and you can log in to the basic window. If you select [Access], you can log in to the basic window after authentication has been completed. In this case, ID & print jobs are not executed.	

Reference
- For details on the ID & print function, refer to the [User's Guide Print Operations].

7.1.3   User Registration

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [User Authentication Setting] ►► [User Registration] ►► [New].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[No.]	Select a registration numbering system. If you specify the registration number, enter the number directly.	

Item	Description	Prior check
[User Name]	Enter a user name (up to 64 characters).	
[E-mail Address]	Enter the E-mail address of the user (up to 320 characters).	
[User Password is changed.]	Select this check box to change the password. This item is displayed when editing the registered information.	
[User Password]	Enter a password (up to 64 characters, excluding space and ").	
[Retype User Password]	Reenter the password for confirmation (up to 64 characters).	
[Account Name]	Enter an account name of the user. Before you specify an account name, you must register the account. This item is displayed if user authentication and account track are synchronized. If you have omitted the account name, the user must specify the user and account name when the user log in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user. If the account information is changed after the account name has been specified, the user and the account will be dissociated.	
[Specify Icon]	From [Search from List], select an icon for the user.	
[Temporarily stop use]	Select whether to temporarily disable a registered user. This item is available when temporarily disabling registered users without deleting them. If you select [Stop Job], the target user cannot log in to or use this machine. This function is available when the MFP authentication is enabled.	
[Function Permission]	Specify whether to permit [Copy], [Scan], [Save to External Memory], [External Memory Document Scan], [Fax], [Print], [User Box], [Print Scan/Fax TX], [Manual Destination Input], [Mobile/PDA], and [Biometric/IC Card Information Registration].	
[Output Permission(TX)]	Select whether to allow the user to send color images.	
[Max. Allowance Set]	Specify the maximum numbers of printed sheets and User Boxes. To specify the limit, select the appropriate check box and enter the desired limit value.	
[Limiting Access to Destinations]	Restrict address book entries the user can access. To specify the reference allowed groups, select this check box and select groups from the list. You can select one or more reference allowed groups. To specify the access allowed level, select the check box and specify the access allowed level. Before you specify the reference allowed groups, you must register reference allowed groups. For details, refer to page 8-36.	

Reference
- You cannot register a password less than eight characters when [Security Settings]▸▸[Security Details]▸▸[Password Rules] is set to [Enable] in the [Administrator Settings] on the **Control Panel**. If a user password containing less than eight characters has already been registered, change the password so that it contains eight characters before setting [Password Rules] to [Enable].
- If you permit the public user access, you can configure the Function Permission and Limiting Access to Destinations settings for the public user. For details, refer to page 8-40.

- Whether to allow the [Save to External Memory] function can be specified when [Save Document] is set to [ON] in [System Settings]▶▶[User Box Settings]▶▶[External Memory Function Settings]. Whether to allow the [External Memory Document Scan] function can be specified when [USB to User Box] is set to [ON] in [External Memory Function Settings]. For details, refer to page 12-7.
- When [Security Settings]▶▶[Security Details]▶▶[Manual Destination Input] is set to [Restrict] in [Administrator Settings] on the **Control Panel**, the user cannot manually enter the address regardless of the setting of this function.
- To connect this machine to a cellular phone or PDA, install the optional **Local Interface Kit EK-605** in this machine. Whether to allow the [Mobile/PDA] function can be specified when [Bluetooth] is set to [Enable] in [Network]▶▶[Bluetooth Setting] and [Bluetooth Print Settings] is set to [ON] in [System Settings]▶▶[System Connection Setting].
- Whether to allow the [Biometric/IC Card Information Registration] function can be specified when [Biometric/IC Card Information Registration] is set to [Allow] in [Security]▶▶[Restrict User Access] while the optional authentication unit is installed.
- The following functions are available only when a **Hard Disk** is installed.
  [Save to External Memory] and [External Memory Document Scan] under [Function Permission]
  [Box Administration] under [Max. Allowance Set]

7.1.4 Account Track Registration

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▶▶ [Account Track Settings] ▶▶ [New Registration].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[No.]	Select a registration numbering system. If you specify the registration number, enter the number directly.	

Item	Description	Prior check
[Account Name]	Enter an account name (up to 8 characters, excluding space and ").	
[Password is changed.]	Select this check box to change the password. This item is displayed when editing the registered information.	
[Password]	Enter a password (up to 8 characters, excluding space and ").	
[Retype Password]	Re-enter the password (up to 8 characters).	
[Temporarily stop use]	Select whether to temporarily disable a registered account. This item is available when temporarily disabling registered accounts without deleting them. If you select [Stop Job], the target account cannot log in to or use this machine. If you disable an account registered as a user's account name, users who belong to the disabled account also cannot log in to this machine.	
[Output Permission(TX)]	Select whether to allow the user to send color images.	
[Max. Allowance Set]	Specify the maximum numbers of printed sheets and User Boxes. To specify the limit, select the appropriate check box and enter the desired limit value.	

Reference

- You cannot register a password less than eight characters when [Security Settings]▶▶[Security Details]▶▶[Password Rules] is set to [Enable] in the [Administrator Settings] on the **Control Panel**. If a user password containing less than eight characters has already been registered, change the password so that it contains eight characters before setting [Password Rules] to [Enable].
- The following functions are available only when a **Hard Disk** is installed.
  [User Administration] under [Max. Allowance Set]

7.2   Restricting users of this machine (Active Directory)

Configure settings to restrict users who use this machine by Active Directory authentication.

These settings are required if you wish to use the user authentication with Active Directory on the Windows Server. You can restrict the functions available to each user.

You can also restrict users who use this machine using Active Directory authentication in an IPv6 environment configured by the Active Directory function of Windows Server 2008.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
            [TCP/IP Settings]

        [External Server Settings]

            [General Settings]

          [Administrative Setting]

        [Default Function Permis-
                  sion]

           [Date/Time Setting]

                 Finish
```
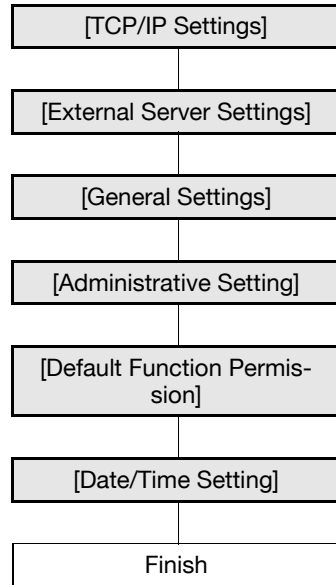
7.2.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.
- To use Active Directory, register the DNS server connected to Active Directory in this machine.
- To perform Active Directory authentication in an IPv6 environment configured by the Active Directory function of Windows Server 2008, configure IPv6. For details on the IPv6 settings, refer to page 2-5.

For details, refer to page 2-2.

7.2.2 [External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [External Server Settings] ▸▸ [Edit].

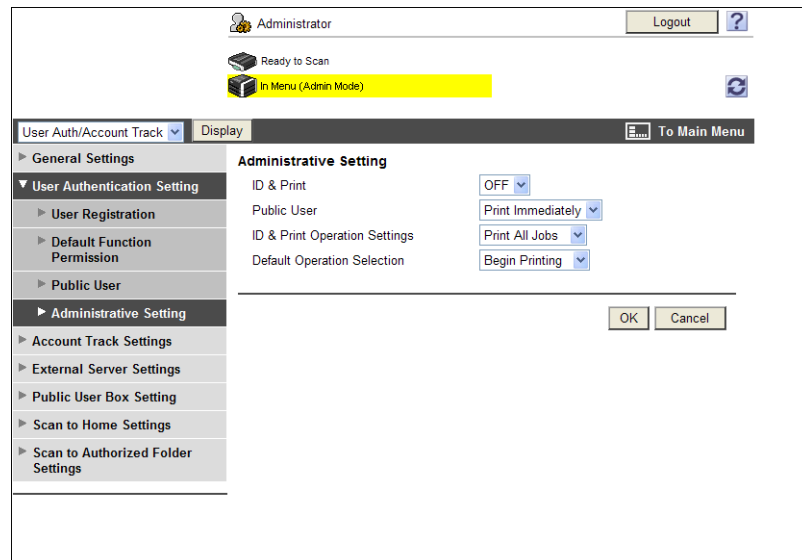| Item	Description	Prior check
[No.]	Displays the registration number.	
[External Server Name]	Enter the name of an external authentication server (up to 32 characters).	
[External Server Type]	Select [Active Directory].	
[Default Domain Name]	Enter the default domain name of Active Directory (up to 64 characters).	Default Domain Name

7.2.3 [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (External Server)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Ticket Hold Time Setting (Active Directory)]	Enter a time to hold the Kerberos authentication tickets.	
[Account Track]	To enable account track, select [ON]. To select [ON], specify the authentication method first, and then register accounts in [Account Track Settings].	Do you use the account track function?
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track and manage users for each account track, select [Synchronize]. To synchronize, specify the account name when logging in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user.	Do you synchronize user authentication with account track?

7.2.4 [Administrative Setting]

Configure settings to use or operate the ID & Print function.

For details, refer to page 7-4.

7.2.5   [Default Function Permission]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track]▶▶[User Authentication Setting]▶▶[Default Function Permission].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[Copy]	Configure the default settings for function permissions to users who are authenticated on the external server. If a user not registered on this machine is authenticated on the external server, the user will be registered on this machine with the function permissions that you configure here. Once the function permissions of a user have been registered on this machine, you can edit them in [User Registration].	
[Scan]		
[Save to External Memory]		
[External Memory Document Scan]		
[Fax]		
[Print]		
[User Box]		
[Print Scan/Fax TX]		
[Manual Destination Input]		
[Mobile/PDA]		

Reference

- Whether to allow the [Save to External Memory] function can be specified when [Save Document] is set to [ON] in [System Settings]▶▶[User Box Settings]▶▶[External Memory Function Settings]. Whether to allow the [External Memory Document Scan] function can be specified when [USB to User Box] is set to [ON] in [External Memory Function Settings]. For details, refer to page 12-7.
- When [Security Settings]▶▶[Security Details]▶▶[Manual Destination Input] is set to [Restrict] in [Administrator Settings] on the **Control Panel**, the user cannot manually enter the address regardless of the setting of this function.
- To connect this machine to a cellular phone or PDA, install the optional **Local Interface Kit EK-605** in this machine. Whether to allow the [Mobile/PDA] function can be specified when [Bluetooth] is set to [Enable] in [Network]▶▶[Bluetooth Setting] and [Bluetooth Print Settings] is set to [ON] in [System Settings]▶▶[System Connection Setting].
- The following functions are available only when a **Hard Disk** is installed.
  [Save to External Memory]
  [External Memory Document Scan]

7.2.6   [Date/Time Setting]

To use Active Directory, specify the date and time of this machine.

- You cannot log in to Active Directory if the system time of this machine and Active Directory is extremely different. Specify the date and time for this machine to match the system time of Active Directory.

For details, refer to page 10-2.

7.3   Restricting users of this machine (Windows domain or work-group)

Configure settings to restrict users who can use this machine by NTLM authentication.

These settings are required if you wish to use NTLM authentication when using the Windows NT 4.0 system or when using Active Directory (NT-compatible domain environment) in the Windows Server system. You can restrict the functions available to each user.

You can also restrict users who can use this machine by NTLM authentication in an IPv6 environment configured by the Active Directory function (NT-compatible domain environment) of Windows Server 2008.

To use NTLM authentication in the IPv6 environment, you must enable the Direct Hosting service. To resolve the names using a DNS server, prepare the DNS server and configure the DNS settings of this machine.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    ┌──────────────────────────┐
                    │     [TCP/IP Settings]     │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │ [External Server Settings]│
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │     [General Settings]    │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │  [Administrative Setting] │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │ [Default Function Permis- │
                    │          sion]            │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │      [Client Setting]     │
                    └──────────────────────────┘
                                 │
                       In an IPv6 environment?
              No                                      Yes
               │                                       │
    Do you use a WINS server?            ┌──────────────────────────┐
      Yes          No                    │  [Direct Hosting Setting] │
       │            │                    └──────────────────────────┘
 ┌──────────────┐   │
 │ [WINS Setting]│  │
 └──────────────┘   │
       └────────────┴─────────────────────────────────┘
                    ┌──────────────────────────┐
                    │          Finish           │
                    └──────────────────────────┘
```

7.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

- To perform NTLM authentication in an IPv6 environment configured by the Active Directory function (NT-compatible domain environment) of Windows Server 2008, configure IPv6. For details on the IPv6 settings, refer to page 2-5.
- To use NTLM authentication in the IPv6 environment, you must enable the Direct Hosting service. To resolve the names using a DNS server, prepare the DNS server and configure the DNS settings of this machine.

For details, refer to page 2-2.

7.3.2 [External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [External Server Settings] ►► [Edit].

Item	Description	Prior check
[No.]	Displays the registration number.	
[External Server Name]	Enter the name of an external authentication server (up to 32 characters).	
[External Server Type]	Select [NTLM v1] or [NTLM v2]. NTLMv2 is applied on the Windows NT 4.0 (Service Pack 4) and later.	
[Default Domain Name]	Enter the NTLM default domain name (up to 64 characters). The default domain name must be uppercase letters.	Default Domain Name

7.3.3   [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (External Server)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Account Track]	To enable account track, select [ON]. To select [ON], specify the authentication method first, and then register accounts in [Account Track Settings].	Do you use the account track function?
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track and manage users for each account track, select [Synchronize]. To synchronize, specify the account name when logging in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user.	Do you synchronize user authentication with account track?

7.3.4   [Administrative Setting]

Configure settings to use or operate the ID & Print function.

For details, refer to page 7-4.

7.3.5   [Default Function Permission]

Configure the default settings for function permissions to users who are authenticated on the external server.

For details, refer to page 7-13.

7.3.6 [Client Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [SMB Setting] ►► [Client Setting].
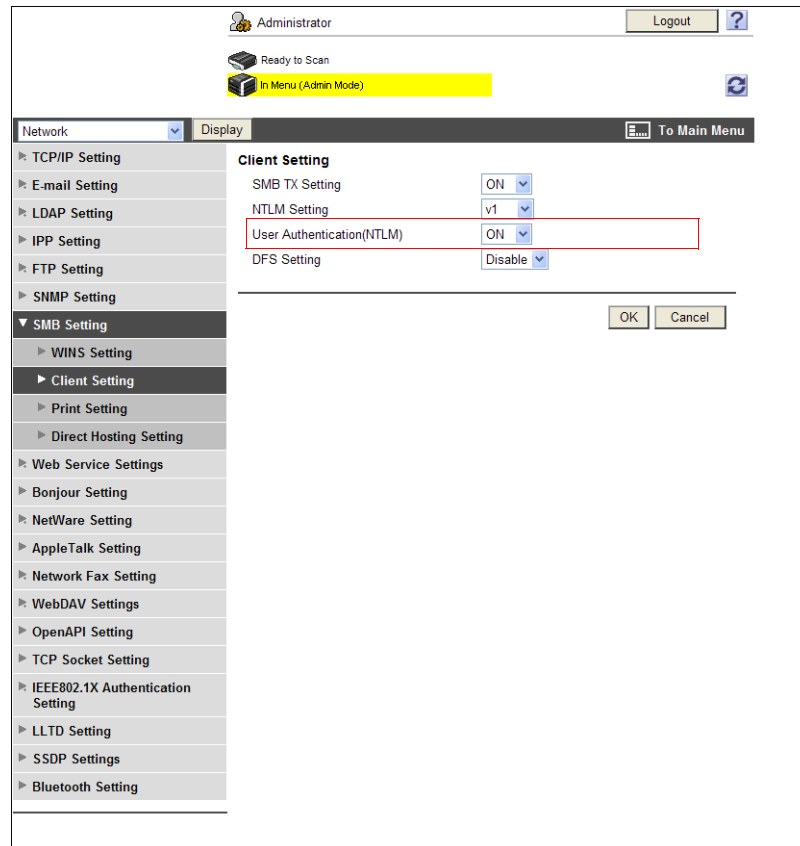
Item	Description	Prior check
[User Authentication (NTLM)]	Select [ON]. If you set this option to [OFF] when NTLM authentication is used, the authentication method will be switched to the MFP authentication.	

7.3.7 [WINS Setting]

When you start NTLM authentication via the router, you must set up the WINS server.

For details, refer to page 4-4.

7.3.8 [Direct Hosting Setting]

To use NTLM authentication in the IPv6 environment, you must enable the direct hosting service.

For details, refer to page 4-5.

7.4   Restricting users of this machine (NDS over IPX/SPX)

Configure settings to restrict users who use this machine by NDS over IPX/SPX authentication.

These settings are required if you use the NetWare 5.1 or later and use the NDS authentication in the IPX/SPX environment. You can restrict the functions available to each user.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
        [External Server Settings]
                   |
           [General Settings]
                   |
         [Administrative Setting]
                   |
      [Default Function Permis-
                sion]
                   |
          [NetWare Settings]
                   |
                Finish
```
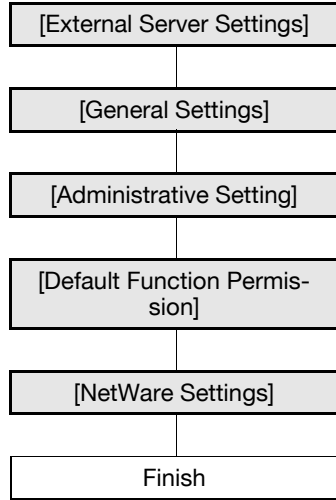
7.4.1   [External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [External Server Settings] ►► [Edit].

Item	Description	Prior check
[No.]	Displays the registration number.	
[External Server Name]	Enter the name of an external authentication server (up to 32 characters).	

Item	Description	Prior check
[External Server Type]	Select [NDS over IPX/SPX].	
[Default NDS Tree Name]	Enter the default NDS tree name (up to 63 characters).	
[Default NDS Context Name]	Enter the default NDS context name (up to 191 characters).	

7.4.2 [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (External Server)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Account Track]	To enable account track, select [ON]. To select [ON], specify the authentication method first, and then register accounts in [Account Track Settings].	Do you use the account track function?
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track and manage users for each account track, select [Synchronize]. To synchronize, specify the account name when logging in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user.	Do you synchronize user authentication with account track?

7.4.3 [Administrative Setting]

Configure settings to use or operate the ID & Print function.

For details, refer to page 7-4.

7.4.4 [Default Function Permission]

Configure the default settings for function permissions to users who are authenticated on the external server.

For details, refer to page 7-13.

7.4.5 [NetWare Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [NetWare Setting] ▶▶ [Net-Ware Setting].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type
[User Authentication Setting]	Select [ON].	

7.5   Restricting users of this machine (NDS over TCP/IP)

Configure settings to restrict users who use this machine by NDS over TCP/IP authentication.

These settings are required if you use the NetWare 5.1 or later and use NDS authentication in the TCP/IP environment. You can restrict the functions available to each user.

To use the authentication with NDS over TCP/IP, you must specify the DNS server in [TCP/IP Settings]. During user authentication, the tree name and context name are inquired to the specified DNS server to obtain the IP address of the NDS authentication server.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference
● Apply the latest service pack to each NetWare version.
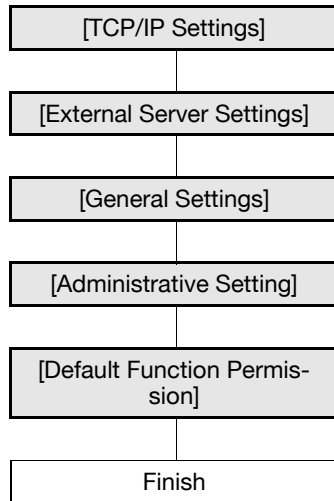
7.5.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.
● To use the authentication with NDS over TCP/IP, you must specify the DNS server.

For details, refer to page 2-2.

7.5.2   [External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [External Server Settings] ►► [Edit].

Item	Description	Prior check
[No.]	Displays the registration number.	
[External Server Name]	Enter the name of an external authentication server (up to 32 characters).	
[External Server Type]	Select [NDS over TCP/IP].	
[Default NDS Tree Name]	Enter the default NDS tree name (up to 63 characters).	
[Default NDS Context Name]	Enter the default NDS context name (up to 191 characters).	

7.5.3 [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (External Server)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Account Track]	To enable account track, select [ON]. To select [ON], specify the authentication method first, and then register accounts in [Account Track Settings].	Do you use the account track function?
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track and manage users for each account track, select [Synchronize]. To synchronize, specify the account name when logging in for the first time. The account name that the user specify at the first login time will be registered as the account name of the user.	Do you synchronize user authentication with account track?

7.5.4 [Administrative Setting]

Configure settings to use or operate the ID & Print function.

For details, refer to page 7-4.

7.5.5 [Default Function Permission]

Configure the default settings for function permissions to users who are authenticated on the external server.

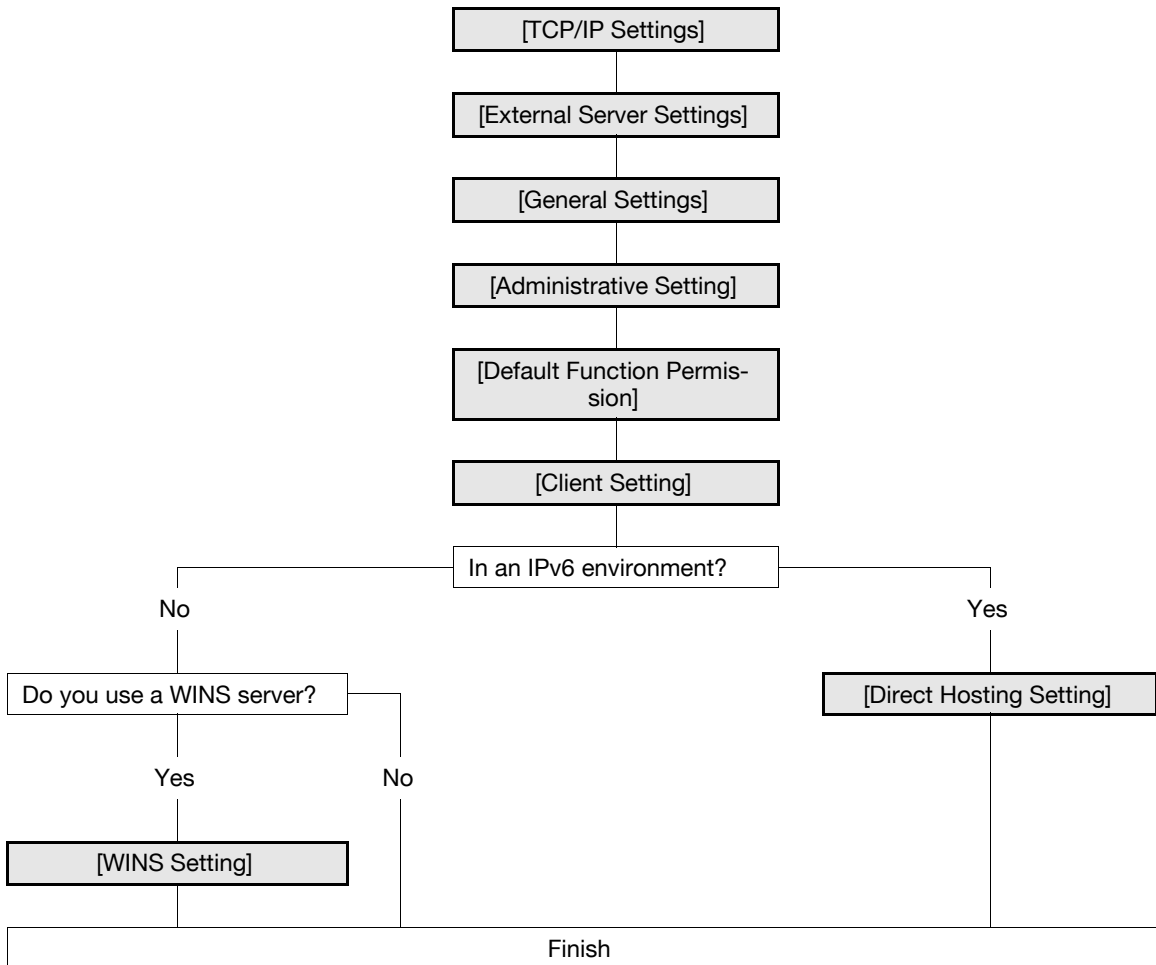For details, refer to page 7-13.

7.6   Restricting users of this machine (LDAP)

Configure settings to restrict users who use this machine by LDAP authentication.

These settings are required if you use the LDAP server for user authentication. You can restrict the functions available to each user.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference

- To use the same LDAP server for both user authentication and destination search, the certificate verification settings of the LDAP server for user authentication specified in [External Server Settings] are determined according to the certificate verification settings of the LDAP server for destination search specified in [Network] ►► [LDAP Settings] ►► [Setting Up LDAP]. For details on LDAP server settings for destination search and certificate verification settings, refer to page 10-5.

```
        ┌──────────────────────────┐
        │     [TCP/IP Settings]     │
        └──────────────────────────┘
                     │
        ┌──────────────────────────┐
        │  [External Server Settings]│
        └──────────────────────────┘
                     │
        ┌──────────────────────────┐
        │     [General Settings]    │
        └──────────────────────────┘
                     │
        ┌──────────────────────────┐
        │  [Administrative Setting] │
        └──────────────────────────┘
                     │
        ┌──────────────────────────┐
        │  [Default Function Per-   │
        │        mission]           │
        └──────────────────────────┘
                     │
        ┌──────────────────────────┐
        │  Do you have an SSL        │──────────┐
        │  communication with the   │          │
        │  LDAP server?             │          │
        └──────────────────────────┘          │
               Yes              No
                │                              │
        ┌──────────────────────────┐          │
        │       LDAP over SSL       │          │
        └──────────────────────────┘          │
                │                              │
        ┌──────────────────────────────────────┐
        │              Finish                   │
        └──────────────────────────────────────┘
```
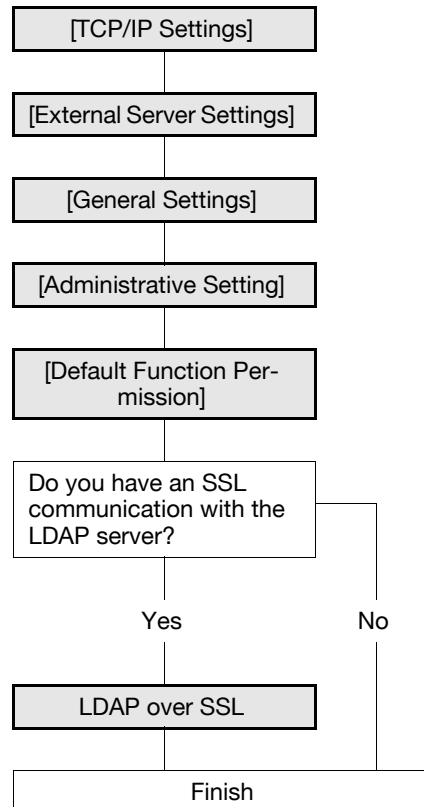
7.6.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

7.6.2 [External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸ [External Server Settings] ▸ [Edit].

Item	Description	Prior check
[No.]	Displays the registration number.	
[External Server Name]	Enter the name of an external authentication server (up to 32 characters).	
[External Server Type]	Select [LDAP].	
[Server Address]	Specify the LDAP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port No.]	Enter a port number. Default setting: 389	
[Search Base]	Enter the search starting point in the directory structure under the LDAP server (up to 255 characters). This search function also covers subdirectories under the entered starting point.	Search base
[Timeout]	Enter the timeout period for LDAP search.	
[General Settings]	Select the authentication method to log in to the LDAP server. Select the same authentication method as that used on the LDAP server.	Server authentication method
[Search Attribute]	Enter attributes to be used for search of user account (up to 64 characters, the only symbol allowed is a hyphen (-)).	

7.6.3 [General Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [General Settings].

(If you use **PageScope Authentication Manager** for authentication, this menu is not displayed. Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

Item	Description	Prior check
[User Authentication]	Select [ON (External Server)].	
[Public User Access]	Select whether to allow the public user access. If [ON (With Login)] is selected, the public user can use this machine by selecting [Public User Access] in the login page to log in to the machine. If [ON (Without Login)] is selected, the public user can use this machine without logging in to the machine in the login page.	Do you permit the public user access?
[Account Track]	To enable account track, select [ON]. To select [ON], specify the authentication method first, and then register accounts in [Account Track Settings].	Do you use the account track function?
[Synchronize User Authentication & Account Track]	To synchronize user authentication with account track, select [Synchronize].	Do you synchronize user authentication with account track?

7.6.4 [Administrative Setting]

Configure settings to use or operate the ID & Print function.

For details, refer to page 7-4.

7.6.5 [Default Function Permission]

Configure the default settings for function permissions to users who are authenticated on the external server.

For details, refer to page 7-13.

7.6.6   LDAP over SSL

[External Server Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [External Server Settings] ▸▸ [Edit].

Item	Description	Prior check
[Enable SSL]	Select this check box to encrypt an SSL communication between this machine and the LDAP server.	Does the server support SSL?
[Port Number (SSL)]	Enter the port number to be used for SSL communication.	Server port number

[Setting Up LDAP]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [LDAP Setting] ▸▸ [Setting Up LDAP] ▸▸ [Edit].

Reference
- To verify a certificate, specify the certificate verification method, and register the same information as for the LDAP server specified in [External Server Settings]. For details, refer to page 10-7.

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	
[CN]	Select whether to check that the CN of the server certificate matches the server address.	
[Key Usage]	Select whether to check that the server certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the server certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

8 Reinforcing security

8 Reinforcing security

8.1 Registering the certificate of this machine for SSL communications

Register the certificate of this machine (device certificate) to configure SSL communication settings.

The device certificate is registered in this machine at the time of shipment; therefore, SSL-encrypted communication is enabled immediately after installation.

This machine allows you to manage multiple device certificates. To register a new device certificate with this machine, create a self-signed certificate, or ask a certificate authority (CA) and install the issued certificate. You can also import an exported device certificate.

When using this machine for the following purposes, you can encrypt a communication from a client computer to this machine using SSL. For details, refer to the relevant reference page.
- "Using PageScope Web Connection" (p. 3-2)
- "Print (IPPS)" (p. 5-9)
- "Using Web services to secure communication from Vista/Server 2008/7 to this machine via SSL" (p. 8-20)
- "Using IEEE802.1X authentication (for EAP-TLS)" (p. 8-29)
- "Linking an OpenAPI system with this machine" (p. 9-4)
- "Using the FTP server and WebDAV server functions (WebDAV server function only)" (p. 9-9)

Also, if this machine is used for any of the following purposes, this machine submits (attaches) a device certificate that has been registered in this machine. For details, refer to the relevant reference page.
- "Sending scanned data by E-mail (with digital signature)" (p. 4-20)
- "Using IEEE802.1X authentication (for EAP-TTLS or PEAP)" (p. 8-29)
- "Using applications that communicate with this machine with TCP Socket" (p. 9-2)
- To submit a certificate upon request from a server (SMTP, POP, LDAP, WebDAV)

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.
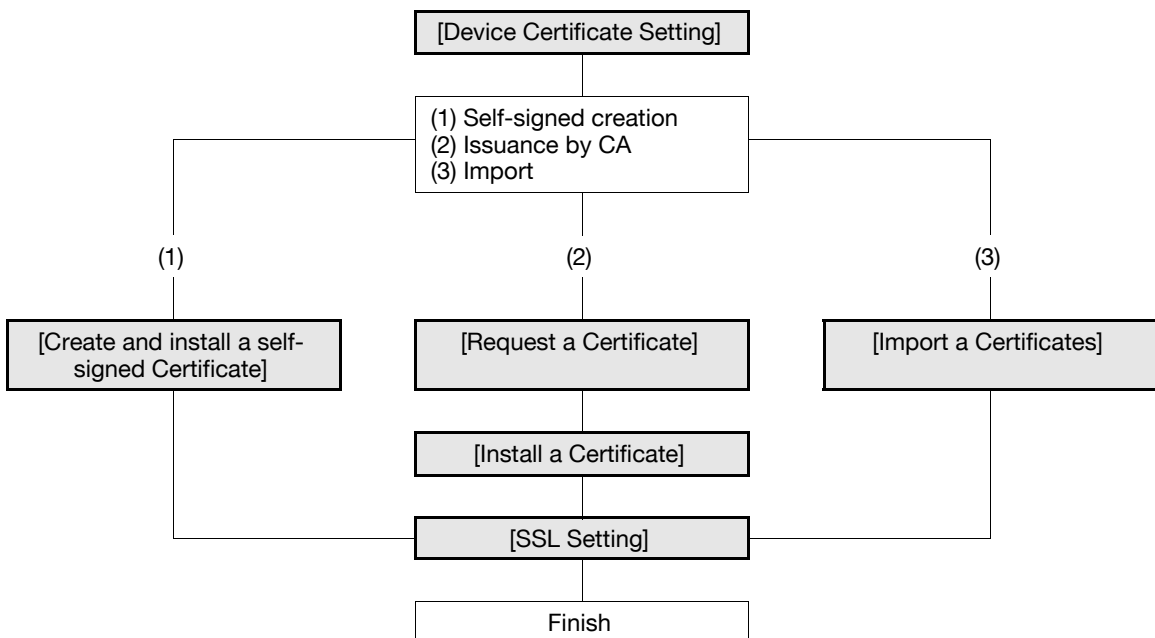
📖 **Reference**
This machine enables you to use multiple registered device certificates depending on protocols. For details on how to use device certificates depending on purposes, refer to page 8-9.

8.1.1   [Device Certificate Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [Device Certificate Setting].

Item	Description	Prior check
[New Registration]	Register a new device certificate. Select a registration method: creating a self-signed certificate, requesting an issuance of a certificate, or importing a certificate. Up to 10 certificates can be registered. If 10 certificates have already been registered, [New Registration] does not appear.	
[Default]	Specify the default device certificate. When not using device certificates depending on protocols, specify the default device certificate.	Default device certificate
[Issuer]	Displays an issuer of a device certificate.	
[Subject]	Displays a destination to issue a device certificate to.	
[Validity Period]	Displays the validity period of a device certificate.	
[Detail]	Enables you to confirm detailed information about a device certificate.	
[Setting]	Enables you to remove or export a device certificate if it is installed. If [Requesting Certificate] is displayed in [Issuer] of the device certificate, you can install a CA-issued certificate in this machine.	

Reference
- If a **Hard Disk** is not installed, only one device certificate can be registered. If one certificate has already been registered, [New Registration] does not appear.

📖 **Reference**

For details on how to remove a device certificate, refer to page 8-8.

For details on how to export a device certificate, refer to page 8-11.

8.1.2   [Create and install a self-signed Certificate]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [Device Certificate Setting] ►► [New Registration] ►► [Create and install a self-signed Certificate].

Item	Description	Prior check
[Common Name]	Displays the IP address or domain name of this machine. This item shows the set value used to access this machine.	
[Organization]	Enter an organization or association name (up to 63 characters).	
[Organizational Unit]	Enter an account name (up to 63 characters). You can also specify a null.	
[Locality]	Enter a city, ward, town, or village name (up to 127 characters).	
[State/Province]	Enter a prefecture name (up to 127 characters).	
[Country]	Enter the country name with a country code defined in ISO03166 (2 characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU	
[Admin. E-mail Address]	Enter the E-mail address of the administrator (up to 128 characters, excluding a space). If the administrator's E-mail address has been specified in [System Settings]►►[Machine Setting], the registered E-mail address is displayed.	E-mail address of the administrator
[Validity Start Date]	Displays the validity period starting date. Displays the date and time (of this machine) when this page was displayed.	
[Validity Period]	Enter the validity period of a certificate with the number of days that have elapsed since the starting date.	
[Encryption Key Type]	Select a type of encryption key.	
[OK]	Click this button to create a self-signed certificate. It may take several minutes to create a certificate.	

8.1.3 [Request a Certificate]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [PKI Settings] ▶▶ [Device Certificate Setting] ▶▶ [New Registration] ▶▶ [Request a Certificate].

Item	Description	Prior check
[Common Name]	Displays the IP address or domain name of this machine. This item shows the set value used to access this machine.	
[Organization]	Enter an organization or association name (up to 63 characters).	
[Organizational Unit]	Enter an account name (up to 63 characters). You can also specify a null.	
[Locality]	Enter a city, ward, town, or village name (up to 127 characters).	
[State/Province]	Enter a prefecture name (up to 127 characters).	
[Country]	Enter the country name with a country code defined in ISO03166 (2 characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU	
[Admin. E-mail Address]	Enter the E-mail address of the administrator (up to 128 characters, excluding a space). If the administrator's E-mail address has been specified in [System Settings]▶▶[Machine Setting], the registered E-mail address is displayed.	E-mail address of the administrator
[Encryption Key Type]	Select a type of encryption key.	
[OK]	Click this button to create certificate signing request data.	

[Certificate Signing Request Data]
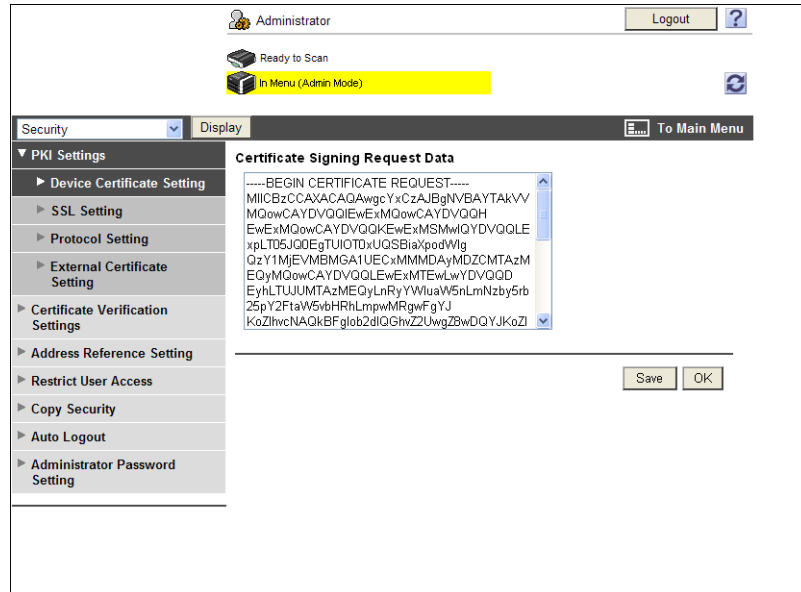
Item	Description	Prior check
[Certificate Signing Request Data]	Displays request data to issue a device certificate. Send the displayed character string to the CA.	
[Save]	Click this button to save certificate signing request data in your computer as a file.	

8.1.4 [Install a Certificate]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [PKI Settings] ▶▶ [Device Certificate Setting] ▶▶ [Setting] ▶▶ [Install a Certificate].

Ask the CA to issue a certificate, and install the certificate sent from the CA in this machine.
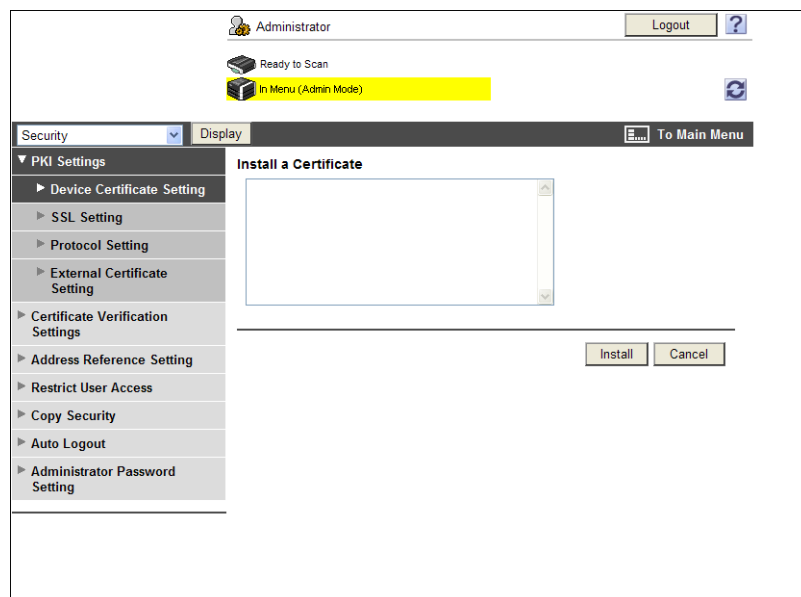
Item	Description	Prior check
[Install a Certificate]	Pastes text data sent from the CA.	
[Install]	Click this button to install a certificate.	

8.1.5 [Import a Certificates]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [Device Certificate Setting] ►► [New Registration] ►► [Import a Certificates].

Item	Description	Prior check
[File]	Specify the file name of the device certificate to be imported. Click [Browse] to specify where to save a certificate file.	
[Password]	Enter the password to decode the encrypted certificate file (up to 32 characters).	

8.1.6 [SSL Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [SSL Setting].

Item	Description	Prior check
[Mode using SSL/TLS]	Select the **PageScope Web Connection** mode to apply SSL. Click [None] to disable SSL.	
[Encryption Strength]	Specify the SSL encryption strength.	

8.1.7 [Remove a Certificate]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [Device Certificate Setting] ►► [Setting] ►► "Remove a Certificate".

Click [OK] to remove the registered device certificate.
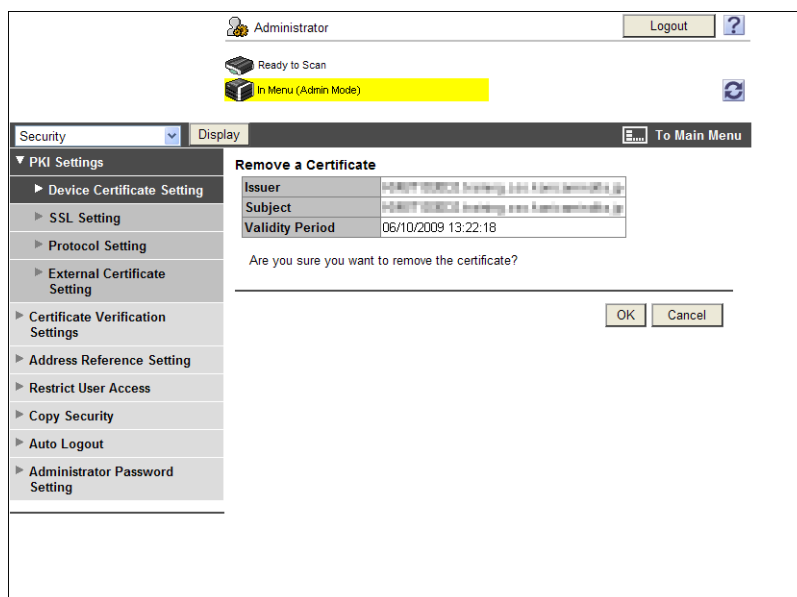
Reference
- To remove the default device certificate while two or more certificates are registered, specify the other one as the default.
- If [Enhanced Security Mode] is enabled, the device certificate cannot be deleted.

8.2   Using device certificates depending on protocol

Configure settings to use device certificates depending on protocol.

This machine enables you to use multiple registered device certificates depending on protocols. Configure settings to fit your environment.

Reference

●   This function is available only when a **Hard Disk** is installed.

You can specify the device certificate to be used for each of the following protocols in this machine.

Protocol1	Protocol2	Description
[SSL]	[http Server]	If this machine is used as an http server • If the client accesses **PageScope Web Connection** via HTTPS, it is used to encrypt communication from the client to this machine. • If the client prints data via IPPS, it is used to encrypt communication from the client to this machine.
[SSL]	[E-Mail Transmission (SMTP)]	If this machine is used as an SMTP client • This machine submits a device certificate upon request from the SMTP server.
[SSL]	[E-mail RX (POP)]	If this machine is used as a POP client • This machine submits a device certificate upon request from the POP server.
[SSL]	[TCP Socket]	If this machine is used as a TCP Socket client • This machine submits a device certificate upon request from the TCP Socket server.
[SSL]	[LDAP]	If this machine is used as an LDAP client • This machine submits a device certificate upon request from the LDAP server.
[SSL]	[WebDAV Client]	If this machine is used as a WebDAV client • This machine submits a device certificate upon request from the WebDAV server.
[SSL]	[OpenAPI]	If this machine is used as an OpenAPI server • If the OpenAPI client accesses this machine via SSL, it is used to encrypt communication from the client to this machine.
[SSL]	[Web Service]	If this machine is used as a Web service server • If Windows Vista or 7 accesses this machine via HTTPS, it is used to encrypt communication from Vista or 7 to this machine.
[IEEE802.1X]		If this machine is used as an IEEE802.1X authentication client • If this machine is authenticated by the IEEE802.1X server via EAP-TLS, it is used to encrypt communication. • This machine submits a device certificate upon request from the server via EAP-TTLS or EAP-PEAP.
[S/MIME]		This machine attaches a device certificate when sending an S/MIME E-mail message.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
        [Device Certificate Setting]
                    |
          [Protocol Setting]
                    |
               Finish
```
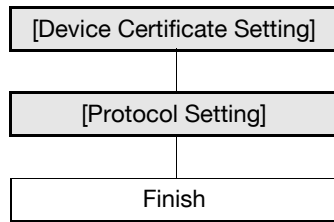
📖 **Reference**

When not using device certificates depending on protocols, specify the device certificate shown in [Default] of [Device Certificate Setting]. For details, refer to page 8-2.

8.2.1   [Device Certificate Setting]

Register a device certificate.

For details, refer to page 8-2.

8.2.2   [Protocol Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [PKI Settings] ▶▶ [Protocol Setting].

Reference
● The function that uses device certificates depending on protocols is not available when a device certificate is not registered or is only in the certificate signing request state.

Item	Description	Prior check
[Protocol 1]/[Protocol 2]	Displays the classification for each protocol. If the target device certificate is registered, the protocol is marked by "*".	
[Create]	Select the protocol to specify a device certificate, and click [Create]. The device certificate registration page appears, and you can specify the target device certificate. If the device certificate is already registered, [Edit] appears. Clicking [Edit] enables you to change the target device certificate or confirm the details of a device certificate.	
[Delete]	If the target device certificate is registered, click this button to delete the registered information.	

