Table of contents

8 Configuring the Printing Environment

9 Configuring the Fax Environment

12 Restricting Users from Using this Device

13 Reinforcing Security

15 Registering Various Types of Information

16 Associating with External Application

1 Web Connection

1 Web Connection

Web Connection

Web Connection is a built in utility software product for management use.

By using a Web browser on your computer, you can simply confirm the status of this machine and configure various machine settings.

Although character input such as address entry and network setting is a difficult process using the touch panel, it can be carried out easily if you use the computer.

Operating environment

Item	Specifications
Network	Ethernet (TCP/IP)
Web browser	Microsoft Internet Explorer 9/10/11 Microsoft Edge Mozilla Firefox 20 or later Google Chrome 26 or later Safari 6.0.3 or later • JavaScript and Cookies must be enabled by your Web browser. • Also, you need to enable the MSXML3.0 (Free Threaded XML DOM Document and XSL Template) add-on.

2 Operations Required to Use Web Connection

2 Operations Required to Use Web Connection

2.1 Configuring network environment settings

Overview

To connect this machine to the network (TCP/IP), follow the procedure below to configure settings.

1 Assigning an IP address to this machine

➔ If this machine has a fixed IP address, enter the IP address, subnet mask, and default gateway. For details, refer to page 2-2.

➔ To automatically obtain the IP address of this machine using DHCP, enable the Auto Input function for automatically obtaining an IP address from DHCP (default: enabled). For details, refer to page 2-2.

➔ For details on how to use this machine in the IPv6 environment, refer to page 5-4.

2 Confirming the IP address assigned to this machine

➔ When you access **Web Connection**, you need the IP address of this machine. For the IP address confirmation procedure, refer to page 2-3.

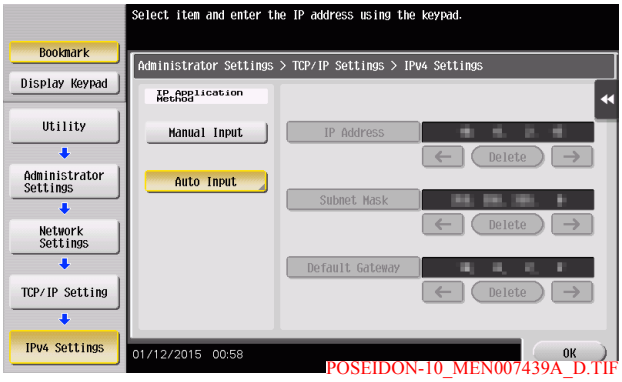
NOTICE

If the IP address of this machine is changed, the screen is displayed to indicate that network setting data is being processed. Never turn the main power off while processing data. When processing is completed, the IP address is updated.

Assigning an IP address

If this machine has a fixed IP address, manually enter the IP address, subnet mask, and default gateway address.

In the **Control Panel**, tap [Utility] - [Administrator Settings] - [Network Settings] - [TCP/IP Setting] - [IPv4 Settings], then configure the following setting.



Settings	Description
[IP Application Method]	To manually enter the IP address, select [Manual Input]. To automatically obtain the IP address using DHCP, select [Auto Input], then specify the auto input method. [Auto Input] is specified by default.
[IP Address]	Enter the fixed IP address assigned to the machine.
[Subnet Mask]	Enter the subnet mask.
[Default Gateway]	Enter the default gateway.

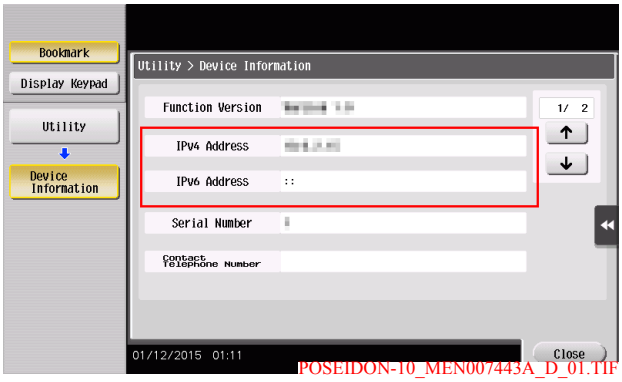
Tips

- When Quick IP Filtering is enabled, you may fail to access **Web Connection**. If you cannot access **Web Connection**, set Quick IP Filtering to [No Filtering]. For details on Quick IP Filtering, refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]".

Confirming the IP address

Confirm the IP address assigned to this machine When you access **Web Connection**, you need the IP address of this machine.

In the **Control Panel**, select [Utility] - [Device Information], then confirm the IP address of this machine.



2.2 Confirming Web browser settings

The **Web Connection** page may not be displayed correctly or changed settings may not be applied depending on your Web browser settings.

Before using **Web Connection**, confirm the following settings in the Web browser.

- JavaScript: Must be enabled.
- Cookies: Must be enabled.
- The MSXML3.0 (Free Threaded XML DOM Document and XSL Template) add-on must be enabled.

If your PC is connected to the Internet via a proxy server in your network environment, register this machine as an exception under the proxy settings of the Web browser.

- If you are using Internet Explorer, select [Internet Options] from the [Tools] menu. In the [Connections] tab, click [LAN settings], and click [Advanced] under [Proxy server]. In the [Exceptions] text box, enter the IP address or the host name of this machine and click [OK].
- If you are using Microsoft Edge, select [Set] - [Network and Internet] - [Ethernet] - [Internet Options] from the Start menu. In the [Connections] tab, click [LAN settings], and click [Advanced] under [Proxy server]. In the [Exceptions] text box, enter the IP address or the host name of this machine and click [OK].
- If you are using Firefox (Windows), select [Options] from the [Tools] menu. Click [Settings] in the [Network] tab under the [Advanced] menu, and select [Manual proxy configuration]. In the [No Proxy for] text box, enter the IP address or the host name of this machine and click [OK].
- If you are using Firefox (Mac OS), select [Preferences...] from the [Firefox] menu. Click [Settings...] in the [Network] tab under the [Advanced] menu, and select [Manual proxy configuration]. In the [No Proxy for] text box, enter the IP address or the host name of this machine and click [OK].

Tips

If the **Web Connection** page is not correctly displayed even though the above settings have been configured, the Web browser cache may be the cause of the problem. If that is the case, clear the Web browser cache.

- If you are using Internet Explorer, select [Internet Options] from the [Tools] menu. In [Browsing history] under the [General] tab, click [Delete]. Select [Temporary Internet files], and click [Delete].
- If you are using Microsoft Edge, select […] - [SETTINGS]. In [Clear browsing data], click [Choose what to clear]. Select the [Cached data and files] check box, then click [Clear].
- If you are using Firefox (Windows), select [Options] from the [Tools] menu. In the [Network] tab under the [Advanced] menu, click [Clear Now] in the cache section.
- If you are using Firefox (Mac OS), select [Preferences...] from the [Firefox] menu. In the [Network] tab under the [Advanced] menu, click [Clear Now] in the cache section.

Reference

For details on how to confirm and change settings, refer to the Help of your Web browser.

3 Basic Usage

3 Basic Usage

3.1 How to access

This section describes how to access **Web Connection**.

1 Start the Web browser.

2 Enter the IP address of the machine in the URL field, then press [Enter].

➔ Example: When the IP address of this machine is 192.168.1.20, enter "http://192.168.1.20/".

➔ For details on how to confirm the IP address of this machine, refer to page 2-3.

The **Web Connection** screen appears.

Tips

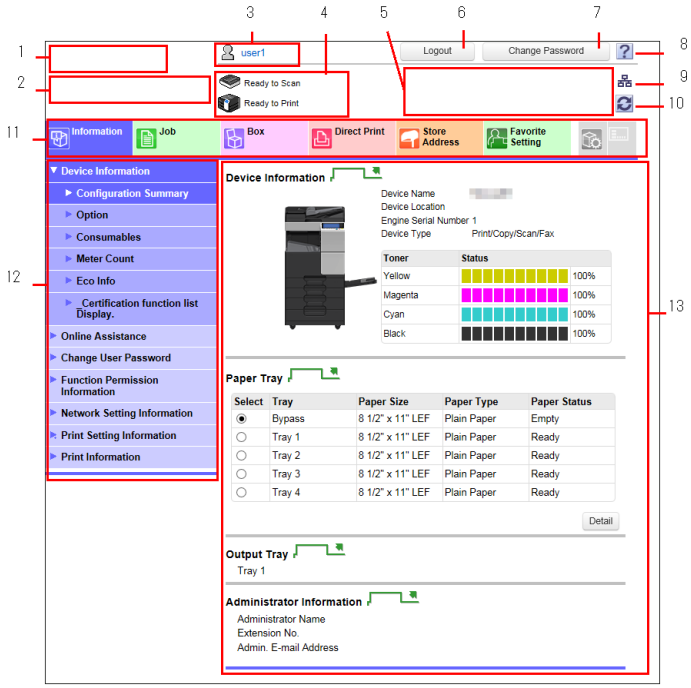
- If the WINS server is installed to resolve the name, you can access by specifying the host name of this machine. The host name of this machine is registered in the hosts file on the computer (C:\Windows\System32\drivers\etc\hosts), and is usually assigned by the administrator. For details, contact the administrator of this machine.
- In the IPv6 environment, enclose the IPv6 address in brackets [ ].
  Example: When the IPv6 address of this machine is fe80::220:6bff:fe10:2f16, enter "http://[fe80::220:6bff:fe10:2f16] /".

3.2 Layout of Web Connection screen

The **Web Connection** screen mainly consists of following three parts.

- Top of the screen: Displays the name of login user and the status of the machine.
- Left of the screen: Displays the function menu of **Web Connection**.
- Right of the screen: Displays the contents of the selected menu.

This example shows the items in [Information] - [Device Information] to explain sections in each screen.



5G-21_MEN010183B_D_01.TIF

No.	Item	Description
1	KONICA MINOLTA logo	Click the logo to jump to the KONICA MINOLTA site (http://www.konicaminolta.com/).
2	**Web Connection** logo	Click this logo to display the version information of **Web Connection**.
3	Login user name	Displays the login mode and user name. Click the user name when you log on as a registered user to confirm the user information.
4	Status display	Displays the status of this machine. Displays the status of the printer and scanner sections of this machine with icons and messages. If you click this icon when an error occurs, you can check the error status such as consumables, paper trays, or user registration information.
5	Message display	You can check the operating status of this machine with the message.
6	[To Login Screen]/[Logout]	Click this button to log out of **Web Connection**.
7	[Change Password]	Changes the password of the registered user. Click this button to jump to the user password change screen. This button is enabled only when you log on as a registered user.
8	Help	Displays the online help of **Web Connection**. Detailed descriptions of the currently set functions can be viewed.
9	Warning indicator icon	Notifies whether a network error has occurred. You can view detailed information on the error if you click this icon when an error occurs.
10	Refresh	Click this button to update the screen.

No.	Item	Description
11	Menu category	Menu items are divided into some categories depending on each content. The available menu categories vary depending on which optional units are installed on this machine.
12	Menu	Click the category of the menu to display the menu items of that category.
13	Information and settings	Click the menu at the left of the screen, and the contents of that menu will appear.

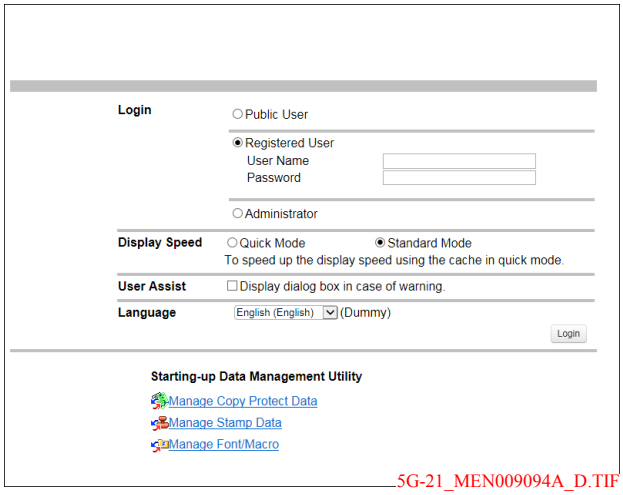
3.3 Login methods

Login screen

When you access **Web Connection**, this screen appears first. Enter the required information such as a user name, and log in to **Web Connection**.

Tips

- If you have not configured authentication settings on this machine, the screen in the public user mode appears instead of the Login screen.
- The screen that appears differs depending on whether Authentication is enabled on this machine. Also, operations available after you log in differ depending on the information you enter in this Login screen.



5G-21_MEN009094A_D.TIF

Item	Description
[Login]	Select a mode to log in. The login mode differs depending on the user type. The user mode and administrator mode are available as login modes. For details, refer to page 3-6.
[Display Speed]	Select the display speed of **Web Connection**. If [Quick Mode] is selected, you can log in to **Web Connection** in the quick mode. The quick mode allows you to save data such as images in the cache memory of the Web browser, thus increasing operation speed.
[User Assist]	Enables display of warning contents in the dialog box when a warning occurs while operating this machine after login.
[Language]	Select a language to be used in display of **Web Connection**.

Tips

- To log in using the quick mode after updating the firmware of this machine, delete cache data of the Web browser once.
- To log in using the standard mode after logging in using the quick mode, delete cache data of the Web browser.

Login mode

Web Connection has multiple login modes, and available operations differ depending on the mode.

Two login modes of **Web Connection** are provided: the "administrator mode" which is used to configure settings of this machine and the "user mode" which enables use of the functions of this machine.

Login mode		Description
Administrator Mode		Enables the administrator of this machine to log in to configure settings of this machine. To log in, you need to enter the administrator password of this machine. Logging in as the administrator enables you to use the following category menus. • [Maintenance] • [System Settings] • [Security] • [User Auth/Account Track] • [Network] • [Box] • [Print Setting] • [Store Address] • [Fax Settings] • [Wizard] • [Customize]
User mode		Enables a user such as a registered user, public user, or User Box administrator to log in to this machine. The user can confirm the status of this machine, use the files in the user box, perform direct print, register an address, and other functions of this machine. The login method and operations available after login differ depending on the login user type.
	[Registered User]	Enables a user or account track registered to this machine to log in. To log in, enable the authentication setting on this machine and register the user or account track. Logging in as a registered user enables you to use the following category menus. • [Information] • [Job] • [User Box] • [Direct Print] • [Store Address] • [Favorite Setting] • [Customize]
	[Administrator (User Mode)]	Enables the administrator of this machine to log in as a user with administrator authority. When you log in to this machine in this mode, you cannot change the settings of this machine. To log in, you need to enter the administrator password of this machine. In this mode, you can delete jobs.
	[User Box Administrator]	Enables you to log in as the administrator dedicated to the user box. To log in, you need to enter the box administrator password of this machine. In this mode, you can use the box registered on this machine regardless of the setting of box password. To use the UserBoxAdmin.Setting mode, enable the box administrator on this machine.
	[Public User]	Enables a user not registered on this machine to log in as a public user. When usage by public users is not allowed on this machine, this mode is not available.

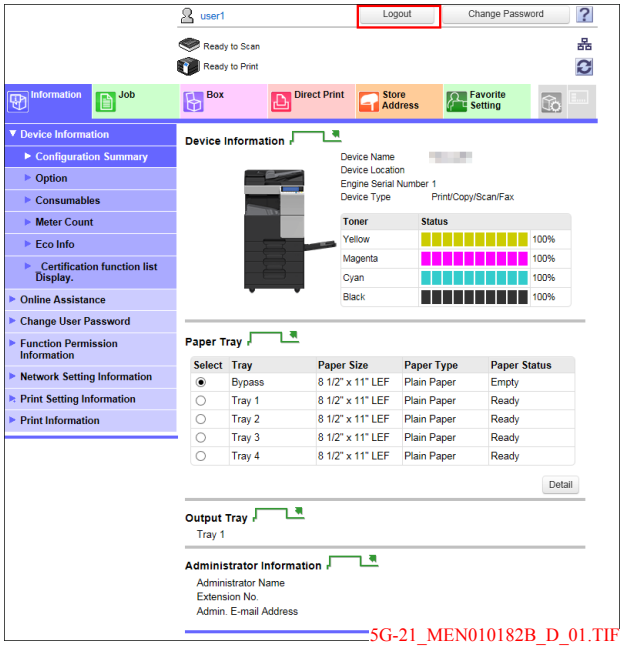
Tips

- The user who has administrator privileges can log in to this machine in administrator mode. For details, refer to page 3-9.
- The **Hard Disk** is optional in some areas. To use the following functions, the optional **Hard Disk** is required.
  [User Box], [User Box Administrator]

Switching login modes

When changing to other login mode after logging in to **Web Connection**, log out of Web Connection once.

1 Log out of **Web Connection**.



5G-21_MEN010182B_D_01.TIF

➔ When you are in the public user mode, click [To Login Screen].

➔ When you are in the mode other than the public user mode, click [Logout].

The Login screen appears.

2 Select a login mode, and enter required information.

➔ To log in to the administrator mode, refer to page 3-7.

➔ To log in to the user mode, refer to page 3-10.

3 Click [Login].

The screen for the selected login mode appears.

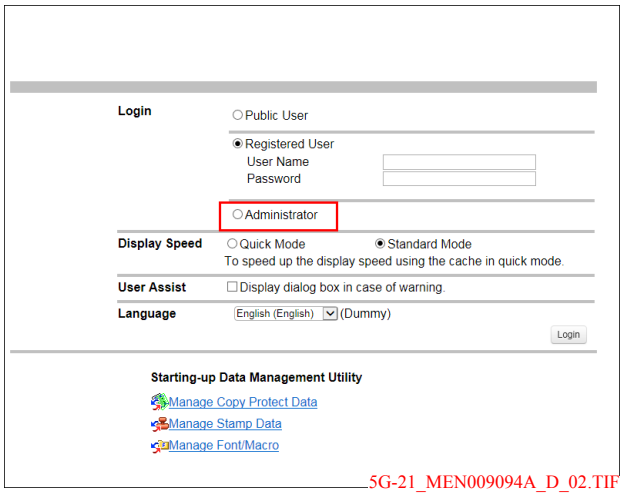
Tips

- If you do not operate this machine for a given period of time after you log in to **Web Connection**, you will automatically be logged out.
- If the authentication setting is changed on the **Control Panel** while you are logging in to the user mode of **Web Connection**, you will automatically be logged out.

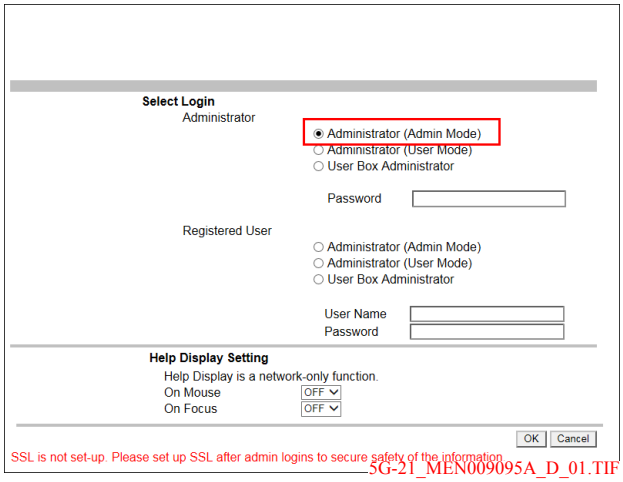
Logging in to the administrator mode

Logging in to the administrator mode enables you to configure settings for this machine.

1 On the Login screen, select [Administrator] and click [Login].



2 Select [Administrator (Admin Mode)].

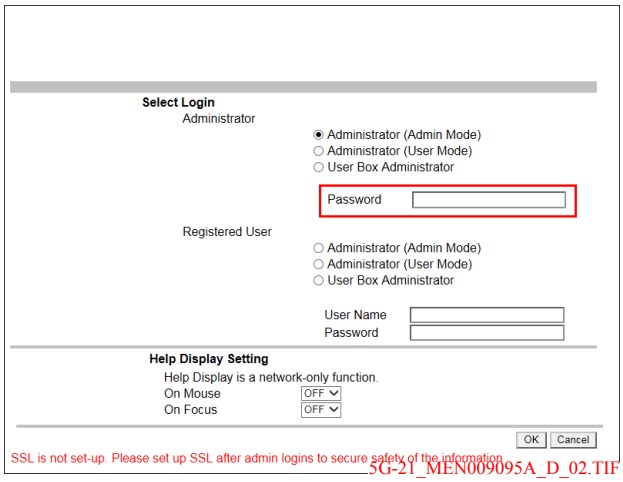


➔ When the administrator of this machine wants to log in to the user mode, select [Administrator (User Mode)].

➔ When the administrator of this machine logs in as a User Box administrator, select [User Box Administrator]. For details on the User Box administrator, refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]".

➔ The display of the password entry screen differs depending on the settings of this machine.

3 Enter the administrator password, then click [OK].



The administrator mode window appears.

Tips

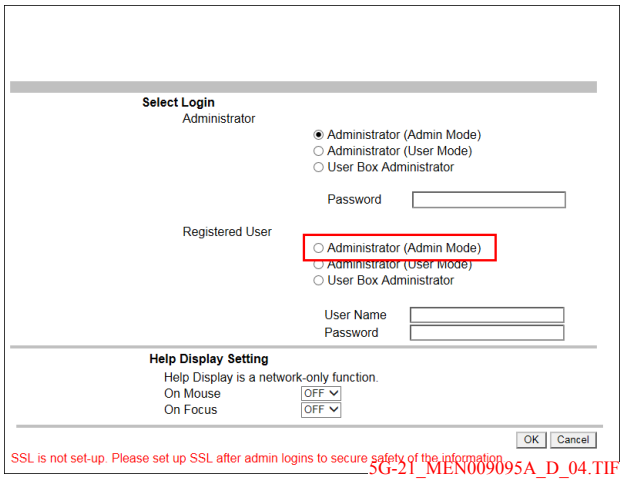
- You can log in to the administrator mode to change settings of this machine even when a job is running or an error or paper jam is occurring on this machine. However, setting change that affects an active job will not be immediately reflected. To check whether settings have been reflected, select [Maintenance] - [Confirm update settings for Held Jobs.] in the administrator mode.
- Depending on the status of this machine, you may not be able to log in to the administrator mode.
- In [Help Display Setting], you can select whether to display pop-up help in the network menu that opens when you log in to this machine in administrator mode. For details on the pop-up help, refer to page 3-19.

Logging in to administrator mode (For a registered user with administrator privileges)

If the registered user has administrator privileges, the user can log in to the administrator mode to configure this machine.

1 On the Login screen, select [Administrator] and click [Login].

2 Select [Administrator (Admin Mode)].



5G-21_MEN009095A_D_04.TIF

➔ When the registered user of this machine logs in to the user mode using administrator privileges, select [Administrator (User Mode)].

➔ When the registered user of this machine logs in as a User Box administrator, select [User Box Administrator]. For details on the User Box administrator, refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]".

➔ The display of the password entry screen differs depending on the settings of this machine.

3 Enter the user name and password, then click [OK].

The administrator mode window appears.

Tips

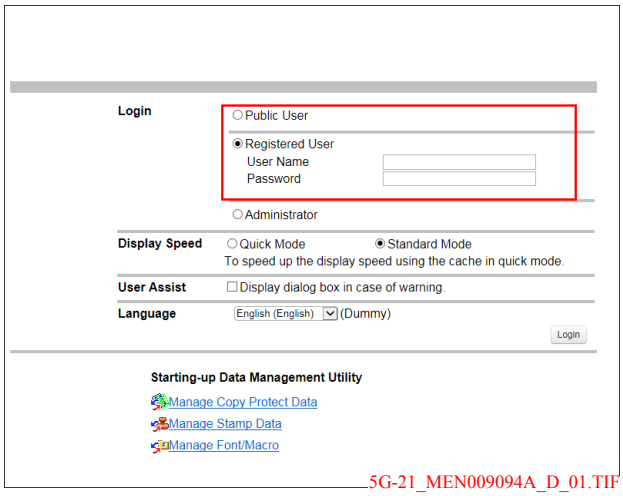
- You can log in to the administrator mode to change settings of this machine even when a job is running or an error or paper jam is occurring on this machine. However, setting change that affects an active job will not be immediately reflected. To check whether settings have been reflected, select [Maintenance] - [Confirm update settings for Held Jobs.] in the administrator mode.
- Depending on the status of this machine, you may not be able to log in to the administrator mode.
- In [Help Display Setting], you can select whether to display pop-up help in the network menu that opens when you log in to this machine in administrator mode. For details on the pop-up help, refer to page 3-19.

Logging in to the user mode

In the user mode, you can use the functions such as box operations and direct print. You can log in as a registered user or public user.

To log in as a registered user, select [Registered User] on the Login screen.

Enter the user name and password, then click [Login].



5G-21_MEN009094A_D_01.TIF

Tips

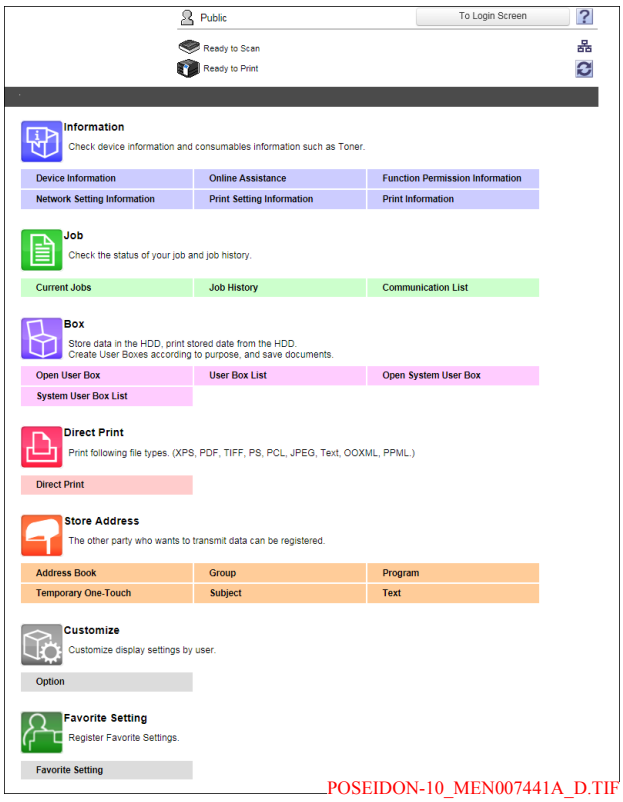
- Displaying a list of user names enables you to select a login user. To display a list of user names, on the **Control Panel**, tap [Utility] - [Administrator Settings] - [User Authentication/ Account Track] - [User Authentication Setting] - [Administrative Settings], and set [User Name List] to [ON].
- When an external authentication server is used, select the server.
- To log in as a public user, select [Public User], then click [Login] on the Login screen.

3.4 User Mode Overview

3.4.1 Main Menu

Displaying the Main Menu enables you to display the menus available in **Web Connection** on a single screen. By doing this, you can quickly access the screen to use to implement required operations.

To display the Main Menu, click the icon on the upper right of the screen (<C754_MEN983A_D.TIF>).

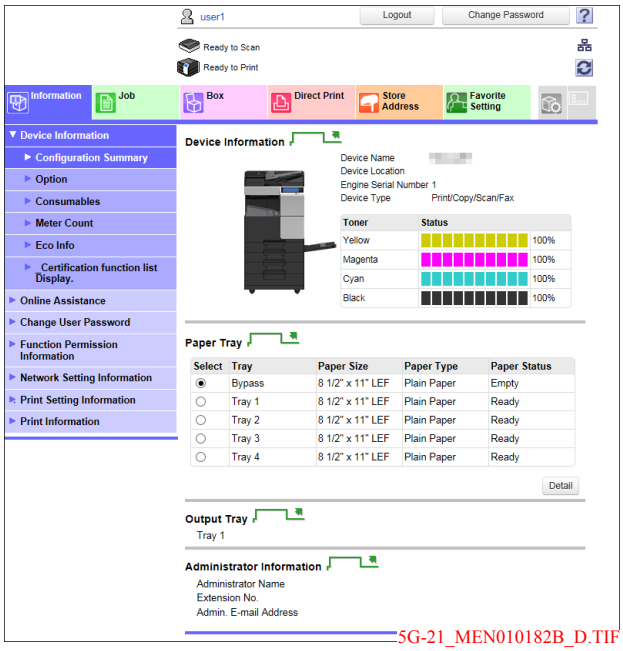


POSEIDON-10_MEN007441A_D.TIF

3.4.2 Each mode in the user mode

[Information]

Enables you to confirm the information on the system configuration and settings of this machine.

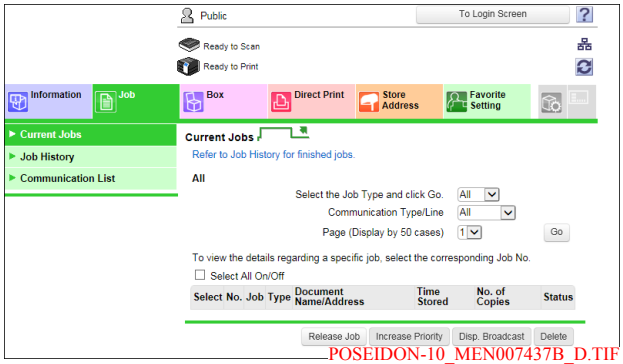


5G-21_MEN010182B_D.TIF

Menu	Description
[Device Information]	Enables you to check the components, options, consumables, meter counts, and eco information of this machine.
[Online Assistance]	Enables you to check the online assistance about this product.
[Change User Password]	Changes the password of the login user.
[Synchronize User Authentication & Account Track]	Enables the login user to change the settings for synchronizing your own user authentication and account track.
[Function Permission Information]	Enables you to check the function permission information about the user or account.
[Network Setting Information]	Enables you to check the network settings of this machine.
[Print Setting Information]	Enables you to confirm the information on the settings for the printer function of this machine.
[Print Information]	Prints font or configuration information.

[Job]

Enables you to check the job currently being performed and the job log.

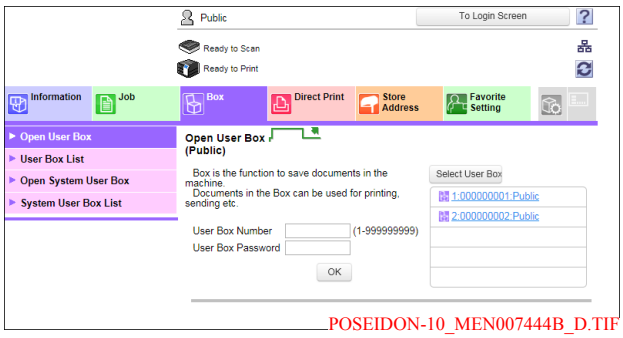


POSEIDON-10_MEN007437B_D.TIF

Menu	Description
[Current Jobs]	Enables you to check the job currently being performed and the job to be performed. Also, it enables you to instruct to preferentially execute a queued print job or delete a send job for which the proof print function is specified through the printer driver. If logged in as a registered user, login user jobs can also be operated.
[Job History]	Enables you to check the log of jobs processed on this machine.
[Communication List]	Enables you to confirm the list of results of scan transmission, fax transmission, and fax reception.

[Box]

Enables you to create a user box on this machine, print a file from the user box, and send a file.



POSEIDON-10_MEN007444B_D.TIF

Menu	Description
[Open User Box]	Allows you to open a Public, Personal, or Group User Box, and print, send, or download a file saved in the User Box. For details on how to use a file in a User Box, refer to "User's Guide[Box Operations]/[Store Documents as Files in MFP and Use Them Again When Necessary]".
[User Box List]	Displays a list of User Boxes registered in this machine. You can create a new User Box or change settings for the created User Box.
[Open System User Box]	Opens the System User Box (Bulletin Board, Polling TX, or Memory RX) to enable you to use a file saved in the User Box. To use this function, install the optional **Fax Kit** in this machine or enable the Internet Fax function.
[System User Box List]	Displays a list of System User Boxes (Bulletin Board, Relay, and Annotation User Box) registered in this machine. You can create a new System User Box or change settings for the created System User Box. To use this function, the optional **Fax Kit** is required.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

[Direct Print]

Direct Print is a function that enables you to directly send PDF (Ver.1.6), JPEG, TIFF, XPS, PS, PCL, Text, OOXML (.docx/.xlsx/.pptx), and PPML (.ppml/.vdx/.zip) files on your computer to this machine to print them without using the printer driver.

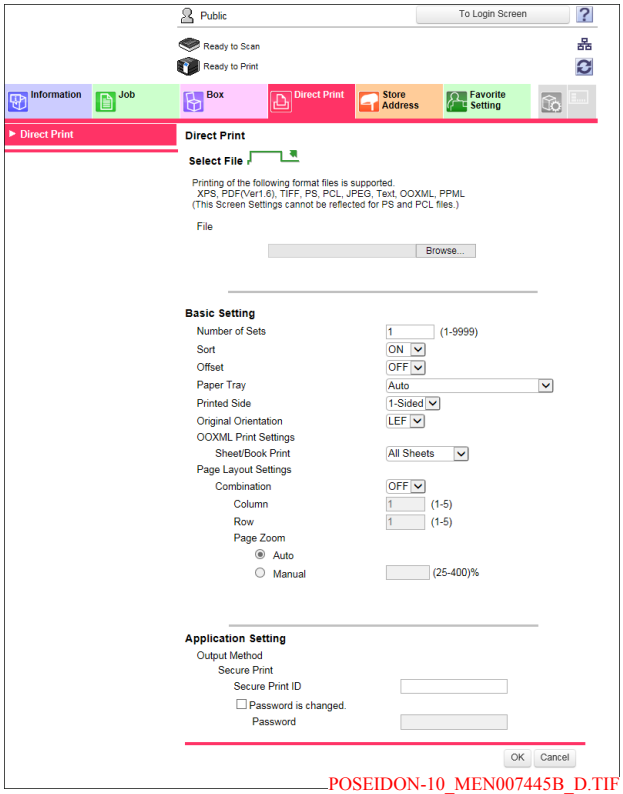
A text file supports only 1-byte characters.

Reference

For details on the direct print function, refer to "User's Guide[Print Operations]/[Printing without Using the Printer Driver]".

Related setting

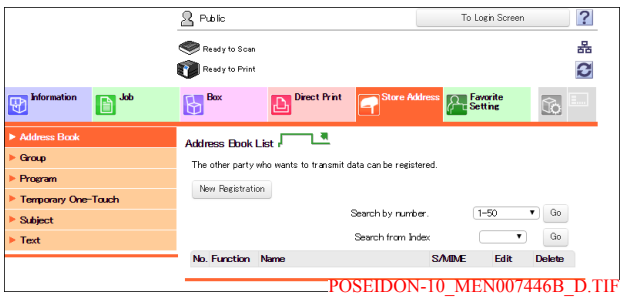
- To print a text file, you need to set [PDL Setting] to [Auto] (default: [Auto]). For details, refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]".



POSEIDON-10_MEN007445B_D.TIF

[Store Address]

Enables you to register frequently-used destinations and edit the registration content.

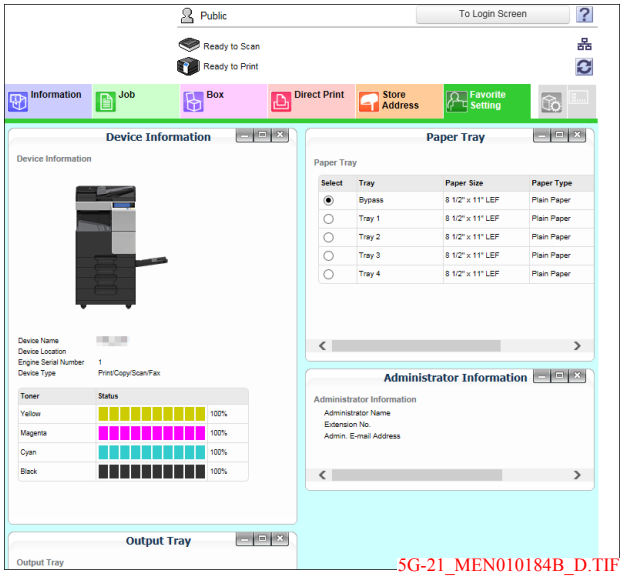


POSEIDON-10_MEN007446B_D.TIF

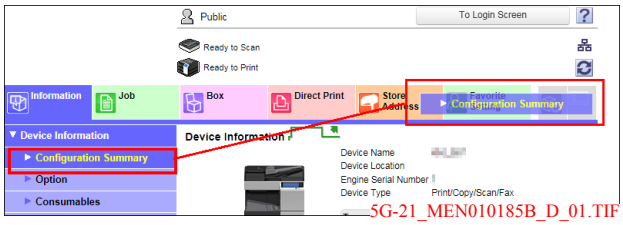
Menu	Description
[Address Book]	Enables you to register frequently-used destinations on this machine. Also, it enables you to confirm or edit the registered content of the destination registered on this machine.
[Group]	Enables you to register multiple destinations as a group. Also, it enables you to confirm or edit the registered content of the group destination registered on this machine.
[Program]	Enables you to register a combination of frequently-used option settings as a recall key (program). Also, it enables you to confirm or edit the registered content of the program registered on this machine.
[Temporary One-Touch]	Enables you to register a program used on a temporary basis. A temporary one-touch destination is deleted once data is sent to the registered destination or when the machine is turned OFF.
[Subject]	Registers subjects when sending E-mails.
[Text]	Registers body messages when sending E-mails.

[Favorite Setting]

Collectively displays frequently used functions as a single tab.

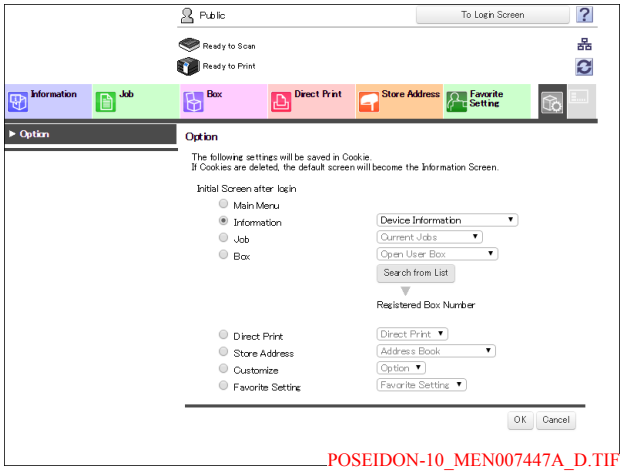


To register a function as [Favorite Setting], drag and drop its menu into the [Favorite Setting] tab.



[Customize]

Enables you to select a screen to be displayed after logging in to the user mode.



POSEIDON-10_MEN007447A_D.TIF

3.5 Using the Shortcut Function

Registering a function in Bookmarks of the Web browser

Each **Web Connection** function page can be registered in Bookmarks of the Web browser.

Display a page of a function to be registered in Bookmarks, and register it in Bookmarks of the Web browser.

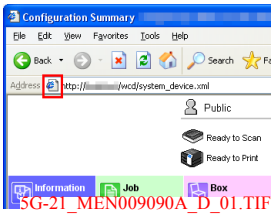
Tips

- For details on how to register a function in Bookmarks, refer to your Web browser's Help function.
- If a page of a registered user is registered in Bookmarks while user authentication is enabled, the page used to log in to the user mode will be displayed when displaying a registered page.
- If a page in Administrator mode is registered in Bookmarks, the page used to log in to Administrator mode will be displayed when displaying a registered page.
- If you have updated the firmware of this machine after logging in using the quick mode, delete cache data of the Web browser before displaying the registered page.

Creating a shortcut for a specific page

You can create a shortcut to each **Web Connection** function page at any location such as the desktop of your computer.

To create a shortcut, drag and drop the icon displayed in the address bar of the Web browser to any location on your computer.



SG-21_MEN009090A_D_01.TIF

3.6 Using the Help function

Using the online help

Log in to **Web Connection** and click <C754_MCO990A_D.TIF>, and you will be able to display the online help. The online help shows you the detailed descriptions of the function being set.

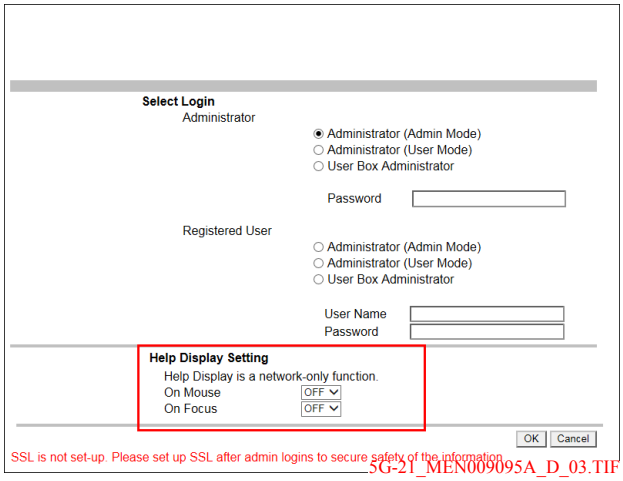
To display the online help, you must connect your computer to the Internet.

Displaying the meaning of the setting in the popup window

In the [Network] menu that appears after you log in to the administrator mode of **Web Connection**, you can use the popup help.

Placing the mouse cursor on the item of the screen (On Mouse) or clicking the item (On Focus) displays the description of that item in the pop-up window. While confirming the meaning of the item, you can configure network settings.

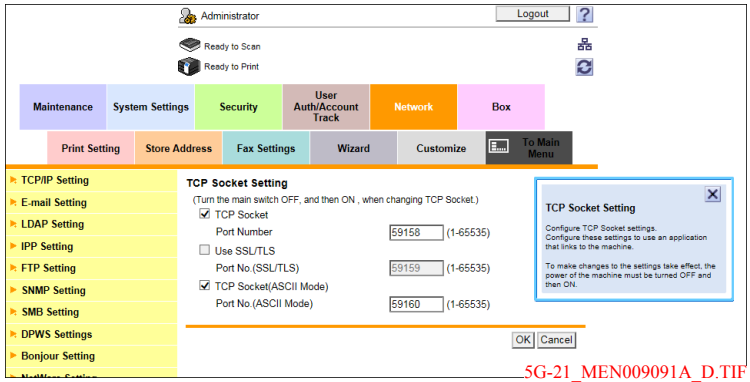
In the screen to log in to the administrator mode, you can specify the method to display the popup help.



5G-21_MEN009095A_D_03.TIF

Settings	Description
[On Mouse]	If you select [ON], the popup help is displayed when you place the mouse cursor on an item of the screen.
[On Focus]	If you select [ON], the popup help is displayed when you click the entry area or option of a setting item.

The popup help is displayed as shown below.



5G-21_MEN009091A_D.TIF

Using the wizard when configuring function settings

Some settings can be simply configured by entering settings as instructed in the screen via a wizard.

Setting using the wizard is available for the following functions.

[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)]

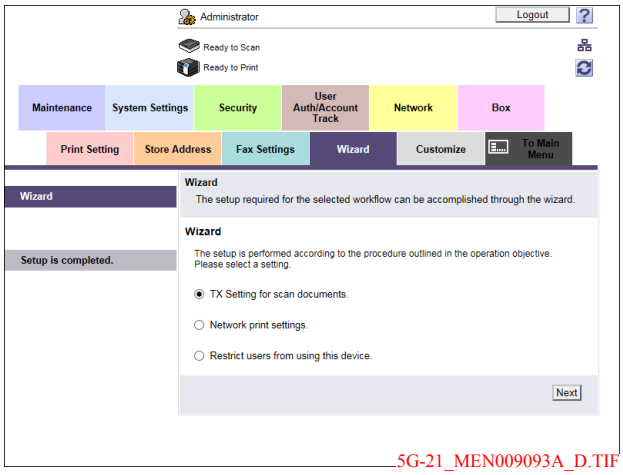
[Network print settings.]

- [LPR Print]
- [Print using RAW port]
- [Print using SMB]

[Restrict users from using this device.]

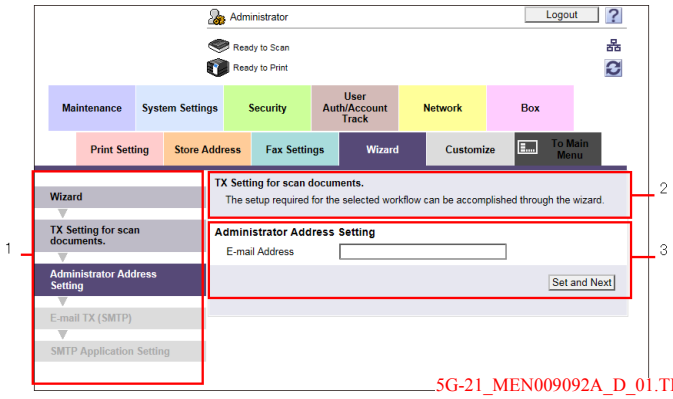
- [Do Not Authenticate]
- [User Authentication Only]
- [Account Track Only]
- [External Authentication Server]

To configure settings using the wizard, log in to the administrator mode, then select [Wizard].



5G-21_MEN009093A_D.TIF

The wizard screen is comprised of the following components.



5G-21_MEN009092A_D_01.TIF

No.	Item	Description
1	Flow	Displays the setting flow. The current setting item is displayed in dark gray by which you can confirm the setting flow step you are in. Click one of the previous setting items to return to it and redo settings.

No.	Item	Description
2	Purpose of the wizard	Displays the title of the wizard being set.
3	Check Job	Displays the setting item conforming to the flow.

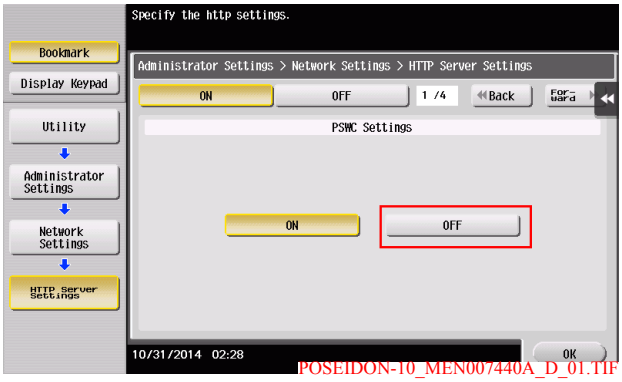
Tips

- If you return to one of the previous setting items in the flow, you must redo settings at that item. The settings subsequent to the item to which you returned are not saved.
- To finish the wizard during the setting process, click [Setup is completed.].

3.7 Restricting use of Web Connection

If you do not want other people to use **Web Connection**, you can restrict use of **Web Connection** on the **Control Panel**.

On the **Control Panel**, tap [Utility] - [Administrator Settings] - [Network Settings] - [HTTP Server Settings], and set [PSWC Settings] to [OFF] (Default: [ON]).



4 Configuring Basic Information Settings of this Machine

4 Configuring Basic Information Settings of this Machine

4.1 Registering information of this machine

Register device information of this machine such as the name, installed place, and information of the administrator.

Registering device information enables you to confirm it by selecting [Information] - [Device Information] - [Configuration Summary] in the user mode of **Web Connection**.

In the administrator mode, select [System Settings] - [Machine Setting], then configure the following settings.

Settings		Description
[Device Location]		Enter the location where to install this machine (using up to 255 characters).
[Administrator Registration]		Register information on the administrator of this machine.
	[Administrator Name]	Enter the administrator name of this machine (using up to 20 characters).
	[E-mail Address]	Enter the E-mail address of the administrator of this machine (using up to 128 characters, excluding spaces). This E-mail address is used as the sender's E-mail address. Therefore, to use the E-mail TX function, you must configure settings.
	[Extension No.]	Enter the extension number of the administrator of this machine (using up to eight characters).
[Input Machine Address]		Register the name and E-mail address of this machine.
	[Device Name]	Enter the name of this machine (using up to 80 characters). The name specified in this item is used as a part of a file name given automatically, for example, when using a scan transmission.
	[E-mail Address]	Enter the E-mail address of this machine with 320 characters, excluding spaces. This E-mail address is used as sender Internet fax address. Therefore, to use the Internet fax function, you must configure settings.

4.2 Registering support information

Enter the support information of the machine such as contact name information for the machine and online help URL.

Registering support information enables the user to confirm it by selecting [Information] - [Online Assistance] in the user mode of **Web Connection**.

In the administrator mode, select [System Settings] - [Register Support Information], then configure the following settings.

Settings	Description
[Contact Name]	Enter the contact name of this machine (using up to 63 characters).
[Contact Information]	Enter the contact information of this machine such as the phone number or URL (using up to 127 characters).
[Product Help URL]	Enter the Product Help URL of this machine (using up to 127 characters).
[Corporate URL]	Enter the URL of the Web page for the manufacturer of this machine (using up to 127 characters).
[Supplies and Accessories]	Enter consumables supplier information (using up to 127 characters).
[Online Help URL]	If necessary, change the **Web Connection** online help URL (using up to 127 characters). The online help appears when you click <C754_MCO990A_D.TIF>on the upper right of the **Web Connection** screen.
[Driver URL]	If necessary, enter the URL of the place where the driver of this machine is stored (using up to 127 characters). Enter an appropriate URL to suit your environment.
[Engine Serial Number]	Enables you to confirm the serial number of this machine.

Tips

- The default values of the [Online Help URL] are as follows. If you have changed the default value or deleted it, enter the following URL.
  For **bizhub C287**:
  http://www.pagescope.com/download/webconnection/onlinehelp/C287/help.html
  For **bizhub C227**:
  http://www.pagescope.com/download/webconnection/onlinehelp/C227/help.html

4.3 Setting the date and time for the machine

Manually configuring settings

Manually specify the current date and time of this machine.

In the administrator mode, select [Maintenance] - [Date/Time Setting] - [Manual Setting], then configure the following settings.

Settings	Description
[Date]	Specify the current date of this machine. • [Year]: Enter the current year. • [Month]: Enter the current month. • [Day]: Enter the current day.
[Time]	Specify the current time of this machine. • [Hour]: Enter the current hour. • [Minute]: Enter the current minute. • [Time Zone]: Select a time zone (time difference from the world standard time) to suit your environment.

Automatically configuring settings using NTP

Using the NTP (Network Time Protocol) server allows you to automatically adjust the date and time of this machine.

Register the NTP server used. To periodically adjust the date and time by connecting to the NTP server, specify an interval for adjusting the date and time.

✔ To adjust the date and time using the NTP server, you must connect this machine to the network.

1 In the administrator mode, select [Maintenance] - [Date/Time Setting] - [Manual Setting], then configure the [Time Zone] setting.

➔ For details on how to configure [Time Zone] setting, refer to page 4-4.

2 In the administrator mode, select [Maintenance] - [Date/Time Setting] - [Time Adjustment Setting], then configure the following settings.

Settings	Description
[Time Adjustment Setting]	To automatically adjust the date and time of this machine via the NTP server, select [ON]. [OFF] is specified by default.
[Auto IPv6 Retrieval]	Select [ON] to automatically specify the NTP server address. In the IPv6 environment, the NTP server address can be automatically specified by DHCPv6. [ON] is specified by default.
[NTP Server Address]	Enter the NTP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the NTP server port number. In normal circumstances, you can use the original port number. [123] is specified by default.
[Auto Time Adjustment]	To periodically adjust the date and time by connecting to the NTP server, select [ON]. Also, specify an interval for adjusting the date and time at [Polling Interval]. [OFF] is specified by default.
[Polling Interval]	If you select [ON] for [Auto Time Adjustment], specify an interval to automatically adjust the date and time of this machine (unit: hours).

3 Click [Adjust].

Connect to the NTP server, and adjust the date and time of this machine.

5 Configuring Network Settings of this Machine

5 Configuring Network Settings of this Machine

5.1 Using in the IPv4 environment

Overview

To use this machine by connecting it to the IPv4 network, follow the below procedure to configure the settings.

1 Setting the method to assign an IP address to this machine

➔ For details on how to assign an IP address, refer to page 5-2.

2 If you resolve the name using the host name when accessing a computer or server on the network from this machine, register your DNS server address to this machine.

➔ For details on how to register the DNS server, refer to page 5-3.

➔ When you are using the DHCP server, information of the DNS server used for resolving the name may be able to be obtained automatically.

3 If your DNS server supports the Dynamic DNS function, register the host name and domain name of this machine and enable Dynamic DNS, if necessary.

➔ For details on how to register the host name of this machine, refer to page 5-3.

➔ For details on how to register the domain name, refer to page 5-3.

Assigning an IP address

To use this machine in the IPv4 network environment, assign an IP address to this machine.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], then configure the following settings.

Settings	Description
[TCP/IP]	Select [ON] to use the TCP/IP. [ON] is specified by default.
[Network Speed]	Select the network speed according to your environment. [Auto (10M/100Mbps)] is specified by default..
[IP Address Setting Method]	To manually enter the IP address, select [Manual Setting]. To automatically obtain the IP address, select [Auto Setting], then specify the auto input method. In normal circumstances, select the [DHCP] check box. [Auto Setting] is specified by default.
[IP Address]	If you select [Manual Setting] for [IP Address Setting Method], enter the fixed IP address assigned to the machine.
[Subnet Mask]	If you select [Manual Setting] for [IP Address Setting Method], enter the subnet mask.
[Default Gateway]	If you select [Manual Setting] for [IP Address Setting Method], enter the default gateway.

