



D330E Series

USER MANUAL/Web Management Tool

- Before using this Product, please read the USER MANUAL carefully and keep it for your reference.





Table of contents

1 Overview of Web Connection

- 1.1 About Web Connection 1-2
- 1.2 Web Connection Specifications 1-3
 - Operating Environment1-3
 - Web Browser Setting1-3
- 1.3 Layout of Web Connection page 1-4

2 Basic Operations of Web Connection

- 2.1 How to access..... 2-2
- 2.2 Login methods..... 2-3
 - About login mode.....2-3
 - Logging in as the administrator2-3
 - The registered user with administrator authority logs in as the administrator.....2-4
 - Logging in as a registered user.....2-5
 - Logging in as a public user2-5
 - Logging in as a administrator user.....2-6
 - Logging in as the User Box administrator2-6
- 2.3 Available Operations in User Mode..... 2-7
- 2.4 Available Operations in Administrator Mode 2-8

3 Configuring Basic Information Settings of this Machine

- 3.1 Registering information of this machine 3-2
- 3.2 Registering support information 3-3
- 3.3 Setting the date and time for the machine 3-4
 - Manually configuring settings3-4
 - Automatically configuring settings using NTP3-4
- 3.4 Configuring the daylight saving time settings..... 3-5

4 Configuring Network Environment Settings

- 4.1 Network Settings 4-2
 - Setting flow4-2
 - Enabling TCP/IP.....4-2
 - Specifying IPv4 address4-2
 - Specifying IPv6 address4-3
 - Registering the DNS server.....4-3
 - Registering the host name4-3
 - Registering the domain name4-4
- 4.2 Displaying on the Windows Network Map..... 4-5
- 4.3 Displaying the network error code on the screen of this machine 4-6

5 Configuring the Scan Transmission Environment

- 5.1 Configuring the Scan to E-mail Environment..... 5-2
 - Setting flow5-2
 - Configuring Basic Settings for Scan to E-mail5-2
 - Using an SSL/TLS communication.....5-4
 - Using SMTP authentication5-4
 - Using the POP before SMTP authentication5-5
 - Using S/MIME5-6
 - Using the Scan to Me function5-8
 - Using the Scan to URL function5-8
- 5.2 Configuring the SMB Send environment 5-9



	Setting flow	5-9
	Configure basic settings for the SMB transmission	5-9
	Using the WINS server	5-10
	Resolving the name using LLMNR.....	5-10
	Using in the DFS environment	5-10
	Using the Scan to Home function.....	5-11
	Constructing a single sign-on environment for the SMB transmission	5-11
	Using the Scan to Authorized Folder function	5-12
	Checking whether there are sub folders when searching for an SMB sharing folder	5-13
5.3	Configuring the operating environment for FTP Send	5-14
	Setting flow	5-14
	Configuring basic settings for the FTP transmission	5-14
	Using a proxy server	5-14
5.4	Configuring the WebDAV transmission environment.....	5-15
	Setting flow	5-15
	Configure basic settings for the WebDAV transmission	5-15
	Using a proxy server	5-15
	Using SSL communication	5-16
5.5	Configuring the WSD scan environment.....	5-17
	Setting flow	5-17
	Configuring basic settings for WSD Scan.....	5-17
	Using a proxy server	5-18
	Using SSL communication	5-18
5.6	Configuring the TWAIN scan environment	5-20
	Setting flow	5-20
	Configuring the basic settings for the TWAIN scan	5-20
	Changing the operation lock time.....	5-20
5.7	Configuring Settings to Search for a Destination via the LDAP Server.....	5-21
	Setting flow	5-21
	Configure basic settings for the LDAP search	5-21
	Using SSL communication	5-22
5.8	Associating with the distributed scan server.....	5-24
	Setting flow	5-24
	Associating with the Distributed Scan Management system	5-24

