KONICA MINOLTA

Giving Shape to Ideas

bizhub 4750/4050

User's Guide: Applied Functions

Table of contents

1 Using Web Connection

2 Configuring the Operating Environment of This Machine

1 Using Web Connection

1 Using Web Connection

1.1 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 easily 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	For Windows • Microsoft Internet Explorer 8 or later • Mozilla Firefox 18 or later For Mac OS • Mozilla Firefox 18 or later • Safari 5 or later For iOS • Safari 5 or later On Linux • Mozilla Firefox 18 or later

Tips

For iPhone/iPod touch, the optimized Web page is displayed.

1.2 Operations required to use this function

1.2.1 Configuring network environment settings

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**, select [Utility] - [Administrator Settings] - [Network Settings] - [TCP/IP Settings] - [IPv4 Settings], then configure the following settings.

Item	Description
[IP Address]	When manually specifying the IP address, enter the fixed IP address assigned to the machine.
[Subnet Mask]	When manually specifying the IP address, enter the subnet mask.
[Default Gateway]	When manually specifying the IP address, enter the default gateway.
[IP Application Method Auto Setting]	When automatically specifying the IP address, select the method for automatic retrieval. • [DHCP Settings]: [ON] is specified by default. • [BOOTP Settings]: [OFF] is specified by default. • [ARP/PING Settings]: [OFF] is specified by default. • [AUTO IP Settings]: Fixed to [Enable].

Confirming the IP address

Print out the Configuration Page, then check that an IP address is assigned to this machine.

To print out the Configuration Page, select [Utility] - [User Settings] - [Printer Settings] - [Print Reports] - [Configuration Page].

1.2.2 Checking Web browser settings

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 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].

Reference

For details, refer to the Help of your Web browser.

1.3 Basic usage

1.3.1 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/". To use SSL communication, enter "https://192.168.1.20/".

➔ For details on how to confirm the IP address of this machine, refer to page 1-3.

The **Web Connection** screen appears.

Tips

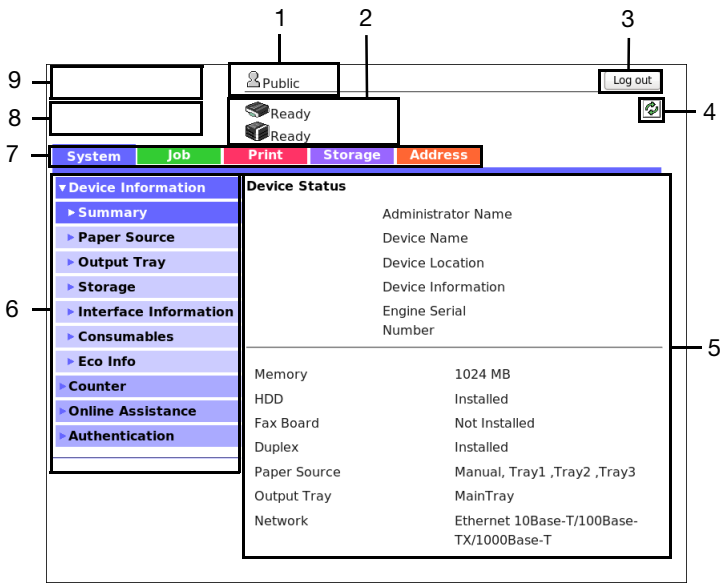
- If the WINS server is installed to resolve the name, you can gain access by specifying the host name of this machine. The host name of this machine is registered in the hosts file on the computer (C:\Windows\System32\drivers\etc\hosts), and is usually assigned by the administrator. For details, contact the machine administrator.
- If you use Internet Explorer 8/9 or a Web browser other than Internet Explorer in the IPv6 environment, enclose the IPv6 address in [ ].
  Example: When the IPv6 address of this machine is fe80::220:6bff:fe10:2f16, enter "http://[fe80::220:6bff:fe10:2f16] /".

1.3.2 Web Connection screen configuration

The **Web Connection** screen primarily consists of the following three parts.

- Top of the screen: Displays the name of the 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 [System] - [Device Information] - [Summary] to explain sections of each screen.



No.	Item	Description
1	Login user name	Displays the login mode and user name.
2	Status display	Displays the status of this machine. Displays the status of the printer and scanner sections of this machine with icons and messages. For details, refer to page 1-5.
3	[Log out]	Click this button to log out of **Web Connection**.
4	Refresh	Click this button to update the screen.
5	Information and settings	Click the menu at the left-hand side of the screen, and the contents of that menu will appear.
6	Menu	Click the category of the menu to display the menu items of that category.
7	Menu category	Menu items are divided into some categories depending on each content.
8	**Web Connection** logo	Click this logo to display the version information of **Web Connection**.
9	KONICA MINOLTA logo	Click the logo to display the KONICA MINOLTA site (http://www.konicaminolta.com/).

1.3.3 Status display

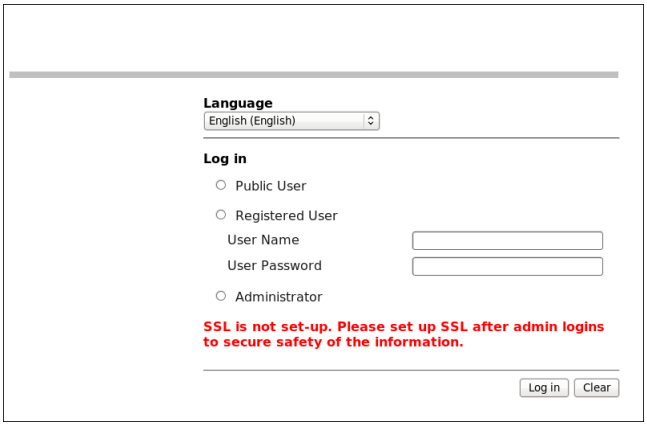
The current status of this machine is always shown at the top of the screen. The following icons represent the types of status.

Icon	Status	Description
	Ready	This machine is on-line, and ready for printing, or the machine is printing.
	Alert	You need to exercise care, however, printing can be continued.
	Error	Exercise care before printing.
	Fatal error	This machine needs to be restarted. If this error persists after restarting the machine, this machine needs to be repaired. Contact your service representative.

1.3.4 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**.



Item	Description
[Language]	Select a language to be used to display the **Web Connection**.
[Log in]	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 1-6.

Tips

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 on this Login screen.

Login mode

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

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

Login mode	Description
Administrator Mode	Enables the machine administrator 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. • [System] • [Security] • [Job] • [Print] • [Storage] • [Address] • [Network]
User mode	Enables a user such as a registered user, or public user to log in to this machine. You can check the status of this machine, check jobs, use files in the HDD, perform direct print, register an address, and other functions of this machine.

Login mode		Description
	[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. • [System] • [Job] • [Print] • [Storage] • [Address]
	[Public User]	Enables a user who is not registered on this machine to log in as a public user. If the user is not permitted to use public users on this machine, this mode is not available.

Tips

- A maximum of 100 clients can be connected at a time, including users and administrators. Also, multiple number of users and administrators can log in at a time.
- 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 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 [Log in].

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

The administrator mode window appears.

Logging in to User mode

You can log in as a registered user or public user.

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

➔ To log in as a public user, select [Public User], then click [Log in] on the Log in screen.

2 Enter the user name and password, then click [Log in].

The user mode window appears.

Tips

When an external authentication server is used, select the server.

1.4 Available operations in User mode

1.4.1 [System] tab

To display: **User mode** - [System]

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

Item		Description
[Device Information]		Enables you to confirm information such as the status of this machine and optional devices that are installed on this machine.
	[Summary]	Displays the components of this machine and the installation status of optional devices.
	[Paper Source]	Displays the status of the machine's paper tray and information about paper in the tray.
	[Output Tray]	Displays the status of the machine's output tray.
	[Storage]	Displays the capacity of the machine's HDD.
	[Interface Information]	Displays the machine's network settings.
	[Consumables]	Displays the status of the machine's consumables.
	[Eco Info]	Displays the machine's Eco Info, such as the paper saving ratio when using two-sided printing or the page combine function, or a transition of power consumption.
[Counter]		Enables you to confirm the machine's counter information.
	[Total Counter]	Displays the total number of sheets of paper printed on this machine by function.
	[Sheets Printer by Paper Size]	Displays the total number of sheets of paper that has been printed on this machine by paper size.
	[Sheets Printer by Paper Type]	Displays the total number of sheets of paper that has been printed on this machine by paper type.
[Online Assistance]		Enables you to check the online assistance about this product.
[Authentication]		Displays the authentication information of the login user. If you are logging in as a registered user, you can change the password.
	[User Password Change]	Enables you to change the password of a user who logs in to the computer.
	[Registration Information]	Enables you to view the registered information of a user who logs in to the computer.

1.4.2 [Job] tab

To display: **User mode** - [Job]

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

Item	Description
[Current jobs]	Displays the print jobs, send jobs, receive jobs, and save jobs that are currently being processed on this machine.
[Job History]	Displays the print jobs, send jobs, receive jobs, and save jobs that have been processed on this machine.
[Communication List]	Displays the communication start times or communication results of scan send jobs, fax send jobs, and fax receive jobs.

1.4.3 [Print] tab

To display: **User mode** - [Print]

Enables you to confirm the printer settings of this machine, print reports, and use the direct print function.

Item		Description
[Default Settings]		Enables you to check the printer-related setting values of this machine.
	[General Settings]	Displays the print settings that are used in common for print functions.
	[Paper Source Settings]	Displays the paper settings for each paper tray.
	[Tray Mapping Settings]	Displays the settings related to the tray mapping.
	[PCL Settings]	Displays the settings related to the PCL printing.
	[PostScript Settings]	Displays the settings related to the PS printing.
	[XPS Settings]	Displays the settings related to the XPS printing.
	[Print Quality Settings]	Displays the settings related to the image quality.
	[OOXML Settings]	Displays the settings related to OOXML printing.
	[Page Layout Settings]	Displays the settings related to the page layout.
[Font/Form]		Enables you to check the font, form and profile information saved on this machine.
	[PCL Font]	Displays the list of PCL fonts saved on this machine.
	[PostScript Font]	Displays the list of PS fonts saved on this machine.
	[Form Overlay]	Displays the list of forms saved on this machine.
[Report Types]		Prints various reports. Select the report that you want to print, and click [Print].
[Direct Print]		Prints the file on the computer by directly sending it to this machine. For details, refer to [User's Guide: Print Functions].

1.4.4 [Storage] tab

To display: **User mode** - [Storage]

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

Item	Description
[Scan to HDD]	Enables you to check, download, or delete the data saved by the Save to HDD function. For details, refer to [User's Guide: Scan Functions].
[PC-Fax]	Enables you to print, download, or delete fax documents saved by PC-Fax RX or Memory RX. For details, refer to [User's Guide: Fax Functions].

1.4.5 [Address] tab

To display: **User mode** - [Address]

Enables you to register frequently used destinations and edit the registered information.

Item	Description
[Address Book List]	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. For details, refer to page 2-25.

Item	Description
[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. For details, refer to page 2-29.
[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 information of the program that is saved on this machine. For details, refer to page 2-29.
[Subject]	Enables you to register subjects that are used when E-mails are being sent. Also, it enables you to confirm or edit the registered information of the title that is saved on this machine.
[Text]	Enables you to register body messages that are used when sending E-mails. Also, it enables you to confirm or edit the registered information of the body that is saved on this machine.

1.5 Available operations in Administrator mode

1.5.1 [System] tab

[Device Information]

To display: **Administrator mode** - [System] - [Device Information]

Enables you to confirm information such as the status of this machine and optional devices that are installed on this machine.

Item	Description
[Summary]	Displays the components of this machine and the installation status of optional devices.
[Paper Source]	Displays the status of the machine's paper tray and information about paper in the tray.
[Output Tray]	Displays the status of the machine's output tray.
[Storage]	Displays the capacity of the machine's HDD.
[Interface Information]	Displays the machine's network settings.
[Consumables]	Displays the status of the machine's consumables.
[Eco Info]	Displays the machine's Eco Info, such as the paper saving ratio when using two-sided printing or the page combine function, or a transition of power consumption.

[Counter]

To display: **Administrator mode** - [System] - [Counter]

Enables you to confirm the machine's counter information.

Item	Description
[Total Counter]	Displays the total number of sheets of paper printed on this machine by function.
[Sheets Printer by Paper Size]	Displays the total number of sheets of paper that has been printed on this machine by paper size.
[Sheets Printer by Paper Type]	Displays the total number of sheets of paper that has been printed on this machine by paper type.

[Online Assistance]

To display: **Administrator mode** - [System] - [Online Assistance]

Register the support information of the machine, such as contact information for the machine or a product support URL.

When the support information is registered, you can confirm it by selecting [System] - [Online Assistance] in user mode of **Web Connection**.

Item	Description
[Contact Name]	Enter the contact name of this machine (using up to 63 bytes).
[Contact Information]	Enter the contact information of this machine, such as the phone number or URL (using up to 127 bytes).
[Product Help URL]	Enter the Product Assistance URL of this machine (using up to 127 bytes).
[Corporate URL]	Enter the URL of the Web page for the manufacturer of this machine (using up to 127 bytes).
[Supplies and Accessories]	Enter information of the consumables supplier (using up to 127 bytes).

Item	Description
[Contact Utility Link]	Enter the URL of the Web page for the Device Management Utility (using up to 127 bytes).
[Driver URL]	If necessary, enter the URL of the location where the driver of this machine is stored (using up to 127 bytes). Enter an appropriate URL to suit your environment.

[Import/Export] - [Authentication]

To display: **Administrator mode** - [System] - [Import/Export] - [Authentication]

Enables you to import or export the authentication information that is registered on this machine in an environment where user authentication and account track are employed.

(This menu is displayed when user authentication or account track is set up on this machine.)

Item	Description
[Import]	Imports the authentication information file on a computer to this machine. Click [Browse] to select a file to import, then click [Import].
[Export]	Exports the authentication information file of this machine to a computer.
[Clear]	Deletes the registered authentication information saved on this machine.

Tips

You cannot edit the exported files.

[Import/Export] - [Address]

To display: **Administrator mode** - [System] - [Import/Export] - [Address]

Enables you to import or export the address information (address book, group, or program) registered on this machine.

Item	Description
[Import]	Imports the address information file on a computer to this machine. Click [Browse] to select a file to import, then click [Import].
[Export]	Exports the address information file of this machine to a computer.
[Clear]	Deletes the registered address information of this machine.

Tips

You cannot edit the exported files.

[Date/Time Settings] - [Manual Settings]

To display: **Administrator mode** - [System] - [Date/Time Settings] - [Manual Settings]

Manually specify the current date and time of this machine.

Item	Description
[Year]	Enter the year.
[Month]	Enter the month.
[Day]	Enter the day.
[Hour]	Enter the hour.
[Minute]	Enter the minute.
[Time Zone]	Select a time zone (time difference from world standard time) to suit your environment. [GMT] is specified by default.

[Date/Time Settings] - [Time Adjustment Settings]

To display: **Administrator mode** - [System] - [Date/Time Settings] - [Time Adjustment Settings]

Using the NTP (Network Time Protocol) server, you can 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.

Item	Description
[Time Adjustment]	To automatically adjust the date and time of this machine using the NTP server, select [Enable]. [Disable] 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 Number]	If necessary, change the NTP server port number. Normally, you can use the original port number. [123] is specified by default.
[Time Zone]	Select a time zone (time difference from world standard time) to suit your environment. [GMT] is specified by default.
[Adjustment Time]	Displays the latest date and time at which time correction was performed by connecting to the NTP server.

Tips

If time zone is specified, the standard time obtained from the server adjusted to your time zone is specified as the correction time.

[Date/Time Settings] - [Daylight Saving Time Settings]

To display: **Administrator mode** - [System] - [Date/Time Settings] - [Daylight Saving Time Settings]

Specify the daylight saving time for the current time.

Item	Description
[Daylight Saving Time]	Select [Enable] to use daylight saving time. Also enter the time to be adjusted for daylight saving time (in minutes). [Disable] is specified by default.

[Machine Settings]

To display: **Administrator mode** - [System] - [Machine Settings] - [Machine Settings]

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

Item	Description
[Device Name]	Enter the name of this machine (using up to 127 bytes). The name specified here is used as a part of the subject of Internet fax.
[Device Location]	Enter the location of this machine (using up to 127 bytes).
[Device Information]	Enter the information of this machine (using up to 127 bytes).
[Administrator Name]	Enter the machine administrator name (using up to 127 bytes).
[Administrator E-mail Address]	Enter the E-mail address of the machine administrator (using ASCII characters of up to 320 bytes).
[Do Startup Page]	Select whether or not to print the start page when this machine is turned on. [Off] is specified by default.

Item	Description
[Unit of Measure]	Select a system of units that are normally used. The default value depends on the region the machine is used in.
[Sleep Mode Time]	Change the time required to automatically change to Sleep mode after you did not operate this machine. The default value depends on the region the machine is used in.
[Low Power Time]	Change the time period before the machine status is automatically changed to Low Power mode if it is not used for the specified length of time. The default value depends on the region the machine is used in.
[Entering Power Save Mode]	When this machine receives a print job from a fax machine or computer in Power Save mode, select the timing to switch to Power Save mode after the print job has completed. • [Normal]: Switches the machine status at the time specified in [Low Power Time] or [Sleep Mode Time]. • [Immediately]: Switches to Power Save mode immediately after a print job has ended. [Immediately] is specified by default.
[Power Consumption in Sleep Mode]	Select whether or not to reduce the power consumption in Sleep mode. • [Enable]: Further reduces power consumption in Sleep mode. Select [Enable] in normal conditions. • [Disable]: Select this option if a smooth network communication is not established while [Enable] is specified. [Enable] 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. • [Power Save]: Press the **Power** key briefly to shift to Power Save mode (Low Power or Sleep mode). Hold down the Power key to turn the sub power off. • [Sub Power Off]: Press the **Power** key briefly to turn the sub power off. If the Power key is held down, Power Save mode shifts to ErP Auto Power Off mode (near the status when the main power is turned off), which offers a greater power saving effect than that in Sub Power Off mode. The default value depends on the region the machine is used in.
[Power Save Setting]	Select the type of power save mode when pressing the **Power** key on the **Control Panel**. • [Low Power]: Switches to Low Power mode. Turns off the **Touch Panel** display to reduce power use. • [Sleep]: Switches to Sleep mode. Sleep mode provides a greater power saving effect than Low Power mode. However, the time required to return to Normal mode is longer than the time required to recover from Low Power mode. [Low Power] is specified by default.
[Hide Personal Information]	Select whether or not to hide document names, in the [Job] tab. [Off] is specified by default.
[PDF/A Setting]	Select whether or not to enable PDF/A when a PDF file is saved. [Off] is specified by default.
[Adjust ADF Skew]	Specify whether to adjust the inclination of the original when scanning the original through the **ADF**. • [OFF]: Does not adjust the inclination of the original. • [ON]: Adjusts the inclination of all originals. • [Auto]: Adjusts the inclination only when the inclination of the original has been detected. [Auto] is specified by default.

[ROM Version]

To display: **Administrator mode** - [System] - [ROM Version] - [ROM Version]

Enables you to check the ROM version of this machine.

[Maintenance] - [Clear Settings]

To display: **Administrator mode** - [System] - [Maintenance] - [Clear Settings]

Initializes the network settings and system settings.

Item	Description
[System Settings]	Initializes the system settings. When this option is selected, this machine restarts automatically.
[Network Settings]	Initializes the network settings. When this option is selected, this machine restarts automatically.
[All Settings]	Initializes the all settings. When this option is selected, this machine restarts automatically.

[Maintenance] - [Reset]

To display: **Administrator mode** - [System] - [Maintenance] - [Reset]

Resets the controller.

[Notification Settings] - [Status Notification Settings]

To display: **Administrator mode** - [System] - [Notification Settings] - [Status Notification Settings]

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.

Item		Description
[IP Address]		Specify the destination IP address to send a notification of the machine status using the SNMP TRAP function. For details on how to specify the SNMP TRAP function, refer to page 1-58.
	[Notification Address]	Enter the IP address (IPv4), IP address (IPv6), or host name.
	[Port Number]	If necessary, change the port number. [162] is specified by default.
	[Community Name]	Enter the community name. [public] is specified by default.
[E-mail Address]		Specify the destination E-mail address to send the machine status via E-mail. For details on the E-mail environment settings, refer to page 2-2.
	[Notification Address]	Enter the E-mail address as a destination (using ASCII characters of up to 320 bytes).
[Alert]		Select an item to be notified automatically.

Item		Description
	[Paper Empty]	Select whether or not to send a notification when the tray is out of paper. [Enable] is specified by default.
	[Paper Jam]	Select whether or not to send a notification when a paper jam occurs. [Enable] is specified by default.
	[Maintenance]	Select whether or not to send a notification when periodic inspection is required. [Enable] is specified by default.
	[Toner Out]	Select whether or not to send a notification when toner runs out. [Enable] is specified by default.
	[Output Tray Full]	Select whether or not to send a notification when the output tray is overloaded. [Enable] is specified by default.
	[Fuser Unit End]	Select whether or not to send a notification when the finishing unit must be replaced. [Enable] is specified by default.
	[Operator Call]	Select whether or not to send a notification when an error occurs. [Enable] is specified by default.
	[Service Call]	Select whether or not to send a notification when a service call occurs. [Enable] is specified by default.
	[Job Complete]	Select whether or not to send a notification when a job is completed. [Enable] is specified by default.
	[Job Error]	Select whether or not to send a notification when a job has terminated abnormally. [Enable] is specified by default.

[Notification Settings] - [Total Counter Notification Settings]

To display: **Administrator mode** - [System] - [Notification Settings] - [Total Counter Notification Settings]

The counter information managed by this machine can be sent to the registered E-mail address. The information is useful for gaining an overall picture of the machine operating status.

Item	Description
[Model Name]	Enter a model name to be included in the notification mail message (using ASCII characters of up to 20 bytes).
[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 a destination E-mail address. Select the notification schedule for each destination.

Tips

After the setting is complete, a test notification is sent to the registered mail addresses when you click [Send Now].

[Job Log] - [Job Log Settings]

To display: **Administrator mode** - [System] - [Job Log] - [Job Log Settings]

Configure settings for obtain a job log.

Item	Description
[Job Log]	Select whether or not to obtain a job log. [Disable] is specified by default.

Item		Description
	[Accounting Log]	Select whether or not to obtain an accounting log. You can obtain information relevant to paper consumption for each user or account. [Enable] is specified by default.
	[Counting Log]	Select whether or not to obtain a counting log. You can obtain information about paper consumption and the reduction rate of paper used for printing. [Enable] is specified by default.
	[Audit Log]	Select whether or not to obtain an audit log. You can obtain user operation or job history. Your can track unauthorized actions or the leakage of information. [Enable] is specified by default.
[Overwrite Setting]		Select whether or not to allow the oldest job log to be overwritten by a new job log when the hard disk becomes full. [Do not Overwrite] is specified by default.

[Job Log] - [Create Job Log]

To display: **Administrator mode** - [System] - [Job Log] - [Create Job Log]

Creates a job log file based on the log information of this machine.

Tips

If there is a job log file that has not been downloaded since it was created, a confirmation dialog box appears, asking whether or not to delete the current job log file and create new job log file.

[Job Log] - [Download Job Log]

To display: **Administrator mode** - [System] - [Job Log] - [Download Job Log]

Downloads the job log file created in [Create Job Log].

[Job Log] - [Erase Job Log]

To display: **Administrator mode** - [System] - [Job Log] - [Erase Job Log]

Deletes a job log file on this machine.

[Sender Registration]

To display: **Administrator mode** - [System] - [Sender Registration] - [Sender Registration]

Enter the machine name, your company name (sender name) that are to be printed as sender information when faxes are transmitted (using up to 30 bytes).

Tips

To use the fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

[License Settings] - [Enabler]

To display: **Administrator mode** - [System] - [License Settings] - [Enabler]

Register the function and license code, which were obtained from the License Management Server, with this machine and enable the expansion function.

[QR Code Settings]

To display: **Administrator Mode** - [System] - [QR Code Settings]

Configure a setting to display network information of this machine, which is required to associate with a mobile terminal, as the QR code on the screen of this machine.

Item	Description
[Display Setting]	Select whether to display the QR code on the screen of this machine. [Not Display] is specified by default.
[Wireless Connection Setting]	Select whether to specify a method to establish a wireless connection between a mobile terminal and this machine. The information specified in this option is applied to the QR code. [Not Set] is specified by default.
[Wireless Connection Method]	Select whether to use the MFP wireless settings or individually specify the appropriate method to establish a wireless connection between a mobile terminal and this machine. [Use Device Wireless Setting] is specified by default.
[Individual Settings]	Specify the method to establish a wireless connection if [Individual Settings] is selected in [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. Select the algorithm that is used for authentication or encryption. [None] is specified by default. • [WEP Key]: This is required when [WEP] is selected in [Authentication/Encryption Algorithm]. In [Key Input Method], select the entry method, then enter the WEP key. • [Pass Phrase]: This is required when an algorithm other than [WEP] is selected in [Authentication/Encryption Algorithm]. In [Pass Phrase Input Method], select the entry method, then enter the passphrase.

1.5.2 [Security] tab

[Authentication] - [General Settings]

To display: **Administrator mode** - [Security] - [Authentication] - [General Settings]

Configure the setting relevant to User Authentication/Account Track.