8.3   Managing a device certificate

To manage a device certificate, use **PageScope Web Connection** to export it.

Obtaining a device certificate enables you to send an encrypted E-mail from the user to this machine using the obtained certificate (public key).

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
        [Device Certificate Setting]
                   │
          [Export Certificate]
                   │
                Finish
```
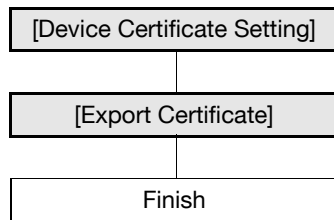
📖 **Reference**
The user can also obtain a device certificate by receiving an E-mail with a digital signature from this machine. For details on how to send an E-mail with a digital signature, refer to page 4-20.

8.3.1   [Device Certificate Setting]

Register a device certificate.

For details, refer to page 8-2.

8.3.2   [Export Certificate]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [PKI Settings] ▶▶ [Device Certificate Setting] ▶▶ [Setting] ▶▶ [Export Certificate].

Item	Description	Prior check
[Password]	Enter the password (up to 32 characters). The entered password is required when importing a certificate.	
[Retype Password]	Reenter the password for confirmation (up to 32 characters).	
[OK]	Click this button to move to the Download page.	

Clicking [Download] downloads a certificate in your computer.

Preparation for download has been completed. Click the "Download" button to start the save. When the save is completed, click the "Back" button.

[Download] [Back]
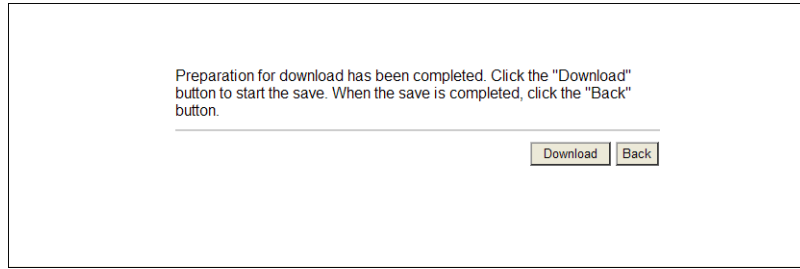
8.4   Registering a user certificate in this machine

Register a user certificate in this machine.

There are two methods of registering a certificate: (1) directly specifying a certificate when registering an E-mail address and (2) automatically registering a certificate by sending an E-mail with a digital signature to this machine.

Registering a user certificate in this machine enables you to send an encrypted E-mail from this machine to the user using the registered certificate (public key).

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.
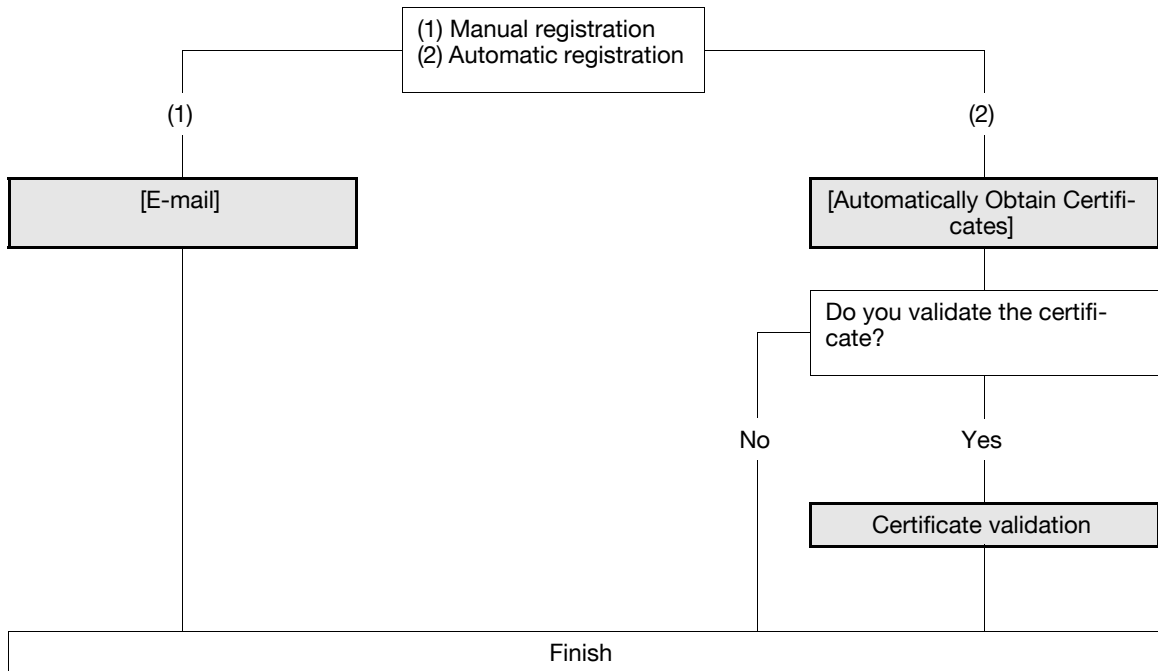
Reference
- [Automatically Obtain Certificates] is available only when a **Hard Disk** is installed.

8.4.1 [E-mail]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▸▸ [Address Book] ▸▸ [Store Address] ▸▸ [New Registration] ▸▸ [E-mail].

Item	Description	Prior check
[Registration of Certification Information]	Select the [Registration of Certification Information] check box. Click [Browse], and specify where to save the certificate information to be registered. Certificate information is supported only as a DER (Distinguished Encoding Rules) file. Clicking [Deletion of Certification Information] deletes the registered certificate information. You cannot register a certificate if the E-mail address to be registered as a destination does not match that of the user certificate. Before registering a certificate, check that those E-mail addresses are the same.	Where to save a certificate

8.4.2 [Automatically Obtain Certificates]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [E-mail Setting] ▶▶ [S/MIME].
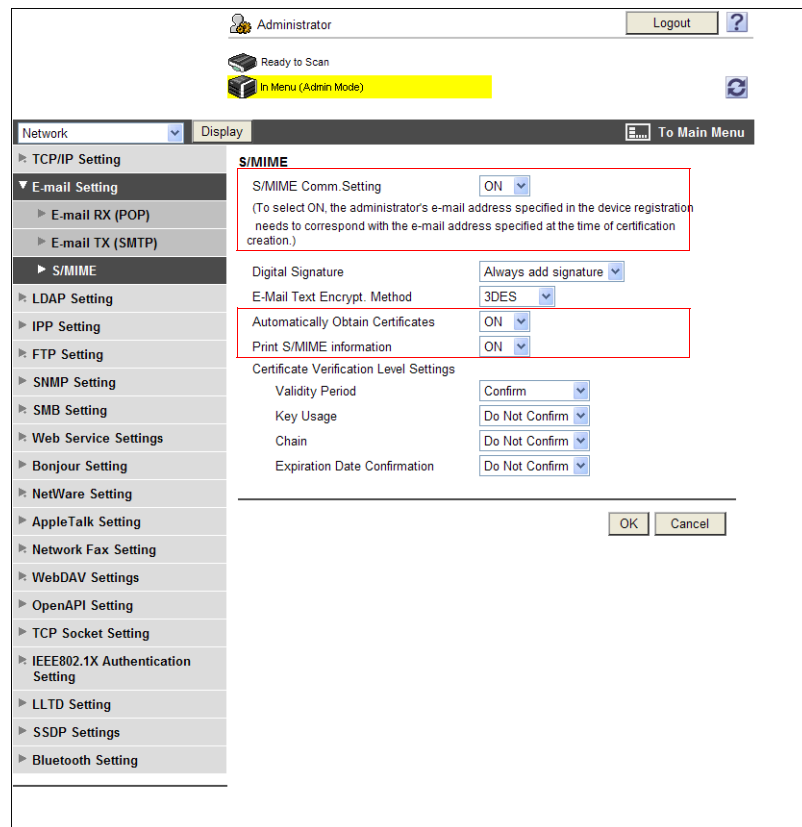
Item	Description	Prior check
[S/MIME Comm. Setting]	Select [ON].	
[Automatically Obtain Certificates]	Select [ON].	
[Print S/MIME Information]	To print S/MIME information, select [ON].	

Reference
● Before you register a certificate, you must register the E-mail address of the user for the certificate with this machine.
● Automatically Obtain Certificates is available only when this machine can receive an E-mail. For details on settings for receiving an E-mail, refer to page 6-9.
● When the conditions above are satisfied, send an E-mail with a digital signature from a computer connected to a network to this machine. The certificate received by this machine is automatically registered when the E-mail address registered in that certificate matches the user's E-mail address registered in this machine.

8.4.3   Certificate validation

[Certificate Verification Level Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [E-mail Setting] ▸▸ [S/MIME].

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the target certificate is within the validity period.	
[Key Usage]	Select whether to check that the certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the target certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ▸▸ [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	

Item	Description	Prior check
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

8.5   Restricting the use of the SMB address registered in the address book

Configure settings to restrict the use of the SMB address registered in the address book.

When the login user selects the required SMB address from the address book to send data, the system performs SMB authentication using the user name and password, which are specified in User Name and Password for user authentication. If the user name and password for user authentication are used for SMB authentication, you do not need to register SMB authentication information in the address book that everyone can access, so you can restrict the use of the SMB address by other people.

To use this function, do not enter any characters in [User ID] and [Password] of the SMB address.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    [TCP/IP Settings]

                    User Authentication

                 [Scan to Authorized Fold-
                      er Settings]

                    [Client Setting]

                    IPv6 environment?
       No                                      Yes

  Do you use the WINS server?            [Direct Hosting Setting]

       Yes              No

   [WINS Setting]

                    Do you send data to Win-
                    dows Vista/Server
                    2008/7?

          No              Yes

                    [LLMNR Setting]

                        Finish
```
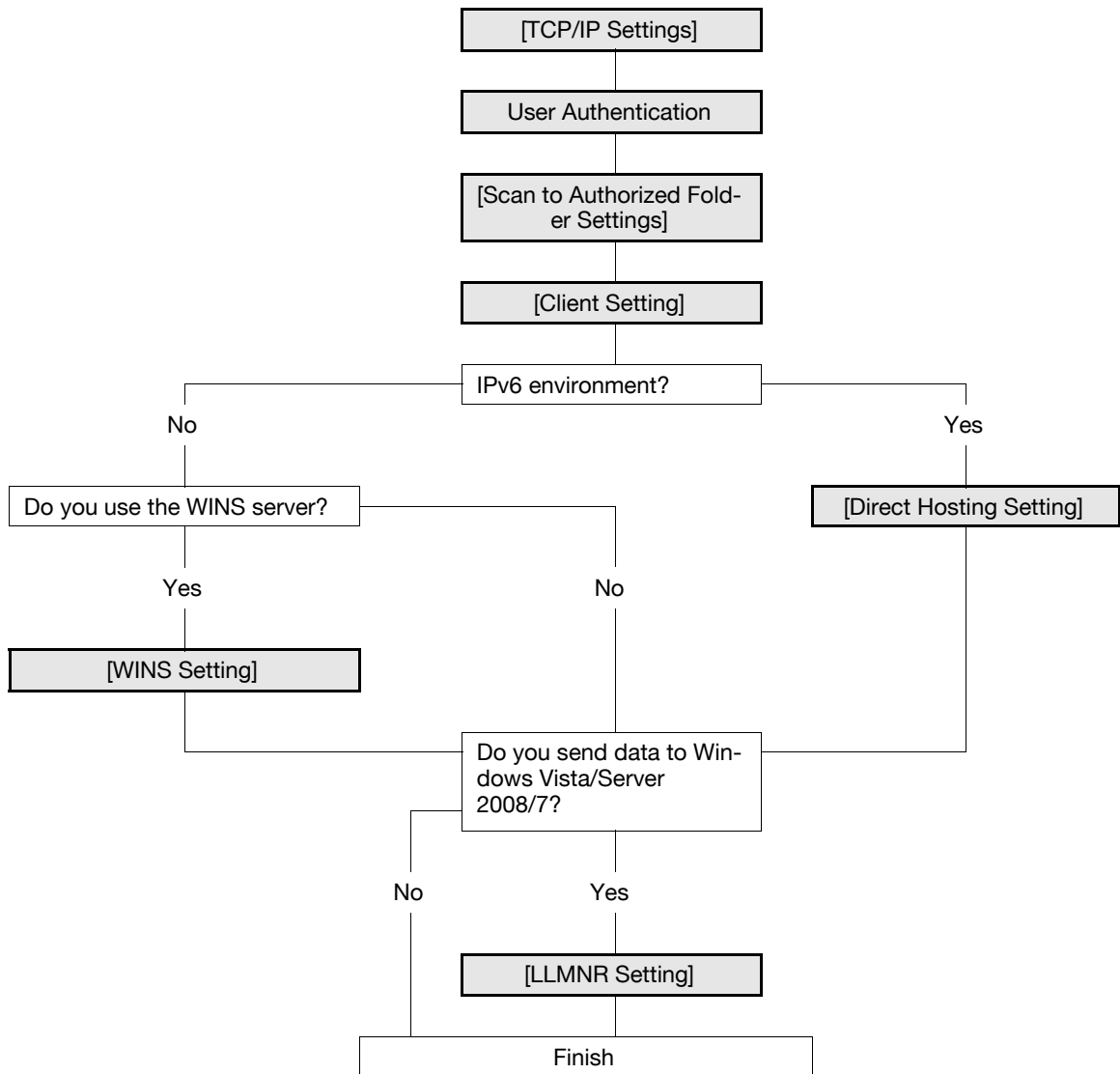
📖 **Reference**
If [Scan to Authorized Folder Settings] is set to [ON], you cannot use some functions. For details, refer to page 8-42.

For details on how to register the SMB address, refer to page 11-7.

8.5.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

●   To specify the destination computer with the computer name (host name) for SMB transmission in IPv6 environment, prepare a DNS server and configure DNS settings in this machine.

For details, refer to page 2-2.

8.5.2   User Authentication

Configure settings to restrict users who use this machine.

For details, refer to the following reference pages.

●   "Restricting users of this machine (MFP authentication)" (p. 7-2)
●   "Restricting users of this machine (Active Directory)" (p. 7-10)
●   "Restricting users of this machine (Windows domain or workgroup)" (p. 7-15)
●   "Restricting users of this machine (NDS over TCP/IP)" (p. 7-22)
●   "Restricting users of this machine (LDAP)" (p. 7-25)

8.5.3   [Scan to Authorized Folder Settings]

Configure settings to restrict the specification of addresses that users directly enter.

For details, refer to page 8-42.

8.5.4   [Client Setting]

Configure SMB client settings.

For details, refer to page 4-3.

8.5.5   [WINS Setting]

To perform SMB transmission via routers, configure the WINS server settings.

For details, refer to page 4-4.

8.5.6   [Direct Hosting Setting]

To perform SMB transmission in an IPv6 environment, enable the Direct Hosting service.

For details, refer to page 4-5.

8.5.7   [LLMNR Setting]

To perform name resolution in the environment configured to communicate with Windows Vista/Server 2008/7, and where the DNS server is not running, enable the LLMNR function.

For details, refer to page 4-5.

8.6   Using Web services to secure communication from Vista/Server 2008/7 to this machine via SSL

Configure settings to use the encrypted SSL communication from a computer running on the Windows Vista/Server 2008/7 to this machine in a Web services environment. Security of Web services communication can be enhanced using the SSL protocol encryption.

When you configure the SSL communication settings, check the following points.

- To use the encrypted SSL communication between this machine and the computer, you must set the bidirectional SSL communication between them. For details on configuring settings to establish an SSL communication from this machine to Windows Vista/Server 2008/7, refer to page 8-21.
- Your computer must be able to resolve the name of this machine using the DNS. Register this machine in the DNS server and configure the DNS settings in your computer in advance.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the device certificate in [Trusted Root Certification Authorities] of the local computer.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
            ┌─────────────────────────┐
            │     [TCP/IP Settings]    │
            └─────────────────────────┘
                         │
            ┌─────────────────────────┐
            │ [Device Certificate Setting] │
            └─────────────────────────┘
                         │
            ┌─────────────────────────┐
            │ [Web Service Common Set- │
            │          tings]          │
            └─────────────────────────┘
                         │
            ┌─────────────────────────┐
            │          Finish          │
            └─────────────────────────┘
```
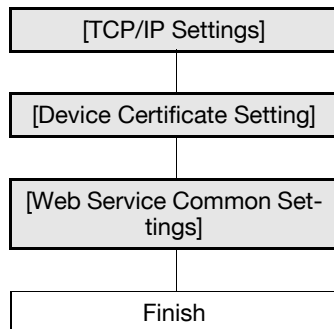
8.6.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

8.6.2   [Device Certificate Setting]

Configure settings for SSL communication.

For details, refer to page 8-2.

8.6.3   [Web Service Common Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Web Service Settings] ►► [Web Service Common Settings].

Item	Description	Prior check
[Friendly Name]	Enter a Friendly Name (up to 62 characters).	
[SSL Setting]	Select [ON].	
[Publication Service]	If you use this machine in an environment where NetBIOS is disabled or only the IPv6 protocol communication is used by the Windows Vista/Server 2008/7 system, set this item to [Enable].	

8.7   Using Web services to establish an SSL communication from this machine to Vista/Server 2008/7

Configure settings to use the encrypted SSL communication from this machine to a computer running on the Windows Vista/Server 2008/7 in a Web services environment. Security of Web services communication can be enhanced using the SSL protocol encryption.

When you configure the SSL communication settings, check the following points.

- To use the encrypted SSL communication between this machine and the computer, you must set the bidirectional SSL communication between them. For details on configuring settings to establish an SSL communication from Windows Vista/Server 2008/7 to this machine, refer to page 8-20.
- Create a certificate at the computer first, and then associate the TCP/IP communication port (the default port number is 5358).

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
        ┌─────────────────────┐
        │   [TCP/IP Settings]  │
        └──────────┬──────────┘
                   │
        ┌──────────┴──────────┐
        │ [Web Service Common │
        │      Settings]      │
        └──────────┬──────────┘
                   │
        ┌──────────┴──────────┐
        │       Finish        │
        └─────────────────────┘
```
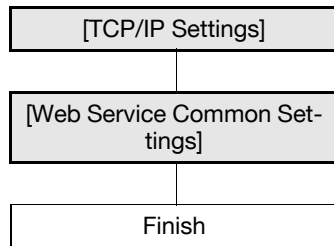
8.7.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

8.7.2   [Web Service Common Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [Web Service Settings] ►► [Web Service Common Settings].

Item	Description	Prior check
[Friendly Name]	Enter a Friendly Name (up to 62 characters).	
[SSL Setting]	Select [ON].	
[Publication Service]	If you use this machine in an environment where NetBIOS is disabled or only the IPv6 protocol communication is used by the Windows Vista/Server 2008/7 system, set this item to [Enable]. The Publication Service function can detect up to 512 destinations, including those detected with the NetBIOS service.	
[Certificate Verification Level Settings]	To verify the certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the target certificate is within the validity period.	
[Key Usage]	Select whether to check that the certificate is used according to the purpose approved by the issuer.	
[Chain]	Select whether to check that the certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the target certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

8.8 Filtering IP addresses

Configure settings to enable IP address filtering.

With IP address filtering, you can restrict access from the specified IP addresses. You can specify both IP addresses that are allowed to access this machine and IP addresses that are not allowed to access this machine.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
┌─────────────────────────┐
│    [TCP/IP Settings]    │
└─────────────────────────┘
             │
┌─────────────────────────┐
│     [IP Filtering]      │
└─────────────────────────┘
             │
┌─────────────────────────┐
│         Finish          │
└─────────────────────────┘
```
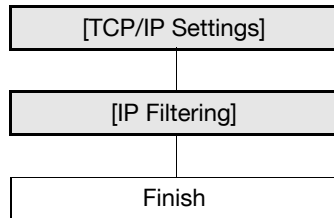
Reference
- IP address filtering is not supported in the IPv6 environment.

8.8.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

8.8.2 [IP Filtering]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [TCP/IP Settings] ▶▶ [IP Filtering].

Item	Description	Prior check
[Permit Access]	To specify addresses you permit access from, select [Enable].	

Item	Description	Prior check
[Set 1] to [Set 5]	Enter the start and end addresses of ranges you permit access from. Format: *.*.*.* (Asterisk * can be 0 to 255)	Address ranges that you permit access from
[Deny Access]	To specify addresses you deny access from, select [Enable].	
[Set 1] to [Set 5]	Specify the start and end addresses of ranges you deny access from. Format: *.*.*.* (Asterisk * can be 0 to 255)	Address ranges that you deny access from

8.9   Communicating using IPsec

Configure settings for IPsec communication.

The IPsec-based communication can prevent a data falsification and reveal of each IP packet. The communication can be secured even if you use the transport and application layers that do not support encryption.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
┌─────────────────────────┐
│     [TCP/IP Settings]    │
└─────────────────────────┘
              │
┌─────────────────────────┐
│         [IPsec]          │
└─────────────────────────┘
              │
┌─────────────────────────┐
│          [IKE]           │
└─────────────────────────┘
              │
┌─────────────────────────┐
│          [SA]            │
└─────────────────────────┘
              │
┌─────────────────────────┐
│         [Peer]           │
└─────────────────────────┘
              │
┌─────────────────────────┐
│         Finish           │
└─────────────────────────┘
```
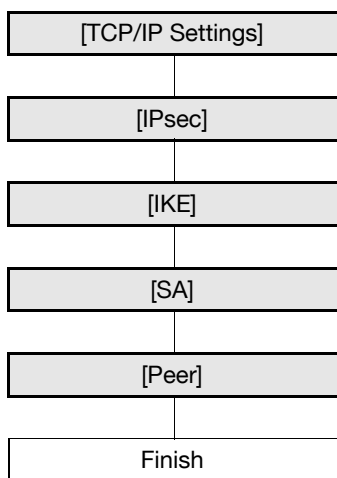
8.9.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

8.9.2 [IPsec]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting]▸▸ [IPsec].

Item	Description	Prior check
[IPsec]	Select [ON].	

8.9.3 [IKE]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [IPsec].

Item	Description	Prior check
[Key Validity Period]	Enter a validation period of the common key that is used for encrypted communication. When this period has expired, a new key is created. This can secure the communication.	
[Diffie-Hellman Group]	Select the Diffie-Hellman group.	

[IKE Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [IPsec] ▸▸ [IKE] ▸▸ [Edit].

(Up to four groups can be registered for the IKE.)

Item	Description	Prior check
[Encryption Algorithm]	Select an encryption algorithm to be used for creation of the common key.	
[Authentication Algorithm]	Select an authentication algorithm to be used for creation of the common key.	

8.9.4   [SA]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [IPsec].

Item	Description	Prior check
[Lifetime After Establishing SA]	Enter a validation period of the common key that is used for encrypted communication. When this period has expired, a new key is created. This can secure the communication.	

[SA Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [IPsec] ▸▸ [SA] ▸▸ [Edit].

(Up to eight groups can be registered for the SA.)

Item	Description	Prior check
[Security Protocol]	Select a security protocol to use.	
[ESP Encryption Algorithm]	If you have set the Security Protocol to [ESP], select the ESP encryption algorithm.	
[ESP Authentication Algorithm]	If you have set the Security Protocol to [ESP], select the ESP authentication algorithm.	
[AH Authentication Algorithm]	If you have set the Security Protocol to [AH], select the AH authentication algorithm.	

8.9.5 [Peer]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [TCP/IP Setting] ▸▸ [IPsec] ▸▸ [Peer] ▸▸ [Edit].

(Up to 10 peers can be registered.)

Item	Description	Prior check
[Perfect Forward Secrecy]	To increase the IKE security level, select [ON]. If you have selected [ON], the communication time increases.	
[Peer]	Enter the IP address of the peer. When using IPv6, you can specify the IPv6 address.	IP address of the peer
[Pre-Shared Key Text]	Enter the Pre-Shared Key text to be shared with the peer (up to 64 characters). This text must be the same as that used at the peer.	
[Encapsulation Mode]	Select an IPsec operation mode.	

8.10   Using IEEE802.1X authentication

If you use this machine in a wired LAN environment having the IEEE802.1x authentication system, you must configure the supplicant (authentication client) function of this machine.

Using IEEE802.1x authentication can restrict any device not permitted by the administrator to connect to this LAN environment. Configure settings to fit your environment.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

[TCP/IP Settings]

[Device Certificate Setting]

[IEEE802.1x Authentication Setting]

Certificate validation

[IEEE802.1X Authentication Trial]

Finish
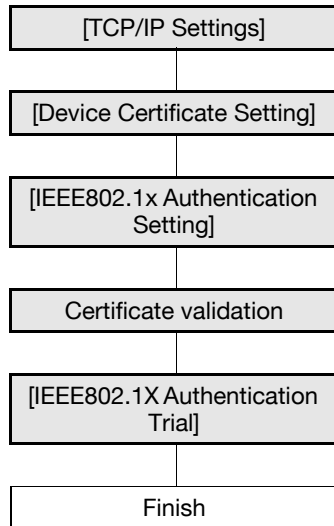
8.10.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

8.10.2   [Device Certificate Setting]

Register the client certificate (device certificate) on this machine, based on the EAP authentication method to be used.
- If [EAP-Type] is [EAP-TLS], you must register the device certificate.
- If [EAP-Type] is [EAP-TTLS] or [PEAP], you may be required to register the device certificate according to your applications.

For details on device certificate registration, refer to page 8-2.

8.10.3   [IEEE802.1x Authentication Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [IEEE802.1x Authentication Setting] ►► [IEEE802.1x Authentication Setting].

Item	Description	Prior check
[Authentication Status]	The authentication status is shown as follows. • [Authenticated]: The authentication has completed. • [Authenticating]: The authentication is in progress. • [Unauthenticated]: Not authenticated status. • [Authentication Failed]: The authentication has failed. • [Failed to Retrieve Status]: No authentication status could be obtained. When you press [Refresh], the authentication status is updated.	
[IEEE802.1x Authentication Setting]	Select [ON].	
[Supplicant Setting]	Configure settings required in order for this machine, which is a supplicant (authentication client), to receive authentication from the authentication server. Configure settings to fit your environment.	
[User ID]	Enter a user ID (up to 128 characters). This user ID is used for all EAP-Type options.	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password (up to 128 characters). The password is used for all EAP-Type options other than [EAP-TLS].	

Item	Description	Prior check
[EAP-Type]	Select an EAP authentication method. If you select [Depend on Server], the EAP-Type provided by the authentication server will be used for authentication. Configure the supplicant settings as required for this machine according to the EAP-Type provided by the authentication server. Do not set this item to [OFF].	EAP authentication method
[EAP-TTLS]	Configure settings for EAP-TTLS.	
[anonymous]	Enter an anonymous name to be used for EAP-TTLS authentication (up to 128 characters). This item is available if [EAP-Type] is set to [EAP-TTLS] or [Depend on Server].	
[Inner Authentication Protocol]	Select an EAP-TTLS inner authentication protocol. This item is available if [EAP-Type] is set to [EAP-TTLS] or [Depend on Server].	
[Server ID]	Enter a server ID (up to 64 characters). This setting is required if you verify the CN of the server certificate.	Whether to verify the CN of the server certificate
[Client Certificate]	Select whether to encrypt authentication information using client certificates of this machine. You can configure this setting when client certificates are registered in this machine. If [EAP-Type] is [EAP-TLS], the client certificates are always required. This setting can be configured even if [EAP-Type] is set to [EAP-TTLS] or [PEAP].	
[Encryption Strength]	Select an encryption strength level for encrypted communication with TLS. • [Low]: Keys of any length are used for communication. • [Mid]: Keys that are more than 56 bits in length are used for communication. • [High]: Keys that are more than 128 bits in length are used for communication. This item is available if [EAP-Type] is set to anything other than [OFF] or [EAP-MD5].	
[Network Stop Time]	If an authentication process does not succeed within the specified time, all network communication will stop. To specify the delay between the start of an authentication process and the stop of network communication, select this box.	
[Stop Time]	Specify the delay (sec.) between the start of an authentication process and the stop of network communication. To restart the authentication process after network communication has stopped, turn the main power of this machine off and on again.	

8.10.4   Certificate validation

[IEEE802.1x Authentication Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [IEEE802.1x Authentication Setting] ▸▸ [IEEE802.1x Authentication Setting].

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	

Item	Description	Prior check
[CN]	Select whether to check that the CN of the server certificate matches the server address. To check the CN, specify [Server ID].	
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	

8.10.5   [IEEE802.1X Authentication Trial]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [IEEE802.1x Authentication Setting] ►► [IEEE802.1X Authentication Trial].

Item	Description	Prior check
[Authentication Status]	The authentication status is shown as follows. • [Authenticated]: The authentication has completed. • [Authenticating]: The authentication is in progress. • [Unauthenticated]: Not authenticated status. • [Authentication Failed]: The authentication has failed. • [Failed to Retrieve Status]: No authentication status could be obtained. When you press [Refresh], the authentication status is updated.	
[Authentication Trial]	Click this button to attempt authentication immediately.	

8.11   Managing external certificates

You can manage external certificates from this machine.

Root certificates or interim certificate issued by a trusted Certification Authority (CA), certificates issued by a trusted End Entity (EE), or distrusted certificates can be registered with this machine for management. The registered external certificates are referenced during chain validation of a certificate, when making sure that its certificate path has no problems.

[External Certificate Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [PKI Settings] ►► [External Certificate Setting].
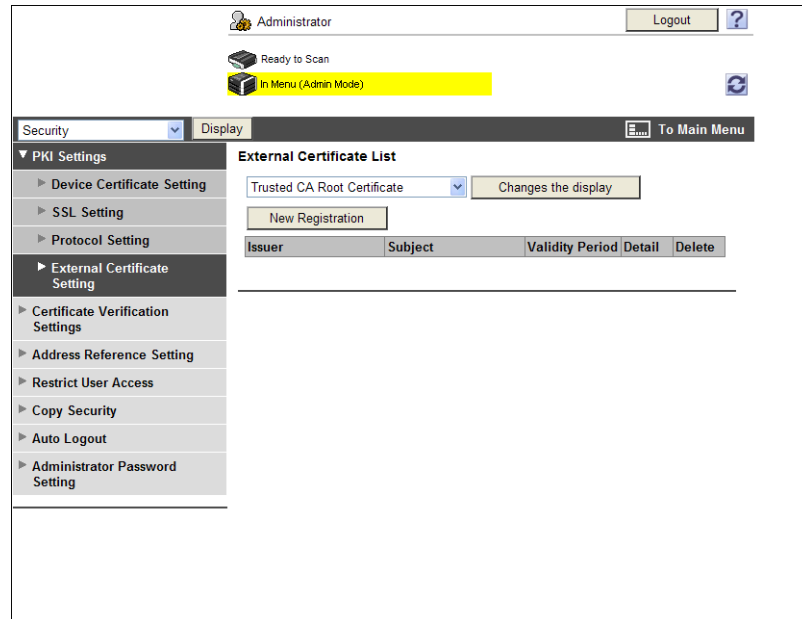
Item	Description
Certificate type	Select the type of an external certificate you want to display, and click [Change the display]. Then external certificates of the selected type are displayed in the list.
[New Registration]	Click this button to register a new external certificate. Click [Browse] in the new registration window to specify a new external certificate to be registered.
[Issuer]	Displays the issuer of an external certificate.
[Subject]	Displays the destination of an external certificate.
[Validity Period]	Displays the validity period of an external certificate.
[Detail]	Check detailed information about an external certificate.
[Delete]	Displays a message asking you to confirm deletion, enables you to delete an external certificate.

Reference
- If a **Hard Disk** is not installed, you cannot select certificate type. Certificates can be registered only with [Trusted CA Root Certificate].

[New Registration]

Item	Description
[File]	Click [Browse] to specify a new external certificate to be registered. • If [Trusted CA Root Certificate] is selected, register the route certificate of the trusted CA (certificate authority). • If [Trusted CA Intermediate Certificate] is selected, register the interim certificate of the trusted CA (certificate authority). • If [Trusted EE (End Entity) Certificate] is selected, individually register the trusted certificates. • If [Non-Trusted Certificate] is selected, individually register the untrusted certificates.

Reference

Type	Description
[Trusted CA Root Certificate]	You must import the certificate of the CA that issued the certificate in question in this machine in advance, if you wish to validate the chain of a submitted certificate.
[Trusted CA Intermediate Certificate]	You must import the certificate of the intermediate certificate authority in this machine in advance, if the submitted certificate is issued by an intermediate certificate authority. You must also import the root certificate of the CA, which certifies the intermediate certificate authority, in this machine in advance.
[Trusted EE (End Entity) Certificate]	Trusted EE refers to the certificate to be submitted. By importing a certificate in this machine in advance, the certificate will be identified as a trusted certificate when it is submitted. If a certificate is registered as the trusted EE certificate in advance, this machine will skip validation of the certificate chain when it is submitted and will recognize it as a trusted certificate.
[Non-Trusted Certificate]	Register non-trusted certificates in this machine.

8.12   Limiting accessible destinations for each user

Register and edit reference allowed groups.

When you register a user with this machine, add the user to a reference allowed group. In addition, when you add a destination to the address book, grant reference access permission only to the reference allowed group you add the user to. This limits the accessible destinations for each user.

You can also specify the access allowed level of each reference allowed group. Even a user who does not belong to a group permitted to reference a destination can still reference the destination if the access allowed level of the user is higher than or equal to that of the group permitted to reference the destination.

📖 **Reference**
For details on the registration of users, refer to page 7-6.

For details on the registration of destinations with the address book, refer to page 11-7.

[Address Reference Setting]

In the administrator mode of **PageScope Web Connection**, select [Security]▶▶[Address Reference Setting]▶▶[Edit].

Item	Description
[No.]	Displays the registration number.
[Reference Allowed Group Name]	Enter the name of the reference allowed group (up to 24 characters).
[Access Allowed Level]	Specify the access allowed level of the reference allowed group.

8.13   Restricting Registration and Change by a User

You can restrict the registering of addresses or biometric/IC card information and the changing of the From address by general users.

[Restrict User Access]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Restrict User Access].

Item	Description
[Registering and Changing Addresses]	Select [Restrict] to restrict registering and changing addresses by users.
[Biometric/IC Card Information Registration]	Select [Restrict] to restrict registering biometric/IC card information by users.
[Changing the "From" Address]	To restrict changing the From address by users when sending an E-mail from this machine, select [Admin. E-mail Address] or [Login User Address]. If [Admin. E-mail Address] is selected, the administrator's E-mail address is set as the From address of the E-mail to be sent from this machine. If [Login User Address] is selected, the user's E-mail address is set as the From address when it is registered. However, when the user's E-mail address is not registered or S/MIME is used to send an E-mail, the administrator's E-mail address is set as the From address. If [Allow] is selected, the user can change the From address before sending an E-mail.

Reference
- If [Enhanced Security Mode] is enabled, [Registering and Changing Addresses] is set to [Restrict].
- [Biometric/IC Card Information Registration] is available when the optional authentication unit is installed in this machine.
- If user authentication is enabled, the default of [Changing the "From" Address] is set to [Login User Address].

8.14   Setting copy security

Configure settings to use the copy guard and password copy functions.

Using the copy guard function enables you to print a copy guard (text with copy inhibit information embedded) on a document. If an attempt is made to copy a document with a copy guard printed, a warning message is displayed to disable copying.

Using the password copy function enables you to embed a password in a document. If an attempt is made to copy a document with a password embedded, the system will prompt you to enter the password. Copying cannot be performed unless the correct password is entered.

Reference
- To use the copy guard and password copy functions, install the optional **Security Kit SC-507** in this machine.
- For details on the copy guard and password copy functions, refer to the [User's Guide Copy Operations].

[Copy Security]

In the administrator mode of **PageScope Web Connection**, select [Security]▶▶[Copy Security].

(If the optional **Security Kit SC-507** is not installed, this menu item will not be displayed.)
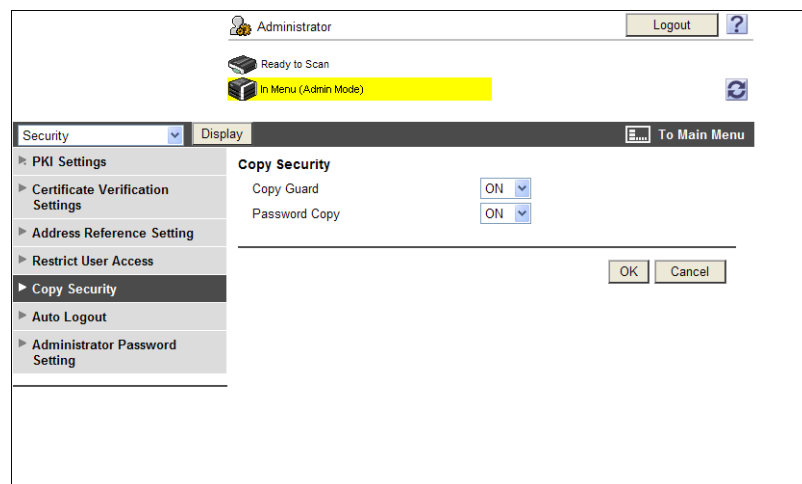
Item	Description
[Copy Guard]	Select [ON] to use the copy guard function.
[Password Copy]	Select [ON] to use the password copy function.

8.15   Configuring the administrator password

Configure the administrator password of this machine.

[Administrator Password Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Administrator Password Setting].

Reference
- If [Enhanced Security Mode] is enabled, this menu item will not be displayed.
- If a device certificate has not been registered, this menu item will not be displayed .
- This menu does not appear if [Mode using SSL/TLS] is set to [None] in [Security] ►► [PKI Settings] ►► [SSL Setting], when a device certificate is already registered.
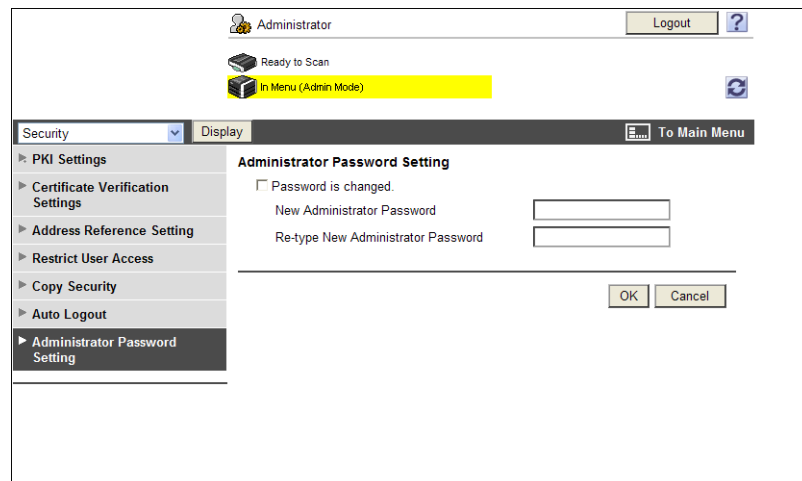
Item	Description
[Password is changed.]	Select this check box to change the password.
[New Administrator Password]	Enter a new administrator password (up to 8 characters, excluding space and ").
[Re-type New Administrator Password]	Enter the new administrator password again for confirmation.

Reference
- You cannot register a password less than eight characters when [Security Settings]►►[Security Details]►►[Password Rules] is set to [Enable] in the [Administrator Settings] on the **Control Panel**. If a user password containing less than eight characters has already been registered, change the password so that it contains eight characters before setting [Password Rules] to [Enable].

8.16   Configuring the function permission of the public user

Configure the function permission and reference permission of the public users.

[Public User]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▶▶ [User Authentication Setting] ▶▶ [Public User].

(This menu item will not be displayed if the public user access is not permitted.)

Item	Description
[Function Permission]	Specify function permissions. Specify whether to permit [Copy], [Scan], [Save to External Memory], [External Memory Document Scan], [Fax], [Print], [User Box], [Print Scan/Fax TX], [Manual Destination Input], and [Mobile/PDA]. If all operations are disabled, no user will not be able to log in to this machine as the public user.
[Output Permission(TX)]	Configure settings to restrict the transmission functions. You can also specify whether to permit the transmission of color images.
[Limiting Access to Destinations]	Restrict address book entries that the public user can reference. To add the public user to a reference allowed group, select the check box and click [Search from List]. From the displayed list, select the reference allowed group to which the public user is added. You can select one or more reference allowed groups. To specify the access allowed level, select the check box and specify the access allowed level.

Reference

- Whether to allow the [Save to External Memory] function can be specified when [Save Document] is set to [ON] in [System Settings]▸▸[User Box Settings]▸▸[External Memory Function Settings]. Whether to allow the [External Memory Document Scan] function can be specified when [USB to User Box] is set to [ON] in [External Memory Function Settings]. For details, refer to page 12-7.
- When [Security Settings]▸▸[Security Details]▸▸[Manual Destination Input] is set to [Restrict] in [Administrator Settings] on the control panel, the user cannot manually enter the address regardless of the setting of this function.
- To connect this machine to a cellular phone or PDA, install the optional **Local Interface Kit EK-605** in this machine. Whether to allow the [Mobile/PDA] function can be specified when [Bluetooth] is set to [Enable] in [Network]▸▸[Bluetooth Setting] and [Bluetooth Print Settings] is set to [ON] in [System Settings]▸▸[System Connection Setting].
- The following functions are available only when a **Hard Disk** is installed.
 [Save to External Memory] and [External Memory Document Scan] under [Function Permission]

8.17   Restricting Users' Direct Entry of Destinations

You can restrict users' direct entry of destinations.

Enabling this item disables direct entry of destinations except for recipients of faxes or IP address faxes. Therefore users can specify sending destinations only by accessing the address book. Enabling this item also applies the following restrictions.

- Users cannot save documents to User Boxes
- Users cannot transmit documents from User Boxes
- Users cannot use annotation User Boxes
- Users cannot use the image panel
- Users cannot select addresses from the transmission history
- Users cannot use the URL notification function

To restrict direct entry of destinations by users, it is effective to combine following settings depending on your operating environments.

- Restrict address registration by users (p. 8-37).
- If you do not want users to use the LDAP server, do not register the LDAP server.(p. 10-5)
- When you permit the public user access, restrict scanning by the public user.(p. 8-40)
- If you are concerned about retrieval of images from User Boxes, do not grant the User Box operation to users.(p. 12-8)
- If you are concerned about retrieval of images via TCP Socket, disable TCP Socket.(p. 9-2)

📖 Reference

By configuring Scan to Authorized Folder Settings in an environment where user authentication is enabled, you can restrict the access to SMB destinations registered in the address book. For details, refer to page 8-18.

[Scan to Authorized Folder Settings]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ▸▸ [Scan to Authorized Folder Settings].
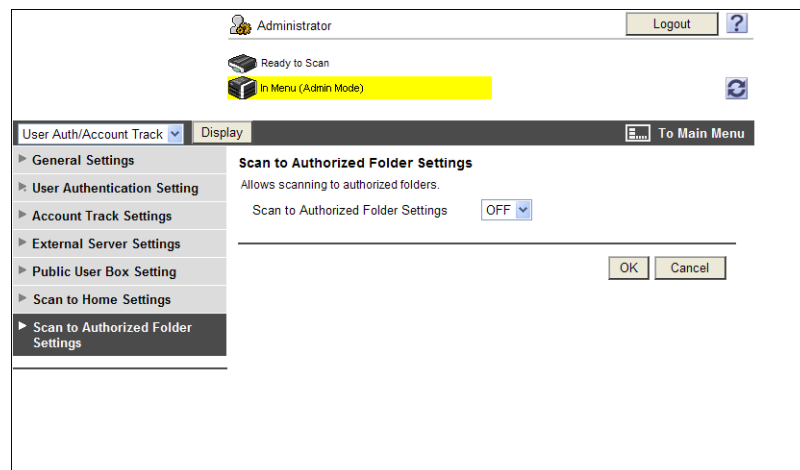
Item	Description
[Scan to Authorized Folder Settings]	To restrict users' direct entry of destinations, select [ON].

9 Cooperating with applications

9   Cooperating with applications

9.1   Using applications that communicate with this machine with TCP Socket

Configure setting for TCP Socket of this machine.

TCP Socket is used for data communication between this machine and application software running on the computer.