6 Configuring the Printing Environment

6.1	Configuring the LPR printing environment.....	6-2
	Setting flow	6-2
	Enabling LPD	6-2
6.2	Configuring the Port9100 printing environment.....	6-3
	Setting flow	6-3
	Changing the RAW port number.....	6-3
6.3	Configuring the SMB printing environment.....	6-4
	Setting flow	6-4
	Configure basic settings for the SMB printing.....	6-4
6.4	Configuring the IPP printing environment	6-5
	Setting flow	6-5
	Configuring basic settings for the IPP printing	6-5
	Using the IPP authentication	6-5
	Communicating using SSL (IPPS).....	6-6
6.5	Configuring the WSD printing environment.....	6-7
	Setting flow	6-7
	Configuring basic settings for WSD Print	6-7
6.6	Configuring the Bonjour printing environment	6-8
6.7	Configuring the E-mail RX Print environment.....	6-9
	Setting flow	6-9
	Configure settings to receive E-mails on this machine.....	6-9
	Configure settings to print a received E-mail attachment	6-9
6.8	Specifying the default print settings for this machine.....	6-11

6.8.1	Specifying the default PCL print settings	6-11
6.8.2	Specifying the default PS print settings.....	6-11
6.8.3	Configuring security settings for XPS or OOXML printing.....	6-11
6.9	Specifying the time-out time by interface	6-12
6.10	Restricting the Obtainment of Device Information from the Drive Using the Password.....	6-13
6.11	Printing from the Bypass Tray Using the Paper Settings Configured in the Printer Driver.....	6-14
6.12	Changing the Time to Light up the LED of this Machine after Printing	6-15

7 Configuring the Fax Environment

7.1	Configuring basic fax settings.....	7-2
7.1.1	Configuring the Line Usage Settings	7-2
7.1.2	Configuring connection settings for a PBX environment.....	7-2
7.1.3	Registering the sender information.....	7-3
7.2	Specifying operations when sending and receiving a fax.....	7-4
7.2.1	Specifying How to Print the Sender Name/Reception Information	7-4
7.2.2	Changing Print Settings When Receiving a Fax	7-4
7.2.3	Canceling stamp setting when sending a fax	7-5
7.2.4	Adjusting the image quality depending on the resolution of a received fax	7-5
7.3	Specifying useful transmission and reception functions	7-6
7.3.1	Enabling/Disabling the Fax Functions	7-6
7.3.2	Using the Closed Network RX function	7-7
7.3.3	Using the Fax Retransmit function.....	7-7
7.3.4	Using the Memory RX function	7-7
7.3.5	Using the Forward TX function	7-8
7.3.6	Using the PC-Fax RX Function	7-9
7.3.7	Using the TSI Routing function	7-9
7.3.8	Restricting PC-FAX transmission.....	7-10
7.4	Specifying fax report print conditions.....	7-11
7.5	Restricting Deletions of Received Faxes.....	7-13
7.6	Registering the number to prohibit its entry	7-14

8 Configuring the Network Fax Environment

8.1	Configuring the Internet fax environment.....	8-2
	Setting flow	8-2
	Configure basic settings for sending and receiving an Internet fax.....	8-2
	Checking a fax reception	8-4
	Specifying the reception ability of this machine	8-4
	Specifying the default compression type for transmission in black and white.....	8-5
	Configuring default compression type setting for transmission in color	8-5
8.2	Configuring the IP address fax environment.....	8-6
	Setting flow	8-6
	Configure basic settings for sending and receiving faxes using IP address fax	8-6
8.3	Configuring the IP fax (SIP) operating environment	8-8
	Setting flow	8-8
	Configuring the basic settings for IP fax (SIP) sending and receiving	8-8
	Configuring the setting to connect to the SIP server.....	8-9
	Configuring the setting to automatically acquire SIP configuration information (IPv4)	8-9
	Configuring the setting to automatically acquire SIP configuration information (IPv6)	8-9