Item	Description
[User Authentication]	Select whether or not to use user authentication. • [Device]: Select this option to use the authentication function of this machine. • [External Server]: Select this option to use an external authentication server. [Off] is specified by default.
[Public Access]	Select whether or not to permit that public users (unregistered users) to use this machine. • [Allow]: Select this option to use the authentication function of this machine. When a public user uses this machine, press [Public User] on the Login screen to log in to this machine. • [Allow (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]: Does not permit to use this machine by public users. [Allow] is specified by default.
[Ticket Hold Time (Active Directory)]	Change the retention time for a Kerberos authentication ticket if authentication is performed by Active Directory. [600] minutes is specified by default.
[Account Track]	Select whether or not to use account track. [Off] is specified by default.
[Account Track 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, select whether or not to synchronize user authentication and account track. [Synchronize] is specified by default.
[Number of Counters Assigned for Users]	When using user authentication and account track in conjunction, enter the number of counters to be assigned to the user. [500] is specified by default.
[Print without Authentication]	Select whether or not to allow print jobs that do not contain authentication information (jobs of which printing is requested without correctly configuring user authentication or account track settings in the printer driver). • [Allow]: Prints a received job as it is. • [Restrict]: Deletes a received job. [Restrict] is specified by default.
[Counter]	Click [Reset] to reset the counters for all users and all accounts.

Reference

For details on how to set the user authentication (MFP authentication), refer to page 2-31.

For details on how to set the user authentication (Active Directory), refer to page 2-33.

For details on how to set the account track, refer to page 2-34.

[Authentication] - [User List]

To display: **Administrator mode** - [Security] - [Authentication] - [User List]

(This menu is displayed when selecting [Device] or [External Server] in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [User Authentication].)

Displays the list of users registered on this machine. You can register, edit, or delete users.

To register or edit users, specify the following information.

Item	Description
[No.]	User registration number. The smallest available number that is not used is automatically assigned.
[User Name]	Enter the user name to log in to this machine (using up to 64 characters). You cannot specify a duplicate name. Also, you cannot specify [Public].
[External Server Name]	Displays the name of the authentication server when external server authentication is employed.
[E-mail Address]	Enter the user's E-mail address (using ASCII characters of up to 320 bytes).
[Password]	Enter the password to log in to this machine (using up to 64 bytes, excluding spaces and "). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Account Track Number]	Specify the department of a user by registration number of the department if the user authentication and account track functions are synchronized.
[Function Permission]	Restrict functions available to users. • [Copy]: Select whether or not to allow use of the copy function. [Allow] is specified by default. • [Scan to Network]: Select whether or not to allow use of the network TX function. [Allow] is specified by default. • [Scan to HDD]: Select whether or not to enable to save files on the HDD of this machine. [Allow] is specified by default. • [Scan to USB Memory]: Select whether or not to enable to save files on a USB memory. [Allow] is specified by default. • [Fax]: Select whether or not to allow use of the fax and Internet fax functions. [Allow] is specified by default. • [Print]: Select whether or not to allow print operations. [Allow] is specified by default. • [Manual Destination Input]: Select whether or not to allow direct input of a destination. [Allow] is specified by default. • [Web browser]: Select whether or not to allow use of the Web browser. [Allow] is specified by default.
[Output Permission (Scan)]	Select whether or not to allow color scan. [Allow] is specified by default.
[Max. Allowance Set]	Set the maximum number of pages that can be printed. • [Total]: To manage the upper limit, select this check box, then enter the maximum allowance.
[Counter]	Click [Reset] to reset the counters for the user.
[Authentication Device Settings]	Displays whether the information on the authentication device is registered.
[Limiting Access to Destinations]	Restricts destinations the user can access if necessary. For details, refer to page 2-38.

[Authentication] - [Account Track List]

To display: **Administrator mode** - [Security] - [Authentication] - [Account Track List]

(This menu is displayed when selecting [On] in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [Account Track].)

Displays the list of accounts registered on this machine. You can register, edit, or delete accounts.

To register or edit accounts, specify the following information.

Item	Description
[No.]	Account registration number. The smallest available number that is not used is automatically assigned.
[Account Name]	Enter the account name to log in to this machine (using ASCII characters of up to 8 bytes, excluding spaces and "). You cannot specify a duplicate name.
[Password]	Enter the password to log in to this machine (using ASCII characters of up to 8 bytes, excluding spaces and "). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Output Permission (Scan)]	Select whether or not to allow color scan. [Allow] is specified by default.
[Max. Allowance Set]	Set the maximum number of pages that can be printed. • [Total]: To manage the upper limit, select this check box, then enter the maximum allowance.
[Counter]	Click [Reset] to reset the counters for the account.

[Authentication] - [External Server List]

To display: **Administrator mode** - [Security] - [Authentication] - [External Server List]

(This menu is displayed when selecting [External Server] in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [User Authentication].)

Displays the list of external authentication servers registered on this machine. You can register, edit, or delete authentication servers.

To register external authentication servers, specify the following information according to the type of authentication server.

When you have selected [Active Directory]

Item	Description
[No.]	Registration number of the authentication server.
[Name]	Enter the name of your authentication server (using ASCII characters of up to 32 bytes).
[Server Type]	Displays the type of authentication server.
[Default Domain Name]	Enter the default domain name of your authentication server (using ASCII characters of up to 64 bytes).

When you have selected [NTLM]

Item	Description
[No.]	Registration number of the authentication server.
[Name]	Enter the name of your authentication server (using ASCII characters of up to 32 bytes).
[Server Type]	Select the type of authentication server from [NTLM v1] and [NTLM v2]. [NTLM v1] is specified by default.
[Default Domain Name]	Enter the default domain name of your authentication server (using ASCII characters of up to 64 bytes).

When you have selected [NDS]

Item	Description
[No.]	Registration number of the authentication server.
[Name]	Enter the name of your authentication server (using ASCII characters of up to 32 bytes).
[Server Type]	Select the type of authentication server. This machine supports [NDS over TCP/IP] only.
[Default Tree]	Enter the default NDS tree name (using ASCII characters of up to 63 bytes).
[Default Context]	Enter the default NDS context name (using ASCII characters of up to 191 bytes).

When you have selected [LDAP]

Item	Description
[No.]	Registration number of the authentication server.
[Name]	Enter the name of your authentication server (using ASCII characters of up to 32 bytes).
[Server Type]	Displays the type of authentication 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. [389] is specified by default.
[SSL]	Select whether or not to use SSL communication. [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. [636] is specified by default.
[Search Base]	Specify the starting point to search for a user (using ASCII characters of up to 255 bytes). 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.
[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. [Digest-MD5] is specified by default.
[Search Attribute]	Enter the search attribute that is used in user account search. [uid] is specified by default.

[Authentication] - [Temporarily Save Authentication Information]

To display: **Administrator** - [Security] - [Authentication] - [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]. [Enable] is specified by default.

If necessary, use [Reconnection Settings] to change the time to reconnect to the authentication server.

- [Reconnect for every login]: Connects to the authentication server when authentication is carried out on this machine. If the authentication server is in the shutdown state when 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]: Connects to the authentication server based on the time specified in [Reconnection Time] to 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.

[Authentication] - [Scan to Home Settings]

To display: **Administrator mode** - [Security] - [Authentication] - [Scan to Home Settings]

Select whether or not to enable the Scan to Home function.

[Disable] is specified by default.

[Authentication] - [Default Function Permission]

To display: **Administrator mode** - [Security] - [Authentication] - [Default Function Permission]

(This menu is displayed when selecting [External Server] in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [User Authentication].)

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.

Item	Description
[Copy]	Select whether or not to allow use of the copy function. [Allow] is specified by default.
[Scan to Network]	Select whether or not to allow use of the network TX function. [Allow] is specified by default.
[Scan to HDD]	Select whether or not to enable to save files on the HDD of this machine. [Allow] is specified by default.
[Scan to USB Memory]	Select whether or not to enable saving of files on a USB memory. [Allow] is specified by default.
[Fax]	Select whether or not to allow use of the fax and Internet fax functions. [Allow] is specified by default.
[Print]	Select whether or not to allow print operations. [Allow] is specified by default.
[Manual Destination Input]	Select whether or not to allow direct input of a destination. [Allow] is specified by default.
[Web Browser]	Select whether or not to allow use of the Web browser. [Allow] is specified by default.

[Authentication] - [Public User Registration]

To display: **Administrator mode** - [Security] - [Authentication] - [Public User Registration]

(This menu is displayed when access to this machine by public users is permitted in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [Public Access].)

Restricts functions available to public users.

Item	Description
[Function Permission]	Restrict functions available to users. • [Copy]: Select whether or not to allow use of the copy function. [Allow] is specified by default. • [Scan to Network]: Select whether or not to allow use of the network TX function. [Allow] is specified by default. • [Scan to HDD]: Select whether or not to enable to save files on the HDD of this machine. [Allow] is specified by default. • [Scan to USB Memory]: Select whether or not to enable to save files on a USB memory. [Allow] is specified by default. • [Fax]: Select whether or not to allow use of the fax and Internet fax functions. [Allow] is specified by default. • [Print]: Select whether or not to allow print operations. [Allow] is specified by default. • [Manual Destination Input]: Select whether or not to allow direct input of a destination. [Allow] is specified by default. • [Web browser]: Select whether or not to allow use of the Web browser. [Allow] is specified by default.
[Output Permission (Scan)]	Select whether or not to allow color scan. [Allow] is specified by default.
[Limiting Access to Destinations]	Restricts destinations the user can access if necessary. For details, refer to page 2-38.

[ID & Print Settings]

To display: **Administrator mode** - [Security] - [ID & Print Settings] - [ID & Print Settings]

(This menu is displayed when selecting [Device] or [External Server] in **Administrator mode** - [Security] - [Authentication] - [General Settings] - [User Authentication].)

Specify the operations of the ID & Print function.

Item	Description
[ID & Print]	Select whether or not to handle jobs normally printed from the printer driver as ID & Print jobs. • [Enable]: Jobs that are normally printed are handled as ID & Print jobs. • [Disable]: Only jobs for which ID & Print is set are handled as ID & Print jobs. [Disable] is specified by default.
[Public User]	Select the processing method to perform when a public user job is received. • [Print Immediately]: Prints the job without saving it on the HDD. • [Save]: Saves to the HDD. [Save] is specified by default.
[Default Operation Selection]	Select the default value for the operation that is performed after the authentication process is carried out on the login screen. • [Begin Printing]: 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 Basic Screen]: Log in to this machine. The ID & Print job is not executed. [Begin Printing] is specified by default.

[Authentication Device Settings] - [General Settings]

To display: **Administrator mode** - [Security] - [Authentication Device Settings] - [General Settings]

(This menu is displayed when this machine is equipped with the optional **Authentication Device** and when the loadable driver is installed on this machine.)

Configure the setting relevant to IC card authentication.

Item	Description
[Authentication Type]	Select how to log in to this machine. • [Card Authentication]: Allows the user to log in by simply placing the IC card. • [Card Authentication+Password]: Allows the user to log in by placing the IC card and entering the password. [None] is specified by default.
[IC Card Type]	Select the type of the IC card to be used. [Type A] is specified by default.

Tips

If this menu is changed, the card information saved on this machine is deleted.

[FeliCa (SSFC) Settings]

To display: **Administrator Mode** - [Security] - [Authentication Device Settings] - [FeliCa (SSFC) Settings]

When FeliCa (SSFC) is used for IC card authentication, configure FeliCa (SSFC) settings.

(This menu is displayed if the loadable driver installed on this machine supports FeliCa (SSFC).)

Item	Description
[Room Code]	Enter the room code. [0000] is specified by default.
[Floor Code]	Enter the floor code. [0000] is specified by default.
[Building Code]	Enter the building code. [0000] is specified by default.
[Area Code]	Enter the area code. [0000] is specified by default.
[Security Level]	Enter the security level. [0000] is specified by default.
[Company Identification Code]	Enter the company identification code. Up to 10 company identification codes can be registered. [00000000000000000000] is specified by default.
[Company Code]	Enter the company code.

[HID (iCLASS) Settings]

To display: **Administrator Mode** - [Security] - [Authentication Device Settings] - [HID (iCLASS) Settings]

When HID (iCLASS) is used for IC card authentication, configure HID (iCLASS) settings.

(This menu is displayed if the loadable driver installed on this machine supports HID (iCLASS).)

Item	Description
[ID Length]	Enter the ID length of the key to be used for access. [8] is specified by default.

Tips

If this menu is changed, the card information saved on this machine is deleted.

[PKI Settings] - [Device Certificate]

To display: **Administrator mode** - [Security] - [PKI Settings] - [Device Certificate]

You can self-create a new certificate of this machine or install a certificate issued by the Certificate Authority (CA).

For details, refer to page 2-35.

[PKI Settings] - [SSL/TLS Settings]

To display: **Administrator mode** - [Security] - [PKI Settings] - [SSL/TLS Settings]

Select whether or not to enable SSL communication. Also select the SSL encryption strength.

Item	Description
[SSL/TLS]	Select whether or not to enable SSL communication. [Disable] is specified by default.
[Encryption Strength]	Select the SSL encryption strength. Select the appropriate strength to suit your environment. [AES-256, 3DES, RC4-128] is specified by default.
[SSL/TLS Version]	Select the version of the SSL to be used. Select the appropriate version to suit your environment.

[PKI Settings] - [Protocol Settings]

To display: **Administrator mode** - [Security] - [PKI Settings] - [Protocol Settings]

This machine can manage multiple certificates and use different certificates depending on the application (protocol). Select a certificate that is used for the protocol.

To use [IEEE802.1X]

Item	Description
[Protocol]	[IEEE802.1X]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [S/MIME]

Item	Description
[Protocol]	[S/MIME]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [HTTP Server]

Item	Description
[Protocol]	[HTTP Server]
[Device Certificate]	Select the certificate to be used.

To use [E-mail Send (SMTP)]

Item	Description
[Protocol]	[E-mail Send (SMTP)]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [E-mail Receive (POP)]

Item	Description
[Protocol]	[E-mail Receive (POP)]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [TCP Socket]

Item	Description
[Protocol]	[TCP Socket]
[Device Certificate]	Select the certificate to be used.

To use [LDAP]

Item	Description
[Protocol]	[LDAP]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [WebDAV Client]

Item	Description
[Protocol]	[WebDAV Client]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [OpenAPI]

Item	Description
[Protocol]	[OpenAPI]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default. • [Client Certificate]: Select whether or not to request a certificate from clients that connect to this machine. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [Web Service]

Item	Description
[Protocol]	[Web Service]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default. • [Client Certificate]: Select whether or not to request a certificate from clients that connect to this machine. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [IPsec]

Item	Description
[Protocol]	[IPsec]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

To use [ThinPrint]

Item	Description
[Protocol]	[ThinPrint]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

Tips

An optional **i-Option LK-111** is required to use the ThinPrint function.

To use [HTTP Client]

Item	Description
[Protocol]	[HTTP Client]
[Certificate Verification Settings]	To verify the certificate, select items to be verified. If you select [Enable] at each item, the certificate is verified for each item. • [Validity Period]: Check whether or not the certificate is within the validity period. [Enable] is specified by default. • [CN]: Check whether or not CN (Common Name) of the certificate matches the server address. [Disable] is specified by default. • [Chain]: Check whether or not there is any problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates that are managed on this machine. [Disable] is specified by default. • [Key Usage]: Check whether or not the certificate is used according to the intended purpose approved by the certificate issuer. [Disable] is specified by default. • [Check CRL Expiration]: Check whether or not the certificate has expired with CRL (Certificate Revocation List). [Disable] is specified by default. • [Check OCSP Expiration]: Check whether or not the certificate has expired with the OCSP (Online Certificate Status Protocol) service. [Disable] is specified by default.
[Device Certificate]	Select the certificate to be used.

[PKI Settings] - [External Certificate]

To display: **Administrator mode** - [Security] - [PKI Settings] - [External Certificate]

Displays the list of external certificates registered on this machine.

Click [New Registration] to register a new external certificate to this machine.

Item	Description
[Certification Type]	Select a type of new external certificate to be registered. • [Trusted Root Certification Authorities]: Register the certificate of the CA that issued the certificate. • [Trusted Intermediate Certification Authorities]: Register the trusted certificate of the intermediate CA. • [Trusted Certificate]: Register the trusted certificate individually. • [Untrusted Certificate]: Register the untrusted certificate individually.
[File]	Click [Browse], and specify the location of the external certificate to be registered.

[PKI Settings] - [Validate Certificate]

To display: **Administrator mode** - [Security] - [PKI Settings] - [Validate Certificate]

You can configure the settings for verifying reliability of the certificate (expiration date, CN, key usage, etc.) for the peers.

Item		Description
[Certificate Verification Settings]		Configure the certificate verification settings.
	[Certificate Verification]	Select whether or not to verify the reliability of the certificate for a peer. [Enable] is specified by default.
	[Timeout]	Change the time-out time of certificate expiration confirmation. [30] sec. is specified by default.
	[OCSP Service]	Select whether or not to use the OCSP service. Using the Online Certificate Status Protocol (OCSP) service, you can check online to find whether or not the certificate has expired. [Disable] is specified by default.
	[URL]	To use the OCSP service, enter the URL of the OCSP service (using up to 511 bytes). If [URL] is left blank, the URL of the OCSP service embedded in the certificate will be used.
[Proxy Settings]		When confirming the expiration date via a proxy server, register the currently used proxy server.
	[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 ASCII characters of up to 63 bytes).
	[Password]	Enter the password (using ASCII characters of up to 63 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[No Proxy for following domain]	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"

[IPsec]

The IPsec technology prevents the falsification or leakage of data on the IP packet basis using encryption technology.

Configure the settings if IPsec is installed in your environment.

1 In the administrator mode, select [Security] - [IPsec] - [IPsec], then click [Edit] in [IPsec Settings].

The [IPsec Settings] screen appears.

2 Click [Edit] from [IKEv1] or [IKEv2] on the [IPsec Settings] screen, then configure the following settings.

Item	Description
[Encryption Algorithm]	Select the encryption algorithm used for generating a common key used in communication.
[Authentication Algorithm]	Select the authentication algorithm used for generating a common key used in communication.
[Encryption Key Validity Period]	Enter a validation period of a common key used for encrypted communication. When this period has expired, a new key is created. This can secure the communication. [28800] sec. is specified by default.
[Diffie-Hellman Group]	Select the Diffie-Hellman group. [Group2] is specified by default.
[Negotiation Mode]	Select the method to securely generate a common key used for encrypted communication. This is required when [IKEv1] is selected on the [IPsec Settings] screen. [Main Mode] is selected by default.

3 Click [Edit] from [SA] on the [IPsec Settings] screen, then register the Security Association (SA).

➔ Up to 10 groups can be registered for the [SA].

Item	Description
[Name]	Enter the SA name (using up to 10 characters).
[Encapsulation Mode]	Select an IPsec operation mode. [Transport] is specified by default.
[Security Protocol]	Select a security protocol. [AH] is specified by default.
[Key Exchange Method]	Select the key replacement method to securely create a common key used to encrypt communications. [IKEv1] is specified by default.
[Tunnel End Point]	Enter the IP address of the peer's IPsec gateway. This is required when [Tunnel] is selected in [Encapsulation Mode].
[IKE Settings]	Configure IKE settings used for this SA. This is required when [IKEv1] or [IKEv2] is selected in [Key Exchange Method].
[Authentication Method]	Select an authentication method. [Pre-Shared Key] is specified by default.
[Replay Detection]	Select whether or not to protect from replay attacks. [Disable] is specified by default.
[ESN]	If you select [Enable] for [Replay Detection], select whether or not to apply extended sequence numbering for IPsec communication. [Disable] is specified by default.
[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. This option is available when [IKEv2] is selected on the [IPsec Settings] screen.
[Diffie-Hellman Group]	Select the Diffie-Hellman group. [Group2] is specified by default.
[Lifetime After Establishing SA]	Enter the lifetime of a common key used to encrypt communications. [3600] sec. is specified by default.

Item		Description
[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]	If you select [ESP] for [Security Protocol], select the algorithm to be used for encryption. If you select [AES_CBC] for [Encryption Algorithm], specify the [Key Length].
	[Authentication Algorithm]	Select the algorithm to be used for authentication. If you select [SHA2] for [Authentication Algorithm], specify the [Key Length].
	[SA Index]	Specify the SA Security Parameter Index to be added to the IPsec header. You can specify different security parameter indexes respectively for send and receive.
	[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] on the [IPsec Settings] screen, click [Edit] and register peers of this machine.

➔ Up to 10 [Peer] can be registered.

Item	Description
[Name]	Enter a peer name (using up to 10 characters).
[Set IP Address]	Select the method to specify the peer address. Specify the IP address of the peer depending on the selected method.
[Pre-Shared Key Text]	Enter the Pre-Shared Key text to be shared with the peer (using ASCII characters of up to 128 bytes). To enter text in HEX code, select the [HEX Format] check box, then enter the text. 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 ASCII characters of up to 128 bytes).

5 From [Protocol Setting] on the [IPsec Settings] screen, click [Edit] and specify the protocol used for IPsec communication.

➔ In [Protocol Setting], up to 10 items can be registered.

Item	Description
[Name]	Enter the protocol name (using up to 10 characters).
[Protocol Identification Setting]	Select a protocol used for IPsec communication.
[Port No.]	If [TCP] or [UDP] has been selected in [Protocol Identification Setting], specify the port number used for IPsec communication.

6 Click [Apply], and close the [IPsec Settings] screen.

7 In the Administrator mode, select [Security] - [IPsec] - [IPsec] - [General Settings], then configure the following settings.

Item	Description
[IPsec]	Select whether or not to enable IPsec. [Disable] is specified by default.
[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. [60] is specified by default.
[Cookies]	Select whether or not to enable the defense using Cookies against denial-of-service attacks. [Disable] is specified by default.
[ICMP Pass]	Select whether or not 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. [Enable] is specified by default.
[ICMPv6 Pass]	Select whether or not 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. [Enable] is specified by default.
[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. [Allow] is specified by default.

8 From [IPsec Policy] on [IPsec] screen, click [Edit], then configure the following settings.

Item	Description
[Name]	Enter a name for the IPsec policy (using up to 10 characters).
[Peer]	Select a peer setting. Select the setting from those registered in [Peer] on the [IPsec Settings] screen.
[Protocol Setting]	Select an appropriate protocol. Select the setting from those registered in [Protocol Setting] on the [IPsec Settings] screen.
[SA]	Select a peer setting. Select the setting from those registered in [SA] on the [IPsec Settings] screen.
[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. • [Refuse]: Refuse the IP packets that met the conditions.

9 In the administrator mode, select [Security] - [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].

[IP Address Filtering]

To display: **Administrator mode** - [Security] - [IP Address Filtering]

You can specify both IP addresses that are permitted to access this machine and those that are refused access to the machine.

Item	Description
[Access Permission Address]	Select [Enable] to specify IP addresses that are permitted to access. Also enter the range of IP addresses permitted to access. If a single IP address is permitted to access, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.
[Access Refuse Address]	Select [Enable] to specify IP addresses refused to access. Also enter the range of IP addresses. If a single IP address is refused to access, you can only enter the address in one side of the range. • Example of entry: "192.168.1.1" [Disable] is specified by default.
[Exclusion Protocol]	Select the check box for the protocol that you want to exclude from access restriction using the IP address filtering. [OFF] (not selected) is specified by default.

Tips

- IP address filtering is not supported in the IPv6 environment.
- When the quick IP filtering function is enabled, IP address filtering cannot be set.

[IEEE802.1X]

To display: **Administrator mode** - [Security] - [IEEE802.1X]

Using IEEE802.1X authentication, you can connect devices that are only authorized by administrators to the LAN environment.

If IEEE802.1X authentication is installed in your environment, configure the following settings.

Item	Description
[IEEE802.1X]	Select [Enable] to use the IEEE802.1X authentication. [Disable] is specified by default.
[EAP Type]	Select an EAP authentication method. • [Server Specification]: 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 that is provided by the authentication server. • Do not select [None]. [None] is specified by default.
[User ID]	Enter the user ID (using ASCII characters of up to 128 bytes). This user ID is used for all EAP types.
[Password]	Enter the password (using ASCII characters of up to 128 bytes). The password is used for all EAP types other than [EAP-TLS]. To enter (change) the password, select the [Change Password] check box, then enter a new password.
[TTLS Anonymous Name]	Enter the anonymous name used for EAP-TTLS authentication (using ASCII characters of up to 128 bytes) if [EAP Type] is set to [EAP-TTLS] or [Server Specification]. [anonymous] is specified by default.
[TTLS Authentication Type]	Select an internal authentication protocol for EAP-TTLS if [EAP Type] is set to [EAP-TTLS] or [Server Specification]. [MS-CHAPv2] is specified by default.

Item	Description
[Send Client Certificate]	Select whether or not 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-TTLS], [PEAP], or [Server Specification] is selected from [EAP Type].
[Server ID]	To verify CN of the certificate, enter the server ID (using ASCII characters of up to 64 bytes).
[Encryption Strength]	If [EAP-TLS], [EAP-TTLS], [PEAP], or [Server Specification] is selected from [EAP Type], select an encryption strength for encryption by TLS, if necessary. • [Medium]: 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. [Medium] is specified by default.
[Network Stop]	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, set [Network Stop] to [Enable], and enter the delay (sec.) in [Limit Time]. To restart the authentication process after network communication stopped, reboot this machine. [Disable] is specified by default.

[Limiting Access to Destination] - [Restrict User Access]

To display: **Administrator mode** - [Security] - [Limiting Access to Destination] - [Restrict User Access]

Specify the functions for which user operation is restricted.

Item	Description
[Registering and Changing Addresses]	Select whether or not to allow the user to register or change destinations. [Allow] is specified by default.

[Auto Logout]

To display: **Administrator mode** - [Security] - [Auto Logout] - [Auto Logout]

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.

Item	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.

[Administrator Password]

To display: **Administrator mode** - [Security] - [Administrator Password] - [Administrator Password]

(This menu is displayed when [SSL/TLS] is set to [Enable] in **Administrator mode** - [Security] - [PKI Settings] - [SSL/TLS Settings] and a connection is established via HTTPS.)

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

Item	Description
[Current Password]	Enter the current administrator password (using up to 8 characters).
[New Password]	Enter a new administrator password (using up to 8 characters).
[Retype New Password]	Retype the new administrator password for confirmation (using up to 8 characters).

Tips

When [Password Rules] is enabled, you cannot specify a password of which the length is less than the minimum number of characters specified in [Password Rules].