If you have registered the device certificate on this machine, you can encrypt TCP Socket communications between the application software and this machine with SSL.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    ┌─────────────────────────┐
                    │     [TCP/IP Settings]    │
                    └─────────────────────────┘
                    ┌─────────────────────────┐
                    │ Do you use SSL communi-  │──────────┐
                    │ cation?                  │          │
                    └─────────────────────────┘          │
                                │                         │
                              Yes                        No
                                │                         │
                    ┌─────────────────────────┐          │
                    │ [Device Certificate Setting] │      │
                    └─────────────────────────┘          │
                    ┌─────────────────────────┐          │
                    │   [TCP Socket Setting]   │──────────┘
                    └─────────────────────────┘
                                │
                    ┌─────────────────────────┐
                    │          Finish          │
                    └─────────────────────────┘
```
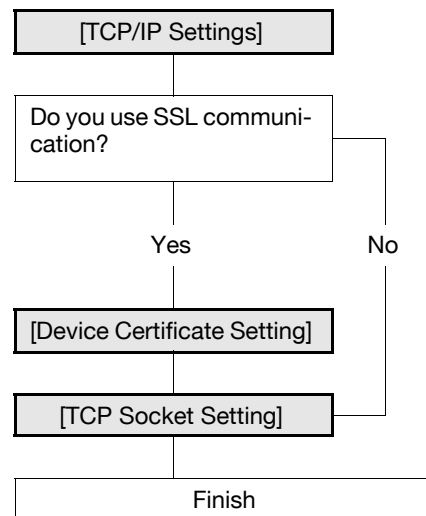
Reference
- If you use **PageScope Authentication Manager** for authentication, configure the TCP Socket setting to use SSL/TLS. (Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)
- If authentication is performed by the external server when using applications that communicate with this machine using TCP Socket, configure the TCP Socket setting to use SSL/TLS.

9.1.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

9.1.2   [Device Certificate Setting]

Configure settings for SSL communication.

For details, refer to page 8-2.

9.1.3   [TCP Socket Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [TCP Socket Setting].

Item	Description	Prior check
[TCP Socket]	Select this check box.	
[Port Number]	Enter a port number.	
[Use SSL/TLS]	To use the SSL/TLS, select the [Use SSL/TLS] check box.	Do you use SSL/TLS?
[Port No.(SSL)]	Enter the port number to be used for SSL communication.	

Reference

● If [Enhanced Security Mode] is enabled, [Use SSL/TLS] is automatically enabled.

● If you select [OK] after changing multiple port numbers together in **PageScope Web Connection** or on the **Control Panel**, a port number duplication error may be displayed. When this error is displayed, first change one port number and select [OK]. Then change another one and select [OK].

9.2 Linking an OpenAPI system with this machine

Configure the OpenAPI settings of this machine.

These settings are required when you want to link an OpenAPI system with this machine.

If you have registered the device certificate on this machine and if you use this machine as a communication server, you can encrypt OpenAPI communications from the client to this machine using SSL. Also, this machine can request the OpenAPI client for a submission of the client certificate. When the client connects to this machine, the submitted client certificate is verified and the client can be authenticated.

When this machine communicates as a client and when the certificate is submitted by the server, this machine can verify the submitted certificate.

If the OpenAPI connection application supports the SSDP function, you can notify the application that the OpenAPI service has started on this machine by using the SSDP function of this machine. If the OpenAPI service is searched by the SSDP function in the application, a response will be returned when this machine satisfies relevant search conditions.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    ┌──────────────────────────┐
                    │     [TCP/IP Settings]     │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │     [SSDP Settings]       │
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │ Do you use SSL communica- │
                    │ tion?                     │──────┐
                    └──────────────────────────┘      │
                                 │                     │
                               Yes                    No
                                 │                     │
                    ┌──────────────────────────┐      │
                    │[Device Certificate Setting]│     │
                    └──────────────────────────┘      │
                                 │                     │
                    ┌──────────────────────────┐      │
                    │     [OpenAPI Setting]     │──────┘
                    └──────────────────────────┘
                                 │
                    ┌──────────────────────────┐
                    │Do you validate the certificate?│──┐
                    └──────────────────────────┘       │
                                 │                      │
                               Yes                     No
                                 │                      │
                    ┌──────────────────────────┐       │
                    │   Certificate validation  │       │
                    └──────────────────────────┘       │
                                 │                      │
                    ┌──────────────────────────┐        
                    │          Finish           │───────┘
                    └──────────────────────────┘
```
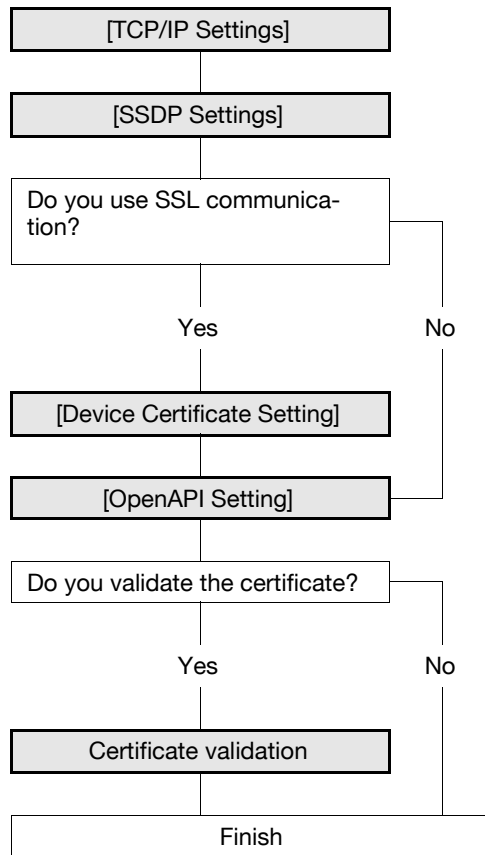
Reference
- If you use **PageScope Authentication Manager** for authentication, configure the OpenAPI setting to use SSL/TLS. (Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)

9.2.1 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

9.2.2 [SSDP Settings]

In the administrator mode of **PageScope Web Connection**, select [Network]▶▶[SSDP Settings].

Item	Description	Prior check
[SSDP]	You can notify the application that the OpenAPI service has started on this machine, if the OpenAPI connection application supports the SSDP function and it is set to [ON]. If the OpenAPI service is searched by the SSDP function in the application, a response will be returned when this machine satisfies relevant search conditions.	Does the application support the SSDP function?
[Multicast TTL Set-ting]	Enter TTL (Time To Live) for SSDP multi-cast packet. The value is decremented by one each time a communication is established via the router. When the value reaches 0, packets are discarded.	

9.2.3 [Device Certificate Setting]

Configure settings for SSL communication.

For details, refer to page 8-2.

9.2.4 [OpenAPI Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [OpenAPI Setting].
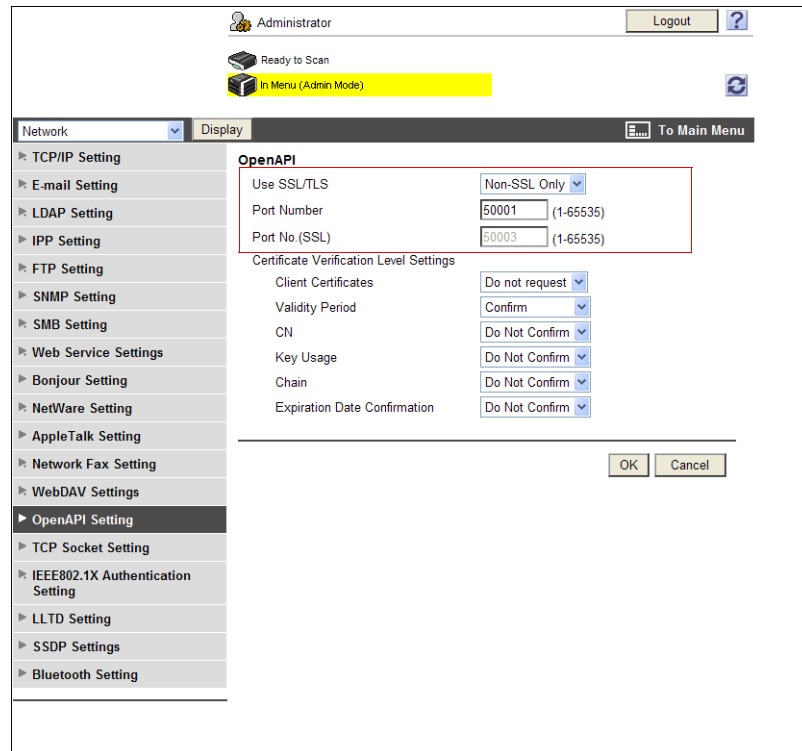
Item	Description	Prior check
[Use SSL/TLS]	To use SSL encryption, select [SSL Only] or [SSL/Non-SSL].	Do you use SSL/TLS?
[Port Number]	Enter a port number.	
[Port No. (SSL)]	Enter the port number to be used for SSL communication.	

Reference

- If [Enhanced Security Mode] is enabled, [Use SSL/TLS] is set to [SSL Only].
- When you use **PageScope Authentication Manager** for authentication from the printer driver, set [System Connection] ►► [OpenAPI Settings] ►► [Authentication] to [OFF] in [Administrator Settings] on the **Control Panel**. (Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)
- If you select [OK] after changing multiple port numbers together in **PageScope Web Connection** or on the **Control Panel**, a port number duplication error may be displayed. When this error is displayed, first change one port number and select [OK]. Then change another one and select [OK].

9.2.5 Certificate validation

[Certificate Verification Level Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [OpenAPI Settings].

Item	Description	Prior check
[Certificate Verification Level Settings]	To verify the certificate, configure settings to verify the certificate.	
[Client Certificate]	Specify whether to request for client certificates. If you authenticate the client by requesting for its certificate (verification of client certificate), select [Request].	Do you request for client certificates?
[Validity Period]	Select whether to check that the target certificate is within the validity period.	
[CN]	Select whether to check that the CN of the certificate matches the server address.	
[Key Usage]	Select whether to check that the certificate key is being used properly.	
[Chain]	Select whether to check that the certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check the target certificate for validation. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ▶▶ [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

9.3   Using the FTP server and WebDAV server functions

Configure settings to use the FTP server and WebDAV server functions of this machine.

These settings are required when you use an application that links with this machine as an FTP client or a WebDAV client.

If you use this machine as the WebDAV server, you can encrypt the communication from the application with SSL for security enhancement.

Use the following flowchart to configure settings.

```
                        ┌─────────────────────┐
                        │   [TCP/IP Settings] │
                        └─────────────────────┘
                        ┌─────────────────────┐
                        │ (1) FTP server      │
                        │ (2) WebDAV server   │
                        └─────────────────────┘
        (1)                                        (2)

┌─────────────────────┐              ┌─────────────────────┐
│ [FTP Server Setting]│              │ Do you use SSL      │
│                     │              │ communication?      │
└─────────────────────┘              └─────────────────────┘
                                       No            Yes

                                          ┌──────────────────────────┐
                                          │ [Device Certificate      │
                                          │  Setting]                │
                                          └──────────────────────────┘
                                          ┌──────────────────────────┐
                                          │ [WebDAV Server Settings] │
                                          └──────────────────────────┘
┌─────────────────────────────────────────────────────────────────────┐
│                               Finish                                  │
└─────────────────────────────────────────────────────────────────────┘
```
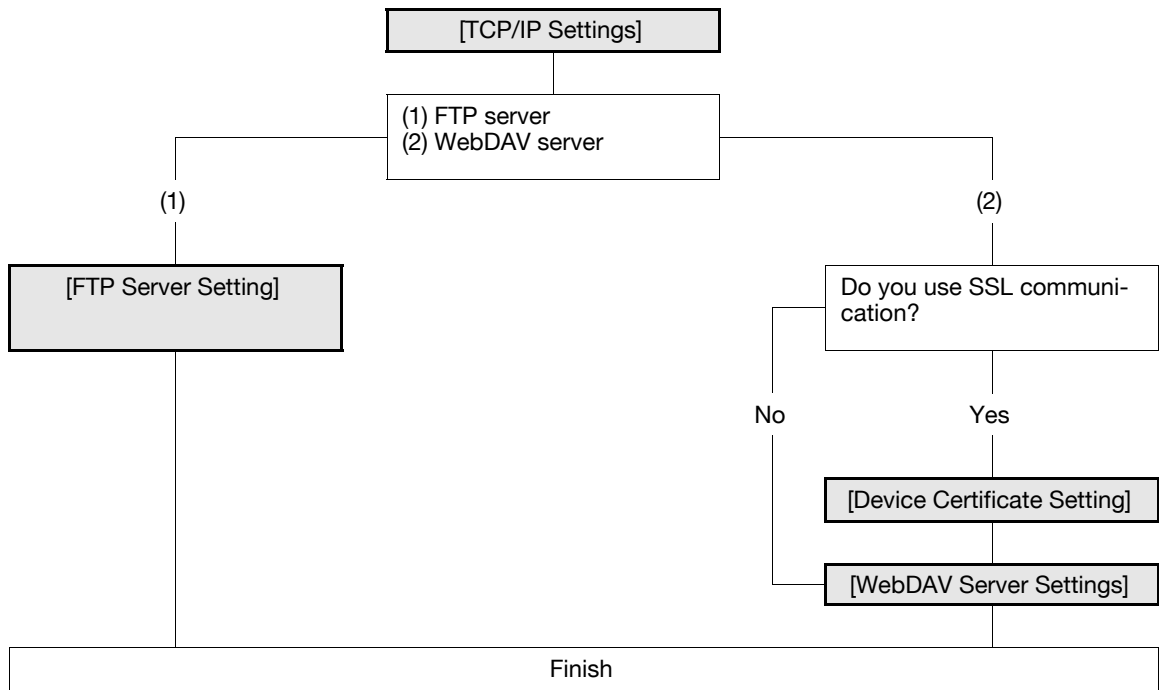
9.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

9.3.2   [Device Certificate Setting]

Configure settings for SSL communication.

For details, refer to page 8-2.

9.3.3 [FTP Server Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▶▶ [FTP Setting] ▶▶ [FTP Server Setting].
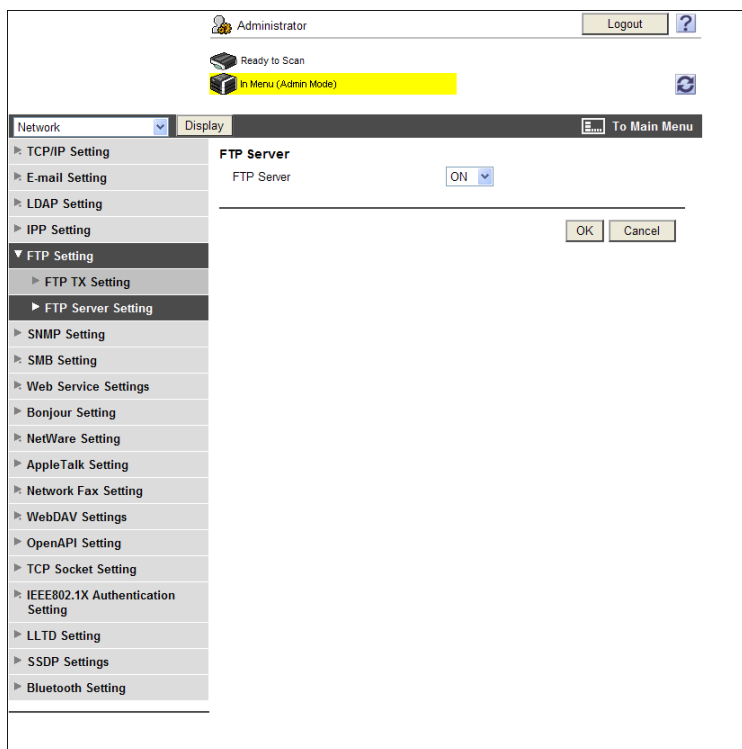
Item	Description	Prior check
[FTP Server]	Select [ON].	

Reference
- If [Enhanced Security Mode] is enabled, this item is set to [OFF].

9.3.4 [WebDAV Server Settings]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [WebDAV Settings] ►► [Web-DAV Server Settings].

Item	Description	Prior check
[WebDAV Settings]	Select [ON].	
[SSL Setting]	To use the SSL/TLS protocol, select [SSL Only] or [SSL/Non-SSL].	Do you use SSL?
[Password is changed.]	Select this check box to change the password.	
[Current Password]	Enter the currently specified password (up to 8 characters). This item is not displayed when the default is not changed.	
[New Password]	Enter the password used to access the WebDAV server (up to 8 characters, excluding space and ").	
[Retype New Password]	Reenter the password for confirmation (up to 8 characters).	
[Initial Password]	To initialize the existing password, click this button. Default setting: sysadm	

Reference
● Before you use the SSL protocol, register the device certificate. For details, refer to page 8-2.

9.4 Canceling the connection with applications

You can cancel the connection from this machine to the server when an error occurs on the server while **Pag-eScope My Panel Manager** is running.

Reference
- This function is available only when a **Hard Disk** is installed.

[System Connection Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings]▸▸[System Connection Setting].
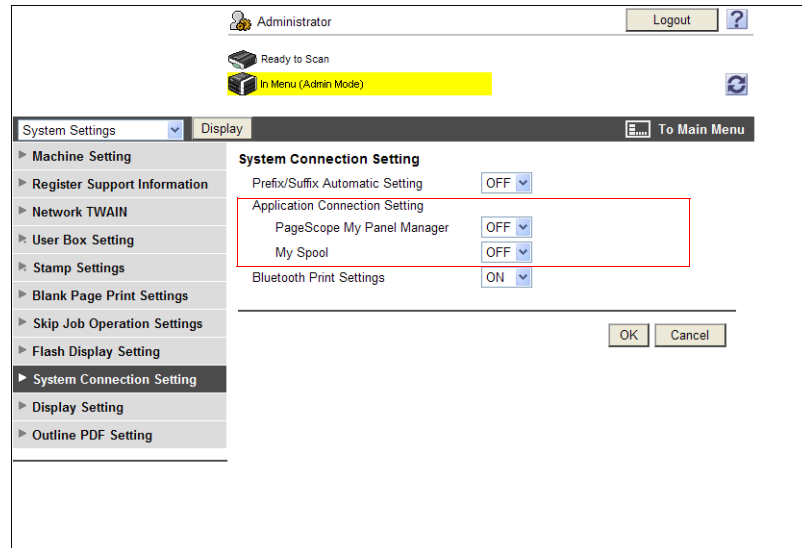
Item	Description
[PageScope My Panel Manager]	Select [OFF] when canceling the connection from this machine to **PageScope My Panel Manager**.
[My Spool]	This item is not available.

10 Managing

10   Managing

10.1   Specifying the date and time of this machine

Specify the date and time of the clock built into this machine.

Select one of two procedures: manually specifying the date and time and obtaining them from the NTP server via the network.

Before using Fax in this machine, specify the date and time of this machine. When connecting this machine to Active Directory, specify the date and time of this machine as required.

Specify the date and time of this machine when using this machine for the following purposes. For details, refer to the relevant reference page.

- "Searching for the E-mail address in the LDAP server" (p. 10-5)
- "Restricting users of this machine (Active Directory)" (p. 7-10)

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.
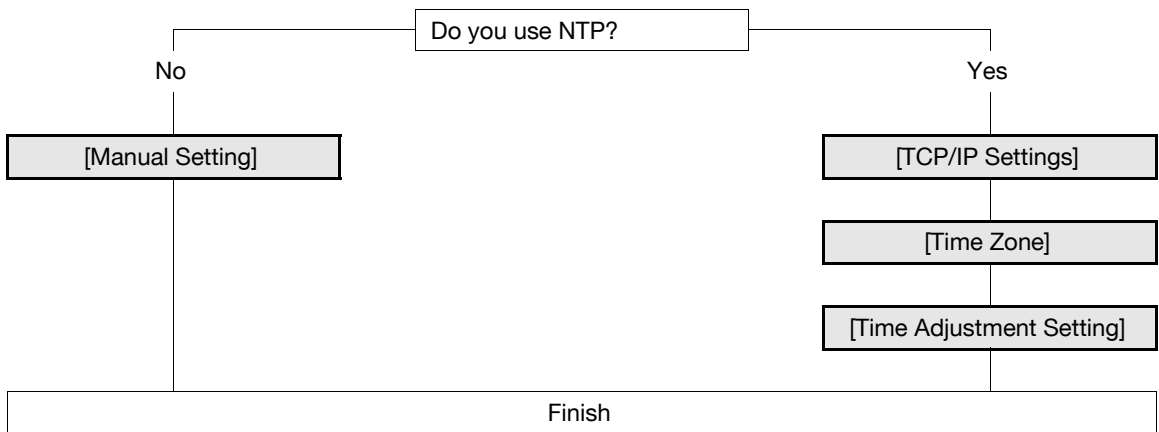
10.1.1 [Manual Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Date/Time Setting] ►► [Manual Setting].

Item	Description	Prior check
[Year]	Enter the year.	
[Month]	Enter the month.	
[Day]	Enter the day.	
[Hour]	Enter the hour.	
[Minute]	Enter the minute.	
[Time Zone]	Specify the time difference from GMT.	Time Zone
[Daylight Saving Time]	Specify the daylight saving time as required.	

10.1.2 [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

10.1.3 [Time Zone]

Specify the time zone.

10.1.4   [Time Adjustment Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Date/Time Setting] ►► [Time Adjustment Setting].

Item	Description	Prior check
[Time Adjustment Setting]	Select [ON].	
[Auto IPv6 Retrieval]	To automatically obtain the IPv6 address of the NTP server, select [ON]. This item is necessary when IPv6 is used while DHCPv6 is enabled.	Can the IPv6 address be obtained automatically?
[NTP Server Address]	Enter the NTP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port No.]	Enter a port number. Default setting: 123	Server port number
[Auto Time Adjustment]	To automatically connect to the NTP server and correct the time, select [ON].	Can the time be corrected automatically?
[Polling Interval]	When automatically correcting the time, specify its interval on a hour basis.	
[Adjust]	Click this button to connect to the NTP server in the specified conditions and adjust the time.	

10.2   Searching for the E-mail address in the LDAP server

Configure settings to search for the E-mail address in the LDAP server.

When the LDAP server is used for user management, you can search for the E-mail address via the LDAP server. Using this setting enables you to display [Address Search] in the Fax/Scan mode and search for the address via the LDAP server. When specifying an address, use the LDAP server to eliminate the need to register the address in this machine or directly enter the address.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

Reference

- When specifying Active Directory as the LDAP server and enabling GSS-SPNEGO authentication, register the DNS server connected to Active Directory in [TCP/IP Settings] of this machine. Also specify the date and time for this machine to match the system time of Active Directory.
- To use the same LDAP server for destination search and for user authentication, the LDAP server certificate verification setting for destination search specified in [Setting Up LDAP] is also applicable to the LDAP server certificate verification setting for user authentication specified in [User Auth/Account Track] ▸▸ [External Server Settings]. For details on configuring the LDAP server for user authentication and certificate verification, refer to page 7-25.

```
                        ┌──────────────────────┐
                        │   [TCP/IP Settings]  │
                        └──────────┬───────────┘
                        ┌──────────┴───────────┐
                        │    [LDAP Setting]    │
                        └──────────┬───────────┘
              ┌────────────────────┴─────────────────────┐
              │             [Setting Up LDAP]            │
              └──┬──────────────────────────────────┬────┘
  ┌──────────────┴──────────┐          ┌────────────┴──────────────┐
  │ Do you have an SSL com-  │          │ Do you use Active Directo- │
  │ munication with the LDAP │          │ ry (GSS-SPNEGO)?           │
  │ server?                  │          │                            │
  └───────┬─────────┬────────┘          └───────┬───────────┬───────┘
        Yes        No                          No          Yes
  ┌───────┴───────┐                                  ┌───────┴──────────┐
  │  LDAP over SSL │                                  │ DNS server setting│
  └───────┬───────┘                                  └───────┬──────────┘
          │                                          ┌───────┴──────────┐
          │                                          │ [Date/Time Setting]│
          │                                          └───────┬──────────┘
  ┌───────┴──────────────────────────────────────────────────┴──────────┐
  │                               Finish                                  │
  └──────────────────────────────────────────────────────────────────────┘
```
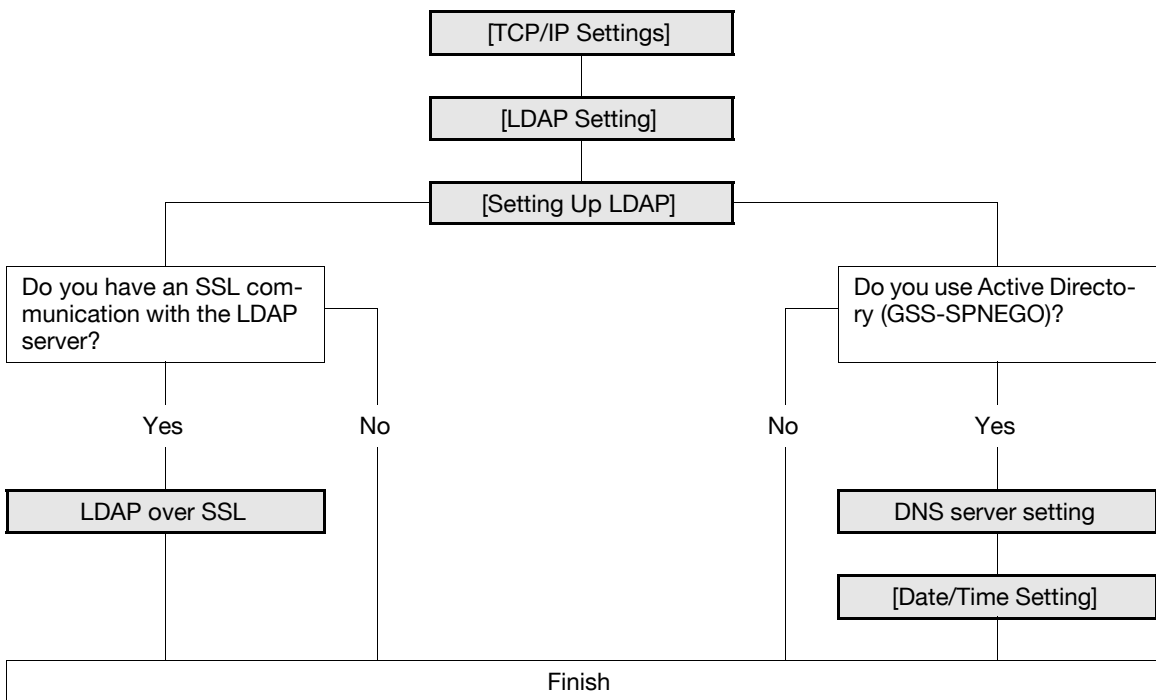
📖 **Reference**
For details on how to send an E-mail using the LDAP search function, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].
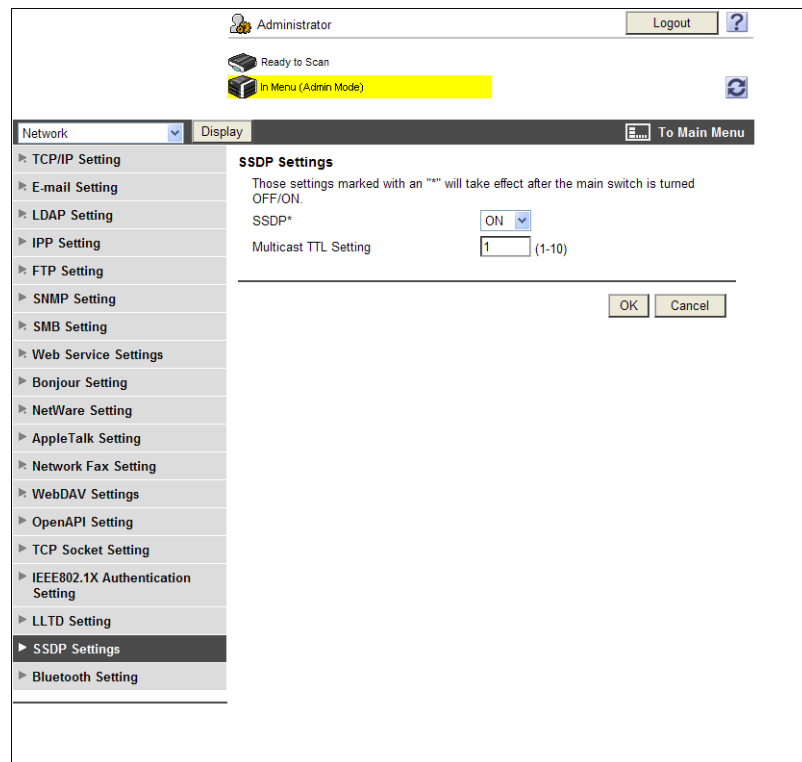
10.2.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

10.2.2 [LDAP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [LDAP Setting] ▸▸ [LDAP Setting].
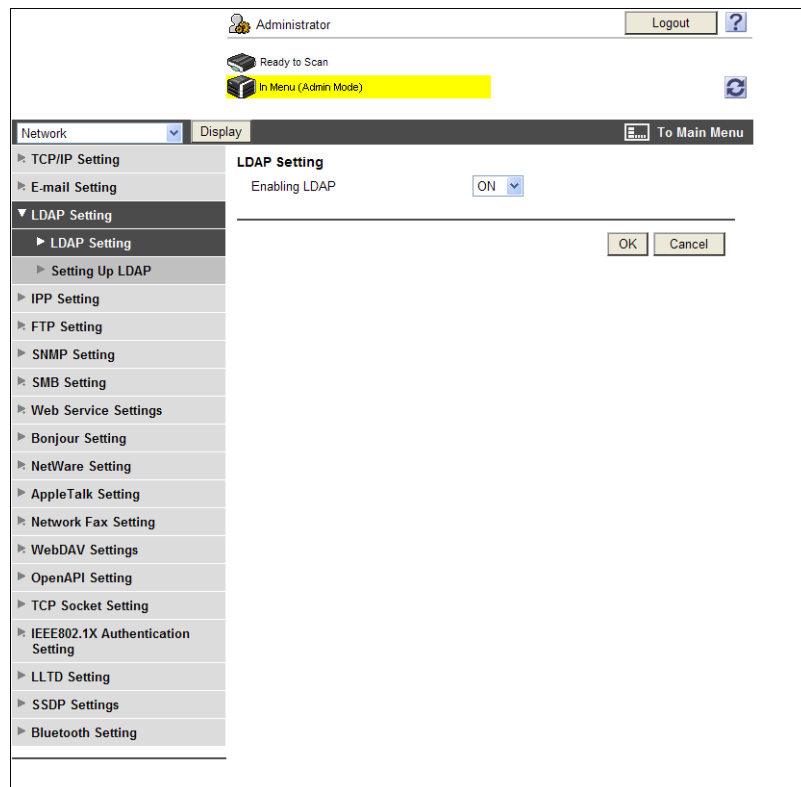
Item	Description	Prior check
[Enabling LDAP]	Select [ON].	

10.2.3   [Setting Up LDAP]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [LDAP Settings] ►► [Setting Up LDAP] ►► [Edit].

Reference

- After registering the LDAP server, click [Check Connection] in [LDAP Server List] to check whether this machine can be connected to the registered LDAP server.
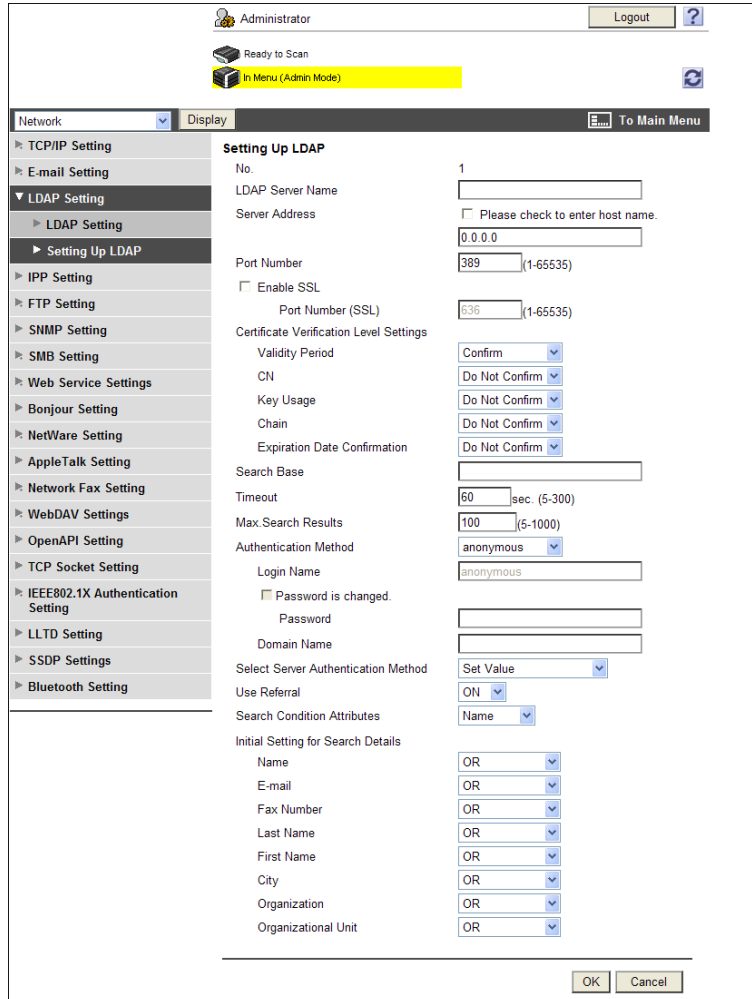
Item	Description	Prior check
[LDAP Server Name]	Enter the name of an LDAP server (up to 32 characters).	
[Server Address]	Specify the LDAP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port Number]	Enter a port number. Default setting: 389	
[Search Base]	Enter the search starting point in the directory structure under the LDAP server (up to 255 characters). This search function also covers subdirectories under the entered starting point.	Search base
[Timeout]	Enter the timeout period for LDAP search.	
[Max.Search Results]	Enter the maximum number of items that can be received as LDAP search results.	

Item	Description	Prior check
[Authentication Method]	Select the authentication method to log in to the LDAP server. The authentication method must match that used in the LDAP server. If [anonymous] is selected, [Login Name], [Password], and [Domain Name] can be omitted. If [GSS-SPNEGO] is selected, log in to the server in the Kerberos authentication method. The Kerberos authentication method is supported by Active Directory.	Server authentication method
[Login Name]	Enter the login name to log in to the LDAP server (up to 255 bytes).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the LDAP server (up to 128 bytes, excluding space and ").	
[Domain Name]	Enter the domain name to log in to the LDAP server (up to 64 characters). If [GSS-SPNEGO] is selected, enter the domain name of Active Directory.	• Authentication Method • Domain name
[Select Sever Authentication Method]	Select the server authentication method. Select [Set Value] to use the settings of [Login Name], [Password], and [Domain Name]. Select [User Authentication] to use the user name and password specified for user authentication. If [Dynamic Authentication] is selected, the system prompts you to enter the user name and password at LDAP searching.	
[Use Referral]	Select whether to use the referral function. Make an appropriate choice to fit the LDAP server environment.	
[Search Condition Attributes]	Select the attribute of the name used for LDAP searching. You can toggle this attribute between [Name] (cn) and [Nickname] (displayName).	Name attribute
[Initial Setting for Search Details]	Specify LDAP search conditions.	

10.2.4   LDAP over SSL

[Setting Up LDAP]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [LDAP Settings] ►► [Setting Up LDAP] ►► [Edit].

Item	Description	Prior check
[Enable SSL]	Select this check box to encrypt an SSL communication between this machine and the LDAP server.	Does the server support SSL?
[Port Number (SSL)]	Enter the port number to be used for SSL communication. Default setting: 636	Server port number
[Certificate Verification Level Settings]	To verify the server certificate, configure settings to verify the certificate.	
[Validity Period]	Select whether to check that the server certificate is within the validity period.	
[CN]	Select whether to check that the CN of the server certificate matches the server address.	
[Key Usage]	Select whether to check that the server certificate is used according to the purpose approved by the issuer.	

Item	Description	Prior check
[Chain]	Select whether to check that the server certificate chain (certification path) is correct. The chain is validated by referencing the external certificates managed on this machine. For details, refer to page 8-34.	
[Expiration Date Confirmation]	Select whether to check that the server certificate is within the validity period. The OCSP service and CRL (Certificate Revocation List) are checked in this order when the expiration date of the certificate is checked.	

[Certificate Verification Setting]

In the administrator mode of **PageScope Web Connection**, select [Security] ►► [Certificate Verification Setting].

Item	Description	Prior check
[Certificate Verification Setting]	Select [ON] to verify the server certificate.	
[Timeout]	Enter a timeout period for expiration date confirmation.	Do you confirm the expiration date?
[OCSP Service]	Select this check box to use the OCSP service.	
[URL]	Enter the URL of the OCSP service (up to 511 characters). If this item is left blank, the machine accesses the URL of the OCSP service embedded in the certificate. If the URL of the OCSP service is not embedded in the certificate, an error will occur.	
[Proxy Server Address]	To confirm the expiration date via a proxy server, enter its address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Proxy Server Port Number]	Enter the port number of a proxy server.	Server port number

Item	Description	Prior check
[User Name]	Enter the user name to log in to the proxy server (up to 63 characters).	
[Password is changed.]	Select this check box to change the password.	
[Password]	Enter the password to log in to the proxy server (up to 63 characters).	
[Address not using Proxy Server]	To enable expiration date confirmation, specify an address that does not use the proxy server depending on your environment. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	

10.2.5   DNS server setting

When specifying Active Directory as the LDAP server and enabling GSS-SPNEGO authentication, register the DNS server connected to Active Directory.

For details on DNS Server Setting, refer to page 2-2.

10.2.6   [Date/Time Setting]

To use Active Directory, specify the date and time of this machine.

For details, refer to page 10-2.

10.3   Displaying this machine on the network map

Configure settings to display this machine on the network map in Windows Vista or Server 2008/7.

When the LLTD function of this machine is enabled, the network position of this machine can be displayed on the network map. Also, when you click the icon of this machine on the network map, you can access **PageScope Web Connection**.

The network map is very useful for checking the location and information of this machine and for network troubleshooting.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
┌──────────────────────┐
│   [TCP/IP Settings]  │
└──────────────────────┘
            │
┌──────────────────────┐
│    [LLTD Setting]    │
└──────────────────────┘
            │
┌──────────────────────┐
│        Finish        │
└──────────────────────┘
```
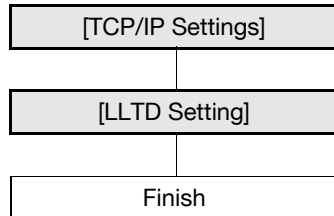
10.3.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

10.3.2   [LLTD Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [LLTD Setting].
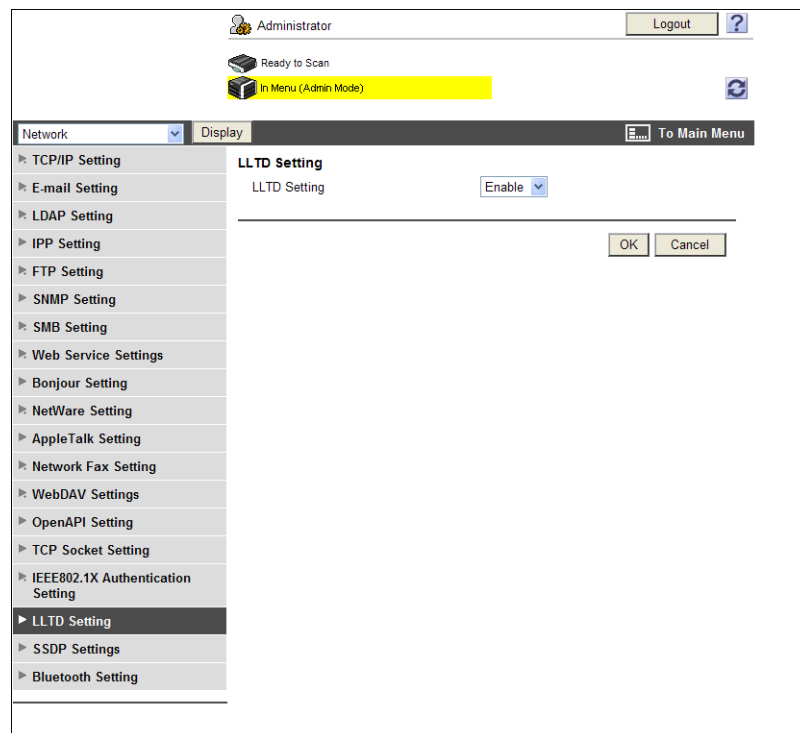
Item	Description	Prior check
[LLTD Setting]	Select [Enable].	

10.4   Monitoring this machine by SNMP Manager

Configure settings to monitor this machine using the SNMP manager.

Using the SNMP manager, you can communicate with the SNMP agent of this machine and get, manage, and supervise this machine information via the network. The SNMP can be used in the TCP/IP environment or IPX/SPX environment.

Also, you can send this machine status information to others using the SNMP TRAP function. For details, refer to page 10-18.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                        (1) Use the TCP/IP
                        (2) Use the IPX/SPX

        (1)                                              (2)

   [TCP/IP Settings]                              [NetWare Settings]

                        [SNMP Setting]

                           Finish
```

10.4.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

10.4.2   [NetWare Settings]

In the administrator mode of **PageScope Web Connection**, select [Network]▶▶[NetWare Settings]▶▶[Net-Ware Settings].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type

10.4.3   [SNMP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [SNMP Setting].

Item	Description	Prior check
[SNMP Setting]	Select [ON]. When you use the SNMP, select whether to use [SNMP v1/v2c (IP)], [SNMP v3 (IP)], or [SNMP v1 (IPX)]. You can select [SNMP v1 (IPX)] only when the IPX is enabled.	The protocol you use (TCP/IP or IPX/SPX)

Item	Description	Prior check
[UDP Port Setting]	Enter a UDP port number. Default setting: 161	
[SNMP v1/v2c Setting]	Configure the settings for SNMP v1/v2c.	
[Read Community Name]	Enter a community name used for reading (up to 15 characters, excluding space and \).	
[Write Community Name]	Enter a community name used for reading and writing (up to 15 characters, excluding space and \).	
[SNMP v3 Setting]	Set the settings for SNMP v3.	
[Context Name]	Enter a context name (up to 63 characters, excluding space and \).	
[Discovery User Name]	Enter a context user for detection (up to 32 characters, excluding space and \).	
[Read User Name]	Enter a user name of the read-only user (up to 32 characters, excluding space and \).	
[Security Level]	Select a security level of the read-only user.	
[Password is changed.]	Select this check box to change the password.	
[auth-password]	Enter the password of the read-only user for authentication (up to 32 from 8 characters, excluding space and \).	
[Password is changed.]	Select this check box to change the password.	
[priv-password]	Enter the privacy password of the read-only user to be used for privacy (encryption) (up to 32 from 8 characters, excluding space and \).	
[Write User Name]	Enter a user name used of the read and write-only user (up to 32 characters, excluding space and \).	
[Security Level]	Select a security level of the read and write-only user.	
[auth-password]	Enter the password of the read and write-only user for authentication (up to 8 to 32 characters, excluding space and \).	
[Password is changed.]	Select this check box to change the password.	
[priv-password]	Enter the privacy password of the read and write-only user to be used for privacy (encryption) (up to 8 to 32 characters, excluding space and \).	
[Password is changed.]	Select this check box to change the password.	
[Encryption Algorithm]	Select an encryption algorithm.	
[Authentication Method]	Select an authentication method.	
[Device Name]	Enter the name of this machine (up to 255 characters).	
[Device Location]	Enter the location to install this machine (up to 255 characters).	
[Administrator Name]	Enter the administrator name (up to 255 characters).	

10.5   Reporting the status of this machine (by E-mail)

Configure settings to report the status of this machine to the administrator by E-mail.

If an alarm has occurred on this machine, it can be reported to the specified destination by E-mail.