Registering the DNS server used by this machine

If you resolve the name using the host name when accessing a computer or server on the network from this machine, register your DNS server address to this machine.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], then configure the following settings.

Settings	Description
[DNS Server Auto Obtain]	To manually enter the DNS server address, select [Disable]. When using the DHCP, select [Enable]. Then, the DNS server address is automatically obtained from the DHCP server. [Enable] is specified by default.
[Primary DNS Server]	Enter the address of your primary DNS server.
[Secondary DNS Server1] to [Secondary DNS Server2]	When using multiple DNS servers, enter the address of your secondary DNS server.

Registering the host name

If your DNS server supports the Dynamic DNS function, registering the host name to this machine enables the DNS server to resolve the host name and IP address name dynamically. Doing this enables a computer on the network to connect to this machine using the host name.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], then configure the following settings.

Settings	Description
[DNS Host Name]	Enter the host name of this machine (using up to 63 characters, including only - for symbol marks). Any symbol cannot be prefixed or suffixed to the host name.
[Dynamic DNS Setting]	Select [Enable] to use the Dynamic DNS function. If your DNS server supports the Dynamic DNS function, the set host name can be automatically registered to the DNS server or changes can be automatically updated. [Disable] is specified by default.

Registering the domain name

Register the name of a domain this machine joins.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], then configure the following settings.

Settings	Description
[DNS Domain Auto Obtain]	When using the DHCP, the domain name can be automatically specified. Select [Enable] to automatically configure setting. [Enable] is specified by default.
[DNS Search Domain Name Auto Retrieval]	When using the DHCP, the search domain name can be automatically specified. Select [Enable] to automatically configure setting. [Enable] is specified by default.
[DNS Default Domain Name]	When not automatically configuring setting using DHCP, enter the default domain name of this machine (using up to 253 bytes including the host name. Only - and . are allowed for symbol marks).
[DNS Search Domain Name1] to [DNS Search Domain Name3]	When not automatically configuring setting using DHCP, enter the search domain name (using up to 63 characters, including only - and . for symbol marks).

5.2 Using in the IPv6 environment

This machine supports the IPv6 network environment.

To use this machine in the IPv6 network environment, assign an IPv6 address to this machine. It can be used in the IPv4 and IPv6 environments simultaneously.

Tips

- The following SMB sharing functions are also available in the IPv6 environment by enabling the direct hosting SMB service (enabled by default).
  Printing on a SMB sharing printer
  Transmission to a SMB sharing folder
  Search of SMB sharing device
  NTLM-based authentication

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], then configure the following settings.

Settings		Description
[TCP/IP]		Select [ON] to use the TCP/IP. [ON] is specified by default.
[IPv6]		Select [ON] to use the IPv6. [ON] is specified by default.
	[Auto IPv6 Setting]	Select [ON] to automatically specify the IPv6 global address. The IPv6 global address is automatically specified based on the prefix length notified from the router and the MAC address of this machine. [ON] is specified by default.
	[DHCPv6 Setting]	Select [ON] to automatically specify the IPv6 global address using the DHCPv6. [ON] is specified by default.
	[Link-Local Address]	Displays the link-local address. The link-local address is automatically specified from the MAC address of this machine.
	[Global Address]	Enter the IPv6 global address. Use Enter this item to manually specify the address.
	[Prefix Length]	Enter the prefix length of the IPv6 global address between 1 and 128. Use this item to manually specify the address.
	[Gateway Address]	Enter the gateway address. Use this item to manually specify the address.
[DNS Server Setting(IPv6)]		Register the address of the IPv6-compatible DNS server.
	[DNS Server Auto Obtain]	To manually enter the DNS server address, select [Disable]. When using the DHCPv6, select [Enable]. Then, the DNS server address is automatically obtained from the DHCP server. [Enable] is specified by default.
	[Primary DNS Server]	Enter the address of your primary DNS server. Use this item to manually specify the address.
	[Secondary DNS Server1] to [Secondary DNS Server2]	When using multiple DNS servers, enter the address of your secondary DNS server.

5.3 Using this Machine in a Wireless Network Environment

Overview

To use this machine by connecting it to a wireless network environment, follow the below procedure to configure the settings.

✔ The optional **Wireless LAN Interface Kit** is required to use this function.

1 Selecting a network interface configuration.

➔ For details on configuring the setting, refer to page 5-5.

2 Configure a setting to connect this machine to the extended network using TCP/IP.

➔ For details on configuring the setting, refer to page 5-5.

3 Configuring a setting to operate this machine as a wireless LAN adapter or wireless LAN access point.

➔ For details on configuring a setting to operate this machine as a wireless LAN adapter, refer to page 5-6.

➔ For details on configuring a setting to operate this machine as a wireless LAN access point, refer to page 5-8.

➔ For details on configuring a setting to operate this machine as a Wi-Fi Direct group owner, refer to page 5-9.

Setting a network interface configuration

Set a network interface configuration of this machine.

Select [Network] - [Network I/F Configuration] in the administrator mode, then select a target network interface.

- [Wired Only]: Select this option to only use this machine in the wired LAN environment.
- [Wireless Only]: Select this option to only use this machine in the wireless LAN environment. This machine runs as a wireless LAN adapter in the wireless LAN environment.
- [Wired + Wireless (Secondary Mode)]: Select this option to use this machine in both the wired LAN environment and wireless LAN environment. This machine runs as a wireless LAN adapter in the wireless LAN environment.
- [Wired + Wireless (Primary Mode)]: Select this option to use this machine in both the wired LAN environment and wireless LAN environment. This machine runs as a wireless LAN access point in the wireless LAN environment.
- [Wired + Wireless (Wi-Fi Direct)]: Select this option to use this machine in both the wired LAN environment and wireless LAN environment. This machine runs as a Wi-Fi Direct group owner in the wireless LAN environment.

Configuring the basic settings for TCP/IP

Configure a setting to connect this machine to the wireless network using TCP/IP.

Set this option when [Wired + Wireless (Secondary Mode)], [Wired + Wireless (Primary Mode)], or [Wired + Wireless (Wi-Fi Direct)] is selected in [Network] - [Network I/F Configuration] in the administrator mode.

In the administrator mode, select [Network] - [TCP/IP Setting] - [Wireless Setting], then click [OK]. In [TCP/IP Setting (Wireless Setting)], configure the following settings.

Settings	Description
[IPv4]	Configure an IPv4 setting when connecting this machine to the wireless network using IPv4.

Settings		Description
	[IP Address Setting Method]	To manually enter the IP address, select [Manual Setting], then enter the IP address and subnet mask of this machine to be used on the wireless network . To automatically obtain the IP address from the DHCP server, select [Auto Setting] . This setting is only available using Manual Setting when [Wired + Wireless (Primary Mode)] or [Wired + Wireless (Wi-Fi Direct)] is selected in [Network I/F Configuration]. [Auto Setting] is specified by default.
	[IP Address]	If you select [Manual Setting] for [IP Address Setting Method], enter the fixed IP address assigned to the machine.
	[Subnet Mask]	If you select [Manual Setting] for [IP Address Setting Method], enter the subnet mask.
[IPv6]		Configure an IPv6 setting when connecting this machine to the wireless network using IPv6.
	[Link-Local Address]	Displays the link-local address. The link-local address is automatically specified from the MAC address of this machine.

Tips

- For the wireless network address, specify a private IP address or other address that is different from the wired network address. If the same network address group is specified, it will disable a transmission from this machine to the wired network.

Configuring a setting to operate this machine as a wireless LAN adapter

Configure a setting to operate this machine as a wireless LAN adapter and connect to your access point.

Set this option when [Wireless Only] or [Wired + Wireless (Secondary Mode)] is selected in [Network] - [Network I/F Configuration] in the administrator mode.

1 In the administrator mode, select [Network] - [Wireless Network Setting] - [Wireless LAN Adapter], then specify the setting method.

Settings	Description
[Direct Input]	Select this option to directly enter all the setting items such as SSID and the encryption scheme that are required for a connection.
[WPS]	Select this option to automatically obtain information required for a connection from the access point. The access point must support the WPS function. When **Web Connection** is used by specifying the IP address of this machine connected to the wireless network, **Web Connection** is disconnected if WPS is executed.

2 Configure the following settings depending on the setting method you selected in Step 1.

➔ When [Direct Input] is selected:

Settings	Description
[AP Search]	Click this to automatically search for an access point around this machine. Select an access point to be connected to this machine from the displayed list.
[SSID]	Enter the SSID of the access point to be connected to this machine (using up to 32 bytes).
[Authentication/Encryption Algorithm]	Select the algorithm to be used for authentication or encryption. [No Authentication/Encryption] is specified by default.
[WEP Key]	Specify [Key Input Method] and [WEP Key] when [WEP] is selected in [Authentication/Encryption Algorithm]. To specify multiple WEP keys, select the required WEP keys in [Key Selection].
[Passphrase Input Method]	Select the passphrase entry method when an algorithm other than [WEP] or [No Authentication/Encryption] is selected in [Authentication/Encryption Algorithm].
[Passphrase]	Enter the passphrase when an algorithm other than [WEP] or [Authentication/Encryption Algorithm] is selected in [Authentication/Encryption Algorithm]. To change the passphrase, select the [Change Passphrase] check box.
[40 to 20 MHz Auto Switch]	Select [ON] to try a high-speed communication using 40MHz. [OFF] is specified by default.

➔ When [WPS] is selected:

Settings	Description
[Push Button Method]	To try a connection with an access point, select [Push Button Method], then click [OK]. If you press the WPS setting button at the access point, settings such as SSID and security required for a connection are configured automatically. For some access points that use the WPS push-button method, the connection may fail. If this occurs, wait approximately 30 seconds after pressing the button on the access point before connecting the machine.
[PIN Method]	To display the PIN code, select [PIN Method], then click [OK]. If you enter the displayed PIN code at the access point, settings such as SSID and security required for a connection are configured automatically. This function requires a computer that contains Windows 7 or later as the operating system.

Configuring a setting to operate this machine as a wireless LAN access point

Configure a setting to operate this machine as a wireless LAN access point.

Set this option when [Wired + Wireless (Primary Mode)] is selected in [Network] - [Network I/F Configuration] in the administrator mode.

In the administrator mode, select [Network] - [Wireless Network Setting] - [Main Device Wireless Setting], then configure the following settings.

Settings	Description
[SSID]	Enter the SSID to use this machine as a wireless LAN access point (using up to 32 bytes).
[Authentication/Encryption Algorithm]	Select the algorithm to be used for authentication or encryption. [No Authentication/Encryption] is specified by default.
[WEP Key]	Specify [Key Input Method] and [WEP Key] when [WEP] is selected in [Authentication/Encryption Algorithm]. To specify multiple WEP keys, select the required WEP keys in [Key Selection].
[Passphrase]	Specify the passphrase when an algorithm other than [WEP] or [No Authentication/Encryption] is selected in [Authentication/Encryption Algorithm]. • [Passphrase Input Method]: Select the method to enter the passphrase. • [Passphrase]: Enter the passphrase. To change the passphrase, select the [Change Passphrase] check box. • [Passphrase Auto Update]: Select [ON] to automatically update the passphrase. Also, enter the interval to update the passphrase.
[40 to 20 MHz Auto Switch]	Select [ON] to try a high-speed communication using 40MHz. [OFF] is specified by default.
[Wireless Channel]	Select a wireless channel to be used by the access point. Selecting [Auto] searches for a channel that is not being used for other access points, and automatically assigns it to the access point. [Auto] is specified by default.
[ANY Connection]	Select whether to allow ANY connection. If [Restrict] is selected, the SSID cannot be detected automatically as an access point in the wireless LAN adapter side. [Allow] is specified by default.
[MAC address Filtering]	Restricts wireless LAN adapters that can be connected to the access point using the MAC address. Enter the MAC addresses of wireless LAN adapters that can be connected to the access point. MAC addresses of up to 16 devices can be registered.
[DHCP Server Settings]	Configure a setting to use the DHCP server function. • [Enable Settings]: Select whether to enable the DHCP server function. [Disable] is specified by default. • [IPv4 lease address]: Specify the range of IPv4 addresses to be leased from the DHCP server when enabling the DHCP server function. • [Subnet Mask]: Specify the subnet mask of the IPv4 address to be leased from the DHCP server when enabling the DHCP server function. • [Lease period]: Specify the lease period of the IPv4 address to be leased from the DHCP server when enabling the DHCP server function.
[Number of Simultaneous Devices Allowed]	Enter the number of devices that can be connected simultaneously to the access point. [5] devices is specified by default.
[Signal Strength Setting]	Select the radio field intensity of the access point from three levels (Low, Middle, and High). [High] is specified by default.
[Display Connected Devices]	Displays a list of names and MAC addresses of wireless LAN adapters that are connected to the access point.

Configuring a setting to operate this machine as a Wi-Fi Direct group owner

Wi-Fi Direct is a standard that enables direct connection with a wireless terminal without an access point. In this step, configure a setting to operate this machine as a Wi-Fi Direct group owner

Set this option when [Wired + Wireless (Wi-Fi Direct)] is selected in [Network] - [Network I/F Configuration] in the administrator mode.

In the administrator mode, select [Network] - [Wireless Network Setting] - [Main Device Wireless Setting], then configure the following settings.

Settings	Description
[SSID]	Enter the SSID to use this machine as a Wi-Fi Direct group owner (using up to 32 bytes). This option is available when a terminal compatible with Wi-Fi Direct is connected to this machine. The SSID specified here is displayed on the Wi-Fi Direct (setting) screen of the terminal compatible with Wi-Fi Direct. If you cannot connect to this machine by specifying the SSID on the Wi-Fi Direct (setting) screen, specify [Virtual SSID] on the Wi-Fi (setting) screen to make a connection.
[Virtual SSID]	Displays the automatically generated virtual SSID. This option is available when a terminal incompatible with Wi-Fi Direct is connected to this machine. A virtual SSID is displayed on the Wi-Fi (setting) screen of a terminal incompatible with Wi-Fi Direct. The virtual SSID is displayed with "DIRECT-XXXXXX" ("XXXXXX" indicates a combination of the random alphanumeric characters and the specified value of [SSID]).
[Authentication/Encryption Algorithm]	Select the algorithm to be used for authentication or encryption. [No Authentication/Encryption] is specified by default.
[Passphrase]	Specify the WPA passphrase. • [Passphrase Input Method]: Select the method to enter the passphrase. • [Passphrase]: Enter the passphrase. To change the passphrase, select the [Change Passphrase] check box. • [Passphrase Auto Update]: Select [ON] to automatically update the passphrase. Also, enter the interval to update the passphrase.
[40 to 20 MHz Auto Switch]	Select [ON] to try a high-speed communication using 40MHz. [OFF] is specified by default.
[Wireless Channel]	Select a wireless channel to be used by the access point. Selecting [Auto] searches for a channel that is not being used for other access points, and automatically assigns it to the access point. [Auto] is specified by default.
[DHCP Server Settings]	Configure a setting to use the DHCP server function. In general use, DHCP server settings are required. • [Enable Settings]: Select whether to enable the DHCP server function. [Disable] is specified by default. • [IPv4 lease address]: Specify the range of IPv4 addresses to be leased from the DHCP server when enabling the DHCP server function. • [Subnet Mask]: Specify the subnet mask of the IPv4 address to be leased from the DHCP server when enabling the DHCP server function. • [Lease period]: Specify the lease period of the IPv4 address to be leased from the DHCP server when enabling the DHCP server function.
[Number of Simultaneous Devices Allowed]	Enter the number of devices that can be connected simultaneously to the access point. [5] devices is specified by default.
[Signal Strength Setting]	Select the radio field intensity of the access point from three levels (Low, Middle, and High). [High] is specified by default.
[Display Connected Devices]	Displays a list of names and MAC addresses of wireless LAN adapters that are connected to the access point.

Tips

- For details on the Wi-Fi Direct connection method, refer to the user's manual of your terminal.

Checking the communication status of the wireless network environment

You can select [Network] - [Wireless Network Setting] - [Wireless LAN Adapter]-[Connection status.] in the administrator mode to check the access point connected to this machine, the radio field intensity of the access point, and the current communication speed.

Checking the MAC address of the wireless network adapter

You can select [Network] - [Wireless Network Setting] - [Device Setting] in the administrator mode to check the MAC address of the wireless network adapter.

5.4 Using in the IPX environment

This machine supports the IPX. IPX is the NetWare communication protocol, which is the network operating system of Novell.

In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings	Description
[IPX Setting]	Select [ON] to connect to the IPX environment. [OFF] is specified by default.
[Ethernet Frame Type]	Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.

Tips

- In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Status] to confirm the NetWare connection status.

5.5 Displaying this machine on the network map

In Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2), you can display this machine on the network map.

The network map is very useful for checking the location and information of this machine as well as for network troubleshooting. Also, when you click the icon of this machine on the network map, you can access **Web Connection**.

To display this machine on the network map, enable LLTD (Link Layer Topology Discovery).

In the administrator mode, select [Network] - [LLTD Setting], and set [LLTD Setting] to [Enable] (Default: [Enable]).

5.6 Displaying the network error code

If an error relating to the network occurs on this machine, the **Touch Panel** displays an error message with a brief description. To view detailed information for troubleshooting purposes, you can configure settings so that the error code is displayed simultaneously.

In the administrator mode, select [Maintenance] - [Network Error Code Display Setting], and set [Error Code Display] to [ON] (Default: [OFF]).

Reference

For details on the error codes, refer to "User's Guide[Troubleshooting]/[Network Error Codes]".

6 Setting up the Operating Environment of Web Connection

6 Setting up the Operating Environment of Web Connection

6.1 Encrypting communication using Web Connection

You can enhance security by encrypting communication between the computer and **Web Connection** with SSL.

The SSL certificate is registered on this machine when it is shipped. Therefore, only enabling SSL/TLS on this machine allows SSL encrypted communication immediately after the setup.

In the administrator mode, select [Security] - [PKI Settings] - [SSL Setting], then configure the following settings.

Settings	Description
[Mode using SSL/TLS]	Select a mode to perform SSL communication. • [Admin. Mode]: Uses SSL communication in the administrator mode only. • [Admin. Mode and User Mode]: Uses SSL communication in both the administrator mode and user mode. • [None]: Does not use SSL communication. [None] is specified by default.
[Encryption Strength]	Select the SSL encryption strength. Select the file according to your environment. [AES-256, 3DES-168, RC4-128] is specified by default.
[SSL/TLS Version Setting]	Select the version of the SSL to be used. Select the file according to your environment.

Reference

You can create a new certificate without using the certificate registered when it is shipped. For details, refer to page 13-2.

6.2 Changing the administrator password

You can change the administrator password of this machine from **Web Connection**.

✔ To display this page, select [Security] - [PKI Settings] - [SSL Setting] in the administrator mode to encrypt communications between your computer and **Web Connection** using SSL. For details, refer to page 6-2.

1 In the administrator mode, select [Security] - [Administrator Password Setting], and enter a new administrator password (using up to 64 characters, excluding ").

➔ For the administrator password, refer to the booklet manual.

➔ To enter (change) the password, select the [Password is changed.] check box, and then enter a new password.

2 Click [OK].

The administrator password is changed.

Tips

- If you change the administrator password in this screen, the administrator password on the **Control Panel** of this machine is also changed.

6.3 Customizing the initial screen

You can specify the screen to be initially displayed when you log in to the user mode of **Web Connection**.

Setting an appropriate screen as the initial screen according to your operating environment improves work efficiency of the user. For example, if you frequently use the direct print function on this machine, set [Direct Print] as the initial screen.

In the administrator mode, select [System Settings] - [Customize], then configure the following settings.

Settings	Description
[No Selection]	If you select [No Selection], you can set the initial display screen. [No Selection] is specified by default.
[Main Menu]	Displays the Main Menu after logging in.
[Information]	Displays the [Information] tab after logging in. In addition, select which screen of the [Information] tab should be displayed.
[Job]	Displays the [Job] tab after logging in. In addition, select which screen of the [Job] tab should be displayed.
[Box]	Displays the [Box] tab after logging in. In addition, select which screen of the [Box] tab should be displayed. A specified user box can also be opened.
[Direct Print]	Displays [Direct Print] after logging in.
[Store Address]	Displays the [Store Address] tab after logging in In addition, select which screen of the [Store Address] tab should be displayed.
[Favorite Setting]	Displays [Favorite Setting] after login.

Tips

Settings configured here are saved using the Cookies function of your Web browser. Therefore, the settings may not be saved when:

- Deleting Web browser Cookies
- Logging in to **Web Connection** from another Web browser
- Logging in to **Web Connection** from another computer
- Logging in to the computer using another user name

6.4 Changing the time period until automatic log out

If you do not operate this machine for a given period of time after you log in to **Web Connection**, you will automatically be logged out. If necessary, you can change the time period before you are automatically logged out.

The time until automatically log out can be specified for the administrator mode and the user mode respectively. For example, if you set a short time for the administrator mode where settings can be changed, you can decrease the likelihood of operation by a third party. On the other hand, if you set a long time for the user mode, you can keep convenience of use of the Web browser such as address registration that is difficult to perform on the **Touch Panel**.

In the administrator mode, select [Security] - [Auto Logout], then configure the following settings.

Settings	Description
[Admin. Mode Logout Time]	Select a time period until the user is automatically logged out of the administrator mode. [10] minutes is specified by default.
[User Mode Logout Time]	Select a time period until the user is automatically logged out of the user mode. [60] minutes is specified by default.

7 Configuring the Scan Environment

7 Configuring the Scan Environment

7.1 Configuring the Scan to E-mail environment

Overview

The Scan to E-mail is a function that transmits original data scanned on this machine as E-mail attachment.

Since this machine supports S/MIME and SSL/TLS encryption, and POP before SMTP authentication, security can be assured.

When the LDAP server or Active Directory is used for user management, you can search for or specify E-mail address from the server.

When using the Scan to E-mail, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for Scan to E-mail

➔ For details on configuring the setting, refer to page 7-2.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the E-mail server using SSL/TLS	page 7-4
Use of SMTP Authentication when sending E-mails	page 7-4
Use of POP Before SMTP Authentication when sending E-mails	page 7-5
Addition of a digital signature by encrypting E-mails with S/MIME	page 7-7
Search for an E-mail address using the LDAP server or Active Directory	page 7-18

Reference

If user authentication is installed on this machine, the Scan to Me function is available with which the login user can easily transmit E-mail to the login user's own address. For details, refer to page 12-23.

Configuring basic settings for Scan to E-mail

Register the E-mail server (SMTP) address and the administrator's E-mail address.

1 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[E-mail TX Setting]	Select this check box to transmit E-mails. [ON] (selected) is specified by default.
[Scan to E-mail]	Select [ON] to use the Scan to E-mail. [ON] is specified by default.
[E-mail Notification]	If a warning such as paper addition, toner replacement, or paper jam occurs on this machine, it can be sent to a registered E-mail address. For details, refer to page 14-11. [ON] is specified by default.
[Total Counter Notification]	Select whether to use the total counter notification function. Using this function allows you to send counter information managed by this machine to the registered E-mail address. For details, refer to page 14-12. [ON] is specified by default.

Settings	Description
[SMTP Server Address]	Enter the address of your E-mail server (SMTP). Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port Number]	If necessary, change the port number of the E-mail server (SMTP). In normal circumstances, you can use the original port number. [25] is specified by default.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (SMTP), as required. [60] sec. is specified by default.
[Max Mail Size]	If you restrict the size of an E-mail to be sent in your environment, select [Limit]. [No Limit] is specified by default.
[Server Capacity]	If you select [Limit] at [Max Mail Size], enter the maximum E-mail size including attachment. E-mails exceeding the specified size are discarded. If you select [Binary Division] to divide an E-mail, this setting is invalid.
[Binary Division]	Select this check box to divide an E-mail. The E-mail is divided according to the size specified at [Divided Mail Size]. This item is necessary if you occasionally send E-mails exceeding the maximum size specified on the E-mail server side. To read a divided E-mail, the mail soft receiving E-mails must have a function to restore the divided E-mail. The mail soft without the restore function may not read the divided E-mail. [OFF] (not selected) is specified by default.
[Divided Mail Size]	Enter the size to divide an E-mail. This item is necessary when [Binary Division] is enabled.

2 In the administrator mode, select [System Settings] - [Machine Setting], and enter the E-mail address of the administrator of this machine into [E-mail Address] (using up to 128 characters, excluding spaces).

➔ The E-mail address entered here is used as a sender address (From address) of E-mails to be sent from this machine.

Tips

- The sender E-mail address can be changed on the **Touch Panel** before sending the E-mail, if necessary.
- If user authentication is installed on this machine, the E-mail address of the login user is used as the sender's E-mail address.

Using an SSL/TLS communication

Encrypt communications between this machine and the E-mail server (SMTP) using SSL or TLS. This machine supports the SMTP over SSL and Start TLS.

Configure the setting if your environment requires SSL/TLS encryption communication with the E-mail server.

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings		Description
[Use SSL/TLS]		Select the method to encrypt communications with the E-mail server (SMTP). Select [SMTP over SSL] or [Start TLS] according to your environment. [OFF] is specified by default.
	[Port Number]	If you select [Start TLS] at [Use SSL/TLS], change the communication port number, if necessary. In normal circumstances, you can use the original port number. [25] is specified by default.
	[Port No.(SSL)]	If you select [SMTP over SSL] at [Use SSL/TLS], change the SSL communication port number, if necessary. In normal circumstances, you can use the original port number. [465] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

Using SMTP authentication

Configure the setting if your environment requires SMTP authentication to send an E-mail.

If the SMTP authentication is used, the user ID and password is sent from this machine when sending an E-mail to perform authentication.

To use the SMTP authentication, enable the SMTP authentication on this machine. In addition, enter information required for authentication.

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[SMTP Authentication]	Select this check box to use the SMTP authentication. In [SMTP Authentication Method], select whether to use SMTP authentication for each authentication method shown below. • Kerberos • NTLMv1 • Digest-MD5 • CRAM-MD5 • LOGIN • PLAIN [OFF] (not selected) is specified by default.
[User ID]	Enter the user ID for SMTP authentication (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [User ID] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name (realm) for SMTP authentication (using up to 253 characters). This item is necessary when the SMTP authentication method is Digest-MD5. • Enter the domain name if two or more domains (realm) exist. • When only one domain (realm) exists, no entry is required. The domain name is notified from the E-mail server (SMTP) at the initial communication, and communication is automatically performed using that domain name.
[Authentication Setting]	Select whether to synchronize the SMTP authentication with the user authentication of this machine. This item is necessary when the user authentication is installed on this machine. • [User Authentication]: Uses the user name and password of the registered user of this machine as [User ID] and [Password] for the SMTP authentication. • [Set Value]: Uses values entered at [User ID] and [Password]. If SMTP authentication fails because the user who sends an E-mail does not match the user specified in the [User ID], select [Set] in [Envelope-From Setting], then enter the E-mail address to be applied to Envelope-From in [From Address]. If you select [Do Not Set] in [Envelope-From Setting], the E-mail address of the administrator of this machine will be applied to Envelope-From. For details on the E-mail address of the administrator of this machine, refer to page 4-2. [Set Value] is specified by default.

Using POP Before SMTP authentication

Configure the setting if your environment requires the POP Before SMTP Authentication to send an E-mail.

The POP Before SMTP authentication is a function that performs POP authentication using the E-mail server (POP) before sending an E-mail and allows E-mail transmission only when the authentication is successful.

To use the POP Before SMTP authentication, enable the POP Before SMTP on this machine. In addition, configure settings for connecting to the E-mail server (POP) used for authentication.

1 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[POP before SMTP]	Select [ON] to use the POP Before SMTP. [OFF] is specified by default.
[POP before SMTP Time]	If necessary, change the waiting time until starting E-mail transmission after the POP authentication is successful. Depending on your environment, it may take time before the E-mail transmission is allowed after the POP authentication is successful. In that case, if a time period that is too short is specified, E-mail transmission may fail. [5] sec. is specified by default.

2 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX (POP)], and configure the following settings.

Settings	Description
[E-mail RX Setting]	Select [ON] to use the POP Before SMTP. [ON] is specified by default.
[POP Server Address]	Enter the address of your E-mail server (POP). Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name when receiving E-mails using the E-mail server (POP) (using up to 63 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 15 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (POP) as required. [30] sec. is specified by default.
[Port Number]	If necessary, change the port number of the E-mail server (POP). In normal circumstances, you can use the original port number. [110] is specified by default.

3 Set the POP over SSL and APOP settings according to your environment. In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX (POP)], and configure the following settings.

Settings		Description
[APOP Authentication]		If you use APOP in your E-mail server (POP), select [ON]. [OFF] is specified by default.
[Use SSL/TLS]		When using SSL to encrypt a communication with the E-mail server (POP), select this check box. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [995] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

Using S/MIME

The S/MIME is one of E-mail encryption methods. By using this function, you can add the E-mail encryption and digital signature functions to avoid the risk such as interception of E-mails or spoofing other sender.

To use the S/MIME, register a certificate on this machine. In addition, enable S/MIME on this machine.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

1 Register a certificate used for E-mail encryption to the destination of E-mail transmission.

➔ For details, refer to page 15-2.

2 Register the certificate of this machine to be added to E-mails as digital signature.

➔ For details, refer to page 13-2.

3 In the administrator mode, select [Network] - [E-mail Setting] - [S/MIME], then configure the following settings.

Settings	Description
[S/MIME Comm.Setting]	Select [ON] to use the S/MIME. To select [ON], the E-mail address of the certificate of this machine must match the E-mail address of the administrator. [OFF] is specified by default.
[Digital Signature]	To add digital signature when sending E-mails, select a method to add it. • [Always add signature]: Always adds the signature. The digital signature is automatically added without performing special setting before sending an E-mail. • [Select when sending]: The user must select whether to add digital signature before sending an E-mail. • [Do not add signature]: Does not add the signature. [Do not add signature] is specified by default.
[Digital Signature Type]	To add digital signature when sending E-mails, select a digital signature type. [SHA-1] is specified by default.
[E-Mail Text Encrypt. Method]	Select an E-mail encryption method. [3DES] is specified by default.

Tips

- When using the S/MIME function, the E-mail address of the administrator (E-mail address of the certificate of this machine) is used as the sender address.

7.2 Configuring the SMB transmission environment

Overview

The SMB Send is a function that transmits original data scanned on this machine to a shared folder in a specified computer. The shared folder is shared using the SMB (Server Message Block) protocol.

If the WINS server is installed to resolve the name, register it.

Enabling the direct hosting SMB service allows communications using the IP address (IPv4/IPv6) or host name. Enabling this service allows you to use the SMB Send function even in the IPv6 environment.

Using LLMNR (Link-local Multicast Name Resolution) enables you to resolve the name even in an environment with no DNS server. This function is supported by the computer loaded with Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2). It is useful to resolve the name in the IPv6 environment.

When using the SMB Send function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the SMB transmission

➔ For details on configuring the setting, refer to page 7-9.

3 Set the following options according to your environment

Purpose	Reference
Resolve the name using the WINS server	page 7-9
Specify a destination computer using the IP address and host name (FQDN)	page 7-10
Use the SMB Send function in the IPv6 environment	page 7-10
Specify a destination with a host name in an environment where the DNS server is not running (supported in the computer loaded with Windows Vista or later)	page 7-10
Use the SMB Send function in the DFS environment	page 7-10

Reference

If user authentication by Active Directory is installed, the Scan to Home function is available, which you can easily send data to a shared folder on the server or that on the login user's computer. For details, refer to page 12-11.

If the user authentication is installed, using the user authentication information (login name and password) as SMB destination authentication information (host name and password) avoids the problem of having to specify SMB destination authentication information, allowing construction of a single sign-on environment for SMB transmission. For details, refer to page 12-24.

Tips

- To use the SMB transmission function in IPv6 environment, you need to enable the direct hosting SMB service.
- In the IPv4 environment, the SMB transmission function can be used regardless of whether or not the direct hosting SMB service is enabled.
- If the direct hosting SMB service is enabled, the system operates as shown below (common to IPv4 and IPv6 environments).
  A destination computer can be specified using the IP address (IPv4 or IPv6).
  If a destination computer is specified using the host name or computer name (NetBIOS name), name resolution is performed in the order of DNS, LLMNR, and NetBIOS (port 137 of a destination computer).
  Connection is attempted to port 445 and port 139 of a destination computer in that order, and transmission is carried out.
- If the direct hosting SMB service is disabled, the system operates as shown below.
  A destination computer can be specified using the IP address (IPv4 only).
  If a destination computer is specified using the computer name (NetBIOS name) or host name, name resolution is performed in the order of NetBIOS (port 137 of a destination computer) and DNS.
  A connection with port 139 of a destination computer is established, and a transmission is carried out.

- To specify a destination computer using the host name, configure the appropriate machine settings and prepare the appropriate environment so that name resolution can be performed with DNS or LLMNR.
  To perform name resolution with DNS, a destination computer can be specified with "Host Name (example: host1)" or "FQDN (example: host1.test.local)".
  To perform name resolution with LLMNR, a destination computer can be specified only with "Host Name (example: host1)".

Configuring basic settings for the SMB transmission

Enable the SMB Send function. Also, specify the authentication method for SMB transmission, and select whether to enable the SMB signature.

In the administrator mode, select [Network] - [SMB Setting] - [Client Setting], then configure the following settings.

Settings	Description
[SMB TX Setting]	Select [ON] to use the SMB transmission function. [ON] is specified by default.
[SMB Authentication Setting]	Select an authentication method for SMB transmission according to your environment. • [NTLM v1]/[NTLM v2]/[NTLM v1/v2]: Select this to use the function in the NT domain environment. If you select [NTLM v1/v2], NTLMv1 authentication is performed when NTLMv2 authentication fails. • [Kerberos]: Select this to use the function in the Active Directory domain environment. • [Kerberos/NTLM v1/v2]: Select this to use the function in an environment both the Active Directory domain and NT domain exist in. NTLMv2 authentication is performed when Kerberos authentication fails, and NTLMv1 authentication is performed when NTLMv2 authentication fails. [NTLM v1] is specified by default.
[SMB security Signature Setting]	Select whether to enable the SMB signature of this machine to suit your environment. • [Disable]: Disables the SMB signature of this machine. • [When Requested]: Enables the SMB signature of this machine (client) only when the SMB signature is requested from the server side. If the SMB signature is not requested from the server side, operations are performed while the SMB signature of this machine (client) remains disabled, and a connection is possible even when the SMB signature in the server side is disabled. • [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the server side. If the SMB signature in the server side is disabled, it will not be possible to make a connection. [When Requested] is specified by default.

Tips

- In Mac OS X 10.7 or later, set [SMB Authentication Setting] to [NTLM v1/v2].
- In Mac OS X 10.7 or later, the direct hosting SMB service must be enabled (default: [ON]). For details, refer to page 7-10.

Using the WINS server

If the WINS server is installed to resolve the name, set the WINS server address and the name resolution method.

In the administrator mode, select [Network] - [SMB Setting] - [WINS/NetBIOS Settings], then configure the following settings.

Settings	Description
[WINS/NetBIOS]	Select [ON] to use the WINS server. [ON] is specified by default.
[Auto Obtain Setting]	Select [Enable] to automatically obtain the WINS server address. This item is necessary when DHCP is enabled. [Enable] is specified by default.

Settings	Description
[WINS Server Address1] to [WINS Server Address2]	Enter the WINS server address. This item is necessary when you do not automatically obtain the WINS server address using the DHCP. Use the following entry formats. • Example of entry: "192.168.1.1"
[Node Type Setting]	Select 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 [H Node] is specified by default.

Using the direct hosting SMB service

Enabling the direct hosting SMB service allows you to specify the destination using the IP address (IPv4/IPv6) or host name.

In the administrator mode, select [Network] - [SMB Setting] - [Direct Hosting Setting], and then set [Direct Hosting Setting] to [ON]. You can use this function with the default settings unless otherwise requested.

Resolving the name using LLMNR

Using LLMNR (Link-local Multicast Name Resolution) enables you to resolve the name even in an environment with no DNS server. This function is supported by the computer loaded with Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2). It is useful to resolve the name in the IPv6 environment.

To perform name resolution with LLMNR, enable the direct hosting SMB service. For details, refer to page 7-10.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], and set [LLMNR Setting] to [Enable]. You can use this function with the default settings unless otherwise requested.

Using in the DFS environment

Configure the setting when your environment requires a distributed file system (DFS, Distributed File System).

In the administrator mode, select [Network] - [SMB Setting] - [Client Setting], and set [DFS Setting] to [Enable]. You can use this function with the default settings unless otherwise requested.

7.3 Configuring the FTP transmission environment

Overview

The FTP transmission is a function that transmits original data scanned on this machine to a specified folder in the FTP server.

When the proxy server is used, you can configure settings so that the FTP server is accessed via the proxy server.

When using the FTP transmission, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the FTP transmission

➔ For details on configuring the setting, refer to page 7-11.

3 Set the following options according to your environment

Purpose	Reference
Send files to the FTP server via the proxy server	page 7-11

Configuring basic settings for the FTP transmission

Enable the FTP transmission. In addition, configure settings for connecting to the FTP server.

In the administrator mode, select [Network] - [FTP Setting] - [FTP TX Setting], then configure the following settings.

Settings	Description
[FTP TX]	Select [ON] to use the FTP transmission function. [ON] is specified by default.
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the FTP server. [60] sec. is specified by default.
[Port Number]	If necessary, change the FTP server port number. In normal circumstances, you can use the original port number. [21] is specified by default.

Using the proxy server

When the proxy server is used in your network environment, you can configure settings so that the FTP server is accessed via the proxy server.

To use the proxy server, register the proxy server information on this machine.

In the administrator mode, select [Network] - [FTP Setting] - [FTP TX Setting], then configure the following settings.

Settings	Description
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [21] is specified by default.

7.4 Configuring the WebDAV transmission environment

Overview

The WebDAV transmission is a function that transmits original data scanned on this machine to a specified folder in the WebDAV Server.

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.

When using the WebDAV transmission, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the WebDAV transmission

➔ For details on configuring the setting, refer to page 7-12.

3 Set the following options according to your environment

Purpose	Reference
Send files to the WebDAV server via the proxy server	page 7-12
Communicate with the WebDAV server using SSL	page 7-13

Configure basic settings for the WebDAV transmission

Enable the WebDAV transmission. In addition, configure the settings for connecting to the WebDAV server.

In the administrator mode, select [Network] - [WebDAV Settings] - [WebDAV Client Settings], then configure the following settings.

Settings	Description
[WebDAV TX Setting]	Select [ON] to use the WebDAV transmission function. [ON] is specified by default.
[Chunk Transmission]	Select whether to transmit data by dividing it into some chunks. Configure the setting if your WebDAV server supports chunk transmission. [OFF] is specified by default.
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the WebDAV server. [60] sec. is specified by default.
[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 **Touch Panel**. [UTF-8] is specified by default.

Using the proxy server

When the proxy server is used in your network environment, you can configure settings so that the WebDAV server is accessed via the proxy server.

To use the proxy server, register the proxy server information on this machine. In addition, configure the settings for connection to the proxy server.

In the administrator mode, select [Network] - [WebDAV Settings] - [WebDAV Client Settings], then configure the following settings.

Settings	Description
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"

Settings	Description
[Proxy Server Port Number]	If necessary, change the proxy server port number. [8080] is specified by default.
[User Name]	Enter the user name to log in to the proxy server (using up to 63 characters).
[Password]	Enter the password of the user name you entered into [User Name] (using up to 63 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

Using SSL communication

Communication between this machine and the WebDAV server is encrypted with SSL.

If a communication with the WebDAV server is encrypted using SSL in your environment, configure its setting.

Enable SSL for WebDAV destinations registered on this machine. In addition, specify how to verify the certificate.

1 In the administrator mode, select [Store Address] - [Address Book] - [WebDAV], and set [SSL Settings] to [ON] (Default: [OFF]).

➔ To directly enter a destination WebDAV server, configure SSL setting when entering the destination.

2 In the administrator mode, select [Network] - [WebDAV Settings] - [WebDAV Client Settings], then configure the certificate verification method.

Settings		Description
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

7.5 Configuring the WS scan environment

Overview

The WS scan transmission is a function that transmits original data scanned on this machine to the computer on the network on the computer loaded with Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2).

The computer uses the Web service function of Windows to automatically detect this machine connected to the network and smoothly install this function as a Web service scanner.

HTTP is used for communication between this machine and the computer. Use SSL to encrypt a communication between the this machine and the computer; you can send a file more securely.

When using the WS scan transmission, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the basic settings for the WS scan transmission

➔ For details on configuring the setting, refer to page 7-14.

3 Set the following options according to your environment

Purpose	Reference
WS scan using the discovery proxy	page 7-15
Communicate with the computer using SSL	page 7-15

Reference

For details on how to configure settings in the computer side, refer to "User's Guide[Scan Operations]/[Sending with Web Service (WS Scan)]".

Configure the basic settings for the WS scan transmission

Enable the scan using the Web service. In addition, configure settings used to detect this machine using the Web service, information for this machine as a scanner, and the method to connect to this machine.

1 In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Common Settings], then configure the following settings.

Settings	Description
[Friendly Name]	Enter the name of this machine to be displayed when being searched using the Web service from the computer (using up to 62 characters). Use a name that helps you easily identify this machine.
[Publication Service]	When using this machine in one of the following environments, select [Enable]. • Environment where NetBIOS is disabled on the computer loaded with Windows Vista or later • Environment constructed so that only communications using IPv6 are allowed. Up to 512 destinations can be detected in Publication Service (including detection counts by NetBIOS). [Enable] is specified by default.

2 In the administrator mode, select [Network] - [DPWS Settings] - [Scanner Settings], then configure the following settings.

Settings	Description
[Scan Function]	Select [ON] to use the WS scan transmission function. [OFF] is specified by default.
[Scanner Name]	Enter the name of this machine when using it as the WS scanner (using up to 63 characters).

Settings	Description
[Scanner Location]	Enter a scanner location if necessary (using up to 63 characters).
[Scanner Information]	Enter scanner information if necessary (using up to 63 characters).
[Connection Timeout]	Change the time-out time to limit a communication with the computer if necessary. [120] sec. is specified by default.

Using the proxy server

Configure settings for scanning through this machine in the environment where the multicast communication is restricted using the discovery proxy defined by WS-Discovery. Configure the setting if your environment requires the discovery proxy server.

In normal circumstances, to perform scan transmission through this machine using the Web service, the computer must be connected at a location where multicast communication is available for this machine. However, installing the discovery proxy server at a location where unicast communication is available for this machine enables it to perform scan transmission.

In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Extension Settings], then configure the following settings.

Settings		Description
[Enable Proxy]		Select [ON] to use the discovery proxy. [OFF] is specified by default.
[Proxy1] to [Proxy3]		Register the discovery proxy server used on this machine.
	[Proxy Server Address]	Enter the discovery proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
	[File Path]	Enter the service name at the path of the URL where the WS-Discovery service is published in the discovery proxy server (using up to 255 characters).
	[Enable SSL]	When using SSL to encrypt a communication with the discovery proxy server, select [ON]. [OFF] is specified by default.
	[Proxy Server Port Number]	If necessary, change the port number of the discovery proxy server. In normal circumstances, you can use the original port number. When [Enable SSL] is set to [OFF], [80] is specified by default. When [Enable SSL] is set to [ON], [443] is specified by default.

Using SSL communication

Communication between this machine and the computer is encrypted with SSL.

To encrypt SSL communication between this machine and the computer, you must set the bidirectional SSL communication between them. Before starting this procedure, confirm the following.

- Name resolution must have been performed in the DNS server.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the certificate of this machine in [Trusted Root Certification Authorities] of the computer.
- Create a certificate in the computer side in advance, and associate it with the TCP/IP communication port (default port number: 5358).

Tips

- In Windows 8/8.1/10, a communication using the Web service cannot be encrypted using SSL.

To make SSL communications, enable SSL. In addition, specify how to verify the certificate.

In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Common Settings], then configure the following settings.

Settings		Description
[SSL Setting]		Select [ON] to make SSL communications. This item is displayed when the device certificate is installed on this machine and SSL communication is enabled by selecting [Security] - [PKI Settings] - [SSL Setting] - [Mode using SSL/TLS] in Administrator mode. [OFF] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

7.6 Configuring the TWAIN scan environment

Overview

Using the TWAIN driver enables you to use this machine as a scanner by controlling it from a computer connected to the network.

When using the TWAIN scan, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the basic settings for the TWAIN scan

➔ For details on configuring the setting, refer to page 7-17.

3 If necessary, configure the following options.

Purpose	Reference
Change the time for locking the **Control Panel** while the TWAIN scan is running.	page 7-17

Configuring the basic settings for the TWAIN scan

On the computer on the network, configure settings necessary for controlling this machine.

1 In the administrator mode, select [Network] - [SNMP Setting], then configure the following settings.

Settings	Description
[SNMP]	To use the TWAIN scan function, select [ON] and select the check box of SNMP version you use. [ON] is specified by default.
[UDP Port Setting]	If necessary, change the UDP port number. In normal circumstances, you can use the original port number. [161] is specified by default.

2 In the administrator mode, select [Network] - [TCP Socket Setting], then configure the following settings.

Settings	Description
[TCP Socket]	Select this check box to use the TWAIN scan function. [ON] (selected) is specified by default.
[Port Number]	If necessary, change the TCP Socket port number. In normal circumstances, you can use the original port number. [59158] is specified by default.

Changing the Control Panel lock time

While the TWAIN scan is running, the **Control Panel** of this machine is automatically locked. If necessary, change the time period before the control panel is unlocked.

In the administrator mode, select [System Settings] - [Network TWAIN], and change the value of [TWAIN Lock Time] (Default: [120] sec.).

7.7 Searching for a destination using the LDAP server

Overview

When a directory server such as the LDAP server or Active Directory is used for user management, you can search for a destination (E-mail address or fax number) from the server.

Use SSL to encrypt a communication with the server; you can make communications more securely.

When using the LDAP server to search for a destination, follow the below procedure to configure the settings.

✔ To use the LDAP function of the Active Directory server, you must register the DNS server that synchronizes the Active Directory on this machine before starting the procedure. For details on how to register the DNS server, refer to page 5-3.

✔ To use the LDAP function of the Active Directory server, you must match the date and time of this machine and Active Directory. For details on how to set the date and time of this machine, refer to page 4-4.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the LDAP search

➔ For details on configuring the setting, refer to page 7-18.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the LDAP server using SSL	page 7-20

Configuring basic settings for the LDAP search

Configure settings so that you can search for a destination from the LDAP server. In addition, register your LDAP server, configure settings for connecting to the LDAP and search method.

1 In the administrator mode, select [Network] - [LDAP Setting] - [LDAP Setting], then configure the following settings.

Settings	Description
[Enabling LDAP]	Select [ON] to use the LDAP search. [OFF] is specified by default.
[Default Search Result Display Setting]	Select whether an E-mail address, fax number, or Internet fax number is given priority to be displayed as the destination search result when searching for destinations from the LDAP server. To use this function, install the optional **Fax Kit** in this machine or enable the Internet Fax function. [E-mail] is specified by default.

2 In the administrator mode, select [Network] - [LDAP Setting] - [Setting Up LDAP] - [Edit], then configure the following settings.

Settings	Description
[LDAP Server Name]	Enter the registered name of the LDAP server (using up to 32 characters). Use a name that helps you easily identify the server.
[Server Address]	Enter your LDAP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port Number]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.

Settings	Description
[Search Base]	Specify the starting point to search for a destination (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.
[Max.Search Results]	Change the maximum number of destinations to be displayed as search results, if necessary. [100] is specified by default.
[Authentication Method]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. • [anonymous]: [Login Name], [Password], and [Domain Name] can be omitted. • [GSS-SPNEGO]: Log in to the server using the Kerberos authentication method. Select this to use the Active Directory. [anonymous] is specified by default.
[Login Name]	Log in to the LDAP server, and enter the login name to search for a destination (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name to log in to the LDAP server (using up to 64 characters). If [GSS-SPNEGO] is selected for [Authentication Method], enter the domain name of Active Directory.
[Select Server Authentication Method]	Select the LDAP server authentication method. • [Set Value]: Use the settings of [Login Name], [Password], and [Domain Name]. • [User Authentication]: Synchronizes with the user authentication of this machine. Uses the user name and password of the registered user of this machine as [Login Name] and [Password]. • [Dynamic Authentication]: The system prompts you to enter the user name and password at LDAP searching. [Set Value] is specified by default.
[Use Referral]	Select whether to use the referral function, if necessary. Make an appropriate choice to fit the LDAP server environment. [ON] is specified by default.
[Search Condition Attributes]	Select attributes to be specified when performing the LDAP search. The setting can be switched between [Name] (cn) and [Nickname] (displayName). [Name] is specified by default.
[Search]	Select [ON] to display candidate destinations when entering a part of the name to search for a destination via the LDAP server. [OFF] is specified by default.
[Initial Setting for Search Details]	Specify LDAP search conditions.
[Search Attributes Authentication]	Select this check box to enable the attribute-based authentication when [Authentication Method] is set to [Simple] and [Select Server Authentication Method] to [Dynamic Authentication]. If this check box is selected, the user does not need to enter all of the DN (Distinguished Name) when performing authentication via the LDAP server. At [Search Attribute], enter the search attribute to be automatically added before the user name. In normal circumstances, specify "uid" before the user name, however, depending on your environment, you need to specify other attribute such as "cn". [uid] is specified by default.

Tips

- Clicking [Check Connection] at [LDAP Server List] enables you to confirm whether you can connect to the LDAP server according to the registered contents.

Using SSL communication

Communication between this machine and the LDAP server is encrypted with SSL.

Configure the setting if your environment requires SSL encryption communication with the LDAP server.

To make SSL communications, enable SSL. In addition, specify how to verify the certificate.

In the administrator mode, select [Network] - [LDAP Setting] - [Setting Up LDAP] - [Edit], then configure the following settings.

Settings		Description
[Enable SSL]		Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
	[Port Number(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

8 Configuring the Printing Environment

8 Configuring the Printing Environment

8.1 Configuring the LPR printing environment

Overview

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

When using the LPR printing function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Enable LPD

➔ For details on configuring the setting, refer to page 8-2.

Enabling LPD

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], and set [LPD] to [Enable] (Default: [Enable]).

8.2 Configuring the Port9100 printing environment

Overview

The Port9100 printing function directly specifies the RAW port (Port9100) of this machine as a printing destination printer and prints data via the network.

When using the Port9100 printing function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 If necessary, change the RAW port number.

➔ For details on how to change the setting, refer to page 8-3.

Changing the RAW port number

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], and change the Raw pot number (Default: [ON] (selected)) as required.

8.3 Configuring the SMB printing environment

Overview

The SMB printing function is a function used to print data by directly specifying this machine on the computer. This machine is shared using the SMB (Server Message Block) protocol.

If the WINS server is installed to resolve the name, register it.

Enabling the direct hosting SMB service allows communications using the IP address (IPv4/IPv6) or host name. Enabling the direct hosting SMB service allows you to use the SMB printing function even in the IPv6 environment.

Using LLMNR (Link-local Multicast Name Resolution) enables you to resolve the name even in an environment with no DNS server. This function is supported by the computer loaded with Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2). It is useful to resolve the name in the IPv6 environment.

When using the SMB printing function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the SMB printing

➔ For details on configuring the setting, refer to page 8-4.

3 Set the following options according to your environment

Purpose	Reference
Resolve the name using the WINS server	page 8-5
Use the SMB printing function in the IPv6 environment	page 8-5
Specify a destination with a host name in an environment where the DNS server is not running (supported in the computer loaded with Windows Vista or later)	page 8-6

Configure basic settings for the SMB printing

Enable the SMB printing. In addition, specify information to share this machine with SMB.

In the administrator mode, select [Network] - [SMB Setting] - [SMB Server Settings], then configure the following settings.

Settings	Description
[SMB Server Settings]	Select [ON] to use the SMB printing function. [OFF] is specified by default.
[SMB Host Name]	Enter the SMB host name of this machine to be displayed as a shared name in uppercase letters (using up to 15 characters, including a symbol mark "-" but not to be used at the beginning or end of the character string).
[Workgroup]	Enter a work group name or domain name in uppercase letters (using up to 15 characters, excluding ", \, ;, :, ,, *, <, >, |, +, =, and ?). [WORKGROUP] is specified by default.
[SMB Authentication Protocol]	Select the SMB authentication protocol to be used in the machine. In Windows Vista or later, select [SMB1.0/SMB2.0] to use the SMB2.0 protocol. [SMB1.0/SMB2.0] is specified by default.

Settings	Description
[SMB security Signature Setting]	Select whether to enable the SMB signature of this machine to suit your environment. • [Disable]: Disables the SMB signature of this machine. • [When Requested]: Enables the SMB signature of this machine (server) only when the SMB signature is requested from the client side. If the SMB signature is not requested from the client side, operations are performed while the SMB signature of this machine (server) remains disabled, and a connection is possible even when the SMB signature in the client side is disabled. • [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the client side. If the SMB signature in the client side is disabled, it will not be possible to make a connection. [When Requested] is specified by default.
[SMB Print]	Select [ON] to use the SMB printing function. [OFF] is specified by default.
[Print Service Name]	Enter a print service name in uppercase letters (up to 12 characters, excluding / and \).