9 Configuring the User Box Environment

9.1	Registering and editing a User Box.....	9-2
------------	--	------------

9.1.1	Registering and editing a User Box	9-2
9.1.2	Registering and editing a Bulletin Board User Box.....	9-3
9.1.3	Registering and editing a Relay User Box	9-3
9.1.4	Registering and editing an Annotation User Box.....	9-4
9.2	Managing User Boxes	9-6
9.2.1	Managing User Boxes.....	9-6
	Specifying the maximum number of User Boxes	9-6
	Deleting all empty User Boxes.....	9-6
	Disabling the user to register or edit a User Box	9-6
9.2.2	Managing files in a User Box	9-6
	Automatically deleting files from a User Box	9-6
	Holding files in a User Box.....	9-7
	Automatically deleting files saved in a User Box using the Scan to URL function	9-7
	Deleting all files saved in a User Box using the Scan to URL function.....	9-7
9.2.3	Sharing files in a User Box via SMB	9-7
	Setting flow	9-7
	Configuring the SMB server.....	9-8
	Creating a Public User Box to share files	9-8
	Automatically deleting files from the SMB folder.....	9-9
	Deleting all files from the SMB folder	9-9
9.2.4	Managing files in a Secure Print User Box	9-9
	Deleting all secure documents.....	9-9
	Automatically deleting all secure documents	9-10
	Specifying the simple print function for secure document	9-10
9.2.5	Managing files in a ID & Print User Box	9-10
	Automatically deleting all ID & Print documents	9-10
	Specifying processing after printing ID & Print documents	9-10
9.2.6	Managing files in a Password Encrypted PDF User Box.....	9-11
	Automatically deleting a Password Encrypted PDF file.....	9-11
9.2.7	Backing up files in a User Box	9-11
9.3	Configuring the USB Memory Device settings.....	9-12

10 Restricting Users from Using this Device

10.1	Overview of User Authentication and Account Track	10-2
	About user authentication.....	10-2
	About account track	10-3
	Combining user authentication and account track.....	10-3
10.2	Installing User Authentication/Account Track	10-5
10.2.1	MFP authentication setting	10-5
	Setting flow	10-5
	Configure basic settings for the user authentication	10-5
10.2.2	Account track setting	10-6
	Setting flow	10-6
	Configure basic account track settings	10-6
10.2.3	Active Directory authentication setting	10-8
	Setting flow	10-8
	Configuring basic settings for the Active Directory authentication.....	10-8
	Using the single sign-on	10-10
	Reinforcing authentication processing when using Active Directory.....	10-10
10.2.4	NTLM authentication setting.....	10-12
	Setting flow	10-12
	Configure basic settings for the NTLM authentication	10-12
10.2.5	LDAP authentication setting	10-13
	Setting flow	10-13
	Configure basic settings for the LDAP authentication	10-14
	Using SSL communication	10-17
10.2.6	Configuring a setting so that a user can log in to this machine using administrator privileges.....	10-17
10.2.7	Extending the number of users to be authenticated.....	10-17



10.2.8	Using the MFP authentication together against in the case where an enhanced server has shut down	10-18
10.3	Managing a Use of this Machine by User or Account	10-20
10.3.1	Restricting available functions	10-20
	Restricting available functions for each user	10-20
	Restricting available functions by account track	10-21
	Configuring the default settings of the functions available for users of external server authentication	10-21
10.3.2	Limiting the accessible destinations	10-22
	Methods to limit access to destinations	10-22
	Setting the reference allowed level	10-22
	Assigning a reference allowed group	10-23
	Simultaneously setting a reference allowed level and reference allowed group	10-23
10.3.3	Managing the maximum number of printable pages	10-25
	Managing the maximum number of printable pages by user	10-25
	Managing the maximum number of printable pages by account	10-25
10.3.4	Managing a use by a public user	10-25
10.3.5	Changing the function key to be displayed on the classic style screen	10-26
	Setting flow	10-26
	Allowing changing the function key display pattern by user or account	10-26
	Selecting a function key display pattern by user	10-27
	Selecting a function key display pattern by account	10-27
10.3.6	Configuring common settings for user authentication and account track	10-28
10.4	Configuring Print Operations in User Authentication Environment	10-29
10.4.1	Specifying the operations of the ID & Print function	10-29
10.4.2	Restricting print jobs without authentication information	10-29
10.4.3	Printing with authentication by user name only (quick authentication)	10-30
	Setting flow	10-30
	Permitting quick authentication	10-30
	Registering the quick authentication server	10-30
	Using SSL communication	10-32
10.5	Installing IC Card Authentication or Biometric Authentication	10-33
10.5.1	Setting biometric authentication operations	10-33
10.5.2	Authenticating in the LDAP server using the authentication card (LDAP-IC Card Authentication)	10-33
	Setting flow	10-33
	Configuring basic settings for the LDAP-IC card authentication	10-33
	Using SSL communication	10-36