A combination of POP before SMTP authentication, APOP authentication, SMTP authentication and SSL/TLS encryption can be used for notification by E-mail.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                        [TCP/IP Settings]
                               |
                        [E-mail TX
                          (SMTP)]
                               |
                     [Status Notifica-
                      tion Setting]
      +------------------------+------------------------+
      |                        |                        |
Do you have an          Do you use SMTP          POP before SMTP?
SSL/TLS communi-        authentication?
cation with the
SMTP server?
   Yes      No           Yes      No           Yes               No
    |                     |                      |
SMTP over            SMTP Authenti-          POP before SMTP
SSL/Start TLS           cation                    |
                                            (1) POP over SSL?
                                            (2) APOP?
                                               Yes        No
                                                |
                                            (1) POP over SSL
                                            (2) APOP Authenti-
                                                cation
      +------------------------+------------------------+
                            Finish
```
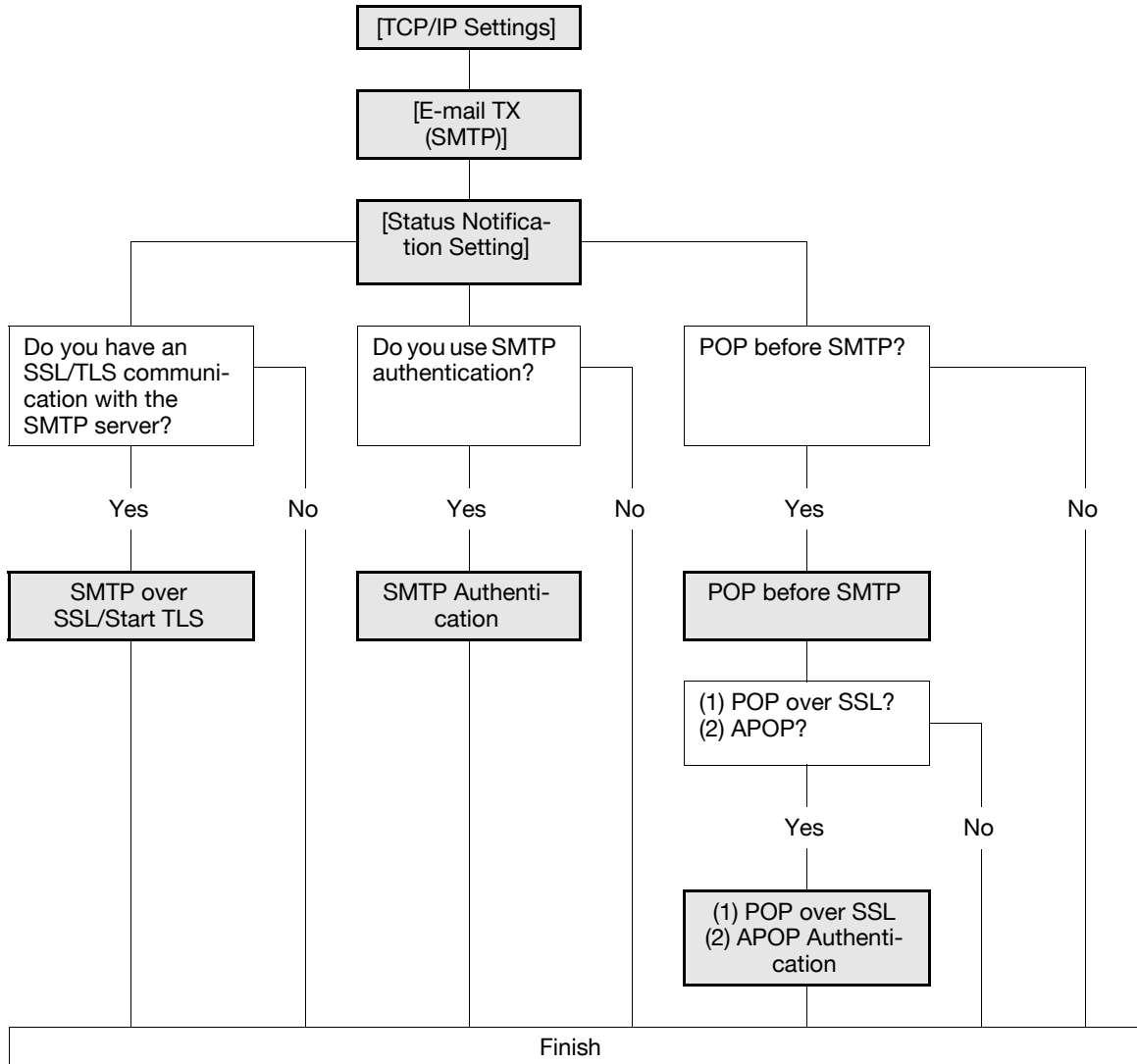
10.5.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

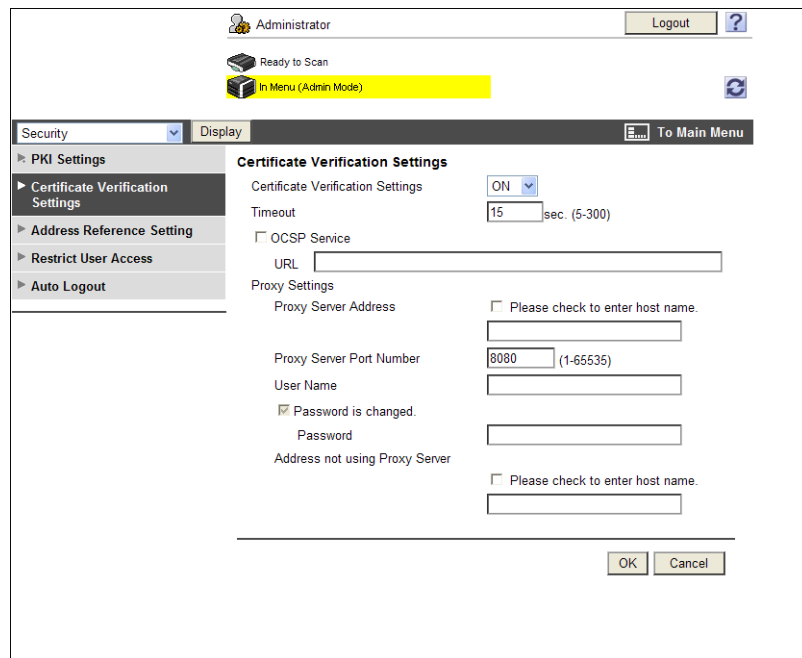For details, refer to page 2-2.

10.5.2   [E-mail TX (SMTP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail TX (SMTP)].

Item	Description	Prior check
[E-mail TX Setting]	Select the [E-mail TX Setting] check box.	
[E-mail Notifica-tion]	Select [ON].	

Item	Description	Prior check
[SMTP Server Address]	Enter the SMTP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port Number]	Enter a port number. Default setting: 25	Server port number
[Connection Timeout]	Specify the timeout period for a communication with a server.	
[Max Mail Size]	Select whether to limit the size of an E-mail to be sent.	
[Server Capacity]	Enter the SMTP server capacity. A mail that exceeds the upper limit of the server capacity will be discarded. If an E-mail is divided, this setting is made invalid.	Server reception limit
[Admin. E-mail Address]	Displays the E-mail address of the administrator. Register the administrator's E-mail address in [System Settings]▸▸[Machine Setting] if it is not registered.	
[Binary Division]	Select this check box to divide an E-mail. If the E-mail software that received an E-mail does not have a restoration function, you may not be able to read the E-mail.	Restoration function of E-mail software
[Divided Mail Size]	Enter the divided mail size to divide an E-mail.	Server reception limit

10.5.3   [Status Notification Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Status Notification Setting] ▸▸ [E-mail Address] ▸▸ [Edit].
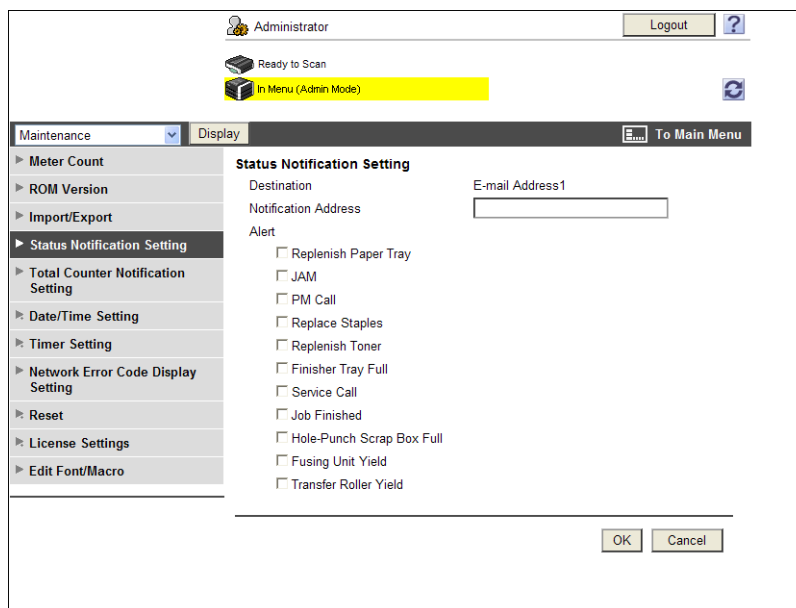
Item	Description	Prior check
[Notification Address]	Enter the destination E-mail address.	Notification address
[Replenish Paper Tray]	Sends a notification when the paper tray is empty.	
[JAM]	Sends a notification when a page has been jammed.	
[PM Call]	Sends a notification when the periodical inspection is required.	
[Replace Staples]	Sends a notification when there are no staples remaining.	

Item	Description	Prior check
[Replenish Toner]	Sends a notification when the toner is empty.	
[Finisher Tray Full]	Sends a notification when the capacity of the finisher tray has been exceeded.	
[Service Call]	Sends a notification when a service call has occurred.	
[Job Finished]	Sends a notification when the job has finished.	
[Hole-Punch Scrap Box Full]	Sends a notification when you need to empty the punch scrap box.	
[Waste Toner Box Full]	Sends a notification when the waste toner box needs to be replaced.	
[Drum Unit/Developing Unit Life]	Sends a notification when the drum unit or developing unit needs to be replaced.	
[Fusing Unit Yield]	Sends a notification when the fusing unit needs to be replaced.	
[Transfer Roller Yield]	Sends a notification when the transfer roller unit needs to be replaced.	
[Transfer Belt Unit Yield]	Sends a notification when the transfer belt needs to be replaced.	
[Ozone Filter Yield]	Sends a notification when the ozon filter needs to be replaced.	

10.5.4   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

10.5.5   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

10.5.6   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

10.5.7   POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

10.5.8   APOP Authentication

Configure APOP authentication settings.

For details, refer to page 4-16.

10.6   Reporting the status of this machine (TRAP)

Configure settings to report the status of this machine to the administrator using the SNMP TRAP functions.

If an alarm has occurred on this machine, it can be reported to the specified IP address or IPX address by the SNMP TRAP.

To use the SNMP TRAP functions, you must set the SNMP in advance. For details, refer to page 10-12.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                    ┌──────────────────────────────┐
                    │ (1) Notification to IP address│
          ┌─────────┤ (2) Notification to IPX ad-   ├─────────┐
          │         │     dress                     │         │
          │         └──────────────────────────────┘         │
         (1)                                                 (2)
          │                                                   │
  ┌───────────────┐                                   ┌───────────────┐
  │[TCP/IP Settings]│                                 │[NetWare Settings]│
  └───────────────┘                                   └───────────────┘
          │                                                   │
          │              ┌─────────────────┐                  │
          └──────────────┤  [TRAP Setting] ├──────────────────┘
                         └─────────────────┘
                                 │
                    ┌────────────────────────────┐
                    │ [Status Notification Setting]│
                    └────────────────────────────┘
                                 │
                         ┌─────────────────┐
                         │     Finish      │
                         └─────────────────┘
```

10.6.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

10.6.2 [NetWare Settings]

In the administrator mode of **PageScope Web Connection**, select [Network]▸▸[NetWare Settings]▸▸[Net-Ware Settings].

Item	Description	Prior check
[IPX Setting]	Select [ON].	
[Ethernet Frame Type]	Select a frame type to be used.	Frame type

10.6.3 [TRAP Setting]

In the administrator mode of **PageScope Web Connection**, select [Network] ▸▸ [SNMP Setting].

Item	Description	Prior check
[Allow Setting]	Select [Allow].	
[Trap Setting when Authentication Fails]	Select whether to enable TRAP transmission at the time of authentication failure.	

10.6.4   [Status Notification Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance]▸▸[Status Notification Setting]▸▸[IP Address] or [IPX Address]▸▸[Edit].

Item	Description	Prior check
[Destination Address]	If the destination has an [IP Address], enter it. If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address. If the destination has an [IPX Address], enter it using an 8-digit hexadecimal value.	Notification address
[Port Number]	If the destination has an [IP Address], enter its port number.	
[Node Address]	If the destination has an [IPX Address], enter the node address using a 12-digit hexadecimal value.	
[Community Name]	Enter a community name (up to 15 characters).	
[Replenish Paper Tray]	Sends a notification when the paper tray is empty.	
[JAM]	Sends a notification when a page has been jammed.	
[PM Call]	Sends a notification when the periodical inspection is required.	
[Replace Staples]	Sends a notification when there are no staples remaining.	
[Replenish Toner]	Sends a notification when the toner is empty.	
[Finisher Tray Full]	Sends a notification when the capacity of the finisher tray has been exceeded.	
[Service Call]	Sends a notification when a service call has occurred.	
[Job Finished]	Sends a notification when the job has finished.	
[Hole-Punch Scrap Box Full]	Sends a notification when you need to empty the punch scrap box.	
[Waste Toner Box Full]	Sends a notification when the waste toner box needs to be replaced.	
[Drum Unit/Developing Unit Life]	Sends a notification when the drum unit or developing unit needs to be replaced.	
[Fusing Unit Yield]	Sends a notification when the fusing unit needs to be replaced.	
[Transfer Roller Yield]	Sends a notification when the transfer roller unit needs to be replaced.	
[Transfer Belt Unit Yield]	Sends a notification when the transfer belt needs to be replaced.	
[Ozone Filter Yield]	Sends a notification when the ozon filter needs to be replaced.	

10.7   Reporting the counter information of this machine (by E-mail)

Configure settings to report the counter information of this machine by E-mail.

You can send the counter information being managed on this machine to the specified destination by E-mail.

A combination of POP before SMTP authentication, APOP authentication, SMTP authentication and SSL/TLS encryption can be used for notification by E-mail.

Use the following flowchart to configure settings. Clicking a step jumps to the associated procedure.

```
                        [TCP/IP Settings]

                         [E-mail TX
                          (SMTP)]

                        [Total Counter
                      Notification Set-
                           tings]

  Do you have an          Do you use SMTP          POP before SMTP?
  SSL/TLS communi-        authentication?
  cation with the
  SMTP server?

  Yes         No         Yes         No           Yes            No

  SMTP over              SMTP Authenti-           POP before SMTP
  SSL/Start TLS          cation

                                                  (1) POP over SSL?
                                                  (2) APOP?

                                                  Yes        No

                                                  (1) POP over SSL
                                                  (2) APOP Authenti-
                                                      cation

                              Finish
```
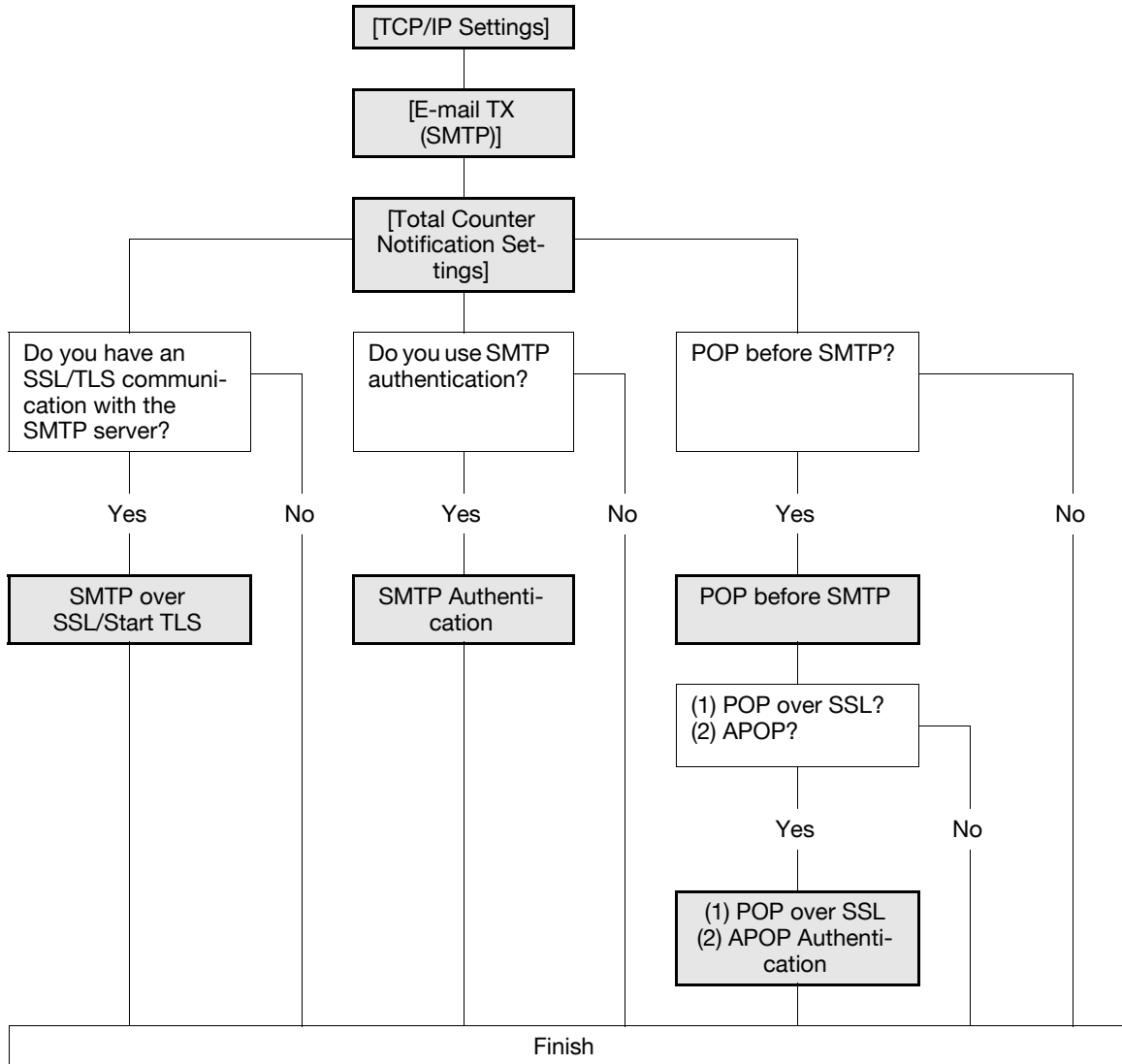
10.7.1   [TCP/IP Settings]

Configure settings to use this machine in the TCP/IP network environment.

For details, refer to page 2-2.

10.7.2   [E-mail TX (SMTP)]

In the administrator mode of **PageScope Web Connection**, select [Network] ►► [E-mail Setting] ►► [E-mail Transmission (SMTP)].

Item	Description	Prior check
[E-mail TX Setting]	Select the [E-mail TX Setting] check box.	
[Total Counter Notification]	Select [ON].	
[SMTP Server Address]	Enter the SMTP server address. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.	Server address
[Port Number]	Enter a port number. Default setting: 25	Server port number
[Connection Timeout]	Specify the timeout period for a communication with a server.	
[Max Mail Size]	Select whether to limit the size of an E-mail to be sent.	
[Server Capacity]	Enter the SMTP server capacity. A mail that exceeds the upper limit of the server capacity will be discarded. If an E-mail is divided, this setting is made invalid.	Server reception limit
[Admin. E-mail Address]	Displays the E-mail address of the administrator. Register the administrator's E-mail address in [System Settings]►►[Machine Setting] if it is not registered.	
[Binary Division]	Select this check box to divide an E-mail. If the E-mail software that received an E-mail does not have a restoration function, you may not be able to read the E-mail.	Restoration function of E-mail software
[Divided Mail Size]	Enter the divided mail size to divide an E-mail.	Server reception limit

10.7.3   [Total Counter Notification Settings]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Total Counter Notification Settings].

Item	Description	Prior check
[Model Name]	Enter a model name to be included in the notification mail message (up to 20 characters).	
[Notification Schedule Setting]	Specify the conditions for the notification schedule. Schedules 1 and 2 can be registered with different settings.	Notification schedule
[Notification Address Setting]	Enter the destination E-mail address (up to 320 characters). In addition, select a notification schedule.	Destination
[Send notice after setting complete]	If [ON] is selected, a notification is tested when you press [OK].	

10.7.4   SMTP over SSL/Start TLS

Configure the settings for SMTP over SSL or Start TLS.

For details, refer to page 4-10.

10.7.5   SMTP Authentication

Configure SMTP authentication settings.

For details, refer to page 4-12.

10.7.6   POP before SMTP

Configure the settings for POP before SMTP.

For details, refer to page 4-13.

10.7.7   POP over SSL

Configure the settings for POP over SSL.

For details, refer to page 4-14.

10.7.8   APOP Authentication

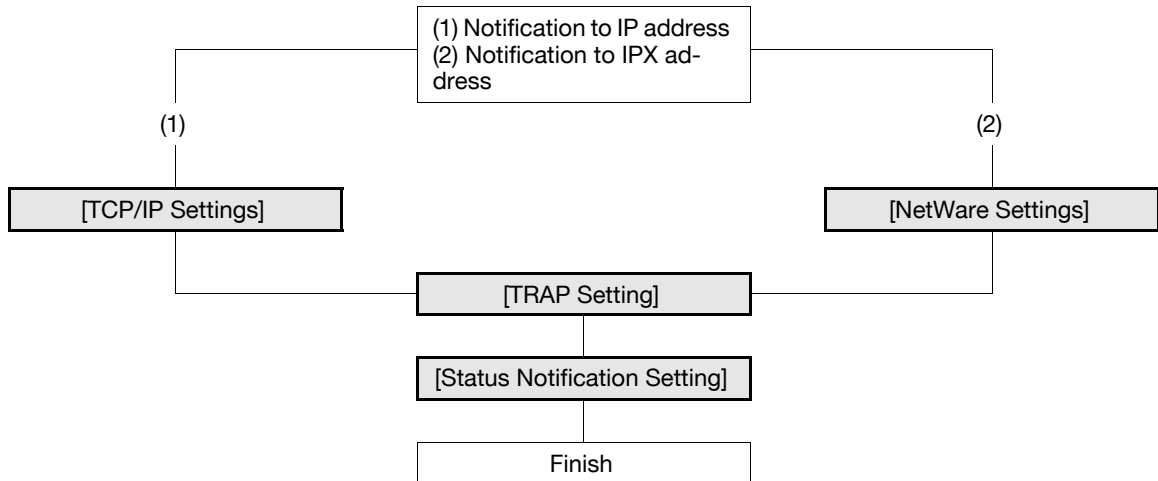Configure APOP authentication settings.

For details, refer to page 4-16.

10.8   Checking the counter of this machine

Check the counter information being managed on this machine.

[Meter Counter]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Meter Counter].

10.9 Checking the machine ROM version

Check the ROM version of this machine.

[ROM Version]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [ROM Version].
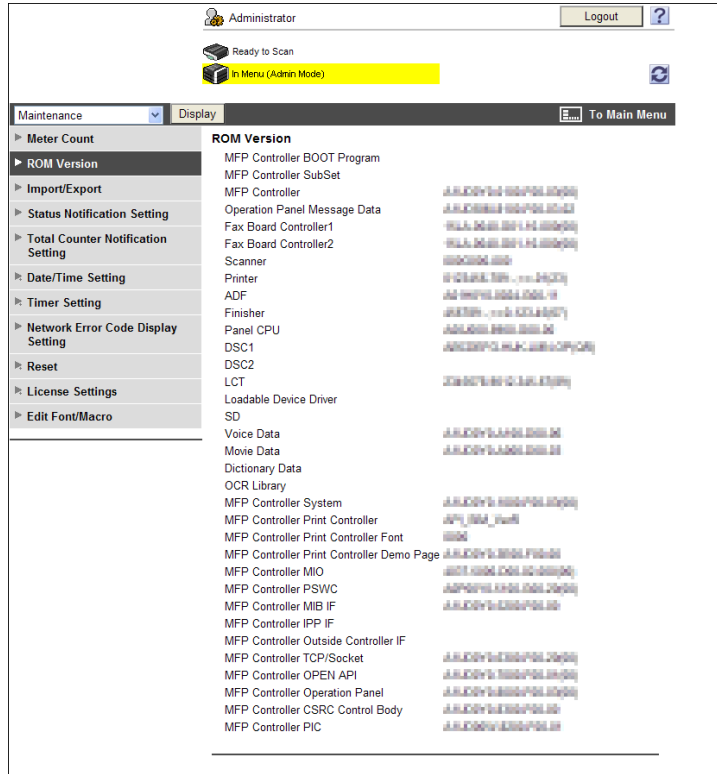
10.10   Importing and exporting the machine configuration information

You can save (export) the configuration information being stored in this machine to the computer. You can also write (import) the information from the computer to this machine.

[Import/Export]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▶▶ [Import/Export].

Item	Description
[Device Setting]	Import or export device setting values.
[Counter]	Export the counter information. The counter can only be exported.
[Authentication Information]	Back up or restore all authentication data. This function also allows you to import or export user registration information or authentication data. When the optional authentication unit is used on this machine, you can import or export the authentication data. When you export the authentication data, you can set a password as required. The specified password is required for importing the authentication information. If you use **PageScope Authentication Manager** for authentication, this item is not displayed. (Linking with **PageScope Authentication Manager** is available only when a **Hard Disk** is installed.)
[Address]	Back up or restore all address data. This function also allows you to import or export address data. When you export the destination information, you can set a password as required. The specified password is required for importing the destination information.
[Copy Protect/Stamp]	Import or export copy protect or stamp data.
[Restriction Code List]	Import or export the list of inhibited codes of our deprecated OpenAPI connection applications.

Reference
- You cannot edit exported files.
- When importing an E-mail address with an exported certificate, register the certificate information again after importing it.
- For details on the list of inhibited codes, contact your service representative.

10.11   Using the timer functions

Configure the Power Save and Weekly Timer functions.

The power save function has two modes: Low Power and Sleep. More electric power will be saved in the Sleep mode when compared with the Low Power mode. However, the Sleep mode takes more time to warm up this machine than the Low Power mode. Select the mode appropriate to your application.

The Weekly Timer function allows you to specify the time before transition to the Sleep mode in units of days or weeks. You can control the power saving according to your application.

[Power Save Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Timer Setting] ►► [Power Save Setting].

Item	Description
[Low Power Mode Setting]	Enter a time interval before transition to the Low Power mode since the last operation of this machine.
[Sleep Mode Setting]	Enter a time interval before transition to the Sleep mode since the last operation of this machine.
[Power Save Key]	If you do not operate this machine for a long time, you can forcibly switch this machine to the power saving mode by pressing the **Control Panel** key on the **Power Save**. Select the mode this machine will transition to when you press the **Power Save** key.
[Enter Power Save Mode]	Specify how to return to the Power Save mode after printout of the fax document that was received in the Power Save mode. Setting this item to [Immediately] returns this machine immediately after receiving a fax while it is not being used (in the night for example), thus saving the electric power more efficiently. If you set this item to [Normal], this machine returns to the Power Save mode after the specified transition time has elapsed.
[Fax Board Power Save]	Specify whether to enable power save mode. When [ON] is specified, the fax board will not enter the power save mode in the following situations: • Number of RX Call Rings is set to 0. • TEL/FAX Auto Switch is enabled. • Disconnect External Telephone is set to [ON].

[Weekly Timer Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Timer Setting] ▸▸ [Weekly Timer Setting].

Item	Description
[Use Weekly Timer]	To use the Weekly Timer function, select this check box and specify the operation date and time. Specify dates or days of every week when the Weekly Timer function is activated. You can also specify both dates and days of the week at the same time. Click [Setting] to specify the days when Weekly Timer operates.
[Use Power Save]	To use the Power Save function, select this check box and specify the OFF Time and the Power Save End Time.
[Use Overtime Password]	Specify the overtime password to restrict the users who can temporarily use this machine while it is being placed in the Sleep mode by the Weekly Timer function. To specify the overtime password, select this check box and enter the password (up to eight characters, excluding + and ").

10.12 Displaying a network error code

If an error has occurred on the network, its error code can be displayed.

Configure this item if you wish to check the network error codes for troubleshooting and other purposes.

📖 Reference
For details on the network error codes, refer to page 15-19.

[Network Error Code Display Setting]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Network Error Code Display Setting].
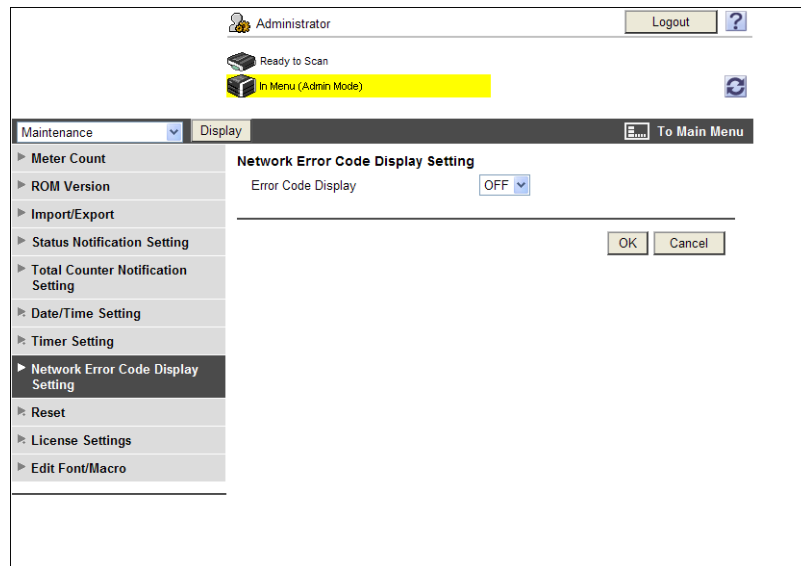
Item	Description
[Error Code Display]	Select [ON].

10.13   Initializing the configuration information

You can initialize the network settings (to the factory defaults), reset the controller, and delete the entire destination information.

[Network Setting Clear]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Reset] ▸▸ [Network Setting Clear].

(If [Enhanced Security Mode] is enabled, this menu item will not be displayed.)

If you click [Clear], the network settings of this machine are cleared to the factory defaults.
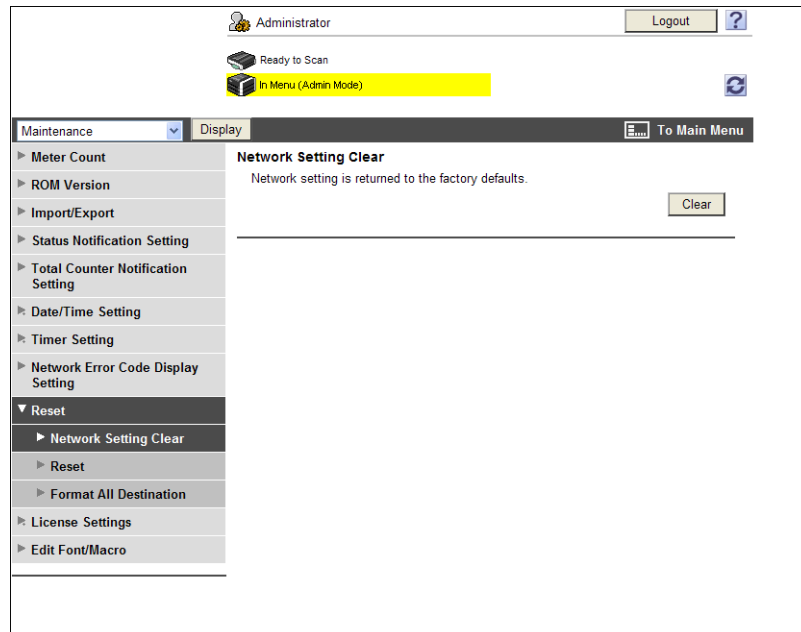
[Reset]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Reset] ▸▸ [Reset].

If you click [Reset], the controller is reset.
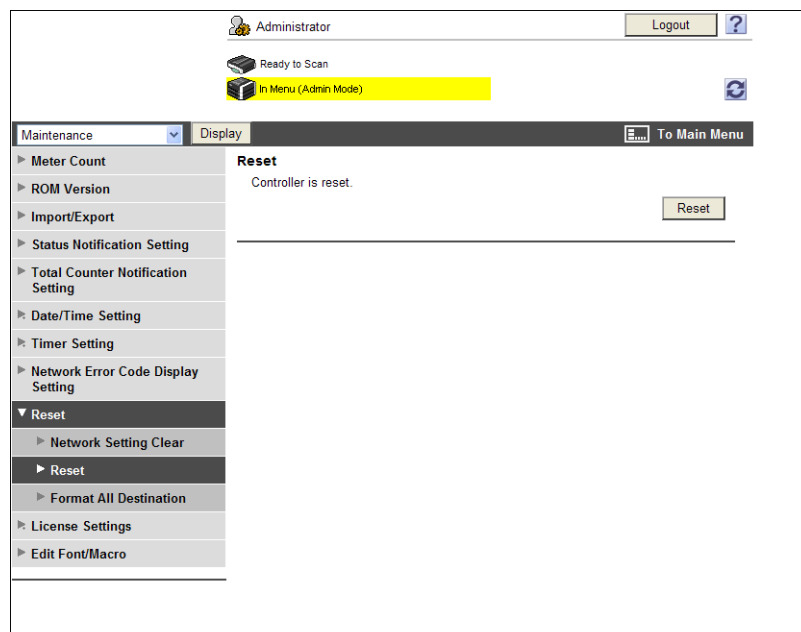
[Format All Destination]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Reset] ►► [Format All Destination].

If you click [Format], the entire destination data being registered on this machine is erased.
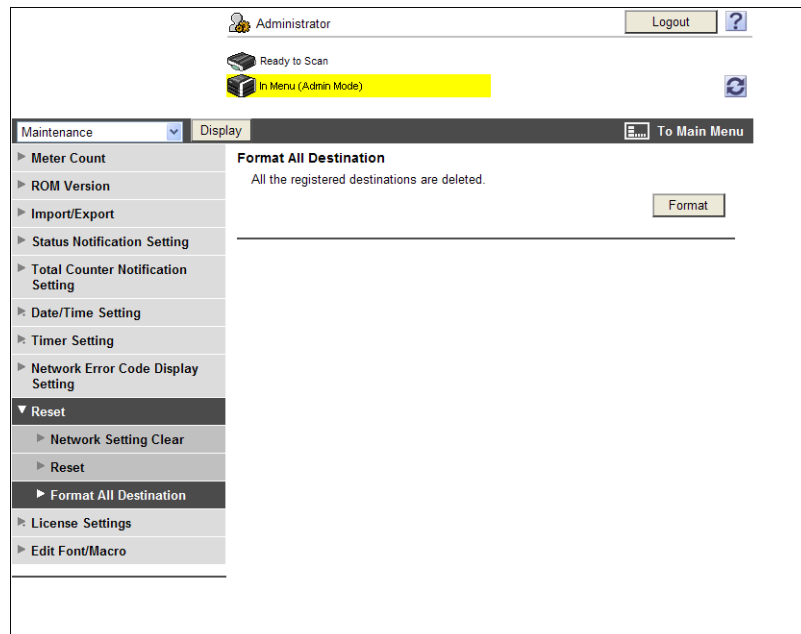
10.14 Enhancing the functions of this machine

To enhance the functions of this machine by registering the optional License kit, you can obtain a request code and enable the functions.

Reference

- This menu item will not be displayed if the extension memory supplied together with the optional **Upgrade Kit UK-203** is not installed.
- This function is available only when a **Hard Disk** is installed.

📖 **Reference**

For details on the license code acquisition and function enabling, refer to the [Quick Guide Copy/Print/Fax/Scan/Box Operations].

[Get Request Code]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [License Settings] ►► [Get Request Code].

If you click [OK], a request code is issued.
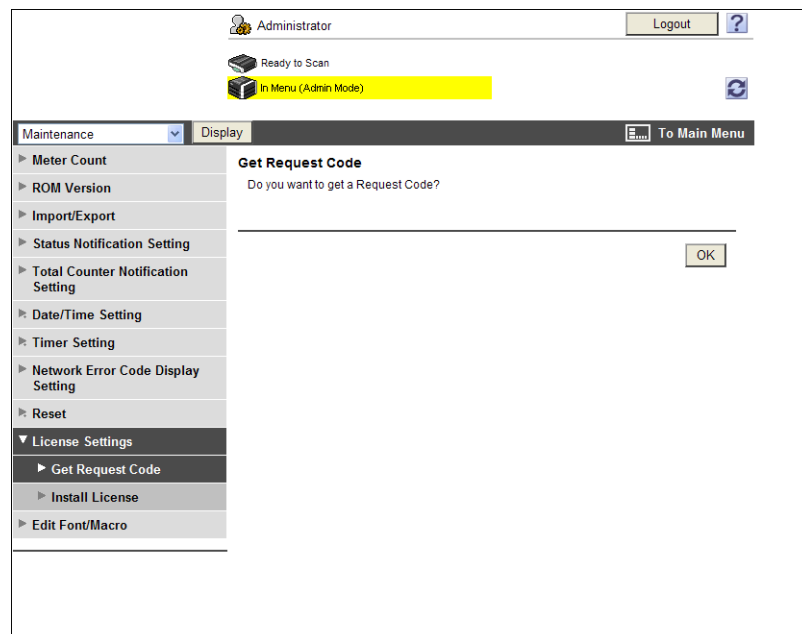
[Install License]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [License Settings] ►► [Install License].

Item	Description
[Function Code]	Enter the function code.
[License Code]	Enter the license code.
[OK]	Click this button to enable the function.

10.15   Outputting job logs

You can create and download log data (accounting log, counting log, or audit log) of the jobs that were executed in this machine. For details on viewing the output job logs, contact your service representative.

(This menu is not displayed when [Security Settings] ▸▸ [Security Details] ▸▸ [Job Log Settings] is set to [No] in the [Administrator Settings] on the **Control Panel**.)

Reference

- For details on [Job Log Settings], refer to the [User's Guide Copy Operations].
- If the job log writing area has reached the upper limit, output job logs.
- This function is available only when a **Hard Disk** is installed.

[Create Job Log]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ▸▸ [Job Log] ▸▸ [Create Job Log].

When you click [OK], the machine starts creating job log data. After creation is completed, you can download job log data using [Download Job Log].
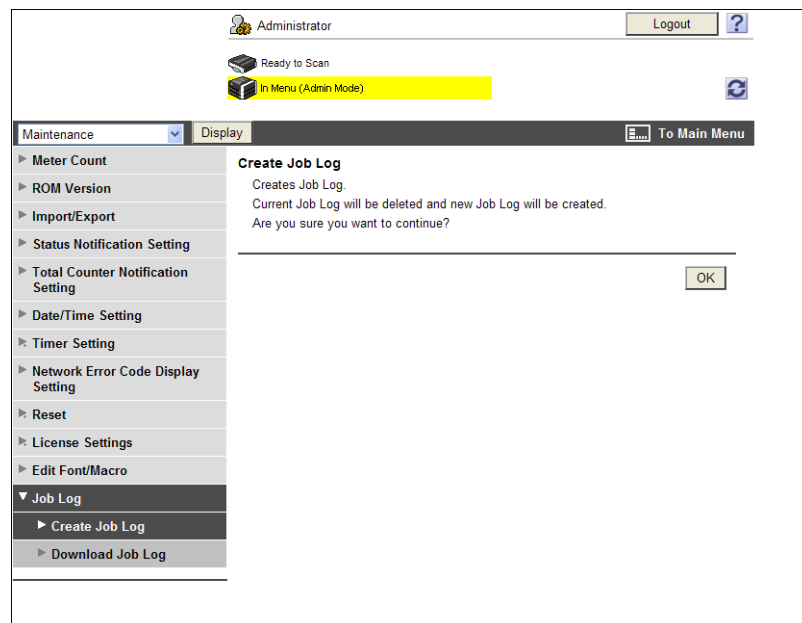
Reference

- If you attempt to create job log data when some already exists, a confirmation message is displayed to check if you want to delete the job log data that is not output in order to create new job log data. When there is job log data that is not output, download it before creating new job log data.

[Download Job Log]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Job Log] ►► [Download Job Log].

When downloading job log data, click [OK] and also click [Download].
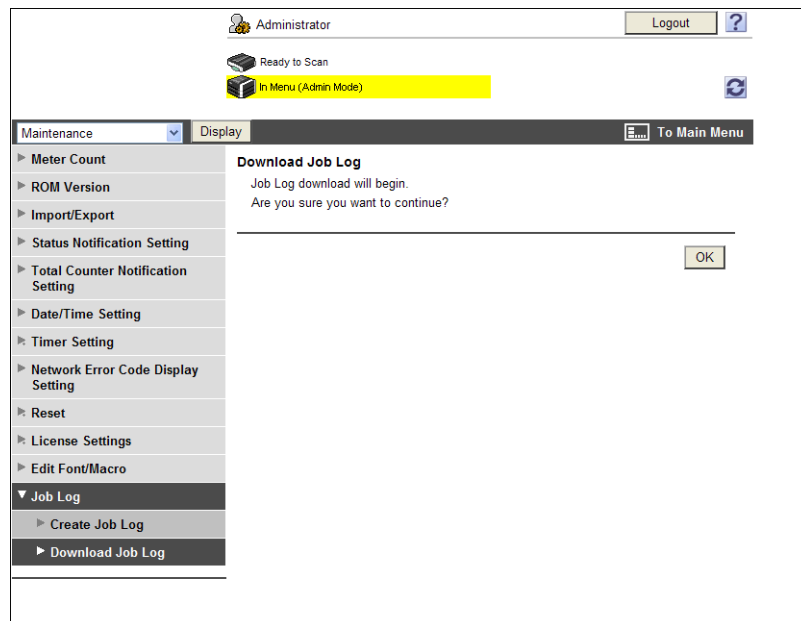
Reference

● To download job log data, create it in [Create Job Log] in advance.

10.16   Configuring settings for printing blank pages

Configure settings related to printing blank pages.

You can specify whether to print text on blank pages when the stamp function prints text.

[Blank Page Print Settings]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▶▶ [Blank Page Print Settings].
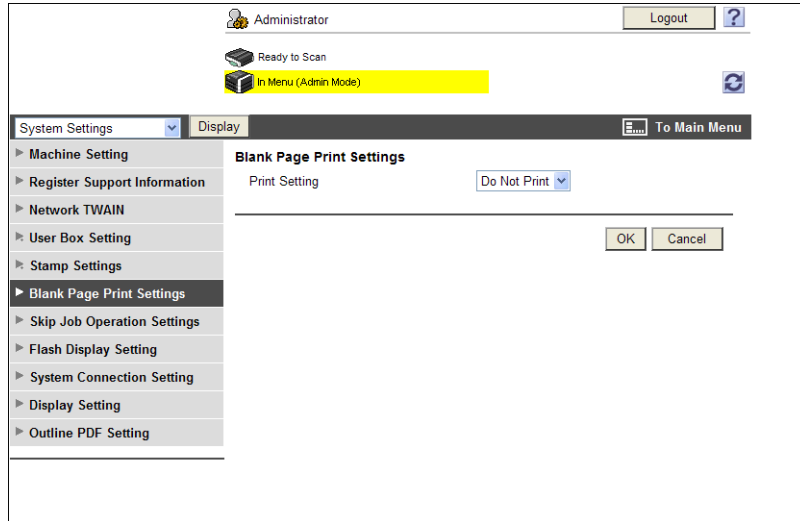
Item	Description
[Print Setting]	Specify whether to print text on blank pages when the stamp function prints text.

10.17   Configuring settings for skipping jobs

Configure settings for skipping jobs.

When the job currently being printed is being halted with a warning message stating the paper is empty, the mailbin has overflowed, or there is no matching paper, you can configure the machine to skip the job and print the next job waiting to be printed if it is eligible for printing.

Two settings are provided: One allows you to specify whether to skip the job when the next job is a fax; the other allows you to specify whether to skip the job when the next job is not a fax.

[Skip Job Operation Settings]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▸▸ [Skip Job Operation Settings].
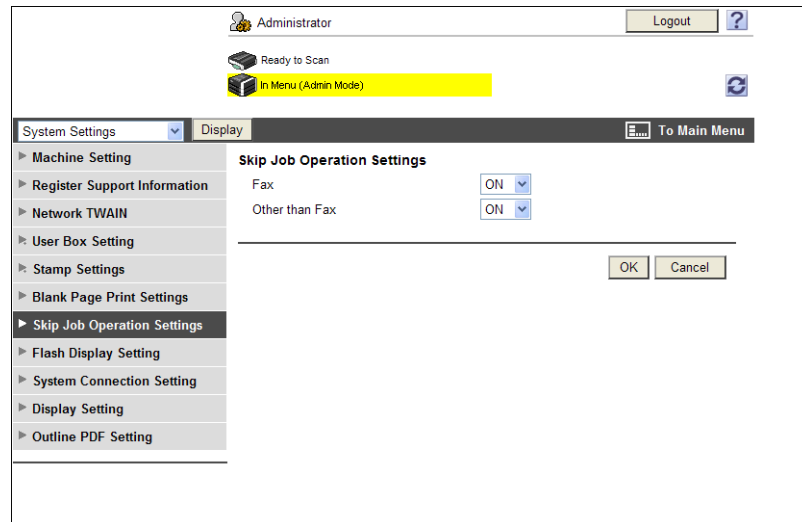
Item	Description
[Fax]	Specify whether to skip the job when the next job is a fax.
[Other than Fax]	Specify whether to skip the job when the next job is not a fax.

10.18   Configuring Outline PDF Settings

Configure settings to outline graphics when creating an outline PDF.

📖 **Reference**

For details on outline PDF, refer to the [User's Guide Network Scan/Fax/Network Fax Operations].

[Outline PDF Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings]▶▶[Outline PDF Setting].
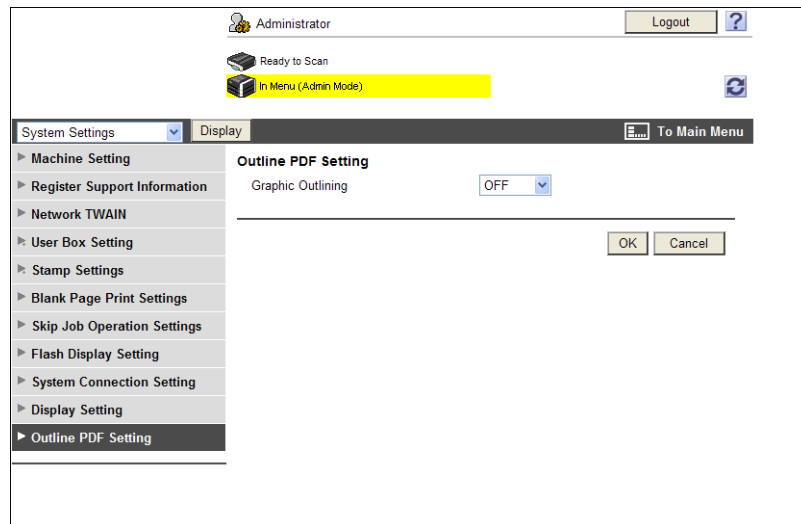
Item	Description
[Graphic Outlining]	Specify the level to scan a graphic (line image) when creating an outline PDF. The graphic (line image) outlining level becomes higher in the order of [LOW], [MIDDLE], and [HIGH]. If [OFF] is specified, the target graphic (line image) will not be outlined.

11 Registering

11   Registering

11.1   Registering Font or Macro

You can register or delete fonts or macros to or from this machine.

Reference

- This function is available only when a **Hard Disk** is installed.

[Edit Font/Macro]

In the administrator mode of **PageScope Web Connection**, select [Maintenance] ►► [Edit Font/Macro].
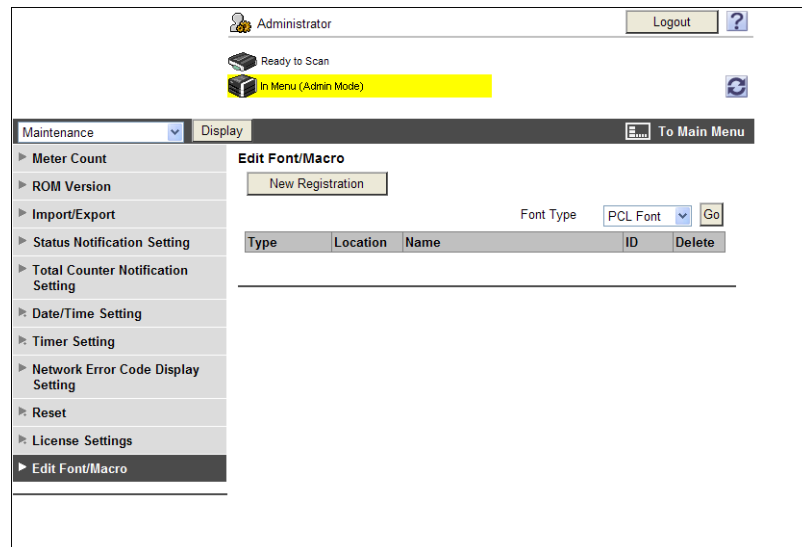
Item	Description
[New Registration]	Click this button to add a font or macro.
[Font Type]	Select a type of font or macro and click [Go], and the list of fonts or macro of the selected type is displayed.
[Type]	Displays the type of each registered font/macro.
[Location]	Displays the location to save the registered font or macro.
[Name]	Displays the name of the registered font or macro.
[ID]	Displays the ID of the registered font or macro.
[Delete]	Click this button to delete the selected font/macro.