Using the WINS server

If the WINS server is installed to resolve the name, set the WINS server address and the name resolution method.

In the administrator mode, select [Network] - [SMB Setting] - [WINS/NetBIOS Settings], then configure the following settings.

Settings	Description
[WINS/NetBIOS]	Select [ON] to use the WINS server. [ON] is specified by default.
[Auto Obtain Setting]	Select [Enable] to automatically obtain the WINS server address. This item is necessary when DHCP is enabled. [Enable] is specified by default.
[WINS Server Address1] to [WINS Server Address2]	Enter the WINS server address. This item is necessary when you do not automatically obtain the WINS server address using the DHCP. Use the following entry formats. • Example of entry: "192.168.1.1"
[Node Type Setting]	Select 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 [H Node] is specified by default.

Using the direct hosting SMB service

Enabling the direct hosting SMB service allows you to specify the destination using the IP address (IPv4/IPv6) or host name.

In the administrator mode, select [Network] - [SMB Setting] - [Direct Hosting Setting], and then set [Direct Hosting Setting] to [ON]. You can use this function with the default settings unless otherwise requested.

Resolving the name using LLMNR

Using LLMNR (Link-local Multicast Name Resolution) enables you to resolve the name even in an environment with no DNS server. This function is supported by the computer loaded with Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2). It is useful to resolve the name in the IPv6 environment.

To perform name resolution with LLMNR, enable the direct hosting SMB service. For details, refer to page 8-5.

In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting], and set [LLMNR Setting] to [Enable]. You can use this function with the default settings unless otherwise requested.

8.4 Configuring the IPP printing environment

Overview

IPP printing uses the Internet Printing Protocol (IPP) and prints information via the network.

IPP that is extended HTTP is used to forward printing data, enabling you to print data on a printer on a distance location via the Internet.

Using authentication when printing with IPP can prevent unauthorized use by a third party(s). In addition, using SSL to encrypt a communication between this machine and the computer enables more secure printing.

When using the IPP printing function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the IPP printing

➔ For details on configuring the setting, refer to page 8-7.

3 Set the following options according to your environment

Purpose	Reference
Perform authentication when performing IPP printing	page 8-8
Communicate with this machine using SSL (IPPS printing)	page 8-8

Configuring basic settings for the IPP printing

Enable the IPP printing. In addition, register the information of this machine used for IPP printing.

In the administrator mode, select [Network] - [IPP Setting], then configure the following settings.

Settings		Description
[IPP Setting]		Select [ON] to use the IPP printing function. [ON] is specified by default.
[Accept IPP job]		Select [ON] to use the IPP printing function. [ON] is specified by default.
[Printer Name]		If necessary, enter a printer name of this machine (using up to 127 characters).
[Printer Location]		If necessary, enter the location where to install this machine (using up to 127 characters).
[Printer Information]		If necessary, enter printer information of this machine (using up to 127 characters).
[Printer URI]		Displays the URI of the printers that can print data using the IPP.
[Support Operation]		If necessary, select the operations to enable in IPP.
	[Print Job]	Select this item to use the IPP printing. Specify whether to allow a print job. [ON] (selected) is specified by default.
	[Valid Job]	Select this item to allow confirmation of a valid job. [ON] (selected) is specified by default.
	[Cancel Job]	Select this item to allow the cancel of a job. [ON] (selected) is specified by default.
	[Open Job Attributes]	Select this item to allow obtaining job attributes. [ON] (selected) is specified by default.
	[Open Job]	Select this item to allow obtaining a job list. [ON] (selected) is specified by default.
	[Open Printer Attributes]	Select this item to allow obtaining printer attributes. [ON] (selected) is specified by default.

Using the IPP authentication

To perform authentication during IPP printing, enable the IPP authentication. In addition, enter information required for authentication.

In the administrator mode, select [Network] - [IPP Setting], then configure the following settings.

Settings	Description
[IPP Authentication Setting]	Select this item to use the IPP authentication. [ON] (selected) is specified by default.
[Authentication Method]	Select the IPP authentication method. [requesting-user-name] is specified by default.
[User Name]	Enter a user name (using up to 20 characters, excluding a colon (:)). This entry is required if you have selected [basic] or [digest] for [Authentication Method].
[Password]	Enter the password of the user name you entered into [User Name] (using up to 20 characters). This entry is required if you have selected [basic] or [digest] for [Authentication Method]. To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[realm]	If [digest] is selected for [Authentication Method], enter the domain (realm) (using up to 127 characters).

Communicating using SSL (IPPS)

You can enhance security by encrypting communication between the computer and this machine with SSL when using IPP printing on this machine.

1 Register a certificate for this machine and enable SSL communication.

➔ For details, refer to page 13-2.

2 In the administrator mode, select [Network] - [IPP Setting] - [IPP Setting], and set [IPP-SSL Setting] to [SSL Only] or [SSL/Non-SSL] (Default: [Non-SSL Only]).

If you use IPPS printing on Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2), confirm the following.

- When using the IPPS to print data on this machine, configure settings for this machine using the following procedure.

- "https://host name.domain name/ipp"
  For the host name and domain name, enter [DNS Host Name] and [DNS Default Domain Name] you specified for [TCP/IP Setting] of this machine.

- Confirm that the name resolution of this machine is possible using the DNS server from the computer. Register this machine in the DNS server in advance. In addition, configure DNS settings on the computer.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the certificate of this machine in [Trusted Root Certification Authorities] of the computer.

8.5 Configuring the WS printing environment

Overview

The computer uses the Web service function of Windows Vista or later (Windows Vista/7/8/8.1/10/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2) to automatically detect this machine connected to the network and easily install this function as Web service printer.

HTTP is used for communication between this machine and the computer. In addition, using SSL to encrypt a communication between the this machine and the computer enables more secure printing.

When using the WS printing function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the WS printing

➔ For details on configuring the setting, refer to page 8-9.

3 Set the following options according to your environment

Purpose	Reference
WS print using the discovery proxy	page 8-10
Communicate with the computer using SSL	page 8-10

Reference

For details on how to configure settings in the computer side, refer to "User's Guide[Print Operations]/[Printing in the Windows Environment]".

Tips

- If this machine joins the Active Directory domain, you can use the "WSD Secure Print function" that can securely perform Web service printing in Windows 8/8.1/10.

Configure basic settings for the WS printing

Enable printing using the Web service. Also, configure settings used to detect this machine using the Web service, and define information of this machine used as a printer.

1 In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Common Settings], then configure the following settings.

Settings	Description
[Friendly Name]	Enter the name of this machine to be displayed when being searched using the Web service from the computer (using up to 62 characters). Use a name that helps you easily identify this machine.
[Publication Service]	When using this machine in one of the following environments, select [Enable]. • Environment where NetBIOS is disabled on the computer loaded with Windows Vista or later • Environment constructed so that only communications using IPv6 are allowed. Up to 512 destinations can be detected in Publication Service (including detection counts by NetBIOS). [Enable] is specified by default.

2 In the administrator mode, select [Network] - [DPWS Settings] - [Printer Settings], then configure the following settings.

Settings	Description
[Print Function]	Select [ON] to use the WS printing function. [OFF] is specified by default.

Settings	Description
[WSD Print V2.0 Setting]	To use functions of WS printing version 2.0, select [Enable]. When you connect this machine from the computer compatible with version 2.0, you can issue a printing prenotification to this machine, send account information, specify parameters for the advanced device functions, or obtain the device capability and localization information. [Enable] is specified by default.
[Printer Name]	Enter the name of this machine when using it as the WS printer (using up to 63 characters).
[Printer Location]	Enter a printer location if necessary (using up to 63 characters).
[Printer Information]	Enter printer information if necessary (using up to 63 characters).

Using the proxy server

Configure settings for printing through this machine in the environment where the multicast communication is restricted using the discovery proxy defined by WS-Discovery. Configure the setting if your environment requires the discovery proxy server.

In normal circumstances, to print data through this machine using the Web service, the computer must be connected at a location where multicast communication is available for this machine. However, installing the discovery proxy server at a location where unicast communication is available for this machine enables printing through this machine.

In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Extension Settings], then configure the following settings.

Settings		Description
[Enable Proxy]		Select [ON] to use the discovery proxy. [OFF] is specified by default.
[Proxy1] to [Proxy3]		Register the discovery proxy server used on this machine.
	[Proxy Server Address]	Enter the discovery proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
	[File Path]	Enter the service name at the path of the URL where the WS-Discovery service is published in the discovery proxy server (using up to 255 characters).
	[Enable SSL]	When using SSL to encrypt a communication with the discovery proxy server, select [ON]. [OFF] is specified by default.
	[Proxy Server Port Number]	If necessary, change the port number of the discovery proxy server. In normal circumstances, you can use the original port number. When [Enable SSL] is set to [OFF], [80] is specified by default. When [Enable SSL] is set to [ON], [443] is specified by default.

Using SSL communication

Communication between this machine and the computer is encrypted with SSL.

To encrypt SSL communication between this machine and the computer, you must set the bidirectional SSL communication between them. Before starting this procedure, confirm the following.

- Name resolution must have been performed in the DNS server.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the certificate of this machine in [Trusted Root Certification Authorities] of the computer.
- Create a certificate in the computer side in advance, and associate it with the TCP/IP communication port (default port number: 5358).

Tips

- In Windows 8/8.1/10, a communication using the Web service cannot be encrypted using SSL.

Enable the SSL communication. In addition, specify how to verify the certificate.

In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Common Settings], then configure the following settings.

Settings		Description
[SSL Setting]		Select [ON] to make SSL communications. [OFF] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

8.6 Configuring the Bonjour printing environment

This machine supports Bonjour used on Mac OS.

Bonjour technology runs based on TCP/IP, enabling you to automatically configure the network settings for networked devices and find available services.

Enabling the Bonjour function on this machine enables the computer to automatically detect this networked machine and display it as an addable printer in the list.

In the administrator mode, select [Network] - [Bonjour Setting], then configure the following settings.

Settings	Description
[Bonjour]	Select [ON] to use Bonjour. [OFF] is specified by default.
[Bonjour Name]	Enter a Bonjour name that is to be displayed as the name of connected device (using up to 63 characters).

8.7 Configuring the AppleTalk printing environment

This machine supports AppleTalk used on Mac OS. AppleTalk connection is supported in Mac OS 9.2/OS X 10.2/10.3/10.4/10.5.

AppleTalk is the generic name of a group of network protocols that enables automatically configure file sharing settings and printing settings for networked devices.

Enabling the AppleTalk function on this machine enables the computer to automatically detect this networked machine and display it as an addable printer in the list.

In the administrator mode, select [Network] - [AppleTalk Setting], then configure the following settings.

Settings	Description
[AppleTalk]	Select [ON] to use the AppleTalk. [OFF] is specified by default.
[Printer Name]	Enter a printer name to be displayed on the selector (using up to 31 characters, excluding = and ~).
[Zone Name]	If necessary, enter the zone name of this machine (using up to 31 characters).
[Current Zone]	The current zone name is displayed.

8.8 Configuring a setting to make prints from an Android terminal using Mopria

Mopria is a standard that enables printing from an Android terminal by wireless connection without having to install a dedicated application such as a printer driver to suit the manufacturer or model of an Android terminal.

You can automatically detect an MFP or printer compatible with Mopria on the same network from an Android terminal to make prints, thereby, reducing the user's or administrator's load.

To use the Mopria print function, the following preparation is required.

- Installing Mopria Print Service in the Android terminal (Android 4.4 or later)
- In the administrator mode, select [Network] - [Mopria Setting] - [Mopria Setting], then set [Mobile Device Request Response Setting] to [ON] (Default: [OFF]).

Tips

If [Mopria Setting] - [Mobile Device Request Response Setting] is changed to [ON], the following settings are also enabled synchronously. If one of the following settings is changed to Disable, [Mobile Device Request Response Setting] is also changed to [OFF] synchronously.

- [Network] - [IPP Setting] - [IPP Setting] - [IPP Setting] in administrator mode
- [Network] - [IPP Setting] - [IPP Setting] - [Accept IPP job] in administrator mode
- [Network] - [Bonjour Setting] - [Bonjour Setting] - [Bonjour] in administrator mode

8.9 Configuring the NetWare printing environment

Overview

This machine supports IPX, which is a communication protocol used in NetWare, enabling printing in IPX-based environment.

Setting items differ depending on the NetWare print mode. Configure the appropriate settings to suit your environment.

Purpose	Reference
In Remote Printer mode using the NetWare 4.x Bindery Emulation	page 8-15
In Print Server mode using the NetWare 4.x Bindery Emulation	page 8-15
In the NetWare 4.x Remote Printer mode (NDS)	page 8-16
In the NetWare 4.x/5.x/6 Print Server mode (NDS)	page 8-17
For NetWare 5.x/6 Novell Distributed Print Service (NDPS)	page 8-17

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 Option] 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.

7 Log in to the administrator mode of **Web Connection**.

8 In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings		Description
[IPX Setting]		Select [ON] to use the IPX. [OFF] is specified by default.
[Ethernet Frame Type]		Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.
[NetWare Print Mode]		Select [Nprinter/Rprinter]. [OFF] is specified by default.
	[Print Server Name]	Enter a print server name to enable Nprinter/Rprinter (using up to 63 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .). Enter the print server name registered in the Pconsole.
	[Printer Number]	Enter the Nprinter/Rprinter number. [255] is specified by default.

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 Option] 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 Log in to the administrator mode of **Web Connection**.

7 In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings		Description
[IPX Setting]		Select [ON] to use the IPX. [OFF] is specified by default.
[Ethernet Frame Type]		Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.
[NetWare Print Mode]		Select [PServer]. [OFF] is specified by default.
	[Print Server Name]	Enter a print server name to enable Pserver (using up to 63 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .). Enter the print server name registered in the Pconsole.
	[Print Server Password]	If necessary, enter a print server password (using up to 63 characters).
	[Polling Interval]	Set a job inquiry interval. [1] sec. is specified by default.
	[Bindery/NDS Setting]	Select [NDS/Bindery Setting]. [NDS] is specified by default.
	[File Server Name]	Enter the priority file server name to be used in the Bindery emulation mode (using up to 47 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .).

In the 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.

6 Log in to the administrator mode of **Web Connection**.

7 In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings	Description
[IPX Setting]	Select [ON] to use the IPX. [OFF] is specified by default.
[Ethernet Frame Type]	Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.

Settings		Description
[NetWare Print Mode]		Select [Nprinter/Rprinter]. [OFF] is specified by default.
	[Print Server Name]	Enter a print server name to enable Nprinter/Rprinter (using up to 63 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .). Enter the print server name registered in the NWadmin.
	[Printer Number]	Enter the Nprinter/Rprinter number. [255] is specified by default.

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].

5 Log in to the administrator mode of **Web Connection**.

6 In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings		Description
[IPX Setting]		Select [ON] to use the IPX. [OFF] is specified by default.
[Ethernet Frame Type]		Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.
[NetWare Print Mode]		Select [PServer]. [OFF] is specified by default.
	[Print Server Name]	Enter a print server name to enable Pserver (using up to 63 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .). Enter the print server name registered in the NWadmin.
	[Print Server Password]	If necessary, enter a print server password (using up to 63 characters).
	[Polling Interval]	Set a job inquiry interval. [1] sec. is specified by default.
	[Bindery/NDS Setting]	Select [NDS]. [NDS] is specified by default.
	[NDS Context Name]	Enter an NDS context name for print server connection (using up to 191 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .).
	[NDS Tree Name]	Enter an NDS tree name for print server connection (using up to 63 characters, excluding /, \, :, ;, ,, *, [,], <, >, |, +, =, ?, and .).

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.

✔ Check that TCP/IP protocol is configured in the NetWare server.

✔ Check that this machine starts and an IP address is assigned.

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] screen, set the Printer to [(None)] and the port hander to [Novell Port Handler], and register the settings.

9 Set [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, then press [Finish].

Display the registration window of the printer driver.

11 On the registration window for the printer driver, select [(None)] for both OS and finish registration.

8.10 Configuring the E-mail RX Print environment

Overview

E-mail RX Print is a function that prints a file attached to the E-mail received by the machine.

If you send an E-mail to the E-mail address of the machine, you can print a PDF, Compact PDF, JPEG, TIFF, XPS, Compact XPS, OOXML (.docx/.xlsx/.pptx), or PPML (.ppml/.vdx/.zip) file on the computer using the machine without using the printer driver.

When using the E-mail RX Print function, follow the below procedure to configure the settings.

✔ To use this function, the optional **Extension Memory** and **i-Option LK-110 v2** are required.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the E-mail address of this machine

➔ In the administrator mode, select [System Settings] - [Machine Setting] - [Input Machine Address], then configure the E-mail address in [E-mail Address]. For details on configuring the setting, refer to page 4-2.

3 Configure settings to receive E-mails on this machine

➔ For details on configuring the setting, refer to page 8-19.

4 Configure settings to print a received E-mail attachment

➔ For details on configuring the setting, refer to page 8-20.

Configure settings to receive E-mails on this machine

Configure settings for connecting to the E-mail server (POP).

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX (POP)], and configure the following settings.

Settings	Description
[E-mail RX Setting]	Select [ON] to use the E-mail RX Print function. [ON] is specified by default.
[POP Server Address]	Enter the address of your E-mail server (POP). Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name when receiving E-mails using the E-mail server (POP) (using up to 63 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 15 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (POP) as required. [30] sec. is specified by default.
[Port Number]	If necessary, change the port number of the E-mail server (POP). In normal circumstances, you can use the original port number. [110] is specified by default.
[Check for New Messages]	Select this check box to check for incoming E-mails by periodically connecting to the E-mail server (POP) on this machine. Also, enter an interval for connecting the E-mail server (POP) at [Polling Interval]. [ON] (selected) is specified by default.

Configure settings to print a received E-mail attachment

Enable the E-mail RX Print function. If necessary, configure settings to restrict E-mail addresses for which printing is to be permitted, or to save E-mail attachments to a User Box.

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX Print], then configure the following settings.

Settings	Description
[E-mail RX Print]	Select [ON] to use the E-mail RX Print function. [OFF] is specified by default.
[E-mail RX Permission]	Select [ON] to restrict E-mail addresses that are available for the E-mail RX Print function. If you select [ON], in [Permit Address 1] to [Permit Address 10], enter the E-mail addresses for which you want to permit the E-mail RX Print function, or enter the E-mail domain.
[Save in User Box]	Select [ON] to save all the E-mail attachments received on this machine to a User Box. If you select [ON], in [User Box No.], enter the number of the User Box where an E-mail attachment is saved. If the number of the User Box to save the E-mail attachment in is not specified by E-mail, the file is saved in the User Box for which you have entered a number. When you receive an encrypted PDF file as an E-mail attachment, the file is saved in the Password Encrypted PDF User Box. [OFF] is specified by default.

Reference

For details on how to specify the User Box number by E-mail, refer to "User's Guide[Print Operations]/[Printing without Using the Printer Driver]".

8.11 Specifying the default print settings for this machine

8.11.1 Specifying the default print settings

This machine operates according to these settings unless the printer driver specifies the print settings. You can configure default settings for tray, finisher processing, and the number of copies.

In the administrator mode, select [Print Setting] - [Basic Setting], then configure the following settings.

Settings	Description
[PDL Setting]	Select the Page Description Language. When you select [Auto], this machine automatically switches between PCL and PS. [Auto] is specified by default.
[Color Setting]	Select the optimum original type mode for the original. • [Document]: The image quality setting suitable for originals containing multiple elements, such as text, graphs, figures, and photos, is applied. • [Photo]: The setting that prioritizes the image quality is applied. • [DTP]: The image quality setting suitable for originals containing both text and figures is applied. What you see on the display is exactly reproduced. • [Web]: The image quality setting suitable for printing Web pages is applied. Low-resolution images are reproduced with enhanced smoothness. • [CAD]: The image quality setting suitable for originals composed of thin lines is applied. Images are reproduced in high resolutions. [Document] is specified by default.
[Paper Tray]	Select the paper tray for the printing paper. [Auto] is specified by default.
[Output Tray]	Select the primary output tray. [Tray 2] is specified by default.
[2-Sided Print]	Select whether to print an original on both sides of paper when data containing multiple pages is printed. [OFF] is specified by default.
[Bind Direction]	Select the binding position for 2-sided printing. [Left Bind] is specified by default.
[Staple]	Select whether to staple printed sheets. To staple printed sheets, select the number of staples. [OFF] is specified by default.
[Punch]	Select whether to punch printed sheets. To punch printed sheets, select the required number of punched holes. [OFF] is specified by default.
[Fold]	Select whether to fold the printed sheets. When you want to fold the printed sheets, select the folding mode. [OFF] is specified by default.
[Half-Fold/Tri-Fold Operation Selection]	Select the unit by which the paper is folded from [By Copy Job(Multiple Sheets)], [Sheet], and [By Page]. When you select [By Page], enter the number of pages to be folded at one time at [Specified Page]. [By Copy Job(Multiple Sheets)] is specified by default.
[Number of Sets]	Enter the number of copies to be printed. [1] is specified by default.
[Default Paper Size]	Select the size of paper for printing. [8 1/2" × 11"] ([A4]) is specified by default.
[Paper Type]	Select the type of paper you want to print on. [No Selection] is specified by default.
[Original Direction]	Select the orientation of the image to be printed. [Portrait] is specified by default.
[Spool Print Jobs in HDD before RIP]	Select whether to save the next print job on the hard disk if the job is received while another print job is being executed. [ON] is specified by default.
[Banner Sheet Setting]	Select whether to print a banner page (front cover) that contains the sender or title of print data. [OFF] is specified by default.

Settings	Description
[Banner Sheet Paper Tray]	Select a paper tray to print a banner page (front cover). [Auto] is specified by default.
[No Matching Paper in Tray Setting]	Select the operation to be taken when there is no appropriate sized paper in the specified paper tray. • [Switch Trays(Tray Priority)]: Switches to the paper tray where paper of the same size is loaded. • [Stop Printing(Tray Fixed)]: Stops printing. Load paper to the specified paper tray or switch to another paper tray manually. [Stop Printing(Tray Fixed)] is specified by default.
[A4/A3<->LTR/LGR Auto Switch]	Select whether to use paper of a size close to the size specified in [Default Paper Size] if the specified paper is not loaded in the paper tray. In normal circumstances, select [OFF]. When you select [ON], size conversion between A4 and Letter and between A3 and Ledger automatically occurs and images may be partially lost. [OFF] is specified by default.
[Binding Direction Adjustment]	Select how the binding position is adjusted on two-sided printed sheets. • [Finishing Priority]: After all pages are received, the binding position is adjusted and printing is started. • [Productivity Priority]: Each time a page is received, the binding position is adjusted and printing is started. • [Control Adjustments]: The printing position is not adjusted. The pages are printed according to the settings specified in the printer driver. [Finishing Priority] is specified by default.
[Line Width Adjustment]	Select how the width of text or lines is adjusted. • [Thin]: Select this option to draw letters and lines thinly. Details of letters and figures can be printed elaborately. • [Slightly Thin]: Select this option to draw letters and lines with a thickness between [Thin] and [Std.]. • [Std.]: Select this option to draw letters and lines with a normal thickness. • [Slightly Thick]: Select this option to draw letters and lines with a thickness between [Std.] and [Thick]. • [Thick]: Select this option to draw letters and lines thickly. Letters and figures are printed clearly. [Std.] is specified by default.
[Gray Background Text Correction]	Select whether to prevent text or lines on a gray background from looking thicker than they actually are. [ON]: Select this option to make the text and lines against a gray back-ground look as thought they have the same width as text and lines against a non-gray background. [ON] is specified by default.
[Minimal Print]	Select whether to slightly reduce the entire page when directly printing a PDF, PPML, or OOXML (docx, xlsx, or pptx) file. [OFF] is specified by default.
[OOXML Print Mode]	Select whether to give priority to either the image quality or speed when directly printing an OOXML (docx, xlsx, or pptx) file. [Prioritize Speed] is specified by default.
[Glossy Mode]	Images are printed with a glossy finish. The printing speed is reduced. [OFF] is specified by default.
[Toner Save]	Select this check box to reduce the printing density in order to save the amount of toner consumed. [OFF] is specified by default.
[Edge Definition]	Select this option to sharpen the edges of images such as text in the table and graphics to improve legibility when clearing small or faint text. [OFF] is specified by default.
[Operation when 1200 dpi file is received]	Select an operation when receiving print data at 1200 dpi. [Convert to 600dpi] is specified by default.

8.11.2 Specifying the default PCL print settings

Configure the PCL settings. Specify the default values for PCL symbol set.

In the administrator mode, select [Print Setting] - [PCL Setting], then configure the following settings.

Settings	Description
[Select Color]	Select colors for printing. • [Auto Color]: The color mode is automatically selected according to the original color. • [Gray Scale]: The original is printed in black and white regardless of whether the original is color or black and white. • [2 Color]: The original is printed in the two specified colors. The gray and color areas of a color original are printed using combinations of the colors specified in [2-Color]. [Auto Color] is specified by default.
[Symbol Set]	Select the font symbol set to be used. The default values vary depending on the area you are in.
[Typeface]	Select Resident Font or Download Font to specify the font to be used. • [Resident Font]: Select a font from those installed on this machine. • [Download Font]: Select a font from those downloaded to this machine. This item is displayed when a download font exists. [Courier] is specified by default.
[Font Size]	Specify the default font size value. • [Scalable Font]: Enter the font size (in points) for scalable fonts (with different widths for each character). [12.00 Point] is specified by default. • [Bitmap Font]: Enter the font width (in pitches) for bitmap fonts (with the same width for each character). [10.00 Pitch] is specified by default.
[Line/Page]	Enter the number of lines of text data to be printed on one page. The default values vary depending on the area you are in.
[CR/LF Mapping]	Select whether to replace the line feed codes when printing text data. When you want to replace the line feed codes, select the replacement method. [OFF] is specified by default.
[Bar Code Font Settings]	Configure settings for the bar code font. • [Bar Code Line Width]: Specify the line width of the bar code font. [0] is specified by default. • [Bar Code Space Width]: Specify the space width of the bar code font. [0] is specified by default. To use this function, the optional **Extension Memory** and **i-Option LK-106** are required.
[Thin Line]	Select this option to prevent thin lines from disappearing in reduced-size printing. This is effective for thin lines such as table borders created in Excel, but not for thin lines used in illustrations. [ON] is specified by default.

8.11.3 Specifying the default PS print settings

Configure the PS print settings. Specify default settings for error information printing and the default settings of various profiles.

In the administrator mode, select [Print Setting] - [PS Setting], then configure the following settings.

Settings	Description
[Select Color]	Select colors for printing. • [Auto Color]: The color mode is automatically selected according to the original color. • [Full Color]: The original is printed in full color regardless of whether the original is in color or in black and white. • [Gray Scale]: The original is printed in black and white regardless of whether the original is in color or in black and white. [Auto Color] is specified by default.

Settings		Description
[PS Error Print]		Specify whether to print error information when an error occurs during PS rasterization. [OFF] is specified by default.
[ICC Profile Settings]		Specify the default profile setting to be displayed in the printer driver. If the details of [ICC Profile Settings] differ between the machine and the printer driver, the settings of the printer driver are given priority.
	[Photo]	Select the default setting for RGB color and output profile for photographs. [RGB Color]: [sRGB]/[Output Profile]: [Auto] are specified by default.
	[Text]	Select the default setting for RGB color and output profile for text. [RGB Color]: [sRGB]/[Output Profile]: [Auto] are specified by default.
	[Figure/Table/Graph]	Select the default setting for RGB color and output profile for figures, tables, and graphs. [RGB Color]: [sRGB]/[Output Profile]: [Auto] are specified by default.
	[Simulation Profile]	Select the default setting for simulation profile. If [Simulation Profile] is set to [Auto] while [PS Designer Settings] is set to [No], use a simulation profile based on your processing. For details on [PS Designer Settings], refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]". [Auto] is specified by default.
[Auto Trapping]		Select whether to superimpose neighboring colors to print so as to prevent white space being generated around a picture. Selecting [ON] prevents the generation of white lines at the boundaries of colors in graphs or figures. [OFF] is specified by default.
[Black Overprint]		Select whether to print so as to prevent white space being generated around a black character or figure. • [Text/Figure]: Adjacent portion between a text and figure is overprinted with black. Use this setting when a white line appears around the black portion in a graph or figure. • [Text]: Black is overprinted on the adjacent colors in the text portion. Use this setting when a white line appears around the text. • [OFF]: The data is printed as is without overprinting with black. [OFF] is specified by default.

8.11.4 Specifying the default TIFF print settings

Specify how to determine the size of print paper when directly printing TIFF, JPEG, or PDF image data.

This setting is enabled when data is printed from a USB memory device or directly printed using the Direct Print function of **Web Connection**.

In the administrator mode, select [Print Setting] - [TIFF Setting], then configure the following settings.

Settings	Description
[Auto Paper Select]	Select how the paper size used for printing is determined. • [Auto]: TIFF/JPEG(JFIF)/PDF images are printed on paper of the same size as the image. However, a JPEG (EXIF) image is enlarged or reduced for printing to fit the paper size specified in [Print Setting] - [Basic Setting] - [Default Paper Size] in the administrator mode. • [Priority Paper Size]: Images are enlarged or reduced to the paper size specified before they are printed. When they are printed from **Web Connection** or a USB memory device, the paper size specified in [Print Setting] - [Basic Setting] - [Default Paper Size] in the administrator mode is used. [Auto] is specified by default.

8.11.5 Configuring security settings for XPS or OOXML printing

Specify whether to perform the verification of a digital signature or printing of error information when directly printing an XPS or OOXML (docx, xlsx, or pptx) file.

In the administrator mode, select [Print Setting] - [Security Setting], and configure the following settings.

Settings	Description
[Verify XPS/OOXML Digital Signature]	Select whether to verify a digital signature when printing an XPS or OOXML (docx, xlsx, or pptx) file with a digital signature added. When [ON] is selected, the data is not printed if the signature is invalid. [OFF] is specified by default.
[Print XPS/OOXML Errors]	Select whether to print error information when an error occurs while printing an XPS or OOXML (docx, xlsx, or pptx) file. [ON] is specified by default.

8.11.6 Configuring the default OOXML print settings

Specify the default value for OOXML print settings during direct printing. An OOXML file is compatible with the file type (*.docx, *.xlsx, or *.pptx) of Microsoft Office 2007 or later.

In the administrator mode, select [Print Setting] - [OOXML Print Settings], and configure the following settings.

Settings	Description
[Sheet/Book Print]	Select whether to print the currently selected sheet or the entire book when handling an Excel file. The [Current Sheet] is specified by default.
[Default Paper Size]	Select a paper size to print an OOXML (docx, xlsx, or pptx) file. [Auto] is specified by default.
[Paper Type]	Select a paper type to print an OOXML (docx, xlsx, or pptx) file. [Auto] is specified by default.

8.11.7 Configuring the default combination settings

Specify the default value for combination settings during direct printing.

In the administrator mode, select [Print Setting] - [Page Layout Settings], and configure the following settings.

Settings	Description
[Combination]	Select [ON] to reduce multiple pages onto one sheet for printing. [OFF] is specified by default.
[Number of Page Combinations]	Enter the number of pages to be combined onto one sheet for [Column] and [Row]. [1] is specified by default for [Column] and [Row].
[Combination Direction]	Select a method to arrange pages. [Sideways from Upper-Left] is specified by default.
[Page Spacing]	Enter the page space in the row and column directions. [0] inch or mm is specified by default.
[Margin]	Enter page margins at the top, bottom, right, and left sides. [0] inch or mm is specified by default.
[Page Zoom]	Select whether to automatically adjust the zoom ratio or specify any zoom ratio to enlarge or reduce a page. [Auto] is specified by default.
[Page Frame]	Select to print a border line between pages. [Do Not Print] is specified by default.

8.12 Specifying the time-out time by interface

Change the time-out time to limit a communication between this machine and the computer if necessary. You can change the time-out time to limit communications via a network and USB respectively.

In the administrator mode, select [Print Setting] - [Interface Setting], then configure the following settings.

Settings	Description
[Network Timeout]	When this machine is connected via a network to the computer, change the communication time-out time if necessary. [60] sec. is specified by default.
[USB Timeout]	When this machine is connected via a USB device to the computer, change the communication time-out time if necessary. [60] sec. is specified by default.

8.13 Restricting users from obtaining device information using password

You can use a password to restrict the obtainment of device information from the printer driver.

When you attempt to obtain device information from the printer driver, this machine prompts you to enter the password. This enables you to restrict users who can obtain device information.

In the administrator mode, select [Print Setting] - [Assign Account to Acquire Device Info], then configure the following settings.

Settings	Description
[Assign Account to Acquire Device Info]	Specify [ON] to restrict users from obtaining device information from the printer driver using a password. [OFF] is specified by default.
[Password]	Enter a password to restrict device information to be obtained (using up to eight characters, excluding spaces and "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password. Inform users who obtain device information from the printer driver of the password you have entered in this field.

9 Configuring the Fax Environment

9 Configuring the Fax Environment

9.1 Configuring basic fax settings

9.1.1 Configuring the Line Usage Settings

Configure the settings such as the telephone line type (dialing method) and fax receiving mode.

In the administrator mode, select [Fax Settings] - [Line Parameter Setting], then configure the following settings.

Settings	Description
[Dialing Method]	Select the line type according to your environment.
[Receive Mode]	Select a receive mode. • [Auto RX]: Automatically start receiving a fax if the call is a fax call. • [Manual RX]: Manually request the reception of a fax. Select this mode if a phone is connected to this machine and you expect frequent voice calls. [Auto RX] is specified by default.
[Number of RX Call Rings]	If necessary, change the number of times the phone rings before automatically receiving a fax. [2] is specified by default.
[Number of Redials]	If the machine fails to send a fax successfully, it automatically redials the same destination after a certain period of time has elapsed. If necessary, change the number of redials. (The setting range varies according to the local standards.)
[Redial Interval]	If necessary, change the redial intervals when you specified a value in [Number of Redials]. [3 min.] is specified by default.
[Manual RX V34 Setting]	Select whether to cancel the V.34 function when manually receiving a fax. To cancel the V.34 function, select [ON]. [OFF] is specified by default.
[Line Monitor Sound]	Select whether to play sounds on the telephone line from speakers during fax communication. [OFF] is specified by default.
[Line Monitor Sound Volume (Send)]	Monitors sounds output from the machine. Specify the monitor sound volume between 0 and 8. This function is available only when [Line Monitor Sound] is set to [ON]. [3] is specified by default.
[Line Monitor Sound Volume (Receive)]	Monitors sounds output from the recipient, including switching equipment or TA. Specify the monitor sound volume between 0 and 8. This function is available only when [Line Monitor Sound] is set to [ON]. [4] is specified by default.

9.1.2 Configuring connection settings for a PBX environment

You can connect this machine to a Private Branch Exchange (PBX) environment. Using PBX enables you to connect multiple telephones and faxes of the organization to the public telephone network.

In the administrator mode, select [Fax Settings] - [PBX Connection Setting], then configure the following settings.

Settings	Description
[PBX Connection Setting]	Select this item to use this machine in a PBX environment. [OFF] (not selected) is specified by default.
[Outside Line]	Enter an outside line number (using up to four digits). The outside line number specified here is added to fax numbers registered with the address book or program.

9.1.3 Registering the sender information

Register the machine name, your company name (sender name), and the fax number that are to be printed as the sender information when faxes are transmitted.

The sender information is automatically added to a fax to be sent from this machine. Up to 20 sender names can be registered. You can use different names for different purposes depending on the destination.

In the administrator mode, select [Fax Settings] - [Header Information], then configure the following settings.

Settings		Description
[Sender Fax No.]		Enter the fax number of this machine (using up to 20 digits, including symbols #, *, +, and spaces). The fax number you entered is printed as the sender information.
[Default]		Select the default setting for the sender name. The sender name, which is specified by default, is automatically added when a fax is sent.
[Sender Name]		Displays registered sender names.
[Edit]		You can register up to 20 sender names. Use this option to use different sender names depending on the destination.
	[No.]	Displays the registration number.
	[Sender Name]	Enter a sender name (using up to 30 characters).
[Delete]		Click this button to delete the registered sender name.

9.2 Specifying operations when sending and receiving a fax

9.2.1 Specifying How to Print the Sender Name/Reception Information

Specify how to print sender information and reception information of a fax to be sent and received.

In the administrator mode, select [Fax Settings] - [Header/Footer Position], then configure the following settings.

Settings	Description
[Header Position]	Select the position at which a sender information is printed on a fax. If you select [OFF], sender information is not printed. If [Inside Body Text] is selected, part of the original may be lost. [Outside Body Text] is specified by default. [OFF] is not available in the USA and Hong Kong models.
[TTI Print Position and Character Size]	Select the size of characters to print a sender information. [Minimal] is the character height that is half that of the characters in [Normal] size. It is recommended that you select [Minimal] to prevent a fax image from being cut off or to prevent a page from being divided when pages are printed at a receiving machine. If [Normal] is selected for the scanning resolution for sending a fax, it is converted into [Normal] to prevent characters from becoming corrupted and unreadable. [Minimal] is specified by default.
[Print Receiver's Name]	Select whether to print a destination fax number as the sender information. If [OFF] is selected, the fax number of this machine is printed instead of the fax number of the destination. [ON] is specified by default. This item is not displayed in the USA and Hong Kong models.
[Footer Position]	Select whether to print the reception information (date, time, and reception number) on faxes received by this machine. To print them, select the position to print the reception information. If you select [OFF], the reception information is not printed. [OFF] is specified by default.

9.2.2 Changing Print Settings When Receiving a Fax

Change print settings for faxes received on this machine In addition, specify how to handle files in a polling transmission.

In the administrator mode, select [Fax Settings] - [TX/RX Settings], then configure the following settings.

Settings	Description
[Duplex Print (RX)]	Select whether to print an original on both sides of paper when multi-page fax is received. This item is not available if [Print Separate Fax Pages] is set to [ON]. [OFF] is specified by default.
[Letter/Ledger over A4/A3]	Select whether to preferentially print an original on inch-sized paper when a fax is received. The default value depends on the area the machine is used in.
[Print Paper Selection]	Select the criterion of selecting paper for printing a fax. • [Priority Size]: Prints a fax on paper specified in [Print Paper Size]. If the machine runs out of specified paper, paper of the next closest size is used. • [Fixed Size]: Always prints a fax on paper specified in [Print Paper Size]. • [Auto Select]: Prints a fax on paper that is automatically selected to suit the fax received. [Auto Select] is specified by default.
[Print Paper Size]	Select size of paper for printing received fax. The initial value varies depending on the setting for [Letter/Ledger over A4/A3].

Settings	Description
[Incorrect User Box No. Entry]	Select the action taken by the machine if unregistered user box is specified for receiving a fax using the machine's box. • [Print]: Prints a received fax without saving it in a user box. • [Show Error Message]: Handles the fax as a communication error. It is neither saved nor printed. • [Auto Create User Box]: Automatically creates a user box with a specified number and stores documents in it. [Print] is specified by default.
[Paper Tray Setting]	Specify the paper tray to print a fax. [Auto] is specified by default.
[Allow Paper Tray Setting]	Specify whether to allow fax printing for each paper tray when [Paper Tray Setting] is set to [Auto]. [Allow] is specified for all paper trays by default.
[Min. Reduction for RX Print]	If necessary, change the reduction ratio that is used when printing a fax. [96%] is specified by default.
[Print Separate Fax Pages]	Select whether to print a fax longer than the standard size on separate pages. This item is not available if [Duplex Print (RX)] is set to [ON]. [OFF] is specified by default.
[File After Polling TX]	Select whether to delete a file after it is sent in response to a polling request if Polling TX is used to register files for polling. [Delete] is specified by default.
[No. of Sets (RX)]	If necessary, change the number of copies to print a fax. [1] is specified by default.
[Fax RX Print Setting]	Select whether to print a received network fax in color or black and white. To restrict the print to only black and white print, select [Black Only]. [Full Color/Black] is specified by default.

9.2.3 Canceling stamp setting when sending a fax

You can automatically cancel stamp setting when sending a fax without a stamp.

In the administrator mode, select [System Settings] - [Stamp Settings] - [Fax TX Settings], then set [Cancel Setting] to [Cancel].

Tips

- This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

9.2.4 Adjusting the image quality depending on the resolution of a received fax

When printing a received fax, specify to give priority to the image quality or to the printing speed, according to the resolution of the received fax.

In the administrator mode, select [Fax Settings] - [Fax Print Quality Settings], then configure the following settings.

Settings	Description
[Low Resolution]	Select whether to give priority to image or speed when printing a received fax having a low resolution. If [Prioritize Quality] is selected, an image is corrected. [Prioritize Quality] is specified by default.
[High Resolution]	Select whether to give priority to image or speed when printing a received fax having a high resolution. If [Prioritize Quality] is selected, an image is corrected. Note that, for a high resolution fax, image correction is less effective relative to a low resolution fax. [Prioritize Speed] is specified by default.

9.3 Specifying useful transmission and reception functions

9.3.1 Enabling/Disabling the Fax Functions

Enable or disable fax transmission and reception functions, such as Confirm Address that prevents wrong fax transmission, F-Code TX, and Relay RX.

In the administrator mode, select [Fax Settings] - [Function Setting] - [Function ON/OFF Setting], then configure the following settings.

Settings	Description
[F-Code TX]	Select whether to use F-Code TX. F-Code TX is a function that sends documents to a destination by entering a SUB address and a sender ID (communication password) of a specific user box. The remote machine must support the F-Code TX/RX. Faxing is possible without specifying a sender ID (communication password). This setting is used for Confidential Communication, Relay Distribution, or PC-Fax RX. [ON] is specified by default.
[Relay RX]	Select whether to use this machine as a fax relaying station. If this machine is used as a relaying station, it is possible to receive a fax from a remote machine and automatically relay it to multiple programmed destinations. [ON] is specified by default.
[Relay Printing]	Select whether to distribute and print a received fax when this machine is used as a fax relaying station. [OFF] is specified by default.
[Destination Check Display Function]	Select whether to show a list of specified destinations before sending a fax. Select [ON] if you want to check destinations before sending a fax. Using this function helps to prevent wrong transmission or not forget sending of a fax. If necessary, select whether to request the user to enter the password for approving the transmission after showing a list of specified destinations. Select [ON] from [TX Approval Password], then enter the password to approve the transmission (using up to 64 characters). To change the password, select the [Password is changed.] check box, then enter a new password. [OFF] is specified by default.
[Confirm Address (TX)]	Select whether to require the user to enter a fax number twice to send a fax by directly entering the fax number. This is helpful to prevent a fax from being sent to an incorrect destination. [OFF] is specified by default.
[Confirm Address (Register)]	Select whether to require the user enter a fax number twice to register it when, for example, registering a destination or forwarding destination. This is helpful to prevent the fax number from being incorrectly registered. [OFF] is specified by default.
[PIN Code Display Mask Function]	Configure a setting to prevent display of the PIN code in a fax report or job history when adding a personal ID (PIN code) to a fax number in order to send a fax. If [ON] is selected, specify the separator to identify the PIN code. To specify the sending destination, enclose the PIN code with the separators you selected in this option. [OFF] is specified by default. When [PIN Code Display Mask Function] is set to [ON], the following functions are not available. • [Fax Settings] - [Function Setting] - [Incomplete TX Hold] • [Fax Settings] - [Header/Footer Position] - [Print Receiver's Name]

9.3.2 Using the Closed Network RX function

Closed Network RX is a function that restricts the peers by passwords. You can use this function only when the remote machine is one of our models that have the Password TX function.

In the administrator mode, select [Fax Settings] - [Function Setting] - [Closed Network RX], and select the [Password is changed.] check box (Default: [OFF] (not selected)). Then, enter the password to restrict communication peers (using up to four digits).

Inform the peer of the password you entered here.

9.3.3 Using the Fax Retransmit function

Fax Retransmit is a function that stores a fax that could not be sent by Redial in the machine's user box for a given period of time.

A stored fax job can be resent later by recalling it from the box.

In the administrator mode, select [Fax Settings] - [Function Setting] - [Incomplete TX Hold], then configure the following settings.

Settings	Description
[Incomplete TX Hold]	Select this option to use the Fax Retransmit function. [OFF] (not selected) is specified by default.
[File Storage Duration]	Specify the time period during which a fax failed to be sent is stored in the machine's user box. [12] hours is specified by default.

9.3.4 Using the Memory RX function

Memory RX is a function to save a received fax in the Memory RX User Box of this machine without printing it. You can check the contents of incoming faxes and print only those you need to print, by which you can reduce the printing cost.

Tips

- The memory RX function cannot be used together with the following functions.
  TSI User Box, PC-Fax RX, Forward TX

1 In the administrator mode, select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [Memory RX Setting], then click [OK].

2 In [Memory RX Setting], configure the following settings.

Settings	Description
[Memory RX User Box Password]	Enter the password to restrict accesses to the Memory RX User Box (using up to eight digits). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

9.3.5 Using the Forward TX function

Forward TX is a function that transfers a received fax, Internet fax, or IP address fax to a pre-specified destination.

Faxes can be forwarded to personal E-mail addresses or saved in a shared folder in a computer. Received faxes can be converted to files that can be handled by a computer, which saves printing costs.

Tips

- If the forwarding destination is not a fax address, the received fax can be converted in the specified file format to be forwarded to a destination. The file types able to be specified are PDF, XPS, and TIFF. Other file types must be specified by the service engineer. For details, contact your service representative.
- This function cannot be used together with the following functions.
  PC-Fax RX, TSI Routing, Memory RX

1 In the administrator mode, select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [Forward TX Setting], then click [OK].

2 Select a fax function to configure the Forward TX function.

- ➔ To forward a fax received on this machine, click [Edit] of G3 Fax in [Select Fax Settings].
- ➔ To forward an Internet fax received on this machine, click [Edit] of Internet Fax in [Select Fax Settings].
- ➔ To forward an IP address fax received on this machine, click [Edit] of IP Address Fax in [Select Fax Settings].

3 In [Forward TX Setting], configure the following settings.

Settings	Description
[Fax Forwarding Settings]	Select [ON] to use the Forward TX function. [OFF] is specified by default.
[Output Method]	Select whether to print a received fax on this machine when forwarding it. • [Forward & Print]: A received fax is forwarded and printed on this machine. • [Forward & Print (If TX Fails)]: A received fax is forwarded and printed on this machine. [Forward & Print] is specified by default.
[Forward Dest.]	Specify a forwarding destination for a received fax. • [Select from Address Book]: Forwards a fax to a destination registered in the address book on this machine. • [Select from Group]: Forwards a fax to a group registered on this machine. • [Select from User Box No.]: Forwards a User Box registered on this machine. • [Direct Input]: Forwards a fax to the fax number you enter.
[File Format]	Select a file type to forward a fax. You can convert a fax into a file except when the forwarding destination is a fax. [PDF] is specified by default.
[Page Setting]	Select a filing page unit when a received fax contains multiple pages. • [Multi Page]: Select this check box to convert all pages to a single file. • [Page Separation]: Select this check box to convert each page to a separate file. [Multi Page] is specified by default.
[E-mail Attachment Method]	You can select the E-mail attachment method when the forward destination is an E-mail address and [Page Setting] is set to [Page Separation]. • [All Files Sent as one (1) E-mail]: Attaches all files to one E-mail. • [One (1) File per E-Mail]: Sends one E-mail for each file. [All Files Sent as one (1) E-mail] is specified by default.

9.3.6 Using the PC-Fax RX Function

PC-Fax RX is a function that automatically saves a received fax to the Memory RX User Box or a user box specified in F-Code (SUB Address).

A stored fax job can be read from the user box into a computer.

Tips

- This function cannot be used together with the following functions.
  Memory RX, Forward TX, TSI Routing

1 In the administrator mode, select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [PC-Fax RX Setting], then click [OK].

2 In [PC-Fax RX Setting], configure the following settings.

Settings	Description
[PC-Fax RX Setting]	Select [Allow] to use the PC-Fax RX function. [Restrict] is specified by default.
[Receiving User Box Destination]	Select the location where you want to a received fax saved from [Memory RX User Box] or [Specified User Box] (a User Box specified in F-Code (SUB Address)). [Memory RX User Box] is specified by default.
[Print]	Select whether to print a received fax after it has been received. [ON] is specified by default.
[Communication Password]	If you select [Specified User Box] for [Receiving User Box Destination], specify whether to check the communication password (Sender ID) for PC-Fax reception. To confirm the communication password, select the [Password Check] check box, then enter a communication password (using up to eight digits, including symbols # and *).

9.3.7 Using the TSI Routing function

TSI (Transmitting Subscriber Identification) is a sender's fax number. TSI (Transmitting Subscriber Identification) Routing is a function that automatically sorts incoming faxes into preset boxes or redirects them to user computers or E-mail addresses based on the fax numbers of the senders.

Tips

- This function cannot be used together with the following functions.
  Forward TX, Memory RX, PC-Fax RX

1 In the administrator mode, select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [TSI User Box Settings], then click [OK].

2 In [TSI User Box Settings], configure the following settings.

Settings	Description
[TSI User Box Setting]	Select [ON] to use the TSI Routing function. [OFF] is specified by default.

Settings	Description
[Action when TSI User Box is not set.]	Select the action to be taken by the machine if a fax number (TSI) is not registered and no forwarding destination is received. • [Automatically Print]: Prints a received fax without saving it in a box. • [Memory RX User Box]: Saves received documents in a Memory RX User Box. • [Specified User Box]: Saves received documents in a specified box. Click [Search from List], then select the box to save the received documents from the list. • [Specified Destination]: Forwards received documents to the specified one-touch destinations To select the desired forwarding destinations from the address book registered on this machine, click [Search from List]. • [Specified Group]: Forwards received documents to the specified group. To select the desired forwarding destinations from the group registered on this machine, click [Search from List]. [Automatically Print] is specified by default.
[Print]	Select whether to print a received fax after it has been received. [OFF] is specified by default.

3 Click [Register Forwarding Destination], then click [OK].

➔ Clicking [Set All] allows you to specify the file type to automatically forward a received fax using the TSI Routing function. The specified file type is applied to all forwarding destinations.
[Set All] is available when the optional **Extension Memory** and **i-Option LK-110 v2** are installed in this machine.

[TSI User Box List] is displayed.

4 In the [TSI User Box List], click [Create], then configure the following settings.

Settings	Description
[Sender (TSI)]	Enter the fax number (TSI) of the sender you want to register the forwarding destination in (using up to 20 digits, including symbols #, *, +, and spaces).
[Forwarding Destination]	Specify a forwarding destination when a fax is received from the fax number entered at [Sender (TSI)]. • [Select from Address Book]: Forwards a fax to a destination registered in the address book on this machine. • [Select from Group]: Forwards a fax to a group registered on this machine. • [Select from User Box No.]: Forwards a user box registered on this machine.
[File Format]	Select a file type to forward a fax. You can convert a fax into a file except when the forwarding destination is a fax. This setting can be configured when the optional **Extension Memory** and **i-Option LK-110 v2** are installed in this machine. [PDF] is specified by default.
[Page Setting]	Select a filing page unit when a received fax contains multiple pages. • [Multi Page]: Select this check box to convert all pages to a single file. • [Page Separation]: Select this check box to convert each page to a separate file. [Multi Page] is specified by default.
[E-mail Attachment Method]	You can select the E-mail attachment method when [Page Setting] is set to [Page Separation] while an E-mail address is set as a fax forwarding destination. • [All Files Sent as one (1) E-mail]: Attaches all files to one E-mail. • [One (1) File per E-Mail]: Sends one E-mail for each file. [All Files Sent as one (1) E-mail] is specified by default.

9.3.8 Restricting PC-FAX transmission

Select whether to allow PC-Fax TX using the fax driver.

To restrict PC-FAX transmission, select, in the administrator mode, [Fax Settings] - [Function Setting] - [PC-FAX TX Setting] - [Restrict] (Default: [Allow]).

9.4 Specifying fax report print conditions

Specify the conditions for printing fax-related reports. There are some reports automatically printed and others to be printed manually.

In the administrator mode, select [Fax Settings] - [Report Settings], then configure the following settings.