11 Reinforcing Security

11.1	Changing Security Settings	11-2
11.1.1	Enhancing the security by simple operation	11-2
11.1.2	Changing the administrator password	11-3
11.2	Encrypting Communications	11-4
11.2.1	Using an SSL/TLS communication	11-4
	About the certificate of this machine	11-4
	Using the certificate registered upon shipment	11-4
	Self-creating a certificate	11-4
	Requesting the Certificate Authority for issuing a certificate	11-5
11.2.2	Using IPsec communication	11-6
11.3	Restricting Communications	11-9
11.3.1	Restricting external accesses using the IP address	11-9
	Automatically specifying the IP Address to restrict accesses	11-9
	Automatically Auto the IP Address to restrict accesses	11-9
11.3.2	Restricting Packet Transfer	11-11
	Registering filter	11-11
	Exporting filter	11-12
	Importing filter	11-12
	Recording logs	11-12

	Downloading logs	11-12
11.3.3	Restricting E-mail recipients using the domain	11-13
11.4	Restricting network or USB connections	11-14
11.4.1	Connecting this machine to IEEE802.1X authentication environment.....	11-14
11.4.2	Restricting functions using the USB port	11-15
11.4.3	Restricting the firmware update using a USB memory with a password	11-16
11.5	Managing the certificates for this machine	11-17
11.5.1	Using Different Certificates Depending on the Application	11-17
11.5.2	Exporting a certificate	11-18
	Exporting information to your computer.....	11-18
	Exporting information to an SMB sharing folder.....	11-18
11.5.3	Importing a certificate	11-19
	Importing information from your computer.....	11-19
	Importing information from an SMB sharing folder	11-19
11.5.4	Deleting a certificate	11-19
11.5.5	Verifying a certificate for peer	11-20
11.5.6	Importing external certificates used for validating the chain	11-20
	Types of external certificates that can be imported	11-20
	How to import	11-21
11.6	Monitoring or Restricting User Operations	11-22
11.6.1	Disabling user's registration/change operations	11-22
11.6.2	Restricting user's Web browser setting operations.....	11-23
11.6.3	Saving the operation log of the control panel.....	11-23

12 Managing the Machine Status

12.1	Managing the machine power for power saving.....	12-2
12.1.1	Setting the Power key/Power save function.....	12-2
12.1.2	Switching to Power Save mode at specified time (Weekly Timer).....	12-3
12.1.3	Recovering this machine from ErP Auto Power Off mode.....	12-4
12.2	Customizing the Control Panel environment	12-5
12.2.1	Changing the default operation screen.....	12-5
12.2.2	Changing the order to sort the communication list on the Job History screen	12-5
12.2.3	Changing the functions to be assigned to the classic-style side menu	12-5
12.2.4	Selecting functions to be displayed in the main menu of classic style.....	12-6
12.2.5	Changing the theme of the classic-style main menu.....	12-6
12.2.6	Selecting function keys to be displayed in each classic-style mode (using a display pattern)	12-7
12.2.7	Selecting function keys to be displayed in each classic-style mode (Individual specification).....	12-7
	Setting flow	12-7
	Allowing the change of functions keys in each mode.....	12-7
	Changing function keys in copy mode	12-8
	Changing function keys in scan/fax mode.....	12-8
	Changing function keys in fax mode	12-8
12.2.8	Allowing the user to change the language to be displayed on the screen of this machine.....	12-8
12.2.9	Changing the Keypad display when entering number of sets	12-9
12.2.10	Arranging widgets on the classic-style screen	12-9
12.2.11	Displaying the default registration menu on the screen of basic style	12-9
12.3	Monitoring and Checking the Status of this Machine	12-10
12.3.1	Checking the ROM version	12-10
12.3.2	Checking the counter of this machine	12-10
12.3.3	Notifying counter information by E-mail	12-10
	Setting flow	12-10
	Configuring the counter notification settings.....	12-10
12.3.4	Notifying a warning occurrence or consumables replacement period by E-mail.....	12-11
	Setting flow	12-11