[New Registration]

Item	Description
[Type]	Select a type of font/macro to be added.
[ID]	Enter the ID of the font/macro. This ID is required if you have set the [Type] to [PCL Font] or [PCL Macro] and if you have selected the [Manual Setting] check box. If you enter an ID that has already been used, the existing ID will be overwritten by it.
[Location]	Select the storage location of the font/macro.

11.2   Registering machine information

Register the administrator information and the address of this machine.

The registration of this machine is required for E-mail or Internet fax transmissions.

[Machine Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▶▶ [Machine Setting].

Item	Description
[Device Location]	Enter the installation location of this machine (up to 255 characters).
[Administrator Registration]	Register the administrator name and contact information of this machine.
[Administrator Name]	Enter the administrator name of this machine (up to 20 characters).
[E-mail Address]	Enter the E-mail address of the administrator (up to 128 characters). This setting is required for sending E-mail messages.
[Extension No.]	Enter the extension number of the administrator (up to eight characters).
[Input Machine Address]	Register the device name and E-mail address of this machine.
[Device Name]	Enter the device name (up to 80 characters). This name is used as a part of an Internet fax subject name.
[E-mail Address]	Enter the E-mail address of this machine (up to 320 characters). This setting is required when sending Internet faxes.

11.3   Registering support information

Register the support information for this machine.

To display this information, select [Information]►►[Online Assistance] in the user mode.

[Register Support Information]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [Register Support Information].

Item	Description
[Contact Name]	Enter the contact name for the machine (up to 63 characters).
[Contact Information]	Enter the contact name information for the machine such as the phone number and URL (up to 127 characters).
[Product Help URL]	Enter the URL of the Web page for product information (up to 127 characters).
[Corporate URL]	Enter the URL of the Web page for the manufacturer (up to 127 characters).
[Supplies and Accessories]	Enter consumables supplier information (up to 127 characters).
[Online Help URL]	Enter the online help URL (up to 127 characters). http://www.pagescope.com/download/webconnection/onlinehelp/
[Driver URL]	Enter the driver storage location (up to 127 characters).
[Engine Serial Number]	Displays the serial number of this machine.

11.4   Register Header/Footer Program

Register the header/footer program.

When copying a document, you can call the header/footer program registered in this item, and print a text or date/time at the top or bottom of the specified pages.

[Header/Footer Registration]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [Stamp Settings] ►► [Header/Footer Registration] ►► [Edit].

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the registered name (up to 16 characters).
[Color]	Select the header or footer color. Color setting is effective for scanned data. Scanned data is printed in black and white in this machine.
[Pages]	Specify whether to print the header or footer only on the first page or all pages.
[Size]	Specify the character size used for the header or footer.
[Text Type]	Specify the character font used for printing.
[Date/Time Setting]	Select the respective display formats for date and time. You can make a selection when [Date/Time Setting] of either [Header] or [Footer] is set to [Print].
[Distribution Number]	Enter the text to be added to the distribution numbers and printed (up to 20 characters). Specify the output method and start number of the distribution numbers. When [Number only] is selected for the output method, two-digit distribution numbers are displayed in two digits. If [Put zeros in front (total 8-digits)] is selected, the numbers are always displayed in eight digits regardless of the specified number of digits. You can make a selection when [Distribution Number] of either [Header] or [Footer] is set to [Print].

Item	Description
[Header]/[Footer]	Specify whether to print the following items. • [Header String]/[Footer String](Up to 40 characters) • [Date/Time Setting] • [Distribution Number] • [Job Number] • [Serial Number] (Engine serial No. of this machine) • [User Name/Account Name] To print a distribution number, specify the desired number in [Distribution Number]. If user authentication or account track is not enabled, data will not be printed even when [User Name/Account Name] is set to [Print].

11.5   Registering Address Book

You can register or edit an address, and register an icon.

If a frequently used destination is registered in the address book, you can specify it and easily send a document. You can also register an icon in the address book.

[Store Address]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▶▶ [Address Book] ▶▶ [Store Address].
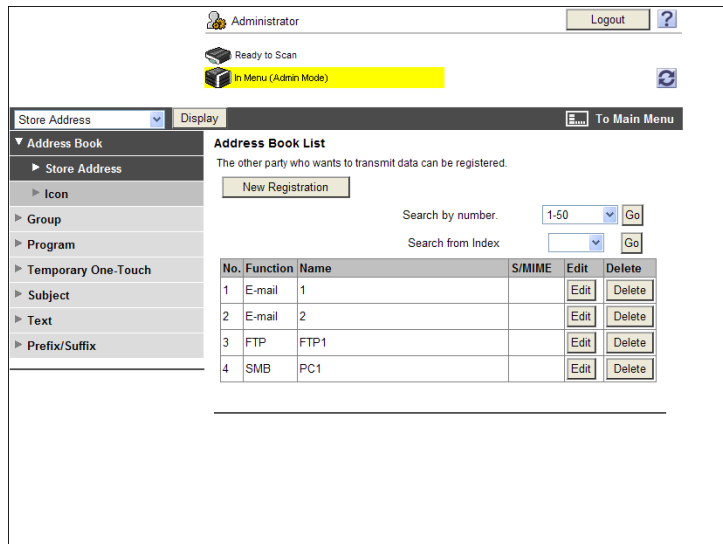
Item	Description
[New Registration]	Add new destinations to the address book.
[Search by number.]	Select a range of registration numbers, and then click [Go] to display the list of destinations in the selected range.
[Search from Index]	Select an index, and then click [Go] to display the list of addresses with the selected index.
[No.]	Displays the registration number.
[Function]	Displays the registered functions.
[Name]	Displays the registered name.
[S/MIME]	Displays whether a certificate is registered with the E-mail address.
[Edit]	Click this button to edit the registered address. The available items are the same as those for registration.
[Delete]	Delete an address from the address book.

Reference
- [S/MIME] is displayed only when a **Hard Disk** is installed.

[New Registration]▶▶[E-mail]

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[E-mail Address]	Enter the E-mail address of the destination (up to 320 characters).

Item	Description
[Registration of Certifi-cation Information]	Select this check box to register certificate information. Click [Browse] to specify the certificate to be registered. Certificate informa-tion is supported only as a DER (Distinguished Encoding Rules) file. To delete the registered certificate information, select [Deletion of Certification Information]. You cannot register a certificate if the E-mail address of the destination does not match that of the certificate. Before registering a certificate, check that those E-mail addresses are the same.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destina-tions. Specify the access allowed level or reference allowed group required to ac-cess this destination.

Reference

- [Registration of Certification Information] is displayed only when a **Hard Disk** is installed.

[New Registration]▸▸[FTP]

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destina-tion.
[Host Address]	Enter the IP address of the destination FTP server. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.
[File Path]	Specify the destination directory (up to 127 bytes).
[User ID]	Enter the user ID to log in to the destination FTP server (up to 63 bytes).
[Password is changed.]	Select this check box to change the password. This item is displayed when editing the registered information.
[Password]	Enter the password to log in to the destination FTP server (up to 63 bytes, ex-cluding space and ").
[anonymous]	Select whether to allow anonymous users to access the FTP server.
[PASV Mode]	Select whether to communicate in PASV mode.
[Proxy]	Select whether to use a proxy server.
[Port No.]	Enter a port number.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destina-tions. Specify the access allowed level or reference allowed group required to ac-cess this destination.

[New Registration]▸▸[SMB]

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destina-tion.

Item	Description
[Host Address]	Enter the IP address of the destination computer. In the IPv4 environment, enter the IPv4 address, NetBIOS name, or host name. Enter the NetBIOS name in uppercase. If the DNS server has already been configured, you can enter the host name instead. For the host name, specify a fully-qualified domain name (FQDN). In the IPv6 environment, enter the IPv6 address or host name. If the DNS server has already been configured, you can enter the host name instead. However, you can also specify the host name in an environment without the DNS server when resolving the names using the LLMNR function while the destination computer is Windows Vista/Server 2008/7.
[File Path]	Specify the destination directory (up to 255 bytes).
[User ID]	Enter the user ID to log in to the destination computer (up to 127 bytes).
[Password is changed.]	Select this check box to change the password. This item is displayed when editing the registered information.
[Password]	Enter the password to log in to the destination computer (up to 127 bytes, excluding space and ").
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[New Registration]▸▸[WebDAV]

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[Host Address]	Enter the IP address of the destination WebDAV server. Format: *.*.*.* (Asterisk * can be 0 to 255) If the DNS server has already been configured, you can enter the host name instead. When using IPv6, you can specify the IPv6 address.
[File Path]	Specify the destination directory (up to 142 bytes).
[User ID]	Enter the user ID to log in to the destination WebDAV server (up to 63 bytes).
[Password is changed.]	Select this check box to change the password. This item is displayed when editing the registered information.
[Password]	Enter the password to log in to the destination WebDAV server (up to 63 bytes, excluding space and ").
[SSL Settings]	Select whether to use SSL for encryption.
[Proxy]	Select whether to use a proxy server.
[Port No.]	Enter a port number.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[New Registration]▸▸[User Box]

(Destinations can be registered only when a **Hard Disk** is installed.)

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.

Item	Description
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[User Box No.]	Select the box number of the destination User Box from User Boxes registered with this machine.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[New Registration]▶▶[Fax]

(This registration is available if the optional **Fax Kit FK-508** is installed.)

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[Destination]	Enter the fax number of the destination (up to 38 characters).
[Confirm Fax Number]	Enter the fax number again to prevent an incorrect fax number from being registered. This item is displayed when [Confirm Address (Register)] is [ON].
[Line Setting]	Select a line to be used. This item is available when two optional **Fax Kit FK-508** are installed.
[Communication Setting]	Click [Display] to display the current communication settings. Select whether to enable each of [V34 Off], [ECM Off], [International Communication] or [Check Destination].
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[New Registration]▶▶[IP Address Fax]

(Registration is possible when the IP address fax function is available.)

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[Destination Type]	Select the address format of the destination.
[Address]	Enter the IP address of the destination IP address fax machine. If [IP Address] is selected in [Destination Type], enter the IP address of the destination. When using IPv6, you can specify the IPv6 address. If [Host Name] is selected in [Destination Type], enter the host name of the destination. If the DNS server has already been configured, you can enter the host name instead. If [E-mail Address] is selected in [Destination Type], enter the E-mail address of the destination. If the DNS server has already been configured, you can enter the E-mail address instead.
[Port No.]	Enter a port number.

Item	Description
[Destination Machine Type]	Select whether the destination machine is a color or monochrome machine.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[New Registration]▶▶[Internet Fax]

(Registration is possible when the Internet fax function is available.)

Item	Description
[No.]	Specify the registration number of the destination. If you select [Direct Input], enter the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Index]	Select the index character used when searching for the destination. It is convenient to select the [Main] check box for a frequently used destination.
[E-mail Address]	Enter the E-mail address of the destination (up to 320 characters).
[Resolution]	Select a resolution the receiver machine supports.
[Paper Size]	Select a paper size the receiver machine supports.
[Compression Type]	Select a compression type the receiver machine supports.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

[Icon]

In the administrator mode of **PageScope Web Connection**, select [Store Address]▶▶[Address Book]▶▶[Icon]▶▶[Edit].
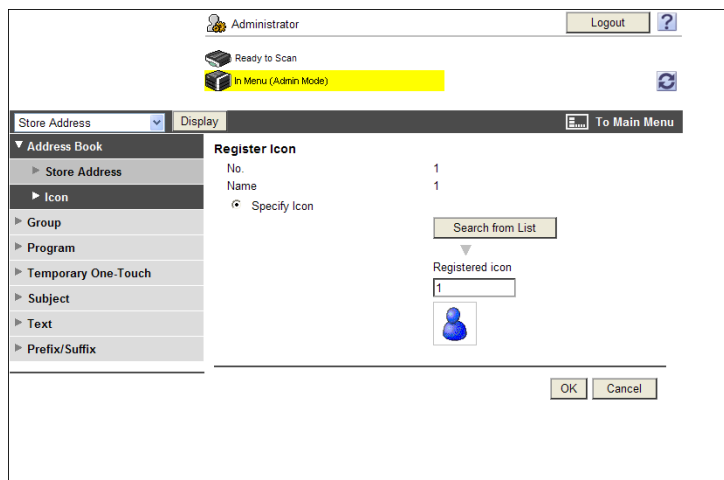
Item	Description
[No.]	Displays the registration number of the destination.
[Name]	Displays the name of the destination.
[Specify Icon]	Select [Specify Icon].
[Search from List]	Click this button to display the list of icons. Select the icon you want to register.

11.6   Registering a group

You can register or edit a group destination.

You can register one or more destinations as a group.

When you want to send (broadcast) the same data to multiple destinations, it is convenient to have those destinations registered as a group. To register a group, you must register the destinations to be added to the group in advance.

[Group]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▸▸ [Group].
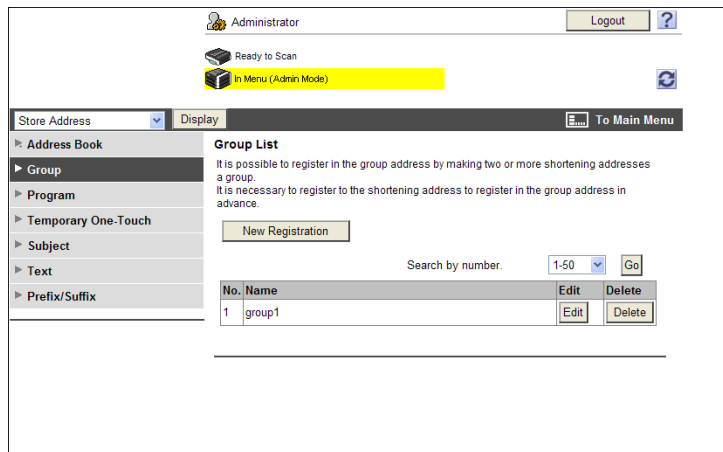
Item	Description
[New Registration]	Click this button to register a new group.
[Registration Number]	Select a range of registration numbers, and then click [Go] to display the list of destinations in the selected range.
[No.]	Displays the registration number.
[Name]	Displays the registered name.
[Edit]	Click this button to edit the registered group. The available items are the same as those for registration.
[Delete]	Click this button to delete the group.

[New Registration]

Item	Description
[Name]	Enter the destination name (up to 24 characters).
[Scan/Fax Address]	Click [Search from List] to display a list of the registered destinations. From the list of destinations in the address book, select the destinations you want to add to the group.
[Check Destination]	Check registered destinations.
[Specify Icon]	Click [Search from List], and then select an icon for a user you want to register from the displayed list.
[Limiting Access to Destinations]	Click [Display] to display the current settings for limiting access to destinations. Specify the access allowed level or reference allowed group required to access this destination.

11.7 Registering a program destination

You can register or edit a group destination.

You can register a combination of address information, communication information, and original information as a program destination.

[Program]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ►► [Program].
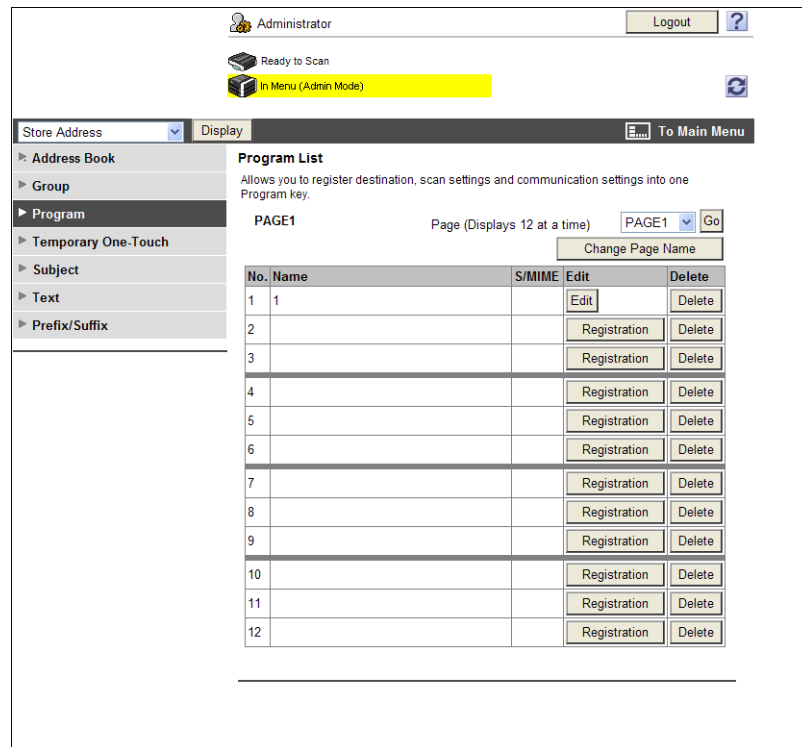
Item	Description
[Page (Displays 12 at a time)]	Select a page, and then click [Go] to display the list of destinations on the selected page.
[Change Page Name]	Change the page name.
[No.]	Displays the registration number.
[Name]	Displays the registered name.
[S/MIME]	Displays whether a certificate is registered with the E-mail address.
[Registration]	Register a new program destination.
[Edit]	Edit a registered program destination. The available items are the same as those for registration.
[Delete]	Delete the program destination.

Reference
- [S/MIME] is displayed only when a **Hard Disk** is installed.

[Registration]►►[E-mail]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).

Item	Description
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the E-mail destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Subject]	Specify the subject of the E-mail message. If you select [Not Specified], the default subject is used. Click [Subject List] to view the content.
[Text]	Specify the body text of the E-mail message. If you select [Not Specified], the default body text is used. Click [Text List] to view the content.
[File Attachment Setting]	Select whether to collectively attach all the divided files to one E-mail to send them (E-mail size: 200MB or less) or attach each file to one E-mail to send it (E-mail size: less than 400MB) when [Page Separation] is selected in [Page Setting]. When attaching each file to one E-mail, E-mails are sent by the number of divided files.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].

Item	Description
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▸▸[FTP]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and specify the FTP destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].

Item	Description
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▸▸[SMB]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the SMB address.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.

Item	Description
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▶▶[Stamp Settings]▶▶[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▶▶[WebDAV]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the Web-DAV destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].

Item	Description
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▸▸[User Box]

(Destinations can be registered only when a **Hard Disk** is installed.)

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the User Box destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.

Item	Description
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▶▶[Stamp Settings]▶▶[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▶▶[Fax]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the fax destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].

Item	Description
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[Timer TX]	Select whether to perform timer transmission. To perform timer transmission, enter the send time.
[Password TX]	Select whether to perform password transmission. To perform password transmission, enter the password.
[F-Code]	Select whether to use the F code for transmission. To use this function, enter the SUB address and password.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▸▸[IP Address Fax]

(Registration is possible when the IP address fax function is available.)

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the IP address fax.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.

Item	Description
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▶▶[Internet Fax]

(Registration is possible when the Internet fax function is available.)

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Select [Select from Address Book] or [Direct Input], and then specify the Internet fax destination.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[Subject]	Specify the subject of the E-mail message. If you select [Not Specified], the default subject is used. Click [Subject List] to view the content.
[Text]	Specify the body text of the E-mail message. If you select [Not Specified], the default body text is used. Click [Text List] to view the content.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.

Item	Description
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▶▶[Stamp Settings]▶▶[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▶▶[Group]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Destination Information]	Specify the destination. Click [Select from Address Book] to select the group to be registered as a program destination. Click [Check Destination] to check registered destinations.
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Subject]	Specify the subject of the E-mail message. If you select [Not Specified], the default subject is used. Click [Subject List] to view the content.
[Text]	Specify the body text of the E-mail message. If you select [Not Specified], the default body text is used. Click [Text List] to view the content.
[File Attachment Setting]	Select whether to collectively attach all the divided files to one E-mail to send them (E-mail size: 200MB or less), or to attach each file to one E-mail to send it (E-mail size: less than 400MB) when [Page Separation] is selected in [Page Setting]. When attaching each file to one E-mail, E-mails are sent by the number of divided files.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.

Item	Description
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].
[Timer TX]	Select whether to perform timer transmission. To perform timer transmission, enter the send time.
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▶▶[Stamp Settings]▶▶[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

[Registration]▶▶[No Destination]

Item	Description
[No.]	Displays the registration number.
[Name]	Enter the destination name (up to 24 characters).
[Resolution]	Select the resolution used for scanning the original.
[File Type]	Select the file type for saving scanned data.
[Outline PDF]	Select whether to use the outline PDF function when [Compact PDF] is selected in [File Type].
[File Name]	Enter the file name (up to 30 characters).
[Page Setting]	Select whether to save the whole scanned pages in one file, or to divide a file into specified number of pages when saving the data. To use the Page Separation function, enter the number of pages for each file. If the number of original pages is less than the setting of Page Separation, the original is saved as one file without being separated.
[Subject]	Specify the subject of the E-mail message. If you select [Not Specified], the default subject is used. Click [Subject List] to view the content.
[Text]	Specify the body text of the E-mail message. If you select [Not Specified], the default body text is used. Click [Text List] to view the content.
[File Attachment Setting]	Select whether to collectively attach all the divided files to one E-mail to send them (E-mail size: 200MB or less), or to attach each file to one E-mail to send it (E-mail size: less than 400MB) when [Page Separation] is selected in [Page Setting]. When attaching each file to one E-mail, E-mails are sent by the number of divided files.
[Simplex/Duplex]	Select whether to scan one side or both sides of the original. You can scan one side of the first page of the original, and then scan both sides of the remaining pages.
[Original Type]	Select the original quality, such as text or photo.
[Color]	Select a color mode. The file formats for saving data may be limited according to the color mode you select.
[Separate Scan]	Select whether to divide the original to scan.
[Density]	Select the density.
[Background Removal]	Adjust the density of the background.
[Scan Size]	Select the paper size of the original. If you select [Standard Size], select the size and the feed direction. If you select [Custom Size], specify the height and width.
[Application Setting]	Click [Display] to display the setting.
[E-mail Notification]	Specify whether to notify via E-mail the destination URL defined for saving scanned data. To notify the URL, specify the notification addresses. You can select the addresses from the list by clicking [Search from List].
[Timer TX]	Select whether to perform timer transmission. To perform timer transmission, enter the send time.
[Password TX]	Select whether to perform password transmission. To perform password transmission, enter the password.
[F-Code]	Select whether to use the F code for transmission. To use this function, enter the SUB address and password.
[Original Direction]	Select the orientation of the original.
[2-Sided Binding Direction]	Select the binding position of the original.
[Special Original]	If the original being sent is a mixed original (original with mixed page sizes), a Z-folded original (original folded in a zigzag shape), or a long original, select whichever is relevant.

Item	Description
[Book Scan]	Select whether to perform book copying. Using the book copy function enables you to divide page spreads (such as a book or catalog) into left and right pages to be scanned individually.
[Erase]	Select whether to erase frames. Using the frame erase function enables you to erase unwanted areas around the original, such as transmission information printed on received faxes and the shadows of punched holes.
[Compose(Date/Time)]	Specify whether to print the date and time data. To print the date and time data, configure the [Date Type], [Time Type], [Print Position], [Fine-Tune], [Color], [Pages], [Size], and [Text Type] settings.
[Compose(Page)]	Select whether to print page numbers. To print data, specify [Start], [Page Number Type], [Print Position], [Fine-Tune], [Color], [Size], and [Text Type].
[Compose(Header/Footer)]	Specify whether to print the header and footer. To print the header and footer, specify the registration number of the header and footer. Click [Confirm Registered Contents] to view the registered headers and footers. To specify a header or footer, you must select [System Settings]▸▸[Stamp Settings]▸▸[Header/Footer Registration] to pre-register the header or footer in this machine.
[Compose(Stamp)]	Select whether to print the stamp. To print the stamp, configure the stamp type ([Preset Stamp] or [Registered Stamp]), [Print Position], [Fine-Tune], [Color], [Pages], and [Size] settings. Click [Confirm Registered Contents] to check the registered stamp. To specify the registered stamp, you must register the stamp with this machine in advance.
[Stamp Combine Method]	Select the combine method for combining elements using [Compose(Stamp)] functions. You can select whether to insert the element as an image or text.
[Limiting Access to Destinations]	Click [Display] to display the setting. Specify the access allowed level or reference allowed group required to access this destination.

11.8   Registering Temporary One-Touch Destination

The Temporary One-Touch function temporarily registers destinations and the operating procedures of transmission.

Unlike program destinations, registration information of a temporary one-touch destination is deleted when transmitting data to the destination registered as a temporary one-touch, or turning off the power of this machine.

Reference
- You cannot register a temporary one-touch destination when [Security Settings]▸▸[Security Details]▸▸[Manual Destination Input] is set to [Restrict] in the [Administrator Setting] on the **Control Panel**.

[Temporary One-Touch]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▸▸ [Temporary One-Touch].

📖 **Reference**

The temporary one-touch destination to be registered is the same as the registered program address. However, [Registration of Certification Information] and [Limiting Access to Destinations] are not available for temporary one-touch destinations. For details on registration for temporary one-touch destinations, refer to page 11-13.

11.9   Registering the E-mail subject and body

Register the subject and message body used for sending E-mail messages or Internet faxes.

[Subject]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ►► [Subject] ►► [Edit].

Item	Description
[No.]	Displays the registration number.
[Subject]	Register the subject of the E-mail message (up to 96 bytes).

[Text]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ►► [Text] ►► [Edit].

Item	Description
[No.]	Displays the registration number.
[Text]	Register the E-mail body (up to 384 bytes).

11.10 Simplifying entering E-mail addresses

Register prefixes and suffixes to simplify entering E-mail addresses.

Registration of domain names and other data in Prefix/Suffix enables you to retrieve registered strings when entering an E-mail address, allowing the prompt address entry.

[Prefix/Suffix]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▶▶ [Prefix/Suffix] ▶▶ [Edit].

Item	Description
[No.]	Displays the registration number.
[Prefix]	Enter a Prefix (up to 20 characters).
[Suffix]	Enter a Suffix (up to 64 characters).

11.11   Using Data Management Utility

Manage copy protect data, stamp data, or font/macro data from a computer on the network using Data Management Utility of **PageScope Web Connection**.
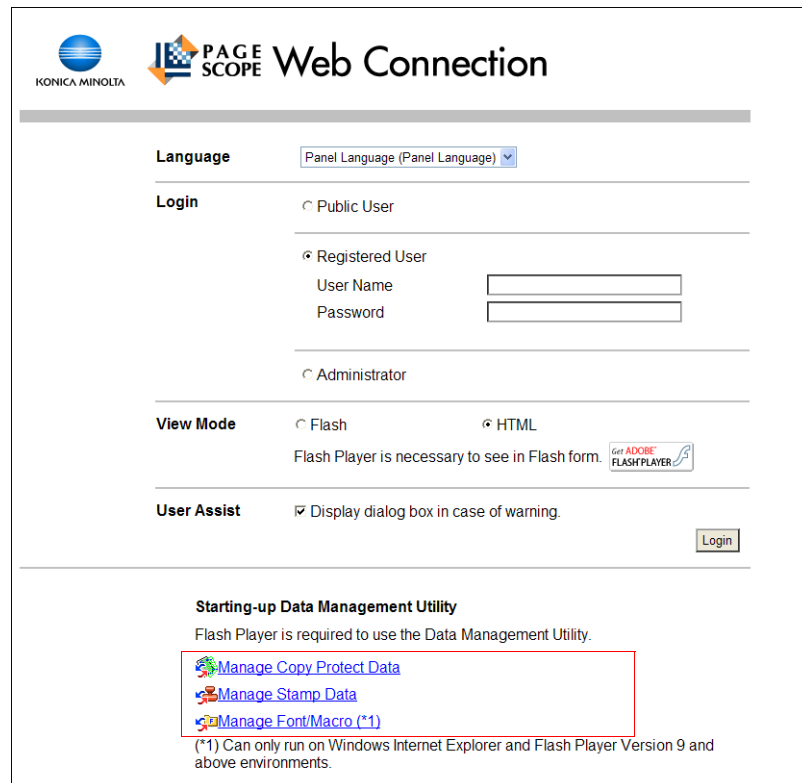
11.11.1   Starting up Data Management Utility

Start up Data Management Utility from the **PageScope Web Connection** login page.
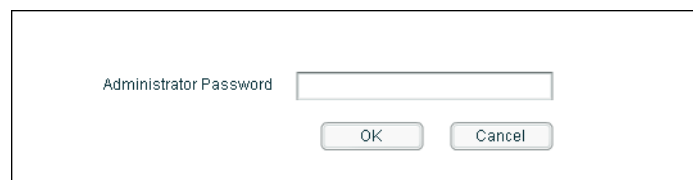
Reference

- To use Data Management Utility, install Flash Player.
- To manage font or macro data, install Flash Player Ver.9.0 or later using Internet Explorer.
- You cannot start up multiple Data Management Utilities at the same time.
- Manage Font/Macro is available only when a **Hard Disk** is installed.

1   In the login page, select the desired Data Management Utility.

2   Enter the administrator password of this machine.

Data Management Utility starts up.

📖 **Reference**
For details on [Manage Copy Protect Data], refer to page 11-32.

For details on [Manage Stamp Data], refer to page 11-34.

For details on [Manage Font/Macro], refer to page 11-36.

11.11.2 Managing copy protect data

Manage copy protect data to be added to this machine.

Copy Protect proves that a document is a copied one by highlighting a character string on the document when a printed or copied document has been recopied. This function is available when preventing highly confidential documents from being copied secondarily.

Reference
- You cannot edit or delete copy protect data that is registered in this machine at shipment.

[Copy Protect List]

When [Manage Copy Protect Data] starts up, the registered copy protect data is listed.

(You can register up to eight copy protect data items.)

Item	Description
[System]	The system menu appears. In the System menu, you can handle [Auto Protect Setting], [Export], [Import], or [Exit]. For details, refer to page 11-33.
?	Displays the help about [Manage Copy Protect Data].
[Edit]	Displays the copy protect editing screen. In this page, you can edit the registered copy protect data or register new one. For details, refer to page 11-33.
[Delete]	Deletes the registered copy protect data. Copy protect data is not displayed in the copy protect list page; however, data is not actually deleted until it is written to this machine by clicking [Export to the device]. To cancel data deletion, click [Undo] [Export to the device] is selected.
[Export to the device]	Writes copy protect data to this machine. After newly registering, editing, or deleting copy protect data, click [Export to the device]. If you do not click [Export to the device], the edited contents are not updated.
[Undo]	Discards the edited contents and return to the previous state.

[System]

In the System menu, you can handle [Auto Protect Setting], [Export], [Import], or [Exit].

Item	Description
[Auto Protect Setting]	Displays the window that prohibits operations when the specified time has elapsed after the user paused operations. This prevents a third person from handling the system without the user's permission if the user leaves the seat while displaying the setting page. To use the Auto Protect function, specify the timeout period ranging from a time the user paused operations to a time the Auto Protect page appears.
[Export]	Backs up (exports) copy protect data defined in this machine in a file. To export data, click [OK] in the Confirmation screen.
[Import]	Reads copy protect data backed up in a file, and writes (imports) its contents to this machine. To import data, specify the file to be imported, and click [OK]. If there is copy protect data currently edited, it will be overwritten by the imported copy protect data.
[Exit]	Exits the application. The Confirmation screen appears. Click [OK].

[Edit]

Edit copy protect data.

You can specify the text, font, character size and style, and rotation angle required to use Copy Protect. You can edit data while checking the result in the preview.

Item	Description
[Copy Protect Name]	Enter a copy protect name (up to 16 characters).
[Copy Protect Text]	Enter the text to be displayed as copy protect data (up to 32 characters).
[Font Name]	Specify the desired font for copy protect text.
[Font Size]	Specify the desired font size for copy protect text.
[Bold]	Select this check box to specify the bold type for copy protect text.
[Italic]	Select this check box to specify the Italic type for copy protect text.
[Rotation Angle]	Specify the rotation angle for a copy protect text. You can enter a slider or numeric value to adjust the text rotation angle in 1-degree steps.

11.11.3 Managing stamp Data

Manage stamp data to be added to this machine.

You can register or delete a stamp image in this machine.

Reference
- You cannot edit or delete stamp data that is registered in this machine at shipment.

[Stamp List]

When [Manage Stamp Data] starts up, the registered stamp data is listed.

(You can register up to eight stamp data items.)

Item	Description
[System]	The system menu appears. In the System menu, you can handle [Auto Protect Setting], [Export], [Import], or [Exit]. For details, refer to page 11-35.
[?]	Displays the help about [Manage Stamp Data].
[Edit]	Displays the stamp editing screen. In this page, you can edit the registered stamp data or register new one. For details, refer to page 11-35.
[Delete]	Deletes the registered stamp data. Copy protect data is not displayed in the copy protect list page; however, data is not actually deleted until it is written to this machine by clicking [Export to the device]. To cancel data deletion, click [Undo] [Export to the device] is selected.
[Export to the device]	Writes stamp data to this machine. After newly registering, editing, or deleting stamp data, click [Export to the device]. If you do not click [Export to the device], the edited contents are not updated.
[Undo]	Discards the edited contents and return to the previous state.

[System]

In the System menu, you can handle [Auto Protect Setting], [Export], [Import], or [Exit].

Item	Description
[Auto Protect Setting]	Displays the window that prohibits operations when the specified time has elapsed after the user paused operations. This prevents a third person from handling the system without the user's permission if the user leaves the seat while displaying the setting page. To use the Auto Protect function, specify the timeout period ranging from a time the user paused operations to a time the Auto Protect page appears.
[Export]	Backs up (exports) stamp data defined in this machine in a file. To export data, click [OK] in the Confirmation screen.
[Import]	Reads stamp data backed up in a file, and writes (imports) its contents to this machine. To import data, specify the file to be imported, and click [OK]. If there is stamp data currently edited, it is overwritten by the imported stamp data.
[Exit]	Exits the application. The Confirmation screen appears. Click [OK].

[Edit]

Edit stamp data.

You can specify an image and enlargement factor for stamp data. You can edit data while checking the result in the preview.
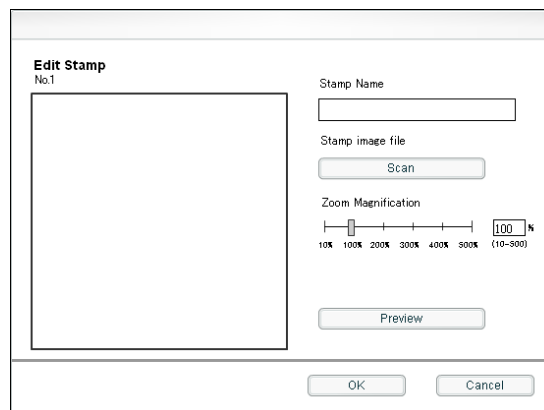
Item	Description
[Stamp Name]	Enter a stamp name (up to 16 characters).
[Stamp image file]	Click [Scan] to specify a bit map image to be used as a stamp, and click [OK].
[Zoom Magnification]	Specify the enlargement factor of a stamp image. You can enter a slider or numeric value to adjust the enlargement factor in steps of 1%.
[Preview]	Enlarges a stamp image. You can check the image details.

11.11.4   Managing font or macro

Manage font or macro data to be added to this machine.

You can register or delete fonts or macros to or from this machine.

Reference
- To manage font or macro data, install Flash Player Ver.9.0 or later using Internet Explorer.
- Manage Font/Macro is available only when a **Hard Disk** is installed.

[Font/Macro List]

When [Manage Font/Macro] starts up, the registered font or macro data is listed.
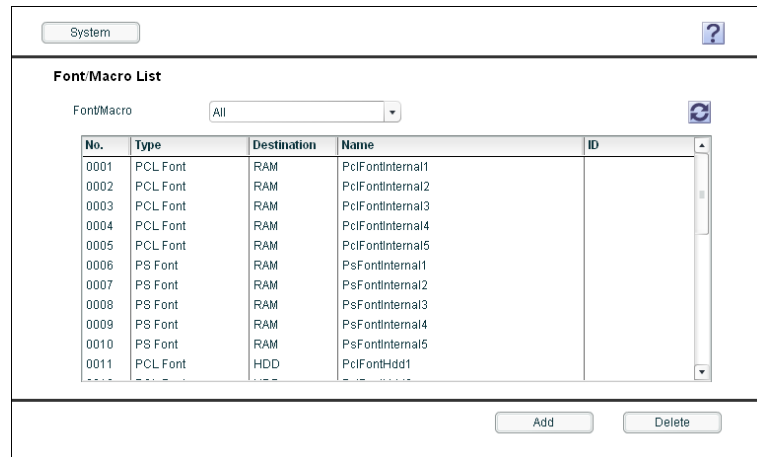
Item	Description
[System]	The system menu appears. In the System menu, you can handle [Auto Protect Setting] or [Exit]. For details, refer to page 11-37.
?	Displays the help about [Font/Macro List].
(refresh icon)	Refreshes the font or macro list.
[Font/Macro]	Toggles the display between the font and macro lists.
[No.]	Displays a font or macro number.
[Type]	Displays a font or macro type.
[Destination]	Displays where the font or macro data is saved.
[Name]	Displays a font or macro name.
[ID]	Displays a font or macro ID number for PCL font or PCL macro.
[Add]	Adds new font or macro data. For details, refer to page 11-37.
[Delete]	Deletes the registered font or macro data.

[System]

In the System menu, you can handle [Auto Protect Setting] or [Exit].

Item	Description
[Auto Protect Setting]	Displays the window that prohibits operations when the specified time has elapsed after the user paused operations. This prevents a third person from handling the system without the user's permission if the user leaves the seat while displaying the setting page. To use the Auto Protect function, specify the timeout period ranging from a time the user paused operations to a time the Auto Protect page appears.
[Exit]	Exits the application. The Confirmation screen appears. Click [OK].

[Add]

Add fonts or macros to this machine.

Item	Description
[Type]	Select a type of font or macro to be added.
[Destination]	Select where to save font or macro data. If data is saved in memory (RAM), it is deleted when this machine has been turned off. To continuously use font or macro data, save it in the HDD.
[ID]	Enter a font or macro ID number for PCL font or PCL macro. If it is not entered, the available ID is assigned automatically.
[Add File]	Click [Reference] to specify a font or macro file to be added to this machine.

12 Configuring Settings for User Box Functions

12   Configuring Settings for User Box Functions

12.1   Configuring the environmental settings for using User Boxes

Configure environmental settings for using User Boxes.

You can configure settings for deleting unused User Boxes, deleting documents saved in User Boxes, or using external memory functions.

[Delete Unused User Box]

Reference

● This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▶▶ [User Box Setting] ▶▶ [Delete Unused User Box].

Click [OK] to delete boxes containing no document.
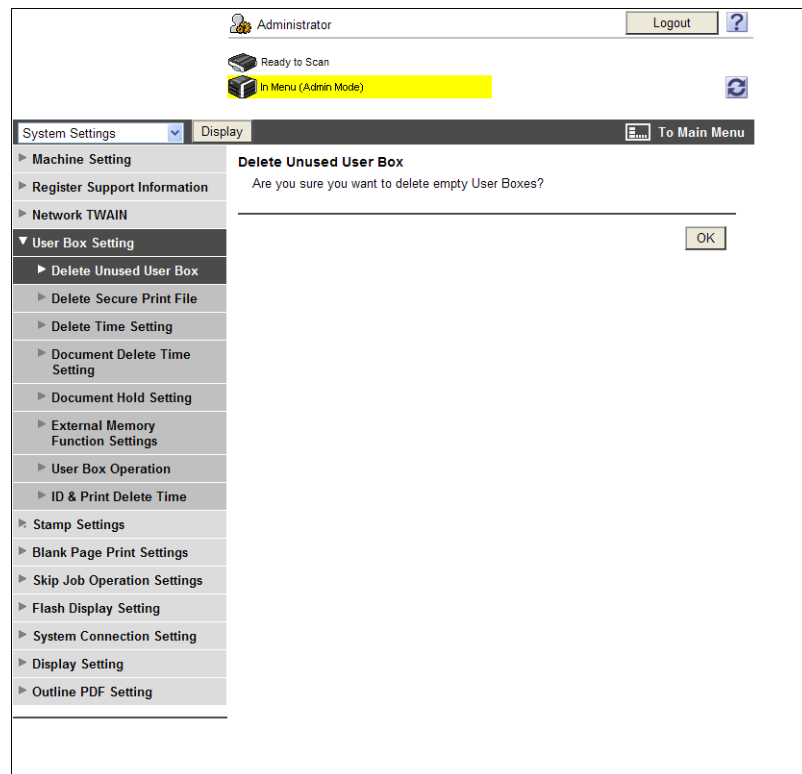
[Delete Secure Print File]

Reference

- This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [User Box Setting] ►► [Delete Secure Print File].

Click [OK] to delete documents stored in secure print User Boxes.
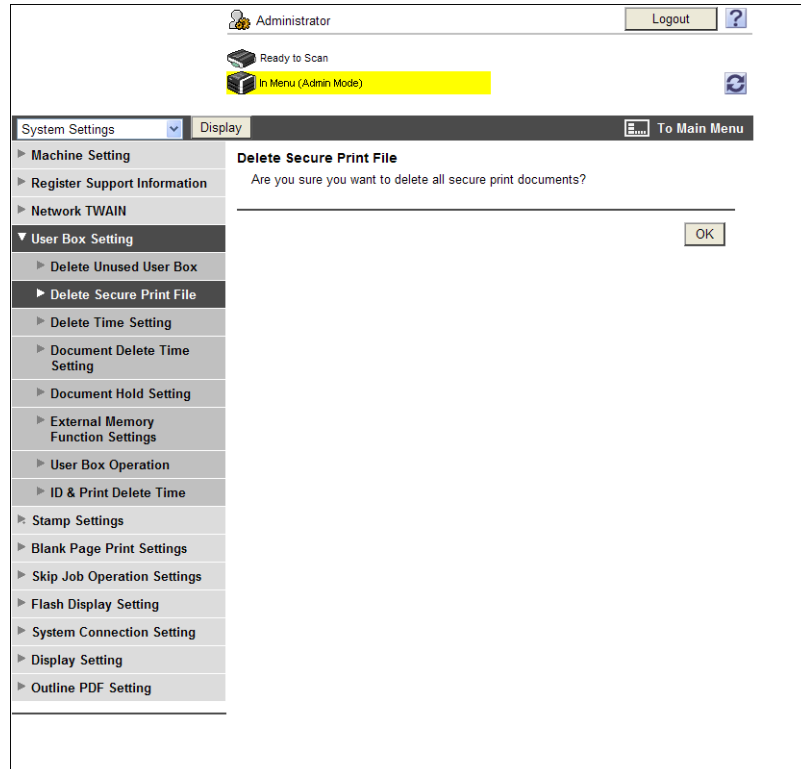
[Delete Time Setting]

Reference

● This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▸▸ [User Box Setting] ▸▸ [Delete Time Setting].

Item	Description
[Auto Delete Secure Document]	Select this check box to specify the time before the documents stored in the Secure Print User Box are to be deleted automatically.
[Specify days]	To specify the document deletion timing by day count, select [Specify days], and specify the number of days before the documents are stored in the Secure Document User Box are to be deleted automatically.
[Specify Time]	To specify the document deletion timing by hour count, select [Specify Time], and specify the number of hours before the documents stored in the Secure Document User Box are to be deleted automatically.
[ID & Print Delete Time]	Select this check box to specify the time before the documents stored in the ID & Print User Box are to be deleted automatically. If user authentication settings are not configured, this item will not be displayed.
[Specify days]	To specify the document deletion timing by day count, select [Specify days], and specify the number of days before the documents stored in the ID & Print User Box are to be deleted automatically. If you have specified not to delete documents stored in the ID & Print User Box after they are printed, the specified deleting timing will be reset. After the specified number of days has elapsed from the date of printing, the document will be deleted automatically.
[Specify Time]	To specify the document deletion timing by hour count, select [Specify Time], and specify the number of hours before the documents stored in the ID & Print User Box are to be deleted automatically. If you have specified not to delete documents stored in the ID & Print User Box after they are printed, the specified deleting timing will be reset. After the specified number of hours has elapsed from the time of printing, the document will be deleted automatically.

Reference
- Specify whether to delete documents stored in the ID & Print User Box after they are printed in [ID & Print Delete Time]. For details, refer to page 12-9.

[Document Delete Time Setting]

Reference
- This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [System Settings] ▶▶ [User Box Setting] ▶▶ [Document Delete Time Setting].

Item	Description
[Delete Setting]	Select whether to specify the time to delete documents in User Boxes. Specify the deletion timing. This setting is applied to all the documents in Public User Boxes, Personal User Boxes, and Group User Boxes. Select [ON] to change the document deletion timing of the registered User Boxes for which deletion timing is specified respectively to that specified in this setting. In this case, you cannot specify the time for the user to delete a document. The document deletion timing specified in this setting is also applied to newly created boxes. Only the administrator can change this setting.
[Do Not Delete]	Select this box when documents in User Boxes are not to be deleted.
[Specify days]	To specify the document deletion timing by day count, select [Specify days], and specify the number of days before the documents stored in User Boxes are to be deleted automatically. If you have specified not to delete documents stored in User Boxes after they are sent or printed, the specified deleting timing will be reset. After the specified number of days has elapsed from the date of transmission or printing, the document will be deleted automatically.
[Specify Time]	To specify the document deletion timing by hour count, select [Specify Time], and specify the number of hours before the documents stored in User Boxes are to be deleted automatically. If you have specified not to delete documents stored in User Boxes after they are sent or printed, the specified deleting timing will be reset. After the specified number of hours has elapsed from the date of transmission or printing, the document will be deleted automatically.

Reference

● Specify whether to delete documents stored in User Boxes after they are sent or printed in [Document Hold Setting]. For details, refer to page 12-6.