[Address Reference Settings] - [Reference Allowed Group List]

To display: **Administrator** - [Security] - [Address Reference Settings] - [Reference Allowed Group List]

Click [Edit] to register a reference allowed group.

Item	Description
[No.]	Displays the registration number of a reference allowed group.
[Reference Allowed Group Name]	Enter the name of the reference allowed group (using up to 24 characters).
[Access Allowed Level]	To manage the address book in a combination comprising the reference allowed level and the reference allowed group, select the reference allowed level of the reference allowed group.

Reference

The reference allowed level can be set to the reference allowed group. You can assign the reference allowed group with the reference allowed level specified in the address book and combine the reference allowed level with the reference allowed group to manage registered destinations. For details, refer to page 2-38.

1.5.3 [Job] tab

[Current jobs]

To display: **Administrator mode** - [Job] - [Current jobs]

Displays the print jobs, send jobs, receive jobs, and save jobs that are currently being processed on this machine.

Item	Description
[No.]	Displays the ID No. of the job.
[User Name]	Displays the user name of the job.
[Document Name]	Displays the name of the job.
[Status]	Displays the current status of the job.
[Time Stored]	Displays the time by which the job is registered.
[Delete]	Deletes the selected job.

[Job History]

To display: **Administrator mode** - [Job] - [Job History]

Displays the print jobs, send jobs, receive jobs, and save jobs that have been processed on this machine.

Item	Description
[No.]	Displays the ID No. of the job.
[User Name]	Displays the user name of the job.
[Document Name]	Displays the name of the job.
[Result]	Displays the execution result of the job.
[Detail]	Displays the detailed information of the job.

[Communication List]

To display: **Administrator mode** - [Job] - [Communication List]

Displays the communication start times or communication results of scan send jobs, fax send jobs, and fax receive jobs.

Item	Description
[No.]	Displays the communication ID.
[Destination]	Displays the communication destination.
[Start Time]	Displays the transmission start time of the job.
[Result]	Displays the execution result of the job.
[Detail]	Displays the detailed information of the job.

1.5.4 [Print] tab

[Default Settings] - [General Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [General Settings]

Configure the paper and paper tray settings used for printing, and the setting on printing condition if no setting is specified by the printer driver.

Item	Description
[PDL]	Select the Page Description Language. When you select [Auto], this machine automatically switches between PCL and PS. [Auto] is specified by default.
[Paper Source]	Select the paper tray for the printing paper. [Tray 1] is specified by default.
[Duplex]	Select whether or not to print an original on both sides of paper when data containing multiple pages is printed. [Off] is specified by default.
[Binding Position]	Select the binding position for 2-sided printing. [Left Bind] is selected by default.
[Staple]	Select whether or not to staple printed sheets. This function is available when the optional **Finisher** is installed. [Off] is specified by default.
[Output Tray]	Displays the primary output tray.
[Copies]	Enter the number of copies to be printed. [1] is specified by default.
[Paper Size]	Select the size of paper for printing. The default value depends on the region the machine is used in.
[Width] / [Length]	When you have selected [Custom Size] in [Paper Size], enter the width and length of the paper.

Item	Description
[Paper Type]	Select the paper type used for printing. [Plain Paper] is specified by default.
[Collate]	When printing multiple sets of copies, select whether to make prints on a set basis. [Off] is specified by default.
[Auto Continue]	Select whether or not to continue printing when the paper size and type of the print job are different from that of the paper loaded in the paper tray. [Off] is specified by default.
[Hold Job Timeout]	Specify the time period during which a print job is stored in the HDD. [Disabled] is specified by default.
[Original Direction]	Select the orientation of the image to be printed. [Portrait] is specified by default.
[Minimal Print]	Select whether or not to slightly reduce the full page size when directly printing a PDF, PPML, or OOXML (docx, xlsx, or pptx) file. This function is available when printing the entire original image, including its edges. [Off] is specified by default.
[TIFF Auto Paper Select]	Specify the method for determining the paper to be used when a TIFF, JPEG, or PDF file is directly printed. • [Auto]: Prints on paper that matches the image size. • [Priority Paper Size]: Prints on the primary paper size. [Priority Paper Size] is specified by default.

[Default Settings] - [Paper Source Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [Paper Source Settings]

Configure the settings on the paper tray. This machine operates according to these settings unless the printer driver specifies the print settings.

Item	Description
[Manual]	Specify the size and type of the paper loaded in the bypass tray. • [Paper Size]: When loading a standard size paper, select the paper size. • [Width]/[Length]: When you have selected [Custom Size] in [Paper Size], enter the width and length of the paper. • [Paper Type]: Select the type of the paper loaded in the tray.
[Tray 1]	Specify the size and type of the paper loaded in tray 1. • [Paper Size]: When loading a standard size paper, select the paper size. • [Paper Type]: Select the type of the paper loaded in the tray.
[Tray 2]	Specify the size and type of paper loaded in tray 2. • [Paper Size]: Displays the size of the loaded paper. • [Paper Type]: Select the type of the paper loaded in the tray.
[Tray 3]	Specify the size and type of paper loaded in tray 3. • [Paper Size]: Displays the size of the loaded paper. • [Paper Type]: Select the type of the paper loaded in the tray.
[Tray 4]	Specify the size and type of the paper loaded in Tray 4. • [Paper Size]: Displays the size of the loaded paper. • [Paper Type]: Select the type of the paper loaded in the tray.
[Tray Chaining]	When the paper tray has become empty during printing, select whether or not to enable automatic switching to the paper tray that contains paper of the same size, orientation and type. [Enable] is specified by default.

Tips

[Tray 2], [Tray 3], and [Tray 4] are available when the optional **Paper Feed Unit** is installed.

[Default Settings] - [Tray Mapping Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [Tray Mapping Settings]

Specify the paper tray to be used for printing when a print job is received by the printer driver of other companies.

Item	Description
[Tray Mapping Mode]	Select whether or not to enable the tray mapping. [Off] is specified by default.
[Logical Tray 0] to [Logical Tray 9]	Assigns logical trays 0 to 9 to physical trays.

[Default Settings] - [PCL Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [PCL Settings]

Configure the PCL settings.

Item		Description
[PCL Settings]		Specify the default values for PCL printing.
	[Font Number]	Specify the default font. The displayed font number corresponds to the PCL font list. [0] is specified by default.
	[Symbol Set]	Select the font symbol set to be used. [PC-8] is specified by default.
	[Lines Per page]	Enter the number of lines of text data to be printed on one page. The default value depends on the region the machine is used in.
	[Font Point Size]	Enter the font size (in points) for proportional fonts (with different widths for each character). [12.00] is specified by default.
	[Font Pitch Size]	Enter the font width (in pitches) for typewriter fonts (with the same width for each character). [10.00] is specified by default.
	[CR/LF Mapping]	Select whether or not to replace the line feed codes when printing text data. When you want to replace the line feed codes, select the replacement method. [CR=CR LF=LF] is selected by default.

[Default Settings] - [PostScript Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [PostScript Settings]

Configure the PostScript print settings.

Item		Description
[PostScript Settings]		Specify the default values for PostScript print settings.
	[Wait Timeout]	Specify the time-out period after it is judged as PS error. If you select [0], time-out will not work. [0] sec. is specified by default.
	[PS Protocol]	Select the protocol that is used for PS data communication. If you select [Auto], an appropriate protocol is automatically determined from the PS print jobs. [Auto] is specified by default.
	[Print to PS Error]	Select whether or not to print error information when an error occurs during PS rasterization. [Off] is specified by default.

[Default Settings] - [XPS Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [XPS Settings]

Specify whether or not to perform the verification of a digital signature or printing of error information when directly printing an XPS file.

Item	Description
[Digital Signature]	Select whether or not to verify a digital signature when an XPS file with a digital signature is printed. When [Enable] is selected, the data is not printed if the signature is invalid. [Disable] is specified by default.
[Print to XPS Error]	Select whether or not to print error information when an error occurs when an XPS file is being printed. [On] is specified by default.

[Default Settings] - [Print Quality Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [Print Quality Settings]

Adjust the image quality of the printed image.

Item		Description
[Print Quality Settings]		Specify the default value for image quality.
	[Brightness]	Adjust the brightness of the printed image. [0] is specified by default.
	[Contrast]	Adjust the shading of a printed image. [0] is specified by default.
	[Halftone]	Select the half-tone image processing method for each of [Image Printing], [Text Printing], and [Graphics Printing] categories. • [Line Art]: Intermediate colors are reproduced with high precision. • [Detail]: Intermediate colors are reproduced with precision. • [Smooth]: Intermediate colors are reproduced smoothly. The following shows the default settings. • [Image Printing]: [Detail] • [Text Printing]: [Line Art] • [Graphics Printing]: [Detail]
	[Edge Enhancement]	Select whether or not to sharpen the edges for each of [Image Printing], [Text Printing], and [Graphics Printing] categories. The following shows the default settings. • [Image Printing]: [Off] • [Text Printing]: [On] • [Graphics Printing]: [On]
	[Edge Strength]	Select the degree of edge enhancement when sharpening the edges. [Middle] is specified by default.
	[Economy Print Mode]	Select whether or not to adjust the printing density in order to save the amount of toner consumed. [Off] is specified by default.
[Calibration Settings]		Adjust the printing quality.
	[Tone Calibration]	Select whether or not to enable the density adjustment. [On] is specified by default.
	[Density]	Adjust the density of black in highlight portions, intermediate portions, and shadow portions. [0] is specified by default in every case.

[Default Settings] - [OOXML Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [OOXML Settings]

Configure the default print settings when directly printing OOXML (docx, xlsx, pptx) files.

Item	Description
[Print Mode]	Select whether to give priority to either the image quality or speed when directly printing of an OOXML (docx, xlsx, or pptx) file is carried out. [Speed] is specified by default.
[Sheet/Book Print]	Select whether to print the currently selected sheet or the entire book when handling an Excel file. The [Sheet] is specified by 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. [Plain Paper] is specified by default.

[Default Settings] - [Page Layout Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [Page Layout Settings]

Configure the default combination settings for direct printing.

Item	Description
[Page Layout]	Select [Enable] to reduce multiple pages onto one sheet for printing. [Disable] is specified by default.
[Row]	Enter a number of pages to be placed in a horizontal orientation. [1] is specified by default.
[Column]	Enter a number of pages to be placed in a vertical orientation. [1] is specified by default.
[Combination Method]	Select a method to arrange pages. [Horizontal] is specified by default.
[Combination Orientation]	Select a direction of page layout. [Top Left to Bottom Right] is specified by default.
[Space]	Enter the page space in the row and column directions. [0] mm is specified by default in every case.
[Margin]	Enter page margins at the top, bottom, right, and left sides. [0] mm is specified by default in every case.
[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.
[Frame]	Select whether or not to print a border line between pages. [Disable] is specified by default.

[Default Settings] - [Barcode Settings]

To display: **Administrator mode** - [Print] - [Default Settings] - [Barcode Settings]

Configure the bar code font settings.

Item	Description
[Width of the Bar]	Specify the line width for bar code font. [0] is specified by default.
[Width of the Space]	Specify the space width for bar code font. [0] is specified by default.

Tips

An optional **i-Option LK-106** is required to use the bar code font.

[Font/Form]

To display: **Administrator mode** - [Print] - [Font/Form]

Enables you to check the font, form and profile information saved on this machine.

Item	Description
[PCL Font]	Displays the list of PCL fonts saved on this machine.
[PostScript Font]	Displays the list of PS fonts saved on this machine.
[Form Overlay]	Displays the list of forms saved on this machine.

[Download Font/Form]

To display: **Administrator mode** - [Print] - [Download Font/Form]

Manage the fonts, forms and profiles that are saved on the HDD of this machine.

Item		Description
[PostScript Font]		Manage the PostScript fonts.
	[Download PostScript Font]	Download PostScript fonts to the HDD of this machine. Specify the storage location and the font to be downloaded, and click [Download].
	[Delete PostScript Font]	Delete the PostScript fonts that are saved on the HDD of this machine. In the list of PostScript fonts, select the check box of the font you want to delete, and click [Delete].
[Form Overlay]		Manage the forms.
	[Download Form Overlay]	Download forms to the HDD of this machine. Specify the storage location and the form to be downloaded, and click [Download].
	[Delete Form Overlay]	Delete the forms that are saved on the HDD of this machine. In the list of forms, select the check box of the form you want to delete, and click [Delete].

[Report Types]

To display: **Administrator mode** - [Print] - [Report Types] - [Report Types]

Prints various reports. Select the report that you want to print, and click [Print].

Item	Description
[Configuration Page]	Prints a list that contains information and settings of this machine.
[PCL Font Page]	Prints the PCL font list.
[PostScript Font Page]	Prints the PostScript font list.
[Statistics Page]	Prints a list that contains statistics information, such as the number of pages printed.
[Directory Listing Page]	Prints a list of HDD directories.

[Direct Print]

To display: **Administrator mode** - [Print] - [Direct Print] - [Direct Print]

Prints the file on the computer by directly sending it to this machine.

For details, refer to Chapter 4 "Printing without Using the Printer Driver" in [User's Guide: Print Functions].

1.5.5 [Storage] tab

[Scan to HDD]

To display: **Administrator mode** - [Storage] - [Scan to HDD]

Enables you to check, download, or delete the data saved by the Save to HDD function.

For details, refer to Chapter 6 "Saving a file in the HDD of this Machine (Save to HDD)" in [User's Guide: Scan Functions].

[PC-Fax]

To display: **Administrator mode** - [Storage] - [PC-Fax]

Enables you to print, download, or delete fax documents saved by PC-Fax RX or Memory RX.

For details, refer to Chapter 6 "Receiving Options" in [User's Guide: Fax Functions].

1.5.6 [Address] tab

[Address Book]

To display: **Administrator mode** - [Address] - [Address Book] - [Address Book List]

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.

To register an address, click [New Registration]. For details on registration information, refer to page 2-25.

[Group]

To display: **Administrator mode** - [Address] - [Group] - [Group List]

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.

To register a group address, click [New Registration]. For details on registration information, refer to page 2-29.

[Program]

To display: **Administrator mode** - [Address] - [Program] - [Program List]

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 information of the program that is saved on this machine.

To register a program, click [Edit]. For details on registration information, refer to page 2-29.

[Subject]

To display: **Administrator mode** - [Address] - [Subject] - [Subject List]

Enables you to register subjects that are used when E-mails are being sent. Also, it enables you to confirm or edit the registered information of the title that is saved on this machine.

To register a subject, click [Edit], then enter a subject to be registered (using up to 64 characters).

Tips

- Up to 10 subjects can be registered, and a subject can be selected from them before transmission.
- By selecting [E-mail Default] in the subject list, you can specify the default subject that is used for E-mail transmission.

[Text]

To display: **Administrator mode** - [Address] - [Text] - [Text List]

Enables you to register body messages that are used when sending E-mails. Also, it enables you to confirm or edit the registered information of the body that is saved on this machine.

To register message text, click [Edit], then enter message text to be registered (using up to 256 characters).

Tips

- Up to 10 bodies can be registered, and a body can be selected from them before transmission.
- By selecting [E-mail Default] in the body list, you can specify the default body that is used for E-mail transmission.

1.5.7 [Network] tab

[General Settings] - [Network Interface Settings]

To display: **Administrator mode** - [Network] - [General Settings] - [Network Interface Settings]

(This menu is displayed when the optional **Network Interface Card** is installed.)

Select the type of the network to be connected.

Item	Description
[Network Type]	Select the type of the network to be connected to this machine. [Ethernet] is specified by default.

[General Settings] - [Ethernet Settings]

To display: **Administrator mode** - [Network] - [General Settings] - [Ethernet Settings]

(This menu is displayed when [Ethernet] is selected in **Administrator mode** - [Network] - [General Settings] - [Network Interface Settings] - [Network Type].)

Specify the network speed, and check the MAC address.

Item	Description
[Speed/Duplex]	Select the network speed according to your environment. Selecting [Auto] enables communication in all network environments. [100Mbps Half Duplex] is specified by default.
[MAC Address]	Displays the MAC address of the network interface card of this machine.

[General Settings] - [Wireless LAN Settings]

To display: **Administrator mode** - [Network] - [General Settings] - [Wireless LAN Settings]

(This menu is displayed when [Wireless LAN] is selected in **Administrator mode** - [Network] - [General Settings] - [Network Interface Settings] - [Network Type].)

Manually configure a setting to connect this machine to the wireless LAN environment.

Item	Description
[SSID]	Enter the SSID of the access point to be connected to this machine (using up to 32 byte ASCII characters).
[Authentication/Encryption Algorithm]	Select the algorithm used for authentication or encryption. [None] is specified by default.
[WEP Key]	Specify the WEP key when [WEP] is selected in [Authentication/Encryption Algorithm]. • [Key Input Method]: Select a WEP key input method. [Text 5 Characters] is specified by default. • [Select Key]: Select the required one of the WEP keys registered using [WEP Key 1] to [WEP Key 4]. [1] is specified by default. • [WEP Key 1] to [WEP Key 4]: Enter WEP keys.

Item	Description
[Pass Phrase Input Method]	Select a passphrase entry method when an algorithm other than [WEP] or [802.1X] is selected in [Authentication/Encryption Algorithm]. [Text 8-63 Characters] is specified by default.
[Pass Phrase]	Enter the passphrase when an algorithm other than [WEP] or [802.1X] is selected in [Authentication/Encryption Algorithm] (using up to 64 byte ASCII characters).
[Enable 2040COEX]	Select [Enable] to attempt high-speed communication at 40 MHz. [Disable] is specified by default.

Tips

The wired network is not available if this machine is used as a wireless LAN adapter.

[General Settings] - [Wireless LAN Status]

To display: **Administrator mode** - [Network] - [General Settings] - [Wireless LAN Status]

(This menu is displayed when [Wireless LAN] is selected in **Administrator mode** - [Network] - [General Settings] - [Network Interface Settings] - [Network Type].)

You can check the communication status of the wireless LAN environment.

Item	Description
[Status]	Displays the connection status.
[SSID]	Displays the SSID.
[Speed]	Displays the communication speed.
[Authentication/Encryption Algorithm]	Displays the specified algorithm.
[Strength]	Displays the radio field intensity.
[Mac Address]	Displays the MAC address of this machine.

[General Settings] - [Wireless LAN Settings (AP mode)]

To display: **Administrator mode** - [Network] - [General Settings] - [Wireless LAN Settings (AP mode)]

(This menu is displayed when [Ethernet+Wireless LAN (AP mode)] or [Ethernet+Wireless LAN (Wi-Fi Direct mode)] is selected in **Administrator mode** - [Network] - [General Settings] - [Network Interface Settings] - [Network Type].)

Manually configure a setting to connect this machine to the wireless LAN environment in access point mode.

Item	Description
[SSID]	Enter the SSID of this machine (using ASCII characters of up to 32 bytes). If [Ethernet+Wireless LAN (AP mode)] is selected in [Network Type], the SSID of the access point is used. If [Ethernet+Wireless LAN (Wi-Fi Direct mode)] is selected in [Network Type], the SSID for Wi-Fi Direct connection is used. The SSID specified here is displayed on the Wi-Fi Direct (setting) screen of the terminal that is 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 establish a connection.
[Virtual SSID]	Displays the automatically generated virtual SSID if [Ethernet+Wireless LAN (Wi-Fi Direct mode)] is selected in [Network Type]. This option is used to connect a terminal that is incompatible with Wi-Fi Direct to this machine. A virtual SSID is displayed on the Wi-Fi Direct (setting) screen of the terminal that is incompatible with Wi-Fi Direct. The virtual SSID is indicated by "DIRECT-XXXXXX" (XXXXXX indicates a combination of random alphanumeric characters and the specified value of [SSID]).
[Authentication/Encryption Algorithm]	Select the algorithm used for authentication or encryption. [None] is specified by default.

Item	Description
[WEP Key]	Specify the WEP key when [WEP] is selected in [Authentication/Encryption Algorithm]. • [Key Input Method]: Select a WEP key input method. [Text 5 Characters] is specified by default. • [Select Key]: Select the required one of the WEP keys registered using [WEP Key 1] to [WEP Key 4]. [1] is specified by default. • [WEP Key 1] to [WEP Key 4]: Enter WEP keys.
[Pass Phrase Input Method]	Select a passphrase entry method when an algorithm other than [WEP] is selected in [Authentication/Encryption Algorithm]. [Text 8-63 Characters] is specified by default.
[Pass Phrase]	Enter the passphrase when an algorithm other than [WEP] is selected in [Authentication/Encryption Algorithm] (using up to 64 byte ASCII characters).
[Pass Phrase AutomaticRenewal]	Select whether or not to automatically update the passphrase. [Enable] is specified by default.
[Renewal Period]	Specify the interval to update the passphrase. [60] minutes is specified by default.
[Enable 2040COEX]	Select [Enable] to attempt high-speed communication at 40 MHz. [Disable] is specified by default.
[Wireless Channel]	Set a wireless LAN channel. [Auto] is specified by default.
[ANY Connection]	Select whether or not to allow ANY connection. [Enable] is specified by default.
[DHCP Server]	Select whether to use the DHCP server function. [Enable] is specified by default.
[IPv4 Lease Address]	Specify the range of the IPv4 address to be leased by the DHCP server when [Enable] is selected in [DHCP Server]. • [Start Address]: Enter the IP address at the head. • [End Address]: Enter the IP address at the end.
[Subnet Mask]	Enter the subnet mask when [Enable] is selected in [DHCP Server].
[Lease Period]	Enter the lease period when [Enable] is selected in [DHCP Server]. [4294967295] seconds 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. This option is displayed if [Ethernet+Wireless LAN (AP mode)] is selected in [Network Type].
[Concurrent Connection Device Setting]	Enter the number of devices that can be connected simultaneously to the access point. [5] devices is specified by default.
[Radio Field Intensity Setting]	Select the radio field intensity of the access point from three levels (Weak, Middle, and Strong). [Strong] is specified by default.
[Connected Device Display Setting]	Displays a list of names and MAC addresses of wireless LAN adapters that are connected to the access point.
[TCP/IP Settings]	Configure settings to connect this machine to the network using TCP/IP.
[IPv4 Settings]	Configure IPv4 settings to connect this machine to the wireless network using IPv4. • [IP Address]: Enter the fixed IP address assigned to the machine. • [Subnet Mask]: Enter the subnet mask.
[IPv6 Settings]	Configure IPv6 settings to connect 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

- If this machine is used as a wireless LAN access point, communications can only be established with a computer and mobile terminal. In addition, up to five devices can be connected to this machine simultaneously.
- For the wireless network address when this machine is used as a wireless LAN access point, specify a network address that is different from that of the backbone network. If the same network address is set for both the wireless network and backbone network, a transmission from this machine to the backbone network will be disabled.
- For details on the Wi-Fi Direct connection method, refer to the user' s guide of your terminal.

[General Settings] - [Local Interface Settings]

To display: **Administrator mode** - [Network] - [General Settings] - [Local Interface Settings]

Change the time-out time to limit a communication with the computer.

Item	Description
[I/O 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.

[TCP/IP Settings] - [TCP/IP Settings]

To display: **Administrator mode** - [Network] - [TCP/IP Settings] - [TCP/IP Settings]

Configure the TCP/IP settings.

Item	Description
[TCP/IP]	Select whether or not to use TCP/IP. [Enable] is specified by default.
[LPD]	Select whether or not to use LPD (Line Printer Daemon). [Enable] is specified by default.
[SLP]	Select whether or not to use SLP (Service Location Protocol). [Enable] is specified by default.
[LLMNR]	Select whether or not to use LLMNR (Link-local Multicast Name Resolution). [Enable] is specified by default.

[TCP/IP Settings] - [IPv4 Settings]

To display: **Administrator mode** - [Network] - [TCP/IP Settings] - [IPv4 Settings]

Assign an IP address (IPv4) to this machine.

Item	Description
[IP Address Setting Method]	When automatically specifying the IP address, select the method for automatic retrieval. • [DHCP]: [ON] (selected) is specified by default. • [BootP]: [OFF] (not selected) is specified by default. • [ARP/PING]: [OFF] (not selected) is specified by default. • [Auto IP]: Fixed to [ON] (selected).
[IP Address]	When manually specifying the IP address, enter the fixed IP address.
[Subnet Mask]	When manually specifying the IP address, enter the subnet mask.
[Default Gateway]	When manually specifying the IP address, enter the default gateway.
[Domain Name Automatic Acquisition]	When using the DHCP or other protocols, select whether or not to automatically retrieve the domain name. [Enable] is specified by default.
[DNS Server Automatic Acquisition]	Select whether or not to automatically obtain the address of the DNS server. [Enable] is specified by default.

[TCP/IP Settings] - [IPv6 Settings]

To display: **Administrator mode** - [Network] - [TCP/IP Settings] - [IPv6 Settings]

Assign an IP address (IPv6) to this machine.

Item	Description
[IPv6]	Select whether or not to use IPv6. [Enable] is specified by default.
[Auto Setting]	Select whether or not to automatically assign the IPv6 global address of this machine. [Enable] is specified by default.
[Link Local Address]	Displays the link-local address that is automatically specified from the MAC address of this machine.
[Global Address]	When manually specifying the IPv6 address, enter the IPv6 global address.
[Gateway Address]	When manually specifying the IPv6 address, enter the gateway address.
[DHCPv6]	Select whether or not to automatically assign the IPv6 global address using DHCPv6. [Enable] is specified by default.
[DNS Server Automatic Acquisition]	Select whether or not to automatically obtain the address of the DNS server. When using DHCPv6, the DNS server address can be specified automatically. [Enable] is specified by default.
[Search Domain Name Automatic Acquisition]	When using the DHCP or other protocols, select whether or not to automatically retrieve the domain name. [Enable] is specified by default.
[NTP Server Automatic Acquisition]	In the IPv6 environment, select whether or not to automatically specify the NTP server address by DHCPv6. [Enable] is specified by default.

[TCP/IP Settings] - [RAW Port Settings]

To display: **Administrator mode** - [Network] - [TCP/IP Settings] - [RAW Port Settings]

Specify a RAW port number required for Port9100 printing.