Settings	Description
[TX Result Report]	Select when to print a report containing the results of fax transmission. • [Always]: The report is printed every time a fax has been transmitted. • [If TX Fails]: The report is printed if a fax transmission has failed. • [OFF]: The report is not printed. [If TX Fails] is specified by default.
[Tx Result Report Print Confirmation Screen]	Select whether to display a screen that asks if you want to print a TX Result Report each time a fax is sent. [Not Specify] is specified by default.
[Sequential TX Report]	Select whether to print a report containing results of faxes sent by polling and broadcast. [ON] is specified by default.
[Broadcast Result Report]	Select whether to combine results of broadcast on all destinations involved or list them for each destination. [All Destinations] is specified by default.
[Bulletin TX Report]	Select whether to print a report containing records of faxes registered with the bulletin for being received by polling. [ON] is specified by default.
[Relay TX Result Report]	Select whether to print a report containing results of faxes sent by relay distribution. [ON] is specified by default.
[Tx Result Report Print Settings]	Select the method to output a TX result report (TX result report, broadcast result report, polling TX result report, replay TX result report, or bulletin board polling TX result report). • [Print]: Prints a TX result report on this machine. • [E-mail Notification]: Sends a TX result report to any destination by E-mail. E-mail settings are required in advance. For details on E-mail settings, refer to page 7-2. [Print] is specified by default. If [E-mail Notification] is selected, configure the following items. • [Notification Address]: Enter the E-mail address of the destination (using up to 320 characters, excluding spaces). • [Notification Address Priority Setting]: Select a notification destination when User Authentication is enabled. Selecting [User Address] issues a notification to the E-mail address of the user who logs in to this machine and sends a fax. If the user's E-mail address is not registered, a notification is issued to the destinations registered in [Notification Address]. If [Notification Address] is selected, a notification is always issued to the destination registered in [Notification Address]. [Notification Address] is specified by default. • [Report File Attachment]: Select whether to convert a TX result report to a file and attach it to an E-mail. [Attach] is specified by default. • [Report Image Setting]: Select whether to display the first page of the sent original on a TX result report. [With image] is specified by default. • [Report File Format]: Select the file type to attach a TX result report to an E-mail. [PDF] is specified by default.
[Activity Report]	Select whether to print a report containing results of faxes sent and received. To print it, select when to print it. • [OFF]: Does not print an activity report. • [Daily]: Prints an activity report at a specified time you entered at [Output Time Settings] every day. • [Every 100 Comm.]: Prints an activity report every 100 communications. • [100/Daily]: Prints an activity report at a specified time you entered at [Output Time Settings] every day. In addition, a report is printed every 100 communications. [Every 100 Comm.] is specified by default.
[Relay Request Report]	Select whether to print the report when the machine has received a fax (Relay RX) as a relaying station. [ON] is specified by default.

Settings	Description
[PC-Fax TX Error Report]	Select whether to print a report if PC-Fax TX using the fax driver has failed. [OFF] is specified by default.
[Timer Reservation TX Report]	Select whether to print a report when transmission is reserved using the Timer TX function. [ON] is specified by default.
[Confidential Rx Report]	Select whether to print a report containing the results of confidential faxes received. [ON] is specified by default.
[Remark Column Print Setup]	Select whether to print user or account name in the remarks column of the activity report if user authentication or account track is enabled for this machine. • [Normal Printing]: The line status or sending setting will be printed. • [User Name Printing]: The user name for user authentication will be printed. • [Account Name Printing]: The account name for user authentication will be printed. [Normal Printing] is specified by default.
[Network Fax RX Error Report]	Select whether to print a report if the machine has failed to receive an Internet fax or IP address fax. [ON] is specified by default.
[Print Job Number]	Select [ON] to display a job number on a report to be printed. The following reports are targeted for this processing. • Activity Report • TX Report • RX Report • TX Result Report • Broadcast Result Report Also, on the job display screen of the **Control Panel**, display a job number instead of the communication time of the communication list. [OFF] is specified by default.
[MDN Message]	Select whether to print a report notifying that an Internet fax has been sent to the recipient machine. [ON] is specified by default.
[DSN Message]	Select whether to print a report notifying that an Internet fax has been sent to the mail server of the recipient machine. [OFF] is specified by default.
[Print E-mail Message Body]	Select whether to print a report notifying that an Internet fax has been successfully received after it was received. The report has the subject and message body of an Internet fax. [Print] is specified by default.
[Legend display Settings]	Select [ON] to display an explanatory note on a report to be printed. If an explanatory note is omitted, the image of the sent original can be displayed on a larger area. [ON] is specified by default.

9.5 Restricting Deletions of Received Faxes

Restrict a deletion of fax documents in the Memory RX User Box or a deletion of fax receive jobs from the job display screen.

Two methods are available to restrict deletions.

- Ask the user to enter the password when deleting to enable deletion when the entered password matches the password that is pre-registered on this machine.
- Allow a deletion when a user logs in with User Box administrator or administrator privileges.

In the administrator mode, select [Fax Settings] - [Function Setting] - [RX Data Deletion Restriction Settings], then configure the following settings.

Settings	Description
[RX Data Deletion Restriction Settings]	Select [ON] to restrict deletion of received faxes. [OFF] is specified by default.
[Password Deletion]	To restrict deletion of received faxes with a password, enter the password (using up to eight digits). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Administrator User Box Deletion]	Makes a restriction to delete received faxes only when a user logs in with User Box administrator or administrator privileges. [Administrator User Box Deletion] is displayed when User Authentication or Account Track is enabled and User Box Administrator is specified.

10 Configuring the Network Fax Environment

10 Configuring the Network Fax Environment

10.1 Configuring the Internet fax environment

Overview

Internet fax is a function used to send and receive fax via enterprise network and Internet. Internet fax is sent or received via E-mail. The same network as computer network is used for fax transmission. Therefore, you can send and receive faxes without having to worry about high communication costs to distant locations or to send a large number of pages.

Since this machine supports SSL/TLS encryption, and POP before SMTP authentication, security can be assured.

When the LDAP server or Active Directory is used for user management, you can search for or specify E-mail address from the server.

When using Internet Fax, follow the below procedure to configure the settings.

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

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for sending and receiving an Internet fax

➔ For details on configuring the setting, refer to page 10-2.

3 Set the following options according to your environment

Purpose	Reference
Check of a fax reception	page 10-4
Change of the reception capability of this machine that is notified to a peer	page 10-5
Change of default compression type setting for transmission in black and white	page 10-5
Change of default compression type setting for transmission in color	page 10-6
Communicate with the E-mail server using SSL/TLS	page 10-6
Use of SMTP Authentication when sending E-mails	page 10-7
Use of POP Before SMTP Authentication when sending E-mails	page 10-7
Search for an E-mail address using the LDAP server or Active Directory	page 7-18

Configure basic settings for sending and receiving an Internet fax

Enable the Internet fax function. In addition, specify the information of this machine and settings required to send and receive E-mail.

1 In the administrator mode, select [Network] - [Network Fax Setting] - [Network Fax Function Settings], and then set [I-Fax Function Setting] to [ON] (Default: [OFF]).

2 In the administrator mode, select [System Settings] - [Machine Setting], then configure the following settings.

Settings	Description
[Device Name]	Enter the name of this machine (using up to 80 characters, excluding spaces). The name set here is used as a part of the subject of Internet fax.

Settings	Description
[E-mail Address]	Enter the E-mail address of this machine with 320 characters, excluding spaces. This E-mail address is used as sender Internet fax address.

3 In the administrator mode, select [Fax Settings] - [Header Information], then configure the following settings.

Settings		Description
[Default]		Select the default setting for the sender name. The sender name, which is specified by default, is automatically added when a fax is sent.
[Sender Name]		Displays registered sender names.
[Edit]		You can register up to 20 sender names. Use this option to use different sender names depending on the destination.
	[No.]	Displays the registration number.
	[Sender Name]	Enter a sender name (using up to 30 characters).
[Delete]		Click this button to delete the registered sender name.

4 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[E-mail TX Setting]	Select this option to use the Internet fax function. [ON] (selected) is specified by default.
[Scan to E-mail]	Select [ON] to use Internet fax. [ON] is specified by default.
[E-mail Notification]	If a warning such as paper addition, toner replacement, or paper jam occurs on this machine, it can be sent to a registered E-mail address. For details, refer to page 14-11. [ON] is specified by default.
[Total Counter Notification]	Select whether to use the total counter notification function. Using this function allows you to send counter information managed by this machine to the registered E-mail address. For details, refer to page 14-12. [ON] is specified by default.
[SMTP Server Address]	Enter the address of your E-mail server (SMTP). Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port Number]	If necessary, change the port number of the E-mail server (SMTP). In normal circumstances, you can use the original port number. [25] is specified by default.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (SMTP), as required. [60] sec. is specified by default.
[Max Mail Size]	If you restrict the size of an E-mail to be sent in your environment, select [Limit]. [No Limit] is specified by default.
[Server Capacity]	If you select [Limit] at [Max Mail Size], enter the maximum E-mail size including attachment. E-mails exceeding the specified size are discarded. If you select [Binary Division] to divide an E-mail, this setting is invalid.

Settings	Description
[Binary Division]	Select this check box to divide an E-mail. The E-mail is divided according to the size specified at [Divided Mail Size]. This item is necessary if you occasionally send E-mails exceeding the maximum size specified on the E-mail server side. To read a divided E-mail, the mail soft receiving E-mails must have a function to restore the divided E-mail. The mail soft without the restore function may not read the divided E-mail. [OFF] (not selected) is specified by default.
[Divided Mail Size]	Enter the size to divide an E-mail. This item is necessary when [Binary Division] is enabled.

5 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX (POP)], and configure the following settings.

Settings	Description
[E-mail RX Setting]	Select [ON] to use Internet fax. [ON] is specified by default.
[POP Server Address]	Enter the address of your E-mail server (POP). Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name when receiving E-mails using the E-mail server (POP) (using up to 63 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 15 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (POP) as required. [30] sec. is specified by default.
[Port Number]	If necessary, change the port number of the E-mail server (POP). In normal circumstances, you can use the original port number. [110] is specified by default.
[Check for New Messages]	Select this check box to check for incoming faxes by periodically connecting to the E-mail server (POP) on this machine. Also, enter an interval for connecting the E-mail server (POP) at [Polling Interval]. [ON] (selected) is specified by default.

Checking a fax reception

Configure the settings for requesting or responding the Internet fax transmission result, and the setting regarding the exchange of capability information between machines.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [I-Fax Advanced Setting], then configure the following settings.

Settings	Description
[MDN Request]	Select whether to request for fax reception result (MDN request) to the destination. If a MDN request is sent, the recipient machine returns a response message upon reception of a fax, so that you can check that the fax is successfully received by the destination. Also, by receiving a response message from the destination, you can obtain the reception capability information of the destination. When new response message is received from a destination registered in the address book, the capability information is overwritten with new one. [ON] is specified by default.

Settings	Description
[DSN Request]	Select whether to request for fax reception result (DSN request) to the destination mail server. If you select [ON] for [MDN Request], priority is given to the MDN request. [OFF] is specified by default.
[MDN Response]	Select whether to return a response message when a sender requests for fax reception result (MDN request). [ON] is specified by default.
[MDN/DSN Response Monitoring Setting]	Select this check box to specify the waiting time for a response from the destination after a MDN request or DSN request is sent by this machine. If necessary, change the waiting time for a response from the destination at [Monitoring Time]. If a response message is received after the specified waiting time, the machine ignores the message. [24] hours is specified by default.
[Maximum Resolution]	If necessary, switch the maximum resolution that this machine can support. [Ultra Fine] is specified by default.
[Add Content-Type Information]	Select whether to add Content-Type information to an Internet fax when sending it. [OFF] is specified by default.

Specifying the reception ability of this machine

This machine notifies its reception capability when returning a MDN response. Change the contents that are notified upon return of an MDN response as necessary.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [Internet Fax RX Ability], then configure the following settings.

Settings	Description
[Compression Type]	Select the check boxes of the compression types of a fax job the machine can receive.
[Paper Size]	Select the check boxes of the paper sizes of a fax job the machine can receive.
[Fax Resolution]	Select the check box of the resolution of a fax job the machine can receive.

Configuring default compression type setting for transmission in black and white

If necessary, change the default compression type setting when sending a fax in black and white.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [Black Compression Level], then configure the following settings.

Settings	Description
[Black Compression Level]	Select the default compression type for transmission in black and white • [MH]: The data size is larger than [MMR]. • [MR]: The data size is intermediate between [MH] and [MMR]. • [MMR]: The data size is the smallest. [MMR] is specified by default.

Configuring default compression type setting for transmission in color

If necessary, change the default compression type setting when sending a fax in full color or gray scale.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [Color/Grayscale Multi-Value Compression Method], then configure the following settings.

Settings	Description
[Color/Grayscale Multi-Value Compression Method]	Select the default compression type for transmission in full color or gray scale. • [JPEG (Color)]: Compresses image data in color JPEG format. • [JPEG (Gray Scale)]: Compresses image data in black and white JPEG format. • [Unset]: Compress data according to the compression type specified in [Black Compression Level]. You cannot send data in color or gray scale. Whichever file format you specify, data is converted to the TIFF format. [JPEG (Color)] is specified by default.

Using an SSL/TLS communication

Encrypt communications between this machine and the E-mail server (SMTP) using SSL or TLS. This machine supports the SMTP over SSL and Start TLS.

Configure the setting if your environment requires SSL/TLS encryption communication with the E-mail server.

Tips

- To send to another company product, do not use SSL/TLS. Using SSL/TLS results in a sending error.

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings		Description
[Use SSL/TLS]		Select the method to encrypt communications with the E-mail server (SMTP). Select [SMTP over SSL] or [Start TLS] according to your environment. [OFF] is specified by default.
	[Port Number]	If you select [Start TLS] at [Use SSL/TLS], change the communication port number, if necessary. In normal circumstances, you can use the original port number. [25] is specified by default.
	[Port No.(SSL)]	If you select [SMTP over SSL] at [Use SSL/TLS], change the SSL communication port number, if necessary. In normal circumstances, you can use the original port number. [465] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

Using SMTP authentication

Configure the setting if your environment requires SMTP authentication to send an E-mail.

If the SMTP authentication is used, the user ID and password is sent from this machine when sending an E-mail to perform authentication.

To use the SMTP authentication, enable the SMTP authentication on this machine. In addition, enter information required for authentication.

In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[SMTP Authentication]	Select this check box to use the SMTP authentication. In [SMTP Authentication Method], select whether to use SMTP authentication for each authentication method shown below. • Kerberos • NTLMv1 • Digest-MD5 • CRAM-MD5 • LOGIN • PLAIN [OFF] (not selected) is specified by default.
[User ID]	Enter the user ID for SMTP authentication (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [User ID] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name (realm) for SMTP authentication (using up to 253 characters). This item is necessary when the SMTP authentication method is Digest-MD5. • Enter the domain name if two or more domains (realm) exist. • When only one domain (realm) exists, no entry is required. The domain name is notified from the E-mail server (SMTP) at the initial communication, and communication is automatically performed using that domain name.
[Authentication Setting]	Select whether to synchronize the SMTP authentication with the user authentication of this machine. This item is necessary when the user authentication is installed on this machine. • [User Authentication]: Uses the user name and password of the registered user of this machine as [User ID] and [Password] for the SMTP authentication. • [Set Value]: Uses values entered at [User ID] and [Password]. If SMTP authentication fails because the user who sends an E-mail does not match the user specified in the [User ID], select [Set] in [Envelope-From Setting], then enter the E-mail address to be applied to Envelope-From in [From Address]. If you select [Do Not Set] in [Envelope-From Setting], the E-mail address of the administrator of this machine will be applied to Envelope-From. For details on the E-mail address of the administrator of this machine, refer to page 4-2. [Set Value] is specified by default.

Using POP Before SMTP authentication

Configure the setting if your environment requires the POP Before SMTP Authentication to send an E-mail.

The POP Before SMTP authentication is a function that performs POP authentication using the E-mail server (POP) before sending an E-mail and allows E-mail transmission only when the authentication is successful.

To use the POP Before SMTP authentication, enable the POP Before SMTP on this machine. In addition, configure settings for connecting to the E-mail server (POP) used for authentication.

1 In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and configure the following settings.

Settings	Description
[POP before SMTP]	Select [ON] to use the POP Before SMTP. [OFF] is specified by default.
[POP before SMTP Time]	If necessary, change the waiting time until starting E-mail transmission after the POP authentication is successful. Depending on your environment, it may take time before the E-mail transmission is allowed after the POP authentication is successful. In that case, if a time period that is too short is specified, E-mail transmission may fail. [5] sec. is specified by default.

2 Set the POP over SSL and APOP settings according to your environment. In the administrator mode, select [Network] - [E-mail Setting] - [E-mail RX (POP)], and configure the following settings.

Settings		Description
[APOP Authentication]		If you use APOP in your E-mail server (POP), select [ON]. [OFF] is specified by default.
[Use SSL/TLS]		When using SSL to encrypt a communication with the E-mail server (POP), select this check box. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [995] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

10.2 Configuring the IP address fax environment

Overview

The IP address fax function is a function used to send and receive faxes within a limited network such as enterprise network. In addition to IP address, you can also use a host name and E-mail address to specify the destination.

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.

When using the IP address fax function, follow the below procedure to configure the settings.

✔ To use the IP Address Fax function, ask your service representative to configure settings. For details, contact your service representative.

✔ To use this function, the optional **Fax Kit** is required.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for sending and receiving faxes using IP address fax

➔ For details on configuring the setting, refer to page 10-9.

3 Set the following options according to your environment

Purpose	Reference
Change of default compression type setting for transmission in black and white	page 10-10
Change of default compression type setting for transmission in color	page 10-10

Configure basic settings for sending and receiving faxes using IP address fax

Enable the IP address fax function. In addition, configure settings for sending and receiving faxes, sender information of this machine, and operation mode for IP address fax.

1 In the administrator mode, select [Network] - [Network Fax Setting] - [Network Fax Function Settings], and then set [IP Address Fax Function Settings] to [ON] (Default: [OFF]).

2 In the administrator mode, select [Network] - [Network Fax Setting] - [SMTP TX Setting], then configure the following settings.

Settings	Description
[Port No.]	If necessary, change the port number of the E-mail server (SMTP). In normal circumstances, you can use the original port number. [25] is specified by default.
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (SMTP), as required. [60] sec. is specified by default.

3 In the administrator mode, select [Network] - [Network Fax Setting] - [SMTP RX Setting], then configure the following settings.

Settings	Description
[SMTP RX]	Select [ON] to use the IP address fax function. [OFF] is specified by default.
[Port Number]	If necessary, change the port number of the E-mail server (SMTP). In normal circumstances, you can use the original port number. [25] is specified by default.

Settings	Description
[Connection Timeout]	Change the timeout period for a communication with the E-mail server (SMTP), as required. [300] sec. is specified by default.

4 In the administrator mode, select [Fax Settings] - [Header Information], then configure the following settings.

Settings		Description
[Default]		Select the default setting for the sender name. The sender name, which is specified by default, is automatically added when a fax is sent.
[Sender Name]		Displays registered sender names.
[Edit]		You can register up to 20 sender names. Use this option to use different sender names depending on the destination.
	[No.]	Displays the registration number.
	[Sender Name]	Enter a sender name (using up to 30 characters).
[Delete]		Click this button to delete the registered sender name.

5 In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [IP Address Fax Operation Settings], then configure the following settings.

Settings	Description
[Operating Mode]	Select an operation mode of IP address fax according to your environment. • [Mode 1]: This mode allows communications between our models that support IP address fax communications and between models that comply with the Direct SMTP standard. However, because a unique method developed by our company is used to send a color fax, only our company's models can receive such a color fax. • [Mode 2]: This mode allows communications between our models that support IP address fax communications and between models that comply with the Direct SMTP standard. The method compatible with the Direct SMTP standard (Profile-C format) is used to send a color fax. [Mode 1] is specified by default.
[Sending Colored Documents]	Select whether or not to accept sending of color faxes when selecting [Operating Mode] for [Mode 2]. To send a fax to a machine that does not support color reception based on the Direct SMTP standard, select [Restrict]. [Allow] is specified by default.

Configuring default compression type setting for transmission in black and white

If necessary, change the default compression type setting when sending a fax in black and white.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [Black Compression Level], then configure the following settings.

Settings	Description
[Black Compression Level]	Select the default compression type for transmission in black and white • [MH]: The data size is larger than [MMR]. • [MR]: The data size is intermediate between [MH] and [MMR]. • [MMR]: The data size is the smallest. [MMR] is specified by default.

Configuring default compression type setting for transmission in color

If necessary, change the default compression type setting when sending a fax in full color or gray scale.

In the administrator mode, select [Fax Settings] - [Network Fax Setting] - [Color/Grayscale Multi-Value Compression Method], then configure the following settings.

Settings	Description
[Color/Grayscale Multi-Value Compression Method]	Select the default compression type for transmission in full color or gray scale. • [JPEG (Color)]: Compresses image data in color JPEG format. • [JPEG (Gray Scale)]: Compresses image data in black and white JPEG format. • [Unset]: Compress data according to the compression type specified in [Black Compression Level]. You cannot send data in color or gray scale. Whichever file format you specify, data is converted to the TIFF format. [JPEG (Color)] is specified by default.

11 Configuring the User Box Environment

11 Configuring the User Box Environment

11.1 Creating and editing a User Box

11.1.1 Creating a User Box

Create a Public, Personal, or Group User Box.

- Personal User Box can be used when user authentication is employed.
- Group User Box can be used when account track is employed.

In the administrator mode, select [Box] - [User Box List] - [New Registration], then configure the following settings.

Settings		Description
[User Box Number]		Registration number of the box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]		Enter the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Assign User Box Password]		When restricting usage of User Box using a password, select this check box and then enter a password (using up to 64 characters, excluding ").
[Index]		Select a corresponding character so that a User Box can be index searched with [User Box Name].
[Type]		Select [Public], [Personal], or [Group] depending on User Authentication or Account Track settings. • If [Personal] is selected, specify the owner user. • If [Group] is selected, specify the owner account.
[Auto Delete Document]		Specify the period from the date/time when a file was saved in, last printed, or sent from a User Box to the date/time when it is to be deleted automatically. • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[User Box Expansion Function]		To configure the User Box Expansion function, click [Display].
	[Confidential RX]	To add the Confidential RX function to a User Box, select the [Confidential RX] check box. Also enter the password for confidential RX (using up to eight characters). The entered password is required for sending a fax using Confidential TX to this machine. Inform the sender of the password you entered here. To use this function, the optional **Fax Kit** is required.
	[Auto Save Document to MFP Shared Folder]	To share files saved in the Public User Box of the machine using the SMB protocol on the network, select [ON]. This setting is available when: • [Public] is selected in [Type]; • [SMB Server Settings] and [Share SMB File Setting] are enabled in [Network] - [SMB Setting] - [SMB Server Settings] of the administrator mode; and • The [Confidential RX] check box is not selected. [OFF] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.1.2 Changing User Box settings

If you log in to the administrator mode, you can change settings for a registered User Box or delete it without entering the password for the User Box.

1 In the administrator mode, click [Box] - [User Box List].

2 Click [Edit] of the User Box to change settings for.

➔ Clicking [Delete] deletes the User Box you selected.

3 Use [User Box Attribute Change] to change User Box settings.

Settings		Description
[User Box Name]		Change the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Index]		Change a character to index-search a target User Box using [User Box Name].
[User Box Expansion Function is changed.]		Select this check box to change the User Box Expansion function.
	[Confidential RX]	Select [ON] to change the Confidential RX function of a User Box. Also enter the password for confidential RX (using up to eight characters). The entered password is required for sending a fax using Confidential TX to this machine. Inform the sender of the password you entered here. To use this function, the optional **Fax Kit** is required.
	[Auto Save Document to MFP Shared Folder]	To share files saved in the Public User Box of the machine using the SMB protocol on the network, select [ON]. This setting is available when: • [Public] is selected in [Type]; • [SMB Server Settings] and [Share SMB File Setting] are enabled in [Network] - [SMB Setting] - [SMB Server Settings] of the administrator mode; and • The [Confidential RX] check box is not selected. [OFF] is specified by default.
[User Box Password is changed.]		To change the password of a User Box, select this check box, then enter a new password (using up to 64 characters, excluding ").
[User Box Owner is changed.]		Select this check box to change the type or owner user of a User Box. Select [Public], [Personal], or [Group] depending on User Authentication or Account Track settings. • If [Personal] is selected, specify the owner user. • If [Group] is selected, specify the owner account.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.2 Creating and editing a System User Box

11.2.1 Creating a Bulletin Board User Box

Bulletin Board User Box is a box used to save multiple types of fax documents required for polling.

If announcement and other fax documents are stored in Bulletin Board User Boxes by purpose and if recipients are notified with the relating box numbers, the users can select the required fax documents and they can be polled.

Tips

- To use this function, the optional **Fax Kit** is required.

In the administrator mode, select [Box] - [System User Box List] - [New Registration] - [Bulletin Board User Box], then configure the following settings.

Settings	Description
[User Box Number]	Registration number of the box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Assign User Box Password]	When restricting usage of User Box using a password, select this check box and then enter a password (using up to 64 characters, excluding ").
[Type]	Select [Public], [Personal], or [Group] depending on User Authentication or Account Track settings. • If [Personal] is selected, specify the owner user. • If [Group] is selected, specify the owner account.
[Auto Delete Document]	Specify the period from the date/time when a file was saved in, last printed, or sent from a User Box to the date/time when it is to be deleted automatically. • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.

11.2.2 Creating a Relay User Box

Relay User Box is a box used to relay data when you use this machine as a relay machine to the facsimile.

If you use the Relay Distribution and when you send a fax to the relay machine, it distributes the fax to all recipients being registered in the Relay User Box.

If you are using broadcasting to distant places, you can reduce the total communication cost by using the relay machine.

Tips

- To use this function, the optional **Fax Kit** is required.

In the administrator mode, select [Box] - [System User Box List] - [New Registration] - [Relay User Box], then configure the following settings.

Settings	Description
[User Box Number]	Registration number of the box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Relay Address]	Click [Search from List], and select a group in which fax destinations are registered. When registering a group destination as a relay destination, be sure to set the fax address in the group destination in advance.

Settings	Description
[Relay TX Password]/[Retype Relay TX Password]	To restrict the usage of User Box using password, enter the password (using up to eight digits, including symbols # and *). The entered password is required when sending a relay request to this machine. Inform the sender who want to use this machine as a relay machine of the password you entered here.

11.2.3 Creating an Annotation User Box

Annotation User Box is a box used to automatically add the date, time and filing number to a file saved in this box when it is printed or sent.

When a file is read from the Annotation User Box and used for printout or transmission to a recipient, the date, time and annotation (previously determined for management) are added to the header or footer of each image automatically. You can prevent the unauthorized use of documents by creating a document that can identify the creation date and time and the serial page number of each document.

In the administrator mode, select [Box] - [System User Box List] - [New Registration] - [Annotation User Box], then configure the following settings.

Settings	Description
[User Box Number]	Registration number of the box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Assign User Box Password]	When restricting usage of User Box using a password, select this check box and then enter a password (using up to 64 characters, excluding ").
[Auto Delete Document]	Specify the period from the date/time when a file was saved in, last printed, or sent from a User Box to the date/time when it is to be deleted automatically. • [Do Not Delete]: Keeps the file in the User Box. • [Do Not Keep]: Select this option to use a document to give an annotation only without saving or using it for copying. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[Count Up]	Select the unit for adding a number to a file, By Job or By Page. • [By Job]: Adds a number per file. Even if a file has multiple pages, a same number is added to the file as one job. • [By Page]: Adds a number per page.
[Stamp Elements]	As necessary, specify the fixed text, date and time, and print position to be added to a file. • [Primary Field]: Add any text (using up to 40 characters). • [Secondary Field]: Add any text at the beginning of the annotation (using up to 20 characters). • [Date/Time Setting]: Select the format for the date and time. • [Print Position]: Select a position in which the annotation is printed. • [Density]: Select the density of characters of the date and time and annotation to be printed. • [Number Type]: Select the digit number of annotation.

Tips

- This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.
- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.2.4 Changing Bulletin Board User Box settings

If you log in to the administrator mode, you can change settings for a registered Bulletin Board User Box or delete it without entering the password for the Bulletin Board User Box.

Tips

- To use this function, the optional **Fax Kit** is required.

1 In the administrator mode, click [Box] - [System User Box List].

2 Click [Edit] of the User Box to change settings for.

➔ Clicking [Delete] deletes the User Box you selected.

3 Use [User Box Attribute Change] to change User Box settings.

Settings	Description
[User Box Name]	Change the User Box name (using up to 20 characters).
[User Box Password is changed.]	To change the password of a User Box, select this check box, then enter a new password (using up to 64 characters, excluding ").
[User Box Owner is changed.]	Select this check box to change the type or owner user of a User Box. Select [Public], [Personal], or [Group] depending on User Authentication or Account Track settings. • If [Personal] is selected, specify the owner user. • If [Group] is selected, specify the owner account.

11.2.5 Changing Relay User Box settings

If you log in to the administrator mode, you can change settings for a registered Relay User Box or delete it without entering the password for the Relay User Box.

Tips

- To use this function, the optional **Fax Kit** is required.

1 In the administrator mode, click [Box] - [System User Box List].

2 Click [Edit] of the User Box to change settings for.

➔ Clicking [Delete] deletes the User Box you selected.

3 Use [User Box Attribute Change] to change User Box settings.

Settings	Description
[User Box Name]	Change the User Box name (using up to 20 characters).
[Relay Address]	To change a destination, click [Search from List], and select a group in which fax destinations are registered. When registering a group destination as a relay destination, be sure to set the fax address in the group destination in advance.
[Relay TX Password is changed]	To change the relay TX password, select this check box, then enter a new password (using up to eight digits, including symbols # and *). The entered password is required when sending a relay request to this machine. Inform the sender who want to use this machine as a relay machine of the password you entered here.

11.2.6 Changing Annotation User Box settings

If you log in to the administrator mode, you can change settings for a registered Annotation User Box or delete it without entering the password for the Annotation User Box.

1 In the administrator mode, click [Box] - [System User Box List].

2 Click [Edit] of the User Box to change settings for.

➔ Clicking [Delete] deletes the User Box you selected.

3 Use [User Box Attribute Change] to change User Box settings.

Settings	Description
[User Box Name]	Change the User Box name (using up to 20 characters).
[Auto Delete Document]	Change the period from the date/time when a file was saved in, last printed, or sent form a User Box to the date/time when it is to be deleted automatically. • [Do Not Delete]: Keeps the file in the User Box. • [Do Not Keep]: Select this option to use a document to give an annotation only without saving or using it for copying. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[User Box Password is changed.]	To change the password of a User Box, select this check box, then enter a new password (using up to 64 characters, excluding ").
[Change Count Up]	To change the Count Up method, select this check box, and change settings. • [By Job]: Adds a number per file. Even if a file has multiple pages, a same number is added to the file as one job. • [By Page]: Adds a number per page.
[Change Stamp Elements]	To change Stamp Elements, select this check box, and change settings. • [Primary Field]: Add any text (using up to 40 characters). • [Secondary Field]: Add any text at the beginning of the annotation (using up to 20 characters). • [Date/Time Setting]: Select the format for the date and time. • [Print Position]: Select a position in which the annotation is printed. • [Density]: Select the density of characters of the date and time and annotation to be printed. • [Number Type]: Select the digit number of annotation.

Tips

- This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.
- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.3 Configuring User Box environment

11.3.1 Specifying the maximum number of User Boxes

You can set the maximum number of Public User Boxes that can be registered on this machine by the user.

In the administrator mode, select [User Auth/Account Track] - [Public User Box Setting], and then select the [Set the maximum number of User Boxes] check box (Default: [OFF] (not selected)).

In addition, enter the maximum number of Public User Boxes that can be registered in this machine by the user (unit: box).

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.3.2 Deleting all empty User Boxes

A User Box in which no files are saved is recognized as an unnecessary User Box and deleted.

In the administrator mode, select [System Settings] - [User Box Setting] - [Delete Unused User Box], then click [OK].

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.3.3 Automatically deleting files from a User Box

For all the Public User Boxes, Personal User Boxes, and Group User Boxes, the administrator specifies the time to automatically delete files from the date/time the files were last printed or sent.

This delete time is used as the time to delete files from an existing User Box and from a User Box you will create.

In the administrator mode, select [System Settings] - [User Box Setting] - [Document Delete Time Setting], then configure the following settings.

Settings	Description
[Delete Setting]	Allows the administrator to set the time to delete files from User Boxes automatically. If [ON] is selected, the [Auto Delete Document] setting will not be displayed during the user box registration process in user mode. Therefore, a user will not be able to specify a file delete time for each user box. [OFF] is specified by default.
[Delete Time Setting]	Sets a time to automatically delete files from a User Box. • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.3.4 Automatically deleting files from the SMB folder

If files in the Public User Box are shared on the network using the Share SMB File function, specify the period from the time when files are saved in the SMB folder via the Public User Box to the time when they are deleted automatically.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.
- This window is displayed when [SMB Server Settings] and [Share SMB File Setting] are enabled in [Network] - [SMB Setting] - [SMB Server Settings] of the administrator mode.

This delete time is used as the time to delete files from an existing SMB folder and from an SMB folder you will create.

In the administrator mode, select [System Settings] - [User Box Setting] - [Document in MFP Shared Folder Delete Time Setting], then configure the following settings.

Settings	Description
[Document in MFP Shared Folder Delete Time Setting]	Select whether the administrator collectively specifies times to automatically delete files in the SMB folder. [ON] is specified by default.
[Document in MFP Shared Folder Delete Time]	Specify the time to automatically delete files from the SMB folder. [1 day] is specified by default.

11.3.5 Specifying how to process a file after printing or transmission

Specify whether to keep the file in the Public User Box, Personal User Box, Group User Box, or Annotation User Box after it is printed or sent.

In the administrator mode, select [System Settings] - [User Box Setting] - [Document Hold Setting], then configure the following settings.

Settings	Description
[Document Hold Setting]	You can specify to hold or clear a file from the box after file printing or sending. [Hold] is specified by default.
[Delete confirmation screen.]	Select whether to display the deletion confirmation dialog box when keeping a file in a User Box. If [ON] is set, the user can select to leave or not the file in the User Box after printing or sending of the file. [Not Specify] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.4 Configuring System User Box environment

11.4.1 Deleting all secure documents

All files saved in the Secure Print User Box are deleted.

In the administrator mode, select [System Settings] - [User Box Setting] - [Delete Secure Print File], then click [OK].

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.4.2 Automatically deleting files from a System User Box

Specify the period from the date/time when a file was saved in or last printed from a Secure Print User Box or ID & Print User Box to the date/time when it is to be deleted automatically.

In the administrator mode, select [System Settings] - [User Box Setting] - [Delete Time Setting], then configure the following settings.

Settings	Description
[Auto Delete Secure Document]	Select this check box to specify the period from the date/time when a file was saved in a Secure Print User Box to the date/time when it is to be deleted automatically. In addition, set a time to automatically delete files. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted. [1 day] is specified by default.
[ID & Print Delete Time]	Select this check box to specify the period from the date/time when a file was saved in an ID & Print User Box to the date/time when it is to be deleted automatically. In addition, set a time to automatically delete files. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted. This item is available if user authentication has been adopted. [1 day] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.4.3 Specifying operations of printed ID & print documents

Select whether to ask the user if they want to delete the file from the ID & Print User Box after it is printed, or to always delete the file after it is printed without requesting confirmation.

In the administrator mode, select [System Settings] - [User Box Setting] - [ID & Print Delete Time], then configure the following settings.

Settings	Description
[Delete after Print]	Select whether to always delete files in the ID & Print User Box without checking with the user if they are to be deleted after printing them. [Confirm with User] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

11.5 Configuring the Share SMB File function

Overview

Share SMB File is a function that shares files in the Public User Box of the machine on the network using the machine as an SMB server.

This function allows you to connect to the device through the computer and easily export files in the Public User Box in the same way as when referencing the shared folder on the network.

To use the Share SMB File function, follow the procedure shown below.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

1 Configuring the SMB server

➔ For details on configuring the setting, refer to page 11-11.

2 Creating a Public User Box to share files

➔ For details on configuring the setting, refer to page 11-12.

Configuring the SMB server

Configure settings to use the machine as an SMB server.

In the administrator mode, select [Network] - [SMB Setting] - [SMB Server Settings], then configure the following settings.

Settings	Description
[SMB Server Settings]	Select [ON] to use the machine as an SMB server. [OFF] is specified by default.
[SMB Host Name]	Enter the SMB host name of the machine in uppercase letters (using up to 15 characters, including a symbol "-" but not to be used at the beginning or end of the character string).
[Workgroup]	Enter a work group name or domain name that contains the machine in uppercase letters (using up to 15 characters, excluding ", \, ;, :, ,, *, <, >, |, +, =, and ?). [WORKGROUP] is specified by default.
[SMB Authentication Protocol]	Select the SMB authentication protocol to be used in the machine. In Windows Vista and after, select [SMB1.0/SMB2.0] to use the SMB2.0 protocol. [SMB1.0/SMB2.0] is specified by default.
[SMB security Signature Setting]	Select whether to enable the SMB signature of this machine to suit your environment. • [Disable]: Disables the SMB signature of this machine. • [When Requested]: Enables the SMB signature of this machine (server) only when the SMB signature is requested from the client side. If the SMB signature is not requested from the client side, operations are performed while the SMB signature of this machine (server) remains disabled, and a connection is possible even when the SMB signature in the client side is disabled. • [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the client side. If the SMB signature in the client side is disabled, it will not be possible to make a connection. [When Requested] is specified by default.
[Share SMB File]	Select [ON] to use the Share SMB File function. [OFF] is specified by default.

Creating a Public User Box to share files

Create a Public User Box. Also, configure the setting to automatically transfer files from the Public User Box and save them in the SMB folder.

In the administrator mode, select [Box] - [User Box List] - [New Registration], then configure the following settings.

Settings		Description
[User Box Number]		Registration number of the box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]		Enter the User Box name (using up to 20 characters). Assign a name that helps you easily identify the User Box.
[Assign User Box Password]		When restricting usage of User Box using a password, select this check box and then enter a password (using up to 64 characters, excluding ").
[Index]		Select a corresponding character so that a User Box can be index searched with [User Box Name].
[Type]		Select [Public] to use the Share SMB File function.
[User Box Expansion Function]		Click [Display].
	[Auto Save Document to MFP Shared Folder]	Select [ON] to use the Share SMB File function. [OFF] is specified by default.

Tips

- This function cannot be used simultaneously with the Confidential RX function.

Reference

If files in the Public User Box are shared on the network using the Share SMB File function, you can specify the period from the time when files are saved in the SMB folder using the Public User Box to the time when they are deleted automatically. For details, refer to page 11-9.

11.6 Configuring the USB Memory Device settings

Specify whether to allow users to print and read files from a USB memory device and to save files to a USB memory device.

In the administrator mode, select [System Settings] - [User Box Setting] - [External Memory Function Settings], then configure the following settings.

Settings	Description
[Save Document]	Select whether to enable to save files on a USB memory. [OFF] is specified by default.
[Print Document]	Select whether to enable to print files from USB memory. [ON] is specified by default.
[USB to User Box]	Select whether to enable to save files from a USB memory into a User Box. [OFF] is specified by default.

Reference

If user authentication is enabled on this machine, you must set a permission for every user to save files in USB Memory ([Save Document]) and read files from USB Memory ([USB to User Box]). For details, refer to page 12-26.

11.7 Disabling user's operation of registration/change of a User Box

You can enable or disable each user's ability to create, edit, and delete a user box.

In the administrator mode, select [System Settings] - [User Box Setting] - [User Box Operation], then configure the following settings.

Settings	Description
[Allow/Restrict User Box]	You can enable or disable each user's ability to create, edit, and delete a user box. If only the administrator creates, edits, and deletes User Boxes, select [Restrict]. [Allow] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

12 Restricting Users from Using this Device

12 Restricting Users from Using this Device

12.1 Overview of User Authentication and Account Track

User Authentication

Employing User Authentication enables you to manage users who can use this machine. It also enables security- and cost-conscious advanced operations of this machine. By employing User Authentication, you can use the following functions to users of this machine.

Functions	Description
Identification	This function allows you to restrict users of this machine by identifying them.
Allow	You can set privileges to use the functions of this machine by user. • For example, you can configure settings so that to make printing is available for a specific user but not available for other users. Also, you can set it up so that users unidentified by this machine (public users) are not allowed to print data. • You can also limit access to destinations for each user. Based on the degree of importance of the address and relation with users, you can set it up so that specific users can access all destinations but other users can access only a part of destinations. Configuring settings according to the business requirements of users provides you with security measures and cost reductions simultaneously.
Accounting	You can record the use status of this machine by user. Analyzing it by user enables efficient operation of this machine. For example, depending on the use status of this machine, you can manage the maximum number of sheets each user can print. This encourages users to develop awareness of costs, contributing to cost reduction.

The user authentication methods are classified into three types: MFP authentication, external server authentication, and MFP authentication + External Server Authentication.

Authentication Method	Description
MFP authentication	The method to manage users of this machine using the authentication function of this machine. Since user information is managed inside this machine, you can use it only by registering it. For details, refer to page 12-5.

Authentication Method	Description
External server authentication	The method to manage users of this machine by synchronizing it with Active Directory or LDAP server. When Active Directory or LDAP server is used for user management in your environment, you can use user information managed using the server. This machine supports the following server types. • Active Directory: For details, refer to page 12-9. • NTLM: For details, refer to page 12-13. • LDAP: For details, refer to page 12-16. • NDS (NDS over IPX): For details, refer to page 12-19. • NDS (NDS over TCP/IP): For details, refer to page 12-21.
MFP authentication + External server authentication	The method using a combination of the authentication function of this machine and authentication by an external server. Even if some sort of problem occurs on the external authentication server, you can use this machine using its authentication function.

Tips

- You can also manage users of this machine by associating with the enhanced server such as **Authentication Manager**. To associate with the enhanced server, "Enhanced Server Authentication" and "ON (MFP) + ON (Enhanced Server)" are supported in addition to the above authentication method.

Account Track

Employing the Account Track function enables you to manage multiple users by account. Account authentication information is managed internally by this machine.

A password can be set by account to restrict users from using this machine. Also, this function allows you to restrict available functions or manage the use status of this machine by account.

For details on how to configure account track settings, refer to page 12-7.

Combining user authentication and account track

You can use a combination of user authentication and account track for management of each user for each department. To combine user authentication and account track, specify whether to synchronize account information with users according to your environment.

Relationship between users and accounts	Description
When the user and account is in one-to-one relation	By synchronizing account information with a user, you can associate the user with an account on a one-to-one basis. For example, you can allow a company staff member belonging to a certain department to print but not allow another member belonging to another department to print. Also, you can count the number of printed sheets by department to encourage each department to develop awareness of costs. If you specify the department of a user when registering him/her, you can log in as the account only by logging in as the user.

Relationship between users and accounts	Description
When a user joins multiple accounts	To manage the use status not only by actual department but also by project, do not synchronize the user with an account. For example, for a project across multiple departments, you can analyze the use status of this machine by project as well as by company staff member or department. To log in to this machine, enter the user name, then specify the account.

Tips

When switching between synchronization and non-synchronization of user authentication and account authentication depending on the business status, configure the following settings to allow each user to select whether to perform synchronization.

- In the administrator mode, select [User Auth/Account Track] - [General Settings], then set [Synchronize User Authentication & Account Track] to [Synchronize by User].
- In the administrator mode, select [Security] - [Restrict User Access], then set [Synchronize User Authentication & Account Track By User] to [Allow].

12.2 Employing the MFP authentication

Overview

Users of this machine can be restricted by the authentication function (ON (MFP)) of this machine. Authentication information of users are managed internally by this machine.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

When employing the MFP authentication, follow the below procedure to configure the settings.

1 Configuring basic settings for the user authentication

➔ For details on configuring the setting, refer to page 12-5.

2 Set the following options according to your environment

Purpose	Reference
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Construct a single sign-on environment for the SMB transmission	page 12-24
Configure a setting so that a user can log in to this machine using administrator privileges	page 12-25
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configuring basic settings for the user authentication

Enable user authentication. In addition, register the user on this machine.

1 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	Select [ON (MFP)] to employ the MFP authentication.
[Public User Access]	Select whether to allow that public users (unregistered users) to use this machine. • [ON (With Login)]: Allows that public users to use this machine. When a public user uses this machine, tap [Public User Access] on the Login screen to log in to this machine. • [ON (Without Login)]: A public user can use this machine without logging in to this machine. Using this option, you do not need to log in to this machine even when there are many public users. • [Restrict]: Restricts public users from using this machine. [Restrict] is specified by default. When public users' accesses are allowed, you can restrict functions available for public users. For details, refer to page 12-28.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.

2 In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [New Registration], then register a user.

Settings	Description
[No.]	User registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[User Name]	Enter the user name to log in to this machine (using up to 64 characters).
[E-mail Address]	If necessary, enter the E-mail address of the user (using up to 320 characters, excluding spaces). If the E-mail address is registered, the Scan to Me function is available to the user. For details, refer to page 12-23.
[User Password]/[Retype User Password]	Enter the password to log in to this machine (using up to 64 characters, excluding ").
[Function Permission]	Restricts functions available to the user if necessary. For details, refer to page 12-26.
[Max. Allowance Set]	Sets the maximum number of sheets the user can print and User Boxes they can register. For details, refer to page 12-29.
[Limiting Access to Destinations]	Restricts destinations the user can access if necessary. For details, refer to page 12-30.
[Permission Setting]	Assigns administrator privileges or User Box administrator privileges to a user as required. For details, refer to page 12-25.

Tips

- If you click [Continue Registration] after registering a user, you can register another user successively without going back to the user list screen.
- If you select [Stop Job] at [Temporarily stop use], you can temporarily disable the registered user.
- If the user authentication and account track functions are synchronized, [Account Name] is displayed. At [Account Name], you can specify the account name of the user.
- In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration], then click [Counter] to check the number of pages used for each user.

12.3 Employing the account track function

Overview

Installing Account Track enables you to collectively manage multiple users on an account basis. Account authentication information is managed internally by this machine.

A password can be set by account to restrict users from using this machine. Also, this function allows you to restrict available functions or manage the use status of this machine by account.

You can use a combination of user authentication and account track for management of each user for each department. For example, you can allow a company staff member belonging to a certain department to print but not allow another member belonging to another department to print. Also, you can count the number of printed sheets by department to encourage each department to develop awareness of costs. You can log in to this machine only by entering the user name. There is no need to specify the account.

When employing Account Track, follow the below procedure to configure the settings.

1 Configuring basic account track settings

➔ For details on configuring the setting, refer to page 12-7.

2 Set the following options according to your environment

Purpose	Reference
Synchronize with User Authentication	page 12-5
Restrict available functions by account	page 12-26
Specify the operations of this machine when you log out	page 12-36

Configuring basic account track settings

Enable the account track function. Also register the account.

1 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[Account Track]	Select [ON] to employ the account track function. [OFF] is specified by default.
[Account Track Input Method]	Select an account authentication method. This setting is required when you only use the account track function. [Account Name & Password] is specified by default.
[Synchronize User Authentication & Account Track]	When using user authentication and account track in conjunction, specify whether to synchronize user authentication and account track. • [Synchronize]: Select this option when the user and account is in one-to-one relation. If you specify the department of a user when registering him/her, you can log in as the account only by logging in as the user. • [Do Not Synchronize]: Select this option when the user joins multiple accounts. To log in to this machine, enter the user name, then specify the account. • [Synchronize by User]: Enables the user to select whether to synchronize the user authentication and account authentication. [Synchronize] is specified by default.
[User Counter]	When using user authentication and account track in conjunction, enter the number of counters to be assigned to the user. Up to 1000 counters can be assigned to the user and account collectively. For example, if you assign 950 user counters, you can assign up to 50 account track counters.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each account can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.

2 In the administrator mode, select [User Auth/Account Track] - [Account Track Settings] - [New Registration], then register an account.

Settings	Description
[No.]	Account registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Account Name]	Enter the account name to log in to this machine (using up to eight characters, excluding spaces and "). This entry is required if you have selected [Account Name & Password] at [Account Track Input Method] in Step 1.
[Password]/[Retype Password]	Enter the password to log in to this machine (using up to 64 characters, excluding ").
[Function Permission]	Restricts functions available to the account if necessary. For details, refer to page 12-26.
[Max. Allowance Set]	Sets the maximum number of sheets the account can print and User Boxes it can register. For details, refer to page 12-29.

Tips

- If you click [Continue Registration] after registering an account, you can register another account successively without going back to the account list screen.
- If you select [Stop Job] at [Temporarily stop use], you can temporarily disable the registered account.
- In the administrator mode, select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration], then click [Counter] to check the number of pages used for each account track.

12.4 Employing the Active Directory authentication

Overview

When you use Active Directory of Windows Server for user management, you can restrict users of this machine by authentication using Active Directory.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

When employing the Active Directory authentication, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Set the date and time for the machine

➔ The date and time of this machine must match those of Active Directory. For details on how to set the date and time of this machine, refer to page 4-4.

3 Configure basic settings for the Active Directory authentication

➔ For details on configuring the setting, refer to page 12-9.

4 Set the following options according to your environment

Purpose	Reference
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Send original data scanned by this machine easily to the login user's Home directory (Scan to Home).	page 12-11
Use the single sign-on	page 12-11
Construct a single sign-on environment for the SMB transmission	page 12-24
Reinforce authentication processing when using Active Directory	page 12-11
Securely execute a print job using the Web service in Windows 8/8.1/10	page 8-9
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configure basic settings for the Active Directory authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[External Server Name]	Enter the name of your Active Directory (using up to 32 characters). Assign an easy-to-understand name to the Active Directory to be registered.
[External Server Type]	Select [Active Directory].
[Default Domain Name]	Enter the default domain name of your Active Directory (using up to 64 characters).

Settings	Description
[Timeout]	Change the time-out time to limit a communication with the Active Directory if necessary. [60] sec. is specified by default.

2 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].
[Overwrite User Info]	When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case. If you select [Allow], the oldest authenticated user information is erased and the new user is registered. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method you use normally. [ON (External Server)] is specified by default.
[Ticket Hold Time Setting (Active Directory)]	Change the time to hold the Kerberos authentication ticket if necessary. [600] minutes is specified by default.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the authentication server. • [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

Sending to Your Computer (Scan to Home)

Scan to Home is a function that easily sends the original data scanned in this machine to a shared folder on a server or that on your computer.

To use the Scan to Home function, the following settings are required.

- Register the Home directory in Active Directory as registration information of the user (When using the host name, enter it using uppercase letters).
- Enable the Scan to Home function of this machine.

In the administrator mode, select [User Auth/Account Track] - [Scan to Home Settings], and then set [Scan to Home Settings] to [Enable] (Default: [Disable]).

Reference

For details on how to use the Scan to Home function, refer to "User's Guide[Scan Operations]/[Sending a File to a Shared Folder of a Computer (SMB Send)]".

Using the single sign-on

This machine supports the single sign-on of Active Directory.

If this machine joins the domain of Active Directory, the user authenticated by Active Directory can use the functions of this machine transparently. For example, once you log in to your computer, you can print data from this machine without setting authentication information in the printer driver.

1 In the administrator mode, select [Network] - [Single Sign-On Setting] - [Domain Login Setting], then register the domain this machine joins.

Settings	Description
[Permission Setting]	Select [ON] to use the single sign-on function. [OFF] is specified by default.
[Host Name]	Enter the host name of this machine (using up to 253 characters, including only - and . for symbol marks). In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting] - [DNS Host Name], to enter a host name.
[Domain Name]	Enter the domain name of Active Directory (using up to 64 characters).
[Account Name]	Enter the account name that has a privilege to participate users in the Active Directory domain (using up to 64 characters).
[Password]	Enter the password of the account you entered in [Account Name] (using up to 64 characters, excluding ").
[Timeout]	Change the time-out time of domain joining processing if necessary. [30] sec. is specified by default.

2 After entering required information in Step 1, click [OK].

The domain joining processing is executed.

3 In the administrator mode, select [Network] - [Single Sign-On Setting] - [Auto Log Out Time], then change the time to hold authentication information on this machine.

➔ Since the user can reuse authentication information while it is held on this machine, they can use the services of this machine without performing authentication again.

➔ [1 hour] is specified by default.

Tips

- In the administrator mode, select [Network] - [Single Sign-On Setting] - [Applications and Settings] to view the list of services of this machine that joins the domain of Active Directory.

Reinforcing authentication processing when using Active Directory

This machine is available to verify authentication information (ticket) obtained from Active Directory when it joins the Active Directory domain. This allows this machine to join a secure site via Active Directory.

1 In the administrator mode, select [User Auth/Account Track] - [Self-Verification Setting in AD Authentication] to configure the following settings.

Settings		Description
[Self-Verification Setting in AD Authentication]		Select [ON] to reinforce authentication processing when using Active Directory. [OFF] is specified by default.
[Domain Setting]		Specify the Active Directory domain this machine joins.
	[Host Name]	Enter the host name of this machine (using up to 253 characters, including only - and . for symbol marks). In the administrator mode, select [Network] - [TCP/IP Setting] - [TCP/IP Setting] - [DNS Host Name], to enter a host name.
	[Domain Name]	Enter the domain name of Active Directory (using up to 64 characters).
	[Account Name]	Enter the account name that has a privilege to participate users in the Active Directory domain (using up to 64 characters).
	[Password]	Enter the password of the account you entered in [Account Name] (using up to 64 characters, excluding ").
	[Timeout]	Change the time-out time of domain joining processing if necessary. [30] sec. is specified by default.