	Configuring the machine status notification settings.....	12-11
12.3.5	Managing the machine via SNMP.....	12-11
	Setting flow	12-11
	Configuring the settings for using SNMP	12-11
12.3.6	Outputting job logs	12-13
	Specifying the job log acquirement method.....	12-13
	Downloading job logs	12-14
12.4	Managing the setting information	12-15
12.4.1	Importing configuration information.....	12-15
	Types of information that can be imported.....	12-15
	Importing information from your computer.....	12-15
	Importing information from an SMB sharing folder	12-16
	Importing information from a USB flash drive	12-16
12.4.2	Exporting configuration information.....	12-17
	Types of information that can be exported.....	12-17
	Exporting information to your computer.....	12-18
	Exporting information to an SMB sharing folder.....	12-18
	Exporting information to a USB flash drive.....	12-19
12.4.3	Importing configuration information of other device.....	12-20
12.4.4	Backing up configuration information.....	12-20
	Backing up data to the server.....	12-20
12.4.5	Initializing configuration information	12-21
	Resetting the network settings	12-21
	Deleting all address information	12-21
	Restarting the network interface.....	12-21
12.4.6	Checking whether settings are updated	12-21
12.5	Setting the operating environment for this machine	12-22
12.5.1	Original/paper setting	12-22
	Configuring the setting to scan the original from the ADF.....	12-22
	Setting the manual staple operation	12-22
12.5.2	Configuring the scan settings	12-22
	Configuring the preview function display settings.....	12-22
	Printing a stamp on blank pages	12-23
	Configuring the default Compact PDF conversion setting	12-23
	Setting the processing accuracy of Outline PDF.....	12-23
	Configuring the default searchable PDF conversion setting	12-23
	Specifying the default for [PDF Web Optimization]	12-24
	Specifying the default for [PDF/A].....	12-24
	Changing the default scan data file name	12-24
12.5.3	Enlarge display settings.....	12-25
	Changing default settings for Normal Display and Enlarge Display collectively	12-25
	Setting the action for switching the display to Enlarge Display.....	12-25
12.5.4	Support settings.....	12-25
	Allowing transmission of the machine usage frequency or function settings information	12-25
12.5.5	Setting the skip job conditions	12-26
12.5.6	Enabling functions that require the authentication by an external institution.....	12-26
12.6	Updating firmware or settings of this machine.....	12-27
12.6.1	Acquiring firmware via Internet to update this machine	12-27
	Setting flow	12-27
	Preparing to download firmware via FTP.....	12-27
	Preparing to download firmware via HTTP	12-27
	Updating the firmware automatically at the specified time	12-28
	Updating the firmware manually.....	12-28
12.6.2	Acquiring the update file from the distribution server to update this machine and other devices	12-28
	Acquiring the update file to update this machine	12-28
	Acquiring the update file on this machine to distribute it to other devices	12-30
12.6.3	Connecting the USB flash drive with firmware stored to update this machine	12-31
12.6.4	Returning the updated firmware to the previous version.....	12-31