Item	Description
[RAW Port]	Select whether or not to use the RAW port. [Enable] is specified by default.
[Port Number]	If necessary, change the RAW port number. [9100] is specified by default.
[Bidirectional]	Select whether or not to enable bidirectional communication of the RAW port. [Disable] is specified by default.

[TCP/IP Settings] - [DNS Settings]

To display: **Administrator mode** - [Network] - [TCP/IP Settings] - [DNS Settings]

Configure the DNS settings when a DNS server is used.

Item	Description
[Host Name]	Enter the host name of this machine (using ASCII characters of up to 63 bytes, including only - for symbol marks). If your DNS server does not support the Dynamic DNS function, register the host name of this machine on the DNS server.
[Domain Name]	When not automatically retrieving the default domain name, enter the default domain name of this machine (using ASCII characters of up to 63 bytes, including only hyphens (-) and periods (.) for symbol marks).
[DNS Server Address (IPv4)]	Enter the address (IPv4) of your DNS server. You can register up to three addresses.
[DNS Server Address (IPv6)]	Enter the address (IPv6) of your DNS server. You can register up to three addresses.
[Search Domain Name]	If the search domain name is not automatically retrieved, enter the search domain name of this machine (using ASCII characters of up to 251 bytes, including only hyphens (-) and periods (.) for symbol marks).
[Dynamic DNS]	Select whether or not to enable the Dynamic DNS function. When your DNS server supports the Dynamic DNS function, the specified host name can be automatically registered on the DNS server or changes can be automatically updated as long as [Enable] is selected. [Disable] is specified by default.

[E-mail Settings] - [E-mail TX (SMTP)]

To display: **Administrator mode** - [Network] - [E-mail Settings] - [E-mail TX (SMTP)]

Configure the settings on the E-mail transmission function of this machine.

Item	Description
[E-mail TX (SMTP)]	Configure the settings to send an E-mail from this machine.

Item		Description
	[E-mail TX (SMTP)]	Select whether or not to send an E-mail from this machine. [Enable] is specified by default.
	[Scan to E-mail]	Select whether or not to use the E-mail transmission function. Using this function, you can send the scanned original data as an E-mail attachment. [Enable] is specified by default.
	[E-mail Notification]	Select whether or not to use the E-mail notification function. 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. [Enable] is specified by default.
	[Total Counter Notification]	Select whether or not to use the total counter notification function. Using this function, you can send counter information managed by this machine to the registered E-mail address. [Enable] is specified by default.
	[SMTP Server Automatic Acquisition]	When using the DNS server, select whether or not to automatically retrieve the E-mail server (SMTP) address. [Disable] 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" **Note** To specify [SMTP Server Address], you need to enter [Device E-mail Address].
	[Port Number]	If necessary, change the port number of the E-mail server (SMTP). [25] is specified by default.
	[SSL/TLS]	Select the method to encrypt communications with the E-mail server (SMTP). Select [Enable] or [Start TLS] according to your environment. [Disable] is specified by default.
	[Port Number (SSL)]	If necessary, change the SSL communication port number. This is required when [Enable] is selected in [SSL/TLS]. [465] is specified by default.
	[Connection Time-out]	Change the time-out time to communicate with the E-mail server (SMTP), if necessary. [60 sec.] is specified by default.
	[Administrator E-mail Address]	Displays the E-mail address of the administrator.
	[Device E-mail Address]	Enter the E-mail address of this machine (using ASCII characters of up to 320 bytes).
	[Max Mail Size]	Select whether or not to limit the maximum E-mail size. [No Limit] is specified by default.
	[Server Capacity]	If you select [Limit] in [Max Mail Size], enter the maximum E-mail size that is available in the E-mail server (SMTP). E-mails that have been exceeded the specified size will be discarded.
	[Binary Division]	Select whether or not to divide a large E-mail before sending it. This item is necessary if the maximum capacity of an E-mail to be sent is restricted in the E-mail server. [Off] is specified by default.
	[Divided Mail Size]	Enter the size to divide an E-mail when selecting [On] in [Binary Division]. [500] KB is specified by default.
[POP Before SMTP]		Configure the setting if your environment requires the POP Before SMTP Authentication for sending an E-mail.

Item		Description
	[POP Before SMTP]	Select whether or not to use POP before SMTP. Configure the setting if your environment requires the POP Before SMTP Authentication for sending an E-mail. [Disable] 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. [5] sec. is specified by default.
[SMTP Authentication]		Configure the setting if your environment requires the SMTP authentication for sending an E-mail.
	[SMTP Authentication]	Select whether or not to use SMTP authentication. [Disable] is specified by default.
	[SMTP Authentication method setting]	When using SMTP authentication, specify whether or not to enable the following authentication methods. • [Kerberos] • [NTLM v1] • [Digest-MD5] • [CRAM-MD5] • [LOGIN] • [PLAIN] [Enable] is specified by default in every case.
	[Account]	When you have selected [Enable] in [SMTP Authentication], enter the user ID for SMTP authentication (using up to 255 bytes).
	[Password]	When you have selected [Enable] in [SMTP Authentication], enter the password (using up to 128 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Domain Name]	When you have selected [Enable] in [SMTP Authentication], enter the domain name (realm) for SMTP authentication (using ASCII characters of up to 255 bytes). This item is necessary when the SMTP authentication method is Digest-MD5.
	[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. • [Use User Authentication]: Uses the user name and password of the user registered in this machine as [Account] and [Password] for SMTP authentication. • [Use SMTP Authentication Setting]: Uses the values you entered in [Account] and [Password]. [Use SMTP Authentication Setting] is specified by default.

[E-mail Settings] - [E-mail RX (POP)]

To display: **Administrator mode** - [Network] - [E-mail Settings] - [E-mail RX (POP)]

Configure the settings on the E-mail reception function of this machine.

Item	Description
[E-mail RX (POP)]	Select whether or not to enable this machine to receive E-mails. [Enable] 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"
[Port Number]	If necessary, change the port number of the E-mail server (POP). [110] is specified by default.
[SSL/TLS]	Select whether or not to use SSL for communication with the E-mail server (POP). [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. [995] is specified by default.

Item	Description
[Login Name]	Enter the login name when E-mails are received using the E-mail server (POP) (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 15 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (POP), if necessary. [60 sec.] is specified by default.
[APOP Authentication]	Select whether or not to enable APOP authentication when logging in to the E-mail server (POP). This item is available when using APOP in your environment. [Disable] is specified by default.
[Auto Check of Arrival]	Select whether or not to check for incoming E-mails by periodically connecting this machine to the E-mail server (POP). [Disable] is specified by default.
[Polling Rate]	Specify the interval to connect to the E-mail server (POP) when [Enable] is selected in [Auto Check of Arrival]. [15] minutes is specified by default.

[E-mail Settings] - [S/MIME]

To display: **Administrator mode** - [Network] - [E-mail Settings] - [S/MIME]

Configure settings to enable use of S/MIME on this machine.

Item	Description
[S/MIME]	Select whether or not to use S/MIME. [Disable] is specified by default.
[Digital Signature]	To add digital signature when E-mails are being sent, select a method to add it. • [Do not add signature]: Does not add the signature. • [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 or not to add digital signature before sending an E-mail. [Do not add signature] is specified by default.
[E-mail Text Encryption Method]	Select the method to encrypt the E-mail text. [3DES] is specified by default.
[Digital Signature Type]	To add a digital signature when sending E-mails, select its authentication method. [SHA-1] is specified by default.

[LDAP Settings] - [LDAP Settings]

To display: **Administrator mode** - [Network] - [LDAP Settings] - [LDAP Settings]

Configure settings so that you can search for a destination from the LDAP server.

Item	Description
[LDAP]	Select whether or not to use the LDAP server to search for a destination. [Disable] is specified by default.

[LDAP Settings] - [LDAP Server Registration]

To display: **Administrator mode** - [Network] - [LDAP Settings] - [LDAP Server Registration]

Register the LDAP server used to search for a destination.

Item	Description
[LDAP Server Registration]	Register the LDAP server used to search for a destination.

Item		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 Number]	If necessary, change the LDAP server port number. [389] is specified by default.
	[SSL/TLS]	Select whether or not to use SSL for communication with the LDAP server. [Disable] is specified by default.
	[Port Number (SSL)]	If necessary, change the SSL communication port number. [636] is specified by default.
	[Search Base]	Specify the starting point to search for a user to be authenticated (using ASCII characters of up to 255 bytes). 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 Result]	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] 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 255 bytes).
	[Password]	Enter the password (using up to 128 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Domain Name]	Enter the domain name to log in to the LDAP server (using ASCII characters of up to 64 bytes). If [GSS-SPNEGO] is selected in [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]. • [Dynamic Authentication]: The system prompts you to enter the user name and password when Address Search (LDAP) is carried out. [Set Value] is specified by default.
	[Use Referral]	Select whether or not 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 the LDAP search is carried out. The setting can be switched between [Name] (cn) and [Nickname] (displayName). [Name] is specified by default.
[Initial Setting for Search Details]		Specify LDAP search conditions. [OR] is specified by default in every case.

[HTTP Settings] - [HTTP Server Settings]

To display: **Administrator mode** - [Network] - [HTTP Settings] - [HTTP Server Settings]

Configure the settings on the HTTP server function of this machine.

Item	Description
[HTTP Server]	Select whether or not to use this machine as an HTTP server. If you select [Disable], you cannot use **Web Connection**. [Enable] is specified by default.

Item	Description
[Port Number]	If necessary, change the HTTP server port number. [80] is specified by default.
[SSL/TLS]	Select whether or not to use SSL for communication with the HTTP server. [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. [443] is specified by default.

[IPP Settings]

To display: **Administrator mode** - [Network] - [IPP Settings] - [IPP Settings]

Configure the operating environment for IPP printing.

Item	Description
[IPP Print]	Select whether or not to use IPP printing. [Enable] is specified by default.
[Accept IPP Job]	Select whether or not to enable reception of the IPP job. [Enable] is specified by default.
[Printer Name]	If necessary, enter a printer name of this machine (using up to 127 bytes).
[Printer Location]	If necessary, enter the installation location of this machine (using up to 127 bytes).
[Printer Information]	If necessary, enter the printer information of this machine (using up to 127 bytes).
[Printer URI]	Displays the URI of the printers that can print data using the IPP.
[Operational Support]	Select whether or not to allow the following IPP operations. • [Print Job]: Allows a print job. • [Validate Job]: Allows you to check a valid job. • [Cancel Job]: Allows you to cancel a job. • [Get Job Attributes]: Allows you to obtain job attributes. • [Get Jobs]: Allows you to obtain a list of job attributes. • [Get Print Attributes]: Allows you to obtain printer attributes. [ON] (selected) is specified by default in every case.
[IPP Authentication]	Select the IPP authentication method. [Requesting-user-name] is specified by default.
[User Name]	Enter the user name (using ASCII characters of up to 20 bytes, excluding a colon (:)). This entry is required if you have selected [Basic] or [Digest] in [IPP Authentication].
[Password]	Enter the password (using ASCII characters of up to 20 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password. This entry is required if you have selected [Basic] or [Digest] in [IPP Authentication].
[Realm]	Enter the domain (realm) (using ASCII characters of up to 127 bytes). This entry is required if you have selected [Digest] in [IPP Authentication].

[FTP Settings] - [FTP Server Settings]

To display: **Administrator mode** - [Network] - [FTP Settings] - [FTP Server Settings]

To use application software with which the FTP server of this machine is used to communicate, configure the FTP server.

Item	Description
[FTP Server]	Select whether or not to use the FTP server function of this machine. [Disable] is specified by default.
[Port Number]	If necessary, change the FTP server port number. [21] is specified by default.

Item	Description
[Command Prohibit]	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 or not to enable the security of this machine against FTP bounce attacks. This option is not available if [Command Prohibit] 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.

[FTP Settings] - [FTP TX Settings]

To display: **Administrator mode** - [Network] - [FTP Settings] - [FTP TX Settings]

Configure settings to enable use of the FTP transmission function on this machine.

Item	Description
[FTP TX]	Select whether or not to use the FTP transmission function of this machine. Selecting this option sends the scanned original data to the FTP server. [Enable] 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.
[Proxy Server Address]	To access to the FTP server via a proxy server, 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.

[SNMP Settings]

To display: **Administrator mode** - [Network] - [SNMP Settings] - [SNMP Settings]

Configure the settings for obtaining the machine information and monitoring the machine using SNMP (Simple Network Management Protocol).

Item		Description
[SNMP Settings]		Configure the SNMP settings.
	[SNMP]	Select whether or not to use SNMP. [Enable] is specified by default.
	[SNMP v1/v2c (IP)]	Select whether or not to use SNMP v1 or SNMP v2. [Enable] is specified by default.
	[SNMP v3 (IP)]	Select whether or not to use SNMP v3. [Enable] is specified by default.
	[UDP Port]	If necessary, change the UDP port number. [161] is specified by default.
[SNMP v1/v2c Settings]		Configure the SNMP v1/v2c settings.

Item		Description
	[Read Community Name]	Enter a read-only community name (using ASCII characters of up to 15 bytes, excluding spaces, \, ,' ,", and #). [public] is specified by default.
	[Write]	Select whether or not to enable the read and write functions. [Enable] is specified by default.
	[Write Community Name]	If [Write] is set to [Enable], enter the community name in the read-write enable state (using ASCII characters of up to 15 bytes, excluding spaces, \, ,' ,", and #). [private] is specified by default.
[SNMP v3 Settings]		Configure the SNMP v3 settings.
	[Context Name]	Enter a context name (using ASCII characters of up to 63 bytes, excluding spaces, \, ,' ,", and #).
	[Discovery]	Select whether or not to allow a user for detection. [Enable] is specified by default.
	[Discovery User Name]	If [Discovery] is set to [Enable], enter a user name for detection (using ASCII characters of up to 32 bytes, excluding spaces, \, ,' ,", and #). [public] is specified by default.
	[Read User Name]	Enter a read-only user name (ASCII characters of up to 32 bytes, excluding spaces, \, ,' ,", and #). [initial] is specified by default.
	[Security Level]	Select a security level for the read-only user. [Auth-password/Priv-password] is specified by default.
	[auth-password]	Enter an authentication password for the read-only user (using ASCII characters between 8 and 32 bytes, excluding spaces, \, ,' ,", and #). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[priv-password]	Enter a privacy password for the read-only user (using ASCII characters between 8 and 32 bytes, excluding spaces, \, ,' ,", and #). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Write User Name]	Enter a user name used by the read and write user (using ASCII characters of up to 32 bytes, excluding spaces, \, ', ", and #). [restrict] is specified by default.
	[Security Level]	Select a security level of the read and write user. [Auth-password/Priv-password] is specified by default.
	[auth-password]	Enter an authentication password for the read and write user (using ASCII characters between 8 and 32 bytes, excluding spaces, \, ,' ,", and #). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[priv-password]	Enter a privacy password for the read and write user (using ASCII characters between 8 and 32 bytes, excluding spaces, \, ,' ,", and #). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Encryption Algorithm]	Select an encryption algorithm. [DES] is specified by default.
	[Authentication Method]	Select an authentication algorithm. [MD5] is specified by default.
[Trap Settings]		Configure the settings on the SNMP TRAP function.
	[Allow Setting]	Select whether or not to allow a notification of the status of this machine using the SNMP TRAP function. [Enable] is specified by default.
	[Trap Setting when Authentication Fails]	Select whether or not to send TRAP when authentication fails. [Disable] is specified by default.

[SMB Settings] - [WINS/NetBIOS Settings]

To display: **Administrator mode** - [Network] - [SMB Settings] - [WINS/NetBIOS Settings]

Register the WINS server when it is installed to resolve the name.

Item	Description
[WINS/NetBIOS]	Select whether or not to use the WINS server. [Enable] is specified by default.
[WINS Automatic Retrieval]	Select whether or not to automatically obtain the address of the WINS server. This item is necessary when DHCP is enabled. [Enable] is specified by default.
[WINS Server Address 1] [WINS Server Address 2]	Enter the WINS server address when manually specifying it. Use the following entry formats. • Example of entry: "192.168.1.1"
[Node Type]	Select the name resolution method. • [B Node]: Query by broadcast. • [P Node]: Makes inquires to the WINS server. • [M Node]: Makes inquiries to the broadcast and WINS server in sequence. • [H Node]: Makes inquiries to the WINS server and broadcast in sequence. [H Node] is specified by default.

[SMB Settings] - [SMB Client Settings]

To display: **Administrator mode** - [Network] - [SMB Settings] - [SMB Client Settings]

Configure settings to enable use of the SMB client function of this machine.

Item	Description
[SMB Client]	Select whether or not to use the SMB client function of this machine. Using this function, you can to send the scanned original data to a shared folder of a computer. [Enable] is specified by default.
[Authentication]	Select an authentication method for SMB transmission according to your environment. • [NTLM v1]: Performs the NTLMv1 authentication. This option is available in the NT domain environment. • [NTLM v2]: Performs NTLMv2 authentication. This option is available in the NT domain environment. • [NTLMv1/v2]: Performs NTLM v1 authentication when NTLM v2 authentication fails. This option is available in the NT domain environment. • [Kerberos]: Performs Kerberos authentication. This option is available in the Active Directory domain environment. • [Kerberos, NTLMv1/v2]: NTLM v2 authentication is performed when Kerberos authentication fails, and NTLM v1 authentication is performed when NTLM v2 authentication fails. This option is available when both the Active Directory and NT domains are specified. [NTLM v1] is specified by default.
[DFS]	Select whether or not to use DFS when the distributed file system (DFS) is employed. [Enable] is specified by default.
[Default Domain Name]	Enter the default domain name to be added to the destination host name when data is sent using SMB (using ASCII characters of up to 64 bytes). 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 Settings] - [Direct Hosting Settings]

To display: **Administrator mode** - [Network] - [SMB Settings] - [Direct Hosting Settings]

Select whether or not to enable the direct hosting SMB service. If enabled, you can specify destination using the IP address (IPv4 or IPv6) or host name.

[Enable] is specified by default.

[Web Service Settings] - [Common Settings]

To display: **Administrator mode** - [Network] - [Web Service Settings] - [Common Settings]

Configure settings to detect this machine using the Web service.

Item	Description
[Friendly Name]	Enter the name of this machine to be displayed when this machine is searched for using the Web service through a computer (using up to 127 bytes).
[Secure Mode]	Select whether or not to use the SSL for Web service communication. [Disable] is specified by default.

[Web Service Settings] - [Printer Settings]

To display: **Administrator mode** - [Network] - [Web Service Settings] - [Printer Settings]

Configure settings to perform Web service printing.

Item	Description
[Print Function]	Select whether or not to use the WS print function. [Enable] is specified by default.
[Printer Name]	Enter the name of this machine when using it as a WS printer (using up to 127 bytes, excluding !, \, and ,).
[Printer Location]	If necessary, enter the installation location of the printer (using up to 127 bytes).
[Printer Information]	If necessary, enter the printer information (using up to 127 bytes).

[Web Service Settings] - [Scanner Settings]

To display: **Administrator mode** - [Network] - [Web Service Settings] - [Scanner Settings]

Configure settings to perform Web service scanning.

Item	Description
[Scan Function]	Select whether or not to use the WS scan transmission function. [Enable] is specified by default.
[Scanner Name]	Enter the name of this machine when using it as the WS scanner (using up to 127 bytes).
[Scanner Location]	If necessary, enter the installation location of the scanner (using up to 127 bytes).
[Scanner Information]	If necessary, enter the scanner information (using up to 127 bytes).
[Connection Timeout]	Change the time-out time to limit a communication with the computer if necessary. [120] sec. is specified by default.

[Bonjour Settings]

To display: **Administrator mode** - [Network] - [Bonjour Settings] - [Bonjour Settings]

Configure the Bonjour operating environment when using this machine in the Mac OS control.

Item	Description
[Bonjour]	Select whether or not to use Bonjour. [Enable] is specified by default.
[Printer Name]	Enter a Bonjour name that is to be displayed as the name of connected device (using up to 63 bytes).
[Priority Protocol]	Select the protocol preferentially used for connection by Bonjour. [RAW Port] is specified by default.

[Network Fax Settings] - [Network Fax Function Settings]

To display: **Administrator mode** - [Network] - [Network Fax Settings] - [Network Fax Function Settings]

Select whether or not to use Internet fax.

[Enable] is specified by default.

Tips

To use the Internet Fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

[Network Fax Settings] - [Internet Fax RX Ability]

To display: **Administrator mode** - [Network] - [Network Fax Settings] - [Internet Fax RX Ability]

This machine notifies its reception capability when returning a MDN message if you are using the Internet Fax function. If necessary, change the reception capability of this machine, which is notified upon returning a MDN message.

Item	Description
[Compression Type]	Change the compression type of a fax job the machine can receive.
[Paper Size]	Displays the paper size of a fax job the machine can receive.
[Resolution]	Change the resolution of a fax job the machine can receive.

Tips

To use the Internet Fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

[Network Fax Settings] - [I-Fax Advanced Setting]

To display: **Administrator mode** - [Network] - [Network Fax Settings] - [I-Fax Advanced Setting]

Configure settings for fax reception confirmation (MDN/DSN) to be sent by this machine if you are using the Internet fax function.

Item	Description
[MDN Request]	Select whether or not 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.
[DSN Request]	Select whether or not 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 or not to return a response message when a sender requests for fax reception result (MDN request) to this machine. [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. [ON] (selected) is specified by default.

Tips

To use the Internet Fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

[WebDAV Settings] - [WebDAV Server Settings]

To display: **Administrator mode** - [Network] - [WebDAV Settings] - [WebDAV Server Settings]

Configure settings to enable use of the WebDAV server function of this machine.

Using this machine as a WebDAV server allows you to associate this machine with an application that operates as a WebDAV client.

Item	Description
[WebDAV Server]	Select whether or not to use the WebDAV server function of this machine. [Enable] is specified by default.
[SSL/TLS]	Specify whether or not to use the SSL for communication or not. • [Non-SSL Only]: Allows only non-SSL communications. • [SSL Only]: Allows only SSL communications. • [SSL/Non-SSL]: Allows both SSL communication and non-SSL communication. [Non-SSL Only] is specified by default.
[Access Rights Settings]	Specify the password to restrict access to the WebDAV server of this machine (using up to 64 byte ASCII characters). Tapping [Initial Password] returns the password to the default. [sysadm] is specified by default.

[WebDAV Settings] - [WebDAV Client Settings]

To display: **Administrator mode** - [Network] - [WebDAV Settings] - [WebDAV Client Settings]

Configure settings to enable use of the WebDAV client function of this machine.

Item		Description
[WebDAV Client]		Select whether or not to use the WebDAV client function of this machine. Selecting this option sends the scanned original data to the WebDAV server. [Enable] is specified by default.
[Proxy]		To access to the WebDAV server via a proxy server, register your proxy server.
	[Proxy Server Address]	To access to the WebDAV server via a proxy server, 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 User Name]	Enter the user name to log in to the proxy server (using ASCII characters of up to 63 bytes).
	[Proxy Server Password]	Enter the password (using ASCII characters of up to 63 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Connection Timeout]		If necessary, change the time-out time to limit a communication with the WebDAV server. [60] sec. is specified by default.
[Authentication]		Select an authentication method for WebDAV transmission according to your environment.
[Domain Name]		Enter the default domain name to be added to the destination host name when data is sent using WebDAV (using ASCII characters of up to 64 bytes).

[OpenAPI Settings]

To display: **Administrator mode** - [Network] - [OpenAPI Settings] - [OpenAPI Settings]

To use application software that communicates with this machine via OpenAPI, configure the OpenAPI settings of this machine.

Item	Description
[OpenAPI]	Select whether or not to use OpenAPI on this machine. [Enable] is specified by default.
[OpenAPI External]	Select whether or not to connect to external application software via OpenAPI. [Enable] is specified by default.
[Port Number]	If necessary, change the OpenAPI communication port number. [50001] is specified by default.
[SSL/TLS]	Select whether or not to use SSL for a communication via OpenAPI. This setting is available when the certification of this machine is registered. [Non-SSL Only] is specified by default.
[Port Number (SSL/TLS)]	If necessary, change the SSL communication port number. [50003] is specified by default.
[Authentication]	Select whether or not to authenticate users accessing via OpenAPI. To authenticate, enter the login name and password in [Login Name] and [Password]. [Off] is specified by default.
[Login Name]	Enter the login name that is used for OpenAPI authentication (using ASCII characters of up to eight bytes, excluding symbols).
[Password]	Enter the password that is used for OpenAPI authentication (using ASCII characters of up to eight bytes, excluding symbols). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Proxy]	Configure a setting for the required proxy server if you want associate this machine with a different system that supports OpenAPI.
[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 (HTTP)]	If necessary, change the proxy server port number for HTTP. [8080] is specified by default.
[Proxy Server Port Number (HTTPS)]	If necessary, change the proxy server port number for HTTPS. [8080] is specified by default.
[Proxy Server Port Number (FTP)]	If necessary, change the proxy server port number for FTP. [21] is specified by default.
[Proxy Server User Name]	Enter the user name to log in to the proxy server (using ASCII characters of up to 63 bytes).
[Proxy Server Password]	Enter the password (using ASCII characters of up to 63 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Specified Application Start Setting]	Configure settings for starting the OpenAPI application if you are using an OpenAPI application.
[Specified Application]	Select whether or not to launch only the pre-specified OpenAPI application when this machine has started up. [Disable] is specified by default. **Note** When the OpenAPI application is selected in [Default Application Selection], the setting can be changed.
[Default Application Selection]	When you use this function, specify the OpenAPI application to be launched. [None] is selected by default.
[Basic Functions Setting]	When using this function, select whether or not to use the basic functions of this machine. [Restrict] is specified by default.

[TCP Socket Settings]

To display: **Administrator mode** - [Network] - [TCP Socket Settings] - [TCP Socket Settings]

Configure the TCP Socket operating environment.