2 Click [OK].

The domain joining processing is executed.

Tips

- If you change [Host Name] or [Domain Name] and click [OK] while Active Directory's single sign-on is enabled on this machine, [Network] - [Single Sign-On Setting] - [Domain Login Setting] - [Permission Setting] in the administrator mode is changed to [OFF].

12.5 Employing the NTLM authentication

Overview

When you use Active Directory of Windows Server (NT-compatible domain environment) for user management, you can restrict users of this machine by authentication using NTLM.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

When employing the NTLM authentication function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the NTLM authentication

➔ For details on configuring the setting, refer to page 12-13.

3 Set the following options according to your environment

Purpose	Reference
Resolve the name using the WINS server	page 12-15
Use the NTLM authentication function in the IPv6 environment	page 12-15
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Construct a single sign-on environment for the SMB transmission	page 12-24
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configuring basic settings for the NTLM authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[External Server Name]	Enter the name of your authentication server (using up to 32 characters). Assign an easy-to-understand name to the authentication server to be registered.
[External Server Type]	Select [NTLM v1] or [NTLM v2].
[Default Domain Name]	Enter the default domain name of your authentication server (using up to 64 characters). The default domain name cannot be prefixed by an asterisk (*).

2 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].
[Overwrite User Info]	When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case. If you select [Allow], the oldest authenticated user information is erased and the new user is registered. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method you use normally. [ON (External Server)] is specified by default.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the authentication server. • [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

Using the WINS server

If the WINS server is installed to resolve the name, set the WINS server address and the name resolution method.

In the administrator mode, select [Network] - [SMB Setting] - [WINS/NetBIOS Settings], then configure the following settings.

Settings	Description
[WINS/NetBIOS]	Select [ON] to use the WINS server. [ON] is specified by default.
[Auto Obtain Setting]	Select [Enable] to automatically obtain the WINS server address. This item is necessary when DHCP is enabled. [Enable] is specified by default.
[WINS Server Address1]/[WINS Server Address2]	Enter the WINS server address. This item is necessary when you do not automatically obtain the WINS server address using the DHCP. Use the following entry formats. • Example of entry: "192.168.1.1"
[Node Type Setting]	Select 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 [H Node] is specified by default.

Using the direct hosting SMB service

Enabling the direct hosting SMB service allows you to specify the destination using the IP address (IPv4/IPv6) or host name.

In the administrator mode, select [Network] - [SMB Setting] - [Direct Hosting Setting], and then set [Direct Hosting Setting] to [ON]. You can use this function with the default settings unless otherwise requested.

12.6 Employing the LDAP authentication

Overview

When you use the LDAP server for user management, you can restrict users of this machine by authentication using LDAP.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

When employing the LDAP authentication function, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure basic settings for the LDAP authentication

➔ For details on configuring the setting, refer to page 12-16.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the LDAP server using SSL	page 12-18
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Construct a single sign-on environment for the SMB transmission	page 12-24
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configuring basic settings for the LDAP authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[External Server Name]	Enter the name of your LDAP server (using up to 32 characters). Assign an easy-to-understand name to the LDAP server to be registered.
[External Server Type]	Select [LDAP].
[Server Address]	Enter your LDAP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.
[Search Base]	Specify the starting point to search for a user (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"

Settings	Description
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.
[General Settings]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. [Simple] is specified by default.
[Search Attribute]	Enter the search attribute to be used for search of user account (using up to 64 characters, including a symbol mark -). The attribute must start with an alphabet character. [uid] is specified by default.
[Search Attributes Authentication]	Select this check box to enable the attribute-base authentication when [Simple] is selected for [General Settings]. If this check box is selected, the user does not need to enter all of the DN (Distinguished Name) when performing authentication via the LDAP server. On this screen, enter authentication information to be used when you log in to the LDAP server to search for the user ID ([Login Name] and [Password]). [OFF] (not selected) is specified by default.

2 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].
[Overwrite User Info]	When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case. If you select [Allow], the oldest authenticated user information is erased and the new user is registered. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method you use normally. [ON (External Server)] is specified by default.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the authentication server. • [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.

Settings	Description
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

Using SSL communication

Communication between this machine and the LDAP server is encrypted with SSL.

Configure the setting if your environment requires SSL encryption communication with the LDAP server.

In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[Enable SSL]	Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.

12.7 Installing the NDS over IPX authentication

Overview

When you use NDS (Novell Directory Service) of NetWare 5.1 or later for user management, you can restrict users of this machine by authentication using NDS.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

This section describes how to use NDS authentication in the IPX environment (NDS over IPX) using NetWare 5.1 or later. Apply the latest service pack to each NetWare version.

When employing the NDS over IPX authentication, configure settings using the following procedure.

1 Configure basic settings for the NDS over IPX authentication

➔ For details on configuring the setting, refer to page 12-19.

2 Set the following options according to your environment

Purpose	Reference
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Construct a single sign-on environment for the SMB transmission	page 12-24
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configure basic settings for the NDS over IPX authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[External Server Name]	Enter the name of your NDS server (using up to 32 characters). Assign an easy-to-understand name to the NDS server to be registered.
[External Server Type]	Select [NDS over IPX].
[Default NDS Tree Name]	Enter the default NDS tree name (using up to 63 characters).
[Default NDS Context Name]	Enter the default NDS context name (using up to 191 characters).

2 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].

Settings	Description
[Overwrite User Info]	When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case. If you select [Allow], the oldest authenticated user information is erased and the new user is registered. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method you use normally. [ON (External Server)] is specified by default.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the authentication server. • [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

3 In the administrator mode, select [Network] - [NetWare Setting] - [NetWare Setting], then configure the following settings.

Settings	Description
[IPX Setting]	Select [ON] to use this machine in the IPX environment. [OFF] is specified by default.
[Ethernet Frame Type]	Select the Ethernet frame type according to your environment. [Auto Detect] is specified by default.
[User Authentication Setting]	Select [ON] to authenticate the users using the NDS server. [ON] is specified by default.

12.8 Employing the NDS over TCP/IP authentication

Overview

When you use NDS (Novell Directory Service) of NetWare 5.1 or later for user management, you can restrict users of this machine by authentication using NDS.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the use status of this machine.

This section describes how to use NDS authentication in the TCP/IP environment (NDS over TCP/IP) using NetWare 5.1 or later. Apply the latest service pack to each NetWare version.

When employing the NDS over TCP/IP authentication, follow the below procedure to configure the settings.

1 Configure basic settings for the NDS over TCP/IP authentication

➔ For details on configuring the setting, refer to page 12-21.

➔ To use the authentication with NDS over TCP/IP, you must register the DNS server. When performing authentication, this machine inquires the DNS server about the tree name and context name to obtain the IP address of the NDS server. For details on how to register the DNS server, refer to page 5-3.

2 Set the following options according to your environment

Purpose	Reference
Send original data scanned by this machine easily to the login user's own address using E-mail (Scan to Me)	page 12-23
Construct a single sign-on environment for the SMB transmission	page 12-24
Restrict available functions by user	page 12-26
Restrict the access to destinations by user	page 12-30
Change function keys displayed in the **Touch Panel** by user	page 12-33
Specify the operations of the ID & Print function	page 12-35
Specify the operations of this machine when you log out	page 12-36
Restrict print jobs without authentication information	page 12-37
Print data from the printer driver without using the password	page 12-38

Configuring basic settings for the NDS over TCP/IP authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Edit], then configure the following settings.

Settings	Description
[External Server Name]	Enter the name of your NDS server (using up to 32 characters). Assign an easy-to-understand name to the NDS server to be registered.
[External Server Type]	Select [NDS over TCP/IP].
[Default NDS Tree Name]	Enter the default NDS tree name (using up to 63 characters).
[Default NDS Context Name]	Enter the default NDS context name (using up to 191 characters).

2 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].
[Overwrite User Info]	When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case. If you select [Allow], the oldest authenticated user information is erased and the new user is registered. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method you use normally. [ON (External Server)] is specified by default.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed. • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job. [Skip Job] is specified by default.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the authentication server. • [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

12.9 Sending to your address (Scan to Me)

The Scan to Me function is a function that transmits original data scanned on this machine to your address easily.

To use the Scan to Me function, the following preparation is required.

- Configuring the environment to use the Scan to E-mail function
- Installing the MFP authentication or external server authentication
- Registering an E-mail address as user's registration information

In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration], and enter your E-mail address into [E-mail Address] (using up to 320 characters, excluding spaces).

Tips

- If Active Directory is used as an authentication server, register the user's E-mail address in Active Directory.

Reference

For details on the E-mail transmission environment, refer to page 7-2.

For details on how to use the Scan to Me function, refer to "User's Guide[Scan Operations]/[Sending Original Data as an E-mail Attachment (Scan to E-mail)]".

12.10 Constructing a single sign-on environment for the SMB transmission

By using the user authentication information (login name and password) of this machine as SMB destination authentication information (host name and password), you can avoid the problem of having to specify SMB destination authentication information, allowing construction of a single sign-on environment for SMB transmission.

In the administrator mode, select [Network] - [SMB Setting] - [Client Setting], then configure the following settings.

Settings	Description
[SMB TX Setting]	Select [ON] to use the single sign-on function. [ON] is specified by default.
[SMB Authentication Setting]	Select [Kerberos/NTLM v1/v2] to use the single sign-on function. NTLMv2 authentication is performed if Kerberos authentication fails, and NTLMv1 authentication is performed if NTLMv2 authentication fails. [NTLM v1] is specified by default.
[Default Domain Name]	Enter the default domain name to be added to the host name of the destination at SMB transmission (using up to 64 characters). The default domain name cannot be prefixed by an asterisk (*). If the domain name of the destination is not specified by the user when sending data using SMB, the domain name specified here is added. This item is not required when Active Directory is used as an authentication server.
[SMB User Credential Setting]	When using the user authentication information (login name and password) of this machine as SMB destination authentication information (host name and password), select [ON]. If Active Directory is used as an authentication server, the domain name of Active Directory is added to the login name. When other authentication method is used, the domain name entered at [Default Domain Name] is added. [OFF] is specified by default.
[Edit SMB User Credentials]	This setting is available when [ON] is selected for [SMB User Credential Setting]. If you select [Restrict], an SMB destination is registered, excluding the user ID and password specified at login. However, using **Web Connection**, an SMB destination is registered, including the user ID and password. If you select [Allow], you can specify whether to register an SMB destination, including or excluding the user ID and password. If you select [Reg. excl. ID and Password] and register an SMB destination, the user ID and password are automatically added at SMB transmission. [Restrict] is specified by default.
[User Authentication(NTLM)]	Select [ON] to use the single sign-on function. [ON] is specified by default.
[SMB security Signature Setting]	Select whether to enable the SMB signature of this machine to suit your environment. • [Disable]: Disables the SMB signature of this machine. • [When Requested]: Enables the SMB signature of this machine (client) only when the SMB signature is requested from the server side. If the SMB signature is not requested from the server side, operations are performed while the SMB signature of this machine (client) remains disabled, and a connection is possible even when the SMB signature in the server side is disabled. • [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the server side. If the SMB signature in the server side is disabled, it will not be possible to make a connection. [When Requested] is specified by default.

12.11 Configuring a setting so that a user can log in to this machine using administrator privileges

You can configure a setting so that a registered user can log in to this machine using administrator privileges.

1 In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [Administrative Setting] - [Login Allowed with Administrative Rights], then click [Allow] (default: [Allow]).

2 In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Permission Setting] to assign administrator privileges to the registered user.

➔ To assign administrator privileges to a user, select [Permission Setting] - [Administrative Rights] - [Allow] (default: [Do not Allow]).

➔ When the User Box administrator is specified, User Box administrator privileges can be assigned to the registered user. To assign User Box administrator privileges to a user, select [Permission Setting] - [User Box Administrator Rights] - [Allow] (default: [Do not Allow]).

12.12 Setting privileges to use the functions of this machine by user or account

12.12.1 Restricting available functions by user or account

Employing User Authentication or Account Track enables you to restrict available functions by user or account.

For example, you can set it up so that specific users or accounts can print, but other users or accounts can not print. Configuring settings according to the business requirements of users or accounts provides you with security measures and cost reductions simultaneously.

Tips

- To use the MFP authentication, set restrictions of functions accessible by users or accounts when registering them.
- To use the external authentication server, user information is registered once you execute authentication. To restrict functions accessible by users, edit user information registered on this machine.

To configure settings for each user, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Function Permission] in the administrator mode.

To configure settings for each account track, select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration] - [Edit] - [Function Permission] in the administrator mode.

The setting items are as follows.

Functions	Description
[Copy]	Select whether to allow use of the copy function. [Black Only] allows black and white copy only. [Full Color/Black] is specified by default.
[Scan]	Select whether to allow use of the scan function. [Black Only] allows scan in black and white only. [Full Color/Black] is specified by default.
[Save to External Memory]	Select whether to enable to save files on a USB memory. This option is available when saving files in a USB memory device is enabled on this machine. This option is disabled for an account. [Restrict] is specified by default.
[External Memory Document Scan]	Select whether to allow to scan files from a USB memory device. This option is available when scanning files from a USB memory device is enabled on this machine. This option is disabled for an account. [Restrict] is specified by default.
[Fax]	Select whether to allow use of the fax and network fax functions. [Black Only] allows black and white transmission only. [Full Color/Black] is specified by default.
[Print]	Select whether to allow printing of the print function. [Black Only] allows black and white printing only. [Full Color/Black] is specified by default.
[User Box]	Select whether to allow to use files saved in the User Box. This option is disabled for an account. [Allow] is specified by default.
[Print Scan/Fax TX]	Select whether to allow to print scan data and fax TX data. [Black Only] allows black and white printing only. If you select [Restrict], you cannot print transmission data during scan and fax transmissions. In addition, you cannot print transmission data saved in the following User Boxes. However, you can print data saved in a User Box from an external memory. • Scan transmission data in Public, Personal, and Group User Box • Fax transmission data in Bulletin Board User Box, Polling Transmission User Box, and Fax Retransmit User Box [Full Color/Black] is specified by default.

Functions	Description
[Manual Destination Input]	Select whether to allow direct input of a destination. [Allow Fax Only] allows direct input of a fax number only. This option is disabled for an account. [Allow] is specified by default.
[Web Browser]	Select whether to allow use of the Web browser function. This function is available when the Web browser function is enabled. When the Web browser function is enabled, [Allow] is specified by default. To allow use of the Web browser function, specify whether to allow the following functions. • [File Upload]: Select whether to allow file uploading. [Allow] is specified by default. • [File Download]: Select whether to allow file downloading. [Allow] is specified by default. Set Web browser function restrictions to each user. They cannot be set to each account track.
[Biometric/IC Card Information Registration]	Select whether to allow registration of bio authentication information and IC card authentication information. This option is disabled for a public user or account. [Restrict] is specified by default.

Tips

- To use [Fax], the optional **Fax Kit** is required.
- The **Hard Disk** is optional in some areas. To use [External Memory Document Scan], [User Box], or [Print Scan/Fax TX], the optional **Hard Disk** is required.

Reference

You can specify the default function permission setting applied to users who use an external authentication server. For details, refer to page 12-27.

When public users' accesses are allowed, you can restrict functions available for public users. For details, refer to page 12-28.

12.12.2 Specifying the default function permission setting when the external server authentication is used

Specify the default function permission applied to users when an external authentication server is used.

Functions available to users who log in to this machine for the first time are limited according to the settings configured here.

In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [Default Function Permission], then configure the default function permission setting when using an external authentication server.

Reference

To use the external authentication server, user information is registered once you execute authentication. To restrict functions accessible by users, edit user information registered on this machine. For details, refer to page 12-26.

12.12.3 Restricting functions available to public users

When public users' (unregistered users') accesses are allowed, you can restrict functions available for public users. Also, you can restrict destinations public users can access.

In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [Public User], then configure the following settings.

Settings	Description
[Function Permission]	Restricts functions available to public users if necessary. For details, refer to page 12-26.
[Limiting Access to Destinations]	Restricts destinations public users can access if necessary. For details, refer to page 12-30.

Tips

- When a public user attempts to use a restricted function, the loin screen appears to switch the user. For example, if color scan is restricted for public users, the Login screen appears when a public user attempts a color scan operation. In this case, the user can log in to this machine as another user for whom color scan is allowed, and use the color scan function. In the administrator mode, select [User Auth/Account Track] - [Prohibited Function Login Setting], then set [Prohibited Function Login Setting] to [Request].

12.13 Managing the maximum number of copies by user or account

Employing User Authentication or Account Track enables you to specify the maximum number of copies by user or account. Also, you can set the upper limit of the number of User Boxes that can be registered.

Management of the upper limit of copies by user or account depending on the use status of this machine encourages users and accounts to develop awareness of costs and also contributes to cost reduction.

Tips

- To use the MFP authentication, set the upper limit when registering each user or account track.
- To use the external authentication server, user information is registered once you execute authentication. To set the upper limit, edit user information registered on this machine.

To configure settings for each user, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Max. Allowance Set] in the administrator mode.

To configure settings for each account track, select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration] - [Edit] - [Max. Allowance Set] in the administrator mode.

The setting items are as follows.

Functions	Description
[Total Allowance]	To manage the upper limit according to a total number of copies in color and black and white, select the [Total] check box, then enter the maximum allowance. [OFF] (not selected) is specified by default.
[Individual Allowance]	To manage the upper limit by color printing or black and white printing separately, select the check boxes of items to be managed, then enter the maximum allowance. [OFF] (not selected) is specified by default.
[Box Administration]	To manage the upper limit of User Boxes that can be registered, select the [Box Count] check box, then enter the maximum allowance. [OFF] (not selected) is specified by default. The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

12.14 Limiting the access to destinations for each user

12.14.1 Methods to limit access to destinations

You can limit access to destinations for each user on this machine. The following three methods are available to limit access to destinations.

Method to limit access	Description
Managing based on the reference allowed level	Sorts destinations depending on the importance level, and set the upper limit of the access level for each user. For details, refer to page 12-30.
Managing based on the reference allowed group	Sorts destinations into groups. A user can only access permitted destinations in the group. For details, refer to page 12-31.
Managing based on a combination of the reference allowed level and the reference allowed group	Set the access range based on a combination of the important level of a destination and the relationship between the destination and the user. For details, refer to page 12-31.

Tips

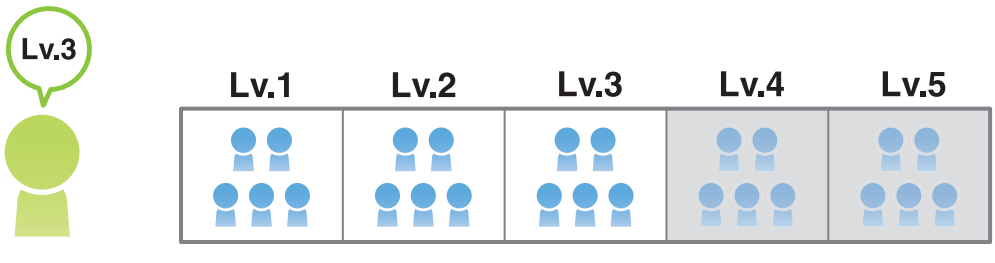
- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

12.14.2 Managing based on the reference allowed level

Reference Allowed Level

This function sorts out destinations registered in this machine from Level 0 to Level 5 in order of importance to set the upper limit of the access level (reference allowed level) for each user.

For example, assume that Level 3 is set for a certain user as a reference allowed level. In this case, that user can access destinations in Reference Allowed Level 1 to 3, but cannot access destinations in Reference Allowed Level 4 and 5.



Tips

- The reference allowed level set for the user is "Level 0" by default. Level-0 users can access only the destinations at level 0.

Setting the reference allowed level

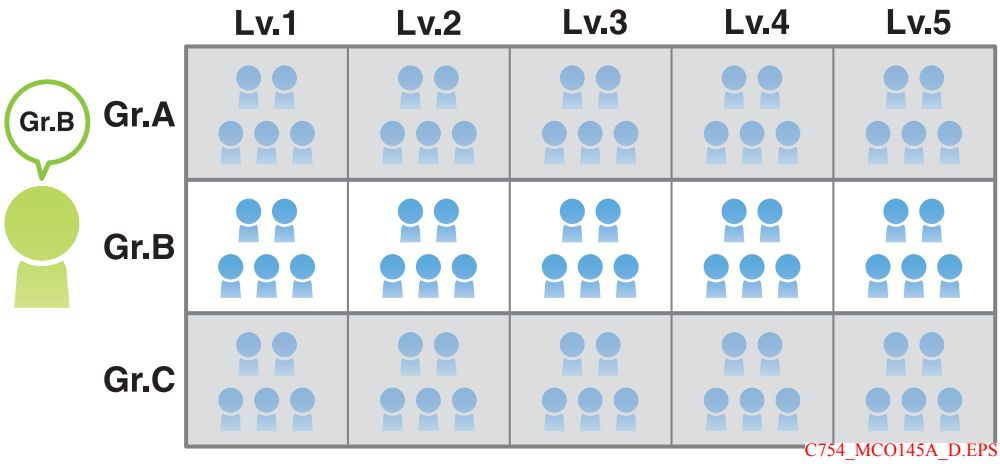
1. In the administrator mode, select [Store Address] - [Address Book] - [Edit], select [Set direct Reference Allowed Level], then set the reference allowed level for the address book.
2. In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit], then select the [Access Allowed Level] check box and set the reference allowed level for the registered user.

12.14.3 Managing based on the reference allowed group

Reference Allowed Group

This function sorts multiple destinations registered in this machine into a related group (reference allowed group) such as a group of customers per department.

Set a reference allowed group for each user to limit access to destinations. For example, assume that Group B is set for a certain user as a reference allowed group. In this case, that user can access destinations in Group B, but cannot access destinations in other reference allowed groups.



Assigning a reference allowed group

Register a reference allowed group on this machine. In addition, assign a reference allowed group to the destination and user.

1. In the administrator mode, select [Security] - [Address Reference Setting] - [Edit], and enter the group name into [Reference Allowed Group Name] (using up to 24 characters) to register the reference-allowed group.
2. In the administrator mode, select [Store Address] - [Address Book] - [Edit], select [Search from Reference Allowed Group], then assign the reference allowed group for the address book.
3. In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit], then select the [Reference Allowed Group] check box and assign a reference allowed group to the registered user.

12.14.4 Managing based on a combination of the reference allowed level and the reference allowed group

Combining the reference allowed level with the reference allowed group

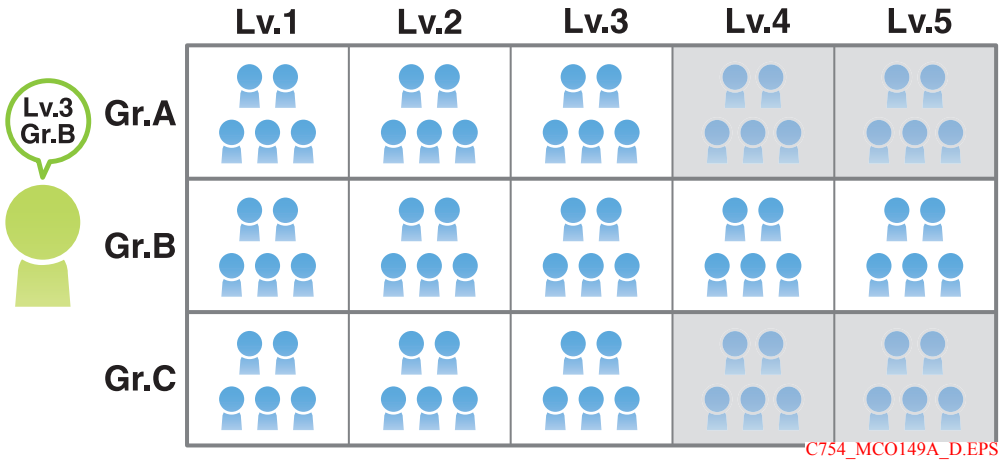
A combination of the reference allowed level and reference allowed group provides more flexible management.

For example, assume that Level 3 is set as a reference allowed level and Group B is set as a reference allowed group for a certain user.

In this case, destinations the user can access are as follows.

- Destinations of Reference Allowed Level 1 to 3: A1 to A3, B1 to B3, C1 to C3

- Destinations belonging to Reference Allowed Group B: B1 to B5



Tips

- You can specify the reference allowed level of each reference allowed group. If you assign a reference allowed group for which a reference allowed level is set to the address book, you can manage destinations by using both the reference allowed level and reference allowed group.

Simultaneously setting a reference allowed level and reference allowed group

Set both a reference allowed level and reference allowed group for a user.

To manage the address book by combining the reference allowed level and reference allowed group, register a reference allowed group for which a reference allowed level is set, and assign it to the address book.

1 In the administrator mode, select [Security] - [Address Reference Setting] - [Edit], then register a reference allowed group.

Settings	Description
[Reference Allowed Group Name]	Enter the name of the reference-allowed group (using up to 24 characters). Assign a name that helps you easily identify the registered group.
[Access Allowed Level]	To manage the address book by combining the reference allowed level and reference allowed group, select a reference allowed level of the reference allowed group.

2 In the administrator mode, select [Store Address] - [Address Book] - [Edit], then set a reference allowed group or reference allowed level for the address book.

➔ To manage the address book by combining the reference allowed level and reference allowed group, assign a reference allowed group for which a reference allowed level is set to the address book.

3 In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit], then set a reference allowed group and reference allowed level for the registered user.

➔ To specify a reference allowed group for a registered user means that you specify a reference allowed group itself. Therefore, even if a reference allowed level has been set for the selected reference allowed group, that setting of reference allowed level is not applied here.

12.15 Changing the function key display pattern by user or account

Overview

This machine provides three display patterns to display or hide function keys in each mode.

If user authentication or account track is installed on this machine, you can select a display pattern of function keys to be displayed in each mode screen for each user or account track.

For example, you can configure settings so that only basic functions are normally displayed on the screen and all functions are displayed on the screen when a specific user or account logs in to this machine. If you select a display pattern according to your environment, you can increase productivity when using this machine.

To select a function key display pattern for each user or account, follow the below procedure to configure the settings.

1 Allow changing the function key display pattern by user or account

➔ For details on configuring the setting, refer to page 12-33.

2 Selecting a function key display pattern by user or account

➔ To change the function key display pattern by user, refer to page 12-33.
➔ To change the function key display pattern by account, refer to page 12-34.

Allowing changing the function key display pattern by user or account

Configure setting to select a display pattern of the function keys to be displayed on the screen in each mode for each user or account track.

In the administrator mode, select [System Settings] - [Custom Function Profile User/Account], set [Custom Function Profile User/Account] to [Allow] (Default: [Restrict]).

Selecting a function key display pattern by user

In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit], then configure the following settings.

Settings	Description
[Copy/Print Screen]	To select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode, select [Allow]. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.
[Send/Save Screen]	To select a display pattern of function keys to be displayed on the send or save settings screen in Fax/Scan or User Box mode, select [Allow]. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.

Tips

- To check the functions available for each pattern setting, select, in the administrator mode, [System Settings] - [Custom Function Pattern Selection], then click [Details].
- A function key display pattern can be added to suit your requirements. For details, contact your service representative.

Selecting a function key display pattern by account

In the administrator mode, select [User Auth/Account Track] - [Account Track Settings] - [Edit], then configure the following settings.

Settings	Description
[Copy/Print Screen]	To select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode, select [Allow]. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.
[Send/Save Screen]	To select a display pattern of function keys to be displayed on the send or save settings screen in Fax/Scan or User Box mode, select [Allow]. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.

Tips

- To check the functions available for each pattern setting, select, in the administrator mode, [System Settings] - [Custom Function Pattern Selection], then click [Details].
- A function key display pattern can be added to suit your requirements. For details, contact your service representative.

12.16 Specifying the operations of the ID & Print function

The ID & Print function saves print data in the ID & Print User Box of this machine in an environment where user authentication is installed. Because the data is not printed soon, this function prevents printed materials from being missing or left unattended.

Specify the operations of the ID & Print function. Also, specify the action that this machine takes when it receives a print job from a public user or a print job without authentication information.

In the administrator mode, select [User Auth/Account Track] - [User Authentication Setting] - [Administrative Setting].

Settings	Description
[ID & Print]	Select whether to handle jobs normally printed from the printer driver as ID & Print jobs. • [ON]: Jobs that are normally printed are handled as ID & Print jobs. • [OFF]: Only jobs for which ID & Print is set are handled as print jobs. [OFF] is specified by default.
[Public User]	Select the process performed when a public user job or a job without user authentication information is received. • [Print Immediately]: Prints the job without saving it in the ID & Print User Box. • [Save]: Saves the job in the ID & Print User Box. [Print Immediately] is specified by default.
[ID & Print Operation Settings]	When using the **Authentication Unit** function on an optional authentication unit, select whether to request user authentication for printing each job or to allow the user to print all jobs once the user is authenticated. • [Print All Jobs]: One successful authentication session allows the user to print all jobs. • [Print Each Job]: One successful authentication session allows the user to print one job. [Print All Jobs] is specified by default.
[Default Operation Selection]	Select the default value for the operation that is performed after authentication in the login window. • [Print & Access Basic Screen]: Prints an ID & Print job without logging in to this machine if there is an ID & Print job. If there is no ID & Print job, log in to this machine. • [Access]: The user is logged in to this machine. The ID & Print job is not executed. [Print & Access Basic Screen] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

12.17 Configuring common settings when using the authentication function

Set how to manage color printing and the operation when logging out of this machine if user authentication or account track is installed on this machine.

In the administrator mode, select [User Auth/Account Track] - [User/Account Common Setting], then configure the following settings.

Settings	Description
[Single Color > 2 Color Output Management]	When necessary, select whether to handle single color and 2 colors as color print or white-and-black print. This option is required when color print is restricted or the maximum numbers of color copies and black and white copies are managed. When you treat single color or 2 color printing as black printing, you can manage only full color printing as color printing. [Color] is specified by default.
[Logout Confirmation Display Setting]	Select whether to display the logout confirmation screen on the **Touch Panel** when you log out of the login mode (Recipient User or Public User) during operation of this machine. [ON] is specified by default.

12.18 Restricting print jobs without authentication information

Select whether to allow print jobs without authentication information, which are jobs instructed without configuring the correct user authentication or account track settings using the printer driver.

In the administrator mode, select [User Auth/Account Track] - [Print without Authentication], then configure the following settings.

Settings	Description
[Print without Authentication]	Select whether to allow a print job without authentication information. • [Full Color/Black]: Allows both color and black and white printing. • [Black Only]: Allows black and white printing only. Color printing jobs are also printed in black and white. • [Restrict]: Restricts a print job without authentication information. [Restrict] is specified by default.
[IP Filtering (Permit Access)]	When you select [Full Color/Black] or [Black Only] in [Print without Authentication], select [Enable] to restrict computers so that printing is to be permitted using the IP address. Also enter the range of IP addresses. To allow access from a single IP address, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.

Tips

- If print jobs without authentication information are allowed, they are counted as public user jobs.

12.19 Printing without a password (Quick Authentication for Printing)

Overview

Configure settings so that authentication (without a password) based only on the user name is allowed when the printer driver is used for printing in an environment where user authentication is employed. This function is called the Quick Authentication for Printing function.

When using the Quick Authentication for Printing function, follow the below procedure to configure the settings.

1 Permit the Quick Authentication for Printing function

➔ For details on configuring the setting, refer to page 12-38.

2 Register information of the LDAP server for confirming the user name (quick authentication for printing server) in an environment where external server authentication is employed

➔ For details on configuring the setting, refer to page 12-38.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the LDAP server using SSL	page 12-39
Provide against shutdown of the quick authentication for printing server	page 12-40

Permit the Quick Authentication for Printing function

Allow the Quick Authentication for Printing function. By this, you can print data from the printer driver only based on user name authentication (without a password) in an environment where MFP authentication is employed.

In the administrator mode, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Simple Print Authentication Setting], and then set [Simple Print Authentication Setting] to [Allow] (Default: [Restrict]).

Registering the quick authentication for printing server

You must inquire the LDAP server about the user name to obtain permission to access this machine in an environment where external server authentication is employed. This LDAP server is called the quick authentication for printing server.

In the administrator mode, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Register Simple Print Authentication Server] - [Edit], then register information of the quick authentication for printing server.

Settings	Description
[Server Address]	Enter the LDAP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.
[Search Base]	Specify the starting point to search for a user to be authenticated (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.

Settings	Description
[General Settings]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. • [Simple] • [Digest-MD5] • [GSS-SPNEGO] • [NTLM v1] • [NTLM v2] [Simple] is specified by default.
[Login Name]	Log in to the LDAP server, and enter the login name to search for a user (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name to log in to the LDAP server (using up to 64 characters). If [GSS-SPNEGO] is selected for [General Settings], enter the domain name of Active Directory.
[Use Referral]	Select whether to use the referral function, if necessary. Make an appropriate choice to fit the LDAP server environment. [ON] is specified by default.
[Search Attribute]	Enter the search attribute to be used for search of user using the LDAP server (using up to 64 characters, including a symbol mark -). The attribute must start with an alphabet character. [uid] is specified by default.
[External Server Connection]	Select the external server name to be used as a part of user information when authentication using the quick authentication for printing server is successfully completed from the external servers registered on this machine. The external server selected here is used for the following purpose. • Using as a part of authentication information saved on this machine • Using for restricting the functions of this machine or managing the maximum allowance [No Selection] is specified by default.

Using SSL communication

Communication between this machine and the LDAP server is encrypted with SSL.

Configure the setting if your environment requires SSL encryption communication with the LDAP server.

In the administrator mode, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Register Simple Print Authentication Server] - [Edit], then configure the following settings.

Settings		Description
[Enable SSL]		Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.

Settings		Description
	[Expiration Date]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Setting a secondary authentication server against shutdown of the quick authentication for printing server

When you are using the quick authentication for printing server, you can set a secondary authentication server to prepare for a case in which the primary authentication server has shut down.

Setting a secondary authentication server automatically changes to the secondary authentication server even if the primary authentication server used for normal operations has shut down, thereby, enabling the quick authentication for printing to be continued.

1 In the administrator mode, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Secondary Authentication Server Settings], then configure the following settings.

Settings	Description
[Secondary Authentication Server Settings]	Select [ON] to use the secondary authentication server. [OFF] is specified by default.
[Reconnection Settings]	Specify the timing at which to reconnect to the primary authentication server. [Set Reconnect Interval] is specified by default. • [Reconnect for every login]: Connects to the primary authentication server each time authentication is carried out on this machine. If the primary authentication server is shutting down, this machine is connected to the secondary authentication server. • [Set Reconnect Interval]: Connects to the secondary authentication server when the primary authentication server is shutting down when machine authentication is occurring. After this, this machine is connected to the secondary authentication server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary authentication server when machine authentication is occurring.

2 In the administrator mode, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Register Secondary Authentication Server], then click [Edit] to configure the following settings.

Settings	Description
[Server Address]	Enter the LDAP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.

Settings	Description
[Search Base]	Specify the starting point to search for a user to be authenticated (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.
[General Settings]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. • [Simple] • [Digest-MD5] • [GSS-SPNEGO] • [NTLM v1] • [NTLM v2] [Simple] is specified by default.
[Login Name]	Log in to the LDAP server, and enter the login name to search for a user (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name to log in to the LDAP server (using up to 64 characters). If [GSS-SPNEGO] is selected for [General Settings], enter the domain name of Active Directory.
[Use Referral]	Select whether to use the referral function, if necessary. Make an appropriate choice to fit the LDAP server environment. [ON] is specified by default.
[Search Attribute]	Enter the search attribute to be used for search of user using the LDAP server (using up to 64 characters, including a symbol mark -). The attribute must start with an alphabet character. [uid] is specified by default.

3 If a communication with the LDAP server is encrypted using SSL, select [User Auth/Account Track] - [Simple Print Authentication Setting] - [Register Secondary Authentication Server] in the administrator mode, then click [Edit] to configure the following settings.

Settings		Description
[Enable SSL]		Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.

Settings		Description
	[Expiration Date]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Primary/Secondary Server Connection Status] - [Print Simple Auth.] in the administrator mode. If [Connection Allowed] is displayed, you can connect to both the primary and secondary authentication servers.

12.20 Using the authentication unit

12.20.1 Setting operations of the authentication unit

Authentication Unit (IC card type)

If you use the optional **Authentication Unit** (IC card type), you can log in to this machine or execute a print job by the authentication that uses an IC card or NFC-compatible Android terminal.

In the administrator mode, select [User Auth/Account Track] - [Authentication Device Settings], and then select how to log in to this machine (Default: [Card authentication]).

- [Card Authentication]: Logs in simply by placing your IC card or NFC-compatible Android terminal on the authentication unit.
- [Card Authentication + Password]: Logs in by placing the IC card or NFC-compatible Android terminal on the NFC area and entering the password.

Authentication Unit (biometric type)

If you use the optional **Authentication Unit** (biometric type), you can log in to this machine or execute a print job using the bio authentication function.

In the administrator mode, select [User Auth/Account Track] - [Authentication Device Settings], then set the operation of the bio authentication unit and how to log in to this machine.

Settings	Description
[Beep Sound]	Select whether to give a "blip" sound when the finger vein pattern is scanned successfully. [ON] is specified by default.
[Operation Settings]	Select how to log in to this machine. • [1-to-many authentication]: Simply place his or her finger to log in. • [1-to-1 authentication]: Enter the user name and place his or her finger to log in. Bio information is used instead of the password. [1-to-many authentication] is specified by default.

12.20.2 Authenticating in the LDAP server using the authentication card (LDAP-IC Card Authentication)

Overview

You can configure settings so that authentication is performed in the LDAP server using the card ID registered in the authentication card (LDAP-IC Card Authentication).

Authentication is completed only by placing the IC card. This enhances security without damaging users' ability to easily operate the machine.

To perform authentication using the authentication card, follow the below procedure to configure the settings.

1 Enabling use of **Authentication Unit** (IC card type) in this machine

➔ **Authentication Unit** (IC card type) must be configured by your service representative. For details, contact your service representative.

2 Configuring basic settings for the LDAP-IC card authentication

3 Set the following options according to your environment

Purpose	Reference
Communicate with the LDAP server using SSL	page 12-45
Provide against shutdown of the LDAP server	page 12-45

Configuring basic settings for the LDAP-IC card authentication

1 In the administrator mode, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [LDAP-IC Card Authentication Setting], set [LDAP-IC Card Authentication Setting] to [ON] (Default: [OFF]).

2 In the administrator mode, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Server Registration] - [Edit], then register information of the LDAP server to be used for authenticating the user ID of the IC card.

Settings	Description
[Server Address]	Enter the address of the LDAP server to be used for authenticating the user ID of the IC card. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.
[Search Base]	Specify the starting point to search for a user to be authenticated (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.
[General Settings]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. • [Simple] • [Digest-MD5] • [GSS-SPNEGO] • [NTLM v1] • [NTLM v2] [Simple] is specified by default.
[Login Name]	Log in to the LDAP server, and enter the login name to search for a user (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name to log in to the LDAP server (using up to 64 characters). If [GSS-SPNEGO] is selected for [General Settings], enter the domain name of Active Directory.
[Use Referral]	Select whether to use the referral function, if necessary. Make an appropriate choice to fit the LDAP server environment. [ON] is specified by default.
[Search Attribute]	Enter the attribute for the location where the IC card information is registered (using up to 63 characters, including a symbol mark -). The attribute must start with an alphabet character. [uid] is specified by default.
[User Name]	Select how to obtain the user name when logging in to this machine. • [Use Card ID]: Select this option when only IC card information is registered on the server. Uses the card ID in the IC card as the user name. • [Acquiring]: Select this option when user information other than IC card information is registered on the server. Uses the user name obtained from the server. Enter the attribute to be searched as the user name ("uid") at [User Name Attribute]. [Use Card ID] is specified by default.

Settings	Description
[External Server Connection]	Select the name of the external server to be used as authentication information saved on this machine. The authentication information is saved on this machine when the LDAP-IC card authentication is successfully completed. This authentication information includes the user name and the external server name. As authentication information to be saved on this machine, the name of external server registered on this machine can be registered. [No Selection] is specified by default.

Using SSL communication

Communication between this machine and the LDAP server is encrypted with SSL.

Configure the setting if your environment requires SSL encryption communication with the LDAP server.

In the administrator mode, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Server Registration] - [Edit], then configure the following settings.

Settings		Description
[Enable SSL]		Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Expiration Date]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Setting a secondary authentication server against shutdown of the LDAP server

When the LDAP server is installed, you can set a secondary authentication server to prepare for a case in which the primary authentication server has shut down.

Setting a secondary authentication server automatically changes to the secondary authentication server even if the primary authentication server used for normal operations has shut down, thereby, enabling the LDAP-IC authentication to be continued.

1 In the administrator mode, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Secondary Authentication Server Settings], then configure the following settings.

Settings	Description
[Secondary Authentication Server Settings]	Select [ON] to use the secondary authentication server. [OFF] is specified by default.

Settings	Description
[Reconnection Settings]	Specify the timing at which to reconnect to the primary authentication server. [Set Reconnect Interval] is specified by default. • [Reconnect for every login]: Connects to the primary authentication server each time authentication is carried out on this machine. If the primary authentication server is shutting down, this machine is connected to the secondary authentication server. • [Set Reconnect Interval]: Connects to the secondary authentication server when the primary authentication server is shutting down when machine authentication is occurring. After this, this machine is connected to the secondary authentication server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary authentication server when machine authentication is occurring.

2 In the administrator mode, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Register Secondary Authentication Server], then click [Edit] to configure the following settings.

Settings	Description
[Server Address]	Enter the LDAP server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number. In normal circumstances, you can use the original port number. [389] is specified by default.
[Search Base]	Specify the starting point to search for a user to be authenticated (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server. [60] sec. is specified by default.
[General Settings]	Select the authentication method to log in to the LDAP server. Select one appropriate for the authentication method used for your LDAP server. • [Simple] • [Digest-MD5] • [GSS-SPNEGO] • [NTLM v1] • [NTLM v2] [Simple] is specified by default.
[Login Name]	Log in to the LDAP server, and enter the login name to search for a user (using up to 64 characters).
[Password]	Enter the password of the user name you entered into [Login Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Domain Name]	Enter the domain name to log in to the LDAP server (using up to 64 characters). If [GSS-SPNEGO] is selected for [General Settings], enter the domain name of Active Directory.
[Use Referral]	Select whether to use the referral function, if necessary. Make an appropriate choice to fit the LDAP server environment. [ON] is specified by default.
[Search Attribute]	Enter the attribute for the location where the IC card information is registered (using up to 63 characters, including a symbol mark -). The attribute must start with an alphabet character. [uid] is specified by default.

Settings	Description
[User Name]	Select how to obtain the user name when logging in to this machine. • [Use Card ID]: Select this option when only IC card information is registered on the server. Uses the card ID in the IC card as the user name. • [Acquiring]: Select this option when user information other than IC card information is registered on the server. Uses the user name obtained from the server. Enter the attribute to be searched as the user name ("uid") at [User Name Attribute]. [Use Card ID] is specified by default.

3 If a communication with the LDAP server is encrypted using SSL, select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Register Secondary Authentication Server] in the administrator mode, then click [Edit] to configure the following settings.

Settings		Description
[Enable SSL]		Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
	[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [636] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Expiration Date]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Primary/Secondary Server Connection Status] - [LDAP-IC Card Authentication] in the administrator mode. If [Connection Allowed] is displayed, you can connect to both the primary and secondary authentication servers.

12.20.3 Recording the authentication card ID in counter information of this machine

You can configure settings so that the authentication card ID is recorded in counter information that collects the use status of this machine.

In the administrator mode, select [User Auth/Account Track] - [Authentication Card ID Number], set [Authentication Card ID Number] to [Notify] (Default: [Not Notify]).

12.21 Using the MFP authentication together against in the case where an enhanced server has shut down

To manage users who use this machine via the enhanced server such as **Authentication Manager**, you can use the MFP authentication together against in the case where an enhanced server has shut down

Using the enhanced server authentication and MFP authentication together, you can use the authentication information temporarily saved on the machine to log in and use the machine even if the enhanced server has shut down.

1 In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	To use enhanced server authentication and MFP authentication together, select [ON (MFP + External Server)].
[Overwrite User Info]	If [ON (MFP + External Server)] is selected in [User Authentication], [Allow] is set forcibly. When the enhanced server authentication is used, the authenticated user information is also managed on this machine. If the number of users who have executed the enhanced server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. In this case, registered user information is overwritten.
[Update Billing Information]	Select whether to overwrite existing billing information if the billing information that can be managed on this machine reached the upper limit when the enhanced server shut down. [Restrict] is specified by default.
[Default Authentication Method]	If you have selected [ON (MFP + External Server)] at [User Authentication], select the authentication method that you use normally. [ON (External Server)] is specified by default.
[Enhanced Counter]	If you have selected [ON (MFP + External Server)] at [User Authentication], assign a counter area to temporarily save information against in the case where an enhanced server has shut down. Up to 1000 counter areas can be specified combined with [User Counter]. The **Hard Disk** is optional in some areas. If the optional **Hard Disk** is not installed, up to 100 counter areas are assigned.
[Temporarily Save Authentication Information]	To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, select [Enable]. [Disable] is specified by default.
[Reconnection Settings]	If necessary, change the time to reconnect to the enhanced server. • [Reconnect for every login]: Connects to the enhanced server at the time authentication is carried out on this machine. If the enhanced server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the enhanced server is down, and use the temporarily saved authentication information to log in to this machine. • [Set Reconnect Interval]: Connects to the enhanced server at the time specified in [Reconnection Time], and check the status of the enhanced server. If the enhanced server is in the shutdown state, use the authentication information that is temporarily saved in the main unit to log in. [Set Reconnect Interval] is specified by default.
[Expiration Date Settings]	Select [Enable] to set the expiration date to the temporarily saved authentication information. If [Enable] is selected, enter the expiration date. [Disable] is specified by default.

2 In the administrator mode, select [User Auth/Account Track] - [Max. Allowance Setting when Enhanced Server down], then configure the following settings.

➔ [Max. Allowance Setting when Enhanced Server down] is displayed when [Temporarily Save Authentication Information] is set to [Enable] in Step 1.

Settings	Description
[Max. Allowance Setting when Enhanced Server down]	Specify whether to manage the maximum allowance for the number of printed sheets or the number of registered User Boxes on this machine when the enhanced server has shut down. [ON] is specified by default.
[Print(Total)] /[Print(Color)]/[Print(Black)]	To manage the maximum allowance for the number of printed sheets, select the [Print Limit] check box, then enter the maximum allowance.
[Personal User Box Allowance]	To manage the maximum allowance for the number of registered Personal User Boxes, select the [Personal User Box Limit] check box, then enter the maximum allowance.
[Billing Allowance]	To manage the maximum billing allowance, select the [Account Limit] check box, then enter the maximum allowance.

12.22 Setting a secondary authentication server against shutdown of an authentication server

When an external server is installed, you can set a secondary authentication server to prepare for a case in which the primary authentication server has shut down.

Setting a secondary authentication server automatically changes to the secondary authentication server even if the primary authentication server used for normal operations has shut down, thereby, enabling a user to continuously use this machine.

1 In the administrator mode, select [User Auth/Account Track] - [External Server Settings] - [Secondary Authentication Server Settings], then configure the following settings.

Settings	Description
[Secondary Authentication Server Settings]	Select [ON] to use the secondary authentication server. [OFF] is specified by default.
[Reconnection Settings]	Specify the timing at which to reconnect to the primary authentication server. [Set Reconnect Interval] is specified by default. • [Reconnect for every login]: Connects to the primary authentication server each time authentication is carried out on this machine. If the primary authentication server is shutting down, this machine is connected to the secondary authentication server. • [Set Reconnect Interval]: Connects to the secondary authentication server when the primary authentication server is shutting down when machine authentication is occurring. After this, this machine is connected to the secondary authentication server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary authentication server when machine authentication is occurring.

2 In the administrator mode, select [User Auth/Account Track]-[External Server Settings], then click [Secondary] of the server you want to set as the secondary authentication server.

➔ [Secondary] is displayed when [Secondary Authentication Server Settings] is set to [ON] in step 1.

➔ The external server set as the primary authentication server is set to [Primary].

➔ The same external server cannot be assigned to both the primary and secondary authentication servers.

Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Primary/Secondary Server Connection Status] - [External Server Authentication] in the administrator mode. If [Connection Allowed] is displayed, you can connect to both the primary and secondary authentication servers.

12.23 Using a mobile terminal for authentication purposes

12.23.1 Employing the NFC authentication

Overview

NFC is the standard for near-field communication that is used for connection between handheld terminals or other devices several tens of centimeters away each other.

If NFC authentication is employed when user authentication is installed on this machine, you can only place your NFC-compatible Android terminal on the mobile touch area on the **Control Panel** of this machine to log in to this machine.

✔ User authentication must be employed on this machine.

1 Installing the application on the Android terminal to configure settings for NFC authentication

➔ For details on configuring the setting, refer to page 12-51.

2 Configuring settings for NFC authentication on this machine

➔ For details on configuring the setting, refer to page 12-51.

Reference

For details on how to log in to this machine using NFC, refer to page 12-51.

Configuring settings for NFC authentication on an Android terminal

To perform user authentication on an Android terminal, prepare the following on the Android terminal.

- Enabling the wireless connection and NFC for Android terminal
- Install **Mobile for Android** on the Android terminal to enable the NFC terminal setting.
  - For details on the procedure, refer to the help of **Mobile for Android**.
- Registering this machine in **Mobile for Android**
  - For details on how to register, refer to page 16-26.
- Registering user authentication information in **Mobile for Android**
  - For details on the procedure, refer to the help of **Mobile for Android**.

Enabling the NFC authentication function on this machine

Set the NFC authentication function to Enable on this machine.

In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[Enable NFC]	Select [ON] to use the NFC. [OFF] is specified by default.
[NFC Authentication Setting]	Select [ON] to use the NFC authentication. [OFF] is specified by default.

Using NFC on an Android terminal to log in to this machine

This section describes how to log in to this machine by placing an Android terminal on the mobile touch area on the **Control Panel** of this machine.

1 Start the Android terminal.

2 Place the Android terminal on the mobile touch area on the **Control Panel** of this machine.

Authentication starts. If authentication succeeds, you can log in to this machine.

Tips

- For details on how to operate NFC authentication, refer to the help of **Mobile for Android**.

12.23.2 Employing Bluetooth LE authentication

Overview

The Bluetooth LE is the standard for power-saving near-field communication that is used for connection between handheld terminals or other devices several meters away each other.

If Bluetooth LE authentication is employed when user authentication is installed on this machine, you can only place your Bluetooth LE-compatible iOS terminal on the mobile touch area on the **Control Panel** of this machine to log in to this machine.

✔ User authentication must be employed on this machine.

✔ The optional **Local Interface Kit EK-609** is required to use this function. This setting must be configured in advance by your service representative. For details, contact your service representative.

1 Installing the application on an iOS terminal to configure settings for Bluetooth LE authentication

➔ For details on configuring the setting, refer to page 12-52.

2 Configuring settings for Bluetooth LE authentication on this machine

➔ For details on configuring the setting, refer to page 12-52.

Reference

For details on how to log in to this machine using Bluetooth LE, refer to page 12-52.

Configuring settings for Bluetooth LE authentication on an iOS terminal

To perform user authentication on an iOS terminal, prepare the following on the iOS terminal.

- Enabling the wireless connection and Bluetooth LE for iOS terminal
- Install **Mobile for iPhone/iPad** on the iOS terminal to enable the Bluetooth LE terminal setting.
  - For details on the procedure, refer to the help of **Mobile for iPhone/iPad**.
- Registering this machine in **Mobile for iPhone/iPad**
  - For details on how to register, refer to page 16-28.
- Registering user authentication information in **Mobile for iPhone/iPad**
  - For details on the procedure, refer to the help of **Mobile for iPhone/iPad**.

Enabling the Bluetooth LE authentication function on this machine

Set the Bluetooth LE authentication function to Enable on this machine.

In the administrator mode, select [User Auth/Account Track] - [General Settings], then configure the following settings.

Settings	Description
[Enable Bluetooth LE]	Select [ON] to use Bluetooth LE. [OFF] is specified by default.
[Bluetooth LE Authentication Setting]	Select [ON] to use Bluetooth LE authentication. [OFF] is specified by default.

Using Bluetooth LE on an iOS terminal to log in to this machine

This section describes how to log in to this machine by placing an iOS terminal on the mobile touch area on the **Control Panel** of this machine.

1 Start **Mobile for iPhone/iPad** on the iOS terminal.

2 Place the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

Authentication starts. If authentication succeeds, you can log in to this machine.

Tips

- For details on how to operate Bluetooth LE authentication, refer to the help of **Mobile for iPhone/iPad**.

13 Reinforcing Security

13 Reinforcing Security

13.1 Creating a certificate for this machine to communicate via SSL

Overview

Communication between this machine and the computer can be encrypted with SSL to enhance security.

A certificate for this machine is used for the SSL communication between the machine and the computer. As a certificate was registered on this machine upon shipment, you can only enable SSL/TLS on the machine to start the SSL encrypted communication immediately after setup.