13 Registering Various Types of Information

13.1	Registering address books	13-2
13.1.1	Registering E-mail Address	13-2
13.1.2	Registering an FTP Destination	13-2
13.1.3	Registering an SMB Destination	13-3
13.1.4	Registering a WebDAV Destination	13-4
13.1.5	Registering a User Box	13-5
13.1.6	Registering a Fax Address	13-5
13.1.7	Registering an Internet Fax Address.....	13-6
13.1.8	Registering an IP Address Fax Destination	13-7
13.1.9	Registering an IP Fax (SIP) Destination	13-8
13.2	Registering a Group	13-9
13.3	Registering a program	13-10
13.3.1	Registering an E-mail address program	13-10
13.3.2	Registering an FTP program	13-10
13.3.3	Registering an SMB program	13-11
13.3.4	Registering a WebDAV program	13-11
13.3.5	Registering a User Box program	13-12
13.3.6	Registering a fax address program.....	13-13
13.3.7	Registering an Internet fax address program	13-13
13.3.8	Registering an IP address fax program	13-14
13.3.9	Registering a group program	13-14
13.3.10	Registering a program without destination.....	13-15
13.3.11	Configuring the scan/fax transmission option settings.....	13-15
13.4	Registering a temporary one-touch destination	13-18
13.5	Registering the subject and body of an E-mail	13-19
	Registering the subject	13-19
	Registering the body.....	13-19
13.6	Registering a prefix and suffix of each destination	13-20
13.7	Registering the information to be added to header/footer	13-21
13.8	Adding a font/macro	13-22
13.9	Registering a paper name and paper type	13-23
13.10	Using data management utility	13-24
13.10.1	Data Management Utility	13-24
13.10.2	Managing the copy protect data.....	13-24
13.10.3	Managing the stamp data	13-26
13.10.4	Managing the font/macro data	13-27

14 Associating with External Application

14.1	Using the Web Browser Function	14-2
	Enabling the Web browser function.....	14-2
	Restricting file operations on a Web browser.....	14-2
	Specifying the operation to be performed when an SSL certificate verification error occurs	14-2
	Configuring settings to display contents	14-3
	Managing bookmarks	14-3
	Managing the history	14-3
	Setting Web browser operations	14-4
14.2	Using TCP Socket	14-5
	Setting flow	14-5
	Configuring the basic TCP Socket settings	14-5
	Using SSL communication	14-5
14.3	Using OpenAPI	14-6
	Setting flow	14-6
	Configure the basic OpenAPI settings.....	14-6
	Using a proxy server	14-7
	Using SSL communication	14-7



14.4	Using the FTP Server Function	14-8
	Setting flow	14-8
	Configuring the FTP server settings	14-8
14.5	Using the WebDAV Server Function.....	14-9
	Setting flow	14-9
	Configuring the WebDAV server settings	14-9
	Using SSL communication	14-9
14.6	Using IWS.....	14-10
	Setting flow	14-10
	Configuring the basic IWS settings.....	14-10
	Configuring the setting to use MarketPlace.....	14-10
	Configuring the execution environment of the IWS application to operate preferentially.....	14-11
14.7	Associating with the remote diagnosis system	14-12
14.7.1	Registering a proxy server used for remote diagnosis	14-12
14.7.2	Allowing acquisition of the machine counter	14-12
14.7.3	Sending the machine operating status	14-12
14.7.4	Allowing read and write of the machine setting information.....	14-13
14.8	Associating with the fax server	14-14
	About association with the fax server.....	14-14
	Registering applications.....	14-14
	Application setting templates	14-15
	Associating with the fax server communicating in E-Mail format.....	14-17
14.9	Remote-controlling the Screen of this Machine	14-18
	About operation method	14-18
	Using the dedicated software	14-18
	Accessing the machine directly	14-19
14.10	Releasing the association with application	14-20





Overview of Web Connection

1 Overview of Web Connection

1.1 About Web Connection

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

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

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

Related setting (for the administrator)

- [HTTP Server Setting] - [Web Connection Setting] ("User's Guide[Descriptions of Functions/Utility Keys]/[Administrator]")
- [HTTP Server Setting] - [Web Conn. HTTP Version Set.] ("User's Guide[Descriptions of Functions/Utility Keys]/[Administrator]")

1.2 Web Connection Specifications

Operating Environment

Item	Specifications
Network	Ethernet (TCP/IP)
Web browser	Microsoft Internet Explorer 10/11 Microsoft Edge Mozilla Firefox latest version Google Chrome latest version Safari latest version (Mac OS/iOS) Microsoft Edge Chromium <ul style="list-style-type: none"> • JavaScript and Cookies must be enabled by your Web browser. • Also, you need to enable the MSXML3.0 (Free Threaded XML DOM Document and XSL Template) add-on.