Item	Description
[TCP Socket]	Select whether or not to use TCP Socket on this machine. [Enable] is specified by default.
[Port Number]	If necessary, change the TCP Socket port number. [59158] is specified by default.
[SSL/TLS]	Select whether or not to use SSL for a communication via TCP Socket. This setting is available when the certification of this machine is registered. [Non-SSL Only] is specified by default. **Note** When [Security] - [PKI Settings] - [SSL/TLS Settings] - [SSL/TLS] is set to [Enable], the setting can be changed.
[Port Number (SSL/TLS)]	If necessary, change the SSL communication port number. [59159] is specified by default.

[LLTD Settings]

To display: **Administrator mode** - [Network] - [LLTD Settings] - [LLTD Settings]

Select whether or not to use LLTD (Link Layer Topology Discovery).

Using LLTD, you can display this machine on the network map if your computer is equipped with Windows Vista or later (Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2).

[Enable] is specified by default.

[Machine Update Settings] - [HTTP Proxy Settings]

To display: **Administrator mode** - [Network] - [Machine Update Settings] - [HTTP Proxy Settings]

(To display this menu, ask your service representative to configure necessary settings. For details, contact your service representative.)

When downloading via HTTP to update the main unit, configure settings of the proxy server for HTTP.

Item	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. [80] is specified by default.
[Proxy Authentication]	Select whether or not to use proxy authentication. If [Enable] is selected, configure the following settings. [Disable] is specified by default. • [Proxy Server User Name]: Enter the user name to log in to the proxy server (using up to 63 byte ASCII characters). • [Proxy Server Password]: Enter the password (using up to 63 byte ASCII characters).

[Web Browser Settings]

To display: **Administrator mode** - [Network] - [Web Browser Settings] - [Web Browser Settings]

(This menu is displayed when the optional **i-Option LK-101 v3** is installed.)

Select whether to enable the Web browser function of this machine.

[Enable] is specified by default.

[IWS Settings]

To display: **Administrator mode** - [Network] - [IWS Settings] - [IWS Settings]

(To display this menu, ask your service representative to configure necessary settings. For details, contact your service representative.)

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.

Item	Description
[IWS Settings]	Select whether or not to use IWS. [Disable] 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 contain dynamic content, such as scripts, select whether or not to allow an external connection to the dynamic content. [Enable] is specified by default.

[AirPrint Setting]

To display: **Administrator Mode** - [Network] - [AirPrint Settings]

Configure settings to print data from an AirPrint-compatible terminal.

Item	Description
[AirPrint]	Select whether or not to use AirPrint. To receive AirPrint print jobs, select [Enable]. [Disable] is specified by default.
[Bonjour Name]	Enter the Bonjour name of this machine, which is to be displayed when the appropriate printer is detected (using up to 63 characters).
[Bonjour Service Name]	Displays the service name of the Bonjour name that is automatically generated from the Bonjour name.
[Location]	Enter the location where this machine is installed (using up to 127 characters).
[Latitude]	Enter the latitude of the location where this machine is installed. If the latitude of the installation location is not known, leave this option blank.
[Longitude]	Enter the longitude of the location where this machine is installed. If the longitude of the installation location is not known, leave this option blank.
[Altitude]	Enter the altitude of the location where this machine is installed. If the altitude of the installation location is not known, leave this option blank.
[Timeout]	Enter the communication timeout. [60] seconds is specified by default.

Tips

If one of the following functions is disabled after the AirPrint function is enabled, the AirPrint function will also be disabled.

- [Utility] - [Administrator Settings] - [Network Settings] - [HTTP Server Settings] - [HTTP Server Settings]
- [Utility] - [Administrator Settings] - [Network Settings] - [HTTP Server Settings] - [IPP Settings]
- [Utility] - [Administrator Settings] - [Network Settings] - [Bonjour Setting]
- In the administrator mode of **Web Connection**, [Network] - [IPP Settings] - [Accept IPP Job]

[SSDP Settings]

To display: **Administrator mode** - [Network] - [SSDP Settings] - [SSDP Settings]

Select whether to use the SSDP (Simple Service Discovery Protocol) or not. To use SSDP, change the multicast TTL as necessary.

Using SSDP allows software on the network or other services to search for services which can be supplied by this machine. It also notifies that services have been started on this machine.

This function is available when using services such as OpenAPI.

Item	Description
[SSDP]	Select whether to use SSDP. [Enable] is specified by default.

2 Configuring the Operating Environment of This Machine

2 Configuring the Operating Environment of This Machine

2.1 Configuring the Scan to E-mail operating environment

Overview

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

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

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 1-3.

2 Configuring basic settings for Scan to E-mail

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

3 Set the following options according to your environment

Purpose	Reference
Communicate with the E-mail server using SSL/TLS	page 2-3
Use of SMTP Authentication when sending E-mails	page 2-3
Use of POP Before SMTP Authentication when sending E-mails	page 2-4
Addition of a digital signature by encrypting E-mails with S/MIME	page 2-5

Configuring basic settings for Scan to E-mail

Register the E-mail server (SMTP) address as well as the E-mail address of this machine.

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

Settings	Description
[E-mail TX (SMTP)]	Select [Enable] to transmit E-mails. [Enable] is specified by default.
[Scan to E-mail]	Select [Enable] to use the Scan to E-mail. [Enable] 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). Normally, you can use the original port number. [25] is specified by default.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (SMTP), if necessary. [60 sec.] is specified by default.
[Device E-mail Address]	Enter the E-mail address of this machine (using ASCII characters of up to 320 bytes). The E-mail address entered here is used as a sender address (From address) of E-mails to be sent from this machine.

Settings	Description
[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 that have been exceeded the specified size will be 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] is specified by default.
[Divided Mail Size]	Enter the size to divide an E-mail. This item is necessary when [Binary Division] is enabled. [500] KB is specified by default.

Tips

- The sender E-mail address can be changed on the **Control Panel** before sending the E-mail, if necessary.
- If user authentication is employed 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 Settings] - [E-mail TX (SMTP)], then configure the following settings.

Settings	Description
[SSL/TLS]	Select the method to encrypt communications with the E-mail server (SMTP). Select [Enable] or [Start TLS] according to your environment. [Disable] is specified by default.
[Port Number (SSL)]	If you select [Enable] in [SSL/TLS], change the communication port number, if necessary. Normally, you can use the original port number. [465] is specified by default.

Using SMTP authentication

Configure the setting if your environment requires the SMTP authentication for sending 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 Settings] - [E-mail TX (SMTP)], then configure the following settings.

Settings	Description
[SMTP Authentication]	Select [Enable] to use the SMTP authentication. [Disable] is specified by default.

Settings		Description
	[SMTP Authentication method setting]	When using SMTP authentication, specify whether or not to enable the following authentication methods. • [Kerberos] • [NTLM v1] • [Digest-MD5] • [CRAM-MD5] • [LOGIN] • [PLAIN] [Enable] is specified by default in every case.
	[Account]	When you have selected [Enable] in [SMTP Authentication], enter the user ID for SMTP authentication (using up to 255 bytes).
	[Password]	When you have selected [Enable] in [SMTP Authentication], enter the password (using up to 128 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Domain Name]	When you have selected [Enable] in [SMTP Authentication], enter the domain name (realm) for SMTP authentication (using ASCII characters of up to 255 bytes). This item is necessary when the SMTP authentication method is Digest-MD5.
	[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. • [Use User Authentication]: Uses the user name and password of the user registered in this machine as [Account] and [Password] for SMTP authentication. • [Use SMTP Authentication Setting]: Uses the values you entered in [Account] and [Password]. [Use SMTP Authentication Setting] is specified by default.

Tips

If the user does not enter the password for IC card authentication, it is necessary to enter the password for E-mail transmission even if [Use User Authentication] is selected in [Authentication Setting].

Using POP Before SMTP authentication

Configure the setting if your environment requires the POP Before SMTP Authentication for sending 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 permits 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) that is used for authentication.

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

Settings	Description
[POP Before SMTP]	Select [Enable] to use POP Before SMTP. [Disable] 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 permitted 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 Settings] - [E-mail RX (POP)], then configure the following settings.

Settings	Description
[E-mail RX (POP)]	Select [Enable] to use POP Before SMTP. [Enable] 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"
[Port Number]	If necessary, change the port number of the E-mail server (POP). Normally, you can use the original port number. [110] is specified by default.
[Login Name]	Enter the login name when E-mails are received using the E-mail server (POP) (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 15 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (POP), if necessary. [60 sec.] 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 Settings] - [E-mail RX (POP)], then configure the following settings.

Settings	Description
[SSL/TLS]	When using SSL to encrypt a communication with the E-mail server (POP), select [Enable]. [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. Normally, you can use the original port number. [995] is specified by default.
[APOP Authentication]	If you use APOP in your E-mail server (POP), select [Enable]. [Disable] is specified by default.

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.

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

➔ For details, refer to page 2-25.

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

➔ For details, refer to page 2-35.

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

Settings	Description
[S/MIME]	Select [Enable] to use the S/MIME. [Disable] is specified by default.

Settings	Description
[Digital Signature]	To add digital signature when E-mails are being sent, select a method to add it. • [Do not add signature]: Does not add the signature. • [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 or not to add digital signature before sending an E-mail. [Do not add signature] is specified by default.
[E-mail Text Encryption Method]	Select the method to encrypt the E-mail text. [3DES] is specified by default.
[Digital Signature Type]	To add a digital signature when sending E-mails, select its authentication method. [SHA-1] 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.

2.2 Configuring the SMB Send operating environment

Overview

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

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

If the direct hosting SMB service is enabled, communications can be carried out using the IP address (IPv4/IPv6) or host name. If this service is enabled, you can use the SMB transmission function even in the IPv6 environment.

Using LLMNR (Link-local Multicast Name Resolution), you can resolve the name even in an environment with no DNS server. This function is supported in an operating system of Windows Vista or later (Windows Vista/7/8/8.1/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 transmission 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 1-3.

2 Configuring basic settings for SMB Send

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

3 Set the following options according to your environment

Purpose	Reference
Resolve the name using the WINS server	page 2-8
Specify a destination computer using the IP address and host name (FQDN)	page 2-9
Use the SMB transmission function in the IPv6 environment	page 2-9
Specify a destination with a host name in an environment where the DNS server is not running (supported on the computer loaded with Windows Vista or later)	page 2-9
Use the SMB transmission function in the DFS environment	page 2-9

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 ports 445 and 139 of a destination computer in this 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).
  When specifying the destination computer with the computer name (NetBIOS name) or host name, perform name resolution in the order of NetBIOS (port 137 of the 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 using 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 SMB Send

Enable the SMB transmission function. In addition, select the authentication method for SMB transmission.

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

Settings	Description
[SMB Client]	Select [Enable] to use the SMB transmission function. [Enable] is specified by default.
[Authentication]	Select an authentication method for SMB transmission according to your environment. • [NTLM v1]/[NTLM v2]/[NTLMv1/v2]: Select this to use the function in the NT domain environment. If you select [NTLMv1/v2], NTLMv1 authentication is performed when NTLMv2 authentication fails. • [Kerberos]: Select this to use the function in the Active Directory domain environment. • [Kerberos, NTLMv1/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.
[Default Domain Name]	Enter the default domain name to be added to the destination host name when data is sent using SMB (using ASCII characters of up to 64 bytes). 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.

Tips

- In Mac OS X 10.7/10.8/10.9, set [Authentication] to [NTLMv1/v2].
- In Mac OS X 10.7/10.8/10.9, the direct hosting SMB service must be enabled (default: [Enable]). For details, refer to page 2-9.

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 Settings] - [WINS/NetBIOS Settings], then configure the following settings.

Settings	Description
[WINS/NetBIOS]	Select [Enable] to use the WINS server. [Enable] is specified by default.
[WINS Automatic Retrieval]	Select [Enable] to automatically obtain the WINS server address. This item is necessary when DHCP is enabled. [Enable] is specified by default.
[WINS Server Address 1] [WINS Server Address 2]	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]	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

If the direct hosting SMB service is enabled, you can specify the destination using the IP address (IPv4/IPv6) or host name.

In the administrator mode, select [Network] - [SMB Settings] - [Direct Hosting Settings], and then set [Direct Hosting] to [Enable].

Resolving the name using LLMNR

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

In the administrator mode, select [Network] - [TCP/IP Settings] - [TCP/IP Settings], and set [LLMNR] to [Enable].

Tips

To perform name resolution using LLMNR, enable the direct hosting SMB service.

Using in the DFS environment

Configure setting when a distributed file system (DFS, Distributed File System) is employed in your environment.

In the administrator mode, select [Network] - [SMB Settings] - [SMB Client Settings], and set [DFS] to [Enable].

2.3 Configuring the FTP transmission operating 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 1-3.

2 Configuring basic settings for the FTP transmission

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

3 Set the following options according to your environment

Purpose	Reference
Send files to the FTP server via the proxy server	page 2-10

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 Settings] - [FTP TX Settings], then configure the following settings.

Settings	Description
[FTP TX]	Select [Enable] to use the FTP transmission function. [Enable] 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.

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 Settings] - [FTP TX 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"
[Proxy Server Port Number]	If necessary, change the proxy server port number. [21] is specified by default.

2.4 Configuring the WebDAV Send operating 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 1-3.

2 Configure basic settings for WebDAV send

➔ For details on configuring the setting, refer to page 2-11.

3 Set the following options according to your environment

Purpose	Reference
Send files to the WebDAV server via the proxy server	page 2-12
Communicate with the WebDAV server using SSL	page 2-12

Configure basic settings for WebDAV Send

Enable WebDAV Send. 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 Client]	Select [Enable] to use the WebDAV Send function. [Enable] is specified by default.
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the Web-DAV server. [60] sec. is specified by default.
[Domain Name]	Enter the default domain name to be added to the destination host name when data is sent using WebDAV (using ASCII characters of up to 64 bytes).

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

Using SSL communication

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

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

In the administrator mode, select [Address] - [Address Book] - [WebDAV], and set [SSL] to [On] (Default: [Off]).

2.5 Configuring the WS Scan operating 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/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 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 1-3.

2 Configuring the basic settings for the WS scan transmission

➔ For details on configuring the setting, refer to page 2-13.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the computer using SSL	page 2-14

Reference

For details on how to configure settings on the computer, refer to [User's Guide: Scan Functions].

Configuring 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] - [Web Service Settings] - [Common Settings], then configure the following settings.

Settings	Description
[Friendly Name]	Enter the name of this machine to be displayed when this machine is searched for using the Web service through a computer (using up to 127 bytes).

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

Settings	Description
[Scan Function]	Select [Enable] to use the WS scan transmission function. [Enable] is specified by default.
[Scanner Name]	Enter the name of this machine when using it as the WS scanner (using up to 127 bytes).
[Scanner Location]	If necessary, enter the installation location of the scanner (using up to 127 bytes).
[Scanner Information]	If necessary, enter the scanner information (using up to 127 bytes).
[Connection Timeout]	Change the time-out time to limit a communication with the computer if necessary. [120] sec. 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 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 on the computer in advance, and associate it with the TCP/IP communication port (default port number: 5358).

To make SSL communications, enable SSL.

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

Settings	Description
[Secure Mode]	Select [Enable] to use SSL communication. [Disable] is specified by default.

Tips

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

2.6 Configuring the WS print operating environment

Overview

If the Web service function that is available in Windows Vista or later (Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2) is used, this machine that is connected to the network is automatically detected and easily installed as a Web service printer.

HTTP is used for communication between this machine and the computer. In addition, using SSL to encrypt a communication between 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 1-3.

2 Configuring basic settings for the WS printing

➔ For details on configuring the setting, refer to page 2-15.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the computer using SSL	page 2-16

Reference

For details on how to configure settings on the computer, refer to page 3-15.

Configuring 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] - [Web Service Settings] - [Common Settings], then configure the following settings.

Settings	Description
[Friendly Name]	Enter the name of this machine to be displayed when this machine is searched for using the Web service through a computer (using up to 127 bytes).

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

Settings	Description
[Print Function]	Select [Enable] to use the WS print function. [Enable] is specified by default.
[Printer Name]	Enter the name of this machine when using it as a WS printer (using up to 127 bytes, excluding !, \, and ,).
[Printer Location]	If necessary, enter the installation location of the printer (using up to 127 bytes).
[Printer Information]	If necessary, enter the printer information (using up to 127 bytes).

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 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 on the computer in advance, and associate it with the TCP/IP communication port (default port number: 5358).

To make SSL communications, enable SSL.

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

Settings	Description
[Secure Mode]	Select [Enable] to use SSL communication. [Disable] is specified by default.

Tips

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

2.7 Configuring the Internet fax operating environment

Overview

Internet fax is a function used to send and receive faxes 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 receiving large bills for communication 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 using Internet fax, 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 1-3.

2 Configuring basic settings for sending and receiving an Internet fax

➔ For details on configuring the setting, refer to page 2-17.

3 Set the following options according to your environment

Purpose	Reference
Check of a fax reception	page 2-19
Change of the reception capability of this machine that is notified to a peer	page 2-20
Communicate with the E-mail server using SSL/TLS	page 2-20
Use of SMTP Authentication when sending E-mails	page 2-20
Use of POP Before SMTP Authentication when sending E-mails	page 2-21

Tips

To use the Internet Fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

Configuring 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 Settings] - [Network Fax Function Settings], and set [I-Fax] to [Enable].

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

Settings	Description
[Device Name]	Enter the name of this machine (using up to 127 bytes). The name specified here is used as a part of the subject of Internet fax.

3 In the administrator mode, select [System] - [Sender Registration] - [Sender Registration], then configure the following settings.

Settings	Description
[Sender]	Enter the machine name, your company name (sender name) that are to be printed as sender information when faxes are transmitted (using up to 30 bytes).

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

Settings	Description
[E-mail TX (SMTP)]	Select [Enable] to use the Internet fax. [Enable] is specified by default.
[Scan to E-mail]	Select [Enable] to use the Internet fax. [Enable] 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). Normally, you can use the original port number. [25] is specified by default.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (SMTP), if necessary. [60 sec.] is specified by default.
[Device E-mail Address]	Enter the E-mail address of this machine (using ASCII characters of up to 320 bytes). This E-mail address is used as sender Internet fax address.
[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 that have been exceeded the specified size will be discarded. If you select [Binary Division] to divide an E-mail, this setting is invalid.
[Binary Division]	Select [On] 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] is specified by default.
[Divided Mail Size]	Enter the size to divide an E-mail. This item is necessary when [Binary Division] is enabled. [500] KB is specified by default.

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

Settings	Description
[E-mail RX (POP)]	Select [Enable] to use the Internet fax. [Enable] 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"
[Port Number]	If necessary, change the port number of the E-mail server (POP). Normally, you can use the original port number. [110] is specified by default.
[Login Name]	Enter the login name when E-mails are received using the E-mail server (POP) (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 15 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (POP), if necessary. [60 sec.] is specified by default.

Settings	Description
[Auto Check of Arrival]	Select whether or not to check for incoming faxes by periodically connecting this machine to the E-mail server (POP). [Disable] is specified by default.
[Polling Rate]	Specify the interval to connect to the E-mail server (POP) when [Enable] is selected in [Auto Check of Arrival]. [15] minutes 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 [Network] - [Network Fax Settings] - [I-Fax Advanced Setting], then configure the following settings.

Settings	Description
[MDN Request]	Select whether or not 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.
[DSN Request]	Select whether or not 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 or not to return a response message when a sender requests for fax reception result (MDN request) to this machine. [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. [ON] (selected) 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, if necessary.

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

Settings	Description
[Compression Type]	Change the compression type of a fax job the machine can receive.
[Paper Size]	Displays the paper size of a fax job the machine can receive.
[Resolution]	Change the resolution of a fax job the machine can receive.

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 Settings] - [E-mail TX (SMTP)], then configure the following settings.

Settings	Description
[SSL/TLS]	Select the method to encrypt communications with the E-mail server (SMTP). Select [Enable] or [Start TLS] according to your environment. [Disable] is specified by default.
[Port Number (SSL)]	If you select [Enable] in [SSL/TLS], change the communication port number, if necessary. Normally, you can use the original port number. [465] is specified by default.

NOTICE

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

Using SMTP authentication

Configure the setting if your environment requires the SMTP authentication for sending 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 Settings] - [E-mail TX (SMTP)], then configure the following settings.

Settings	Description
[SMTP Authentication]	Select [Enable] to use the SMTP authentication. [Disable] is specified by default.
[Account]	When you have selected [Enable] in [SMTP Authentication], enter the user ID for SMTP authentication (using up to 255 bytes).
[Password]	When you have selected [Enable] in [SMTP Authentication], enter the password (using up to 128 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Domain Name]	When you have selected [Enable] in [SMTP Authentication], enter the domain name (realm) for SMTP authentication (using ASCII characters of up to 255 bytes). This item is necessary when the SMTP authentication method is Digest-MD5.

Using POP Before SMTP authentication

Configure the setting if your environment requires the POP Before SMTP Authentication for sending 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 permits 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) that is used for authentication.

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

Settings	Description
[POP Before SMTP]	Select [Enable] to use POP Before SMTP. [Disable] 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 permitted 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 Settings] - [E-mail RX (POP)], then configure the following settings.

Settings	Description
[E-mail RX (POP)]	Select [Enable] to use POP Before SMTP. [Enable] 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"
[Port Number]	If necessary, change the port number of the E-mail server (POP). Normally, you can use the original port number. [110] is specified by default.
[Login Name]	Enter the login name when E-mails are received using the E-mail server (POP) (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 15 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Connection Timeout]	Change the time-out time to communicate with the E-mail server (POP), if necessary. [60 sec.] 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 Settings] - [E-mail RX (POP)], then configure the following settings.

Settings	Description
[SSL/TLS]	When using SSL to encrypt a communication with the E-mail server (POP), select [Enable]. [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. Normally, you can use the original port number. [995] is specified by default.
[APOP Authentication]	If you use APOP in your E-mail server (POP), select [Enable]. [Disable] is specified by default.

2.8 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.

✔ To use the LDAP function of the Active Directory server, you must match the date and time of this machine to that of Active Directory.

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 1-3.

2 Configuring basic settings for the LDAP search

➔ For details on configuring the setting, refer to page 2-22.

3 Set the following options according to your environment

Purpose	Reference
Communicate with the LDAP server using SSL	page 2-24

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 Settings] - [LDAP Settings], then configure the following settings.

Settings	Description
[LDAP]	Select [Enable] to use the LDAP search. [Disable] is specified by default.

2 In the administrator mode, select [Network] - [LDAP Settings] - [LDAP Server Registration], then configure the following settings.

Item		Description
[LDAP Server Registration]		Register the LDAP server used to search for a destination.
	[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 Number]	If necessary, change the LDAP server port number. Normally, 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 ASCII characters of up to 255 bytes). 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 Result]	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] 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 255 bytes).
	[Password]	Enter the password (using up to 128 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
	[Domain Name]	Enter the domain name to log in to the LDAP server (using ASCII characters of up to 64 bytes). If [GSS-SPNEGO] is selected in [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]. • [Dynamic Authentication]: The system prompts you to enter the user name and password when Address Search (LDAP) is carried out. [Set Value] is specified by default.
	[Use Referral]	Select whether or not 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 the LDAP search is carried out. The setting can be switched between [Name] (cn) and [Nickname] (displayName). [Name] is specified by default.
[Initial Setting for Search Details]		Specify LDAP search conditions. [OR] is specified by default in every case.

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 the administrator mode, select [Network] - [LDAP Settings] - [LDAP Server Registration], then configure the following settings.

Settings	Description
[SSL/TLS]	Select [Enable] to use SSL communication. [Disable] is specified by default.
[Port Number (SSL)]	If necessary, change the SSL communication port number. Normally, you can use the original port number. [636] is specified by default.

2.9 Registering a destination

2.9.1 Registering an address book

Registering E-mail addresses

E-mail addresses can be registered or edited using **Web Connection**.

When using S/MIME function, you can register a user certificate an the E-mail address.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [E-mail] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[E-mail Address]	Enter the E-mail address as a destination (using ASCII characters of up to 320 bytes).
[S/MIME Certification]	Register or delete the certificate to be used for S/MIME. Select the [Edit a Certification] check box, then select [Register a Certification] or [Delete a Certification]. • To register the certificate, the E-mail address of the destination to be registered and that in the certificate must be identical. • Only the DER (Distinguished Encoding Rules) format is supported as a file of certificate information.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 2-38.

Registering an FTP destination

An FTP destination can be registered or edited using **Web Connection**.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [FTP] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[Host Address]	Enter the host name or IP address of the destination FTP server. • 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 the file path is not specified, only enter the "/". • Entry example: "/"
[anonymous]	When authentication is not required for the destination FTP server, select [On]. [Off] is specified by default.

Settings	Description
[User ID]	If authentication is required in the destination FTP server, enter the available user name to log in (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 63 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[PASV Mode]	If the PASV mode is used in your environment, select [On]. [On] is specified by default.
[Proxy]	When a proxy server is used in your environment, select [On]. [Off] is specified by default.
[Port Number]	If necessary, change the port number. Normally, 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 2-38.

Registering an SMB destination

An SMB destination can be registered or edited using **Web Connection**.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [SMB] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[Host Address]	Enter the host name or IP address of a destination computer. • 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). • Entry example: "scan" When specifying a folder in the shared folder, insert a symbol, "\", between folder names. • Entry example: "scan\document"
[User ID]	Enter the name of a user who has privileges to access the folder specified in [File Path] (using up to 255 bytes).
[Password]	Enter the password (using up to 127 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 2-38.

Registering a WebDAV destination

A WebDAV destination can be registered or edited using **Web Connection**.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [WebDAV] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.

Settings	Description
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[Host Address]	Enter the host name or IP address of the destination WebDAV server. • 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 has privileges to access the folder specified in [File Path] (using ASCII characters of up to 63 bytes).
[Password]	Enter the password (using ASCII characters of up to 63 bytes). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[SSL]	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 Number]	If necessary, change the port number. Normally, 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 2-38.