This machine can manage multiple certificates and use different certificates depending on the application (protocol). You can self-create a new certificate or install a certificate issued by the Certificate Authority (CA).

The following shows how to use the certificate on this machine.

Usage	Description
Using the certificate registered upon shipment	The certificate that was registered on this machine upon shipment can be used as it is.
Using a self-created certificate	Create a certificate with this machine. The Certificate Authority (CA) is not required for a self-created certificate, and it can be used simply after entering necessary information for creating the certificate.
Using a certificate issued by the Certificate Authority (CA)	Create certificate signing request data in this machine, and request a trusted Certificate Authority (CA) for issuing a certificate for the machine. When the data is returned from the Certificate Authority after its review, register the data with this machine.

Reference

You can also use a certificate exported from other device by importing it on this machine. For details, refer to page 13-6.

For details on how to use different certificates depending on the application (protocol), refer to page 13-5.

Using the certificate registered upon shipment

Select a login mode to enable SSL communication. Also select the SSL encryption strength.

In the administrator mode, select [Security] - [PKI Settings] - [SSL Setting], then configure the following settings.

Settings	Description
[Mode using SSL/TLS]	Select a mode to perform SSL communication. • [Admin. Mode]: Uses SSL communication in the administrator mode only. • [Admin. Mode and User Mode]: Uses SSL communication in both the administrator mode and user mode. • [None]: Does not use SSL communication. [None] is specified by default.
[Encryption Strength]	Select the SSL encryption strength. Select it according to your environment. [AES-256, 3DES-168, RC4-128] is specified by default.
[SSL/TLS Version Setting]	Select the version of the SSL to be used. Select the file according to your environment.

Self-creating a certificate

Create a certificate with this machine. The Certificate Authority (CA) is not required for a self-created certificate, and it can be used simply after entering necessary information for creating the certificate.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Create and install a self-signed Certificate.], and enter information required for creating a certificate, then click [OK].

The certificate is created and installed on this machine. It may take several minutes to create a certificate.

Settings	Description
[Common Name]	Displays the IP address of this machine.
[Organization]	Enter an organization or association name (using up to 63 ASCII characters).
[Organizational Unit]	Enter the organization unit name (using up to 63 ASCII characters). You can also specify a null.
[Locality]	Enter the locality name (using up to 127 ASCII characters).
[State/Province]	Enter the state or province name (using up to 127 ASCII characters).
[Country]	Enter the country name. As the country name, specify a country code defined in ISO03166 (using up to two ASCII 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 of this machine (using up to 128 characters, excluding spaces). If the E-mail address of the administrator was already registered from [System Settings] - [Machine Setting] in the administrator mode, this field displays the registered E-mail address.
[Validity Start Date]	Displays the starting date of the certificate validity period. Displays the date and time of this machine when this screen is 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.

2 When the certificate has been installed, enable SSL communication.

➔ For details, refer to page 13-2.

Requesting the Certificate Authority for issuing a certificate

Create certificate signing request data in this machine, and request a trusted Certificate Authority (CA) for issuing a certificate for the machine. When the data is returned from the Certificate Authority after its review, register the data with this machine.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Request a Certificate], and enter information required for issuing a certificate, then click [OK].

The certificate signing request data to be sent to the Certificate Authority is created.

Settings	Description
[Common Name]	Displays the IP address of this machine.
[Organization]	Enter an organization or association name (using up to 63 ASCII characters).
[Organizational Unit]	Enter the organization unit name (using up to 63 ASCII characters). You can also specify a null.
[Locality]	Enter the locality name (using up to 127 ASCII characters).
[State/Province]	Enter the state or province name (using up to 127 ASCII characters).
[Country]	Enter the country name. As the country name, specify a country code defined in ISO03166 (using up to two ASCII 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

Settings	Description
[Admin. E-mail Address]	Enter the E-mail address of the administrator of this machine (using up to 128 characters, excluding spaces). If the E-mail address of the administrator was already registered from [System Settings] - [Machine Setting] in the administrator mode, this field displays the registered E-mail address.
[Encryption Key Type]	Select a type of encryption key.

2 Click [Save].

➔ Click this button to save certificate signing request data on your computer as a file.

3 Send the certificate signing request data to the Certificate Authority.

When the data is returned from the Certificate Authority after its review, register the data with this machine.

4 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Install a Certificate], and paste the text data sent from the Certificate Authority (CA), and then click [Install].

5 When the certificate has been installed, enable SSL communication.

➔ For details, refer to page 13-2.

13.2 Managing the certificates for this machine

13.2.1 Using Different Certificates Depending on the Application

This machine can manage multiple certificates and use different certificates depending on the application (protocol).

In the administrator mode, click [Security] - [PKI Settings] - [Protocol Setting] - [Create], then select a certificate to be used for the protocol.

Protocol	Application
[SSL]: [http Server]	If this machine is used as an http server, it encrypts transmission from a client to the machine. For example, it is used for the following application. • Accessing **Web Connection** via HTTPS • Printing via IPPS
[SSL]: [E-Mail Transmission (SMTP)]	If this machine is used as an SMTP client, it submits a certificate of the machine according to a request from the E-mail server (SMTP).
[SSL]: [E-mail RX (POP)]	If this machine is used as an POP client, it submits a certificate of the machine according to a request from the E-mail server (POP).
[SSL]: [TCP Socket]	If this machine is used as a TCP Socket client, it submits a certificate of the machine according to a request by the TCP Socket server.
[SSL]: [LDAP]	If this machine is used as an LDAP client, it submits a certificate of the machine according to a request by the LDAP server.
[SSL]: [WebDAV Client]	If this machine is used as a WebDAV client, it submits a certificate of the machine according to a request by the WebDAV server.
[SSL]: [OpenAPI]	If this machine is used as an OpenAPI server, it encrypts transmission from an OpenAPI client to the machine.
[SSL]: [Web Service]	If this machine is used as a Web service server, it encrypts transmission from a client to the machine. It is used when a computer running Windows Vista or later accesses the machine via HTTPS.
[IEEE802.1X]	If this machine is used as an IEEE802.1X authentication client, it is used for the following applications: • Encrypting communication if this machine is authenticated by the IEEE802.1X server via EAP-TLS. • Submitting a certificate of this machine upon request by the server via EAP-TTLS or EAP-PEAP.
[S/MIME]	When sending an S/MIME E-mail, it attaches a certificate of this machine to ensure the sender of the E-mail.
[SSL]: [IPsec]	Used to activate IPsec communication on this machine.
[SSL]: [Remote Panel]	When the control panel on this machine is operated remotely with the dedicated software, it is used for the following applications: • Submitting a certificate of this machine, in the client settings, according to a request by the server in which the dedicated software installed. • Encrypting communication, in the server settings, from a client viewing the control panel of this machine to the machine.
[SSL]: [ThinPrint]	If this machine is used as a ThinPrint client, it submits a certificate of the machine according to a request by the ThinPrint server (.print Engine). After this machine validates the certificate, the ThinPrint server performs encrypted communication. Specify the certificate of this machine to use for communication that is issued by the Certificate Authority (CA).

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.
- If the certificate to be used was registered, a "*" mark appears for the protocol.
- Clicking [Edit] changes the registered certificate or check details of the certificate.
- Clicking [Delete] deletes the registration information.

13.2.2 Exporting a certificate

A certificate for this machine can be exported. You can export the certificate if you wish to manage it on the computer or transfer it to other device.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Export Certificate], and enter a password (using up to 32 characters), and click [OK].

➔ The entered password is required for importing the certificate.

2 Click [Download].

The certificate for this machine is saved to the computer.

13.2.3 Importing a certificate

The exported certificate can be imported on this machine.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Import Certificate], then click [Browse] to specify the certificated to be imported.

2 Enter the password (using up to 32 characters), and click [OK].

➔ Enter the password specified when exporting the certificate.

The import result is displayed.

13.2.4 Deleting a certificate

A certificate for this machine can be deleted if necessary.

In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Remove a Certificate], then click [OK].

Tips

- The certificate specified as default cannot be deleted. Before deleting it, specify another certificate as default.

13.3 Configuring certificate verification settings

13.3.1 Verifying a certificate for peer

You can configure the settings for verifying reliability of the certificate (expiration date, CN, key usage, etc.).

To check the expiration of certificate, register the URL of the Online Certificate Status Protocol (OCSP) service.

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure the following settings.

Settings		Description
[Certificate Verification Settings]		Select [ON] to verify reliability of the certificate for peer. [ON] is specified by default.
[Timeout]		Change the time-out time of certificate expiration confirmation if necessary. [30] sec. is specified by default.
[OCSP Service]		Using the Online Certificate Status Protocol (OCSP) enables you to check online whether or not the certificate is expired. Select this check box to use the OCSP service. Enter the URL of the OCSP service (using up to 511 characters). If [URL] is left blank, the URL of the OCSP service embedded in the certificate will be used.
[Proxy Settings]		To confirm the expiration date via a proxy server, register the proxy server currently used.
	[Proxy Server Address]	Enter the address of the proxy server you are using. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
	[Proxy Server Port Number]	If necessary, change the proxy server port number. [8080] is specified by default.
	[User Name]	Enter the user name to log in to the proxy server (using up to 63 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 63 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Address not using Proxy Server]	If necessary, enter the address that does not use the proxy server. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"

13.3.2 Importing external certificates used for validating the chain

Types of external certificates that can be imported

Import external certificates used for validating the certificate chain (certificate path) in this machine.

The following certificates can be imported on this machine.

Type	Description
[Trusted CA Root Certificate]	You must import the certificate of the CA that issued the certificate in question on this machine in advance, if you wish to validate the chain of a submitted certificate.

Type	Description
[Trusted CA Intermediate Certificate]	You must import the certificate of the intermediate certificate authority on 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, on this machine in advance.
[Trusted EE (End Entity) Certificate]	"Trusted EE" refers to the certificate to be submitted. By importing a certificate on 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 on this machine.

How to import

Import external certificates used for validating the certificate chain (certificate path) in this machine.

1 In the administrator mode, select [Security] - [PKI Settings] - [External Certificate Setting], then click [New Registration].

➔ To change certificates to be shown in the list, select a certificate you wish to change, and click [Changes the display].

➔ To delete the registered certificate, click [Delete].

2 Click [Browse] to specify the certificate to be imported.

3 Click [OK].

The import result is displayed.

Tips

- The **Hard Disk** is optional in some areas. If the optional **Hard Disk** is not installed, only one external certificate can be imported.

13.4 Registering user's certificates automatically on this machine

Register a user's certificate used for encrypting E-mail message with S/MIME.

The following two methods are available for registering a user's certificate:

- Registering a user's certificate as destination registration information when the E-mail address is registered on this machine.
- Sending an E-mail attached with a digital signature (user's certificate) to this machine to register the certificate automatically in this machine using S/MIME function.

The following describes the method to send an E-mail attached with digital signature (user's certificate) to this machine for automatic registration.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

✔ Before registering the certificate, you must register on this machine the E-mail address of the user whose certificate you wish to register.

✔ This machine must be able to receive E-mail messages.

1 In the administrator mode, select [Network] - [E-mail Setting] - [S/MIME], then configure the following settings.

Settings		Description
[S/MIME Comm.Setting]		Select [ON] to use the S/MIME. To select [ON], the E-mail address of the certificate of this machine must match the E-mail address of the administrator. [OFF] is specified by default.
[Automatically Obtain Certificates]		To register digital signature (user's certificate), select [ON]. [OFF] is specified by default.
[Print S/MIME information]		Select whether to print the S/MIME information, if necessary. [OFF] is specified by default.
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

2 Send the E-mail attached with digital signature from the computer 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 on this machine.

13.5 Controlling the access to this machine by IP address

IPv4 address filtering

The computers' access to this machine can be controlled via IP address. This is called "IP address filtering."

You can specify both IPv4 addresses that are allowed to access this machine and those refused to access the machine.

In the administrator mode, select [Network] - [TCP/IP Setting] - [IPv4 Filtering], then configure the following settings.

Settings	Description
[Permit Access]	Select [Enable] to specify IPv4 addresses that allow access. Also enter the range of IPv4 addresses that allow access. To allow access from a single IPv4 address, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.
[Deny Access]	Select [Enable] to specify IPv4 addresses refused to access. Also enter the range of IPv4 addresses. To refuse access from a single IPv4 address, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.

IPv6 address filtering

The computers' access to this machine can be controlled via IP address. This is called "IP address filtering."

You can specify both IPv6 addresses that are allowed to access this machine and those refused to access the machine.

In the administrator mode, select [Network] - [TCP/IP Setting] - [IPv6 Filtering], then configure the following settings.

Settings	Description
[Permit Access]	Select [Enable] to specify IPv6 addresses that allow access. Also enter the range of IPv6 addresses that allow access. Prefix-specified format: ****:****:****:****:****:****:****:****/@ Available range for entering asterisk "*": Hexadecimal characters Available range for entering symbol "@": 3 to 128 [Disable] is specified by default.
[Deny Access]	Select [Enable] to specify IPv6 addresses refused to access. Also enter the range of IPv6 addresses. Prefix-specified format: ****:****:****:****:****:****:****:****/@ Available range for entering asterisk "*": Hexadecimal characters Available range for entering symbol "@": 3 to 128 [Disable] is specified by default.

13.6 Using IPsec communication

Configure the setting if your environment requires IPsec.

The IPsec technology prevents the falsification or leakage of data on the IP packet basis by using encryption technology. As IPsec encrypts data in the network layer, secure communication is ensured even if you use protocols in an upper layer or applications that do not support encryption.

1 In the administrator mode, select [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting], then click [OK].

2 Click [Edit] from [IKEv1] or [IKEv2] in [IPsec Setting], then configure the following settings.

Settings	Description
[Encryption Algorithm]	Select the encryption algorithm to create a common key used for communication.
[Authentication Algorithm]	Select the authentication algorithm to create a common key used for communication.
[Encryption Key Validity Period]	Specify the validity period of a common key to securely create a common key used to encrypt communications. When this period has expired, a new key is created. This can secure the communication.
[Diffie-Hellman Group]	Select the Diffie-Hellman group.
[Negotiation Mode]	Select the method to securely create a common key used to encrypt communications.

3 From [SA] in [IPsec Setting], click [Create] and register the Security Association (SA).

➔ Up to 10 groups can be registered for the SA.

Settings	Description
[Name]	Enter the SA name (using 1 to 10 characters, excluding ").
[Encapsulation Mode]	Select an IPsec operation mode.
[Security Protocol]	Select a security protocol.
[Key Exchange Method]	Select the key replacement method to securely create a common key used to encrypt communications.
[Tunnel End Point]	Enter the IP address of the peer's IPsec gateway. This is required when [Tunnel] is selected in [Encapsulation Mode].
[IKE Setting]	Configure IKE settings used for this SA. This is required when [IKEv1] or [IKEv2] is selected in [Key Exchange Method].

Settings		Description
	[Authentication Method]	Select an authentication method.
	[Local Authentication Method]	Select the authentication method of this machine when [IKEv2] is selected in [Key Exchange Method].
	[Peer Authentication Method]	Select the peer authentication method when [IKEv2] is selected in [Key Exchange Method].
	[ESP Encryption Algorithm]	If you select [ESP] for [Security Protocol], configure the ESP encryption algorithm.
	[ESP Authentication Algorithm]	If you select [ESP] for [Security Protocol], configure the ESP authentication algorithm.
	[AH Authentication Algorithm]	If you select [AH] for [Security Protocol], configure the AH authentication algorithm.
	[Perfect Forward-Secrecy]	Select this check box if you wish to increase the IKE strength. Selecting this check box increases the time spent for communication.
	[Diffie-Hellman Group(IKEv1)]/[Diffie-Hellman Group(IKEv2)]	Select the Diffie-Hellman group.
[Manual Key Settings]		When using a device that does not support automatic key exchange using IKE, configure each parameter manually. This is required when [Manual Key] is selected in [Key Exchange Method].
	[Encryption Algorithm]	Select the algorithm to be used for encryption.
	[Authentication Algorithm]	Select the algorithm to be used for authentication.
	[SA Index]	Specify the SA Security Parameter Index to be added to the IPsec header.
	[Common Key Encryption]	Specify the common key used for encryption. You can specify different common keys respectively for send and receive.
	[Common Key Authentication]	Specify the common key used for authentication. You can specify different common keys respectively for send and receive.

4 From [Peer] in [IPsec Setting], click [Create] and register peers of this machine.

➔ Up to 10 peers can be registered.

Settings	Description
[Name]	Enter the peer name (using 1 to 10 characters, excluding ").
[Set IP Address]	Specify the IP address of the peer.
[Pre-Shared Key Text]	Enter the Pre-Shared Key text to be shared with the peer. • [ASCII]: Enter the Pre-Shared Key text using ASCII characters (up to 128). • [HEX]: Enter the Pre-Shared Key text using hexadecimal characters (up to 256). Specify the same text as that for the peer.
[Key-ID String]	Enter the Key-ID to be specified for the Pre-Shared Key (using up to 128 characters).

5 From [Protocol Setting] in [IPsec Setting], click [Create] and specify the protocol used for IPsec communication.

➔ Up to 10 protocols can be specified.

Settings	Description
[Name]	Enter the protocol name (using 1 to 10 characters, excluding ").
[Protocol Identification Setting]	Select a protocol used for IPsec communication.
[Port Number]	If [TCP] or [UDP] has been selected in [Protocol Identification Setting], specify the port number used for IPsec communication.
[ICMP Message Type]	Select the ICMP message type when [ICMP] is selected in [Protocol Identification Setting]. • [Echo Request/Reply]: Specify an ICMP message for echo request or response. • [No Selection]: You do not specify the ICMP message type.
[ICMPv6 Message Type]	Select the ICMP message type when [ICMPv6] is selected in [Protocol Identification Setting]. • [Echo Request/Reply]: Specify an ICMP message for echo request or response. • [No Selection]: You do not specify the ICMP message type.

6 In the administrator mode, select [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec], then click [OK].

7 In [Enable IPsec], configure the following settings.

Settings	Description
[IPsec]	Select [ON] to use the IPsec.
[Dead Peer Detection]	If no response can be confirmed from the peer in a certain period, the SA with the peer is deleted. Select a time that elapses before sending survival confirmation information to the peer how has not responded.
[Cookies]	Select whether to enable the defense using Cookies against denial-of-service attacks.
[ICMP Pass]	Select whether to apply IPsec to the Internet Control Message Protocol (ICMP). Select [Enable] to allow the ICMP packets to pass without applying IPsec to the ICMP.
[ICMPv6 Pass]	Select whether to apply IPsec to the Internet Control Message Protocol for IPv6 (ICMPv6). Select [Enable] to allow the ICMPv6 packets to pass without applying IPsec to the ICMPv6.
[Default Action]	Select an action to be taken if no settings meet the [IPsec Policy] while IPsec communication is enabled. Select [Deny] to discard IP packets that do not meet the [IPsec Policy] settings.

Settings		Description
[Certificate Verification Level Settings]		To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

8 From [IPsec Policy] in [Enable IPsec], click [Create], then configure the following settings.

➔ IP packet conditions can be specified to pass or allow the IP packets that meet each of the conditions.

Settings	Description
[Name]	Enter the IPsec policy name (using 1 to 10 characters, excluding ").
[Peer]	Select a peer setting. Select the setting from those registered in [Peer] in [IPsec Setting].
[Protocol Setting]	Select a protocol. Select the setting from those registered in [Protocol Setting] in [IPsec Setting].
[IPsec Setting]	Select a peer setting. Select the setting from those registered in [SA] in [IPsec Setting].
[Communication Type]	Select a direction of IPsec communication.
[Action]	Select an action to be taken for the IP packets that met [Peer], [Protocol Setting], and [Communication Type]. • [Protected]: Protect the IP packets that met the conditions. • [Allow]: Do not protect the IP packets that met the conditions. • [Deny]: Discard the IP packets that met the conditions. • [Cancel]: Refuse the IP packets that met the conditions.

9 In the administrator mode, select [Network] - [TCP/IP Setting] - [IPsec] - [Communication Check], then check that a connection with a peer can be established normally by the specified setting.

➔ Enter the peer's IP address into [IP Address], then click [Check Connection].

13.7 Using the IEEE802.1X authentication

Configure the setting if your environment requires the IEEE802.1X authentication.

Using IEEE802.1X authentication enables you to only connect devices authorized by administrators to the LAN environment. Devices that are not authenticated will not be allowed to even join the network, and this ensures rigid security.

In the administrator mode, select [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting], then configure the following settings.

Settings	Description
[IEEE802.1X Authentication Setting]	Select [ON] to use IEEE802.1X authentication. [OFF] is specified by default.
[Supplicant Setting]	In IEEE802.1x authentication, this machine acts as a supplicant (client to be authenticated). Configure the settings required for authentication by the authentication server.

Settings		Description
	[User ID]	Enter a user ID (using up to 128 characters). This user ID is used for all EAP-Type options.
	[Password]	Enter a password with 128 characters. The password is used for all EAP-Type options other than [EAP-TLS]. To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[EAP-Type]	Select an EAP authentication method. • [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 select [OFF]. [OFF] is specified by default.
	[EAP-TTLS]	Configure the EAP-TTLS settings if [EAP-Type] is set to [EAP-TTLS] or [Depend on Server]. • [anonymous]: Enter the anonymous name used for EAP-TTLS authentication (using up to 128 characters). • [Inner Authentication Protocol]: Select an internal authentication protocol for EAP-TTLS.
	[Server ID]	To verify CN of the certificate, enter the server ID (using up to 64 characters).
	[Client Certificates]	Select whether to encrypt the authentication information using a certificate for this machine, if necessary. This setting can be configured if the following conditions are satisfied: • The certificate is registered on this machine • [EAP-TLS], [EAP-TTLS], [PEAP], or [Depend on Server] is selected from [EAP-Type].
	[Encryption Strength]	If [EAP-TLS], [EAP-TTLS], [PEAP], or [Depend on Server] is selected from [EAP-Type], select an encryption strength for encryption by TLS, if necessary. • [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.
	[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item. • [Validity Period]: Confirm whether the certificate is within the validity period. [Confirm] is specified by default. • [CN]: Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default. • [Chain]: Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Network Stop Time]	Specify the delay time between the start of an authentication process and the end of network communication, if necessary. If an authentication process does not succeed within the specified time, all network communication will stop. To specify the delay time, select the [Network Stop Time] check box, and enter the delay (sec.) in [Stop Time]. To restart the authentication process after network communication stopped, reboot this machine.

Tips

- In the administrator mode, select [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Trial] to confirm the current authentication status. The authentication process can be activated for the authentication server.
- This setting is not displayed on **Web Connection** when [Network I/F Configuration] is set to [Wireless Only]. In a wireless-only environment, if [WPA-EAP(AES)] or [WPA2-EAP(AES)] is selected in [Wireless Network Setting] - [Authentication/Encryption Algorithm], configure the supplicant settings in [Utility] on the **Control Panel**. For details, refer to "User's Guide[Descriptions of Functions/Utility Keys]/[Utility]".

13.8 Sending data to the authenticated share folder (Scan to Authorized Folder)

Scan to Authorized Folder

Authentication information of the users who have logged in to this machine is used for accessing a shared folder on the network, allowing them to send original data scanned on this machine. This function is called Scan to Authorized Folder.

Using the Scan to Authorized Folder function allows you to limit destinations for each user. The function also allows users to access the share folder using the authentication information generated when they logged on this machine. This enhances security without damaging users' ability to easily operate the machine.

To use the Scan to Authorized Folder function, the following settings are required on this machine.

Settings	Description
User Authentication	Enable user authentication.
SMB Send	Enable the SMB send function.
SMB Registration	Register the SMB destinations. • Addresses other than SMB cannot be used concurrently with Scan to Authorized Folder. If address book, group, and program data other than SMB are registered, delete all of them. • The [User ID] of the registered SMB address must be left blank.
Limit user's registration/change of address	Disable user's registration/change of address.
Limit Public User Function	When public users' accesses are allowed, disable the scan function for public users.
Delete LDAP server registration	If the LDAP server is not used, delete the registration information of the LDAP server from this machine.
[Scan to Authorized Folder Settings]	Limit the direct input of addresses. For details, refer to page 13-17.

The following restrictions are enabled when Scan to Authorized Folder is used:

- Addresses cannot be specified by direct input for scan transmission.
- Users cannot save files to User Boxes.
- Users cannot send files from User Boxes.
- Users cannot use annotation User Boxes.
- Users cannot select addresses from transmission log.
- Users cannot use the URL notification function.

Limiting the direct input of addresses

In the administrator mode, select [User Auth/Account Track] - [Scan to Authorized Folder Settings], and set [Scan to Authorized Folder Settings] to [ON] (Default: [OFF]).

13.9 Disabling user's operation of registration/change

This machine can disable the following user's operations:

- Registering/changing addresses
- Registering the biometric/IC card information
- Changing the sender address ("From" address) for E-mail transmissions
- Synchronizing user authentication and account track for each user
- Using the copy program and fax/scan program

In the administrator mode, select [Security] - [Restrict User Access], then configure the following settings.

Settings	Description
[Registering and Changing Addresses]	Select [Restrict] to disable registering and changing addresses by users. [Allow] is specified by default.
[Biometric/IC Card Information Registration]	Select [Restrict] to disable registering biometric/IC card information by users. To use this function, the optional **Authentication Unit** is required. [Restrict] is specified by default.
[Changing the "From" Address]	To disable changing the sender's address ("From" address) by user for E-mail transmissions, select [Admin. E-mail Address] or [Login User Address]. • [Admin. E-mail Address]: Set the administrator's E-mail address to "From" address. • [Login User Address]: When user authentication is installed, set the user's E-mail address to "From" address. If the user's E-mail address is not registered, Set the administrator's E-mail address to "From" address. [Allow] is specified by default.
[Synchronize User Authentication & Account Track By User]	Select [Restrict] to disable the user's synchronization setting between user authentication and account track. [Allow] is specified by default.
[Restrict Program Function Setting]	Select [Restrict] to prevent users from using the copy program or fax/scan program by users. [Allow] is specified by default.

13.10 Restricting user's Web browser setting operations

Specify whether to allow the user to perform the following setting operations on the Web browser.

- Home page
- Start Up Page
- Cookie
- Authentication information

To restrict user's setting operations, select [Security] - [Security Details] - [Browser Setting User Open] in the administrator mode, then select [Restrict] (default: [Restrict]).

Tips

- This function is available when the Web browser function is enabled.

13.11 Saving the operation log of the control panel

The operation log on the **Control Panel** for scanning or sending faxes can be saved as a send operation log.

The **Control Panel** of this machine can be used to save the log information of when and what keys are pressed. This helps to analyze a security issue if it occurs.

In the administrator mode, click [Security] - [TX Operation Log Setting], and select [Save] (Default: [Do Not Save]).

Tips

- To print the saved sending operation logs or save them in USB memory, select [Utility] - [Administrator Settings] - [System Settings] - [List/Counter] - [TX Operation Log Output] on the **Control Panel**.

13.12 Enhancing the security of this machine by simple operation

[Quick Security Setting] summarizes settings to enhance the security level of this machine.

If the quick IP filtering function is employed, the range of the IP addresses accessible to this machine is set automatically, enabling you to quickly specify access restrictions.

Furthermore, if the administrator password remains set to the default or password rules are not satisfied, the security warning screen is displayed on the **Control Panel**, prompting you to change to the administrator password that satisfies password rules.

In the administrator mode, select [Security] - [Quick Security Setting], then configure the following settings.

Settings	Description
[Quick IP Filtering]	Allows you to restrict the devices that can access this machine using the IP address (IPv4/IPv6). The range of IP addresses for which access is to be restricted is specified automatically. • [Synchronize IP Address]: In IPv4, this option only permits access for an IP address that has a different end from the end of the IP address set for this machine. In IPv6, this option only permits access for the IP address set for this machine, and the IP addresses of which the high-order 64 bits are the same. • [Synchronize Subnet Mask]: This option only permits access for the IP address set for this machine, and the IP addresses that belong to the same network using subnet masks or prefixes. • [No Filtering]: Does not use the filtering function. [No Filtering] is specified by default.
[Security Warning Display Setting]	Select whether to display the security warning screen if the administrator password remains set to the default or if password rules are not satisfied. [OFF] is specified by default.

Tips

- If the quick IP filtering function is used, the range of IP addresses for which access is to be restricted is specified automatically. To manually specify the range of IP addresses for which access is to be restricted, set [Network] - [TCP/IP Setting]-[IPv4 Filtering] or [IPv6 Filtering] instead of using [Quick IP Filtering].

14 Managing the Machine Status

14 Managing the Machine Status

14.1 Managing the machine power for power saving

14.1.1 Setting the Power key/Power save function

The usage of the **Power** key on the **Control Panel** and settings relevant to the power save function of this machine can be changed.

In the administrator mode, select [Maintenance] - [Timer Setting] - [Power Settings], then configure the following settings.

Settings	Description
[Low Power Mode Setting]	Change the time required to automatically change to the Low Power mode after you did not operate this machine. In the Low Power mode, the display of the **Touch Panel** is turned off to reduce power consumption. [15] min. is specified by default (allowable range: [2] to [60] min.).
[Sleep Mode Setting]	Change the time required to automatically change to the Sleep mode after you did not operate this machine. Sleep mode provides a greater power saving effect than the Low Power mode. However, the time required to return to the normal mode is longer than the time required to recover from the Low Power mode. [15] min. is specified by default (allowable range: [2] to [60] min.).
[Power Consumption in Sleep Mode]	Select whether to reduce the power consumption in the Sleep mode. • [High]: Further reduces the power consumption in the Sleep mode. However, this machine cannot be returned from the Sleep mode when the **Front Door** is opened or closed or when the original is loaded. • [Enabled]: Reduces the power consumption in the Sleep mode. • [Disabled]: Select this option when a smooth network communication is not established while [High] or [Enabled] is enabled. [High] is specified by default.
[Power Save Settings]	When using this machine in the factory default status, choose this setting to select the type of the power save mode when pressing the **Power** key on the **Control Panel**. • [Low Power]: Switches to the Low Power mode. Turns off the display of the **Touch Panel** to reduce power consumption. • [Sleep]: Switches to the Sleep mode. Sleep mode provides a greater power saving effect than the Low Power mode. However, the time required to return to the normal mode is longer than the time required to recover from the Low Power mode. [Low Power] is specified by default.
[Power Key Setting]	Select whether to use the **Power** key on the **Control Panel** as a sub power OFF key or as a power save key. • [Sub Power OFF]: Press the **Power** key briefly to turn the sub power off. If the Power key is held down, the power save mode is switched to the ErP Auto Power Off mode (similar to main power off mode), which provides a higher power saving effect than when the sub power is turned off. • [Power Save]: Press the **Power** key briefly to shift to the Power Save mode (Low Power or Sleep mode). Hold down the Power key to turn the sub power off. [Power Save] is specified by default.
[Enter Power Save Mode]	When this machine receives a print job from a fax machine or computer in the Power Save mode, select the timing to switch to the Power Save mode after the print job has ended. • [Normal]: Switches to the Power Save mode based on the time specified in [Low Power Mode Setting] or [Sleep Mode Setting]. • [Immediately]: Switches to the Power Save mode immediately after a print job has ended. [Immediately] is specified by default.

Settings	Description
[Power Saving Fax/Scan]	Select whether to give priority to the power saving when returning from the Sleep or sub power off mode to a mode other than the copy mode. When returning to a mode without printing such as the scan/fax mode, do not adjust the temperature of the **Fusing Unit** in this machine, reducing the power consumption. You can set this option when you have selected an option other than [Copy] in [Priority Mode] that is selected by [Administrator Settings] - [System Settings] - [Reset Settings] - [System Auto Reset] on the **Control Panel**. • [Power Save]: The temperature of **Fusing Unit** is not adjusted when the machine returns to the normal mode. • [Standard]: The temperature of **Fusing Unit** is adjusted when the machine returns to the normal mode. [Standard] is specified by default.

Reference

*For details on the **Power** key and Power Save functions, refer to "User's Guide[Control Panel]/[Managing the Power Supply of this Machine]".*

14.1.2 Switching to Power Save mode at specified time (Weekly Timer)

You can use the weekly timer for automatic switching between normal and power save modes. Using the weekly timer function enables you to save power efficiently according to your operating environment.

The following two methods are available to configure the weekly timer schedule.

- Setting the switching schedule manually
- Using the tracking function to automatically set On or Off time according to the operating status of this machine

In the administrator mode, select [Maintenance] - [Timer Setting] - [Weekly Timer Setting], then configure the following settings.

Settings		Description
[Use Weekly Timer]		Select this check box to use the weekly timer function. Also specify the power save mode to be switched by the weekly timer, and the weekly timer schedule. The weekly timer schedule can be used with [Date Setting] and [Work Time Setting]. If the [Enable Tracking Function] check box is selected, the schedule automatically set by the tracking function is specified by default for [Date Setting] and [Work Time Setting]. More flexible operation is possible by changing the automatically set schedule as required. [ON] (selected) is specified by default.
	[Power Save Mode Setting]	Select a power save mode to which the machine enters based on the weekly timer. • [ErP Auto Power OFF]: A mode that provides a higher more effective power saving effect. In this mode, you cannot receive all jobs. • [Sleep]: This mode has a lower power saving effect than the [ErP Auto Power OFF] mode; however, it allows you to receive print jobs from a fax machine or computer. The received jobs are printed when the machine returns to the normal mode. [ErP Auto Power OFF] is specified by default.
	[Date Setting]	Specify the date by day.
	[Work Time Setting]	Specify the operating time for each day of the week. Select the check box for a day of the week you wish to set the timer, and enter the time period that power is turned on.
[Use Power Save]		Select this check box if you wish to turn the power off when the machine is not used during lunch break. Also enter the range of time during which the power is turned off. [OFF] (not selected) is specified by default.

Settings	Description
[Use Overtime Password]	Select this check box to restrict the use of this machine in the Power Save mode using a password. Also enter the password (using up to eight characters, excluding + and "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password. [OFF] (not selected) is specified by default.
[Enable Tracking Function]	Select this check box to use the tracking function that automatically sets the weekly timer schedule to fit your office use status. To use the tracking function, select [Auto Standby Adjustment Level] to specify the level at which it is judged that this machine is inactive. As the level is higher, it is more easily judged that this machine is inactive. Therefore, the off time is set to a longer time. Select the [Clear Usage Data] check box to delete data of the use status learned in this machine and the schedule that is set automatically as the learning result. [ON] (selected) is specified by default.

14.1.3 Returning the machine from the Power Save mode via the wireless network

Configure the setting to return the machine from the ErP Auto Power Off mode via the wireless network when the machine is connected to an Android/iOS terminal.

Tips

- The optional **Wireless LAN Interface Kit** is required to use this function.
- To use an Android/iOS terminal, you need to install **Remote Access** on the terminal.
- This function is not available when the machine is used in the IPv6 environment.
- To return the machine from the ErP Auto Power Off mode using an Android/iOS terminal, connect this machine to the Android/iOS terminal once in advance.

Reference

For details on the ErP Auto Power OFF mode, refer to "User's Guide[Control Panel]/[Managing the Power Supply of this Machine]".

For details on the settings for using this machine in the wireless network environment, refer to page 5-5.

In the administrator mode, select [Network] - [Wireless Network Setting] - [Awake from ErP], then configure the following settings.

Settings	Description
[Awake from ErP]	Select the method to return the machine from the ErP Auto Power Off mode. • [Awake with Magic Packet]: The machine returns from the ErP Auto Power Off mode when receiving a magic packet. • [Awake with ARP + Unicast Communication]: The machine returns from the ErP Auto Power Off mode when receiving a unicast communication packet. [Awake with Magic Packet] is specified by default.

14.2 Configuring the daylight saving time settings

Enable the daylight saving time function on this machine. You can also set the daylight saving time to be automatically enabled on this machine at the specified date.

In the administrator mode, select [Maintenance] - [Daylight Saving Time], then configure the following settings.

Settings	Description
[Daylight Saving Time]	Select [ON] to use the daylight saving time. Also enter the time to be adjusted for the daylight saving time (in minutes). [OFF] is specified by default.
[Specify Method]	Select the method to specify the date and time to start the daylight saving time and the date and time to end it. • [Weekly]: Specify the start date and end date by week and day of the week. • [Day]: Specify the start date and the end date by date.
[Start Date/Time]/[End Date/Time]	Respectively select the date and time to start the daylight saving time and the date and time to end it.

14.3 Customizing the Control Panel environment

14.3.1 Changing a Function to be Assigned to a Register Key

You can select functions to be assigned to the hardkeys on the **Control Panel** and softkeys on the slide menu to suit your requirements.

In the administrator mode, click [System Settings] - [Registered Key Settings], then select a function to be assigned to each **Register** key.

The following default functions are assigned to the hardkeys on the **Control Panel**.

- [Register Key 1]: [Enlarge Display]
- [Register Key 2]: [Guidance]
- [Register Key 3]: [10 Keypad]
- [Register Key 4]: [Preview]

The following default functions are assigned to the softkeys on the slide menu.

- [Register Key 1]: [Copy]
- [Register Key 2]: [Scan/Fax]
- [Register Key 3]: [Box]
- [Register Key 4]: [Interrupt]
- [Register Key 5]: [OFF]

Tips

- If the OpenAPI application is registered on this machine, the registered application or registered application list can be assigned to a **Register** key. For details on the registered application list, refer to page 16-24.

14.3.2 Selecting functions to be arranged in the main menu

Press the **Menu** key on the **Control Panel** to display the main menu. In the main menu, shortcut keys can be arranged to which you have assigned desired functions.

The main menu can be expanded to triple-screen, and you can freely select up to 25 shortcut keys according to your operating environment.

1 In the administrator mode, select [System Settings] - [Main Menu Default Settings] to select [Assignment No.] for the main menu key arranging shortcut keys, then click [Edit].

➔ [Assignment No.] 1 to 11 are assigned to the first screen of the main menu. These keys should be assigned to frequently used functions.

2 Select a function to be assigned to a shortcut key.

Settings	Description
[Function Name]	Select a category of function to be assigned to a shortcut key. • [Function]: Create a shortcut key to the main screen such as Copy mode or Fax/Scan mode. • [Copy Function Settings]: Create a shortcut key to the setting screen for copy function. • [Scan/Fax Function Settings]: Create a shortcut key to the setting screen for fax/scan function. • [System User Box]: Create a shortcut key to the System User Box. • [Copy Program]: Create a shortcut key to a copy program. This option is available when copy programs are registered on this machine. • [Scan/Fax Program]: Create a shortcut key to a fax/scan program. This option is available when fax/scan programs are registered on this machine. • [Registered Application]: Create a shortcut key to the registration application. • [Registered Application Group]: Create a shortcut key to the registered application group. • [QR Code Setting]: Create a shortcut key to the QR code display screen. • [Widget Placement]: Create a shortcut key to the widget setting screen. • [Eco Function Settings]: Create a shortcut key to the Eco-related function. • [Not Set]: Do not create any shortcut key.

Settings	Description
[Shortcut Key]	Select a function to be assigned to a shortcut key corresponding to the category selected in [Function Name].
[Scan/Fax Program Shortcut Key]	Select a program to be displayed from the list when a shortcut key to a scan/fax program is created.
[Specify Icon]	Select an icon to be displayed on the main menu, if necessary, when a shortcut key is created for a copy program or fax/scan program.

Tips

- If the OpenAPI application is registered on this machine, you can arrange keys for the registered applications or registered application groups in the main menu. For details, contact your service representative.

14.3.3 Changing the theme of the main menu

The background color, etc. of the main menu can be changed according to your preference.

In the administrator mode, select [System Settings] - [Main Menu Display Settings], and select your favorite theme. (Default: [Theme 1])

Reference

For details on the theme of the main menu, refer to "User's Guide[Control Panel]/[Operations of Touch Panel and Explanation of Major Screens]".

14.3.4 Selecting Function Keys to Be Displayed on the Main Screen (Using a Display Pattern)

This machine provides three display patterns to display or hide function keys in each mode.

The display pattern can be changed to any of the above three types depending on function key usage conditions.

In the administrator mode, select [System Settings] - [Custom Function Pattern Selection], then configure the following settings.

Settings	Description
[Copy/Print Screen Pattern]	Select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.
[Send/Save Screen Pattern]	Select a display pattern of function keys to be displayed on the send or save settings screen in Fax/Scan or User Box mode. • [Full]: Displays all function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. [Full] is specified by default.

Tips

- Click [Details] to check the functions that can be used in each display pattern.

14.3.5 Selecting function keys to be displayed on the main screen (Individual specification)

Overview

You can change the type or layout of function keys to be displayed in the main screen in each mode.

You can arrange the frequently used function keys in the main screen or hide unused function keys depending on function key usage conditions.

To change function keys to be displayed on the screen in each mode, take the following procedure to configure the settings.

1 Allow the change of functions keys in each mode

➔ For details on configuring the setting, refer to page 14-9.

2 Change function keys to be displayed on the screen in each mode.

➔ For details on how to change the function keys to be displayed on the main screen in the copy mode and the print settings screen in the User Box mode, refer to page 14-9.

➔ For details on how to change the function keys to be displayed on the main screen in the fax/scan mode and the send or save setting screen in the User Box mode, refer to page 14-9.

➔ For details on how to change the function key to be displayed in the main screen in fax mode, refer to page 14-9.

Allowing the change of functions keys in each mode

Allow a change of function keys to be displayed on the main screen in each mode.

In the administrator mode, select [System Settings] - [Function Display Key Permission Setting], then set [Copy/Print] or [Send/Save] to [Allow].

Settings	Description
[Copy/Print]	Select whether or not to allow a change of function keys to be displayed on the main screen in the copy mode and the print settings screen in the User Box mode. [Restrict] is specified by default.
[Send/Save]	Select whether or not to allow a change of function keys to be displayed on the main screen in the fax/scan mode and the send or save settings screen in the User Box mode. [Restrict] is specified by default.

Changing function keys in copy mode

Select the function keys to be displayed on the main screen in the copy mode and the print settings screen in the User Box mode. You can register up to 14 function keys.

1 In the administrator mode, select [System Settings] - [Function Display Key] - [Copy/Print] to select the number of the function key for which you wish to change the setting, then click [Edit].

➔ Keys No.1 to No.7 are assigned to basic function 1, and No.8 to No.14 are to basic function 2. It is recommended that you assign frequently-used functions to No.1 to No.7.

2 Select a function to be assigned to a shortcut key.

➔ Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

Changing function keys in Fax/Scan mode

Select the function key to be displayed on the main screen in the fax/scan mode and the send or save settings screen in the User Box mode. You can register up to 7 function keys.

1 In the administrator mode, select [System Settings] - [Function Display Key] - [Send/Save] to select the number of the function key for which you wish to change the setting, then click [Edit].

2 Select a function to be assigned to a shortcut key.

➔ Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

Changing function keys in fax mode

Select the function key to be displayed in the main screen in fax mode. You can register up to 7 function keys.

1 In the administrator mode, select [System Settings] - [Function Display Key] - [Fax TX] to select the number of the function key for which you wish to change the setting, then click [Edit].

2 Select a function to be assigned to a shortcut key.

➔ Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

14.3.6 Allowing the change of display language on the Touch Panel

Display the [Language] key on the **Touch Panel** to allow temporary change of the display language on the **Touch Panel** of this machine.

In the administrator mode, select [System Settings] - [Temporarily Change Language], and set [Temporarily Change Language] to [ON] (Default: [OFF]).

14.3.7 Changing the Keypad display when entering number of sets

Select whether to always display the **Keypad** on the screen where you can enter the number of copies on the **Touch Panel** or display it when you tap the number of copies.

In the administrator mode, select [System Settings] - [Display 10 Keypad when entering Number of Sets], then specify [Always] or [When Number of Sets is pressed] (default: [When Number of Sets is pressed]).

Settings	Description
[Always]	Always displays the **Keypad** on the screen where you can enter the number of copies.
[When Number of Sets is pressed]	Tapping [No. of Sets] displays the **Keypad**.

14.3.8 Registering shortcut keys for setting items of [Administrator Settings]

Register shortcut keys for setting items of [Administrator Settings] on the **Control Panel**.

The registered shortcut keys are displayed in [Utility] - [Administrator Shortcut Settings] on the **Control Panel**. You can register up to 16 shortcut keys.

1 In the administrator mode, select [System Settings] - [Administrator My Panel] to select [Assignment No.] for registering shortcut keys, then click [Edit].

2 Select setting items to be assigned to shortcut keys.

Settings	Description
[Function Name]	Select a category of setting items of [Administrator Settings] that are to be assigned to shortcut keys.
[Shortcut Key]	Select setting items to be assigned to shortcut keys in the category selected in [Function Name].

14.3.9 Configuring settings to display the slide menu

You can change the contents to be displayed on the slide menu to suit your environment.

In the administrator mode, select [System Settings] - [Slide Menu Settings], then configure the following settings.

Settings	Description
[Slide Menu Settings]	Select whether to use the slide menu. [ON] is specified by default.
[Soft Numeric Keypad]	Select whether to display the keypad on the slide menu. [Not Specify] is specified by default.
[Settings in Enlarge Display mode]	Select whether to also enlarge the slide menu when displaying it in the Enlarge Display mode. [Enlarge] is specified by default.
[Slide Menu Theme]	Select the background color of the slide menu. [Theme 1] is specified by default.

14.3.10 Placing Widgets on the Touch Panel

You can place texts, icons, GIF animation, or other items as widgets at the desired positions on the main menu or the copy-mode screen. By arranging widgets on frequently used screens, important information can be highlighted.

In the administrator mode, select [System Settings] - [Widget Function Settings], and set [Widget Function Settings] to [Enable] (Default: [Enable]).

14.4 Notifying of the machine status via E-mail

Overview

If a warning such as paper addition, toner replacement, or paper jam occurs on this machine, it can be sent to a registered E-mail address.

To send the machine status via E-mail, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the environment to use the Scan to E-mail function

➔ For details on configuring the setting, refer to page 7-2.

➔ In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and set [E-mail Notification] to [ON].

3 Configure the machine status notification settings

➔ For details on configuring the setting, refer to page 14-11.

Configuring the machine status notification settings

Register destination E-mail addresses. Up to 10 destination E-mail addresses can be registered. Also select warnings to send a notification when any of them occurs.

In the administrator mode, select [Maintenance] - [Status Notification Setting] - [E-mail Address] - [Edit], then configure the following settings.

Settings	Description
[Notification Address]	Enter the E-mail address of the destination with 320 characters, excluding spaces.
[Replenish Paper Tray]	Select this check box to send a notification when paper on tray runs out.
[JAM]	Select this check box to send a notification when paper jam occurs.
[PM Call]	Select this check box to send a notification when periodic inspection is required.
[Replace Staples]	Select this check box to send a notification when staples run out.
[Replenish Toner]	Select this check box to send a notification when toner runs out.
[Finisher Tray Full]	Select this check box to send a notification when the finisher tray is full.
[Service Call]	Select this check box to send a notification when a service call occurs.
[Job Finished]	Select this check box to send a notification when a job is completed.
[Hole-Punch Scrap Box Full]	Select this check box to send a notification when hole-punch scrap must be removed.
[Waste Toner Box Full]	Select this check box to send a notification when the waste toner box must be replaced.
[IU Life Stop]	Select this check box to send a notification when this machine has stopped because it was time to replace the imaging unit.
[Drum Unit Life]	Select this check box to send a notification when the drum unit must be replaced.
[Developing Unit Life]	Select this check box to send a notification when the developing unit must be replaced.
[Fusing Unit Yield]	Select this check box to send a notification when the finishing unit must be replaced.
[Transfer Roller Yield]	Select this check box to send a notification when the transfer roller unit must be replaced.
[Transfer Belt Unit Yield]	Select this check box to send a notification when the transfer belt unit must be replaced.

14.5 Notifying of the machine counter via E-mail

Overview

The counter information managed by this machine can be sent to the registered E-mail address. The information is useful for seeing the picture of the machine operating status.

To send the counter information via E-mail, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the Scan to E-mail environment

➔ For details on configuring the setting, refer to page 7-2.

➔ In the administrator mode, select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and set [Total Counter Notification] to [ON].

3 Configure the counter notification settings

➔ For details on configuring the setting, refer to page 14-12.

Configuring the counter notification settings

Register destination E-mail addresses. Up to three destination E-mail addresses can be registered. Also set the notification schedule.

In the administrator mode, select [Maintenance] - [Total Counter Notification Setting], then configure the following settings.

Settings	Description
[Model Name]	Enter a model name to be included in the notification mail message (using up to 20 characters). Assign a name that helps you easily identify the device.
[Schedule Setting]	Specify the notification schedule by day, week, or month. Up to two schedules can be registered. You can use different schedules for different purposes.
[Register Notification Address]	Enter the E-mail address of the destination with 320 characters, excluding spaces. Select the notification schedule for each destination. Also select whether to send eco-related information.

Tips

- If [Send notice after setting complete] is set to [ON], a test notification is sent to the registered mail addresses when you click [OK].

14.6 Managing the machine via SNMP

Overview

If you manage network devices using Simple Network Management Protocol (SNMP), you can acquire the information of this machine and monitor it via the network. This machine support the TCP/IP and IPX environments.

Using SNMP TRAP function enables you to notify the specified IP address or IPX address of a warning occurred on this machine.

To manage this machine via SNMP, follow the below procedure to configure the settings.

1 Configure the settings for using this machine in a TCP/IP or an IPX environment.

➔ To use it in a TCP/IP environment, refer to page 2-2.

➔ To use it in an IPX environment, refer to page 5-11.

2 Configure the settings for using SNMP

➔ For details on configuring the setting, refer to page 14-13.

Configuring the settings for using SNMP

Enable SNMP. Also specify whether to use the authentication setting or TRAP function of SNMP.

1 In the administrator mode, select [Network] - [SNMP Setting], then configure the following settings.

Settings		Description
[SNMP]		To enable SNMP, select [ON] and select the check box of SNMP version you use. Select [SNMP v1(IPX)] when you use SNMP in an IPX environment.
[UDP Port Setting]		If necessary, change the UDP port number. In normal circumstances, you can use the original port number.
[SNMP v1/v2c Setting]		When you use SNMP v1/v2c, configure the settings relevant to SNMP v1/v2c.
	[Read Community Name]	Enter a read-only community name (using between 1 to 15 characters, excluding spaces, \, ', ", and #).
	[Write Community Name]	Select this check box to allow read and write. Also enter a community name used for reading and writing (using between 1 to 15 characters, excluding spaces, \, ', ", and #).
[SNMP v3 Setting]		When you use SNMP v3, configure the settings relevant to SNMP v3.

Settings		Description
	[Context Name]	Enter the context name (using up to 63 characters, excluding spaces, \, ', ", and #).
	[Discovery User Name]	Select this check box if you allow a user for detection. Enter a user name for detection (using between 1 to 32 characters, excluding spaces, \, ', ", and #).
	[Read User Name]	Enter a read-only user name (using up to 32 characters, excluding spaces, \, ', ", and #).
	[Security Level]	Select a security level for the read-only user.
	[auth-password]	If [auth-password] or [auth-password/priv-password] is selected from [Security Level], enter an authentication password for the read-only user (using between 8 to 32 characters, excluding spaces, \, ', ", and #). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[priv-password]	If [auth-password/priv-password] is selected from [Security Level], enter a password used for privacy (encryption) of the read-only user (using between 8 to 32 characters, excluding spaces, \, ', ", and #). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Write User Name]	Enter a user name used of the read and write user (using up to 32 characters, excluding spaces, \, ', ", and #).
	[Security Level]	Select a security level of the read and write user.
	[auth-password]	If [auth-password] or [auth-password/priv-password] is selected from [Security Level], enter an authentication password for the read and write user (using between 8 to 32 characters, excluding spaces, \, ', ", and #). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[priv-password]	If [auth-password/priv-password] is selected from [Security Level], enter a password used for privacy (encryption) of the read and write user (using between 8 to 32 characters, excluding spaces, \, ', ", and #). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[Encryption Algorithm]		Select an encryption algorithm.
[Authentication Method]		Select an authentication method.
[TRAP Setting]		Set TRAP function to notify of the machine status using the SNMP TRAP function.
	[Allow Setting]	Select [Allow] to use the SNMP TRAP function.
	[Trap Setting when Authentication Fails]	Select whether to send TRAP when authentication fails.
[Administrator Information]		If necessary, enter the information of this machine.
	[Device Name]	Enter the name of this machine (MIB sysName) (using up to 255 characters).
	[Device Location]	Enter the location where to install this machine (MIB sysLocation) (using up to 255 characters).
	[Administrator Name]	Enter the administrator name (MIB sysContact) (using up to 255 characters).

2 To notify of the machine status using SNMP TRAP function, select in the administrator mode [Maintenance] - [Status Notification Setting] - [IP Address] or [IPX Address] - [Edit], then configure the following settings.