[Document Hold Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [User Box Setting] ►► [Document Hold Setting].
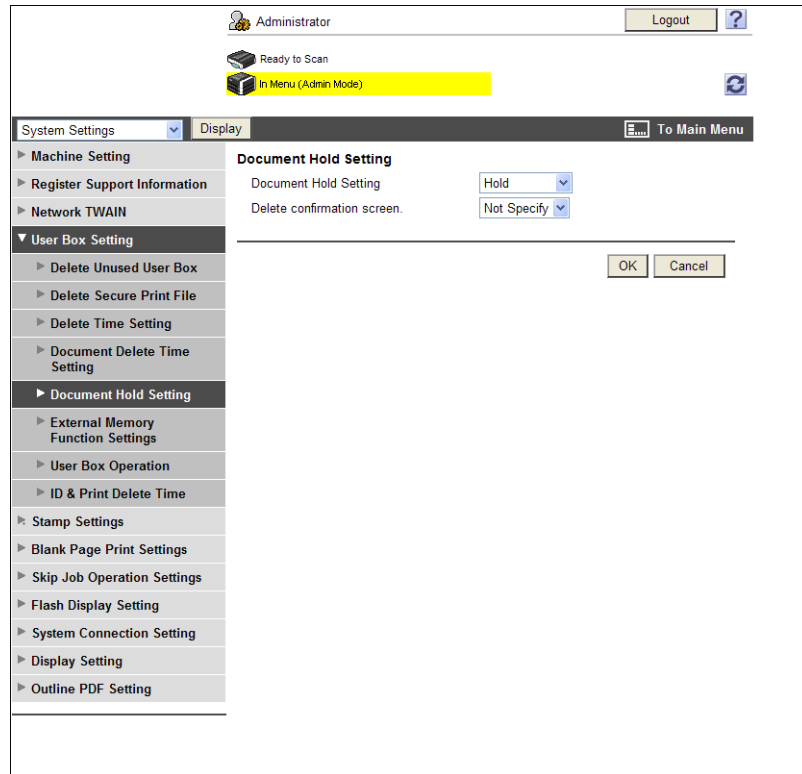
Item	Description
[Document Hold Setting]	Specify whether to automatically delete a document from a User Box after sending or printing it. When [Hold] is selected, the data of a document can be retained even after transmitting or printing the document.
[Delete confirmation screen.]	Specify whether to display the page for selecting whether to delete a document from a User Box after sending or printing it. This item is available when [Hold] is selected in [Document Hold Setting].

[External Memory Function Settings]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [User Box Setting] ►► [External Memory Function Settings].
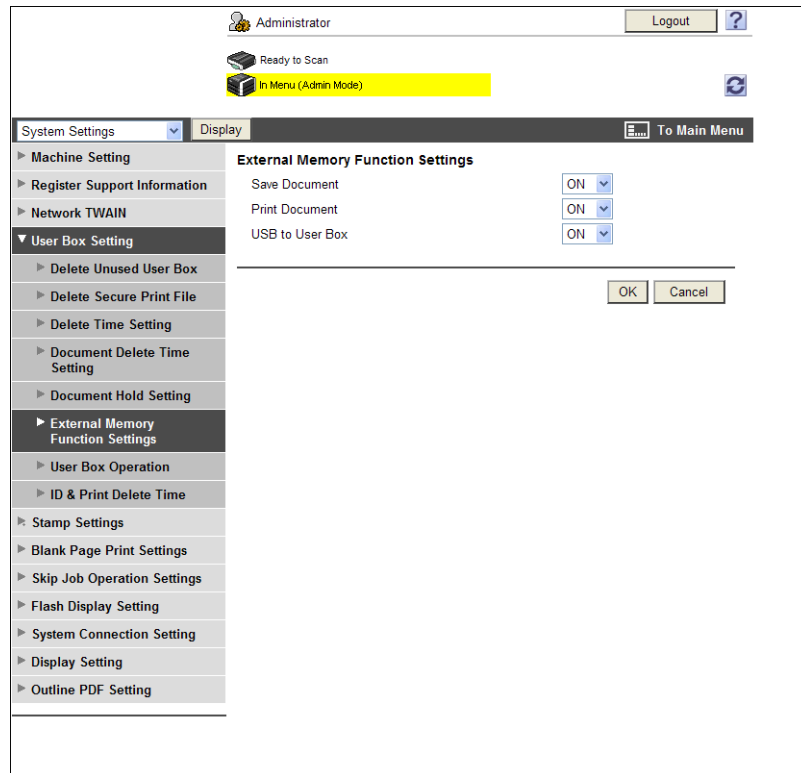
Item	Description
[Save Document]	Select [ON] when sending scanned data to external memory or sending data stored in a User Box to external memory. To prevent data from being stolen, [OFF] is selected as the default setting. Change it to [ON] to enable this function.
[Print Document]	To print data in external memory, select [ON]. You can print prints only the file formats supported by this machine.
[USB to User Box]	Select [ON] when saving data stored in external memory to a User Box.

Reference
- Do not disconnect the external memory device while handling it.
- To enable [Save Document] (sending data to external memory) and [USB to User Box] (saving data stored in external memory in a User Box), you must permit the use of the function for each user. For details, refer to page 7-6.
- [USB to User Box] is displayed only when a **Hard Disk** is installed.

[User Box Operation]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [User Box Setting] ►► [User Box Operation].
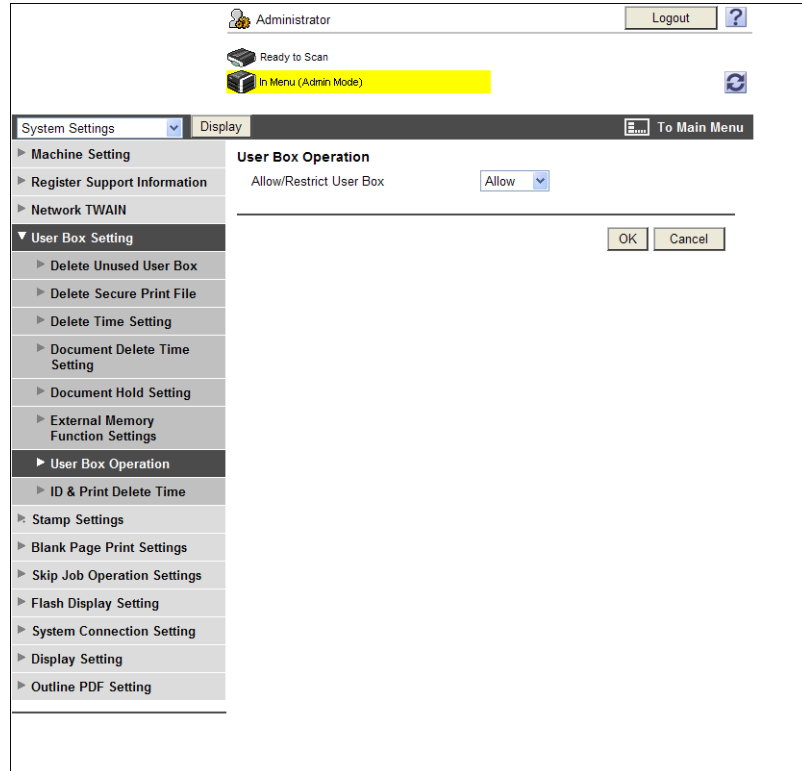
Item	Description
[Allow/Restrict User Box]	Select whether to grant the User Box operation permissions to users. Selecting [Restrict] disables users to create, edit or delete User Boxes.

[ID & Print Delete Time]

Reference

● This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [User Box Setting] ►► [ID & Print Delete Time].
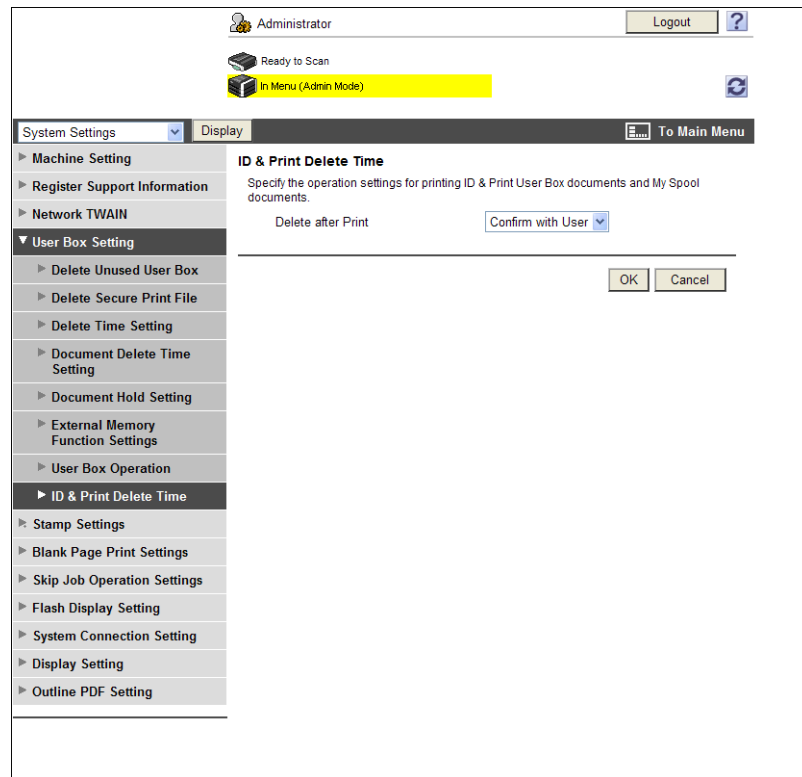
Item	Description
[Delete after Print]	Configure the post-print operation of documents in ID & Print User Boxes. Selecting [Confirm with User] displays a confirmation message, asking whether to delete the document that has been printed. Selecting [Always Delete] automatically deletes the document after printing.

12.2   Specifying the maximum number of Public User Boxes

Specify the maximum number of Public User Boxes.

Reference

●   This function is available only when a **Hard Disk** is installed.

[Public User Box Setting]

In the administrator mode of **PageScope Web Connection**, select [User Auth/Account Track] ►► [Public User Box Setting].
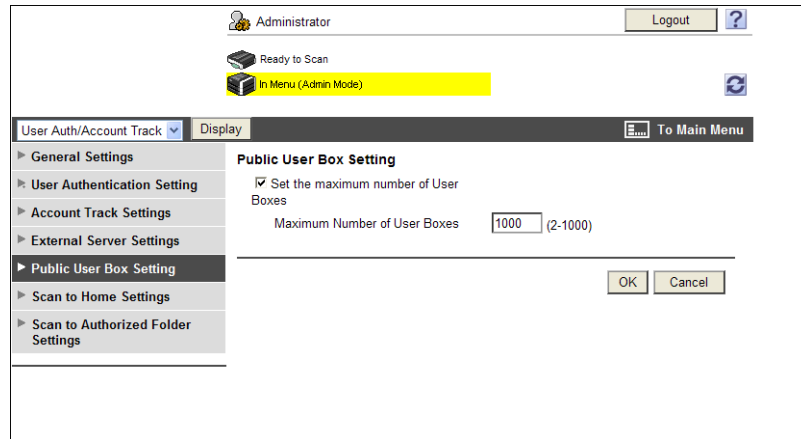
Item	Description
[Set the maximum number of User Boxes]	Select this check box to specify the maximum number of Public User Boxes.
[Maximum Number of User Boxes]	Enter the maximum number of Public User Boxes (in units of pieces).

12.3   Changing User Box settings

You can change settings of created User Boxes or delete them.

In the administrator mode, you can change the settings of a User Box or delete a User Box without entering the User Box password.

📖 **Reference**

Use the user mode to handle documents in User Boxes. For details, refer to the [User's Guide Box Operations].

[Open User Box]

Reference

● This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [Box]▶▶[Open User Box], and specify the User Box to change settings.

Item	Description
[User Box Setting]	Change the User Box settings. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected a Personal User Box.
[Delete User Box]	Delete User Boxes. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected a Personal User Box.

[User Box Setting]

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Index]	Select the indexing characters.
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically. This item is available when [Delete Setting] is set to [ON] in [System Settings]▶▶[User Box Setting]▶▶[Document Delete Time Setting].
[User Box Expansion Function is changed.]	Select whether to add the confidential reception function to the User Box. If you add the function, enter the password (up to eight characters). This item appears when the optional **Fax Kit FK-508** is installed.

Item	Description
[User Box Password is changed.]	To change the User Box password, select this check box and then enter the new password (up to eight characters, excluding space and double quotation (")).
[User Box Owner is changed.]	To change the User Box owner, select this check box and then select the User Box Type. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected the Public User Box.

12.4   Creating new User Boxes

Enables to create a new User Box.

[Create User Box]

Reference

● This function is available only when a **Hard Disk** is installed.

In the administrator mode of **PageScope Web Connection**, select [Box] ►► [Create User Box].

Item	Description
[User Box Number]	Specify the User Box number to be created. If you have selected [Input directly], enter the box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Use Box Password.]	To use the User Box password, select this check box and then enter the password (up to eight characters, excluding space and double quotation (")).
[Index]	Select the indexing characters.
[Type]	Select the User Box type. If [Personal] is selected, specify the owner user name. If [Group] is selected, specify the owner account track name.
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically.
[User Box Expansion Function]	Click [Display] to display details of the User Box expansion function. Select whether to add the confidential reception function to the User Box. If you add the function, enter the password (up to eight characters). This item appears when the optional **Fax Kit FK-508** is installed.

Reference

● You cannot register a password less than eight characters when [Security Settings]▸[Security Details]▸[Password Rules] is set to [Enable] in the [Administrator Settings] on the **Control Panel**. If a user password containing less than eight characters has already been registered, change the password so that it contains eight characters before setting [Password Rules] to [Enable].

12.5   Changing System User Box settings

You can change settings of created System User Boxes (Bulletin Board User Boxes, Confidential RX User Boxes, Relay User Boxes or Annotation User Boxes) or delete them.

Reference
- If the optional **Fax Kit FK-508** is installed, Bulletin Board User Boxes and Relay User Boxes can be selected.
- Annotation User Box is available only when a **Hard Disk** is installed.
- The Confidential RX User Boxes are available when the optional **Fax Kit FK-508** is installed and a **Hard Disk** is not installed.

[Open System User Box]

In the administrator mode of **PageScope Web Connection**, select[Box]▶▶[Open System User Box], and specify the User Box to change settings.

(The following shows a page that is displayed when [Bulletin Board User Box] is selected)

Item	Description
[User Box Setting]	Change the User Box settings. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected a Personal User Box.
[Delete User Box]	Delete User Boxes. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected a Personal User Box.

[User Box Setting] (When [Bulletin Board User Box] is selected)

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically. This item is available when [Delete Setting] is set to [ON] in [System Settings]▶▶[User Box Setting]▶▶[Document Delete Time Setting].
[User Box Password is changed.]	To change the User Box password, select this check box and then enter the new password (up to eight characters, excluding space and double quotation (")).

Item	Description
[User Box Owner is changed.]	To change the User Box owner, select this check box and then select the User Box Type. When **PageScope Authentication Manager** is used for authentication and you are logged in to the administrator mode, this item will not appear if you have selected the Public User Box.

Reference
● [Auto Delete Document] is displayed only when a **Hard Disk** is installed.

[User Box Setting] (When [Confidential RX User Box] is selected)

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Communication Password is changed.]	To change the communication password, select this check box and then enter the new password (up to eight characters).
[User Box Password is changed.]	To change the user box password, select this check box and then enter the new password (up to eight characters).
[User Box Owner is changed.]	To change the User Box owner, select this check box and then select the User Box Type.

[User Box Setting] (When [Relay User Box] is selected)

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Relay Address]	Specify the relay address.
[Relay TX Password is changed]	To change the relay transmission password, select this check box and then enter the new password (up to eight characters).

[User Box Setting] (When [Annotation User Box] is selected)

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To print the numbers specified in the Annotation User Box without saving a document in the User Box, select [Do Not Keep]. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically.
[User Box Password is changed.]	To change the User Box password, select this check box and then enter the new password (up to eight characters, excluding space and double quotation (")).
[Change Count Up]	To change the count up, select the check box, and then select the count up. If the User Box contains documents, this item cannot be configured.
[Change Stamp Elements]	To change the stamp elements, select this check box, and then specify [Primary Field], [Secondary Field], [Date/Time Setting], [Print Position], [Density] and [Number Type].

12.6   Creating a new System User Box

Create new System User Boxes.

Reference

- If the optional **Fax Kit FK-508** is installed, Bulletin Board User Boxes and Relay User Boxes can be created.
- Annotation User Box can be created only when a **Hard Disk** is installed.
- If the optional **Fax Kit FK-508** is installed and a **Hard Disk** is not installed, the Confidential RX User Boxes can be created.

[Create System User Box]

In the administrator mode of **PageScope Web Connection**, select[Box]▶▶[Create System User Box], and specify the System User Box to be created.

(The following shows a page that is displayed when [Bulletin Board User Box] is selected)

[Bulletin Board User Box]

Item	Description
[User Box Number]	Specify the User Box number to be created. If you have selected [Input directly], enter the box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Use Box Password.]	To use the User Box password, select this check box and then enter the password (up to 8 characters, excluding space and ").
[Type]	Select the User Box type. If [Personal] is selected, specify the owner user name. If [Group] is selected, specify the owner account track name.
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically.

[Confidential RX User Box]

Item	Description
[User Box Number]	Displays the User Box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Use Box Password.]	To use the User Box password, select this check box and then enter the password (up to 8 characters, excluding space and ").
[Type]	Select the User Box type. If [Personal] is selected, specify the owner user name. If [Group] is selected, specify the owner account track name.
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically.
[Communication Password]	To set the communication password, enter the password (up to eight characters).
[Retype Communication Password]	Reenter the communication password for confirmation (up to eight characters).

[Relay User Box]

Item	Description
[User Box Number]	Specify the User Box number to be created. If you have selected [Input directly], enter the box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Relay Address]	Specify the relay address.
[Relay TX Password]	Enter the relay TX password (up to eight characters).
[Retype Relay TX Password]	Reenter the relay TX password for confirmation (up to eight characters).

[Annotation User Box]

Item	Description
[User Box Number]	Specify the User Box number to be created. If you have selected [Input directly], enter the box number.
[User Box Name]	Enter a User Box name (up to 20 characters).
[Use Box Password.]	To use the User Box password, select this check box and then enter the password (up to 8 characters, excluding space and ").
[Auto Delete Document]	Specify the time before documents in users boxes are deleted. Select [Do Not Delete] if you do not delete documents in User Boxes. To print the numbers specified in the Annotation User Box without saving a document in the User Box, select [Do Not Keep]. To specify the document deletion timing by day count, select [Specify days], and specify the number of days before documents are to be deleted automatically. To specify the document deletion timing by hours and minutes, select [Specify Time], and specify the time before documents are to be deleted automatically.
[Count Up]	Select the count up.
[Stamp Elements]	Specify [Primary Field], [Secondary Field], [Date/Time Setting], [Print Position], [Density], and [Number Type].

Reference
- You cannot register a password less than eight characters when [Security Settings]▸[Security Details]▸[Password Rules] is set to [Enable] in the [Administrator Settings] on the **Control Panel**. If a user password containing less than eight characters has already been registered, change the password so that it contains eight characters before setting [Password Rules] to [Enable].

13 Configuring Settings for Printer Function

13   Configuring Settings for Printer Function

13.1   Configuring initial settings for the printer function

Configure the initial settings for the printer function.

[Basic Setting]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ►► [Basic Setting].

Item	Description
[PDL Setting]	Select the printer definition language.
[Paper Tray]	Select the primary paper tray.
[Output Tray]	Select the primary output tray.
[2-Sided Print]	Select whether to print in the 2-sided print format.
[Bind Direction]	Select the binding position for 2-sided printing.
[Staple]	Select whether to staple printed sheets. To staple printed sheet, select the number of staples. The staple function is available only when the optional finisher is installed.
[Punch]	Select whether to punch printed sheets. To punch printed sheets, select the number of punched holes. The punch function is available only when the optional finisher and punch kit are installed.
[Number of Sets]	Enter the number of copies to be printed.
[Default Paper Size]	Select the paper size.
[Original Direction]	Select the orientation of an image to be printed.
[Spool Print Jobs in HDD before RIP]	Select whether to spool print jobs to HDD. This function can be specified only when a **Hard Disk** is installed.

Item	Description
[Banner Sheet Setting]	Select whether to print banner sheets for each print job. Printing banner sheets prevent mixing different printing materials.
[Banner Sheet Paper Tray]	Select the primary paper tray for printing banner sheets.
[No Matching Paper in Tray Setting]	Select the operation to be taken when there is no appropriate sized paper in the specified paper tray. Select [Switch Trays (Tray Priority)] to supply paper from a different paper tray. Select [Stop Printing (Tray Fixed)] to stop printing and display a warning message.
[A4/A3<->LTR/LGR Auto Switch]	Converts between inch and metric units. Select whether to print an A4 (Letter)/A3 (Ledger)-sized original by full size when a paper tray containing Letter (A4)/Ledger (A3)-sized paper is selected. Selecting [ON] forces full size printing, which may cause images be defective.
[Binding Direction Adjustment]	Select the binding position adjustment method used for 2-sided printing.
[Line Width Adjustment]	To adjust the line width so as to make thin lines and small letters easier to see, select the line breadth.
[Gray Background Text Correction]	To adjust the line width in gray scale background so as to make thin lines and small letters easier to see, select [ON]. Selecting [OFF] applies the [Line Width Adjustment] setting in gray scale background.

13.2   Configuring the initial settings for the PCL print function

Configure the initial settings for the PCL print function.

[PCL Setting]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ▸▸ [PCL Setting].

Item	Description
[Symbol Set]	Select the symbol set.
[Typeface]	Specify whether to select a font from internal fonts (resident fonts) or from downloaded fonts (download fonts) when the font being used is not specified.
[Font Size]	Specify either the font pitch or the font point size, depending on the selected typeface.
[Line/Page]	Enter the number of lines per page.
[CR/LF Mapping]	Select the CR/LF substitution method when printing text data.

13.3   Configuring the initial settings for the PS print function

Configure the initial settings for the PS print function.

[PS Setting]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ►► [PS Setting].
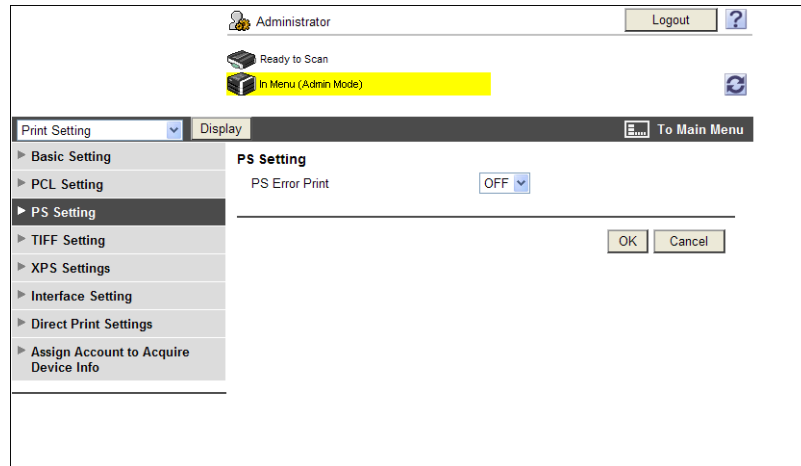
Item	Description
[PS Error Print]	Select whether to print error information when an error occurs during PS rasterization.

13.4   Configuring the initial settings for the TIFF print function

Select this option to configure how to determine the paper size when directly printing TIFF or JPEG image data.

The direct print function provides three modes: printing data using the direct print function, printing data in external memory, and printing data in a cellular phone or PDA.

[TIFF Setting]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ▶▶ [TIFF Setting].

Item	Description
[Auto Paper Select]	Configure how to determine the paper size when directly printing image data. [Auto]: For TIFF/JPEG (JFIF), select this option to calculate the size of the image based on its resolution and the number of pixels to print the image on paper that fits the image size. Select this option to print images on paper of the same size as the image. For JPEG (EXIF), an image is printed based on the paper size that is specified in [User Settings] of **Control Panel**▶▶[Printer Settings]▶▶[Paper Setting]▶▶[Paper Size]. An image is enlarged or reduced to fit the paper size. [Priority Paper Size]: When printing from a cellular phone or PDA, an image is printed based on the paper size that is specified in [User Settings] of **Control Panel**▶▶[Cellular Phone/PDA Setting]▶▶[Print]▶▶[Paper]. When using the direct print function of **PageScope Web Connection** or printing from the external memory, an image is printed based on the paper size that is specified in [User Settings] of **Control Panel**▶▶[Printer Settings]▶▶[Paper Setting]▶▶[Paper Size]. An image is enlarged or reduced to fit the paper size.

13.5   Configuring the initial settings for the XPS print function

Configure the initial settings for the XPS print function.

[XPS Settings]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ►► [XPS Settings].
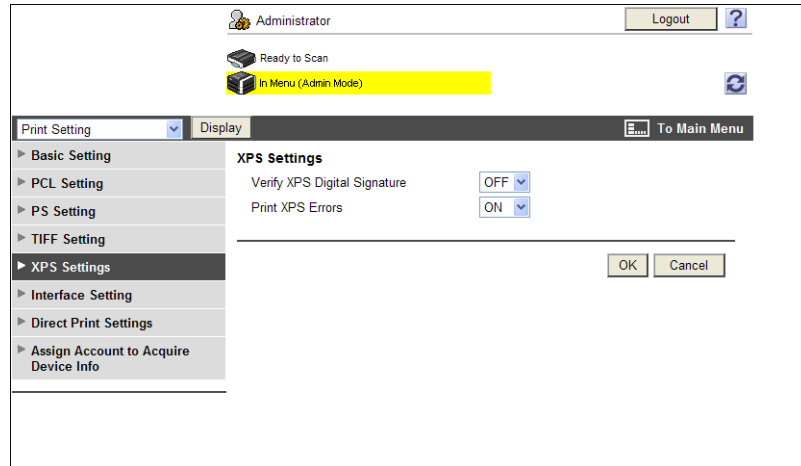
Item	Description
[Verify XPS Digital Signature]	Select whether to verify a digital signature when printing XPS data. Selecting [ON] prevents printing data whose signature is invalid.
[Print XPS Errors]	Select whether to print an error information when the digital signature of XPS data is invalid.

13.6 Specifying the timeout of the interface

Specify the timeout for interface.

[Interface Setting]

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ►► [Interface Setting].
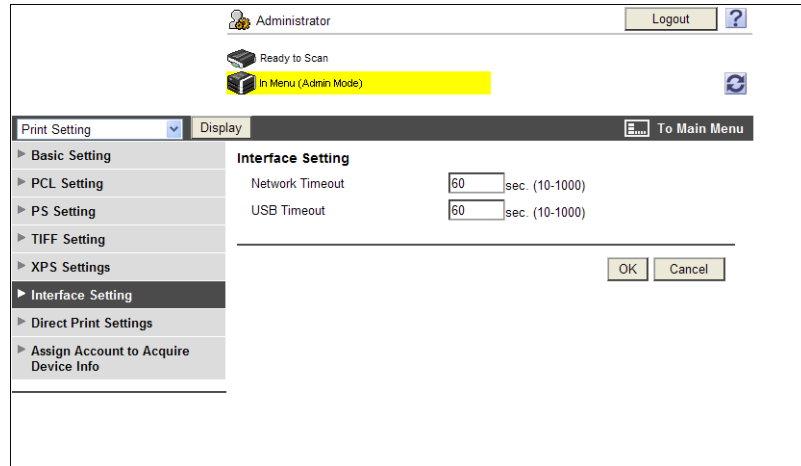
Item	Description
[Network Timeout]	Enter the timeout of network communication.
[USB Timeout]	Enter the timeout of USB communication.

13.7 Disabling the direct print function

You can disable the direct print function of **PageScope Web Connection** which is enabled by default.

Direct Print Settings

In the administrator mode of **PageScope Web Connection**, select [Print Setting] ►► [Direct Print Settings].
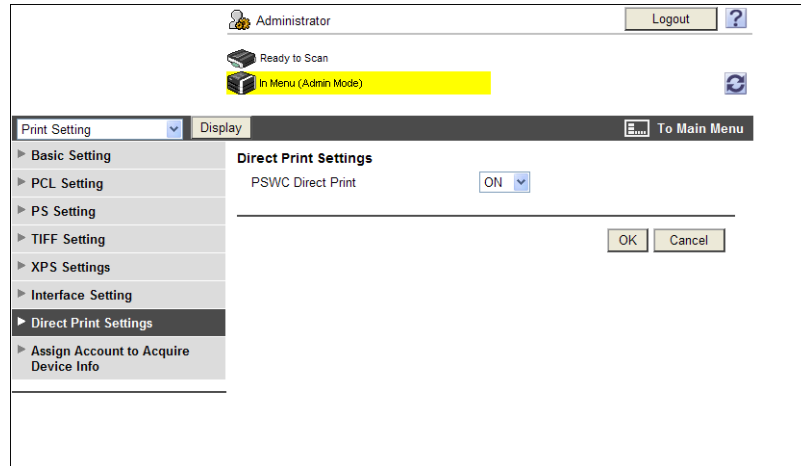
Item	Description
[PSWC Direct Print]	To disable using the direct print function, select "OFF".

13.8   Restricting users from obtaining device information using password

You can specify a password to obtain device information from the printer driver and restrict users from obtaining device information.

Reference

- For details on obtaining device information from the printer driver, refer to the [User's Guide Print Operations].

[Assign Account to Acquire Device Info]

In the administrator mode of **PageScope Web Connection**, select [Print Setting]▸▸[Assign Account to Acquire Device Info].
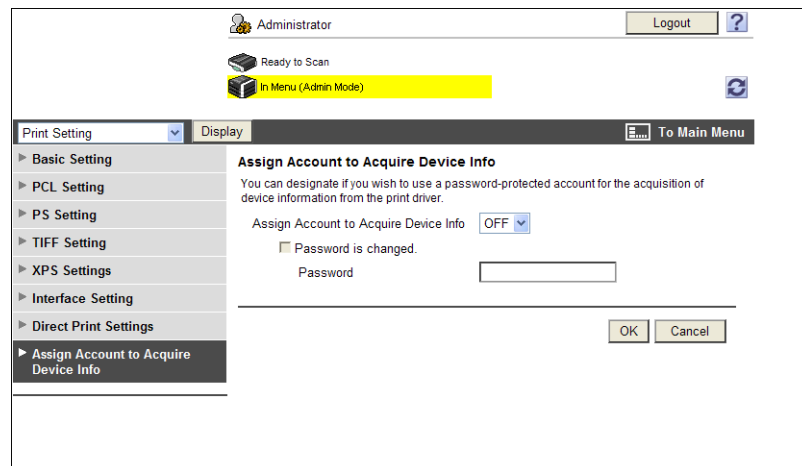
Item	Description
[Assign Account to Acquire Device Info]	Select [ON] when using a password to restrict users from obtaining device information from the printer driver.
[Password is changed.]	Select this check box to change the password.
[Password]	Enter a password (up to 8 characters, excluding space and ").

14 Configuring Settings for Fax Functions

14   Configuring Settings for Fax Functions

14.1   Configuring Settings to Print a Stamp when Sending a Fax

You can specify whether to cancel stamp setting when sending a fax.

[Fax TX Settings]

In the administrator mode of **PageScope Web Connection**, select [System Settings] ►► [Stamp Settings] ►►
[Fax TX Settings].
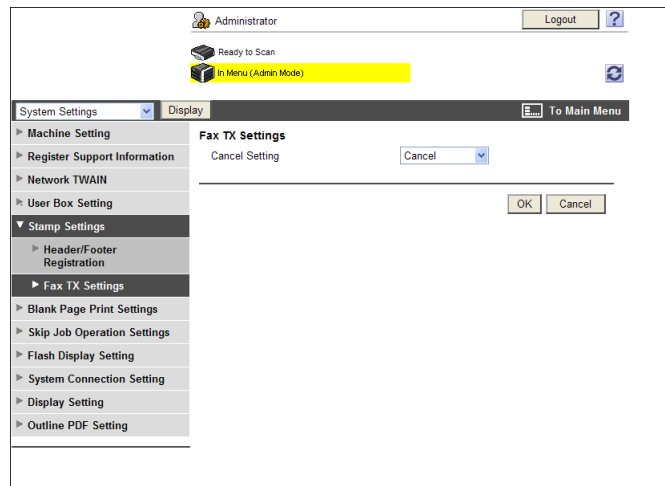
Item	Description
[Cancel Setting]	Specify whether to cancel stamp setting when sending a fax. Selecting [Cancel] sends faxes without printing the stamp on the originals.

14.2   Configuring Settings to Print the Header/Footer Position

Configure settings to print sender and reception information.

[Header/Footer Position]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▶▶ [Header/Footer Position].

Item	Description
[Header Position]	Specify the position of the sender information to be added on a fax document sent from this machine. The added sender information is printed as a part of the image on the document received by the recipient. If you select [OFF], the sender information will not be added. [OFF] is not displayed for Hong Kong or USA models.
[Print Receiver's Name]	Specify the items to be added as the sender information. If you select [ON], sender name, destination fax number (To: xxxxx), transmission start date and time, transmission number, and the number of pages are added as the sender information. If you select [OFF], sender name, fax ID of this machine, transmission start date and time, transmission number, and the number of pages are added as the sender information. This item is not displayed for Hong Kong or USA models.
[Footer Position]	Specify the position of the reception information (reception time and reception number) to be printed on a fax document received by this machine. If you select [OFF], the reception information will not be printed.

14.3   Configuring settings for telephone and fax lines

Configure settings related to telephone and fax lines including the telephone dialing method, fax receive mode, and number of incoming calls.

[Line Parameter Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▶▶ [Line Parameter Setting].

Item	Description
[Dialing Method]	Select a dialing method. Incorrect configuration of the dialing method may hamper a successful phone call.
[Receive Mode]	Select a receive mode. If you select [Auto RX], faxes are received automatically. If you expect frequent phone calls, for example if an external telephone is connected to this machine, set this mode to [Manual RX].
[Number of RX Call Rings]	Specify the number of quasi-ring back tone count between fax arrival and the start of reception.
[Number of Redials]	Specify the number of automatic redials when this machine cannot connect to the destination because the line is busy.
[Redial Interval]	Specify the interval of redials for automatic redialing.
[TEL/FAX Auto Switch]	Specify whether to automatically switch telephone and fax when an external telephone is connected to this machine. This item is displayed for Taiwan models.
[External Phone Monitor Call Sound]	Specify whether to output the telephone calling monitor sound from this machine when an external telephone is connected to this machine. This item is available when the [TEL/FAX Auto Switch] check box is selected.
[External Phone Call Time]	Specify the period from the time an incoming call is received to the time when an external telephone is called when an external telephone is connected to this machine. This item is available when the [TEL/FAX Auto Switch] check box is selected.
[External Phone Disconnection]	Specify whether to ring a connected external telephone when a fax is received. • [ON]: An external telephone does not ring when a fax is received. • [OFF]: An external telephone rings when a fax is received.
[Line Monitor Sound]	Specify whether to hear the line sound from the speaker during communication.
[Line Monitor Sound Volume (Send)]	Specify the speaker volume when sending a fax.

Item	Description
[Line Monitor Sound Volume (Receive)]	Specify the speaker volume when receiving a fax.

14.4   Configuring settings to send or receive faxes

Configure settings related to transmission and reception of faxes including file handling at the time of a polling transmission and printing method at the time of reception of a fax.

[TX/RX Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▸▸ [TX/RX Settings].

Item	Description
[Duplex Print (RX)]	Select whether to print a received fax on both side of sheets. This item is not available when [Print Separate Fax Pages] is set to [ON].
[Letter/Ledger over A4/A3]	Specify whether to use paper in inch-sized paper first when printing received faxes. This item is not displayed for Taiwan models.
[Print Paper Selection]	Select the priority order of paper trays used to print received faxes. If you select [Priority Size], received faxes are printed on paper of the prioritized size. If the prioritized size is not specified, received faxes are printed on paper of the nearest size. If you select [Fixed Size], received faxes are printed on paper of only the specified size. If [Tray Selection for RX Print] is set to other than [Auto], this item will be set to [Auto Select].
[Print Paper Size]	Select the size of paper used to print received faxes.
[Incorrect User Box No. Entry]	Select an action to be taken when the unregistered User Box number is specified when a fax is received by using User Boxes. This function can be specified only when a **Hard Disk** is installed.
[RX from Rejected Fax No.]	This item is not available.
[Tray Selection for RX Print]	If you want to fix the paper tray used to print received faxes, select the paper tray to be fixed. If [Print Paper Selection] is set to other than [Auto Select], this item will be set to [Auto].
[Min. Reduction for RX Print]	Specify a reduction ratio of received faxes. When a received fax does not fit within the standard paper size, this setting is used to adjust the size.
[Print Separate Fax Pages]	Select whether to divide a received fax into two or more pages when the document is larger than the standard paper size. This item is not available when [Duplex Print (RX)] is set to [ON].
[File After Polling TX]	Specify whether to delete a file after completing polling transmission of the file.
[No. of Sets (RX)]	If you need two or more sets of a received fax, specify the number of sets.

Item	Description
[Individual Receiving Line Setup]	Specify whether to receive a fax for each line. This item is available when two optional **Fax Kit FK-508** are installed. This item is not displayed when [Line 2 Setting] is set to [TX Only] in [Multi Line Settings].
[Individual Sender Line Setup]	Specify whether to register sender information for each line. This item is available when two optional **Fax Kit FK-508** are installed. This item is not displayed when [Line 2 Setting] is set to [RX Only] in [Multi Line Settings].

14.5 Configuring settings for the fax functions

Configure settings to use fax functions.

[Function ON/OFF Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ▸▸ [Function Setting] ▸▸ [Function ON/OFF Setting].
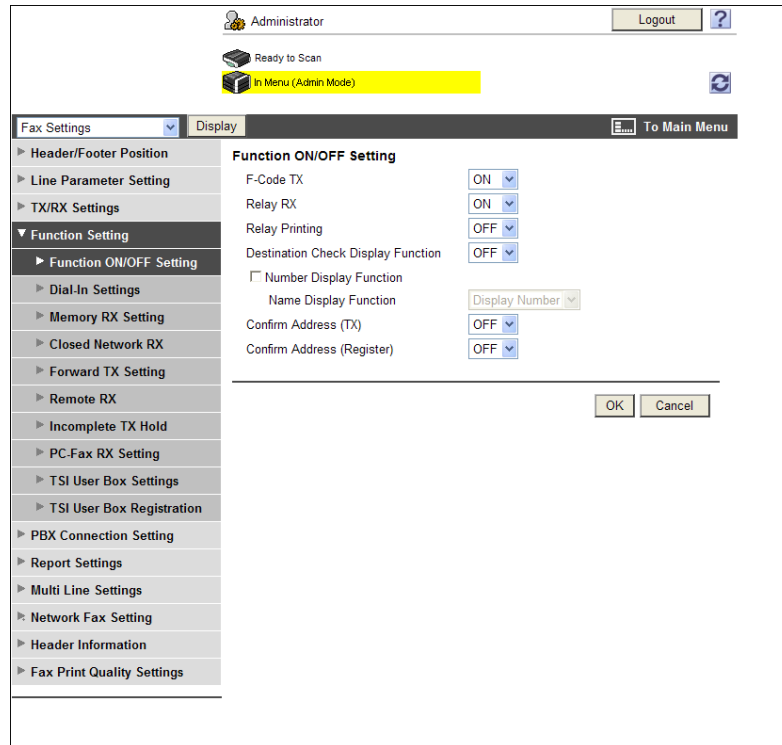
Item	Description
[F-Code TX]	Select whether to use the F-code transmission function. This function sends documents to a specific User Box of a remote machine by entering the SUB address and the sender ID. To use the F-Code for transmission, the remote machine must support the F-Code function.
[Relay RX]	Select whether to use this machine as a relay distribution station. A relay distribution station broadcasts documents received from a relay instruction station to the relay distribution destinations. To use the relay distribution function, you must register a relay User Box.
[Relay Printing]	Specify whether to print relayed documents after the relay distribution.
[Destination Check Display Function]	Select whether to display the list of the specified destinations when sending a fax.
[Number Display Function]	This item is not available.
[Name Display Function]	This item is not available.
[Confirm Address (TX)]	Specify whether to require re-entry of a fax destination for confirmation purposes when the user specifies the destination by directly entering the fax number. By having the user enter it twice, you can prevent the destination from being incorrectly entered.
[Confirm Address (Register)]	Specify whether to require re-entry of a fax destination for confirmation purposes when adding the destination with the address book. By having the user enter it twice, you can prevent the destination from being incorrectly entered and registered.

[Memory RX Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►► [Memory RX Setting].

Reference
- The Memory RX function stores received documents in the Memory RX User Box, and prints them when required.
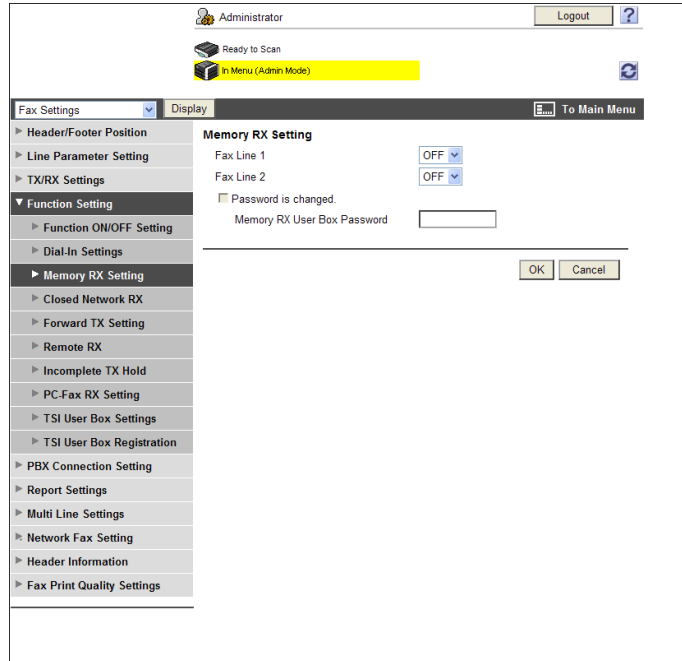
Item	Description
[Fax Line 1]	Select whether to perform the forced memory reception via fax line 1. This item is available when two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings].
[Fax Line 2]	Select whether to perform the forced memory reception via fax line 2. This item is available when two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings].
[Password is changed.]	Select this check box to change the password.
[Memory RX User Box Password]	Enter the password for the Memory RX User Box (up to eight characters).

[Closed Network RX]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►►
[Closed Network RX].

Reference

- The Closed area Rx function accepts only transmissions from recipient machines with a matching password. It is available only when the remote machine is one of our models and supports the closed network reception (with password) function.
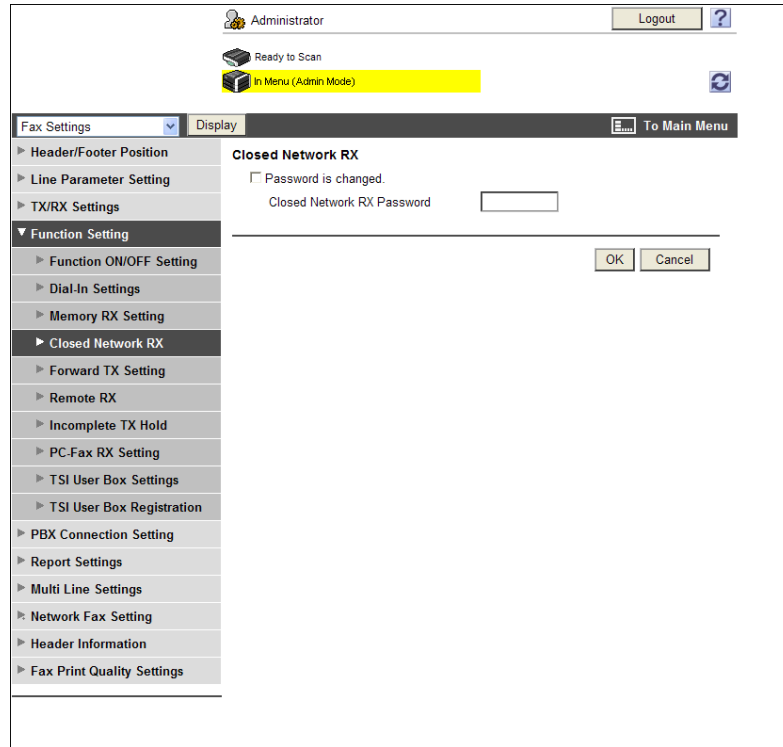
Item	Description
[Password is changed.]	Select this check box to change the password.
[Closed Network RX Password]	Enter the password for the closed network reception (four digits).

[Forward TX Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►► [Forward TX Setting].

Reference

- The Forward TX function transfers the received document to a pre-specified destination.
- This function cannot be configured together with [PC-Fax RX Setting], [TSI User Box Settings], or [Memory RX Setting].
- The Forward TX Setting can be configured for each line when receiving faxes for each line (two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings]).
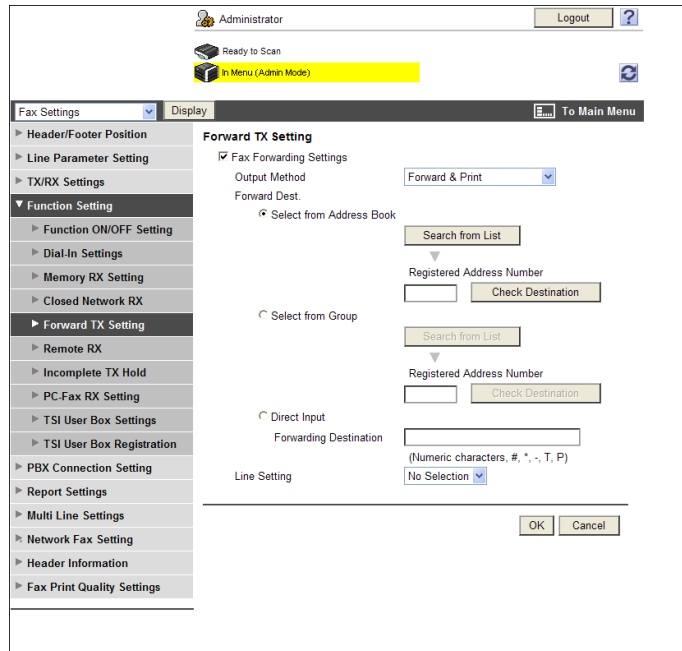
Item	Description
[Forward TX Setting]	Specify whether to use the forward transmission function.
[Output Method]	Select an output function. If [Forward & Print] is selected, received faxes are forwarded and printed on this machine. If [Forward & Print (If TX Fails)] is selected, received faxes are printed on this machine only when they cannot be forwarded.
[Forward Dest.]	Specify the forward destination of received faxes. Specify the destination using one of the three methods: [Select from Address Book], [Select from Group], and [Direct Input].
[Line Setting]	If two **Fax Kit FK-508** are installed, specify the line used to forward received faxes.