Registering a fax destination

A fax address can be registered or edited using **Web Connection**.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [Fax] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[Address]	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". • Enter "-" to separate a dial number. It does not affect the dialing of the number.
[Destination (Confirmation)]	Enter a destination fax number again to make a confirmation. This option is displayed when you select [Utility] - [Administrator Settings] - [Fax Settings] - [Function Settings] on the **Control Panel** and set [Confirm Address (Register)] to [ON].

Settings	Description
[Communication Setting]	If necessary, specify how to send a fax to a destination you want to register. You may change the settings you made here before sending a fax. • [V34 Off]: V34 is a communication mode that is used for super G3 fax communication. However, when the remote machine or this machine is connected to a telephone line via PBX, you may not establish a communication in super G3 mode depending on telephone line conditions. In this case, it is recommended that you set the V34 mode to 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. If you send a fax using a telephone line in an environment containing static, it may take a longer time to communicate. In this case, the communication time can be reduced by setting ECM to OFF for transmission. However, image or communication errors may occur depending on the specified communication time value, so change the value to suit conditions. • [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 2-38.

Tips

To use the fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

Registering an Internet fax address

An Internet fax address can be registered or edited using **Web Connection**.

In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [New Registration] - [I-Fax] - [Next], then configure the following settings.

Settings	Description
[No.]	Destination registration number. If you enter 0, the smallest available number is automatically assigned. If you want to specify a number, enter the number within the range of 1 to 2000.
[Name]	Enter the destination name (using up to 72 bytes).
[Index]	Select a corresponding character so that the destination can be index searched by registration name. If the [Main] check box is selected, you can easily specify a destination.
[E-mail Address]	Enter the E-mail address as a destination (using ASCII characters of up to 320 bytes).
[Compression Type]	Select a compression type 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.
[Resolution]	Select a resolution 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 2-38.

Tips

To use the Internet Fax function, the optional **Fax Kit FK-512** and **Mount Kit MK-P03** are required.

2.9.2 Registering a group

A group can be registered or edited using **Web Connection**.

Multiple one-touch destinations can be grouped and managed as a single group.

1 In the administrator mode, select [Address] - [Group] - [Group List] - [New Registration], then configure the following settings.

2 Select the type of the destination that you want to register as a group from [Scan] or [Fax], then click [Next].

➔ [Fax] is displayed when the fax function is available.

3 Configure the following settings, then click [Apply].

Settings	Description
[Name]	Enter the destination name (using up to 72 bytes).
[Destination]	In the destination list, select the check box for the address book to be registered as a group. You can narrow down the destinations that appear in the list by [Search by Number], [Search from Index] or [Search from Function].
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 2-38.

2.9.3 Registering a program

A program can be registered or edited using **Web Connection**.

A combination of address information and the fax/scan transmission option settings can be registered in a program.

1 In the administrator mode, select [Address] - [Program] - [Program List], then click [Edit].

2 Select the type of the destination, then click [Next].

3 Specify address information and the destination limit, then click [Apply].

➔ For information on the settings of address information, refer to page 2-25.

➔ For details on the destination limit, refer to page 2-38.

4 Change the program settings, then click [Apply].

➔ The available setting items vary by the destination type that you have selected in Step 2.

Settings	Description
[Resolution]	Select a resolution at which to scan the original. [300×300] is specified by default.
[File Type]	Select the file type used for saving the scanned data. [PDF] is specified by default.
[Page Setting]	Tap this button to select a filing page unit when an original consists of multiple pages. [Multi Page] is specified by default.
[Subject]	Select the fixed subject phrase that is used for E-mail message. [Not Specified] is specified by default.
[Text]	Select the fixed text phrase used for E-mail message. [Not Specified] is specified by default.
[Simplex/Duplex]	Select whether or not 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] 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/Photo] is specified by default.

Settings	Description
[Auto Color]	Select whether or not to automatically specify the color mode according to the original. [On] is specified by default.
[Color Mode]	Select a color mode for scanning originals from Full Color, Grayscale, and Black. [Grayscale] is specified by default.
[Separate Scan]	When there are too many original sheets that cannot be loaded into the **ADF** at the same time, if you want to load them in several batches and handle them as one job, select [On]. [Off] is specified by default.
[Density]	Adjust the density (Dark or Light) to scan the original. [0] 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. [0] is specified by default.
[Sharpness]	Sharpen the edges of images to improve legibility. Smoothen the rough contours of images or sharpen blurred images. [0] is specified by default.
[Scan Size]	Specify the size of the original.
[E-mail Notification]	Select [On] to use the E-mail notification function. Also, enter the destination E-mail address. [Off] 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. [Left] 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 [Long Original] to scan a long original. [Normal] 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.
[Document Name]	Change the file name of the scanned original data (using up to 30 characters).
[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] is specified by default.

2.10 Employing MFP authentication

Overview

Users of this machine can be restricted by the authentication function (MFP authentication) 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.

Configuring basic settings for the user authentication

Enable user authentication. In addition, register the user on this machine.

1 In the administrator mode, select [Security] - [Authentication] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	Select [Device] to employ MFP authentication.
[Public Access]	Select whether or not to permit that public users (unregistered users) to use this machine. • [Allow]: Select this option to use the authentication function of this machine. When a public user uses this machine, press [Public User] on the Login screen to log in to this machine. • [Allow (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]: Does not permit to use this machine by public users. [Allow] is specified by default.

2 In the administrator mode, select [Security] - [Authentication] - [User List] - [New Registration], then register a user.

Settings	Description
[User Name]	Enter the user name to log in to this machine (using up to 64 characters).
[E-mail Address]	If necessary, enter the user's E-mail address (using ASCII characters of up to 320 bytes).
[Password]	Enter the password to log in to this machine (using up to 64 bytes, excluding spaces and "). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Function Permission]	Restrict functions available to users. • [Copy]: Select whether or not to allow use of the copy function. [Allow] is specified by default. • [Scan to Network]: Select whether or not to allow use of the network TX function. [Allow] is specified by default. • [Scan to HDD]: Select whether or not to enable to save files on the HDD of this machine. [Allow] is specified by default. • [Scan to USB Memory]: Select whether or not to enable to save files on a USB memory. [Allow] is specified by default. • [Fax]: Select whether or not to allow use of the fax and Internet fax functions. [Allow] is specified by default. • [Print]: Select whether or not to allow print operations. [Allow] is specified by default. • [Manual Destination Input]: Select whether or not to allow direct input of a destination. [Allow] is specified by default. • [Web browser]: Select whether or not to allow use of the Web browser. [Allow] is specified by default.
[Output Permission (Scan)]	Select whether or not to allow color scan. [Allow] is specified by default.

Settings	Description
[Max. Allowance Set]	Set the maximum number of pages that can be printed. • [Total]: To manage the upper limit, select this check box, then enter the maximum allowance.
[Limiting Access to Destinations]	Restricts destinations the user can access if necessary. For details, refer to page 2-38.

2.11 Employing 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 1-3.

2 Setting 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 1-12.

3 Configuring basic settings for the Active Directory authentication

➔ For details on configuring the setting, refer to page 2-33.

Tips

When employing the Active Directory authentication, you can configure the following setting to use the Scan to Home function. The Scan to Home function can easily send the original data scanned in this machine to a shared folder on a server or that on your computer.

- Registering the Home directory in Active Directory as user's registration information
- Enabling the Scan to Home function of this machine (page 1-23)

Configuring basic settings for the Active Directory authentication

Change the authentication method of this machine so that authentication is performed using an external authentication server.

1 In the administrator mode, select [Security] - [Authentication] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	Select [External Server] to perform authentication using an external authentication server.
[Ticket Hold Time (Active Directory)]	Change the time to hold the Kerberos authentication ticket if necessary. [600] minutes is specified by default.

2 In the administrator mode, select [Security] - [Authentication] - [External Server List], then click [Edit].

3 Select [Active Directory], and click [Next].

4 Register the Active Directory information.

Settings	Description
[Name]	Enter the name of your authentication server (using ASCII characters of up to 32 bytes).
[Default Domain Name]	Enter the default domain name of your authentication server (using ASCII characters of up to 64 bytes).

Reference

You can configure a setting to temporarily save authentication information in the main unit against a case where an external authentication server shuts down. For details, refer to page 1-23.

2.12 Employing account track

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, using this function, you can restrict available functions or manage the use status of this machine by account.

You can use a combination of user authentication and account track to manage each user for each department. You can log in to this machine only by entering the user name. There is no need to specify the account.

Configuring basic account track settings

Enable the account track function. Also register the account.

1 In the administrator mode, select [Security] - [Authentication] - [General Settings], then configure the following settings.

Settings	Description
[Account Track]	Select [On] to employ the account track. [Off] is specified by default.
[Account Track 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, select whether or not to synchronize user authentication and account track. [Synchronize] is specified by default.
[Number of Counters Assigned for Users]	When using user authentication and account track in conjunction, enter the number of counters to be assigned to the user. [500] is specified by default.

2 In the administrator mode, select [Security] - [Authentication] - [Account Track List] - [New Registration], then register an account.

Settings	Description
[Account Name]	Enter the account name to log in to this machine (using up to 8 bytes, excluding spaces and "). You cannot specify a duplicate name.
[Password]	Enter the password to log in to this machine (using up to 8 bytes, excluding spaces and "). To enter (change) the password, select the [Change Password] check box, then enter a new password.
[Output Permission (Scan)]	Select whether or not to allow color scan. [Allow] is specified by default.
[Max. Allowance Set]	Set the maximum number of pages that can be printed. • [Total]: To manage the upper limit, select this check box, then enter the maximum allowance.

2.13 Using the certificate of this machine

2.13.1 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.

The following shows how to use the certificate on this machine.

Usage	Description
Using a self-created certificate	Create a certificate with this machine. The Certificate Authority (CA) is not required, and the certificate can be used simply after entering necessary information to create it. For details, refer to page 2-35.
Using a certificate issued by the Certificate Authority (CA)	Create certificate signing request data on this machine, and request the trusted Certificate Authority (CA) for issuing a certificate for the machine. When the data is returned from the Certificate Authority after review, register the data with this machine. For details, refer to page 2-36.

Self-creating a certificate

Create a certificate with this machine. The Certificate Authority (CA) is not required, and the certificate can be used simply after entering necessary information to create it.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [New Registration] - [Create a Self-signed Certificate] - [Next], and enter information required for creating a certificate, then click [Apply].

Settings	Description
[Common Name]	Displays the IP address of this machine.
[Organization]	Enter the organization or association name (using ASCII characters of up to 63 bytes).
[Organization Unit]	Enter the account name (using ASCII characters of up to 63 bytes). You can also specify a null.
[Locality]	Enter the locality name (using ASCII characters of up to 127 bytes).
[State/Province]	Enter the state or province name (using ASCII characters of up to 127 bytes).
[Country]	Enter the country name. For the country name, specify a country code defined in ISO03166 (using ASCII characters of up to 2 bytes). 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
[Administrator E-mail Address]	Enter the E-mail address of the machine administrator (using ASCII characters of up to 127 bytes).
[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.

2 When the certificate has been installed, enable SSL communication.

➔ For details, refer to page 1-26.

Requesting CA for a certificate issuance

Create certificate signing request data on this machine, and request the trusted Certificate Authority (CA) for issuing a certificate for the machine. When the data is returned from the Certificate Authority after review, register the data with this machine.

1 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [New Registration] - [Request a Certificate] - [Next], and enter information required for issuing a certificate, then click [Apply].

Settings	Description
[Common Name]	Displays the IP address of this machine.
[Organization]	Enter the organization or association name (using ASCII characters of up to 63 bytes).
[Organization Unit]	Enter the account name (using ASCII characters of up to 63 bytes). You can also specify a null.
[Locality]	Enter the locality name (using ASCII characters of up to 127 bytes).
[State/Province]	Enter the state or province name (using ASCII characters of up to 127 bytes).
[Country]	Enter the country name. For the country name, specify a country code defined in ISO03166 (using ASCII characters of up to 2 bytes). 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
[Administrator E-mail Address]	Enter the E-mail address of the machine administrator (using ASCII characters of up to 127 bytes).

2 Click [Save].

➔ Click this button to save certificate signing request data in 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 review, register the data with this machine.

4 In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [Edit] - [Install a Certificate] - [Next], and specify the text data sent from the Certificate Authority (CA), and then click [Apply].

5 When the certificate has been installed, enable SSL communication.

➔ For details, refer to page 1-26.

2.13.2 Managing the certificates for this machine

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.

In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [Edit] - [Export a Certificate] - [Next], and enter the password (using ASCII characters of up to 32 bytes), and then click [Export].

Tips

The entered password is required to import the certificate.

Importing a certificate

The exported certificate can be imported on this machine.

In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [New Registration] - [Import a Certificate] - [Next], specify the certificated to be imported, enter the password, and then click [Apply].

Tips

Enter the password specified when the certificate is exported.

Deleting a certificate

A certificate for this machine can be deleted if necessary.

In the administrator mode, select [Security] - [PKI Settings] - [Device Certificate] - [Edit] - [Delete a Certificate], then click [Next].

2.14 Limiting access to destinations for each user

2.14.1 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.

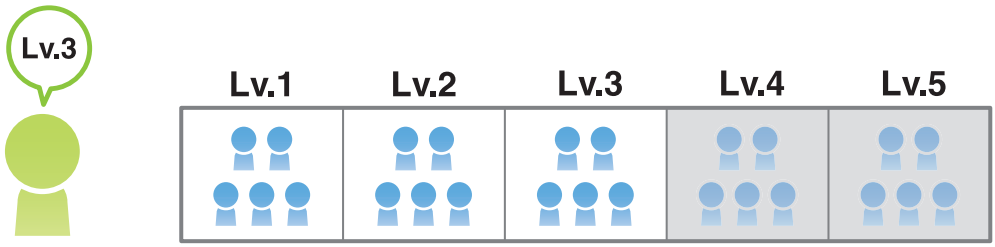
Settings	Description
Managing destinations at the reference allowed level	Sorts destinations depending on the importance level, and set the upper limit of the access level for each user. For details, refer to page 2-38.
Management based on the reference allowed group	Sorts destinations into groups. A user can only access permitted destinations in the group. For details, refer to page 2-39.
Managing destinations in a combination comprising the reference allowed level with 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 2-40.

2.14.2 Managing destinations at the reference allowed level

Reference allowed level

Classify destinations registered in this machine into levels 0 to 5 depending on the importance level, and specify the upper limit (reference allowed level) of the allowable level for each user.

For example, suppose that the reference allowed level 3 is set to a specific user. In this case, the user can refer destinations for which the reference allowed level 1 to 3 are set to, however, they cannot refer destinations for which the reference allowed levels 4 and 5 are set to.



Tips

By default, the reference allowed level, "0", is set to users. Level-0 users can only refer the destinations at level 0.

Specifying the reference allowed level

1 In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [Edit], then select [Reference Allowed Level] to set the reference allowed level to the address book.

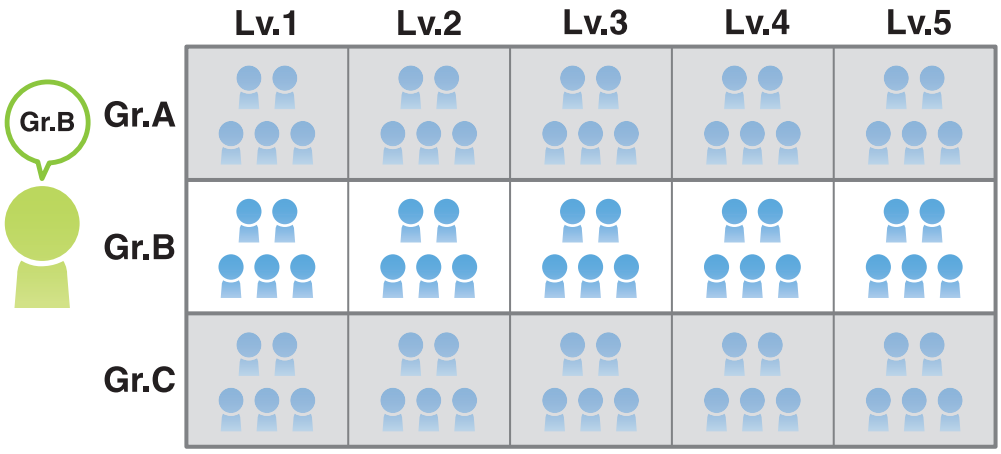
2 In the administrator mode, select [Security] - [Authentication] - [User List] - [Edit], set [Access Allowed Level] to [Enable], then set the reference allowed level to the registered user.

2.14.3 Management 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 Settings] - [Reference Allowed Group List] - [Edit], enter the group name into [Reference Allowed Group Name] (using up to 24 characters), then register the reference allowed group.

2 In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [Edit], then select [Reference Allowed Group] to assign the reference allowed group to the address book.

3 In the administrator mode, select [Security] - [Authentication] - [User List] - [Edit], set [Reference Allowed Group] to [Enable], then assign the reference allowed group to the registered user.

2.14.4 Managing destinations in a combination comprising the reference allowed level with the reference allowed group

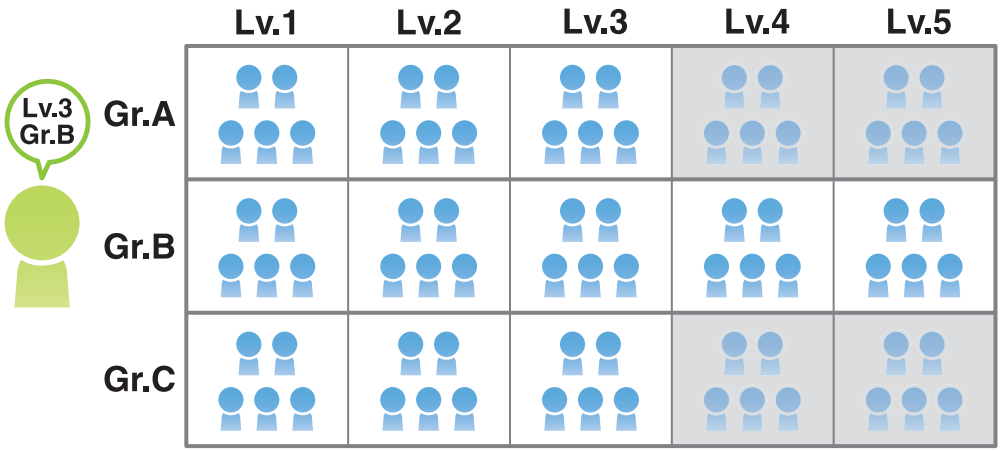
Combining the reference allowed level with the reference allowed group

Management can become more flexible by combining the reference allowed level with the reference allowed group.

For example, suppose that a specified user is set to the reference allowed level 3 and the reference allowed group B.

In this case, the user can refer the following destinations.

- Destinations with reference allowed level 1 to 3: A1 to A3, B1 to B3, C1 to C3
- Destinations included in reference allowed group B: B1 to B5



Tips

The reference allowed level can be set to the reference allowed group. You can assign the reference allowed group with the reference allowed level specified in the address book and combine the reference allowed level with the reference allowed group to manage registered destinations.

Specifying the reference allowed level and the reference allowed group simultaneously

Specify both the reference allowed level and the reference allowed group for a user.

To manage the address book in a combination comprising the reference allowed level and the reference allowed group, register a reference allowed group with the reference allowed level specified , then assign it to the address book.

1 In the administrator mode, select [Security] - [Address Reference Settings] - [Reference Allowed Group List] - [Edit], then register a reference allowed group.

Settings	Description
[No.]	Displays the registration number of a reference allowed group.
[Reference Allowed Group Name]	Enter the name of the reference allowed group (using up to 24 characters).
[Access Allowed Level]	To manage the address book in a combination comprising the reference allowed level and the reference allowed group, select the reference allowed level of the reference allowed group.

2 In the administrator mode, select [Address] - [Address Book] - [Address Book List] - [Edit], then set the reference allowed group or reference allowed level to the address book.

➔ To manage the address book in a combination comprising the reference allowed level and the reference allowed group, assign a reference allowed group with the reference allowed level specified in the address book.

3 In the administrator mode, select [Security] - [Authentication] - [User List] - [Edit], then set the reference allowed group and reference allowed level to 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 the reference allowed level is set to the reference allowed group you selected, it is not involved here.

2.15 Associating a mobile terminal with this machine using the QR code

You can display network information of this machine, which is required to associate with a mobile terminal, as the QR code on the screen of this machine. In the mobile terminal, this machine can be easily registered only by reading the QR code.

✔ Install **Mobile (for iPhone/iPad/Android)** on your mobile terminal in advance.

1 Configure a setting to display network information of this machine using the QR code.

➔ For details on configuring the setting, refer to page 1-18.

2 Tap [Utility] - [User Settings] - [QR Code Display] on the **Control Panel**.

The QR code appears.

3 Start **Mobile (for iPhone/iPad/Android)** to read the QR code.

➔ For details on how to operate **Mobile (for iPhone/iPad/Android)**, refer to the Help of **Mobile (for iPhone/iPad/Android)**.

This machine is registered, and connection settings are completed.

3 Manually Installing the Printer Driver (for Windows)

3 Manually Installing the Printer Driver (for Windows)

3.1 Checking the connection method

In Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2

The installation method for the printer driver differs depending on the method used to connect this machine to the computer. When this machine is connected to the network, there are several printing protocols. The installation method for the printer driver also differs depending on the protocol.

Installation method	Connection method	
Connection method in which setup is possible using Add Printer Wizard	LPR	A network connection using the LPR (Line Printer Remote) print service. It uses a TCP/IP protocol and the LPR printing port. • For the installation procedure, refer to page 3-4.
	Port 9100	A network connection using the PORT9100 print service. It uses a TCP/IP protocol and the RAW printing port. • For the installation procedure, refer to page 3-4.
	IPP/IPPS	A network connection using the IPP (Internet Printing Protocol) print service. Printing can be carried out via the Internet using the HTTP (HyperText Transfer Protocol) of the TCP/IP protocol. IPPS is an IPP for SSL encrypted communication. • For the installation procedure, refer to page 3-11.
	Web service print	It is a connection corresponding to Web service function of Windows Vista and later operating systems and capable of automatically detecting the printer on the network. • For the installation procedure, refer to page 3-15.
	USB	A connection using a USB port.
Connection method in which plug and play-based setup is possible	USB	A connection using a USB port. • For the installation procedure, refer to page 3-16.

In Windows Server 2003

The installation method for the printer driver differs depending on the method used to connect this machine to the computer. When this machine is connected to the network, there are several printing protocols. The installation method for the printer driver also differs depending on the protocol.

Setup procedures	Connection method	
Connection method in which setup is possible using Add Printer Wizard	LPR	A network connection using the LPR (Line Printer Remote) print service. It uses a TCP/IP protocol and the LPR printing port. • For the installation procedure, refer to page 3-4.
	Port 9100	A network connection using the PORT9100 print service. It uses a TCP/IP protocol and the RAW printing port. • For the installation procedure, refer to page 3-4.
	IPP/IPPS	A network connection using the IPP (Internet Printing Protocol) print service. Printing can be carried out via the Internet using the HTTP (HyperText Transfer Protocol) of the TCP/IP protocol. IPPS is an IPP for SSL encrypted communication. • For the installation procedure, refer to page 3-11.
	USB	A connection using a USB port.

Setup procedures	Connection method	
Connection method in which plug and play-based setup is possible	USB	A connection using a USB port. • For the installation procedure, refer to page 3-16.

3.2 Using LPR/Port9100 connection for installation

Operations required to use this function (for administrators)

Configure the LPR/Port 9100 operating environment.

- When using port 9100:
  Make sure that the RAW port number has been set. (In normal circumstances, you can use the default settings.) For details on how to configure the settings, refer to page 1-52.
- When using the LPR:
  Check that LPD is enabled. (In normal circumstances, you can use the default settings.) For details on how to configure the settings, refer to page 1-50.

3.2.1 Installing the printer driver by automatically detecting the printer

In Windows 8/8.1/Server 2012/Server 2012 R2

You can install the printer driver by automatically detecting the printer on the network or by creating a new port.

✔ Administrator privileges are required to perform this task.

✔ Since the printer is searched for during the installation, be sure to connect this machine to the network before turning it on.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

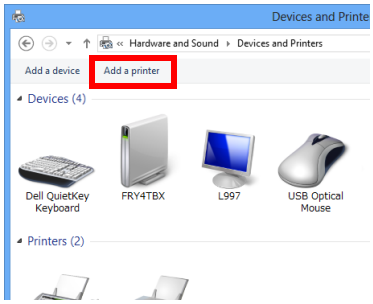
2 Display the printer window.

➔ In Windows 8.1, click [⊕] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].

➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].

➔ In Windows Server 2012/Server 2012 R2, open the Start window, then click [Control Panel] - [Hardware] - [View devices and printers].

3 Select Add a printer.



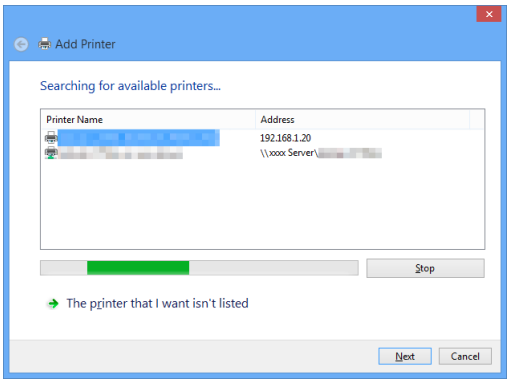
The [Add Printer] wizard appears.

4 Select your machine from the list, then click [Next].

➔ If no printers are detected, restart this machine.

➔ Use the IP address to confirm the printer that you want to connect to.

➔ It may take some time to finish searching the entire list of printers.



5 Click [Have Disk...].

6 Click [Browse...].

7 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver, PS driver, and XPS driver

8 Click [OK].

The [Printers] list appears.

9 Click [Next].

10 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

11 Click [Finish].

12 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Devices and Printers] window.