Tips

- When an attempt is made to connect this machine to **Web Connection** using Safari for iOS via a proxy server, it may cause a connection failure. In this case, change the HTTP setting of the proxy server to HTTP1.1, then retry a connection.

Web Browser Setting

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

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

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

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

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

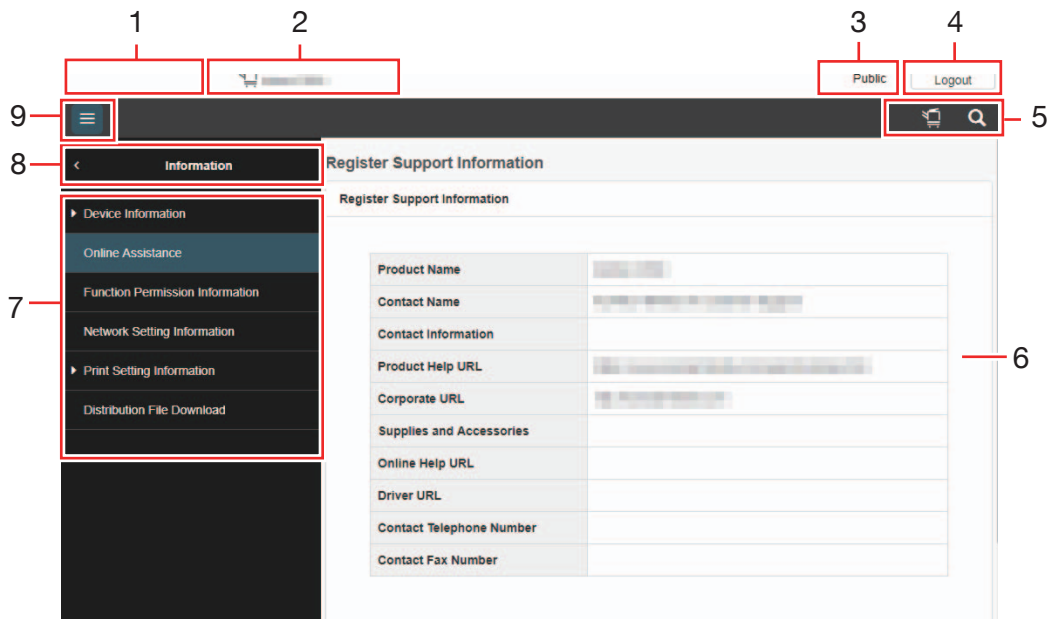
Tips

If the **Web Connection** page is not correctly displayed even though the above settings have been configured, the Web browser cache may be the cause of the problem. If that is the case, clear the Web browser cache. For details on how to confirm and change settings, refer to the Help of your Web browser.

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

1.3 Layout of Web Connection page

This section describes each part on the **Web Connection** page.



No.	Item	Description
1	Web Connection logo	Click this logo to display the version information of Web Connection .
2	Status display	Displays the status of the printer and scanner sections of this machine as well as the network connection status. If an error occurs, you can view detailed information on the error.
3	Login user name	Displays the login mode and user name. Click the user name when you log on as a registered user to confirm the user information.
4	[Logout]	Logs out from the login mode.
5	Device search icon	Displays the menu to access Web Connection of another device on the network. <ul style="list-style-type: none"> [Search surrounding MFPs]: Searches for another device. You can select a device from the search result list to access Web Connection. [Register MFP Information]: Manually register another device. [Displays MFP Information]: Displays a list of registered devices. You can select a device from the list to access Web Connection.
	Function search icon	Searches for setting items to go to the target function screen from the search result.
	Favorite icon	Enables you to register frequently-accessed pages in the Favorite Setting. Only available in administrator mode.
6	Information and settings	Click the menu at the left of the screen, and the contents of that menu will appear.
7	Menu item	Displays information and settings in the selected higher-level menu.
8	Move to higher-level menu	Move to a higher-level menu when a menu has a hierarchical structure.
9	Menu show/hide switching icon	Switches whether to show or hide the icon.