[Incomplete TX Hold]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►► [Incomplete TX Hold].

Reference

● The Fax Retransmit function temporarily saves documents, which were not sent within the specified number of times for attempts to send, in the fax retransmit User Box. You can use this function to open the fax retransmit User Box later to manually redial.
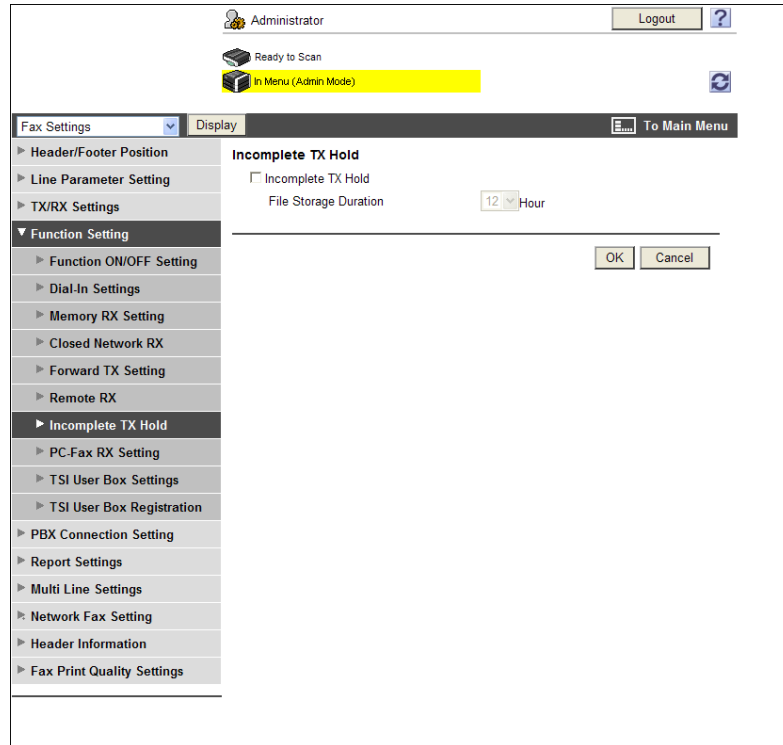
Item	Description
[Incomplete TX Hold]	Specify whether to temporarily retain the fax that even the auto-redialing function has failed to send for such reasons as a communications error or the recipient machine being busy, in the Fax Retransmit User Box.
[File Storage Duration]	Specify a duration to retain the file.

[PC-Fax RX Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►► [PC-Fax RX Setting].

Reference

- The PC-Fax RX function saves a document received as a fax in a User Box of this machine. You can print and send saved data. Data is saved in the Memory RX User Box or a specified User Box.
- This function cannot be configured together with [TSI User Box Settings], [Forward TX Setting], or [Memory RX Setting].
- The PC-Fax RX setting can be configured for each line when receiving faxes for each line (two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings]).

Item	Description
[PC-Fax RX Setting]	Specify whether to permit receiving PC-FAX.
[Receiving User Box Destination]	Select a receiving User Box destination of PC-FAX.
[Print]	Specify whether to print received faxes after completing the reception.
[Password Check]	Select this check box to check the password.
[Communication Password]	Enter the communication password. (up to eight characters)

[TSI User Box Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Setting] ►► [TSI User Box Settings].

Reference

- The TSI distribution function automatically distributes the document received with the sender fax number (TSI) to the forwarding destination specified for each sender.

- This function cannot be configured together with [PC-Fax RX Setting], [Forward TX Setting], or [Memory RX Setting].

- The TSI User Box Setting can be configured for each line when receiving faxes for each line (two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings]).

Item	Description
[TSI User Box Setting]	Select whether to enable the TSI distribution. This function distributes received faxes to each phone number based on the TSI (telephone numbers information) of the fax transmitter.
[Action when TSI User Box is not set.]	Select an action to be taken when receiving unregistered TSI information. If you select [Automatically & Print], the received document is printed. If you select [Memory RX User Box], the received document is saved in the Memory RX User Box. If you select [Specified Box] and specify a User Box in [Select from User Box No.], the received document is saved in the specified user box. For the destination User Box, a Public, Personal, or Group User Box can be specified. [Specified User Box] is displayed only when a **Hard Disk** is installed.
[Print]	Specify whether to print received faxes after completing the reception.

[TSI User Box Registration]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Function Settings] ►► [TSI User Box Registration] ►► [Create].

Reference

● The forwarding destinations can be registered for each line when receiving faxes for each line (two optional **Fax Kit FK-508** are installed while [Individual Receiving Line Setup] is set to [ON] in [TX/RX Settings]).

Item	Description
[No.]	Displays the registration number.
[Sender (TSI)]	Enter the fax ID of the sender (TSI: telephone numbers information).
[Forwarding Destination]	Specify forwarding destinations for each TSI. Specify the destination using one of the three methods: [Select from Address Book], [Select from Group], and [Select from User Box No.]. [Select from User Box No.] is displayed only when a **Hard Disk** is installed.

14.6   Configuring Settings for PBX Connection

Configure settings for PBX connection.

[PBX Connection Setting]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [PBX Connection Setting].

Item	Description
[PBX Connection Setting]	Select this check box when you connect this machine to a PBX line.
[Outside Line]	Enter the outside line number. When a fax number registered in the address book or a program destination is specified as an outside line, the outside line number specified in this setting is dialed prior to the fax number.

14.7 Configuring Settings to Output Fax Reports

Configure settings to output fax reports.

[Report Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Report Settings].

Item	Description
[Activity Report]	Select the output method of activity reports.
[Output Time Settings]	When you set the output timing of activity reports to [Daily] or [100/ Daily], specify the report output time.
[TX Result Report]	Select the output conditions for transmission result reports.
[Sequential TX Report]	Specify whether to print sequential transmission reports.
[Timer Reservation TX Report]	Specify whether to print timer reservation transmission reports.
[Confidential Rx Report]	Specify whether to print confidential reception reports.
[Bulletin TX Report]	Specify whether to print Bulletin transmission reports.
[Relay TX Result Report]	Specify whether to print relay transmission result reports.
[Relay Request Report]	Specify whether to print relay request reception reports.
[PC-Fax TX Error Report]	Specify whether to print PC-FAX transmission error reports.
[Broadcast Result Report]	Select the output method of broadcast result reports.
[TX Result Report Check]	Specify whether to view the transmission result report check pages.

Item	Description
Remark Column Print Setup	Configure settings to print remarks for activity reports. If you select [Normal Printing], the line status or sending setting will be printed. If User Authentication or Account Track is not enabled, the mode is set to [Normal Printing]. If you select [User Name Printing], the user name will be printed. This item is available when User Authentication is enabled. If you select [Account Name Printing], the account name will be printed. This item is available when Account Track is enabled.
[Network Fax RX Error Report]	Specify whether to print reception error reports when using the network fax function.
[MDN Message]	Specify whether to print a report when receiving the response to a MDN request.
[DSN Message]	Specify whether to print a report when receiving the response to a DSN request.
[Print E-mail Message Body]	Specify whether to print the message body of an E-mail message received successfully.

Reference

- The following functions are available only when a **Hard Disk** is installed.
  [Network Fax RX Error Report]
  [MDN Message]
  [DSN Message]
  [Print E-mail Message Body]

14.8   Using extension lines

If two **Fax Kit FK-508** are installed, configure settings for the second line.

[Multi Line Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Multi Line Settings].

Item	Description
[Line Parameter Set-ting]	Configure line parameters for the extension line.
[Dialing Method]	Select a dialing method for the extension line.
[Number of RX Call Rings]	Specify the number of quasi-ring back tone count between fax arrival and the start of reception.
[Line Monitor Sound]	Specify whether to hear the line sound from the speaker during communica-tion.
[Function Setting]	Configure settings for the extension line function.
[PC-FAX TX Setting]	Select the line used for PC-FAX transmission.
[Number Display Func-tion]	This item is not available.
[Name Display Func-tion]	This item is not available.
[Multi Line Usage Set-ting]	Configure the operation settings of Line 2 (an extension line).
[Line 2 Setting]	Specify the communication method for Line 2 (an extension line). You can specify [TX Only], [RX Only], or [TX and RX] for an extension line.
[Sender Fax No.]	Enter the fax ID (up to 20 characters, including + and space). Usually enter the fax number of the fax machine. The registered fax number is printed as the sender information on the fax re-ceived by the recipient.

14.9   Registering the Sender Name and Fax ID

You can register the sender name and fax ID of this machine.

Reference

● The sender name can be registered for each line when registering sender information for each line (two optional **Fax Kit FK-508** are installed while [Individual Sender Line Setup] is set to [ON] in [TX/RX Settings]).
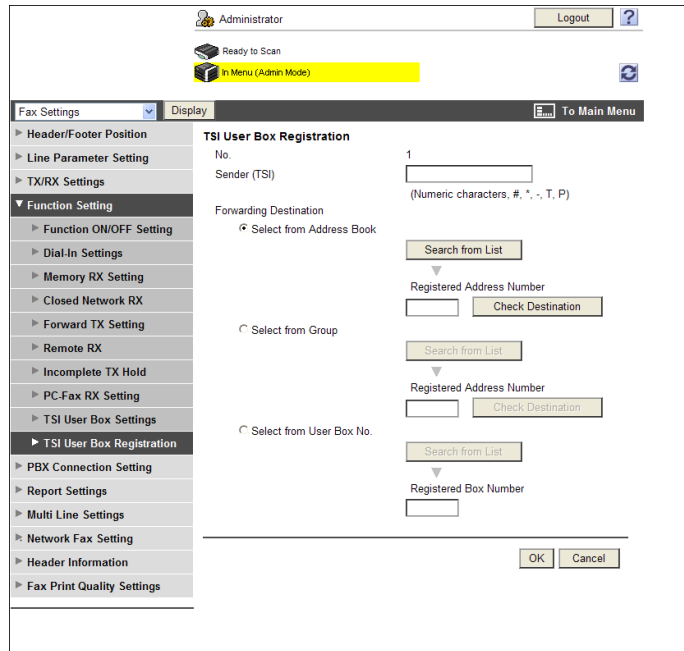
[Header Information]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings] ►► [Header Information].

Item	Description
[Sender Fax No.]	Enter the fax ID (up to 20 characters, including #, *, +, and space). Normally enter the fax number of this machine. This setting is not required when sending an Internet fax.
For 1 line: [Default] For 2 lines: [Line 1]	Specify the default sender name to be used for line 1. If the sender name is not specified when sending a fax, the default specified in this item is printed on an original.
[Line 2]	Specify the default sender name to be used for line 2. If the sender name is not specified when sending a fax, the default specified in this item is printed on an original. This item is available when two optional **Fax Kit FK-508** are installed while [Individual Sender Line Setup] is set to [ON] in [TX/RX Settings].
[Sender Name]	Displays the registered sender name.
[Edit]	Click this button to register or edit the sender name.
[Delete]	Click this button to delete the registered sender name.

[Edit]

Item	Description
[No.]	Displays the registration number.
[Sender Name]	Enter the sender name (up to 30 characters).

Reference
- The header position can be specified as required. If necessary, you can configure settings to prevent sender information from being printed. For details, refer to page 14-3.

14.10   Specifying fax print qualities

Specify whether to correct a received G3 fax according to the resolution.

[Fax Print Quality Settings]

In the administrator mode of **PageScope Web Connection**, select [Fax Settings]▶▶[Fax Print Quality Settings].

Item	Description
Low Resolution	Corrects a received document with low resolution (200 dpi × 100 dpi, 200 dpi × 200 dpi, and 300 dpi × 300 dpi). • [Prioritize Quality]: Corrects a received image and prints it. • [Prioritize Speed]: The print time is reduced because a received image is not corrected.
High Resolution	Corrects a document with high resolution (400 dpi × 400 dpi). • [Prioritize Quality]: Corrects a received image and prints it. • [Prioritize Speed]: The print time is reduced because a received image is not corrected.

14.11   Using a fax server

To use this machine with fax servers, register applications and servers using the applications.

You can register up to five applications and servers. You can also configure custom items for each registered application.

[Application Registration]

In the administrator mode of **PageScope Web Connection**, select [Store Address] ▸▸ [Application Registration] ▸▸ [Registration/Edit].

Reference

- The [Application Registration] menu is displayed when the optional **Fax Kit FK-508** is not installed.
- Only when the optional **Fax Kit FK-508** is not installed and the Internet fax function is disabled, registered applications can be displayed and operated from the **Control Panel** of this machine.

PageScope Web Connection provides the following templates. Each template provides different custom items predefined for each application.

[WalkUp Fax]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[Sender Name (CS)]	[Name]	[ASCII]	[Walkup]	–
2	[Fax Number (CS)]	[PersonalFaxNumber]	[ASCII]	–	–
3	[TEL Number (CS)]	[PersonalVoiceNumber]	[ASCII]	–	–
4	[Subject]	[Subject]	[ASCII]	–	–
5	[Billing Code 1]	[BillingCode1]	[ASCII]	–	–
6	[Billing Code 2]	[BillingCode2]	[ASCII]	–	–

[Fax with Account]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	–
2	[Sender Name (CS)]	[Name]	[ASCII]	–	–
3	[Password]	[Password]	[ASCII]	–	–
4	[Password Auth#]	[Authentication]	–	–	[None]
5	[Subject]	[Subject]	[ASCII]	–	–
6	[Billing Code 1]	[BillingCode1]	[ASCII]	–	–
7	[Billing Code 2]	[BillingCode2]	[ASCII]	–	–
8	[CoverSheet Type]	[CoverSheet]	–	–	–
9	[Hold For Preview]	[HoldForPreview]	–	–	[No]

[Secure Docs]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	–
2	[Password]	[Password]	[ASCII]	–	–
3	[Password Auth#]	[Authentication]	–	–	[None]
4	[Delivery Method]	[Delivery]	–	–	[Secure]
5	[Subject]	[Subject]	[ASCII]	–	–
6	[Billing Code 1]	[BillingCode1]	[ASCII]	–	–

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
7	[Billing Code 2]	[BillingCode2]	[ASCII]	–	–
8	[CoverSheet Type]	[CoverSheet]	–	–	–
9	[Document PW]	[DocumentPassword]	[ASCII]	–	–

[Certified Delivery]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	–
2	[Password]	[Password]	[ASCII]	–	–
3	[Password Auth#]	[Authentication]	–	–	[None]
4	[Delivery Method]	[Delivery]	–	–	[Certified]
5	[Subject]	[Subject]	[ASCII]	–	–
6	[Billing Code 1]	[BillingCode1]	[ASCII]	–	–
7	[Billing Code 2]	[BillingCode2]	[ASCII]	–	–
8	[CoverSheet Type]	[CoverSheet]	–	–	–
9	[Document PW]	[DocumentPassword]	[ASCII]	–	–

After selecting the template type, configure the following settings.
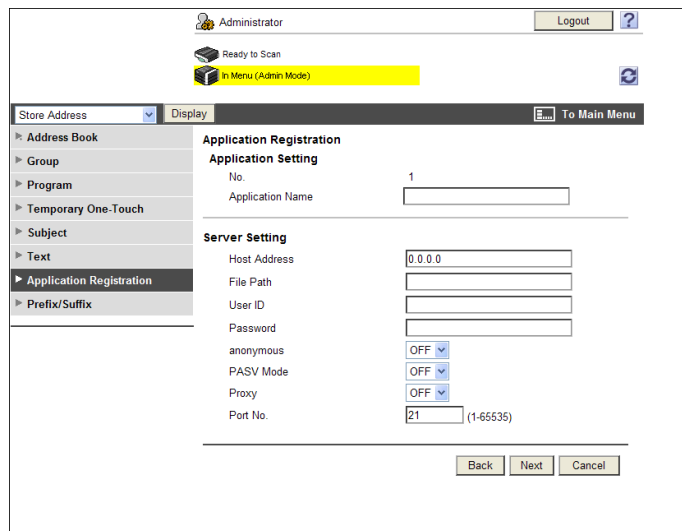
Item	Description
[No.]	Displays the registration number of the application.
[Application Name]	Enter the application name (up to 16 characters).
[Host Address]	Enter the host address of the server using the application (up to 15 characters).
[File Path]	Enter the destination file path (up to 96 characters).
[User ID]	Enter the user ID used to log in to the server (up to 47 characters).
[Password is changed.]	Select this check box to change the password.
[Password]	Enter the password used to log in to the server (up to 31 characters).
[anonymous]	Select whether to enable anonymous access.
[PASV Mode]	Select whether to enable the PASV mode.
[Proxy]	Select whether to enable the proxy.

Item	Description
[Port No.]	Enter a port number.
[Next]	Click this button to display the custom items list. Click [Edit] of the item you want to add or change. The function setting page is displayed.

[Function Settings]

Item	Description
[No.]	Displays the number of the selected item.
[Button Name]	Enter the button name (up to 16 characters).
[Function Name]	Select the function name. The required setting items differ depending on the selected function.
[Message on Panel]	Enter the name displayed on the **Control Panel** (up to 32 characters).
[Display Method]	Select the display method on the **Control Panel**.
[Default Value]	Enter the default value. To hide the default value, select the [Input string shown as ****] check box. The allowable number of characters differ depending on the selected function.
[Keyboard Type]	Select the keyboard type to display on the **Control Panel**.
[Options] (when "Authentication" is selected)	Configure options for Authentication.
[Options] (when "Delivery" is selected)	Configure options for Delivery.
[Options] (when "HoldForPreview" is selected)	Configure options for Hold For Preview.
[Input Type] (when "DelaySendDataTime" is selected)	Select the time specification.
[Default] (when "DelaySendDataTime" is selected)	Select whether to display the device time.

14.12   Using the Fax Server Communicating in E-Mail Format

When using the fax server communicating in E-mail format, you can configure settings to automatically add a prefix and suffix to a destination number.

[System Connection Setting]

In the administrator mode of **PageScope Web Connection**, select [System Settings]▸▸[System Connection Setting].
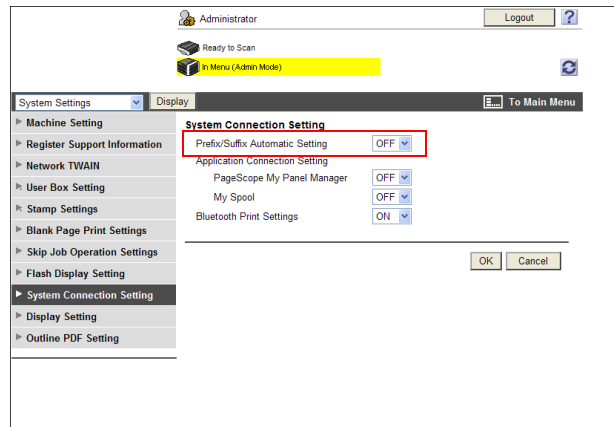
Item	Description
[Prefix/Suffix Automatic Setting]	Select whether to automatically add a prefix and suffix to a destination number. To automatically add a prefix and suffix, select [Store Address]▸▸[Prefix/Suffix], and register the target prefix and suffix in No. 1. For details, refer to page 11-30.

Reference

If [Prefix/Suffix Automatic Setting] is set to [ON], the following restrictions will be applied.

- [Fax Settings] is not available (excluding [Destination Check Display Function], [Confirm Address (TX)], and [Confirm Address (Register)]).
- [Store Address]▸▸[Application Registration] are not available.
- [Bulletin Board User Box], [Polling TX User Box], [Compulsory Memory RX User Box], and [Re-Transmission User Box] are not available.
- [Bulletin Board User Box] and [Relay User Box] cannot be registered.
- Confidential RX is not available.
- [Off-Hook] is not available.
- When sending, [Line Settings], [Communication Method Settings], [Fax Header Settings] is not available in [Communication Setting].
- The Network Fax function is not available.
- [Tone], [Pause], [-], and [Line Settings] are not available when registering a fax destination in the address book.
- You can output [Activity Report], [TX Report], and [RX Report] in [Job History].
- A number excluding a prefix and suffix is displayed in [Address] of [Job History].
- [Address Type] is set to E-mail in [Current Jobs] and [Job History].
- [Meter Count] is updated only when [Scans] is enabled in [Scan/Fax]; however, [Fax TX] is not updated.

15 Appendix

15   Appendix

15.1   Product specifications (Network functions)

Item	Specification
Type	Embedded
Frame type	IEEE802.2/802.3/Ethernet II/IEEE802.3SNAP
Cable type	10Base-T/100Base-TX/1000Base-T
Connector	RJ-45
Bluetooth performance [1]	Communication protocol: Bluetooth 2.0 + EDR Supported profile: OPP/BPP/SPP
Main supported protocols	TCP/IP (IPv4/IPv6), BOOTP, ARP, ICMP, DHCP, DHCPv6, AutoIP, SLP, SNMP, FTP, LPR/LPD, RAW Socket, SMB over TCP/IP, IPP, HTTP, POP, SMTP, LDAP, NTP, SSL, IPX/SPX, AppleTalk, Bonjour, NetBEUI, WebDAV, DPWS, S/MIME, IPsec, DNS, DynamicDNS, LLMNR, LLTD, SSDP, SOAP
Supported LDAP Servers	OpenLDAP 2.1x, Active Directory, Exchange 5.5/2000/2003, Sun Java Directory Server (Netscape/iPlanet Directory Server), Novell NetWare 5.x/6.x NDS, Novell eDirectory 8.6/8.7, and Lotus Domino Server (5.x/6.x)[2].
Supported LDAP protocol	LDAP Protocol Version 3 (Version 2 is not supported)
Supported SSL versions	SSL2, SSL3, and TLS1.0 (An x.509 certificate must be installed on the server.)
Multiprotocol	Auto detection
Operating environments of **PageScope Web Connection**	Compatible Web browsers: <For Windows NT4.0/2000/XP/Server 2003/Vista/Server 2008/7> • Microsoft Internet Explorer Ver. 6/7/8 (JavaScript and Cookies enabled) • Netscape Navigator 7.02 or later (JavaScript and Cookies enabled) • Mozilla Firefox 1.0 or later (JavaScript and Cookies enabled) <For Macintosh MacOS 9.x/MacOS X> • Netscape Navigator 7.02 or later (JavaScript and Cookies enabled) Mozilla Firefox 1.0 or later (JavaScript and Cookies enabled) <For Linux> • Netscape Navigator 7.02 or later (JavaScript and Cookies enabled) Mozilla Firefox 1.0 or later (JavaScript and Cookies enabled) Adobe® Flash® Player : • Plug-in Ver.7.0 or later required to select Flash as the display format. Plug-in Ver.9.0 or later required to use the Data Management Utility (font/macro data management).
Settings	Saved to non-volatile memory

[1] Install the optional **Local Interface Kit EK-605** in this machine.

[2] When using the Lotus Domino Server, and setting the search condition to "OR", the function will not work correctly.

15.2   Displaying the [Network Settings] Screen (Control Panel)

This section describes a procedure for displaying the [Network Settings] menu from the **Control Panel**.

1   Press **Utility/Counter**.

2   Press [Administrator Settings].

➜ In [Utility], an item can also be selected by pressing the key on the **Keypad** for the correspondent number. For [Administrator Settings], press the **3** key on the **Keypad**.

3   Enter the password, and then press [OK].

The [Administrator Settings] screen appears.
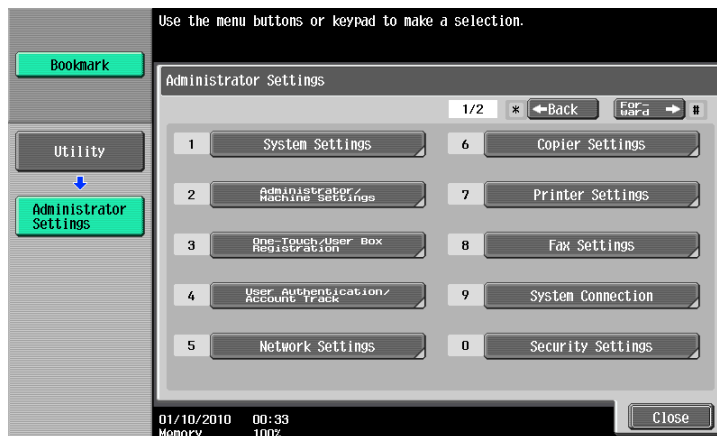
4 Press [Network Settings].

The [Network Settings] screen appears.

NOTICE

To enable changed network settings, turn the main power of this machine off and on again.

To turn the main power switch off and on, first turn the main power off, and then turn it on after 10 or more seconds have elapsed. Not doing so may result in an operation failure.

15.3   [Network Settings] menu list (Control Panel)

To configure network settings in the **Control Panel** of the machine, refer to this menu list.

This section describes the keys displayed when you press [Network Settings].

📖 **Reference**
For details on displaying the [Network Settings] screen, refer to page 15-3.

15.3.1   [Network Settings] (1/2)

You can configure the following items in the [Network Settings] (1/2) screen.
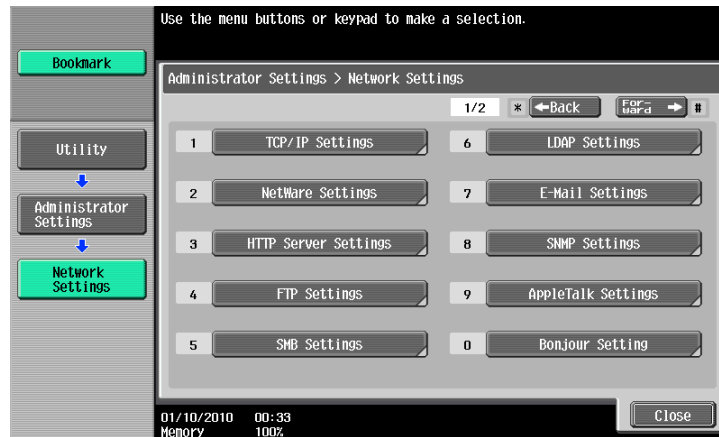
[TCP/IP Settings]

First level	Second level	Third level	Fourth level	Fifth level
[IPv4 Settings]	[Manual Input]	[IP Address]		
		[Subnet Mask]		
		[Default Gateway]		
	[Auto Input]	[DHCP Settings]	[ON]/[OFF]	
		[BOOTP Settings]	[ON]/[OFF]	
		[ARP/PING Settings]	[ON]/[OFF]	
		[AUTO IP Settings]	[ON]/[OFF]	
[IPv6 Settings]	[Auto IPv6 Settings]	[ON]		
		[OFF]	[Global Address]	[Prefix Length]
			[Gateway Address]	
			[Link-Local Address]	
	[DHCPv6 Setting]	[ON]/[OFF]		
[DNS Host]	[DNS Host Name]			
	[Dynamic DNS Settings]	[Enable]/[Disable]		
[DNS Domain]	[Domain Name Auto Retrieval]	[Enable]/[Disable]		
	[Search Domain Name Auto Retrieval]	[Enable]/[Disable]		
	[Default DNS Domain Name]			
	[DNS Search Domain Name 1] to [DNS Search Domain Name 3]			

First level	Second level	Third level	Fourth level	Fifth level
[DNS Server Settings (IPv4)]	[DNS Server Auto Obtain]	[Enable]/[Disable]		
	[Priority DNS Server]			
	[Secondary DNS Server 1] to [Secondary DNS Server 2]			
[DNS Server Settings (IPv6)]	[DNS Server Auto Obtain]	[Enable]/[Disable]		
	[Priority DNS Server]			
	[Secondary DNS Server 1] to [Secondary DNS Server 2]			
[IPsec Settings]	[IKE Settings]	[Group 1] to [Group 4]		
		[Encryption Algorithm]	[DES_CBC]	
			[3DES_CBC]	
			[OFF]	
		[Authentication Algorithm]	[MD5]	
			[SHA-1]	
			[OFF]	
		[Key Validity Period]		
		[Diffie-Hellman Group]	[Group 1]	
			[Group 2]	
	[IPsec SA Settings]	[Group 1] to [Group 8]	[Security Protocol]	[AH]
				[ESP]
				[ESP_AH]
				[OFF]
			[ESP Encryption Algorithm]	[DES_CBC]
				[3DES_CBC]
				[AES_CBC]
				[AES_CTR]
				[NULL]
				[OFF]
			[ESP Authentication Algorithm]	[MD5]
				[SHA-1]
				[OFF]
			[AH Authentication Algorithm]	[MD5]
				[SHA-1]
				[OFF]
		[Lifetime After Establishing SA]		
	[Peer]	[Group 1] to [Group 10]	[Encapsulation Mode]	[Tunnel Mode]
				[Transport Mode]
				[OFF]
			[IP Address]	
			[Pre-Shared Key Text]	
			[Perfect Forward Secrecy]	[ON]/[OFF]
[IP Filtering (Permit Access)]	[Enable]	[Set 1] to [Set 5]		
	[Disable]			

First level	Second level	Third level	Fourth level	Fifth level
[IP Filtering (Deny Access)]	[Enable]	[Set 1] to [Set 5]		
	[Disable]			
[RAW Port Number]	[Port 1] to [Port 6]	[Job Setting]		
		[OFF]		
[LLMNR Setting]	[Enable]/[No Limit]			

[NetWare Settings]

First level	Second level	Third level	Fourth level	Fifth level
[IPX Settings]	[ON]	[Ethernet Frame Type]	[Auto Detect]	
			[802.2]	
			[802.3]	
			[Ethernet]	
			[802.3SNAP]	
	[OFF]			
[NetWare Print Settings]	[ON]	[PServer]	[Print Server Name]	
			[Print Server Password]	
			[Polling Interval]	
			[NDS/Bindery Setting]	[NDS]
				[NDS & Bindery]
			[File Server Name]	
			[NDS Context Name]	
			[NDS Tree Name]	
		[Nprinter/Rprinter]	[Print Server Name]	
			[Printer Number]	
	[OFF]			
	[Status]			
[User Authentication Setting (NDS)]	[ON]/[OFF]			

[HTTP Server Settings]

First level	Second level	Third level	Fourth level	Fifth level
[PSWC Settings]	[ON]/[OFF]			
[IPP Settings]	[ON]/[OFF]			
[Accept IPP Jobs]	[ON]/[OFF]			
[Support Information]	[Print Job]			
	[Valid Job]			
	[Cancel Job]			
	[Open Job Attributes]			
	[Open Job]			
	[Open Printer Attributes]			
[Printer Information]	[Printer Name]			
	[Printer Location]			
	[Printer Information]			
	[Print URI]			
[IPP Authentication Settings]	[ON]/[OFF]			
[Authentication Method]	[requesting-user-name]			
	[basic]			
	[digest]			
[User Name]				
[Password]				
[realm]				

[FTP Settings]

First level	Second level	Third level	Fourth level	Fifth level
[FTP TX Settings]	[ON]	[Proxy Server Address]	[Input Host Name]	
			[IPv4 Address Input]	
			[IPv6 Address Input]	
		[Proxy Server Port Number]		
		[Port No.]		
		[Connection Timeout]		
	[OFF]			
[FTP Server Settings]	[ON]/[OFF]			

[SMB Settings]

First level	Second level	Third level	Fourth level	Fifth level
[Client Settings]	[ON]	[NTLM Settings]	[v1]	
			[v2]	
			[v1/v2]	
		[User Authentication (NTLM)]	[ON]/[OFF]	
		[DFS Setting]	[Enable]/[Invalid]	
	[OFF]			
[Print Settings]	[ON]	[NetBIOS Name]		
		[Print Service Name]		
		[Workgroup]		
	[OFF]			
[WINS Settings]	[ON]	[Automatic Retrieval Settings]	[Enable]/[Disable]	
		[WINS Server Address]		
		[Node Type Setting]	[B Node]	
			[P Node]	
			[M Node]	
			[H Node]	
	[OFF]			
[Direct Hosting Setting]	[ON]/[OFF]			

[LDAP Settings]

First level	Second level	Third level	Fourth level	Fifth level
[Enabling LDAP]	[ON]/[OFF]			
[Setting Up LDAP]	[LDAP Server Name]			
	[Max.Search Results]			
	[Timeout]			
	[Initial Setting for Search Details]	[Name]		
		[E-Mail]		
		[Fax Number]		
		[Last Name]		
		[First Name]		
		[City]		
		[Company Name]		
		[Department]		
	[Change Search Attribute]	[Name]		
		[Nickname]		
	[Server Address]			
	[Search Base]			
	[SSL Setting]	[ON]/[OFF]		
	[Port Number]			
	[Port Number (SSL)]			
	[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]	
		[Key Usage]	[Confirm]/[Do Not Confirm]	
		[Chain]	[Confirm]/[Do Not Confirm]	
		[Expiration Date Confirmation]	[Confirm]/[Do Not Confirm]	
		[CN]	[Confirm]/[Do Not Confirm]	
	[Authentication Type]	[Anonymous]		
		[Simple]		
		[Digest-MD5]		
		[GSS-SPNEGO]		
		[NTLM v1]		
		[NTLM v2]		
	[Select Sever Authentication Method]	[Use Settings]		
		[Use User Authentication]		
		[Dynamic Authentication]		
	[Referral Setting]	[ON]/[OFF]		
	[Login Name]			
	[Password]			
	[Domain Name]			
	[Reset All Settings]			
	[Check Connection]			

[Default LDAP Server Setting]

[E-Mail Settings]

First level	Second level	Third level	Fourth level	Fifth level
[E-Mail TX (SMTP)]	[Scan to E-mail]	[ON]/[OFF]		
	[Status Notification]	[ON]/[OFF]		
	[Total Counter Notification]	[ON]/[OFF]		
	[SMTP Server Address]	[Input Host Name]		
		[IPv4 Address Input]		
		[IPv6 Address Input]		
	[Binary Division]	[ON]/[OFF]		
	[Divided Mail Size]			
	[Connection Timeout]			
	[Server Capacity]			
	[SSL Settings]	[SMTP over SSL]		
		[Start TLS]		
		[OFF]		
	[Port No.]			
	[Port Number (SSL)]			
	[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]	
		[Key Usage]	[Confirm]/[Do Not Confirm]	
		[Chain]	[Confirm]/[Do Not Confirm]	
		[Expiration Date Confirmation]	[Confirm]/[Do Not Confirm]	
		[CN]	[Confirm]/[Do Not Confirm]	
	[Detail Settings]	[SMTP Authentication]	[ON]	[User ID]
				[Password]
				[Domain Name]
				[Authentication Setting]
			[OFF]	
		[POP Before SMTP Authentication]	[ON]/[OFF]	
		[POP Before SMTP Time]		

First level	Second level	Third level	Fourth level	Fifth level
[E-Mail RX (POP)]	[ON]	[POP Server Address]	[Input Host Name]	
			[IPv4 Address Input]	
			[IPv6 Address Input]	
		[Connection Timeout]		
		[SSL Setting]	[ON]/[OFF]	
		[Port Number]		
		[Port Number (SSL)]		
		[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]
			[Key Usage]	[Confirm]/[Do Not Confirm]
			[Chain]	[Confirm]/[Do Not Confirm]
			[Expiration Date Confirmation]	[Confirm]/[Do Not Confirm]
			[CN]	[Confirm]/[Do Not Confirm]
		[Login Name]		
		[Password]		
		[APOP Authentication]	[ON]/[OFF]	
		[Check for New Messages]	[Yes]/[No]	
		[Polling Interval]		
	[OFF]			

First level	Second level	Third level	Fourth level	Fifth level
[S/MIME Communication Settings]	[ON]	[Digital Signature]	[Do not add signature]	
			[Always add signature]	
			[Select when sending]	
		[E-Mail Text Encryption Method]	[RC2-40]	
			[RC2-64]	
			[RC2-128]	
			[DES]	
			[3DES]	
			[AES-128]	
			[AES-192]	
			[AES-256]	
		[Print S/MIME Information]	[Yes]/[No]	
		[Automatically Obtain Certificates]	[Yes]/[No]	
		[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]
			[Key Usage]	[Confirm]/[Do Not Confirm]
			[Chain]	[Confirm]/[Do Not Confirm]
			[Expiration Date Confirmation]	[Confirm]/[Do Not Confirm]
	[OFF]			

Reference
- [S/MIME Communication Settings] is displayed only when a **Hard Disk** is installed.

[SNMP Settings]

First level	Second level	Third level	Fourth level	Fifth level
[SNMP v1/v2c (IP)]	[ON]/[OFF]			
[SNMP v3 (IP)]	[ON]/[OFF]			
[SNMP v1 (IPX)]	[ON]/[OFF]			
[UDP Port Number]				
[SNMP v1/v2c Settings]	[Read Community Name Settings]			
	[Write Setting]	[Enable]/[Invalid]		
	[Write Community Name Settings]			

First level	Second level	Third level	Fourth level	Fifth level
[SNMP v3 Settings]	[Context Name Settings]			
	[Discovery User Permissions]	[ON]/[OFF]		
	[Discovery User Name Settings]			
	[Read User Name Settings]			
	[Security Level]	[OFF]		
		[auth-password]		
		[auth-password/priv-password]		
	[Password Setting] (Read)	[Read auth]		
		[Read priv]		
		[Write auth]		
		[Write priv]		
	[Write User Name Settings]			
	[Security Level]	[OFF]		
		[auth-password]		
		[auth-password/priv-password]		
	[Password Setting] (Write)	[Read auth]		
		[Read priv]		
		[Write auth]		
		[Write priv]		
	[Encryption Algorithm]	[DES]		
		[AES-128]		
	[Authentication Algorithm]	[MD5]		
		[SHA-1]		
[TRAP Setting]	[Allow]/[Restrict]			
[TRAP Setting When Authentication Failed]	[Enable]/[Invalid]			

[AppleTalk Settings]

First level	Second level	Third level	Fourth level	Fifth level
[AppleTalk Settings]	[ON]	[Printer Name]		
		[Zone Name]		
		[Current Zone]		
	[OFF]			

[Bonjour Setting]

First level	Second level	Third level	Fourth level	Fifth level
[Bonjour Setting]	[ON]	[Bonjour Name]		
	[OFF]			

15.3.2 [Network Settings] (2/2)

You can configure the following items in the [Network Settings] (2/2) screen.
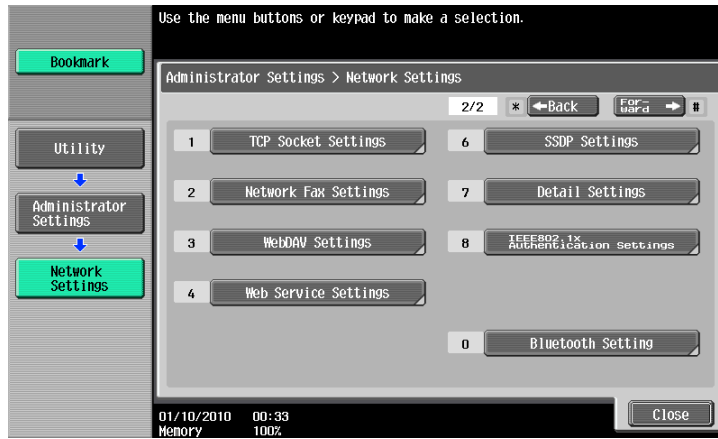
[TCP Socket Settings]

First level	Second level	Third level	Fourth level	Fifth level
[TCP Socket]	[ON]	[Use SSL/TLS]	[ON]/[OFF]	
		[Port Number]		
		[Port Number (SSL)]		
	[OFF]			
[TCP Socket (AS-CII Mode)]	[ON]	[Port Number (ASCII Mode)]		
	[OFF]			

[Network Fax Settings]

Reference
- Ask your service representative to configure this setting. For details, contact your service representative.
- This function is available only when a **Hard Disk** is installed.

First level	Second level	Third level	Fourth level	Fifth level
[Network Fax Function Settings]	[IP Address Fax Function]	[ON]/[OFF]		
	[Internet Fax Function]	[ON]/[OFF]		
[SMTP TX Settings]	[Port No.]			
	[Connection Timeout]			
[SMTP RX Settings]	[ON]	[Port No.]		
		[Connection Timeout]		
	[OFF]			

[WebDAV Settings]

First level	Second level	Third level	Fourth level	Fifth level
[WebDAV Client Settings]	[ON]	[Proxy Server Address]	[Input Host Name]	
			[IPv4 Address Input]	
			[IPv6 Address Input]	
		[Proxy Server Port Number]		
		[User Name]		
		[Password]		
		[Chunk Transmission]	[Yes]/[No]	
		[Connection timeout]		
		[Server Auth. Character Code]	[UTF-8]	
			[Windows Code Page]	
		[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]
			[Key Usage]	[Confirm]/[Do Not Confirm]
			[Chain]	[Confirm]/[Do Not Confirm]
			[Expiration Date Confirmation]	[Confirm]/[Do Not Confirm]
			[CN]	[Confirm]/[Do Not Confirm]
	[OFF]			
[WebDAV Server Settings]	[ON]	[SSL Setting]	[Non-SSL Only]	
			[SSL Only]	
			[SSL/Non-SSL]	
		[Password Setting]	[Password Setting]	
			[Initial Password]	
	[OFF]			

[Web Service Settings]

First level	Second level	Third level	Fourth level	Fifth level
[Web Service Common Settings]	[Friendly Name]			
	[Publication Service]	[Enable]/[Invalid]		
	[SSL Setting]	[ON]/[OFF]		
[Printer Settings]	[ON]	[Printer Name]		
		[Printer Location]		
		[Printer Information]		
	[OFF]			
[Scanner Settings]	[ON]	[Scanner Name]		
		[Scanner Location]		
		[Scanner Information]		
		[Connection Timeout]		
	[OFF]			

[SSDP Settings]

First level	Second level	Third level	Fourth level	Fifth level
[ON]	[Multicast TTL Setting]			
[OFF]				

[Detail Settings]

First level	Second level	Third level	Fourth level	Fifth level
[Device Setting]	[MAC Address]			
	[LLTD Setting]	[Enable]/[Disable]		
	[Network Speed]	[Auto (10M/100Mbps)]		
		[Auto (10M/100M/1Gbps)]		
		[10Mbps Half Duplex]		
		[10Mbps Full Duplex]		
		[100Mbps Half Duplex]		
		[100Mbps Full Duplex]		
		[1Gbps Full Duplex]		
[Time Adjustment Setting]	[ON]	[Auto IPv6 Retrieval]	[On]/[Off]	
		[Host Address]	[Input Host Name]	
			[IPv4 Address Input]	
			[IPv6 Address Input]	
		[Port Number]		
		[Set Date]		
		[Auto Time Adjustment]	[On]/[Off]	
		[Polling Interval]		
	[OFF]			
[Status Notification Setting]	[Register Notification Address]	[IP Address 1] to [IP Address 5]	[Address]	[Input Host Name]
				[IPv4 Address Input]
				[IPv6 Address Input]
			[Port Number]	
			[Community Name]	
			[Notification Items]	
		[IPX Address]	[Address]	[Network Address]
				[Node Address]
			[Community Name]	
			[Notification Items]	
		[E-mail 1] to [E-mail 10]	[Edit E-Mail Address]	
			[Notification Items]	

First level	Second level	Third level	Fourth level	Fifth level
[Total Counter Notification Settings]	[Notification Schedule Setting]	[Schedule 1] to [Schedule 2]	[Monthly]	[Monthly Frequency]
				[Date Setting]
			[Weekly]	[Weekly Frequency]
				[Day of the Week]
			[Daily]	[Interval of Day(s)]
	[Notification Address Setting]	[Address 1] to [Address 3]	[Edit E-Mail Address]	
			[Schedule Settings]	[Schedule 1] to [Schedule 2]
	[Model Name]			
	[Send Now]			
[PING Confirmation]	[PING TX Address]	[Input Host Name]		
		[IPv4 Address Input]		
		[IPv6 Address Input]		
	[Check Connection]			
[SLP Setting]	[Enable]/[Disable]			
[LPD Setting]	[Enable]/[Disable]			
[Prefix/Suffix Setting]	[ON/OFF Setting]	[ON]/[OFF]		
	[Prefix/Suffix Setting]	[Prefix]		
		[Suffix]		
[Error Code Display Setting]	[ON]/[OFF]			

[IEEE802.1x Authentication Settings]

First level	Second level	Third level	Fourth level	Fifth level
[ON]	[Auth. Status]			
	[Reset Job Settings]			
	[Certificate Verification Level Settings]	[Expiration Date]	[Confirm]/[Do Not Confirm]	
		[CN]	[Confirm]/[Do Not Confirm]	
		[Chain]	[Confirm]/[Do Not Confirm]	
[OFF]				

[Bluetooth Setting]

Reference
- This function is available when the optional **Local Interface Kit EK-605** is installed in this machine.