13 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

In Windows Vista/7/Server 2008/Server 2008 R2

You can install the printer driver by automatically detecting the printer on the network or by creating a new port.

The procedure for installing the printer driver by automatically detecting the printer on the network is as follows:

✔ Administrator privileges are required to perform this task.

✔ Since the printer is searched for during the installation, be sure to connect this machine to the network before turning it on.

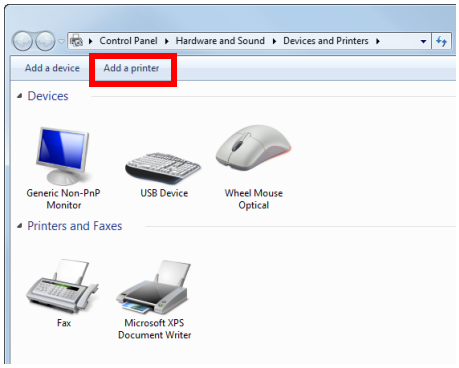
1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 Display the printer window.

➔ In Windows 7/Server 2008 R2, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers]. When [Control Panel] is displayed in an icon, double-click [Devices and Printers].

➔ In Windows Vista/Server 2008, click the Start menu, and select [Control Panel] - [Hardware and Sound] - [Printers]. When [Control Panel] is displayed in Classic View, double-click [Printers].

3 Select Add a printer.



The [Add Printer] wizard appears.

4 Click [Add a network, wireless or Bluetooth printer].

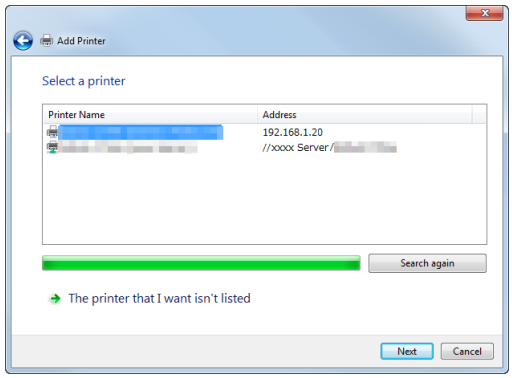
Connected printers are detected.

5 Select your machine from the list, then click [Next].

➔ If no printers are detected, restart this machine.

➔ Use the IP address to confirm the printer that you want to connect to.

➔ It may take some time to finish searching the entire list of printers.



6 Click [Have Disk...].

7 Click [Browse...].

8 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver, PS driver, and XPS driver

9 Click [OK].

The [Printers] list appears.

10 Click [Next].

11 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

12 Click [Finish].

13 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers] or [Devices and Printers] window.

14 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

3.2.2 Installing the printer driver by creating a new port

In Windows 8/8.1/Server 2012/Server 2012 R2

The procedure for installing the printer driver by creating a new port is as follows:

✔ Administrator privileges are required to perform this task.

✔ Since the printer is searched for during the installation, be sure to connect this machine to the network before turning it on.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

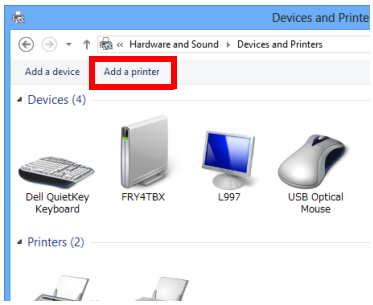
2 Display the printer window.

➔ In Windows 8.1, click [⊙] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].

➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].

➔ In Windows Server 2012/Server 2012 R2, open the Start window, then click [Control Panel] - [Hardware] - [View devices and printers].

3 Select Add a printer.



4 In the window showing the detected printer, click [The printer that I want isn't listed].

5 Click [Add a local printer or network printer with manual settings].

6 Click [Create a new port:], then select [Standard TCP/IP Port].

7 Click [Next].

8 Select [TCP/IP Device], then enter the IP address.

9 Click [Next].

10 Click [Have Disk...].

11 Click [Browse...].

12 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver, PS driver, and XPS driver

13 Click [OK].

The [Printers] list appears.

14 Click [Next].

15 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

16 Click [Finish].

17 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Devices and Printers] window.

18 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

In Windows Vista/7/Server 2008/Server 2008 R2

The procedure for installing the printer driver by creating a new port is as follows:

✔ Administrator privileges are required to perform this task.

✔ Since the printer is searched for during the installation, be sure to connect this machine to the network before turning it on.

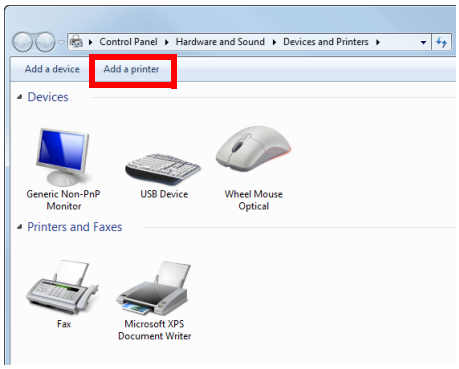
1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 Display the printer window.

➔ In Windows 7/Server 2008 R2, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers]. When [Control Panel] is displayed in an icon, double-click [Devices and Printers].

➔ In Windows Vista/Server 2008, click the Start menu, and select [Control Panel] - [Hardware and Sound] - [Printers]. When [Control Panel] is displayed in Classic View, double-click [Printers].

3 Select Add a printer.



The [Add Printer] wizard appears.

4 Click [Add a local printer].

The [Choose a printer port] dialog box appears.

5 Click [Create a new port:], then select [Standard TCP/IP Port].

6 Click [Next].

7 Select [TCP/IP Device], then enter the IP address.

8 Click [Next].

➔ If the [Additional Port Information Required] dialog box appears, go to Step 9.

➔ If the [Install the printer driver] dialog box appears, go to Step 12.

9 Select [Custom], and then click [Settings...].

10 Change the settings according to the port, and then click [OK].

➔ For an LPR connection, select the [LPR] check box, then enter "Print" in [Queue Name:]. You must discriminate between upper and lower case letters when entering it.

➔ For the Port 9100 connection, select the [Raw] check box, then enter a RAW port number ([9100] by default) in [Port Number:].

➔ If both LPR and Port9100 are enabled on this machine, the printer driver is connected to this machine using LPR.

11 Click [Next].

The [Install the printer driver] dialog box appears.

12 Click [Have Disk...].

13 Click [Browse...].

14 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver, PS driver, and XPS driver

15 Click [OK].

The [Printers] list appears.

16 Click [Next].

17 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

18 Click [Finish].

19 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers] or [Devices and Printers] window.

20 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

In Windows Server 2003

✔ Administrator privileges are required to perform this task.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 From the Start menu, click [Printers and Faxes].

➔ If [Printers and Faxes] is not displayed, select [Control Panel] - [Printers and Other Hardware] - [Printers and Faxes] from the Start menu.

3 Double-click [Add Printer].

[Add Printer Wizard] appears.

4 Click [Next >].

5 Select [Local printer attached to this computer], then click [Next >].

➔ Clear the [Automatically detect and install my Plug and Play printer] check box.

The [Select a Printer Port] page appears.

6 Click [Create a new port:], then select [Standard TCP/IP Port] as the [Type of port:].

7 Click [Next >].

[Add Standard TCP/IP Printer Port Wizard] starts.

8 Click [Next >].

9 In the [Printer Name or IP Address:] box, enter the IP address for the machine, and then click [Next >].

➔ If the [Additional Port Information Required] window appears, go to Step 10.

➔ If the [Finish] screen appears, go to Step 13.

10 Select the [Custom] check box, then click [Settings:].

11 Change the settings according to the port, and then click [OK].

➔ For an LPR connection, select the [LPR] check box, then enter "Print" in [Queue Name:]. You must discriminate between upper and lower case letters when entering it.

➔ For the Port 9100 connection, select the [Raw] check box, then enter a RAW port number ([9100] by default) in [Port Number:].

12 Click [Next >].

13 Click [Finish].

[Add Printer Wizard] appears.

14 Click [Have Disk...].

15 Click [Browse...].

16 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver and PS driver

17 Click [OK].

The [Printers] list appears.

18 Click [Next >].

19 Follow the on-screen instructions to carry out operations.

➔ To use a network connection, perform a test print after the network settings have been configured.

20 Click [Finish].

21 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers and Faxes] window.

22 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

3.3 Using IPP connection for installation

Operations required to use this function (for administrators)

Configure the IPP operating environment.

For details on how to configure the settings, refer to page 1-57.

Tips

You can enhance security by encrypting communication between the computer and this machine with SSL when IPP printing is carried out on this machine (IPPS printing). To use SSL communications, a certificate must be registered in advance. For details on how to configure the settings, refer to page 2-35.

In Windows 8/8.1/Server 2012/Server 2012 R2

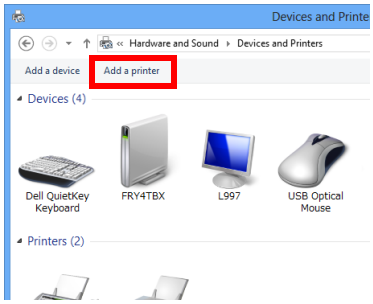
✔ Administrator privileges are required to perform this task.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 Display the printer window.

- ➔ In Windows 8.1, click [⊕] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].
- ➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].
- ➔ In Windows Server 2012/Server 2012 R2, open the Start window, then click [Control Panel] - [Hardware] - [View devices and printers].

3 Select Add a printer.



The [Add Printer] wizard appears.

4 In the window showing the detected printer, click [The printer that I want isn't listed].

5 In [Select a shared printer by name], enter the URL for the machine in the following format, then click [Next].

- ➔ http://<IP address of this machine>/ipp
  Example: http://192.168.1.20/ipp
- ➔ When specifying to use IPPS printing, enter "https://[host name].[domain name]/ipp".
  For [host name].[domain name], specify the host name and domain name registered for the DNS server being used.
- ➔ If the certificate for the machine is not the one issued by the certifying authority, you must register the certificate for the machine on the Windows 8/8.1/Server 2012/Server 2012 R2 system as the certificate by "Trusted Root Certification Authorities" for the computer account.
- ➔ When registering the certificate in the machine, check that the certificate shows [host name].[domain name] as the common name.

6 Click [Have Disk...].

7 Click [Browse...].

8 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver, PS driver, and XPS driver

9 Click [OK].

The [Printers] list appears.

10 Click [Next].

11 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

12 Click [Finish].

13 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Devices and Printers] window.

14 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

In Windows Vista/7/Server 2008/Server 2008 R2

✔ Administrator privileges are required to perform this task.

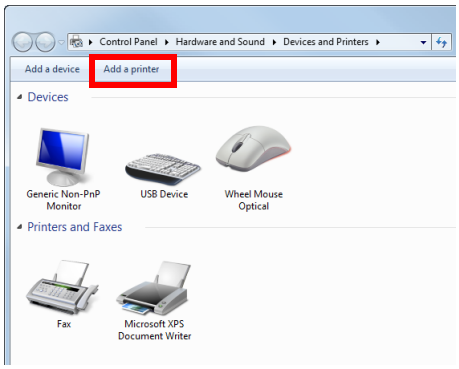
1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 Display the printer window.

➔ In Windows 7/Server 2008 R2, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers]. When [Control Panel] is displayed in an icon, double-click [Devices and Printers].

➔ In Windows Vista/Server 2008, click the Start menu, and select [Control Panel] - [Hardware and Sound] - [Printers]. When [Control Panel] is displayed in Classic View, double-click [Printers].

3 Select Add a printer.



The [Add Printer] wizard appears.

4 Click [Add a network, wireless or Bluetooth printer].

Connected printers are detected.

5 In the window showing the detected printer, click [The printer that I want isn't listed].

6 In [Select a shared printer by name], enter the URL for the machine in the following format, then click [Next].

➔ http://<IP address of this machine>/ipp
Example: http://192.168.1.20/ipp

➔ When specifying to use IPPS printing, enter "https://[host name].[domain name]/ipp".
For [host name].[domain name], specify the host name and domain name registered for the DNS server being used.

➔ If the certificate for the machine is not the one issued by the certifying authority, you must register the certificate for the machine on the Windows Vista/7/Server 2008/Server 2008 R2 system as the certificate by "Trusted Root Certification Authorities" for the computer account.

➔ When registering the certificate in the machine, check that the certificate shows [host name].[domain name] as the common name.

7 Click [Have Disk...].

8 Click [Browse...].

9 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used.
Selectable printer drivers: PCL driver, PS driver, and XPS driver

10 Click [OK].

The [Printers] list appears.

11 Click [OK].

12 Follow the on-screen instructions to carry out operations.

➔ If the [User Account Control] window appears, click [Continue] or [Yes].

13 Click [Finish].

14 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers] or [Devices and Printers] window.

15 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed. Once the settings for the printer have been configured, you can use the printer in the same way as a general local printer.

In Windows Server 2003

✔ Administrator privileges are required to perform this task.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 From the Start menu, click [Printers and Faxes].

➔ If [Printers and Faxes] is not displayed, select [Control Panel] - [Printers and Other Hardware] - [Printers and Faxes] from the Start menu.

3 Double-click [Add Printer].

[Add Printer Wizard] appears.

4 Click [Next >].

5 In the [Local or Network Printer] page, select [A network printer, or a printer attached to another computer], then click [Next >].

6 In the [Specify a Printer] page, select [Connect to a printer on the Internet or on a home or office network:].

7 In [URL:], enter the URL for the machine in the following format, then click [Next >].

➔ http://<IP address of this machine>/ipp
Example: http://192.168.1.20/ipp

➔ When specifying to use IPPS printing, enter "https://[IP address of this machine]/ipp".

➔ If a confirmation dialog box appears after clicking [Next >], click [OK].

8 Click [Have Disk...].

9 Click [Browse...].

10 Select the folder on the CD-ROM containing the desired printer driver, then click [Open].

➔ Select the folder according to the printer driver, operating system, and language to be used.
Selectable printer drivers: PCL driver and PS driver

11 Click [OK].

The [Printers] list appears.

12 Click [OK].

13 Follow the on-screen instructions to carry out operations.

14 Click [Finish].

15 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers and Faxes] window.

16 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed. Once the settings for the printer have been configured, you can use the printer in the same way as a general local printer.

3.4 Using the Web service connection for installation

Web service

The Web service function automatically detects devices on the network and installs the necessary printer drivers.

If you are using Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2, locate the printers that support the Web service print function on the network to install the printer drivers.

Operations required to use this function (for administrators)

Configure the Web service operating environment.

For details on how to configure the settings, refer to page 2-15.

Installation methods

✔ Administrator privileges are required to perform this task.

✔ To install a different printer driver on the computer where one has already been installed, you must uninstall the whole package of the currently installed printer driver.

1 Install the printer driver for this machine.

➔ For details, refer to [User's Guide: Print Functions]. The printer driver can be installed in any port.

2 Turn on the power of the machine while it is connected to the network.

3 In [Network and Sharing Center] on the computer, check that [Network Discovery] is enabled.

4 Open the [Network] window.

➔ In Windows 8/8.1/Server 2012/Server 2012 R2, open [Control Panel], select the [Network and Internet] category, then click [View network computers and devices].

➔ In Windows 7/Server 2008 R2, open [Computer] and click [Network].
If [Network] is not displayed, click the [Network and Internet] category on [Control Panel], then click [View network computers and devices].

➔ In Windows Vista/Server 2008, open the Start menu, and click [Network].

Connected computers and devices are detected.

5 Select the device name of the machine, then click [Install] on the toolbar.

➔ In Windows 8/8.1/Server 2012/Server 2012 R2, click [Network] - [Add devices and printers] on the toolbar. In the displayed window, select the device name of this machine, then click [Next].

The printer driver for this machine is detected and the machine is ready to print.

6 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers] or [Devices and Printers] window.

Reference

If the printer driver is not correctly installed, the driver must be updated using [Update Driver...]. For details, refer to page 3-17.

3.5 Using USB connection for installation

In Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2

To connect this machine using the USB port in Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2, first install the printer driver and then associate it with this machine through plug and play.

- ✔ In Windows 7/8/8.1/Server 2008 R2/Server 2012/Server 2012 R2, the installation disk cannot be specified after the connection has been established. Install the printer driver in advance.
- ✔ In Windows Vista/Server 2008, you can continue the task and specify the printer driver installation disk to install the printer driver if it is not installed in advance.
- ✔ Administrator privileges are required to perform this task.

1. Install the printer driver for this machine.
   - ➔ For details, refer to [User's Guide: Print Functions].
2. Connect this machine to the computer using a USB cable.
3. Turn on the power of this machine.

   The printer driver for this machine is detected and the machine is ready to print.
   - ➔ If the printer driver is not detected, restart this machine.
4. After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers] or [Devices and Printers] window.

Reference

If the printer driver is not correctly installed, the driver must be updated using [Update Driver...]. For details, refer to page 3-17.

In Windows Server 2003

- ✔ Administrator privileges are required to perform this task.

1. Connect this machine to the computer using a USB cable, and then start the computer.
2. Insert the printer driver CD-ROM into the CD-ROM drive of the computer.
3. Turn on the power of this machine.

   The [Found New Hardware Wizard] dialog box appears.
   - ➔ If the [Found New Hardware Wizard] dialog box does not appear, restart this machine.
   - ➔ If a page with a message saying "Windows connect to Windows Update" appears, select [No, not this time].
4. Select [Install from a list or specific location (Advanced)], then click [Next >].
5. Under [Search for the best driver in these locations.], select [Include this location in the search:], then click [Browse].
6. Select the folder on the CD-ROM containing the desired printer driver, then click [OK].
   - ➔ Select the folder according to the printer driver, operating system, and language to be used. Selectable printer drivers: PCL driver and PS driver
7. Click [Next >], and perform the procedure by following the on-screen instructions.
8. Click [Finish].
9. After finishing the installation, make sure that the icon for the installed printer is displayed in the [Printers and Faxes] window.

10 Remove the CD-ROM from the CD-ROM drive.
Installation of the printer driver is then completed.

Updating the printer driver

In Windows 7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2, if this machine is connected without the printer driver having first been installed, the printer driver will not be correctly identified. If the printer driver is not correctly identified, the driver must be updated using [Update Driver...].

1 Display the printer window.

- ➔ In Windows 8.1, click [⊛] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].
  When [Control Panel] is displayed in an icon, double-click [Devices and Printers].
- ➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].
  When [Control Panel] is displayed in an icon, double-click [Devices and Printers].
- ➔ In Windows Server 2012/Server 2012 R2, open the Start window, then click [Control Panel] - [Hardware] - [View devices and printers].
  When [Control Panel] is displayed in an icon, double-click [Devices and Printers].
- ➔ In Windows 7/Server 2008 R2, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers].
  When [Control Panel] is displayed in an icon, double-click [Devices and Printers].

2 Right-click the device name of the machine that is under [Unspecified] and then click [Properties].

- ➔ If [Unknown Device] appears instead of the device name of the machine, right-click to remove the device, and install the printer driver.

3 In the [Hardware] tab, click [Properties].

4 In the [General] tab, click [Change Settings].

5 In the [Driver] tab, click [Update Driver...].

6 In the page in which to select how to search the driver software, click [Browse my computer for driver software anyway].

7 Click [Browse...].

8 Select the folder on the CD-ROM containing the desired printer driver, then click [OK].

- ➔ Select the folder according to the printer driver, operating system, and language to be used.
  Selectable printer drivers: PCL driver, PS driver, and XPS driver

9 Click [Next].

10 Follow the on-screen instructions to carry out operations.

11 Click [Close].

12 After finishing the installation, make sure that the icon for the installed printer is displayed in the [Devices and Printers] window.

13 Remove the CD-ROM from the CD-ROM drive.
This completes the update of the printer driver.

3.6 Manually uninstalling the printer driver

If the printer driver was installed without using the installer, manually uninstall the printer driver.

1 Display the printer window.

- ➔ In Windows 8.1, click [⊕] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].
- ➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].
- ➔ In Windows Server 2012/Server 2012 R2, open the Start window, then click [Control Panel] - [Hardware] - [View devices and printers].
- ➔ In Windows 7/Server 2008 R2, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers].
- ➔ In Windows Vista/Server 2008, click the Start menu, and select [Control Panel] - [Hardware and Sound] - [Printers]. When [Control Panel] is displayed in Classic View, double-click [Printers].
- ➔ In Windows Server 2003, click the Start menu, then select [Printers and Faxes].
  If [Printers and Faxes] is not displayed, select [Control Panel] - [Printers and Other Hardware] - [Printers and Faxes]. When [Control Panel] is displayed in Classic View, double-click [Printers].

2 Click the icon of the printer driver to be uninstalled.

3 Uninstall the printer driver.

- ➔ In Windows 7/8/8.1/Server 2008 R2/Server 2012/Server 2012 R2, click [Remove device] on the toolbar.
- ➔ In Windows Vista/Server 2003/Server 2008, press the [Delete] key on the computer keyboard.

4 From then on, follow the on-screen instructions to carry out operations.

When the printer driver ha been uninstalled, the icon disappears from the window.

5 Open [Server Properties].

- ➔ In Windows 7/8/8.1/Server 2008 R2/Server 2012/Server 2012 R2, select a different printer, and click [Print Server Properties] on the toolbar.
- ➔ In Windows Vista/Server 2008, right-click on the area that has nothing displayed in the [Printers] window, click [Run as administrator] - [Server Properties].
- ➔ In Windows Server 2003, click the [File] menu, then [Server Properties].
- ➔ If the [User Account Control] window appears, click [Continue] or [Yes].

6 Click the [Driver] tab.

7 From the [Installed printer drivers:] list, select the printer driver to be uninstalled, then click [Remove...].

- ➔ In Windows Vista/7/8/8.1/Server 2008 R2/Server 2012/Server 2012 R2, go to Step 8.
- ➔ In Windows Server 2003, go to Step 9.

8 Select [Remove driver and driver package.] in the dialog box for confirming to remove the target, then click [OK].

9 In the dialog box for confirming if you are sure to remove the printer, click [Yes].

- ➔ If you are using Windows Vista/7/8/8.1/Server 2008 R2/Server 2012/Server 2012 R2, the dialog box appears to reconfirm whether you are sure you want to remove the printer. Click [Uninstall].

10 Close the open windows, and then restart the computer.

- ➔ Be sure to restart the computer.

Uninstallation of the printer driver is then completed.

Tips

In Windows Server 2003, if the printer driver is uninstalled in the above procedure, the model information files remain on the computer. For this reason, when reinstalling the same version of the printer driver, the driver may not be rewritten. In this case, remove the following files as well.

- Check the "C:\WINDOWS\system32\spool\drivers\w32×86" folder ("C:\WINDOWS\system32\spool\drivers\×64" folder in the ×64 system), and if there is a folder of the corresponding model, remove it. However, if multiple drivers are installed including the PCL KONICA MINOLTA driver, PostScript KONICA MINOLTA driver and fax driver, the model information of all drivers is deleted. To leave drivers other than the fax driver, do not remove the folder.
- From the "C:\WINDOWS\inf" folder, remove "oem*.inf" and "oem*.PNF" ("*" included in the file name indicates a number, which differs depending on the computer environment).
  Before removing these files, open the inf file, and then check the model name described on the last few lines to confirm it is the file for the corresponding model. The number of the PNF file is the same as that of the inf file.
- If you have deleted a file using [Remove driver and driver package.] in Windows Vista/7/8/8.1/Server 2008/Server 2008 R2/Server 2012/Server 2012 R2, this operation is not required.

4 Adding a Printer Using LPR/IPP Connection (Mac OS Environment)

4 Adding a Printer Using LPR/IPP Connection (Mac OS Environment)

4.1 Using LPR connection

Operations required to use this function (for administrators)

Configure the LPR operating environment.

For details on how to configure the settings, refer to page 1-50.

In Mac OS X 10.4 and later

In Mac OS X 10.4 and later, use the following procedure to add a printer using an LPR connection:

1 Select [System Preferences...] in the Apple menu.

2 Click the [Network] icon.

3 The Ethernet setting window appears.

➔ In Mac OS X 10.5 and later, select [Ethernet], then click [Advanced...].

➔ In Mac OS X 10.4, select [Built-in Ethernet], then click [Configure...].

4 Click the [TCP/IP] tab.

5 Configure the settings including the IP address and subnet mask according to the settings of the network to which the computer is connected.

6 Click the close button at the top left corner of the window.

➔ When the [Apply configuration changes] message appears, click [Apply].

Then, add the printer to the computer.

7 Select [System Preferences...] in the Apple menu.

8 Click the [Print & Fax] icon.

➔ In Mac OS X 10.7/10.8, click the [Print & Scan] icon. In Mac OS X 10.9, click the [Printer & Scanner] icon.

9 Click [+] in the lower left of the screen.

➔ In Mac OS X 10.7/10.8/10.9, select [Add Other Printer or Scanner...] or [Add Printer or Scanner...] in the list that is displayed by clicking [+].

10 Click [IP] or [IP Printer].

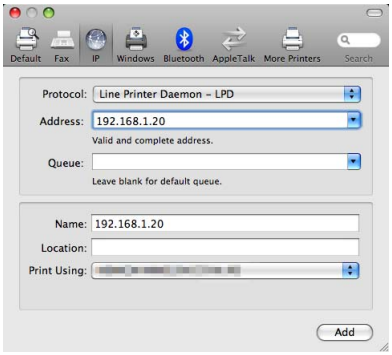
11 In [Protocol:], select [Line Printer Daemon - LPD].

12 In [Address:], enter the IP address for the machine.

The printer driver for the machine specified with the IP address is displayed in [Print Using:].

➔ When the printer driver is displayed, go to Step 14.

➔ When the printer driver is not correctly displayed, go to Step 13.



13 Manually select the printer driver.

➔ In Mac OS X 10.9, select [Select Software...] from [Print Using:], then click the driver of the desired printer from the list that is displayed in another window.

➔ In Mac OS X 10.6/10.7/10.8, select [Select Printer Software...] from [Print Using:], then click the driver of the desired printer from the list that is displayed in another window.