Settings	Description
[Notification Address]	Specify the address to be notified of the machine status. • If [IP Address] is used as the destination, enter the IP address (IPv4), IP address (IPv6), or host name (using up to 253 characters). • If the destination is an [IPX Address], enter the address by an 8-digit hexadecimal number.
[Port Number]	If the destination is an [IP Address], change the port number if necessary. In normal circumstances, you can use the original port number.
[Node Address]	If the destination is an [IPX Address], enter the node address by an 12-digit hexadecimal number.
[Community Name]	Enter the community name (using up to 15 characters).
[Replenish Paper Tray]	Select this check box to send a notification when paper on tray runs out.
[JAM]	Select this check box to send a notification when paper jam occurs.
[PM Call]	Select this check box to send a notification when periodic inspection is required.
[Replace Staples]	Select this check box to send a notification when staples run out.
[Replenish Toner]	Select this check box to send a notification when toner runs out.
[Finisher Tray Full]	Select this check box to send a notification when the finisher tray is full.
[Service Call]	Select this check box to send a notification when a service call occurs.
[Job Finished]	Select this check box to send a notification when a job is completed.
[Hole-Punch Scrap Box Full]	Select this check box to send a notification when hole-punch scrap must be removed.
[Waste Toner Box Full]	Select this check box to send a notification when the waste toner box must be replaced.
[IU Life Stop]	Select this check box to send a notification when this machine has stopped because it was time to replace the imaging unit.
[Drum Unit Life]	Select this check box to send a notification when the drum unit must be replaced.
[Developing Unit Life]	Select this check box to send a notification when the developing unit must be replaced.
[Fusing Unit Yield]	Select this check box to send a notification when the finishing unit must be replaced.
[Transfer Roller Yield]	Select this check box to send a notification when the transfer roller unit must be replaced.
[Transfer Belt Unit Yield]	Select this check box to send a notification when the transfer belt unit must be replaced.

14.7 Checking the printer information

14.7.1 Checking the counter of this machine

You can check the information of various types of counters such as the total counter and counters for respective functions.

In the administrator mode, select [Maintenance] - [Meter Count] to check the information of various counters of this machine.

14.7.2 Checking the ROM version

Check the ROM version of this machine.

To check the information of ROM version of this machine, select in the administrator mode [Maintenance] - [ROM Version].

14.8 Managing the setting information

14.8.1 Writing the setting information to this machine (Import)

Types of information that can be imported

Various types of setting information, which are saved (exported) from this machine to the computer, can be written (imported) to this machine. You can migrate setting information that is exported from other device of the same model to exchange the device.

The following information can be imported on this machine.

Item	Description
[Device Setting]	Various settings of this machine.
[Authentication Information]	Authentication information to be managed by this machine. To import the authentication information, enter the password that was specified for export.
[Select Group]	The information of addresses registered on this machine. To import the address information, enter the password that was specified for export.
[Copy Protect/Stamp]	The registration information of copy protect or stamp.
[Restriction Code List]	This is a list of restriction codes for the OpenAPI connection application.

How to import

1 In the administrator mode, select [Maintenance] - [Import/Export] to select the information to be imported, then click [Import].

2 Specify the location of the file to be imported, and click [OK].

➔ To import the [Authentication Information] or [Address], enter the password that was specified for export.

➔ When importing [Address], if you select [Updates containing only Registration number, leave the original data of the address and Registration Number.], address information, in a file to be imported, containing only a registration number, is not registered in the machine. If you select [Updates containing only Registration number, delete the original data of the address and Registration Number.], address information containing only a registration number is deleted from the machine.

The import process starts.

Tips

- The counter information cannot be imported.
- For details on the list of inhibited codes, contact your service representative.

14.8.2 Saving the setting information of this machine (Export)

Types of information that can be exported

Various types of setting information of this machine can be saved (exported) to the computer. Use this function to back up various types of setting information of this machine.

The following information can be exported from this machine.

Item	Description
[Device Setting]	Various settings of this machine.
[Counter]	Information of various types of counters on this machine. Select counter information to be exported from counters for respective users or accounts, and others.

Item	Description
[Authentication Information]	Authentication information to be managed by this machine. Select whether to export all authentication information or only user registration information. If necessary, the authentication information file to be exported can be encrypted using password.
[Address]	The information of addresses registered on this machine. Select information to be exported from all address information, address book, group, program, and E-mail subject/body. If necessary, the address information file to be exported can be encrypted using password.
[Copy Protect/Stamp]	The registration information of copy protect or stamp.
[Restriction Code List]	The restriction codes list of our depreciated the OpenAPI connection application.

How to export the information

1 In the administrator mode, select [Maintenance] - [Import/Export] to select the information to be exported, then click [Export].

2 Specify a location to save the exported file.

➔ When exporting the [Authentication Information] or [Address], enter the password if necessary.

The file is saved on the computer.

Tips

- When an E-mail address with a registered certificate is exported, the certificate is not exported. Register the certificate again after importing the address on this machine.
- For details on the list of inhibited codes, contact your service representative.

14.8.3 Resetting the network settings

The network settings of this machine can be reset to the factory default status.

In the administrator mode, select [Maintenance] - [Reset] - [Network Setting Clear], then click [Clear].

14.8.4 Restarting the network interface

Reset the controller of this machine and restart the network interface.

In the administrator mode, select [Maintenance] - [Reset] - [Reset], then click [Reset].

14.8.5 Deleting all address information

All of the address information registered on this machine can be deleted.

In the administrator mode, select [Maintenance] - [Reset] - [Format All Destination], then click [Format].

14.9 Outputting job logs

Operations required to use Closed Network RX

You can download logs of the jobs executed on this machine. You can check usage, paper usage, operations and job history for each user or account in the job log.

For details on viewing the output job logs, contact your service representative.

On the **Control Panel**, tap [Utility] - [Administrator Settings] - [Security Settings] - [Security Details] - [Job Log Settings], and configure the following setting.

Settings	Description
[Yes]/[No]	To output job logs, select [Yes]. [No] is specified by default.
[Obtain Log Type]	Select whether to obtain job logs for each type. • [Accounting Log]: Enables you to obtain information relevant to paper consumption for each user or account. [On] is specified by default. • [Counting Log]: Enables you to obtain information about paper consumption and the reduction rate of paper used for printing. [On] is specified by default. • [Audit Log]: Enables you to obtain user operation or job history. Your can track unauthorized actions or the leakage of information. [On] is specified by default.
[Overwrite]	Select whether to allow the oldest job log to be overwritten by a new job log when the hard disk space becomes full. [Allow] is specified by default.
[Erase Job Log]	Select this to delete job logs saved on this machine.

Downloading job logs

1 In the administrator mode, select [Maintenance] - [Job Log] - [Create Job Log], then click [OK].

➔ If any job logs have not been obtained, download them before creating new job log data. The job logs that have not been obtained are deleted when the new job log data is created.

This starts creating job log data.

2 In the administrator mode, select [Maintenance] - [Job Log] - [Download Job Log], then click [OK].

3 Click [Download].

This starts downloading the job log.

14.10 Setting the operating environment for this machine

14.10.1 Configuring default settings for Normal Display and Enlarge Display collectively

Select whether to arrange a single setting key for [Default Copy Settings] and [Default Enlarge Display Settings], or [Default Scan/Fax Settings] and [Default Enlarge Display Settings].

If you wish to change the settings in Normal Display and Enlarge Display at the same time, select in the administrator mode [System Settings] - [Reset Settings], and then set [Default Basic/Enlarge Display Common Setting] to [Apply to all] (Default: [Do not Apply]).

14.10.2 Setting the action for switching the display to Enlarge Display

The default display mode of the **Touch Panel** can be set to Enlarge Display mode. You can also set the action to be taken when the display mode is switched to Enlarge Display.

In the administrator mode, select [System Settings] - [Enlarge Display Settings], then configure the following settings.

Settings	Description
[Default Enlarge Display Setting]	Select whether to use Enlarge Display mode as the initial display of the **Touch Panel**. [OFF] is specified by default.
[Enlarge Display Setting]	If you have set [Default Enlarge Display Setting] to [ON], select whether to enable Enlarge Display mode when the **Reset** key is pressed. If you wish to enable Enlarge Display mode when the **Reset** key is pressed, select [Enlarge]. [Normal] is specified by default.
[Apply Basic Setting to Enlarge Display]	Select whether to inherit the settings configured on the normal screen display when switching the screen from Normal to Enlarge Display. • [Mode 1]: Inherit all normal mode settings. • [Mode 2]: In Copy mode, only inherit Normal mode settings that can be set in Enlarge Display mode. In Fax/Scan mode, reset the settings. [Mode 2] is specified by default.

14.10.3 Configuring the default method to display destinations

Configure the default method to display destinations in the scan/fax mode or fax mode.

In the administrator mode, select [System Settings] - [Default Address Display Settings] - [Scan/Fax Settings] or [Fax Settings], and configure the following settings.

Settings	Description
[Default Address Sort Method]	Select the list order of destinations by registration number and registration name. If you select the registration name, destinations are sorted according to [Name] specified for the destinations. [Registered No.] is specified by default.
[Default Address Display Method]	Select the button or list type to display destinations. [One-Touch Button Layout] is specified by default.

14.10.4 Changing the default scan data file name

Change the default file name of scanned original data when saving it.

The file name is:"initial of the function" + "text to be added" + "date" + "sequential number" + "page number" + "file extension".

In the administrator mode, select [System Settings] - [Scan File Name Settings], then configure the following settings.

Settings	Description
[Function Mode Initial]	Select whether to use an initial of the relevant function as a prefix for the file name. The following letters are used as a prefix for the file name. C: Copy S: Scan/Fax or User Box P: Print [Attach] is specified by default.
[Supplementary File Name]	Select whether to add a device name or desired text to the file name. • [Device Name]: Use the name of this machine for the file name. The name of this machine can be changed from, in the administrator mode, [System Settings] - [Machine Setting] - [Device Name]. • [Arbitrary Characters]: Use any desired text for the file name. Enter a text to be added to the [Arbitrary Characters] (using up to 10 characters). [Device Name] is specified by default.

14.10.5 Configuring settings to display the preview function

Specify whether to display the original being scanned in realtime. Also, configure the initial display of the preview screen.

In the administrator mode, select [System Settings] - [Preview Settings], then configure the following settings.

Settings	Description
[Real time preview]	Select whether to display a preview image for each page while scanning the original. [OFF] is specified by default.
[Set key Initial display]	Select whether to display the Setting Key when the preview screen opens. [ON] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

14.10.6 Printing a stamp on blank pages

Print date/time or stamp on blank pages inserted by the cover seat or inter sheet function.

In the administrator mode, select [System Settings] - [Blank Page Print Settings], and set [Print Setting] to [Print] (Default: [Do Not Print]).

Tips

- This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

14.10.7 Setting the skip job conditions

When a job being output is stopped by a warning such as shortage of paper, overloaded output tray, or unmatched paper, the subsequent job can be executed. This is called "Skip Job."

Whether to skip the current job can be selected for each case where the subsequent job is a fax job or it is other than a fax job.

In the administrator mode, select [System Settings] - [Job Priority Operation Settings], then configure the following settings.

Settings	Description
[Fax RX Job Priority]	Select whether to give priority to the printing of a fax if it is received during copying or printing. [OFF] is specified by default.
[Skip Job (Fax)]	Select whether to handle the subsequent job as long as it is a printing job for the received fax when printing has stopped because, for example, there is no paper. [ON] is specified by default.
[Skip Job (Copy, Print)]	Select whether to handle the subsequent job as long as it is not a printing job for the received fax when printing has stopped because, for example, there is no paper. [ON] is specified by default.

14.10.8 Setting the processing accuracy of outline PDF

When you save data in the Outline PDF format, the text is extracted from the original and converted into a vector image. The following explains how to set the outline processing accuracy of images (figures).

In the administrator mode, select [System Settings] - [Outline PDF Setting], then configure the following settings.

Settings	Description
[Graphic Outlining]	Select the outline processing accuracy of images (graphics) when saving data in the Outline PDF format. The outline processing accuracy is improved in the order of [LOW], [MIDDLE], and [HIGH]. If you select [OFF], outline processing is not performed. [OFF] is specified by default.

14.10.9 Allowing transmission of the machine usage frequency or function settings information

Information relevant to usage frequency of this machine and the machine function settings can be transmitted to our company. The information about this machine will be used by us for the improvement of service and functions in future.

Tips

- Information about IP address and others related to security as well as private information such as address books will not be transmitted.

In the administrator mode, select [System Settings] - [List/Counter], and set [Meter Count and Device Confirmation Tx Settings] to [Allow]. (Default: [Restrict])

14.10.10 Allowing acquisition of machine usage information

Select whether to allow us to acquire log data pertaining to the machine usage.

If log acquisition is allowed, the logging process starts immediately, which makes it useful if you need to analyze the cause of a problem that may occur later on this machine or to improve the product quality.

The screen to confirm whether to allow log acquisition is displayed when:

- The administrator password has been changed by selecting [Security] - [Administrator Password Setting] in the administrator mode;
- Registration information has been edited by selecting [System Settings] - [Machine Setting] in the administrator mode; or
- The user has logged in to the administrator mode while the number of copies exceeded 100.

Settings	Description
[Allow]	Tap this button to start log acquisition. Once this option is selected, the screen will no longer be displayed.
[Restrict]	Tap this button to not acquire log data. Once this option is selected, the screen will no longer be displayed.
[Confirm Later]	Tap this button to display the screen again the next time the conditions are satisfied.

14.11 Using an advanced function by registering the license

14.11.1 Issuing the request code

To use an advanced function by registering the optional license kit with this machine, you must access the License Management Server (LMS) to obtain the function and license codes. The following explains how to issue the request code required for requesting LMS for function and license codes.

In the administrator mode, select [Maintenance] - [License Settings] - [Get Request Code], then click [OK].

Tips

- To use this function, the optional **Extension Memory** is required.

14.11.2 Enabling the advanced function

Enabling the function using the function and license codes

Register the function and license code, which were obtained from the Licence Management Server (LMS), with this machine and enable the advanced function.

In the administrator mode, select [Maintenance] - [License Settings] - [Install License], and enter the function and license codes, then click [OK].

Tips

- To use this function, the optional **Extension Memory** is required.

Enabling the function using the token number

Automatically perform a procedure from a step to register a license in this machine via the Licence Management Server (LMS) on the Internet to a step to enable an advanced function on this machine.

This machine must be able to connect with the Internet because you must enter a token number included in the token certificate and obtain information required for enabling the advanced function from LMS.

In the administrator mode, select [Maintenance] - [License Settings] - [Install License], and enter the token number, then click [OK].

Tips

- To use this function, the optional **Extension Memory** is required.

14.12 Updating the firmware of this machine

Overview

You can externally download firmware and configuration information of this machine to update them.

You can keep using the machine even while downloading firmware or configuration information.

To externally download firmware and configuration information of this machine and update them, follow the procedure shown below.

✔ The firmware and configuration information must be updated by your service representative. For details, contact your service representative.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

1 Prepare for downloading a firmware

➔ You can download it either via FTP or HTTP. Configure the proxy server setting according to your operating environment.

➔ For details on how to configure a setting for downloading firmware via FTP, refer to page 14-25.

➔ For details on how to configure a setting for downloading firmware via HTTP, refer to page 14-25.

2 Update the firmware of this machine

➔ To update the firmware automatically by specifying the time, refer to page 14-26.

➔ To update the firmware manually, refer to page 14-26.

Preparing to download firmware via FTP

Configure the setting to download firmware to this machine via FTP.

In the administrator mode, select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [FTP Server Setting], then configure the following settings.

Settings	Description
[FTP Server Setting]	Select [ON] to connect with the Internet via a proxy. [OFF] is specified by default.
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [21] is specified by default.

Preparing to download firmware via HTTP

Configure the setting to download firmware to this machine via HTTP.

In the administrator mode, select [Network] - [Machine Update Settings] - [HTTP Proxy Settings], then configure the following settings.

Settings	Description
[HTTP Proxy Settings]	Select [ON] to establish an external connection via a proxy server. [OFF] is specified by default.
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [80] is specified by default.

Settings	Description
[Proxy Authentication]	Select whether to use Proxy Authentication. [OFF] is specified by default. • [User Name]: Enter the login name used for proxy authentication (using up to 32 characters). • [Password]: Enter the password of the user name you entered into [User Name] (using up to 32 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

Updating the firmware automatically at the specified time

This machine can download a firmware automatically at the specified time and update the firmware.

In the administrator mode, select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [Update Firmware at Specified Time], then configure the following settings.

Settings	Description
[Update Firmware at Specified Time]	Select [Enable] to enable this machine to automatically update the firmware at the specified time. [Disable] is specified by default.
[Firmware Update Start Time]	Enter the time when this machine should update the firmware automatically.

Updating the firmware manually

Externally download firmware to this machine and update the firmware manually.

You can keep using the machine as usual while downloading a firmware.

However, you cannot use this machine while updating the machine firmware. When the firmware updating process has been completed, this machine reboots automatically.

In the administrator mode, select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [Firmware Update Parameters], then configure the following settings.

Settings	Description
[Firmware Download Status]	Displays the status of downloading a firmware. Clicking [Refresh] refreshes the status.
[Firmware Download]	Click this button to download firmware externally.
[Delete Firmware]	Click this button to delete the downloaded firmware.
[Firmware Update Parameters]	Click this button to update the firmware of this machine using the firmware downloaded.

14.13 Automatically updating firmware of this machine or other devices

14.13.1 Configuring settings to update firmware of this machine

This machine can automatically update its firmware and configuration information.

In this step, configure settings so that this machine monitors the firmware update server on the network at periodic intervals to automatically download and update the latest firmware and configuration information.

1 In the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Auto Update Settings for This Machine], then configure the following settings.

Settings		Description
[Auto Update Settings for This Machine]		Select [ON] to automatically update firmware of this machine. [OFF] is specified by default.
[Download Protocol]		Select a protocol used to obtain firmware from the firmware update server. [SMB] is specified by default.
[SMB Setting]		Configure settings to obtain firmware using the SMB protocol.
	[Host Name]	Enter the IP address of the firmware update server (using up to 255 characters) or the host name (using up to 253 characters, including -, ., and _). To enter the host name, select the [Please check to enter host name.] check box.
	[File Path]	Enter the path of the shared folder that contains firmware (using up to 255 characters).
	[User Name]	Enter the user name to connect to the firmware update server (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Number of Retries]	Specify the number of retries to be executed when a connection with the firmware update server has failed. [3] is specified by default.
[HTTP Settings]		Configure settings to obtain firmware using the HTTP protocol (WebDAV).
	[URL]	Enter the URL of the firmware storage location on the firmware update server (using up to 253 characters, excluding spaces).
	[User Name]	Enter the user name to connect to the firmware update server (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Proxy]	Select [ON] to connect to the firmware update server via a proxy server.
	[Connection Timeout]	Specify the timeout period for a connection with the firmware update server. [60] sec. is specified by default.
[Update Time]		Specify the time to start applying the firmware obtained from the firmware update server to this machine. It is advantageous to specify the time when this machine is not operating such as a break time or night time.
[Polling Interval]		Specify the interval to check whether the latest firmware exists on the firmware update server. [60] minutes is specified by default.
[Retry Interval]		Specify the interval to retry processing when the system failed to check the latest firmware on the firmware update server. [5] minutes is specified by default.

2 To automatically update configuration information of this machine, in the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Machine Update Password], then enter the password to decode the encrypted configuration file (using up to 32 characters).

➔ To enter (change) the decryption passphrase, select the [Change Machine Update Password] check box, then enter a new decryption passphrase.

3 If necessary, in the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Log TX Settings], then configure a setting to send firmware update logs.

Settings		Description
[Update File Download/Update Log]		Select [ON] to send firmware update logs of this machine to a different location. [OFF] is specified by default.
[TX Protocol]		Select a protocol to send log data. [SMB] is specified by default.
[SMB Setting]		Configure settings to send log data using the SMB protocol.
	[Host Name]	Enter the host name of the log sending destination (using up to 253 characters, including -, ., and _).
	[File Path]	Enter the path of the shared folder of the log sending destination (using up to 255 characters).
	[User Name]	Enter the user name to log in to the log sending destination (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[WebDAV Settings]		Configure settings to send log data using the HTTP protocol (WebDAV).
	[URL]	Enter the URL of the log sending destination (using up to 253 characters, excluding spaces).
	[User Name]	Enter the user name to log in to the log sending destination (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Proxy]	Select [ON] to connect to the log sending destination via a proxy server. [OFF] is specified by default.

4 If necessary, in the administrator mode, select [Network] - [Machine Update Settings] - [HTTP Proxy Settings], then configure the proxy settings.

Settings	Description
[HTTP Proxy Settings]	Select [ON] to establish an external connection via a proxy server. [OFF] is specified by default.
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [80] is specified by default.
[Proxy Authentication]	Select whether to use Proxy Authentication. • [User Name]: Enter the login name used for proxy authentication (using up to 32 characters). • [Password]: Enter the password of the user name you entered into [User Name] (using up to 32 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

14.13.2 Configuring settings to update firmware of other devices

Configure settings to operate this machine as a relay server.

Operating this machine as a relay server allows you to establish a relay between a different firmware update server on the network and other devices to distribute firmware to them.

If this machine monitors a different firmware update server on the network at periodic intervals and checks that the server contains the latest firmware, firmware is downloaded to the firmware storage area of this machine.

Other devices on the network monitor this machine, which is running as a relay server, at periodic intervals. If the latest firmware exists in the firmware storage area of this machine, firmware is downloaded and updated based on the settings of that device.

In this example, configure settings required when this machine monitors a different firmware update server as well as settings required when other devices access the firmware storage area of this machine.

1 In the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Relay Server Function Settings], then configure the following settings.

Settings		Description
[Update File Download Settings]		Select [ON] to use this machine as a relay server. [OFF] is specified by default.
	[URL]	Enter the URL of the firmware storage location on the firmware update server (using up to 253 characters, excluding spaces).
	[User Name]	Enter the user name to connect this machine to the firmware update server (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Proxy]	Select [ON] to connect this machine to the firmware update server via a proxy server. [OFF] is specified by default.
	[Connection Timeout]	Specify the timeout period for a connection with the firmware update server. [60] sec. is specified by default.
	[Polling Interval]	Specify the interval to check whether the firmware update server contains the latest firmware. [60] minutes is specified by default.
	[Retry Interval]	Specify the number of retries to be executed when the system failed to check that the latest firmware was loaded on the firmware update server. [5] minutes is specified by default.
[HTTP Settings]		If you select [ON], other devices on the network can access the firmware storage area of this machine using the HTTP protocol (WebDAV).
	[User Name]	Enter the user name to connect to the firmware update server (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[SMB Setting]		If you select [ON], other devices on the network can access the firmware storage area of this machine using the SMB protocol. [OFF] is specified by default.

Settings		Description
	[User Name]	Enter the user name to connect to the firmware update server (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Update Log Save Folder]	Select [ON] to save firmware update log data in a shared folder. [OFF] is specified by default.

2 If necessary, in the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Log TX Settings], then configure a setting to send firmware update logs.

Settings		Description
[Relay Update File Download Log]		Select [ON] to send log data, which is obtained when this machine is running as a relay server, to a different location. [OFF] is specified by default.
[TX Protocol]		Select a protocol to send log data. [SMB] is specified by default.
[SMB Setting]		Configure settings to send log data using the SMB protocol.
	[Host Name]	Enter the host name of the log sending destination (using up to 253 characters, including -, ., and _).
	[File Path]	Enter the path of the shared folder of the log sending destination (using up to 255 characters).
	[User Name]	Enter the user name to log in to the log sending destination (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
[WebDAV Settings]		Configure settings to send log data using the HTTP protocol (WebDAV).
	[URL]	Enter the URL of the log sending destination (using up to 253 characters, excluding spaces).
	[User Name]	Enter the user name to log in to the log sending destination (using up to 64 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Proxy]	Select [ON] to connect to the log sending destination via a proxy server. [OFF] is specified by default.

3 If necessary, in the administrator mode, select [Network] - [Machine Update Settings] - [HTTP Proxy Settings], then configure the proxy settings.

Settings	Description
[HTTP Proxy Settings]	Select [ON] to establish an external connection via a proxy server. [OFF] is specified by default.
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [80] is specified by default.

Settings	Description
[Proxy Authentication]	Select whether to use Proxy Authentication. • [User Name]: Enter the login name used for proxy authentication (using up to 32 characters). • [Password]: Enter the password of the user name you entered into [User Name] (using up to 32 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

14.14 Returning the updated firmware to the previous version

Return the firmware of this machine to the previous version.

In the administrator mode, select [Network] - [Machine Update Settings] - [Firmware Rollback], then click [Rollback]. Clicking [Rollback] applies the firmware displayed in [Backup File Version] to this machine.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

14.15 Checking whether settings are updated

If settings are changed via **Web Connection** when a job is running, it notifies the administrator that a setting change will not be immediately updated.

In the administrator mode, select [Maintenance] - [Confirm update settings for Held Jobs.] to check whether settings are updated.

14.16 Enabling functions that require the authentication by an external institution

Some functions that require the authentication by an external institution are disabled at product shipment. After authentication has been obtained, enter the target function code to enable the function.

In the administrator mode, select [Maintenance] - [Certification function management setting.] - [Enable Function], and enter the function code, then click [OK].

Tips

- For details on the functions that require the authentication by an external institution and function codes, contact your service representative.
- Select [Maintenance] - [Certification function management setting.] - [Certification function list Display.]; you can check the functions that are enabled on this machine.

15 Registering Various Types of Information

15 Registering Various Types of Information

15.1 Registering address books

15.1.1 Registering E-mail Address

E-mail addresses can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

When using S/MIME function, you can register a user certificate an the E-mail address.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [E-mail], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[E-mail Address]	Enter the E-mail address of the destination with 320 characters, excluding spaces.
[Registration of Certification Information]	To encrypt E-mail messages using S/MIME, select this check box and register a user's certificate. Click [Browse], and specify the location of the certificate to be registered. • To register the certificate, the E-mail address must be matched between the certificate and the destination to be registered. • Only the DER (Distinguished Encoding Rules) format is supported as a file of certificate information. The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.1.2 Registering an FTP Destination

An FTP destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [FTP], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.

Settings	Description
[Host Address]	Enter the host name or IP address of the destination FTP server (using up to 253 characters). • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[File Path]	Enter the name of a destination folder in the FTP server specified in [Host Address] (using up to 127 bytes). • Entry example: "scan" When specifying a folder in the FTP folder, insert a symbol, "/", between the folder names. • Entry example: "scan/document" When not specifying a file path, enter only "/". • Entry example: "/"
[User ID]	If authentication is required in the destination FTP server, enter the available user name to log in (using up to 64 characters).
[Password]	Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding ").
[anonymous]	When authentication is not required in the destination FTP server, select [ON]. [OFF] is specified by default.
[PASV Mode]	When the PASV mode is used in your environment, select [ON]. [OFF] is specified by default.
[Proxy]	When a proxy server is used in your environment, select [ON]. [OFF] is specified by default.
[Port No.]	If necessary, change the port number. In normal circumstances, you can use the original port number. [21] is specified by default.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.1.3 Registering an SMB Destination

An SMB destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [SMB], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[Host Address]	Enter the destination computer name (host name) or IP address (using up to 253 characters). • Example of computer name (host name) entry: "HOME-PC" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[File Path]	Enter the shared folder name of the computer specified in [Host Address] (using up to 255 bytes). The shared folder name is generally referred to as a share name. • Entry example: "scan" When specifying a folder in the shared folder, insert a symbol, "\", between folder names. • Entry example: "scan\document"

Settings	Description
[User ID]	Enter the name of a user who is authorized to access the folder specified in [File Path] (using up to 64 characters).
[Password]	Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding ").
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.1.4 Registering a WebDAV Destination

A WebDAV destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [WebDAV], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[Host Address]	Enter the host name or IP address of the destination WebDAV server (using up to 253 characters). • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[File Path]	Enter the name of a destination folder in the WebDAV server specified in [Host Address] (using up to 142 bytes). • Entry example: "scan" When specifying a folder in the WebDAV folder, insert a symbol, "/", between the folder names. • Entry example: "scan/document"
[User ID]	Enter the name of a user who is authorized to access the folder specified in [File Path] (using up to 64 characters).
[Password]	Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding ").
[SSL Settings]	When SSL is used in your environment, select [ON]. [OFF] is specified by default.
[Proxy]	When a proxy server is used in your environment, select [ON]. [OFF] is specified by default.
[Port No.]	If necessary, change the port number. In normal circumstances, you can use the original port number. [80] is specified by default.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.1.5 Registering a User Box

A User Box can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [User Box], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[User Box No.]	Click [Search from List], and select a User Box from the list to save data. If the User Box is already known, you can manually enter the User Box number.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

15.1.6 Registering a Fax Address

A fax address can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [Fax], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[Destination]	Enter the destination fax number (using up to 38 digits, including symbols #, *, -, T, P, and E). • If your environment is Private Branch Exchange (PBX), entering "E-" first inserts the registered outside line number automatically. • If your environment is Private Branch Exchange (PBX), entering "P" following the outside line number ensures the dialing. • If you wish to send out a push signal over the dial line, enter "T". • Tap "-" to separate a dial number. It does not affect the dialing of the number.
[Confirm Fax Number]	Enter a destination fax number again for confirmation purposes. This option is displayed when [ON] is set by selecting [Fax Settings] - [Function Setting] - [Function ON/OFF Setting] - [Confirm Address (Register)] in Administrator mode.

Settings	Description
[Communication Setting]	As necessary, click [Display] and specify how to send a fax to a destination you wish to register. You may change the settings you made here before sending a fax. • [V34 Off]: V.34 is a communication mode used for super G3 fax communication. When the remote machine or this machine is connected to a telephone line via PBX, however, you may not establish a communication in the super G3 mode depending on telephone line conditions. In this case, it is recommended that you turn the V.34 mode off to send data. • [ECM Off]: ECM is an error correction mode defined by ITU-T (International Telecommunication Union - Telecommunication Standardization Sector). Fax machines equipped with the ECM feature communicate with each other, confirming that the sent data is free of errors. This prevents image blurring caused by telephone line noise. The communication time can be reduced by setting ECM to OFF for transmission. However, an image error or communication error may occur depending on the specified communication time value, so change the value to suit conditions. • [International Communication]: Select this option to send a fax to areas where communication conditions are poor. Faxes are sent at a lower speed. • [Check Destination]: Select this option to use Check Dest. & Send. The fax number specified for fax is checked against the destination fax number (CSI) and the fax is sent only when they match.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- To use this function, the optional **Fax Kit** is required.

15.1.7 Registering an Internet Fax Address

An Internet fax address can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [Internet Fax], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[E-mail Address]	Enter the E-mail address of the destination with 320 characters, excluding spaces.
[Fax Resolution]	Select a resolution of the original data that the recipient machine can receive.
[Paper Size]	Select a paper size of the original data that the recipient machine can receive.
[Compression Type]	Select a compression type of the original data that the recipient machine can receive.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

15.1.8 Registering an IP Address Fax Destination

An IP address fax destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

In the administrator mode, select [Store Address] - [Address Book] - [New Registration] - [IP Address Fax], then click [OK] to configure the following settings.

Settings	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Direct Input] and then enter a number.
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[Destination Type]	Select an address type of the destination. [IP Address] is specified by default.
[Address]	If [IP Address] or [Host Name] was selected for [Destination Type], enter the destination IP address or host name. • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16" • Example of host name entry: "host.example.com" (Also enter a domain name.) If [E-mail Address] was selected for [Destination Type], enter the destination mail address. To specify a destination by E-mail address, enter the destination IP address or host name following "ipaddrfax@". To enter an IP address following the @ symbol, put the IP address in brackets "[ ]". • Example of IP address (IPv4) entry: "ipaddrfax@[192.168.1.1]" To enter an IP address (IPv6), enter "IPv6:" following left bracket "[". • Example of IP address (IPv6) entry: "ipaddrfax@[IPv6:fe80::220:6bff:fe10:2f16]" To enter a host name following the @ symbol, brackets "[ ]" are unnecessary. • Example of host name entry: "ipaddrfax@host.example.com" To enter a host name or mail address, a DNS server must be specified on this machine.
[Port No.]	If necessary, change the port number. In normal circumstances, you can use the original port number. [25] is specified by default.
[Destination Machine Type]	Select whether the recipient machine supports color print. [Mono Model] is specified by default.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- To use this function, the optional **Fax Kit** is required.

15.2 Registering a Group

A group can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Multiple one-touch destinations can be grouped and managed as a single group.

In the administrator mode, select [Store Address] - [Group] - [New Registration], then configure the following settings.

Settings	Description
[Name]	Enter the destination name using up to 24 characters. Assign a name that helps you easily identify the destination.
[Index]	Select a corresponding character so that the destination can be index-searched by registration name. • For a frequently used destination, select also the [Main] check box. If the [Main] check box is selected, the destination will appear in the main screen of the fax/scan mode, enabling the user to easily select a destination.
[Scan/Fax Address]	Click [Search from List], and select destinations you wish to include in the registered group. You can register up to 500 destinations in a group. You can also register different types of destinations, such as E-mail address and fax number, in a group.
[Check Destination]	If necessary, click [Check Destination] to check the registered address books.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3 Registering a program

15.3.1 Registering an E-mail address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the E-mail address program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [E-mail], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination E-mail address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination E-mail address, select [Direct Input] and enter the address. To register certificate information select the [Registration of Certification Information] check box. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.2 Registering an FTP program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the FTP program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [FTP], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination FTP from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination FTP, select [Direct Input] and enter the FTP. • [Host Address]: Select the [Please check to enter host name.] check box, and enter the host name or IP address of a destination FTP server (using up to 253 characters). • [File Path]: Enter the name of a destination folder in the FTP server specified in [Host Address] (using up to 127 bytes). • [User ID]: Enter the available user name to log in (using up to 64 characters) if authentication is required in the destination FTP server. • [Password]: Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding "). • [anonymous]: When authentication is not required in the destination FTP server, select [ON]. • [PASV Mode]: When the PASV mode is used in your environment, select [ON]. • [Proxy]: When a proxy server is used in your environment, select [ON]. • [Port No.]: If necessary, change the port number. In normal circumstances, you can use the original port number. Only one destination can be specified.

Settings	Description
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.3 Registering an SMB program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the SMB program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [SMB], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination SMB from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination SMB, select [Direct Input] and enter the SMB. • [Host Address]: Select the [Please check to enter host name.] check box, and enter the destination computer name (host name) or IP address (using up to 253 characters). • [File Path]: Enter the shared folder name of the computer specified in [Host Address] (using up to 255 bytes). The shared folder name is generally referred to as a share name. • [User ID]: Enter the name of a user who is authorized to access the folder specified in [File Path] (using up to 64 characters). • [Password]: Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding "). Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.4 Registering a WebDAV program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the WebDAV program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [WebDAV], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.

Settings	Description
[Destination Information]	Click [Search from List], and select a destination WebDAV from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination WebDAV, select [Direct Input] and enter the WebDAV. • [Host Address]: Select the [Please check to enter host name.] check box, and enter the host name or IP address of a destination WebDAV server (using up to 253 characters). • [File Path]: Enter the name of a destination folder in the WebDAV server specified in [Host Address] (using up to 142 bytes). • [User ID]: Enter the name of a user who is authorized to access the folder specified in [File Path] (using up to 64 characters). • [Password]: Enter the password of the user you entered into [User ID] (using up to 64 characters, excluding "). • [SSL Settings]: When SSL is used in your environment, select [ON]. • [Proxy]: When a proxy server is used in your environment, select [ON]. • [Port No.]: If necessary, change the port number. In normal circumstances, you can use the original port number. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.5 Registering a User Box program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the User Box program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [User Box], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination User Box from the list. Click [Check Destination] to check registered address books. If you wish to manually specify a destination User Box, select the [Direct Input] option. Click [Search from List], and select a destination User Box from the list. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

15.3.6 Registering a fax address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the fax address program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [Fax], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination fax address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination fax address, select [Direct Input] and enter the address. • [Destination]: Enters the destination fax number. • [Communication Setting]: As necessary, specify how to send a fax to a destination you wish to register. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the fax transmission option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- To use this function, the optional **Fax Kit** is required.

15.3.7 Registering an Internet fax address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the Internet fax address program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [Internet Fax], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination Internet fax address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination Internet fax, select [Direct Input] and enter the FTP. • [E-mail Address]: Enters the destination E-mail address. • [Fax Resolution]/[Paper Size]/[Compression Type]: Select the specifications of original data that the recipient machine can receive. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

15.3.8 Registering an IP address fax program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the IP address fax program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [IP Address Fax], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination IP address fax from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination IP address fax, select [Direct Input] and enter the IP address fax. • [Destination Type]: Select an address type of the destination. • [Address]: Enters the destination IP address or host name. You can also specify a destination by E-mail address. To specify a destination by E-mail address, enter the destination IP address or host name following "ipaddrfax@". To enter an IP address following the @ symbol, put the IP address in brackets "[ ]". Example of IP address (IPv4) entry: "ipaddrfax@[192.168.1.1]" To enter an IP address (IPv6), type "IPv6:" following the left bracket "[". Example of IP address (IPv6) entry: "ipaddrfax@[IPv6:fe80::220:6bff:fe10:2f16]"To enter a host name following the @ symbol, brackets "[ ]" are unnecessary. Example of host name entry: "ipaddrfax@host.example.com" • [Port No.]: If necessary, change the port number. In normal circumstances, you can use the original port number. • [Destination Machine Type]: Select whether the recipient machine supports color print.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

Tips

- To use this function, the optional **Fax Kit** is required.

15.3.9 Registering a group program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

The following describes the group program.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [Group], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Destination Information]	Click [Search from List], and select a destination group from the list. Click [Check Destination] to check registered address books.
[Basic Setting]/[Application Setting]	Configure the fax/scan transmission option settings. For details, refer to page 15-14.

Settings	Description
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.10 Registering a program without destination

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

The following describes the program that does not specify a destination. You can only register the fax/scan transmission option settings with the program so that it can apply to various types of destinations.

In the administrator mode, select [Store Address] - [Program] - [Registration] - [No Destination], then click [OK] to configure the following settings.

Settings	Description
[Name]	Enter the program name (using up to 24 characters). Assign a name that helps you easily identify the program.
[Basic Setting]/[Application Setting]	Configure the fax/scan transmission option settings. For details, refer to page 15-14.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 12-30.

15.3.11 Configuring the fax/scan transmission option settings

A combination of address information and the fax/scan transmission option settings can be registered in a program. The following describes details on the option settings.

In [Basic Setting], configure the basic option settings for the fax/scan mode.

Settings	Description
[Fax Resolution]/[Scan Resolution]	Select a resolution to use to scan the original. [Fine]/[200 × 200] is specified by default.
[File Type]	Select the file type used for saving the scanned original data. The available file types are PDF, TIFF, JPEG, XPS, PPTX, DOCX, XLSX, and other types. You should use the password encrypted PDF file format to store important original data. [PDF] is specified by default.
[Outline PDF]	This can be configured when the [File Type] is set to [Compact PDF]. If you select [ON], the text is extracted from the original and converted into a vector image. [OFF] is specified by default.
[PDF Web Optimization]	This option is available when [File Type] is set to [PDF] or [Compact PDF] while the PDF processing function is enabled. Selecting [ON] linearizes a PDF file to quickly load the first page in the Web browser. [OFF] is specified by default.
[PDF/A]	This option is available when [File Type] is set to [PDF] or [Compact PDF] while the PDF processing function is enabled. Selecting [PDF/A-1a] or [PDF/A-1b] allows you to create a PDF file based on PDF/A. [OFF] is specified by default.

Settings	Description
[Searchable PDF]	This option is available when [File Type] is set to [PDF] or [Compact PDF] while the searchable PDF function is enabled. Selecting [ON] creates a searchable PDF file using OCR character recognition technology. • [Language Selection]: Select a language for OCR processing. Select the language used in the original to recognize text data properly. • [Adjust Rotation]: Select [Adjust] to automatically perform the rotation adjustment for each page based on the direction of text data detected by OCR processing. • [Document Name Auto Extraction]: Select [ON] to automatically extract a character string appropriate for a document name from the OCR character recognition result, and specify it as a document name. [OFF] is specified by default.
[Character Recognition]	This option is available when [File Type] is set to [PPTX], [DOCX], or [XLSX] while the searchable PDF function is enabled. Selecting [ON] creates a searchable file using the OCR character recognition technology. • [Language Selection]: Select a language for OCR processing. Select the language used in the original to recognize text data properly. • [Adjust Rotation]: Select [Adjust] to automatically perform the rotation adjustment for each page based on the direction of text data detected by OCR processing. • [Output Method]: Select how to create a file using the text detected by OCR processing. The selectable output method varies depending on the file type you have selected in [File Type]. [OFF] is specified by default.
[File Name]	If necessary, change the file name of the scanned original.
[Page Setting]	Tap this button to select a filing page unit when an original consists of multiple pages. • [Multi Page]: Select this check box to convert all pages to a single file. However, if [File Type] is set to [JPEG], you cannot select [Multi Page]. • [Page Separation]: Used to convert the specified number of pages as a single file. [Multi Page] is specified by default.
[Subject]	Click [Subject List] or select a fixed phrase used as the E-mail subject. If you select [Not Specified], the subject specified by default will be inserted. When necessary, it can be changed before transmission. [Not Specified] is specified by default.
[Text]	Click [Text List] or select a fixed phrase used as the E-mail body. If you select [Not Specified], the body specified by default will be inserted. When necessary, it can be changed before transmission. [No Selection] is specified by default.
[File Attachment Setting]	You can select the E-mail attachment method when [Page Setting] is set to [Page Separation]. • [All Files Sent as one (1) E-mail]: Attaches all files to one E-mail. • [One (1) File per E-Mail]: Sends one E-mail for each file. [All Files Sent as one (1) E-mail] is specified by default.
[Simplex/Duplex]	Select whether to scan the front and back sides of an original automatically. You can only scan a single side of the first page and both sides of the remaining pages automatically. • [1-Sided]: Scan one side of an original. • [2-Sided]: Scan both sides of an original. • [Cover Sheet + 2-Sided]: Scans a single side of the first page, and scans both sides of the remaining pages. [1-Sided] is specified by default.
[Original Type]	Select the setting appropriate for the contents of the original, and scan the original with the optimum image quality. [Text Printed Photo] is specified by default.
[Color]	Select a color mode for scanning originals. There are four color modes: [Auto] to scan based on the original color, [Full Color], [Gray Scale], and [Black and White]. [Auto] is specified by default.

Settings	Description
[Separate Scan]	When there are too many original sheets that cannot be loaded into the **ADF** at the same time, if you load them in several batches and handle them as one job, select [ON]. You can also scan the original using both **ADF** and **Original Glass** alternately. [OFF] is specified by default.
[Density]	Adjust the density (Dark or Light) to scan the original. [0(Standard)] is specified by default.
[Background Removal]	Adjust the density of the background area when printing originals with colored background (newspaper, recycled paper, etc.) or originals that are so thin that text or images on the back would be scanned. • [Bleed Removal]: Select this option to prevent a back-side bleeding when printing a 2-sided original that is so thin that the contents of the back side would be scanned. • [Discoloration Adjust]: Select this option to scan an original with the colored background such as a map. [Bleed Removal] is specified by default.
[Scan Size]	Select the size of the original to be scanned. [Auto] is specified by default.

In [Application Setting], configure the application option settings for the fax/scan mode.

Settings	Description
[E-mail Notification]	Send an E-mail, which contains a destination where to save original data, to a specified E-mail address after SMB transmission, FTP transmission, WebDAV transmission, or User Box filing has been ended. Click [Search from List], and select a destination E-mail address from the list. You can manually enter an E-mail address. [OFF] (not selected) is specified by default.
[Timer TX]	To set a time to start fax transmission, select [ON]. Also specify when to start fax transmission. [OFF] is specified by default.
[Password TX]	To send fax with a password to a destination for which fax destinations are restricted by passwords (Closed Network RX enabled), select [ON]. Also enter the password. [OFF] is specified by default.
[F-Code]	Select [Enable] to enable F-Code TX. Also enter [SUB Address] and [Password]. [Disable] is specified by default.
[Original Direction]	When scanning a double-sided original, you can specify the original loading direction so that the vertical direction is set correctly after scanning. [Top] is specified by default.
[2-Sided Binding Direction]	Select the biding position of original when scanning both sides of the original. [Auto] is specified by default.
[Special Original]	Select an original type when scanning special documents. • [Same Width]/[Different Width]: Even for an original with pages of different sizes, by using **ADF**, you can scan data while detecting the size for each page. • [Z-Folded Original]: Even folded originals, the original size can be detected accurately. • [Long Original]: Load a long original that cannot be placed on the **Original Glass** and that is larger in the feeding direction that the full standard size (11 × 17 or A3) into the **ADF**. There is no need to enter the original size in advance: the **ADF** will detect the size automatically. [Normal] is specified by default.
[Skip Blank Page(s) During Scan]	When scanning an original that contains blank pages, select whether to exclude blank pages from scanning. [OFF] is specified by default.
[Thin Paper Original]	Reduce the original feed speed of the **ADF** to prevent thin paper from paper jam. [OFF] is specified by default.

Settings	Description
[Despeckle]	Selecting [ON] scans an original using the **ADF** while removing dusts on the **Slit Scan Glass**. [OFF] is specified by default.
[Book Original]	Select this option if you scan two-page spreads such as book and catalog separately into the left and right pages, or scan a page spread as a single page. • [Method]: Select a method to scan two-page spreads from [Book Spread], [Separation], [Front Cover], and [Front/Back Cover]. • [Center Erase]: Erases the shadow created in the center when the original cover cannot be closed properly due to the thickness of the original. • [Bind Direction]: If [Separation], [Front Cover] or [Front/Back Cover] is selected for [Method], select an output bind position of two-page spreads to be scanned. Select [Left Bind] for originals of left binding, and [Right Bind] for originals of right binding. [OFF] (not selected) is specified by default.
[Frame Erase]	Erases an area of an identical specified width along the four sides of an original. You can erase the four sides of the original to different widths. [OFF] (not selected) is specified by default.
[Compose(Date/Time)]	Select this option to print on a specified page the date/time that the original was scanned. You can select a print position in the page and format. [OFF] (not selected) is specified by default.
[Compose(Page)]	Select this option to print all page numbers and chapter numbers. You can select a print position and format. [OFF] (not selected) is specified by default.
[Compose(Header/Footer)]	Select this option to print text or date/time on the top and bottom margins in a specified page Select a content from previously registered ones. [OFF] (not selected) is specified by default.
[Compose(Stamp)]	Select this check box to print a text such as "PLEASE REPLY" and "DO NOT COPY" on the first page or all pages. You can select the text to be printed from the registered fix stamps and arbitrary registered stamps. [OFF] (not selected) is specified by default.
[Stamp Combine Method]	When combining date/time, page, header/footer, and stamp, select whether to combine them as text or an image. [Image] is specified by default.

15.4 Registering a temporary one-touch destination

The temporary one-touch function registers a combination of address information and the fax/scan transmission option settings temporarily with this machine.

A temporary one-touch destination is deleted once data is sent to the registered destination or when the machine is turned OFF.

In the administrator mode, select [Store Address] - [Temporary One-Touch], then configure the settings. The temporary one-touch destination to be registered is the same as the registered program address.

Tips

- However, [Registration of Certification Information] and [Limiting Access to Destinations] are not available for temporary programs.

15.5 Registering the subject and body of an E-mail

Registering the subject

Register the subject used for sending E-mail messages or Internet faxes. Up to 10 subjects can be registered, and a subject can be selected from them before transmission.

In the administrator mode, select [Store Address] - [Subject] - [Edit], and enter a subject to be registered in [Subject] (using up to 64 characters, excluding a symbol "•").

Registering the body

Register the body used for sending E-mail messages or Internet faxes. Up to 10 bodies can be registered, and a body can be selected from them before transmission.

In the administrator mode, select [Store Address] - [Text] - [Edit], and enter a text to be registered in [Text] (using up to 256 characters, excluding a symbol "•").

15.6 Registering a prefix and suffix of each destination

Register a prefix and suffix of an E-mail address.

If a domain contains many E-mail addresses, register a character string (domain name) following an at mark @ as a suffix. This recalls the registered domain name when you enter an E-mail address, facilitating your entry. You can also register a long domain name of an E-mail address to prevent entry mistakes.

Up to 8 prefixes/suffixes can be registered.

In the administrator mode, select [Store Address] - [Prefix/Suffix] - [Edit], and register prefixes and suffixes.

Settings	Description
[Prefix]	Enter a prefix (using up to 20 characters, excluding spaces).
[Suffix]	Enter a suffix (using up to 64 characters, excluding spaces).

15.7 Registering the information to be added to header/footer

When printing an original, you can recall the registered header/footer and print it at the top or bottom of a page. Up to 20 headers/footers can be registered.

In the administrator mode, select [System Settings] - [Stamp Settings] - [Header/Footer Registration] - [Edit], then configure the following settings.

Settings	Description
[Name]	Enter the name of the header or footer to be registered (using up to 16 characters). When selecting a header or footer, give it a name that helps you easily identify it.
[Color]	If necessary, select the print color of the text.
[Pages]	Select the range of pages on which the text is printed in the header/footer.
[Size]	If necessary, select the size of the text.
[Text Type]	If necessary, select the font type of the text.
[Date/Time Setting]	Select the display format of date and time if the [Date/Time Setting] of [Header] or [Footer] is set to [Print].
[Distribution Number]	Specify the content of distribution number to be displayed if the [Distribution Number] of [Header] or [Footer] is set to [Print]. • [Text]: Enter a text to be added to the distribution number for printing (using up to 20 characters). • [Output Method]: Select the number of digits. • [Start Number Specification]: Specify the number to start distribution numbers.
[Header]/[Footer]	Specify the items to be printed on header/footer • [Header String]/[Footer String]: Enter a text to be printed (using up to 40 characters). • Select whether to print [Date/Time Setting], [Distribution Number], [Job Number], [Serial Number] (Engineering number of the machine), and [User Name/Account Name].

Tips

- This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

15.8 Adding a font/macro

Add a font or macro to this machine. Also delete the registered font or macro.

In the administrator mode, select [Maintenance] - [Edit Font/Macro] - [New Registration], then configure the following settings.

Settings	Description
[Type]	Select a type of font or macro to be registered.
[ID]	Enter the ID of the font/macro. This item cannot be configured if the PS font, OOXML font, or PS macro is selected. 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. Save the OOXML font in the hard disk (HDD).

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

15.9 Registering a paper name and paper type

Register a paper name and paper type as custom paper. Custom paper can be added to the paper type option.

1 In the administrator mode, select [System Settings] - [Set Paper Name by User], then set [Set Paper Name by User] to [ON].

2 In the administrator mode, select [System Settings] - [Set Paper Name by User] - [Edit Paper Name] - [Edit], then configure the following settings.

Settings	Description
[Paper Name]	Enter the paper name (using up to 12 characters). Assign a name that helps you easily identify the registered paper.
[Paper Type]	Select a paper type. [Plain Paper] is specified by default.

15.10 Using data management utility

15.10.1 Data Management Utility

Data Management Utility is a tool capable of managing copy protect data, stamp data, and font/macro data of this machine from a computer on the network.

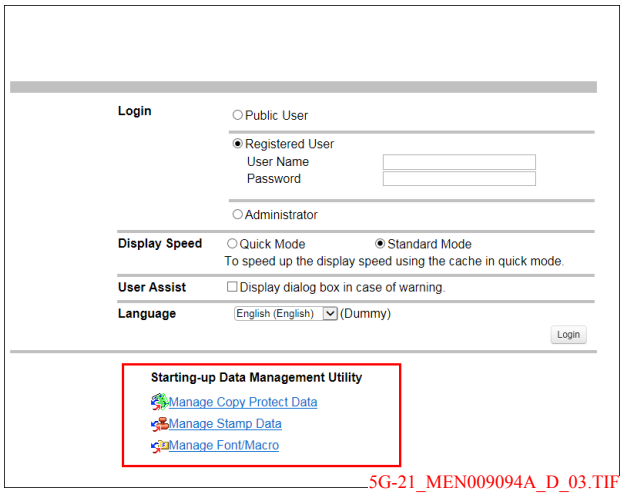
Start up Data Management Utility from the **Web Connection** login page.

Tips

- You cannot start up multiple Data Management Utilities at the same time.

Follow the below procedure to use Data Management Utility.

1 In the **Web Connection** login page, select the Data Management Utility to be started.



➔ For details on [Manage Copy Protect Data], refer to page 15-24.
➔ For details on [Manage Stamp Data], refer to page 15-26.
➔ For details on [Manage Font/Macro], refer to page 15-27.

2 Enter the administrator password of this machine, then click [OK].

➔ When the registered user who has administrator privileges logs in, select [Registered User], then enter the user name and password.

Data Management Utility starts up.

15.10.2 Managing the copy protect data

Copy Protect is a function that prints a text such as "Copy" and "Private" as a concealed text in all pages.

You can register or edit copy protect data using Data Managing Utility. Up to eight units of copy protect data can be managed.