First level	Second level	Third level	Fourth level	Fifth level
[Enable]/[Invalid]				

15.4   Network Error Codes

Functions	Code	Description
IEEE802.1X	1	Connection has already been established.
	2	Parameter error.
	3	Unable to find the destination AP (SSID).
	4	The authentication mode does not match the AP (IEEE8021X/WPA-EAP/WPA-PSK/NONE).
	5	Negotiation of the EAP method failed.
	6	The EAP authentication failed (user ID, password, certificate, etc.)
	7	Encryption negotiation with the AP failed (TKIP/CCMP).
	8	Failed to retrieve the client certificate.
	9	The client certificate has expired.
	10	Verification error of the server certificate (EAP-TLS/EAP-TTLS/PEAP).
	11	Although the WPA-PSK mode is selected, the Pre-Shared Key is not specified.
	12	An authentication error occurred in the WPA-PSK mode (un-matched Pre-Shared Key).
	13	The phase 2 method is not specified (PEAP).
	14	Negotiation of the phase 2 method failed (PEAP).
	15	Response from the server has timed out.
	16	Failed to allocate memory.
	17	Failed to start the supplicant task.
	18	The driver does not work.
	19	The server certificate has expired (EAP-TLS/EAP-TTLS/PEAP).
	20	CA verification error of the server certificate (EAP-TLS/EAP-TTLS/PEAP).
	21	Server ID verification error of the server certificate (EAP-TLS/EAP-TTLS/PEAP).
	22	The CA certificate is not specified (EAP-TLS/EAP-TTLS/PEAP).
	23	The server ID is not specified (EAP-TLS/EAP-TTLS/PEAP).
	24	The setting combination is correct.
	25	Connection and authentication are complete.
	26	The server certificate does not have the expected usage (EAP-TLS/EAP-TTLS/PEAP).
	27	The server certificate has expired (EAP-TLS/EAP-TTLS/PEAP).
	28	Access to the server to check for expiration of the server certificate is rejected (EAP-TLS/EAP-TTLS/PEAP).
	29	Access to the server to check for expiration of the server certificate has timed out (EAP-TLS/EAP-TTLS/PEAP).
	30	Unable to check for expiration because the CRL size that has been retrieved to check for the expiration of the server certificate exceeds the maximum capacity that can be retained (1MB) (EAP-TLS/EAP-TTLS/PEAP).
	31	Incorrect format of the server certificate (EAP-TLS/EAP-TTLS/PEAP).
	32	Verification of the server certificate is invalid (EAP-TLS/EAP-TTLS/PEAP).

Functions	Code	Description
IEEE802.1X	33	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified (EAP-TLS/EAP-TTLS/PEAP).
	34	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20) (EAP-TLS/EAP-TTLS/PEAP).
	35	Parameter error of the certificate (EAP-TLS/EAP-TTLS/PEAP).
	36	Internal error of the certificate verification (EAP-TLS/EAP-TTLS/PEAP).
LDAP	1	An invalid operation occurred.
	4	The number of search results has exceeded the maximum number of items allowed.
	7	The LDAP server does not support SASL.
	10	Unable to trace the link although Referral is specified.
	32	Cannot find the search route.
	49	Failed to log in to the LDAP server.
	80	An unexpected error occurred.
	85	The connection has timed out.
	86	The supported SASL does not match the LDAP server side.
	88	Cancelled by the user.
	90	A memory shortage occurred.
	91	Unable to connect to the LDAP server.
	92	The supported LDAP version does not match the LDAP server side.
	128	Failed to resolve the LDAP server name using the DNS server.
	129	The certificate of the LDAP server has expired.
	130	Mutual authentication using GSS-SPNEGO (Kerberos v5) failed.
	131	The search result remains.
	2238	The CN field of the LDAP server certificate does not match the server address.
	2239	The LDAP server certificate does not have the expected usage for a server.
	2240	The LDAP server certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	2241	The LDAP server certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	2261	The format of the LDAP server certificate is invalid.
	2263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.
	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.

Functions	Code	Description
LDAP	10000	Failed in authentication using a PKI card.
	12236	The ticket certificate has expired.
	12239	The ticket certificate does not have the expected usage for a server.
	12240	The ticket certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	12241	The ticket certificate has expired.
	12242	The CA server rejected the connection.
	12243	The connection to the server that checks for expiration of the certificate has timed out.
	12244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	12261	The format of the ticket certificate is invalid.
	12263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.
	12264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	12266	Internal error of the certificate verification.
E-Mail/ Internet Fax	1	Failed to log in to the E-mail server.
	2	An internal error occurred.
	3	Failed to connect to the server.
	4	The connection has timed out.
	5	Decoding failed due to invalid MIME format or S/MIME format.
	6	Available free memory is insufficient. Reception is not possible.
	7	Job ID is invalid.
	9	Failed to delete an E-mail message.
	10	The mail box is full.
	11	Failed to search the certificate.
	12	Failed to retrieve the device certificate or private key.
	13	An I/O error occurred. An HDD operation error occurred, or memory capacity of the computer may be insufficient.
	14	The S/MIME function is disabled.
	15	The HDD is disabled.
	16	The format of the certificate from the E-mail sender is invalid.
	2236	The certificate has expired, or the validity period has not yet started.
	2238	The CN field of the certificate does not match the server address.
	2239	The certificate does not have the expected usage.
	2240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	2241	The certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).

Functions	Code	Description
E-Mail/ Internet Fax	2261	The format of the certificate is invalid.
	2263	Failed to initialize the certificate verification.
	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.
FTP TX	22	Parameter error (e.g. the file name is NULL).
	27	Parameter is invalid.
	42	The specified protocol is unavailable.
	52	The process is cancelled by a device reset.
	55	A buffer shortage occurred.
	56	The FTP connection is already open.
	57	Failed to connect to the server.
	60	The connection has timed out.
	61	The connection has been interrupted.
	62	The device is not connected to the network.
	70	The network connection is busy.
	450	The file has not been deleted.
	451	The file transfer failed (e.g. due to insufficient server capacity).
	452	The file transfer failed (e.g. due to insufficient server capacity).
	530	Incorrect login name or password.
	550	The specified folder does not exist.
	552	The file operation failed (e.g. due to insufficient server capacity).
SMB transmission	42	The specified protocol is unavailable.
	52	The process is cancelled by a device reset.
	55	A buffer shortage occurred.
	57	Failed to connect to the server.
	62	The device is not connected to the network. The connection has been interrupted.
	70	The network connection is busy.
	4096	The host name is not specified. The specified host name does not exist on the network.
	4097	The user name is not specified. Unable to log in with the specified user name and password. The user does not have write permission to the folder. Failed to log in due to an SMB protocol error.
	4098	The folder name is not specified. The specified folder does not exist.
	4099	The user name is not specified. Unable to log in with the specified user name and password. The user does not have write permission to the folder. Failed to log in due to an SMB protocol error.
	4100	The specified file name is invalid.
	4101	The specified file already exists and is write-protected. The folder and the disk are write-protected.
	4102	The specified media to be written is not formatted. The file system of the specified media to be written is faulty.

Functions	Code	Description
SMB transmission	4103	The server capacity is full.
	4104	The server capacity has become full while writing data.
	4105	Other errors to which an error code is not assigned.
	10000	Failed in authentication using a PKI card.
	12236	The certificate has expired, or the validity period has not yet started.
	12239	The certificate does not have the expected usage.
	12240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	12241	The certificate has expired.
	12242	The CA server rejected the connection.
	12243	The connection to the server that checks for expiration of the certificate has timed out.
	12244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	12263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.
	12264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	12266	Internal error of the certificate verification.
	12267	The device certificate does not exist.
	12268	No certificate is sent from the server.
SMTP transmission	22	Invalid argument.
	27	The file size is too large.
	28	Insufficient memory of the device.
	32	The pipe is broken.
	42	The specified protocol is unavailable.
	51	Unable to reach the destination network.
	52	The connection aborted by the network.
	55	A buffer shortage occurred.
	57	The socket is not connected.
	58	The connection has been interrupted.
	60	The operation has timed out.
	61	The connection is rejected.
	62	The device is not connected to the network.
	67	The host is shut down.
	70	The operation is expected to be blocked.
	421	SMTP server error. Since the service is unavailable, the transfer channel is closed.
	432	SMTP server error. The password must be changed.
	450	SMTP server error. Unable to access to the mail box.
	451	SMTP server error. The requested action has been cancelled because an error occurred while processing a job.

Functions	Code	Description
SMTP transmission	452	SMTP server error. Shortage of the system storage capacity.
	453	SMTP server error. No E-mail massage.
	454	SMTP server error. Temporary authentication failure.
	458	SMTP server error. Unable to queue a message to the node.
	459	SMTP server error. The node is not permitted.
	499	SMTP server error. An unsupported SMTP error code of 400s is received from the SMTP server.
	500	SMTP server error. Syntax error (command unrecognized).
	501	SMTP server error. Syntax error in parameters or arguments.
	502	SMTP server error. The command is not implemented.
	503	SMTP server error. Bad sequence of commands.
	504	SMTP server error. The command parameter is not implemented.
	521	SMTP server error. The server does not receive E-mail messages.
	530	SMTP server error. The access is rejected.
	534	SMTP server error. The authentication mechanism is too weak.
	535	SMTP server error. Authentication error.
	538	SMTP server error. The requested authentication mechanism requires encryption.
	550	SMTP server error. The requested action is not executed.
	551	SMTP server error. The user is not connected locally.
	552	SMTP server error. The requested E-mail action is cancelled.
	553	SMTP server error. The requested action is not accepted.
	554	An SMTP server error, or an internal error when sending data. The transaction failed.
	555	SMTP server error. MAIL/RCPT parameter error.
	599	SMTP server error. An unsupported SMTP error code of 500s is received from the SMTP server.
	2236	The certificate has expired, or the validity period has not yet started.
	2238	The CN field of the certificate does not match the server address.
	2239	The certificate does not have the expected usage.
	2240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.

Functions	Code	Description
SMTP transmission	2241	The certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	2261	The format of the certificate is invalid.
	2263	Failed to initialize the certificate verification.
	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.
	3000	An unexpected error occurred.
	3001	An unexpected error occurred within the library being used.
	3002	An invalid channel is specified.
	3003	SMTP server address is invalid.
	3004	Parameter error (MIMEBodyHeader).
	3005	Parameter error (DisplayName).
	3006	Parameter error (character set).
	3007	Parameter error (From address).
	3008	Parameter error (To address).
	3009	Parameter error (CC address).
	3010	Parameter error (BCC address).
	3011	Parameter error (pEmailSet is NULL).
	3012	Parameter error (destination certificate is NULL).
	3013	Parameter error (E-mail body).
	3014	The HDD is disabled.
	3015	The S/MIME function is disabled.
	3016	The device certificate cannot be used in S/MIME (e.g. self-signed certificate error, the private key type is not RSA).
	3018	An invalid encryption algorithm is specified.
	3019	An invalid signature algorithm is specified.
	3020	The E-mail address included in the destination certificate does not match the destination address (To/Cc/Bcc).
	3021	The E-mail address included in the certificate does not match the sender (From) address.
	3022	Format error of the certificate.
	3023	Parameter error (Disposition-Notification-To).
	3024	Message syntax error of the receiver side.
	3025	The SMTP server does not support the STARTTLS command.
	3026	PKI card access error.

Functions	Code	Description
WebDAV transmission	22	The format of the URL of the target resource is invalid. Parameter error.
	27	Attempted to send data that exceeds the maximum transferrable size for transfer coding.
	42	The specified protocol is unavailable.
	52	The process is cancelled by a device reset.
	55	A buffer shortage occurred.
	56	The connection has already been established.
	57	The connection to the WebDAV server failed (including connection time out).
	62	The device is not connected to the network.
	70	The network connection is busy.
	72	The connection has been interrupted with the condition that is insufficient to the specified size.
	1001	The server does not support WebDAV. Unable to upload data to the server.
	1002	The intermediate resource is not a collection (directory) (e.g. the specified folder does not exist).
	1003	The target resource is a collection (directory).
	1011	Although "https" is specified for the resource URL, it is unavailable because the SSL library is not included for the modularity.
	1012	Although "https" is specified for the resource URL, the connection is interrupted because the WebDAV server certificate has expired.
	1013	The CONNECT method is issued to the proxy server to establish an SSL connection via a proxy, but it is rejected.
	1017	A communication error occurred while sending a request.
	1018	A communication error occurred while receiving a response.
	1027	nContentLength exceeds the maximum transferable size.
	1030	Although use of a proxy has been specified, the proxy setting information is unavailable.
	1031	The connection to the proxy server failed (including connection time out).
	1098	Failed in chunk TX to SharePoint Server.
	1099	Other internal error occurred (e.g. memory shortage).
	2236	The certificate has expired, or the validity period has not yet started.
	2238	The CN field of the certificate does not match the server address.
	2239	The certificate does not have the expected usage.
	2240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	2241	The certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	2261	The format of the certificate is invalid.
	2263	Failed to initialize the certificate verification.

Functions	Code	Description
WebDAV transmission	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.
SMB browsing	32	The connection has been interrupted.
	42	The specified protocol is unavailable.
	57	Failed to connect to the server.
	62	The device is not connected to the network. The internal channel detected an error immediately before establishing communication.
	67	The host is shut down.
	4096	The group name/host name is not specified. The specified group name/host name does not exist on the network.
	4097	The user name is not specified. Unable to log in with the specified user name and password. Failed to log in due to an SMB protocol error.
	4098	Administrative shares do not exist. The shared resource name is not specified. The shared resource does not exist.
	4099	The user name is not specified. Unable to log in with the specified user name and password. Failed to log in due to an SMB protocol error.
	4102	The specified media to be written is not formatted. The file system of the specified media to be written is faulty.
	4105	Other errors to which an error code is not assigned.
	4352	The browser machine (master browser/backup browser) is not found.
	4353	Unable to log in to the browser machine (master browser/backup browser).
	4354	The sub folder does not exist.
	4355	The request is not accepted due to an invalid call sequence etc.
	4368	The number of groups is too large.
	4369	The number of host PCs is too large.
	4370	The number of shared resources is too large.
	10000	Failed in authentication using a PKI card.
	12236	The certificate has expired, or the validity period has not yet started.
	12239	The certificate does not have the expected usage.
	12240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	12241	The certificate has expired.
	12242	The CA server rejected the connection.
	12243	The connection to the server that checks for expiration of the certificate has timed out.
	12244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	12263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.

Functions	Code	Description
SMB browsing	12264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	12266	Internal error of the certificate verification.
	12267	The device certificate does not exist.
	12268	No certificate is sent from the server.
User Authentication	1	Invalid parameter (e.g. the number of characters exceeds the limit, blank). The authentication function setting is disabled.
	2	Failed to resolve the name using the DNS server.
	3	Unable to find the authentication server.
	4	Failed to authenticate.
	5	Failed to allocate memory. An unexpected error occurred (which does not occur under normal usage conditions).
	6	An authentication request is received while an internal task of the user authentication client is being performed.
	7	The connection was interrupted while the user authentication was being performed.
	10000	Failed in authentication using a PKI card.
	12236	The certificate has expired, or the validity period has not yet started.
	12239	The certificate does not have the expected usage.
	12240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	12241	The certificate has expired.
	12242	The CA server rejected the connection.
	12243	The connection to the server that checks for expiration of the certificate has timed out.
	12244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	12261	The format of the certificate is invalid.
	12263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.
	12264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	12266	Internal error of the certificate verification.
WebDAV client	0	When receiving a response: Successfully received data, but the response body is missing. When sending a request: Successfully sent data, and is waiting for a response to be received.
	1	When receiving a response: Successfully received data, and continuously receives the response body. When sending a request: Successfully sent data, and is waiting for an instruction to send the request body.
	2	When receiving a response: Successfully received the response body, and its reception has been completed. When sending a request: The ID of the client that is not opened is specified.
	3	When receiving a response: The reception has timed out. When sending a request: An invalid request method has been specified.

Functions	Code	Description
WebDAV client	4	When receiving a response: A reception error occurred. Or an invalid request URL is specified. When sending a request: An invalid request URL is specified.
	5	When receiving a response: Content-Length or the received data size exceeds the maximum transferable size. Or the size of the message body is too large. When sending a request: The size of the message body is too large.
	6	When receiving a response: The process is cancelled by a reset. Or the size of the message body exceeds the maximum transferable size. When sending a request: The size of the message body exceeds the maximum transferable size.
	7	When receiving a response: An internal error occurred. Or the process is cancelled by an internal reset. When sending a request: The process is cancelled by an internal reset.
	8	Failed to connect to the WebDAV server.
	9	An error occurred while sending data to the WebDAV server.
	10	A timeout occurred while sending data to the WebDAV server.
	11	Failed to connect to the proxy server.
	12	The proxy server rejected the connection request.
	13	Although use of a proxy has been specified, the proxy setting information is unavailable.
	14	Failed to authenticate the proxy server.
	15	Other error was returned from the proxy server.
	16	An internal error occurred.
	17	The process is cancelled because MIO_REQBODY_ERROR is specified by the device application.
	2236	The certificate has expired, or the validity period has not yet started.
	2238	The CN field of the certificate does not match the server address.
	2239	The certificate does not have the expected usage.
	2240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	2241	The certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	2261	The format of the certificate is invalid.
	2263	Failed to initialize the certificate verification.
	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.

Functions	Code	Description
WS scan	1	The specified client is not registered.
	2	Parameter is invalid.
	3	The Web service or WS scan function is disabled.
	4	The device is not connected to the network.
	5	Waiting for connection from CP.
	6	The certificate of the destination computer is not valid when the validity period of a certificate is checked.
	22	Invalid argument.
	42	The specified protocol is unavailable.
	52	The connection aborted by the network.
	53	The connection has been interrupted.
	55	A buffer shortage occurred.
	57	The socket is not connected.
	60	The operation has timed out.
	70	The operation is expected to be blocked.
	72	The RetrieveImage waiting period has timed out.
	2236	The certificate has expired, or the validity period has not yet started.
	2238	The CN field of the certificate does not match the server address.
	2239	The certificate does not have the expected usage.
	2240	The certificate is not trusted. To trust the certificate, the certificate must be registered to the system.
	2241	The certificate has expired.
	2242	The CA server rejected the connection.
	2243	The connection to the server that checks for expiration of the certificate has timed out.
	2244	Unable to check for expiration because the CRL size exceeds the maximum capacity that can be retained (1MB).
	2261	The format of the certificate is invalid.
	2263	Although the environment is configured to use the HDD, it is unable to perform verification because the HDD path has not been specified.
	2264	Unable to perform verification because there are too many certificates to be verified (the maximum number of certificates that can be verified at a time is 20).
	2265	Parameter of the certificate verification is invalid.
	2266	Internal error of the certificate verification.
	2267	The device certificate does not exist.
	2268	No certificate is sent from the server.
Bluetooth	0	The reception of the object data specification range has been completed (not the last data).
	1	The reception of the object data specification range has been completed (the last data).
	2	Failed in communication.
	3	An error was detected in the peripheral hardware of Bluetooth.
	4	Failed to allocate memory.
	5	The process has been cancelled by the device.

15.5   Glossary

Term	Description
10Base-T /100Base-TX /1000Base-T	A set of specifications under the Ethernet standards. Those cables that consist of twisted copper wire pairs are used. The transmission speed of 10Base-T is 10 Mbps, of 100Base-TX is 100 Mbps, and of 1000Base-T is 1000 Mbps.
2in1	A function to send the original by double-page spread, consolidating two pages on a sheet.
2-Sided Binding Direction	A function to specify the binding position of a double-sided document when it is sent using ADF. Two types of binding positions are available for a double-sided original: One is the top/bottom binding with the binding position at the top or bottom of the original. The other is left/right binding with the binding position at the left (or right) of the original. Note that the second side of the original has a different top/bottom relationship.
Abbreviated/address	A function to register frequently used fax numbers of recipients. When registering abbreviated/addresses, you should also register the destination name and the search string, so that you can specify the destination using the search string to select.
Active Directory	A network service provided by Microsoft. Active Directory can centrally manage all types of information including servers, clients, printers and other hardware resources, as well as properties and access permissions of users on the network.
Adobe® Flash®	Software or its file format developed by Adobe Systems Inc. (formerly by Macromedia, Inc.), used to create a content by compiling vector-graphic animations and sounds. The software allows handling interactive contents using keyboard or mouse. The files can be kept relatively compact and accessed from a Web browser with dedicated plug-in software.
Anonymous FTP	While FTP sites are usually protected using some account name and password mechanism, an anonymous FTP system permits anyone to access the FTP site by simply entering "anonymous" as the account name, without a password.
APOP	The acronym for Authenticated Post Office Protocol. While usual POP does not encrypt the password used for receiving an E-mail, APOP encrypts the password. This authentication method helps enhance the E-mail security.
AppleTalk	The generic name for the protocol suite developed by Apple Computer for computer networking.
Auto IP	A function to obtain an IP address automatically. If one fails to get an IP address via DHCP, the auto IP gets an IP address from the space of "169.254.0.0".
Background Removal	A function to adjust the shading of background color before sending the original.
Batch transmission	A function to send documents as one document at a specified time if the documents have the same transmission conditions such as destination, transmission time, memory transmission or resolution, and are stored in the same memory.
Baudrate	The transmission rate of a modem. This machine can communicate at a high transmission rate of 33,600bps. When selecting overseas communication mode, the machine communicates at 7200bps or 4800bps, a rate suitable for noise-resistance.
bit	The abbreviation for binary digit. The smallest unit of information (data quantity) handled by a computer or printer. A bit uses only a 0 or a 1 to indicate data.
Bitmap Font	A font using a collection of dots to present characters. Jagged edges are conspicuous for the larger size Bitmap Font characters.
Bluetooth	One of short-range wireless communication technologies used to connect portable information devices, which are a few meters apart. This function enables you to wirelessly connect a laptop computer, PDA, or cellular phone to transfer voices or data.
BMP	The abbreviation for bitmap. It is a file format used to save image data. (The file extension is ".bmp"). Commonly used on Windows platforms. BMP covers the color depth from monochrome (2 values) to full color (16,777,216 colors). BMP images are not suitable for compressed storage.

Term	Description
Bonjour	A Macintosh network technology, automatically detecting a device connected to the network for automatic configuration. Previously called "Rendezvous", and has been changed to "Bonjour" since Mac OS X v10.4.
Book Copy	A function to separate the front cover, back cover, right pages, and left pages into individual pages when sending a book or catalog by fax.
BOOTP	The abbreviation for Bootstrap Protocol. The protocol is used for a client computer on the TCP/IP network to load network configuration automatically from a server. Instead of BOOTP, DHCP, an advanced protocol based on BOOTP, is typically used today.
bps	The acronym for bit per second, which is a unit of data transmission, indicating the amount of data transmitted per second.
Brightness	Brightness of a display or other screen.
Broadcast	A transmission of a single original to multiple recipients in one operation.
Bulletin board	A function to post documents to be viewed, or to store the documents to be transmitted via polling.
Byte	A byte indicates a unit of information (data quantity) handled by a computer or printer. A byte consists of eight bits.
Check Dest. & Send	A function to send a fax after comparing the specified fax number with the fax number information of the recipient (CSI). Only when those numbers match, the function sends the fax. If the numbers are not matched, a transmission error occurs. Therefore, this prevents misdirected transmissions.
Client	A computer using services provided by servers via the network.
Closed Network RX	A function to accept only transmissions from recipient machines with a matching password.
Compact PDF/XPS	A compression method for minimizing the data size using the PDF or XPS format, used when digitalizing color documents. Compact PDF allows high compression performance by identifying the text and image regions, and applying the resolution and compression method optimized for each region. The compact PDF method can be selected in this machine when using the scanning function to digitalize documents.
Confidential communication	A function used to transmit an original only to specific people who you want to read it. Originals sent via confidential communication are not printed when received, and are saved in a confidential box of the recipient's fax machine. The document can be printed by some specific operation such as entering the access code for the confidential box.
Contrast	The difference in intensity between the light and dark parts of the image (light/dark variation). "Low contrast" indicates an image with little light/dark variation, while "High contrast" an image with large light/dark variation.
CSV	The acronym for Comma Separated Values, which is one of the formats used for saving database or spreadsheet data as a text file. (The file extension is ".csv".) Data can be shared among different applications by being separated by commas (as the delimiter).
Default	An initial setting. The settings selected in advance and enabled when the machine is turned on, or the settings selected in advance and enabled when the function is activated.
Default Gateway	A device, such as a computer or router, used as a "gateway" to access computers on different LANs.
Default value	A setting value configured for the machine prior to shipment from the factory. Some default values can be changed by using the settings menu. It will be convenient to set a frequently used value to the default value according to your application.
Density	The amount of density of an image.
Density Compensation	A color tone correction function used for output devices such as printers and displays.

Term	Description
DHCP	The acronym for Dynamic Host Configuration Protocol. The protocol is used for a client computer on the TCP/IP network to load network configuration automatically from a server. Just using a DHCP server to centrally manage IP addresses of the DHCP clients enables you to construct a network without IP address conflicts or other troubles.
Dialing Method	There are three Dialing methods: PB (push-button dialing), 10PPS (pulse dialing /10 pps), and 20PPS (pulse dialing /20 pps).
Dither	A method of presenting the quasi-shading of gray using black and white colors. This method is easier to process than error diffusion, but may stir some unevenness on the image.
DNS	The acronym for Domain Name System. DNS allows for obtaining the IP address corresponding to a host name in network environments. This system enables a user to access other computers on the network by specifying host names instead of elusive and non-intuitive IP addresses.
DPI (dpi)	The acronym for Dots Per Inch. A unit of resolution used for printers and scanners. This indicates the number of dots used to represent an inch. The higher this value, the higher the resolution.
Driver	Software that works as a bridge between a computer and a peripheral device.
DSN	The acronym for Delivery Status Notifications, which is a delivery status notification message being returned from a receiver to a sender when the E-mail is delivered to the receiver's mail server.
Dynamic authentication (LDAP setting)	An authentication method option used when connecting to a LDAP server form a multifunctional product. Select this option if you want an user to enter the login name and password each time the user logs on the LDAP server to refer to destination information.
ECM	The acronym for Error Correction Mode. An error resending method used for G3 communication. ECM checks whether the data is correctly sent to the destination, and should it be not the case, ECM resends the same data while maintains the serial communication. If a receiver also provides the ECM mode, this machine uses the ECM-based communication with the receiver unless the ECM mode is disabled.
Erase	A function of erasing dark shadow around the document before transmitting it via fax, when scanning a booklet form document or a document with ADF kept open.
Ethernet	LAN transmission line standard.
F-Code	A communication procedure related to the usage of subaddress of T.30* standardized by ITU-T (international telecommunication union).F code is provided by Japanese Communications Industrial Corporation. Various kinds of capabilities are available for the communication among fax machines with the F code function irrespective of difference of the fax machine brand. This machine uses F code for the bulletin boards, relay request, confidential communication, and password transmission. (* a communication standard)
File extension	Characters added to a file name for the recognition of the file format. The file extension is added after a dot of a file name, for example, ".bmp" or ".jpg".
Forced memory reception	A function to store received documents in memory, and print them when required.
Frame type	A type of communication format used in NetWare environments. For mutual communication, the same frame type is required.
FTP	The acronym for File Transfer Protocol, which is used to transfer files via the Internet, intranet or other TCP/IP network.
G3	A fax communication mode standardized by the ITU-T (International Telecommunication Union). G3 and G4 are provided for the communication modes. Today, G3 is more widely used than G4.
Gateway	Hardware and software used as the point where a network is connected to a network. A gateway not only connects networks but also changes data formats, addresses, and protocols according to the connected networks.
Gradation	The shading levels of an image. Larger number of the levels can reproduce smoother transition of the shading.

Term	Description
Gray scale	A form presenting monochrome image by using the gradation information shifting from black to white.
Group	The grouping of multiple abbreviation numbers. It will be convenient to use the group when a volume of serial broadcasts or serial pollings are distributed to the same destination addresses.
GSS-SPNEGO/ Simple/Digest MD5	Authentication methods used for logging in to the LDAP server. The different authentication method, GSS-SPENEGO, SIMPLE or Digest MD5 is used for a LDAP server depending on the type of the server being used or server settings.
Halftone	A method for presenting the shading of an image by using different sizes of black and white dots
Hard disk	A large capacity storage device for storing data. The data is retained even after the power is turned off.
Host name	The name of a device on the network.
HTTP	The acronym for HyperText Transfer Protocol. This is a protocol used to send or receive data between a Web server and a client (such as a Web browser). HTTP can exchange files such as images, sounds, and movies that are associated with documents, including their presentation formats and other information.
IEEE802.1X	A standard used in a wired or wireless LAN to authenticate terminals gaining access to the network. A LAN switch compatible with IEEE802.1X permits a user to connect with the LAN after authentication (to confirm whether the user is authorized).
Install	To install hardware, operating systems, applications, printer drivers, or other software on to a computer.
Internet Fax	A transmission method by which the scanned original data is transmitted among Internet fax machines and computers as TIFF format E-mail attachments via the intranet (in-house network) and the Internet.
IP Address	An address or a code used to identify an individual network device on the Internet. IPv4 (Internet Protocol version 4), a protocol widely used today, adopts a 32-bit number for an IP address separated into four sections. An example of an IPv4 IP address is: 192.168.1.10. On the other hand, IPv6 (Internet Protocol version 6), the next generation protocol, adopts 128-bit IP addresses. The IP address is assigned to every computer or other device connected to the Internet.
IP Address Fax	The IP is an address or code used to identify individual devices on the Internet. IP Address Fax uses the addresses to send or receive faxes within the intranet.
IPP	The acronym for Internet Printing Protocol, which is used to send or receive print data or control printers via the Internet or other TCP/IP network. IPP can also send and print data to printers in remote areas via the Internet.
IPsec	The name of a security technology used for the TCP/IP network. IPsec allows service with enhanced security by determining the protocol used for the encryption of transmit packets and for authentication.
IPv6	The acronym for Internet Protocol version 6. With the number of devices on the Internet increasing, the IPv6 protocol has been arranged to replace the current IPv4 protocol. 128-bit IP addressing system and expanded security features.
IPX	One of the protocols used for NetWare. IPX runs in the network layer of the OSI reference model.
IPX/SPX	The abbreviation for Internetwork Packet Exchange/Sequenced Packet Exchange, which is a protocol developed by Novell, Inc., typically used in NetWare environments.
JPEG	The acronym for Joint Photographic Experts Group. It is a file format used to save image data. The compression ratio is generally 1/10 to 1/100. JPEG is an effective method to compress photographs and other natural images.
Kerberos	A network authentication system used for Windows 2000 or later, used as the Active Directory authentication. Kerberos arranges an authentic site within the network to provide two-phase authentication processes of users login and the use of network resources, allowing users to be securely and efficiently authenticated.

Term	Description
LAN	The acronym for Local Area Network, which is a network constructed by connecting computers on the same floor, in the same building, or in neighboring buildings.
LDAP	The acronym for Lightweight Directory Access Protocol, which is a protocol used to access a database that can manage E-mail addresses and environmental information of network users on the Internet, intranet, or other TCP/IP network.
LLMNR	The acronym for Link-local Multicast Name Resolution,which is a protocol used for the name resolution of neighboring computers. LLMNR uses simple exchange of request and response messages to perform name resolution of neighboring computers without configuring DNS server or clients.
LLTD	The acronym for Link Layer Topology Discovery,which is a technology investigating how the devices on the network are connected.Network devices with this technology are recognized by Windows Vista/Server 2008/7 on the network, and displayed as icons configured on the network map of Windows Vista/7
Local printer	A printer connected to a parallel or USB port of a computer.
Long Original	A function to send original pages longer than the standard size. Long size documents can be sent by selecting this function.
LPD	The acronym for Line Printer Daemon. This is a platform-independent printer protocol running on the TCP/IP network. The protocol was originally developed for BSD UNIX, and has become one of the printing protocols typically used among general computers.
LPR/LPD	The acronym for Line Printer Request/Line Printer Daemon. This is a printing method implemented via networks, used for Windows NT or UNIX based systems. It uses TCP/IP to output printing data from Windows or UNIX to a printer on the network.
MAC address	MAC is the acronym for Media Access Control. A MAC address is an ID number unique to each Ethernet card, enabling sending or receiving data to or from other Ethernet cards. A Mac address consists of 48-bit numbers. The first 24 bits are controlled by IEEE and used to allocate a unique number to each manufacture, whereas the latter 24 bits are used by each manufacturer to assign a unique number to each card.
Main Scanning	The operation of scanning a document optically, and converting the document into image data.
Main scanning direction	The horizontal direction for scanning originals.
Manual transmission	An operation to send a fax while checking the status of the receiver.
MDN	The acronym for Message Disposition Notifications,which is a message sent to confirm that the mail has been unsealed, a response to a sender when the sender requests for doing so.
Memory	A storage device used for storing data temporarily. Some types of memory retain data even after the power is turned off, while others not.
Memory overflow	A condition where the fax memory becomes full while scanned documents or temporarily stored documents are saved.
Memory transmission	A method used to start a fax transmission after scanning originals and storing them in memory. If memory transmission is used, the total number of pages are automatically printed in the page number of the transmission source information and an image of the first page of the sent document is printed in the transmission report. However, the memory may become full if the document contains many pages, or there is a large amount of information due to high image quality.
MH	The acronym for Modified Huffman, which is a data compression encoding method used for fax transmissions. Text-based originals are compressed to approximately 1/10 the original size.
MIB	The acronym for Management Information Base, which defines the format of management information for network devices that are collected using SNMP in TCP/IP communication. Two types of MIB are provided, that is, the private MIB specific to each manufacturer and the standardized MIB.
Mixed Original	A function to set different sizes of originals, detect the size of each original, and send them accordingly.

Term	Description
MMR	The acronym for Modified Modified Read, which is a data compression encoding method used for fax transmissions. Text-based originals are compressed to approximately 1/20 the original size.
Multi Page TIFF	A TIFF file that contains multiple pages.
NDPS	The acronym for Novell Distributed Print Services. This provides a high performance printing solution in NDS environments. By using the NDPS as a printer server, you can output from the desired printer, automatically download the printer driver of a newly installed printer, simplify and automate complicated management environments related to printer use, and integrate management related to the network printer.
NDS	The acronym for Novell Directory Services. This allows the centralized management in a hierarchical structure of shared resources such as servers, printers and users information on the network, as well as the access privilege and other information related to the users.
NetBEUI	The abbreviation for NetBIOS Extended User Interface. This is a network protocol developed by IBM. NetBEUI enables you to construct a small-scale network simply by configuring computer names.
NetBIOS	The abbreviation for Network Basic Input Output System,which is a communication interface developed by IBM.
NetWare	A network operating system developed by Novell. This uses NetWare IPX/SPX for the communication protocol.
Nprinter/Rprinter	A remote printer support module used when using a printer server in NetWare environments. Rprinter is used for NetWare 3.x, and Nprinter for NetWare 4.x.
NTLM	The acronym for NT LAN Manager, which is a user authentication method used for Windows NT or later. NTLM encodes password using MD4 or MD5 encoding method.
NTP	The acronym for Network Time Protocol, which is a protocol used to adjust the computer's internal clock precisely via the network. In a hierarchical method, the time is adjusted with the server at the highest level using GPS to acquire the correct time, which is then referenced by each lower level host.
Number of Originals	Transmission with information of the total number of pages. A function used for quick memory transmission. This allows the recipient to check whether the all pages were received or not (In case of memory transmission, the total no. of pages are automatically added).
OCR	The acronym for Optical Character Reader, which is a device or software that converts handwritten or printed characters to text data by optically scanning them and comparing them with previously stored patterns for identification.
OHP/OHT	A transparent sheet used for OHP (Overhead projector). This is used for presentations.
OS	The acronym for Operating System. This is base software used to control the system of a computer. Windows, MacOS, or Unix is an OS.
Outline font	A font using lines and curves to display an outline of a character. Large characters can be displayed on a screen or printed with no jagged edges.
Overseas communication	This is a function used to communicate with an overseas recipient. If an overseas communication mode is set, the fax is sent with a lower speed. Specifying an overseas transmission mode ensures the fax transmission when faxing to the location where transmission conditions are poor, even within the country.
Password TX	A function to send a fax with a password. If the recipient's fax machine is set to closed network reception, the sender's fax machine should transmit the same password as used for the closed network reception.
PASV	The abbreviation for PASsiVe, a mode used to connect to an FTP server from within a firewall. If this mode is not selected, the firewall regards the access as unauthorized and blocks the connection, disabling any file transmission.
Pause	A temporary break in dialing. In this machine, each pause creates a one second break during dialing.
PB	A push telephone line.
PC-FAX	A function to send a fax directly from a computer without using paper.

Term	Description
PDF	The acronym for Portable Document Format. This is an electronically formatted document with file extension of ".pdf". PDF is a PostScript based format, and can be viewed using Adobe Acrobat Reader, a free viewer software.
PDL	The acronym for Page Description Language. This is a language used to instruct a page printer about images being printed on each page.
Peer-to-peer	A type of network allowing connected devices to communicate each other without using a dedicated server.
Pixel	The smallest constitutional unit of an image.
Plug and play	A mechanism of immediately detecting a peripheral device when it is connected to a computer, and automatically searching an appropriate driver so that the device becomes operable.
Polling	A function available on the receiver's side to request a sender to send originals set or stored in the sender's machine or memory.
POP Before SMTP	A user authentication method used when sending E-mail messages. POP Before SMTP receives E-mail messages first, then authenticates the user using the POP server. The IP address, passed through the user authentication by the POP server, is then permitted to use the SMTP server. This method prevents third parties without permission to use the mail server from sending mail messages.
POP3	The acronym for Post Office Protocol - Version 3,which is a commonly used transmission protocol (transmission convention) for the transmission and reception of E-mail. POP3 has functions including mail box authentication, E-mail download, list information check, and E-mail deletion.
Port Number	A number used to identify the transmission port assigned to each process running on a computer on the network. The same port cannot be used by multiple processes.
PostScript	A typical page-descriptive language developed by Adobe and is commonly used for high quality printing.
PPD	The acronym for PostScript Printer Description, which is a file with the description of resolution, available paper sizes, and other information specific to a PostScript printer model.
PPI	The acronym for Pixels Per Inch, which is a unit of resolution used mainly for monitors or scanners. PPI indicates how many pixels are contained per inch.
Preview	A function allowing you to view an image before being processed for printing or scanning.
Print job	Print request transmitted from a computer to a printing device.
Print queue	A software system used by a spooler to save generated print jobs.
Printer buffer	A memory area temporarily used for processing data of print jobs.
Printer driver	Software that works as a bridge between a computer and a printer.
Program	A function to register frequently used destination fax numbers, or stereotyped transmission operation procedures. By simply pressing a program key, you can specify the destination, or configure a function automatically to start communication.
Property	Attribute information. When using a printer driver, you can use its property to configure different functions. Also by using a file property, you can check the attribute information about the file.
Protocol	A rule enabling a computer to communicate with other computers or peripherals.
Proxy server	A server installed for the connection with the Internet. A proxy server acts as a proxy of client computers to contact the Internet to ensure security effectively for the total organization.
PServer	A print server module available in Netware environments. This module monitors, changes, pauses, restarts, or cancels print jobs.
Queue name	A logical printer name required for LPD/LPR printing. A name assigned to each device for allowing printing to the device via network.

Term	Description
Quick memory transmission	A method used to start sending fax immediately after scanning a page of the original. This method allows even an original with many pages to be sent without overflowing the memory.
RAW port number	A TCP port number used when the RAW protocol is selected for Windows or other TCP printing. The RAW port number is usually set to 9100.
realm (IPP setting)	An area used for allowing security functions. The area is used to organize user names, passwords and other authentication information, and define the security policy in the area.
Receiving	A fax machine status when it receives a call.
Redial	A function to re-dial a fax number after waiting for a specified length of time when recipient's line is busy. Both manual redial and automatic redial functions are available.
Reference Allowed Level	A feature for specifying settings so that only certain people are able to view certain destination information for the security of the information. When synchronized with user authentication, only information with an access permission level matching that specified for the user can be viewed.
Referral setting (LDAP setting)	If no relevant destination data is found on an LDAP server, the LDAP server itself instructs which LDAP server to be searched for the next. The referral setting configures whether the multifunctional product is responsible for searching the next LDAP server.
Relay broadcast	A function to broadcast fax messages via other fax machine (called a relay distribution station). When you have multiple broadcast destinations in remote place, you may configure one of the destinations as a relay station to transfer the broadcast via the relay station, so that you can reduce the total communication rate.
Relay distribution station	A feature to broadcast the fax to the relay distribution destination by receiving the relay request from the relay instruction station. The relay distribution function is not available in this machine.
Relay instruction station	A fax machine sending a relay broadcast request.
Resending	A function to select and resend a document that was not send but stored in the memory. The document can be resent either to the same destination or to another destination.
Resolution	The resolution value indicates how much detail of an object can be reproduced precisely on an image or a print matter.
RGB	The acronym for Red, Green, and Blue. The RGB are the three primary colors used on monitors and other devices to reproduce full colors by changing their brightness ratio.
RIP	The acronym for Raster Image Processor. RIP extracts picture images from text data created using PostScript or other page description language. This processor is usually integrated into a printer.
S/MIME	The acronym for Secure/Multipurpose Internet Mail Extensions,which is a protocol used to add encryption, digital signature, and other features to MIME (E-mail operations). Public key method is used for encryption, using a different key for encryption and decryption.
Samba	UNIX server software which uses SMB (Server Message Block) to make UNIX system resources available to Windows environments.
Scan Size	A function to specify the scanning size of an original to transmit it. If the width of the paper in the recipient's fax machine is smaller than that of the transmitted document, the document will usually be reduced for printing purposes. If you do not want to reduce the document size, specify the same document size as that of the paper in the recipient's fax machine, so that you can send the document with its original size.
Scanning	The reading of an image in scanner operation by moving aligned image sensors step by step. The direction of moving image sensors is called the main scanning direction, and the direction of image sensors alignment is called the sub-scanning direction.
Screen font	A font used for displaying characters/symbols on a CRT or other monitor.

Term	Description
Screen frequency	The density of dots used to create the image.
Sender Fax No.	An identification code used for the mutual recognition for fax transmission. Usually the fax number is registered for the fax ID.
Sender Name	The name of a sender. On the receiver's side, the name is printed as a part of the sender's information at the edge of the transmitted original.
Sending	Sending indicates making a call. For fax, sending indicates sending originals or dialing for pollings.
Shared printer	A printer connected to a server on the network and configured to be used by multiple computers.
Sharpness	A function to enhance the edge of characters before sending the document.
Single-page TIFF	A TIFF file that contains only a single page.
SLP	The acronym for Service Location Protocol, which is a protocol capable of finding services on the TCP/IP network, and the automatic configuration of clients.
SMB	The acronym for Server Message Block, which is a protocol allowing the share of files and printers mainly over the Windows network.
SMTP	The acronym for Simple Mail Transfer Protocol, which is a protocol used to transmit or transfer E-mail.
SNMP	The acronym for Simple Network Management Protocol, which is a management protocol in the TCP/IP network environments.
Spool	The acronym for Simultaneous Peripheral Operation On-Line. Data to be output to a printer is not sent directly to the printer, but is temporarily stored in another location. The stored data is then sent collectively to the printer.
SSL/TLS	The acronym for Secure Socket Layer/Transport Layer Security,which is an encoding method used to transmit data between the Web server and a browser in a secure manner.
Subnet mask	A value used to divide a TCP/IP network into small networks (subnetworks). This is used to identify how many higher-order bits of an IP address are used for the network address.
Sub-scanning direction	The vertical direction for scanning originals.
Super G3 (SG3)	A G3 communication mode complying with ITU-T V.34. Compared with usual G3 communication, it allows the higher rate transmission (up to 33,400bps).
TCP/IP	The acronym for Transmission Control Protocol/Internet Protocol, which is a de facto standard protocol widely used for the Internet. An IP address is used to identify each network device.
TCP Socket	TCP Socket indicates an API used for the TCP/IP network. This socket is used to open a transmission route for input or output of usual files.
Temporary document saving	A function to save received documents automatically to memory when the machine is unable to print the documents for some reason such as running out of paper. When a proper action is taken such as refilling of paper, the temporarily saved document is printed out.
Temporary forward transmission	A function to manually forward the received original that is in the standby state to be output, by using the setting check button on the **Control Panel**. The function must be set while the fax/scan screen is displayed, otherwise the operation will be halted due to the paper running out or a paper jam.
Thumbnail	A function to display the content of an image or document file as a small image (image displayed when the file is opened).
TIFF	The acronym for Tagged Image File Format. It is a file format used to save image data. (The file extension is ".tif"). By using the "tag" indicating the data type, information for various image formats can be saved in a single image data.
Timer TX	A function to transmit a fax at the specified time. It reduce costs by transmitting faxes in the late evening or early morning when discount telephone services are available.
Transmission reservation	A function to program the next transmission during transmission or printing.

Term	Description
Transmission source record	The transmission time, name, telephone number, page number, and other information on the sender's side printed at the edge of the document on the receiver's side.
Transmission time	The time needed to send a fax. The higher the resolution or larger the paper, the longer the transmission takes.
TrueType	A type of outline font developed by Apple and Microsoft, and currently used as a standard font type for Macintosh and Windows. This type of font can be used both for display and printing.
TSI	The acronym for Transmitting Subscriber Identification, which is the ID of a fax transmission terminal.
TWAIN	An interface standard defined for between imaging devices including scanners and digital cameras and applications including graphics software. To use a TWAIN compatible device, a relevant TWAIN driver is required.
Uninstallation	To delete software installed on a computer
USB	The acronym for Universal Serial Bus,which is a general-purpose interface defined for connecting a mouse, printer, and other devices with a computer.
V34	A communication mode used for super G3 fax transmission. Super G3 mode transmission may not be activated because of a telephone line status where the receiver's or sender's machine is connected to a telephone line via a private branch exchange switchboard. If this occurs, the G3 mode should be disabled by turning V34 off.
Web browser	Software used to view Web pages. Typical Web browsers include Internet Explorer and Netscape Navigator.
Web service	Which is a technology useful for detecting a device on the network, using the device functions or obtaining the device information. Web service comes equipped with Windows Vista/7, and is used to detect devices on the network and to perform printing or scanning via the network.
WINS	The acronym for Windows Internet Naming Service. This is a service, available in Windows environments, to call the name server responsible for conversion between a computer name and an IP address.
Z-Folded Original	This function first determines the document size that cannot be detected correctly because of folds, then scans and sends the document after the verification. This function is available only when the original is scanned by ADF.
Zone	A name used for an AppleTalk network. Zone is used to group multiple devices on the AppleTalk network.

16 Index

16   Index

16.1   Index by item

16.2   Index by button

KONICA MINOLTA

http://konicaminolta.com