➔ In Mac OS X 10.5, select [Select a driver to use...] in [Print Using:], then click the driver of the desired printer from the list.

➔ In Mac OS X 10.4, select [KONICA MINOLTA] in [Print Using:], and then click the driver of the desired printer from the list.

14 Click [Add].

Addition of the printer is then completed.

In Mac OS X 10.3

In Mac OS X 10.3, use the following procedure to add a printer using an LPR connection:

1 Select [System Preferences...] in the Apple menu.

2 Click the [Network] icon.

3 From [Show], select [Built-in Ethernet].

4 Click the [TCP/IP] tab.

5 Select the [Settings:] item and configure the settings including the IP address and subnet mask according to the settings for the network to which the computer is connected.

6 Click the close button at the top left corner of the window.

➔ When the [Apply configuration changes] message appears, click [Apply].

Then, add the printer to the computer.

7 Select [Macintosh HD] (hard disk of the system) - [Applications] - [Utilities], then double-click [Printer Setup Utility] to open the dialog box.

8 When the [You have no printers available.] window appears, click [Add]. When the Printer List appears, click [Add].

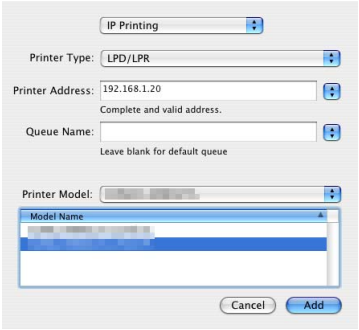
➔ If available printers have already been specified, the [You have no printers available.] window does not appear.

9 Select [IP Printing] as the connection method.

10 In [Printer Type:], select [LPD/LPR].

11 In [Printer Address:], enter the IP address for the machine.

12 In [Printer Model:], select [KONICA MINOLTA], then click the driver of the desired printer from the model list.



13 Click [Add].

Addition of the printer is then completed.

4.2 Using IPP connection

Operations required to use this function (for administrators)

Configure the IPP operating environment.

For details on how to configure the settings, refer to page 1-57.

In Mac OS X 10.4 and later

In Mac OS X 10.4 and later, use the following procedure to add a printer with an IPP connection:

1 Select [System Preferences...] in the Apple menu.

2 Click the [Network] icon.

3 The Ethernet setting window appears.

➔ In Mac OS X 10.5 and later, select [Ethernet], then click [Advanced...].

➔ In Mac OS X 10.4, select [Built-in Ethernet], then click [Configure...].

4 Click the [TCP/IP] tab.

5 Configure the settings including the IP address and subnet mask according to the settings of the network to which the computer is connected.

6 Click the close button at the top left corner of the window.

➔ When the [Apply configuration changes] message appears, click [Apply].

Then, add the printer to the computer.

7 Select [System Preferences...] in the Apple menu.

8 Click the [Print & Fax] icon.

➔ In Mac OS X 10.7/10.8, click the [Print & Scan] icon. In Mac OS X 10.9, click the [Printer & Scanner] icon.

9 Click [+] in the lower left of the screen.

➔ In Mac OS X 10.7/10.8/10.9, select [Add Other Printer or Scanner...] or [Add Printer or Scanner...] in the list that is displayed by clicking [+].

10 Click [IP] or [IP Printer].

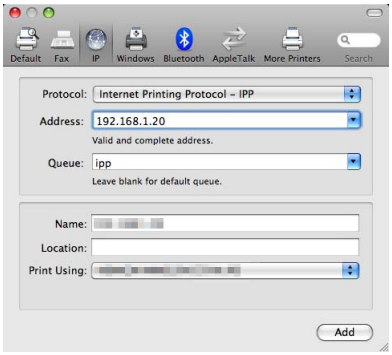
11 In [Protocol:], select [Internet Printing Protocol - IPP].

12 In [Address:], enter the IP address for the machine. In [Queue:], enter "ipp".

The printer driver for the machine specified with the IP address is displayed in [Print Using:].

➔ When the printer driver is displayed, go to Step 14.

➔ When the printer driver is not correctly displayed, go to Step 13.



13 Manually select the printer driver.

➔ In Mac OS X 10.9, select [Select Software...] from [Print Using:], then click the driver of the desired printer from the list that is displayed in another window.

➔ In Mac OS X 10.6/10.7/10.8, select [Select Printer Software...] from [Print Using:], then click the driver of the desired printer from the list that is displayed in another window.

➔ In Mac OS X 10.5, select [Select a driver to use...] in [Print Using:], then click the driver of the desired printer from the list.

➔ In Mac OS X 10.4, select [KONICA MINOLTA] in [Print Using:], and then click the driver of the desired printer from the list.

14 Click [Add].

Addition of the printer is then completed.

In Mac OS X 10.3

In Mac OS X 10.3, use the following procedure to add a printer with IPP connection:

1 Select [System Preferences...] in the Apple menu.

2 Click the [Network] icon.

3 From [Show], select [Built-in Ethernet].

4 Click the [TCP/IP] tab.

5 Select the [Settings:] item and configure the settings including the IP address and subnet mask according to the settings for the network to which the computer is connected.

6 Click the close button at the top left corner of the window.

➔ When the [Apply configuration changes] message appears, click [Apply].

Then, add the printer to the computer.

7 Select [Macintosh HD] (hard disk of the system) - [Applications] - [Utilities], then double-click [Printer Setup Utility] to open the dialog box.

8 When the [You have no printers available.] window appears, click [Add]. When the Printer List appears, click [Add].

➔ If available printers have already been specified, the [You have no printers available.] window does not appear.

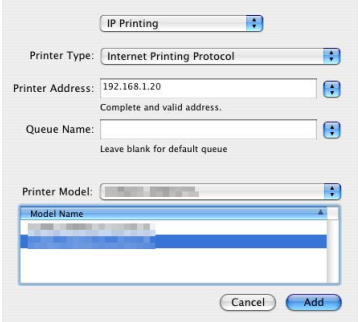
9 Select [IP Printing] as the connection method.

10 In [Printer Type:], select [Internet Printing Protocol - IPP].

11 In [Printer Address:], enter the IP address for the machine.

➔ Leave [Queue Name:] blank.

12 In [Printer Model:], select [KONICA MINOLTA], then click the driver of the desired printer from the model list.



13 Click [Add].

Addition of the printer is then completed.

5 Printing in the Linux Environment

5 Printing in the Linux Environment

5.1 System environment requirements

Before installing the printer driver, check the following operating environment.

Item	Specifications
Operating system	Red Hat Enterprise Linux 4/5/6 Desktop SUSE Linux Enterprise Desktop 9/10/11 Red Hat Enterprise Linux 4/5/6 server SUSE Linux Enterprise Server 9/10/11
CPU	Any processor of the same or higher specifications as recommended for your operating system
Memory	Memory capacity as recommended for your operating system
Drive	CD-ROM drive

Tips

The following describes the operation procedure using Red Hat Enterprise Linux 5, as an example.

5.2 Preparation for printing

5.2.1 Adding the printer

✔ Before installing the printer driver, exit all application software.
✔ Root authority is required to add a printer.

1 Connect this machine to the computer via USB or network.

➔ If a dialog box to specify the printer driver appears when you use USB to connect this machine, click [Cancel] to close the dialog box.

2 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

3 From the [System] menu, select [Administration] - [Printing].

4 Click [New Printer].

5 Enter the [Printer name], [Description], and [Location], and click [Forward].

The printer is automatically detected in the device column.

6 Select the connection method.

➔ When USB is used, select "Name of this machine USB #1" in the device column.
➔ When connecting via network, select this machine that was automatically detected in the device column.
➔ If this machine is not displayed in the device column, select the port according to the connection method.
[AppSocket/HP jetDirect], [Internet Printing Protocol (ipp)], or [LPD/LPR Host or Printer]

7 Click [Forward].

8 Select [Provide PPD file].

9 Click the folder icon, and specify the PPD file on the CD-ROM.

➔ You can obtain the PPD file of the various languages in the "Drivers/LinuxPPD/<language>" folder. Select the PPD file suitable for your language.

10 Click [Forward].

11 Click [Apply].

12 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed.

5.2.2 Manually adding the printer driver

Manually installing the PPD file

✔ Before installing the printer driver, exit all application software.
✔ Root authority is required to install the printer driver.

1 Insert the printer driver CD-ROM into the CD-ROM drive of the computer.

2 From the CD-ROM, copy the PPD file to "/usr/share/cups/model".

➔ You can obtain the PPD file of the various languages in the "Drivers/LinuxPPD/<language>" folder. Select the PPD file suitable for your language.

3 From the main menu, select [Application] - [Accessories] - [Terminal].

4 Restart CUPS.

➔ Enter "/etc/init.d/cups restart", and press the Enter key.

5 Exit the [Terminal].

6 Remove the CD-ROM from the CD-ROM drive.

Installation of the printer driver is then completed. Continue to "Adding a printer from CUPS Administration Web Page".

Adding a printer from CUPS Administration Web Page

✔ Root authority is required to install the printer driver.

1 Connect this machine to the computer via USB or network.

➔ If a dialog box to specify the printer driver appears when you use USB to connect this machine, click [Cancel] to close the dialog box.

2 Start the Web browser.

3 Enter "http://localhost:631" in the URL field.

The CUPS Administration Web page appears.

4 Click [Add Printer].

5 Enter the [Name], [Location], and [Description], then click [Continue].

6 Select the connection method in the device list, then click [Continue].

➔ When the TCP/IP connection is used: Select [AppSocket/HP jetDirect], [Internet Printing Protocol (ipp)], or [LPD/LPR Host or Printer].

➔ When the USB connection is used: Select [USB Printer #1], then go to Step 8.

7 Enter the device URI in the following format, then click [Continue].

➔ socket://(printer name or IP address of this machine): (port number)
Example of IP address entry: socket://192.168.1.190:9100
Example of printer name entry: socket://Hostname:9100
(You can use the IP address as a substitute for the printer name. Also, you can omit the port number.)

8 In the manufacturer column, select [KONICA MINOLTA], then click [Continue].

➔ You can obtain the PPD file of the various languages in the "Drivers/LinuxPPD/<language>" folder. Select the PPD file suitable for your language.

9 Select this machine in the model column, then click [Add Printer].

10 To use the administrator privileges, enter the user name and password, then click [OK].

5.2.3 Configuring the default settings of the printer driver

When you use this machine for the first time, properly configure the printer driver so that it contains information such as the options installed on this machine. If necessary, you can change the default print settings of the printer driver.

Tips

- The name and display order of the settings vary depending on your operating system, its version, or the CUPS version.
- The following describes the print functions unique to this machine.

1 Start the Web browser.

2 Enter "http://localhost:631" in the URL field.

3 Click [Manage Printer].

4 Click [Set Printer Options].

The printer drive setup page appears.

[Options Installed]

Item	Description
[Paper Source Unit]	Select the paper feed unit that is installed on this machine. [None] is specified by default.
[Hard Disk]	Select [Installed] for this machine.
[Finisher]	Select [Installed] if the optional **Finisher** is installed on this machine. [None] is specified by default.

NOTICE

You cannot use the optional functions unless the name of this machine and installed options are specified. If any option is installed, be sure to specify it.

[General]

Item	Description
[Collate]	When printing multiple sets of copies, select this check box to output sets of copies one by one. [On] is specified by default.
[Paper Source]	Select the paper tray for the printing paper.
[Paper Type]	Select the paper type used for printing.
[Resolution]	Select the print resolution. [600dpi] is specified by default.
[Paper Size]	Select the size of paper for printing.
[Nearest Size and Scale]	Select whether or not to use paper of the appropriate size by automatically enlarging or reducing the original data if the size of sheets of the paper loaded in the paper tray does not match that of original data. [Off] is specified by default.
[Print Type]	Select the print sides of paper. [2-Sided] is specified by default.
[Staple]	Specify the staple position when stapling printed sheets of paper. [Off] is specified by default.
[Original Direction]	Specify the orientation of the original. [Portrait] is specified by default.
[Binding Position]	Select the binding position. [Left Bind] is specified by default.

Item	Description
[Edge Strength]	Select the degree of edge enhancement when sharpening the edges. [Middle] is specified by default.

[Image Options]

Item	Description
[Image Halftone]	Select the half-tone image processing method. [Detail] is specified by default.
[Image Edge Enhancement]	Select whether or not to sharpen the edges. [Off] is specified by default.

[Text Options]

Item	Description
[Text Halftone]	Select the half-tone image processing method. [Line Art] is specified by default.
[Text Edge Enhancement]	Select whether or not to sharpen the edges. [On] is specified by default.

[Graphics Options]

Item	Description
[Graphics Halftone]	Select the half-tone image processing method. [Detail] is specified by default.
[Graphics Edge Enhancement]	Select whether or not to sharpen the edges. [On] is specified by default.

5.3 Printing procedure

The following describes the printing procedure using OpenOffice in Red Hat Enterprise Linux 5.

✔ The contents of the print dialog and print setting dialog vary depending on the application.

✔ The following steps and operations may vary depending on the version of your operating system.

1 Open data of the original using the application software. From the [File] menu, select [Print].

2 Specify the printer that you want to use for printing.

3 Click [Print].

Printing is executed.

6 Using the Authentication Unit (IC Card Type)

6 Using the Authentication Unit (IC Card Type)

6.1 Authentication Unit (IC card type)

The **Authentication Unit** (IC card type) is an "IC card authentication" system that reads the IC Card / NFC-compatible mobile terminal to perform personal authentication. If you register a compatible noncontact IC card such as an employee ID card, you can use this machine synchronously with functions such as the user entering-leaving management to integrate the authentication system.

If this machine provides user authentication, you can log in to this machine or execute a print job using the IC Card / NFC-compatible mobile terminal authentication function.

Tips

- To enable IC card authentication, settings made by the service representative are required in addition to the optional **Authentication Unit AU-201/AU-201S**. For details, contact your service representative.
- To employ user authentication using an NFC-compatible mobile terminal, settings by the service representative are required in addition to the optional **Authentication Unit AU-201S**. For details, contact your service representative.
- To use an NFC-compatible mobile terminal, Android 4.4 or later must be supported as the operating system, and the HCE function must be provided.

6.2 Status of Authentication Device

The status of the authentication device is indicated by status indicator LEDs.

LED Status indicator LED	Status of authentication device
Light-up (Yellow green)	Normally running
Light-up (Orange)	USB communications are not available.
Light-up (Red)	Out of order

6.3 Operations required to use this function (for Administrators)

6.3.1 Configuring authentication settings of this machine

You must specify user authentication as MFP authentication on this machine.

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

2 In the administrator mode, select [Security] - [Authentication] - [General Settings], then configure the following settings.

Settings	Description
[User Authentication]	Select [Device] to employ MFP authentication.

3 In the administrator mode, select [Security] - [Authentication Device Settings] - [General Settings], then configure the following settings.

Settings	Description
[Authentication Type]	Select how to log in to this machine. • [Card Authentication]: Allows the user to log in by simply placing the IC Card / NFC-compatible mobile terminal. • [Card Authentication+Password]: Allows the user to log in by placing the IC Card / NFC-compatible mobile terminal and entering the password. [None] is specified by default.
[IC Card Type]	Select the type of the IC card to be used. [Type A] is specified by default.

The authentication setting is then completed.

After the authentication function of this machine (MFP authentication) has been configured, register user authentication information.

6.3.2 Registering user authentication information

Connect the authentication unit to a computer, and use **Data Administrator** through a computer to register information.

Data Administrator

Data Administrator is a management tool to edit or register authentication information or address information of the target device through a computer on the network.

Using this tool, you can import authentication information or address information from a device and rewrite it to the device after editing.

Setting up Data Administrator

For setup, install the **IC CardDriver (USB-Driver)** of the authentication unit, then install **Data Administrator PlugIn for IC Card Authentication Unit AU-201/AU-201S**.

✔ The following describes the setup procedure in the Windows 7/8/8.1 system.

✔ Before setup, install **Data Administrator V4.1.31500** or later on your computer. For details on installation, refer to the relevant **Data Administrator** manual.

✔ To check the version of your **Data Administrator**, select the [Help] menu in **Data Administrator**, and also select [Version Information] - [Plug-in version].

✔ **IC CardDriver (USB-Driver)** and **Data Administrator PlugIn** are stored on the CD-ROM included in the authentication unit.

1 Turn the **Power Switch** of this machine off, and disconnect the authentication unit from this machine.

2 Install **IC CardDriver (USB-Driver)**.

➔ Connect the authentication unit to the USB port of your computer.

NOTICE

When connecting or disconnecting the USB cable, hold the plug. Otherwise, the machine may be damaged or a failure may occur.

Do not connect another USB device to the same port as for the authentication unit. Doing so reduces the USB power supply, resulting in an operation failure.

To use the USB hub, connect the self-power USB hub that supplies 500 mA or more.

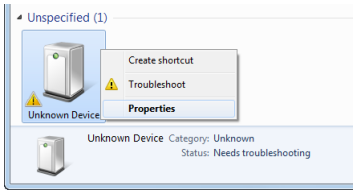
3 Open the [Devices and Printers] window.

➔ In Windows 8.1, click [⊕] in the Start window, then click [Control Panel] - [Hardware and Sound] - [View devices and printers].

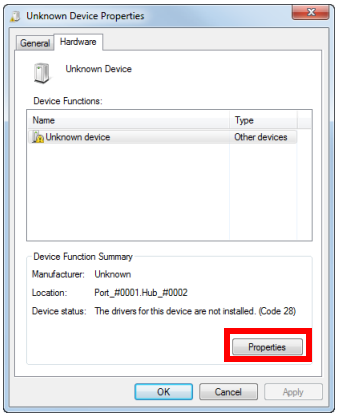
➔ In Windows 8, right-click the Start window, then click [All apps] - [Control Panel] - [Hardware and Sound] - [View devices and printers].

➔ In Windows 7, open the Start menu, then click [Devices and Printers]. If [Devices and Printers] is not displayed, select [Control Panel] - [Hardware and Sound], and click [View devices and printers].

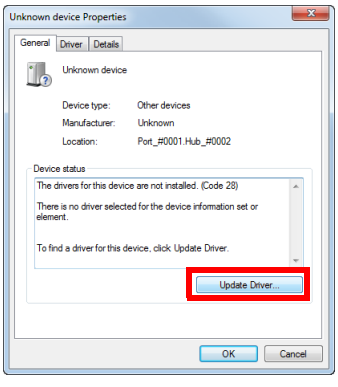
4 Right-click the device name or [Unknown Device] of the authentication unit displayed in the [Unspecified] category, then click [Properties].



5 In the [Hardware] tab, click [Properties].



6 In the [General] tab, click [Update Driver...].



7 On the screen in which to select how to search the driver software, click [Browse my computer for driver software anyway].

8 Click [Browse...].

9 Select the IC CardDriver (USB-Driver) file on the computer, then click [OK].

10 Click [Next], and perform the procedure by following the on-screen instructions.

➔ If the [Windows Security] dialog box for verifying the publisher appears, click [Install this driver software anyway].

11 When the installation is complete, click [Close].

Then, install **Data Administrator PlugIn for IC Card Authentication Unit AU-201/AU-201S**.

12 Click setup.exe of **Data Administrator PlugIn**.

13 If necessary, select the setup language, and click [OK].

14 Follow the on-screen instructions to proceed the installation.

15 Click [Next].

16 Select [I accept the terms in the license agreement], then click [Next].

17 Click [Install].

18 When the installation is complete, click [Finish].

This completes the installation of **Data Administrator PlugIn for IC Card Authentication Unit AU-201/AU-201S**, which completes the setup.

Registering user authentication information

✔ To register user authentication information with **Data Administrator**, connect the authentication unit to the computer's USB port, and also connect the computer to this machine via network.

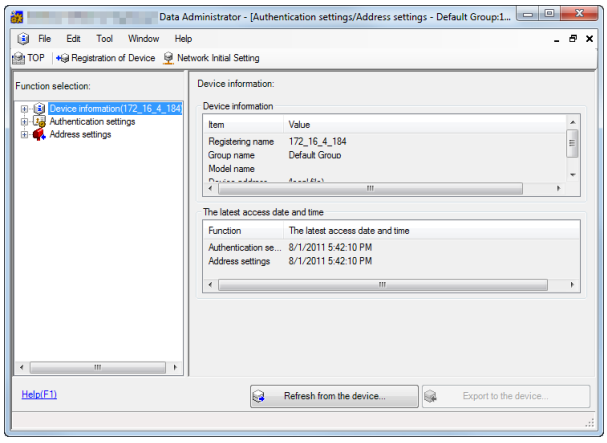
✔ To use an NFC-compatible mobile terminal, **Mobile for Android** must be installed on the terminal. In addition, the NFC authentication function for the IC card reader must be enabled on the **Mobile for Android** setting screen. For details on the setting method, refer to the Help of **Mobile for Android**.

1 Turn on the **Power Switch** of this machine.

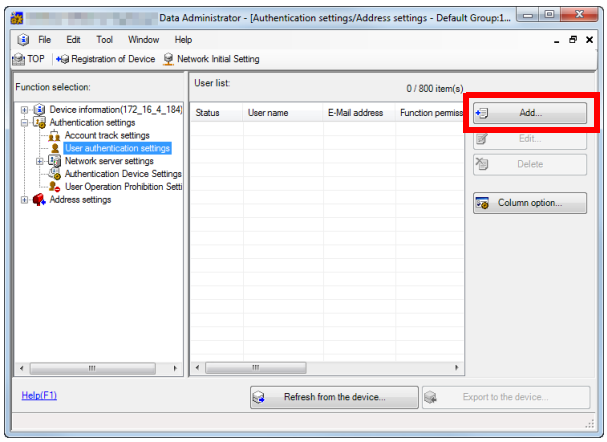
2 Start **Data Administrator**, and import device information of this machine.

➔ Restart the procedure five or more seconds after connecting the authentication unit.

➔ For details about how to import device information, refer to the relevant **Data Administrator** manual.



3 In [Function selection], select [Authentication Settings] - [User authentication settings], and then click [Add].



4 Select a user template, and click [OK].

➔ For details on templates, refer to the relevant **Data Administrator** manual.

The User Registration screen appears.

5 Enter the user name and password, and select the [IC Card / NFC authentication] tab.

6 Place the IC Card / NFC-compatible mobile terminal on the authentication unit, then click [Start reading].

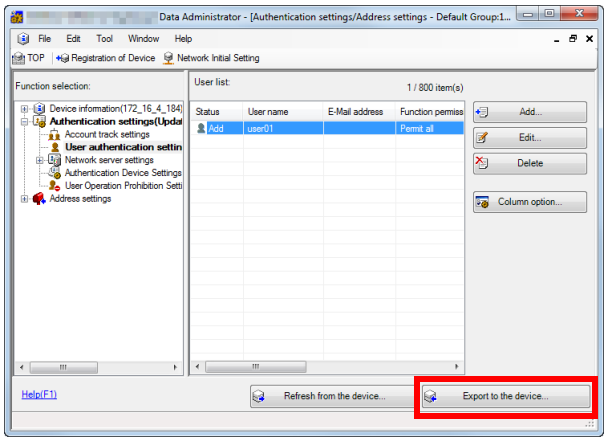
➔ You can also register the card by directly entering the card ID.

➔ To use an NFC-compatible mobile terminal, display its screen in advance. You do not need to start **Mobile for Android**.

7 Click [OK], and register authentication information of the next user.

8 After the registration of authentication information has been completed for all users, click [Export to the device].

➔ When necessary, select a user name, and click [Edit] to change registered information.



9 Click [Write].

➔ **Data Administrator** supports the batch copy function. If necessary, you can collectively write the registered authentication information to multiple devices.

10 When writing to this machine has finished, click [OK].

11 Disconnect the authentication unit from the computer's USB port.

NOTICE
When connecting or disconnecting the USB cable, hold the plug. Otherwise, the machine may be damaged or a failure may occur.

12 Connect the authentication unit to the machine's **USB Port**.

NOTICE
When connecting or disconnecting the USB cable, hold the plug. Otherwise, the machine may be damaged or a failure may occur.

13 Restart this machine.

NOTICE
*When restarting this machine, turn the **Power Switch** off and on again after 10 or more seconds have elapsed. Not doing so may result in an operation failure.*

Associating user information with the card ID

If user information is not associated with the card ID or when the registered card ID is changed, you can associate the user information with the card ID using the **Control Panel**.

1 In the **Control Panel**, tap [Utility] - [Administrator Settings] - [User Authentication/Account Track] - [Card Authentication].

2 Specify a user for whom you want to register the card ID, then tap [OK].

3 Tap [Edit].

➔ Tapping [Delete] to delete the registered card ID.

4 Touch the IC Card / NFC-compatible mobile terminal to or place it on the authentication unit, then tap [OK].

➔ To use an NFC-compatible mobile terminal, display its screen in advance. You do not need to start **Mobile for Android**.

NOTICE
During scanning, do not leave the IC Card / NFC-compatible mobile terminal within 1-9/16 inches (40 mm) from the card reader.

5 Tap [Close].

6.4 Logging in to this machine

The login methods vary depending on the machine's authentication settings.

- For [Card Authentication], you can login by simply touching the IC Card / NFC-compatible mobile terminal to or place it on the authentication unit.
- For [Card Authentication+Password], you can login by touching the IC Card / NFC-compatible mobile terminal to or placing it on the authentication unit and entering the password.

1 Check that [Authentication Device] is selected in [Authentication Method].

2 Touch the IC Card / NFC-compatible mobile terminal to or place it on the authentication unit.

➔ To use an NFC-compatible mobile terminal, display its screen in advance. You do not need to start **Mobile for Android**.

➔ For [Card Authentication+Password], enter the password, and tap [Login].

Authentication starts. If authentication succeeds, you can log in to this machine.

Tips

If authentication fails frequently, the IC Card / NFC-compatible mobile terminal information may not be registered appropriately. Register an IC card / NFC-compatible mobile terminal information again.

7 Index

7 Index

KONICA MINOLTA

http://konicaminolta.com

A6F7-9569-33A

2015. 3