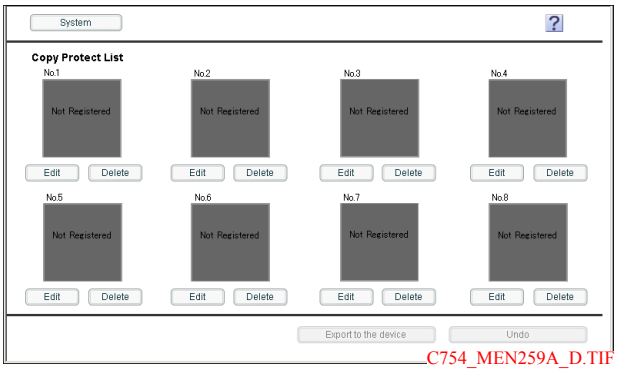
✔ This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

1 In the **Web Connection** login page, start the [Manage Copy Protect Data].

The copy protect data list registered on this machine appears.

2 To register or edit the copy protect data, click [Edit].

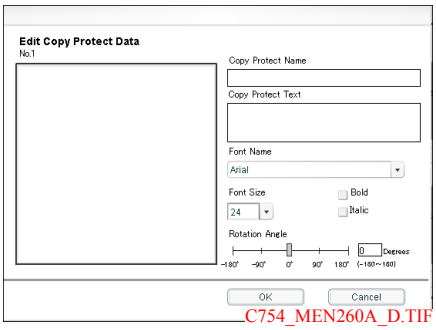
➔ Clicking [Delete] deletes the registered copy protect data. The copy protect data will not be deleted until you click [Export to the device] and write it to this machine.



C754_MEN259A_D.TIF

3 Register or edit the copy protect data, and click [OK].

➔ You can edit data while checking the result in the preview.



C754_MEN260A_D.TIF

Settings	Description
[Copy Protect Name]	Enter the Copy Protect name using up to 16 characters.
[Copy Protect Text]	Enter a text to be printed (using up to 32 characters).
[Font Name]	Select the font type of the text.
[Font Size]	Select the size of the text to be printed.
[Bold]	Select this check box to display the text in bold.
[Italic]	Select this check box to display the text in italic.
[Rotation Angle]	Specify the rotation angle of the text. The angle can be adjusted in increments of one degree.

4 Click [Export to the device].

➔ Clicking [Undo] returns to the state before the change.

The registered or edited copy protect data is written to this machine.

Tips

Clicking [System] displays the system menu. The following menu items are available in the system menu.

- [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
- [Export]: Save the data registered on this machine to the computer as a file.
- [Import]: Write the data stored in a file to this machine.
- [Exit]: Exit the utility.

15.10.3 Managing the stamp data

You can register or edit stamp data using Data Managing Utility. Up to eight units of stamp data can be managed. You cannot edit or delete stamp data that was registered on this machine when it was shipped.

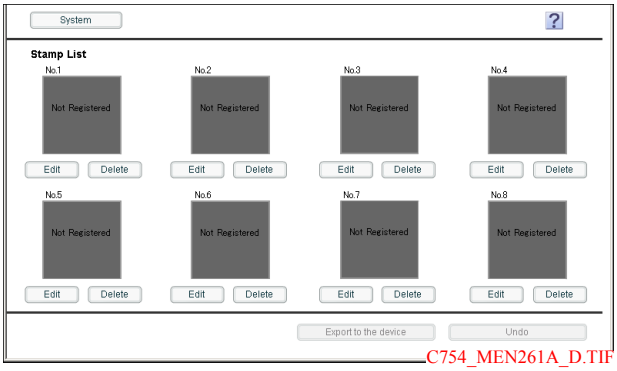
✔ This function is available when the Web browser function is disabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

1 In the **Web Connection** login page, start the [Manage Stamp Data].

The stamp data list registered on this machine appears.

2 To register or edit the stamp data, click [Edit].

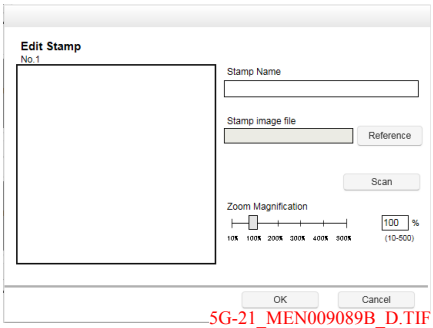
➔ Clicking [Delete] deletes the registered stamp data. The stamp data will not be deleted until you click [Export to the device] and write it to this machine.



C754_MEN261A_D.TIF

3 Register or edit the stamp data, and click [OK].

➔ You can edit data while checking the result in the preview.



5G-21_MEN009089B_D.TIF

Settings	Description
[Stamp Name]	Enter the stamp name (using up to 16 characters).
[Stamp image file]	Click [Choose File] and specify the location of the image (BMP) file used as a stamp.
[Scan]	Enlarges a stamp image. You can check the image details.
[Zoom Magnification]	Specify the zoom ratio of the stamp image. The ratio can be adjusted in increments of 1%.

4 Click [Export to the device].

➔ Clicking [Undo] returns to the state before the change.

The registered or edited stamp data is written to this machine.

Tips

Clicking [System] displays the system menu. The following menu items are available in the system menu.

- [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
- [Export]: Save the data registered on this machine to the computer as a file.
- [Import]: Write the data stored in a file to this machine.
- [Exit]: Exit the utility.

15.10.4 Managing the font/macro data

You can add or delete font/macro data using Data Managing Utility.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

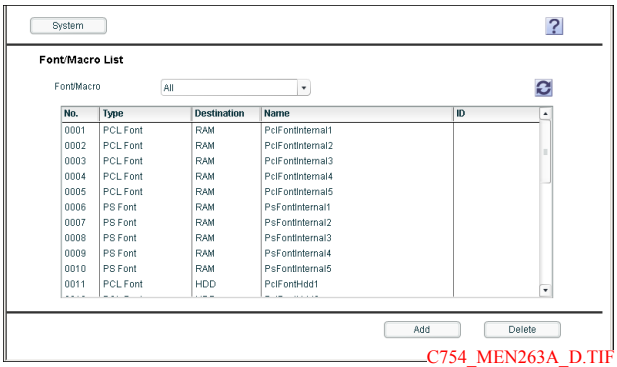
1 In the **Web Connection** login page, start the [Manage Font/Macro].

The font/macro data list registered on this machine appears.

2 To add font or macro data, click [Add].

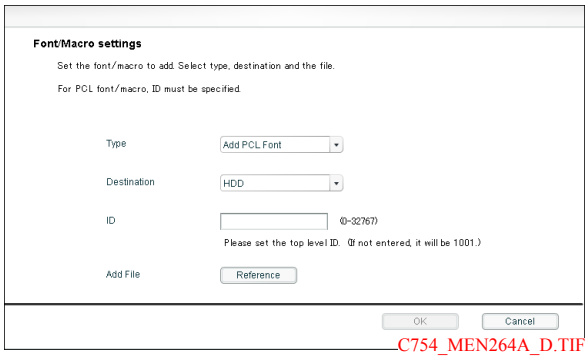
➔ The lists of font and macro can be switched by [Font/Macro].

➔ Clicking [Delete] deletes the selected font or macro data.



C754_MEN263A_D.TIF

3 Specify the font or macro to be added, and click [OK].



C754_MEN264A_D.TIF

Settings	Description
[Type]	Select a type of font or macro to be added.
[Destination]	Select where to save font or macro. • [HDD]: Save the font or macro to the hard disk on this machine. • [RAM]: Save the font or macro to the memory on this machine. When you turn off the power of the machine, the saved font/macro will be erased. To continuously use font or macro data, save it in the HDD. Save the OOXML font in the hard disk (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], and specify the location of a font file or macro file.

Tips

Clicking [System] displays the system menu. The following menu items are available in the system menu.

- [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
- [Exit]: Exit the utility.

16 Associating with External Application

16 Associating with External Application

16.1 Using the Web browser function

Overview

If the Web browser function is enabled on this machine, you can display or print contents on websites and upload files via the Web browser using the **Touch Panel** of this machine.

Enabling the Web browser function

To enable the Web browser function, this machine is automatically connected to the License Management Server (LMS) on the Internet in order to register the license. Check that this machine can be connected to the Internet before beginning this procedure.

In the administrator mode, select [Network] - [Web Browser Setting] - [Web Browser Setting], and set [Web Browser] to [Enable]. Setting to [Enable] restarts this machine automatically.

Tips

- If this machine cannot be connected to the License Management Server, you need to manually register the license. Before enabling the Web browser function, access the Web site of the License Management Server from the computer, then obtain license information required to enable the Web browser function. For details on how to obtain license information, refer to "User's Guide[Advanced Function Operations]/[Using the Web Browser Function]".

Restricting file operations on a Web browser

Select whether to allow file uploading or downloading on a site displayed on the Web browser.

In the administrator mode, select [Network] - [Web Browser Setting] - [File Operation Permission Setting], then configure the following settings.

Settings	Description
[Upload]	Select whether to allow uploading of data scanned on this machine to the site displayed on the Web browser. To allow uploading of data to only the specified site, select [Permitted URL Only], then enter the URL of the site to allow uploading of files to (using up to 256 characters). [ON] is specified by default.
[Download]	Select whether to allow downloading of files from the site displayed on the Web browser. When you allow downloading of data from only the specified site, select [Permitted URL Only], then enter the URL of the site to allow downloading of files from (using up to 256 characters). [ON] is specified by default.

16.2 Associating via TCP Socket

Overview

To use application software that communicates with this machine via TCP Socket, configure the TCP Socket settings of this machine.

If a certificate for this machine is registered, you can encrypt communication between the machine and application software using SSL.

To perform the association via TCP Socket, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the basic TCP Socket settings

➔ For details on configuring the setting, refer to page 16-3.

3 Set the following options according to your environment

Purpose	Reference
Encrypting communication between this machine and application software with SSL. (If you installed user authentication using an external authentication server, relevant settings are required.)	page 16-3

Configuring the basic TCP Socket settings

Enable TCP Socket.

In the administrator mode, select [Network] - [TCP Socket Setting], then configure the following settings.

Settings	Description
[TCP Socket]	Select this option to use TCP Socket. [ON] (selected) is specified by default.
[Port Number]	If necessary, change the port number. In normal circumstances, you can use the original port number. [59158] is specified by default.

Tips

- If you click [OK] after changing multiple port numbers collectively in **Web Connection** or on the **Control Panel**, a port number duplication error may appear. If a port number duplication error appears, change multiple port numbers one by one instead of changing them collectively.

Using SSL communication

Use SSL to encrypt communication between this machine and application software via TCP Socket.

1 Register a certificate for this machine and enable SSL communication.

➔ For details, refer to page 13-2.

2 In the administrator mode, select [Network] - [TCP Socket Setting], then configure the following settings.

Settings	Description
[Use SSL/TLS]	Select this check box to use SSL communication. [OFF] (not selected) is specified by default.
[Port No.(SSL/TLS)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [59159] is specified by default.

16.3 Associating via OpenAPI

Overview

To use application software that communicates with this machine via OpenAPI, configure the OpenAPI settings of this machine.

If a certificate for this machine is registered, you can use SSL to encrypt communication between this machine and a client when the machine acts as a server.

By using the Simple Service Discovery Protocol (SSDP) function of this machine, you can associate with OpenAPI connection application software smoothly.

To perform the association via OpenAPI, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the basic OpenAPI settings

➔ For details on configuring the setting, refer to page 16-4.

3 Set the following options according to your environment

Purpose	Reference
Communicating with application software via a proxy server	page 16-5
Encrypting communication between this machine and application software with SSL.	page 16-5
Referencing authentication information from the extended server when the OpenAPI application starts (Single Sign-On)	page 16-6

Configure the basic OpenAPI settings

Enable the SSDP function. If necessary, change the OpenAPI communication port number.

1 In the administrator mode, select [Network] - [SSDP Settings], then configure the following settings.

Settings	Description
[SSDP]	Select [ON] to use the OpenAPI. This allows for the following actions: • Notifying of OpenAPI service having started on this machine. • Returning a response to a search for OpenAPI service. [ON] is specified by default.
[Multicast TTL Setting]	Change TTL (Time To Live) for SSDP multi-cast packet if necessary. The value is decremented by one each time a communication is established via the router. When the value reaches 0, packets are discarded. [1] is specified by default.

2 In the administrator mode, select [Network] - [OpenAPI Setting], and change the port number if necessary (Default: [50001]).

➔ In normal circumstances, you can use the original port number.

Tips

- If you click [OK] after changing multiple port numbers collectively in **Web Connection** or on the **Control Panel**, a port number duplication error may appear. If a port number duplication error appears, change multiple port numbers one by one instead of changing them collectively.

Using the proxy server

When the proxy server is used in your network environment, you can configure settings to communicate with applications via the proxy server.

To use the proxy server, register the proxy server information on this machine. In addition, configure the settings for connection to the proxy server.

In the administrator mode, select [Network] - [OpenAPI Setting], then configure the following settings.

Settings	Description
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [8080] is specified by default.
[Proxy Server Port Number (HTTPS)]	If necessary, change the port number of the proxy server when using the HTTPS protocol. [8080] is specified by default.
[Proxy Server Port Number (FTP)]	If necessary, change the port number of the proxy server when using the FTP protocol. [21] is specified by default.
[User Name]	Enter the user name to log in to the proxy server (using up to 63 characters).
[Password]	Enter the password of the user name you entered into [User Name] (using up to 63 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

Using SSL communication

Use SSL to encrypt communication between this machine and application software via OpenAPI.

1 Register a certificate for this machine and enable SSL communication.

➔ For details, refer to page 13-2.

2 In the administrator mode, select [Network] - [OpenAPI Setting], then configure the following settings.

Settings	Description
[Use SSL/TLS]	To use SSL communication, select [SSL Only] or [SSL/Non-SSL]. [SSL Only] is specified by default.
[Port No.(SSL)]	If necessary, change the SSL communication port number. In normal circumstances, you can use the original port number. [50003] is specified by default.
[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.

Settings		Description
	[Client Certificates]	Select whether to request a certificate from clients that connect to this machine. [Do not request] is specified by default.
	[Validity Period]	Confirm whether the certificate is still valid. [Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

Using the single sign-on

Reference authentication information from the extended server when the OpenAPI application starts. This allows you to build up a single sign-on environment with the OpenAPI application to be started and the back-end system that is associated with the OpenAPI application.

In the administrator mode, select [Network] - [OpenAPI Settings] - [Single Sign-On Setting], then configure the following settings.

Settings	Description
[Authentication Info. Reference]	Select whether to reference authentication information from the extended server when the OpenAPI application registered on this machine starts. [OFF] is specified by default.
[Registered Application List]	Specify the OpenAPI application in which a reference of authentication information is to be permitted in the list of OpenAPI applications registered on this machine. Click [Edit], then select whether to reference authentication information in each application.

16.4 Using the machine FTP server for association

Overview

To use application software with which the FTP server of this machine is used to communicate, configure the FTP server.

To use the FTP server of this machine for the association, follow the below procedure to configure the settings.

✔ The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the FTP server settings

➔ For details on configuring the setting, refer to page 16-7.

Configuring the FTP server settings

Enable the FTP server. Configure the security relevant settings.

In the administrator mode, select [Network] - [FTP Setting] - [FTP Server Setting], then configure the following settings.

Settings	Description
[FTP Server]	Select [ON] to use the FTP server. [OFF] is specified by default.
[Deny Reception Command]	Select a command to deny a receiving job from an FTP client when using the FTP server of this machine. Set this option to return an error when a PORT/EPRT command or PASV/EPSV command is sent from an FTP client to this machine. [Allow] is specified by default.
[PORT Command Enhanced Security]	Select whether to enable the security of this machine against FTP bounce attacks. This option is not available if [Deny Reception Command] is set to [PORT/EPRT]. When a PORT/EPRT command is sent from an FTP client, the data connection is established only if both of the following conditions are satisfied: • A port number less than 1024 is not specified. • The IP address specified by the command is same as that specified when a control connection is established. [Enable] is specified by default.

16.5 Using the machine WebDAV server for association

Overview

To use application software with which the WebDAV server of this machine is used to communicate, configure the WebDAV server function.

If a certificate for this machine is registered, you can encrypt communication between the machine and application software using SSL.

To use the WebDAV server of this machine for the association, follow the below procedure to configure the settings.

1 Configure settings for connecting to the network such as setting of the IP address of this machine

➔ For details on configuring the setting, refer to page 2-2.

2 Configure the WebDAV server settings

➔ For details on configuring the setting, refer to page 16-8.

3 Set the following options according to your environment

Purpose	Reference
Encrypting communication between this machine and application software with SSL.	page 16-8

Configuring the WebDAV server settings

Enable the WebDAV server. Also set an access right to the WebDAV server.

In the administrator mode, select [Network] - [WebDAV Settings] - [WebDAV Server Settings], then configure the following settings.

Settings	Description
[WebDAV Settings]	Select [ON] to use the WebDAV server. [ON] is specified by default.
[Access Rights Settings]	Specify the password to restrict accesses to the WebDAV server of this machine (using up to 64 characters, excluding "). To enter (change) the password, select the [Password is changed.] check box, then enter a new password. Clicking [Initial Password] resets the set password (Default: sysadm). [OFF] (not selected) is specified by default.

Using SSL communication

Encrypt communication between this machine and the WebDAV client application with SSL.

1 Register a certificate for this machine and enable SSL communication.

➔ For details, refer to page 13-2.

2 In the administrator mode, select [Network] - [WebDAV Settings] - [WebDAV Server Settings], and set [SSL Setting] to [SSL Only] or [SSL/Non-SSL] (Default: [Non-SSL Only]).

16.6 Releasing the association with application

You can set this to prevent this machine from being connected to the server when an error occurs on the server while **My Panel Manager** or **My Print Manager** is running.

In the administrator mode, select [System Settings] - [System Connection Setting] - [System Connection Setting], then configure the following settings.

Settings	Description
[PageScope My Panel Manager]	Select [OFF] to cancel the connection from this machine to **My Panel Manager**. [ON] is specified by default.
[My Spool]	Select [OFF] to cancel the connection from this machine to **My Print Manager**. [ON] is specified by default.

Tips

- The **Hard Disk** is optional in some areas. To use this function, the optional **Hard Disk** is required.

16.7 Associating with the distributed scan server

Overview

This machine can be integrated into the system using the Distributed Scan Management. The Distributed Scan Management is a function of Windows Server 2008 R2/Server 2012/Server 2012 R2, integrating scanner devices supporting the function into the document workflow of an organization.

The function sends the original data scanned on this machine to the distributed scan server. When receiving the file, the scan server carries out sending to the SMB folder, E-mail address, or Microsoft Office SharePoint Server based on the registered scan process.

✔ This machine must join the Active Directory domain in advance.

1 Enable WS scan and configure the SSL communication settings

➔ For details on configuring the setting, refer to page 16-10.

2 Enable the Distributed Scan Management

➔ For details on configuring the setting, refer to page 16-10.

Configuring the environment to use Distributed Scan Management

Enable WS scan and configure SSL communication settings.

1 In the administrator mode, select [Network] - [DPWS Settings] - [Scanner Settings], then set [Scan Function] to [ON] (Default: [OFF]).

2 In the administrator mode, select [Network] - [DPWS Settings] - [DPWS Common Settings], then set [SSL Setting] to [ON] (Default: [OFF]).

Enable the Distributed Scan Management

Enable the Distributed Scan function.

In the administrator mode, select [Network] - [Distributed Scan Function Settings], and set [Distributed Scan Function Settings] to [ON] (Default: [OFF]).

16.8 Associating with the ThinPrint system

Configure settings to enable the ThinPrint function in this machine.

ThinPrint is a function that realizes speedy printing by performing data compression or broadband control when sending a print job from ThinPrint Engine (.print Engine) to ThinPrint Client (.print Client). This machine operates as ThinPrint Client (.print Client).

Tips

- To use this function, the optional **i-Option LK-111** is required.

In the administrator mode, select [Network] - [ThinPrint Setting], then configure the following settings.

Settings		Description
[.print client Settings]		Select whether to use the ThinPrint protocol on this machine. Select [ON] to use this machine as ThinPrint Client (.print Client). [ON] is specified by default.
	[Port Number]	Enter the port number of ThinPrint Engine (.print Engine) to be connected. [4000] is specified by default.
	[Data Size Before Compression]	Specify the maximum packet size between 128 and 128000 to compress data in the ThinPrint Engine (.print Engine) side (units: bytes). ThinPrint Engine (.print Engine) compresses data in these sizes before sending a print job to this machine. [8192] is specified by default.
	[Connection Timeout]	Enter the connection timeout value to send a print job from ThinPrint Engine (.print Engine) between 5 and 300 (units: seconds). [90] is specified by default.
	[Printer Class Name]	Enter the printer class name of this machine to be used in ThinPrint Engine (.print Engine) (using up to seven characters).
	[Printer Name]	Enter the printer name of this machine to be used in ThinPrint Engine (.print Engine) (using up to 32 characters).
	[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item. • [Validity Period]: Confirm whether the certificate is within the validity period. [Confirm] is specified by default. • [CN]: Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default. • [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default. • [Chain]: Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default. • [Expiration Date Confirmation]: Confirm whether the certificate has expired. Whether the certificate has expired is confirmed in the order of OCSP (Online Certificate Status Protocol) service, then CRL (Certificate Revocation List). [Do Not Confirm] is specified by default.
[Connection Service Setting]		Select whether to use Connection Service. [OFF] is specified by default.
	[Server Address]	Enter the address of the server that supplies Connection Service. Use the following entry formats. • Example of entry: "192.168.1.1"
	[Port Number]	Enter the number of the port that is used for Connection Service. [4001] is specified by default.
	[AYT Interval]	Enter the reconnection interval to check Connection Service operations (units: seconds). [60] is specified by default.
	[Client ID]	Enter the client ID of this machine to be used for Connection Service. [1] is specified by default.
	[Authentication Key]	Enter the authentication key used to connect to Connection Service. [0] is specified by default.

Settings	Description
[Server Connection Status]	Displays the status of the connection with Connection Service. Clicking [Refresh] updates the status.

16.9 Allowing for upload of contents to this machine

If the Internal Web Server (IWS) function is enabled, you can transfer Web page contents to this machine and use the machine as a Web server.

Transfer the Web page contents to this machine using WebDAV. You can also use static content and script-base dynamic content to fit your environment.

In the administrator mode, select [Network] - [IWS Settings], then configure the following settings.

Settings		Description
[IWS Settings]		Select [ON] to use the IWS function. [OFF] is specified by default.
[Port Number (Web Server)]		If necessary, change the port number used for accessing the Web page contents uploaded to this machine. [8090] is specified by default.
[Port Number (Application Installation)]		If necessary, change the port number to be used for dynamic contents of this machine. [8091] is specified by default.
[Connect IWS Apps to Network]		If Web page contents uploaded to this machine have dynamic contents, such as scripts, select whether to allow an external connection of the dynamic contents. [Allow] is specified by default.
[Communication Between Applications]		Configure settings to operate the IWS application installed on this machine through the IWS application installed on a different device or an external application such as an application on an Android/iOS terminal.
	[Permit Access for Communication between Applications]	Select whether to allow an external application to operate the IWS application on this machine. [Deny] is specified by default.
	[Authentication]	Configure authentication information for logging in to this machine that is required when an external application operates the IWS application on this machine. • [User Name]: Enter the user name (using up to eight characters). • [Password]: Enter the password of the user name you entered into [User Name] (using up to eight characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.
	[Login Information Notification Setting]	Select whether to notify you of the user name and password of the user who is using this machine, when the IWS application on this machine operates that of a different device. [Allow] is specified by default.

Tips

- This function is available when the Web browser function is enabled. When the optional **Extension Memory** is installed, this function is available regardless of whether the Web browser function is enabled or disabled.

16.10 Associating with the remote diagnosis system

16.10.1 Registering a proxy server used for remote diagnosis

To use a proxy server for using a service that diagnoses the machine status remotely, register the proxy server information with this machine.

A proxy server used for WebDAV transmission can also be used as a proxy server for remote diagnosis. You can also a different proxy server.

In the administrator mode, select [Network] - [WebDAV Settings] - [Proxy Setting for Remote Access], then configure the following settings.

Settings		Description
[Proxy Setting for Remote Access]		Select [ON] to use a proxy server for remote diagnosis. [OFF] is specified by default.
[Proxy Settings]		Configure the proxy server used for remote diagnosis
	[Synchronize WebDAV Client Setting]	Select whether to use the proxy server used for WebDAV transmission as a proxy server for remote diagnosis. To use a different proxy server for remote diagnosis, select [OFF] and enter the proxy server information. [ON] is specified by default.
	[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
	[Proxy Server Port Number]	If necessary, enter the proxy server port number.
	[User Name]	Enter the user name to log in to the proxy server (using up to 63 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 63 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

16.10.2 Allowing acquisition of the machine counter

When using a service that diagnoses the machine status remotely, the counter information managed by this machine can be acquired from the remote diagnosis system.

In the administrator mode, select [User Authentication/Account Track] - [Counter Remote Control], and set [Counter Remote Control] to [Allow] (Default: [Restrict]).

Tips

- This setting is available if you use the remote diagnosis system, and user authentication and account track is installed on this machine.

16.10.3 Sending the machine operating status

When using a service that diagnoses the machine status remotely, send the operating status of this machine to the remote diagnosis system.

In the administrator mode, select [Maintenance] - [Call Remote Center], then click [Call Remote Center].

Tips

- This setting is available if you use the remote diagnosis system.

16.10.4 Allowing read and write of the machine setting information

When using a service that diagnoses the machine status remotely, addresses (address book, group, and program) registered with this machine and authentication information (user authentication and account track) can be imported or exported from/to the remote diagnosis system.

In the administrator mode, [Maintenance] - [Remote Access Setting], then set [Import/Export User Data] to [Allow].

16.11 Associating with the fax server

Overview

When using a fax server, you can configure the server for registering and using applications.

When using the fax server communicates in the E-mail format, you can configure settings to automatically add a prefix and suffix to a destination number.

Tips

You can view and operate the registered application from the **Control Panel** of this machine. However, the following conditions must be satisfied:

- The optional **Fax Kit** is not installed
- The Internet fax function is disabled

Registering applications

Register applications and configure a server for using the application.

✔ This setting is not available when the optional **Fax Kit** is installed.

1 In the administrator mode, select [Store Address] - [Application Registration] to select the location where you wish to register applications, and click [Registration/Edit].

2 Select [Use application template.] and select a template to be used.

➔ If you do not use a template, select [Not use application template].

➔ For details on template that can be used on this machine, refer to page 16-17.

3 Click [Next].

4 Register applications and configure the server settings, then click [Next].

Settings		Description
[Application Setting]		Configure an application to be registered.
	[Application Name]	Enter the application name (using up to 16 characters).
[Server Setting]		Configure a server for using the application
	[Host Address]	Enter the host address of the server for using the application (using up to 15 characters, including a period).
	[File Path]	Enter the destination file path (using up to 96 characters).
	[User ID]	Enter the user ID used to log in to the server (using up to 47 characters).
	[Password]	Enter the password of the user name you entered into [User ID] (using up to 31 characters).
	[anonymous]	When authentication is not required in the destination server, select [ON].
	[PASV Mode]	When the PASV mode is used in your environment, select [ON].
	[Proxy]	When a proxy server is used in your environment, select [ON].
	[Port No.]	If necessary, change the port number. In normal circumstances, you can use the original port number.

5 Select a custom item you wish to configure, and click [Edit].

6 In the [Function Setting] page of the selected custom item, configure the following settings.

Settings	Description
[Button Name]	Enter the button name (using up to 16 characters).
[Function Name]	Select a function name.
[Message on Panel]	Enter the name to be displayed on the **Touch Panel** (using up to 32 characters).
[Display Method]	Select a method to display on the **Touch Panel**.
[Default Value]	Enter the default value. The number of characters that can be entered differs depending on the function selected in [Function Name]. To hide the default value, select the [Input string shown as ****] check box.
[Keyboard Type]	Select a keyboard type displayed on the **Touch Panel**.
[Options]	Set the option according to the function selected in [Function Name].

7 Click [OK].

Application setting templates

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]	Not specified.
2	[Fax Number (CS)]	[Personal Fax Number]	[ASCII]	Not specified.	Not specified.
3	[TEL Number (CS)]	[Personal Voice Number]	[ASCII]	Not specified.	Not specified.
4	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
5	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.

[Fax with Account]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Sender Name (CS)]	[Name]	[ASCII]	Not specified.	Not specified.
3	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
4	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
5	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
7	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
8	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
9	[Hold For Preview]	[Hold For Preview]	Not specified.	Not specified.	[No]

[Secure Docs]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
3	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
4	[Delivery Method]	[Delivery]	Not specified.	Not specified.	[Secure]
5	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
7	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.
8	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
9	[Document PW]	[Document Password]	[ASCII]	Not specified.	Not specified.

[Certified Delivery]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
3	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
4	[Delivery Method]	[Delivery]	Not specified.	Not specified.	[Certified]
5	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
7	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.
8	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
9	[Document PW]	[Document Password]	[ASCII]	Not specified.	Not specified.

Associating with the fax server communicating in E-Mail format

When using a fax server that communicates in the E-mail format, a prefix and a suffix can be automatically added to the destination number.

In the administrator mode, select [System Settings] - [System Connection Setting] - [System Connection Setting], then configure the following settings.

Settings	Description
[Prefix/Suffix Automatic Setting]	Select whether to automatically add a prefix and suffix to a destination number. If [ON] is selected, characters set in registration No.1 are automatically added in the administrator mode [Store Address] - [Prefix/Suffix]. [OFF] is specified by default.

If [Prefix/Suffix Automatic Setting] is set to [ON], the following restrictions will be applied:

- The [Fax Settings] are not available in the administrator mode (excluding [Destination Check Display Function], [Confirm Address (TX)], [Confirm Address (Register)], [PC-Fax Permission Setting], and [PIN Code Display Mask Function]).
- [Store Address] - [Application Registration] is not available in the administrator mode.
- Bulletin Board User Box, Polling TX User Box, 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.
- The [Off-Hook] key is not available.
- You cannot configure [Fax Header Settings], [Line Setting], [Quick Memory TX], [Polling TX], [Polling RX], [Timer TX], [Password TX], and [F-Code TX] in the Scan/Fax mode.
- The network fax function is not available.
- [Outside], [Tone], [Pause], [-], and [Line Settings] are not available when registering a fax destination in the address book.
- You cannot print an activity report, TX report, and RX report from the job display screen of the **Control Panel**.
- Numbers excluding a prefix and suffix are displayed in job history.
- Send job types are handled as E-mail.
- The Fax TX in the counter is not updated.

16.12 Operating the machine Control Panel remotely

Overview

The **Control Panel** of this machine can be operated remotely from a computer on the network.

The following three methods are available for operating the **Control Panel**.

Operation procedure	Description
Using the dedicated software	This method uses the dedicated software that collects screen information of the **Control Panel** of this machine periodically, and operates the **Control Panel** from a computer on the network. You must prepare a dedicated remote control software program and server. Despite the burden, this method enables you to control the machine remotely even from a computer located outside the router network.
Accessing the machine directly	This method accesses this machine directly from another computer on the network, and operates the **Control Panel** of the machine using a Web browser. A dedicated remote control software program is not required, but the computer used for the remote control must be able to access this machine.
Using an Android/iOS terminal	This method remotely operates the **Control Panel** of this machine using an Android/iOS terminal.

Using the dedicated software

Configure the settings for operating the **Control Panel** of this machine from a computer on the network using a dedicated software program.

In the administrator mode, select [Network] - [Remote Panel Settings] - [Remote Panel Client Settings], then configure the following settings.

Settings	Description
[Client Setting]	To control the **Control Panel** of this machine remotely using the dedicated software, select [ON]. [OFF] is specified by default.
[Server Address]	Enter the address of the server where the dedicated software was installed. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
[Port Number]	If necessary, change the port number of the server where the dedicated software was installed. [443] is specified by default.
[Connection Timeout]	If necessary, change the timeout time of communication with the server where the dedicated software was installed. [60] sec. is specified by default.
[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. If you select [Confirm] at each item, the certificate is verified for each item.

Settings		Description
	[Validity Period]	Confirm whether the certificate is still valid. [Do Not Confirm] is specified by default.
	[CN]	Confirm whether CN (Common Name) of the certificate matches the server address. [Do Not Confirm] is specified by default.
	[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer. [Do Not Confirm] is specified by default.
	[Chain]	Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine. [Do Not Confirm] is specified by default.
	[Expiration Date Confirmation]	Confirm whether the certificate has expired. Confirm for expiration of the certificate in the following order. • OCSP (Online Certificate Status Protocol) service • CRL (Certificate Revocation List) [Do Not Confirm] is specified by default.
[Synchronize WebDAV Client Setting]		Select whether to use the proxy server for WebDAV transmission as a proxy server for the server where the dedicated software was installed. To use a different proxy server, select [OFF] and enter the proxy server information. [ON] is specified by default.
[Proxy Settings]		If you set the [Synchronize WebDAV Client Setting] to [OFF], register the proxy server.
	[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. • Example of host name entry: "host.example.com" • Example of IP address (IPv4) entry: "192.168.1.1" • Example of IP address (IPv6) entry: "fe80::220:6bff:fe10:2f16"
	[Proxy Server Port Number]	If necessary, change the proxy server port number. [8080] is specified by default.
	[User Name]	Enter the user name to log in to the proxy server (using up to 63 characters).
	[Password]	Enter the password of the user name you entered into [User Name] (using up to 63 characters). To enter (change) the password, select the [Password is changed.] check box, then enter a new password.

Reference

In the administrator mode, select [Security] - [Certificate Verification Settings], then configure whether to verify the certificate. The certificate is verified by default. For details, refer to page 13-7.

Accessing the machine directly

Configure the settings for accessing this machine directly from another computer on the network and operating the **Control Panel** of the machine using a Web browser.

In the administrator mode, select [Network] - [Remote Panel Settings] - [Remote Panel Server Settings], then configure the following settings.

Settings	Description
[Server Setting]	To access this machine directly and control the **Control Panel** of the machine remotely, select [ON]. [OFF] is specified by default.
[Port No.(SSL)]	If necessary, change the port number used when operating the **Control Panel** of this machine. [50443] is specified by default.

Settings	Description
[Password Authentication]	Select whether to request password entry for connecting with this machine. To request for a password entry, select [ON], and enter the password (using up to 64 characters). To enter (change) the password, select the [Password is changed.] check box, and enter the current password and new password.
[IP Filtering(Permit Access)]	Select [Enable] to specify IP addresses allowed to access. Also enter the range of IP addresses allowed to access. To allow access from a single IP address, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.

Using an Android/iOS terminal for operations

Configure communication settings to connect an Android/iOS terminal to this machine using **Remote Access** and transfer image data or operation contents of the **Control Panel**.

Tips

- To remote-control the **Control Panel** of this machine through an Android/iOS terminal using **Remote Access**, [TCP Socket] must be set to [ON] (selected) (default: [ON] (selected) by selecting [Network] - [TCP Socket Settings] in the administrator mode.
- To connect the terminal to this machine through **Remote Access** using NFC, configure a setting to enable NFC on this machine in advance. For details, refer to page 16-26.
- To connect the terminal to this machine through **Remote Access** using Bluetooth LE, configure a setting to enable Bluetooth LE on this machine in advance. For details, refer to page 16-28.

In the administrator mode, select [Network] - [bizhub Remote Access Setting], then configure the following settings.

Settings	Description
[bizhub Remote Access Setting]	Select whether to allow a connection from an Android/iOS terminal using **Remote Access**. [OFF] is specified by default.
[Connection Method]	Compresses image data of the **Control Panel** of this machine before sending it to an Android/iOS terminal. Select whether to give priority to the operation speed at an Android/iOS terminal or give priority to the image quality of the Android/iOS terminal screen when compressing images. [Standard] is specified by default.
[Connection Timeout]	If necessary, specify the timeout period to establish a communication between this machine and an Android/iOS terminal. [20] minutes is specified by default.
[Operation Change Screen]	Select whether to display the screen for checking whether to continue a remote operation on the screen of an Android/iOS terminal when the **Control Panel** of this machine has been touched while a remote operation is being performed using an Android/iOS terminal. [ON] is specified by default.
[Connection Permission Screen]	Select whether to display the screen for checking whether to allow a connection on the **Control Panel** of this machine when a remote control connection is requested from the Android/iOS terminal while you are operating the **Control Panel** of this machine. [ON] is specified by default.

Settings	Description
[Keyboard Link]	Select whether to allow text to be entered from the text entry application on the Android/iOS terminal. You can enter characters using the keyboard, handwriting, or voice input function. If [Allow] is selected, you can enter text using the text entry application on the Android/iOS terminal during panel operation. To restrict the method for connecting to this machine using Keyboard Link, select [Allow Send Operations using Touch Method only], then select the connection method to be allowed in [Touch Method]. Selecting [Allow Send Operations using Touch Method only] prohibits a connection by the "Send" key of **Remote Access**, and only allows NFC and Bluetooth LE connections. If necessary, you can specify whether to allow each of NFC and Bluetooth LE connections. [Deny] is specified by default.
[Address Link]	Select whether to allow a user to obtain the E-mail address from the address book of the Android/iOS terminal. If [Allow] is selected, you can select an address from the address book on the Android/iOS terminal and set it as the direct-input destination in fax or scan mode. To restrict the method for connecting to this machine using Address Link, select [Allow Send Operations using Touch Method only], then select the connection method to be allowed in [Touch Method]. Selecting [Allow Send Operations using Touch Method only] prohibits a connection by the "Send" key of **Remote Access**, and only allows NFC and Bluetooth LE connections. If necessary, you can specify whether to allow each of NFC and Bluetooth LE connections. [Deny] is specified by default.
[Panel Link Scan]	Select whether to enable the function that sends the image scanned on this machine to the storage of the Android terminal or Google Drive. [Deny] is specified by default.
[Priority start mode]	Select which mode is used to start **Remote Access** via NFC by placing the Android/iOS terminal on the mobile touch area on the **Control Panel**. [Panel Link] is specified by default.

16.13 Customizing the OpenAPI application key arrangement on the main menu

Overview

If the OpenAPI application is registered on this machine, the application shortcut keys registered on this machine are displayed within Registered Application List Key (default: [APP]) on the main menu.

According to your system environment, you can change the name and icon of Registered Application List Key or manage the application shortcut keys by group on the main menu.

Reference

For details on the main menu, refer to "User's Guide[Control Panel]/[Operations of Touch Panel and Explanation of Major Screens]".

Changing the name and icon of Registered Application List Key

Change the name and icon of Registered Application List Key (default: [APP]) displayed on the main menu.

In the administrator mode, select [System Settings] - [Registered Application List Setting] - [Registered Application List Setting], then configure the following settings.

Settings	Description
[Name]	Enter the Registered Application List Key name (using up to 16 characters). [APP] is specified by default.
[Change Icon]	Select whether or not to change the Registered Application List Key icon. To change an icon, select [Registration] and click [Browse], then specify the location of the image file to be used for the icon. Only a 64 × 80 dot bitmap (*.bmp) image file can be used for the icon. [OFF] is specified by default.

Managing application shortcut keys by group

If multiple OpenAPI applications are registered on this machine, the application shortcut keys to be displayed on the main menu can be managed by group.

The application shortcut keys are displayed within the group keys on the main menu, which enables easy access to the desired applications. You can register up to six groups.

1 In the administrator mode, select [System Settings] - [Registered Application List Setting] - [Registered Application Group Setting], then click [Edit] for the group to be newly registered.

2 Enter the information of the group that the application will be registered to, and click [OK].

Settings	Description
[Group Name]	Enter the group name (using up to 16 characters).
[Display Setting]	Select [Enable] to display the group keys on the main menu. [Disable] is specified by default.
[Change Icon]	Select whether or not to change the group key icons. To change an icon, select [Registration] and click [Browse], then specify the location of the image file to be used for the icon. Only a 64 × 80 dot bitmap (*.bmp) image file can be used for the icon. [OFF] is specified by default.

3 In the administrator mode, select [System Settings] - [Registered Application List Setting] - [Registered Application Join Group Setting], then select the application to be registered in the group and click [Edit].

4 Select the group that the selected application belongs to, and click [OK].

16.14 Associating this machine with an Android/iOS terminal using the QR code

Displaying network information of this machine using the QR code

Configure settings to display network information of this machine as the QR code on the screen of this machine. Also, set network information of this machine, including the QR code.

Using the QR code allows you to only read the QR code on the Android/iOS terminal to easily establish a pairing between this machine and the Android/iOS terminal.

In the administrator mode, select [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Quick Connection Setting], then configure the following settings.

Settings		Description
[QR Code Display Setting]		Select whether to display the QR code on the screen of this machine. [OFF] is specified by default.
[Wireless Connection Use Setting]		Select whether to specify a method to establish a wireless connection between an Android/iOS terminal and this machine. The information specified in this option is applied to the QR code. [Disable] is specified by default.
	[Wireless Connection Method]	Specify the method to establish a wireless connection between an Android/iOS terminal and this machine. Selecting [Individual Settings] allows you to configure detailed settings. [Use MFP Wireless Setting] is specified by default.
	[Individual Settings]	Specify the method to establish a wireless connection between an Android/iOS terminal and this machine when [Individual Settings] is selected for [Wireless Connection Method]. • [SSID]: Enter the SSID of the access point (using up to 32 bytes). • [Authentication/Encryption Algorithm]: Select the algorithm used for authentication or encryption. [No Authentication/Encryption] is specified by default. • [WEP Key]: This is required when [WEP] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the WEP key in [WEP Key Input Method], check [Change WEP Key] and enter the WEP key. • [Passphrase]: This is required when an algorithm other than [WEP] or [No Authentication/Encryption] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the passphrase in [Passphrase Input Method], check [Change Passphrase] and enter the passphrase.

Reference

A shortcut key to the QR code can be placed on the main menu. For details on the setting procedure, refer to "User's Guide[Control Panel]/[Operations of Touch Panel and Explanation of Major Screens]".

Tips

- When [Network] - [Network I/F Configuration] is set to [Wireless Only] in the administrator mode, a pairing is established by applying the wireless settings of this machine; therefore, [Wireless Connection Setting] is not displayed.

Reading the QR code to pair with an Android/iOS terminal

This section describes how to read the QR code displayed on the screen of this machine using an Android/iOS terminal and establish a pairing.

✔ Install **Mobile (for iPhone/iPad/Android)** on your Android/iOS terminal.

✔ Configure a setting to display the QR code on this machine. For details, refer to page 16-25.

1 On the **Control Panel** of this machine, tap [Utility] - [Device Information] - [QR Code Display].

➔ If the shortcut key to the QR code is placed on the main menu, you can also display the QR code from the main menu.

2 Start **Mobile (for iPhone/iPad/Android)** to read the QR code.

➔ For details on the procedure, refer to the help of **Mobile (for iPhone/iPad/Android)**.

This starts a pairing with this machine, and registers this machine in **Mobile (for iPhone/iPad/Android)**.

16.15 Associating this machine with an Android/iOS terminal using NFC

Setting network information of this machine via NFC

NFC is the standard for near-field communication that is used for connection between handheld terminals or other devices several tens of centimeters away each other.

Configure a setting to support NFC on this machine. Also, set network information of this machine required to connect an Android terminal to this machine.

Using NFC allows you to easily establish a pairing between this machine and an Android terminal simply by placing the Android terminal on the mobile touch area on the **Control Panel** of this machine.

In the administrator mode, select [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Quick Connection Setting], then configure the following settings.

Settings		Description
[NFC Use Setting]		Select whether to use NFC. [OFF] is specified by default.
[Wireless Connection Use Setting]		Select whether to specify a method to establish a wireless connection between an Android terminal and this machine. The information specified in this option is applied to the NFC tag. [Disable] is specified by default.
	[Wireless Connection Method]	Specify a method to establish a wireless connection between an Android terminal and this machine. Selecting [Individual Settings] allows you to configure detailed settings. [Use MFP Wireless Setting] is specified by default.
	[Individual Settings]	Specify the method to establish a wireless connection between an Android terminal and this machine when [Individual Settings] is selected for [Wireless Connection Method]. • [SSID]: Enter the SSID of the access point (using up to 32 bytes). • [Authentication/Encryption Algorithm]: Select the algorithm used for authentication or encryption. [No Authentication/Encryption] is specified by default. • [WEP Key]: This is required when [WEP] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the WEP key in [WEP Key Input Method], check [Change WEP Key] and enter the WEP key. • [Passphrase]: This is required when an algorithm other than [WEP] or [No Authentication/Encryption] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the passphrase in [Passphrase Input Method], check [Change Passphrase] and enter the passphrase.

Tips

- If [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Quick Connection Setting] - [NFC Use Setting] is changed to [OFF] in the administrator mode, [User Authentication/Account Track] - [General Settings] - [NFC Use Setting] is also changed to [OFF].
- When [Network] - [Network I/F Configuration] is set to [Wireless Only] in the administrator mode, a pairing is established by applying the wireless settings of this machine; therefore, [Wireless Connection Setting] is not displayed.

Connecting an Android terminal to this machine via NFC using Mobile for Android

This section describes how to establish a pairing by placing an Android terminal on the mobile touch area on the **Control Panel** of this machine.

✔ Install **Mobile for Android** on the Android terminal to enable the NFC terminal setting.

✔ Enable the wireless connection and NFC for the Android terminal.

✔ Configure a setting to support NFC on this machine. For details, refer to page 16-26.

1 Start the Android terminal.

2 Place the Android terminal on the mobile touch area on the **Control Panel** of this machine.

➔ If the Android terminal is in the sleep mode (the screen is off) or the screen is locked, cancel the sleep mode of the Android terminal, unlock the screen, then place the Android terminal on the mobile touch area.

➔ When both **Mobile for Android** and **Remote Access** are installed on the Android terminal, the application, whichever has priority, is started. For details on the setting, refer to page 16-27.

This starts a pairing with this machine, and registers this machine in **Mobile for Android**.

Tips

- For details on the procedure, refer to the help of **Mobile for Android**.
- If the printable screen such as the Web browser or E-mail screen is displayed in advance using **Mobile for Android**, you can directly print it on this machine simply by placing the Android terminal on the mobile touch area on the **Control Panel** of this machine.
- Also, if the scannable screen is displayed in advance using **Mobile for Android**, you can import the original loaded on this machine to the Android terminal simply by placing the Android terminal on the mobile touch area on the **Control Panel** of this machine.

Connecting an Android terminal to this machine via NFC using Remote Access

This section describes how to connect an Android terminal to this machine using **Remote Access** by placing the Android terminal on the mobile touch area on the **Control Panel** of this machine.

✔ On this machine, allow a connection from an Android terminal using **Remote Access**. For details, refer to page 16-22.

✔ Enable the wireless connection and NFC for the Android terminal.

✔ Configure a setting to support NFC on this machine. For details, refer to page 16-26.

✔ When using NFC to connect an Android terminal to this machine using **Remote Access**, connect the Android terminal to this machine or the access point that can be connected to this machine in advance.

1 Start the Android terminal.

2 Place the Android terminal on the mobile touch area on the **Control Panel** of this machine.

➔ If the Android terminal is in the sleep mode (the screen is off) or the screen is locked, cancel the sleep mode of the Android terminal, unlock the screen, then place the Android terminal on the mobile touch area.

➔ When both **Mobile for Android** and **Remote Access** are installed on the Android terminal, the application, whichever has priority, is started. For details on the setting, refer to page 16-27.

This starts a pairing with this machine to automatically connect the Android terminal to this machine.

Tips

- For details on the procedure, refer to the help of **Remote Access**.
- If the primary start mode is set to [Address Link] to start **Remote Access** via NFC, the Android terminal is not connected automatically. When you place the Android terminal on the mobile touch area on the **Control Panel** of this machine, network information of this machine is automatically input to **Remote Access**; therefore, you need to manually connect the Android terminal to this machine.

Configuring the application to be started on the Android terminal

If both **Mobile for Android** and **Remote Access** are installed on the Android terminal, select whether to preferentially start either application when the Android terminal is placed on the mobile touch area on the **Control Panel** of this machine.

In the administrator mode, select [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Touch Connection Link Application Settings], then click [PageScope Mobile] or [bizhub Remote Access].

[PageScope Mobile] is specified by default.

16.16 Associating this machine with an iOS terminal using Bluetooth LE

Setting network information of this machine via Bluetooth LE

The Bluetooth LE is the standard for power-saving near-field communication that is used for connection between handheld terminals or other devices several meters away each other.

Configure a setting to support Bluetooth LE on this machine. Also, set network information of this machine required to connect an iOS terminal to this machine.

Using Bluetooth LE allows you to easily establish a pairing between this machine and an iOS terminal simply by placing the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

In the administrator mode, select [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Quick Connection Setting], then configure the following settings.

Settings		Description
[Bluetooth LE Use Setting]		Select whether to use Bluetooth LE. [OFF] is specified by default.
[Wireless Connection Use Setting]		Select whether to specify a method to establish a wireless connection between an iOS terminal and this machine. [Disable] is specified by default.
	[Wireless Connection Method]	Specify a method to establish a wireless connection between an iOS terminal and this machine. Selecting [Individual Settings] allows you to configure detailed settings. [Use MFP Wireless Setting] is specified by default.
	[Individual Settings]	Specify the method to establish a wireless connection between an iOS terminal and this machine when [Individual Settings] is selected for [Wireless Connection Method]. • [SSID]: Enter the SSID of the access point (using up to 32 bytes). • [Authentication/Encryption Algorithm]: Select the algorithm used for authentication or encryption. [No Authentication/Encryption] is specified by default. • [WEP Key]: This is required when [WEP] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the WEP key in [WEP Key Input Method], check [Change WEP Key] and enter the WEP key. • [Passphrase]: This is required when an algorithm other than [WEP] or [No Authentication/Encryption] is selected in [Authentication/Encryption Algorithm]. Select the method to enter the passphrase in [Passphrase Input Method], check [Change Passphrase] and enter the passphrase.

Tips

- The optional **Local Interface Kit EK-609** is required to use this function. This setting must be configured in advance by your service representative. For details, contact your service representative.
- If [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Quick Connection Setting] - [Bluetooth LE Use Setting] is changed to [OFF] in the administrator mode, [User Authentication/Account Track] - [General Settings] - [Bluetooth LE Use Setting] is also changed to [OFF].
- When [Network] - [Network I/F Configuration] is set to [Wireless Only] in the administrator mode, a pairing is established by applying the wireless settings of this machine; therefore, [Wireless Connection Setting] is not displayed.

Connecting an iOS terminal to this machine via Bluetooth LE using Mobile for iPhone/iPad

This section describes how to connect an iOS terminal to this machine by placing the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

✔ Install **Mobile for iPhone/iPad** on the iOS terminal to enable the Bluetooth LE terminal setting.

✔ Enable the wireless connection and Bluetooth LE for iOS terminal.

✔ Configure a setting to support Bluetooth LE on this machine. For details, refer to page 16-28.

1 Start **Mobile for iPhone/iPad** on the iOS terminal to display the screen that allows you to register a device.

2 Place the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

➔ If the iOS terminal is in the sleep mode (the screen is off) or the screen is locked, cancel the sleep mode of the iOS terminal, unlock the screen, then place the iOS terminal on the mobile touch area.

This starts a pairing with this machine, and registers this machine in **Mobile for iPhone/iPad**.

Tips

- For details on the procedure, refer to the help of **Mobile for iPhone/iPad**.
- If the printable screen such as the Web browser or E-mail screen is displayed in advance using **Mobile for iPhone/iPad**, you can directly print it on this machine simply by placing the iOS terminal on the mobile touch area on the **Control Panel** of this machine.
- Also, if the scannable screen is displayed in advance using **Mobile for iPhone/iPad**, you can import the original loaded on this machine to the iOS terminal simply by placing the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

Connecting an iOS terminal to this machine via Remote Access using Bluetooth LE

This section describes how to connect an iOS terminal to this machine using **Remote Access** by placing the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

✔ On this machine, allow a connection from an iOS terminal using **Remote Access**. For details, refer to page 16-22.

✔ Enable the wireless connection and Bluetooth LE for iOS terminal.

✔ Configure a setting to support Bluetooth LE on this machine. For details, refer to page 16-28.

1 Start **Remote Access** on the iOS terminal.

2 Place the iOS terminal on the mobile touch area on the **Control Panel** of this machine.

➔ If the iOS terminal is in the sleep mode (the screen is off) or the screen is locked, cancel the sleep mode of the iOS terminal, unlock the screen, then place the iOS terminal on the mobile touch area.

This starts a pairing with this machine to automatically connect the Android terminal to this machine.

Tips

- For details on the procedure, refer to the help of **Remote Access**.

Configuring the application to be started on the iOS terminal

If both **Mobile for iPhone/iPad** and **Remote Access** are active in the background on the iOS terminal, select whether to preferentially display either application in the foreground when the iOS terminal is placed on the mobile touch area on the **Control Panel** of this machine.

In the administrator mode, select [System Settings] - [System Connection Setting] - [Mobile Connection Settings] - [Touch Connection Link Application Settings], then click [PageScope Mobile] or [bizhub Remote Access].

[PageScope Mobile] is specified by default.