Basic Operations of Web Connection

2 Basic Operations of Web Connection

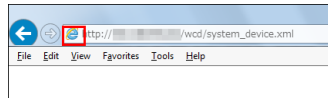
2.1 How to access

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] key.
 - For details on how to confirm the IP address of this machine, refer to "User's Guide[Introduction]/[Connecting to the Network]".The **Web Connection** screen appears.

Tips

- This machine does not support the method to simultaneously access **Web Connection** of this machine from multiple tabs of the same Web browser.
- When the DNS server is installed, you can specify the host name of this machine instead of the IP address of this machine in order to make access. For details, contact the administrator of this machine.
- In the IPv6 environment, enclose the IPv6 address in brackets [].
For example, when the IPv6 address of this machine is "fe80::220:6bff:fe10:2f16", type "http://[fe80::220:6bff:fe10:2f16]/".
- You can create a shortcut to each **Web Connection** function page at any location such as the desktop of your computer. To create a shortcut, drag and drop the icon displayed in the address bar of the Web browser to any location on your computer.



2.2 Login methods

About login mode

Two login modes of **Web Connection** are provided: the "administrator mode" and the "user mode".

Login mode	Description
Administrator mode	Available for the administrator of this machine. To log in, you need to enter the administrator password. In this mode, you can perform settings and operations for administrators.
User mode	Available for users of this machine. The following types of users exist. The login method and operations available after logging in differ depending on the login user type.
Registered user	Log in as the registered user when user authentication is enabled. In this mode, you can perform settings and operations for registered users.
Administrator user	The administrator of this machine logs in as a user with administrator authority. To log in, you need to enter the administrator password. In this mode, you can delete all user jobs.
User Box administrator	Available when the User Box administrator is specified. To log in, you need to enter the User Box administrator password of this machine. In this mode, you can use the User Box registered on this machine regardless of the setting of User Box password.
Public user	Log in as a general user, which is not registered in this machine, when user authentication is enabled. This is available when Public User is enabled. In this mode, you can perform settings and operations for public users.

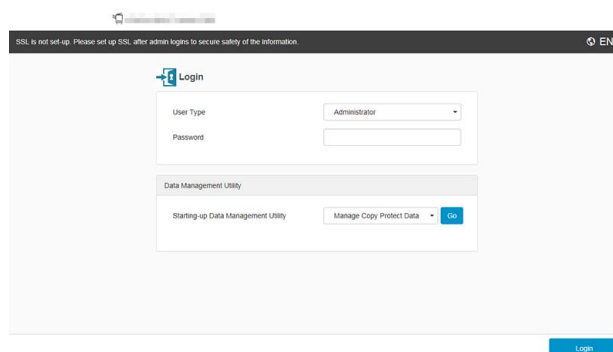


Tips

- The user who has administrator authority can log in to this machine as the administrator. For details, refer to page 2-4.

Logging in as the administrator

- 1 Select [Administrator] in [User Type].



- 2 Enter the administrator password for this machine.
- 3 Click [Login].
The administrator mode window appears.
- 4 After a target operation is completed, click [Logout].
- 5 Click [OK] in the logout confirmation window.

Tips

- You can log in to the administrator mode to change settings of this machine even when a job is running or an error or paper jam is occurring on this machine. However, setting change that affects an active job will not be immediately reflected. To check whether settings have been reflected, select [Maintenance] - [Confirm update settings for Held Jobs.] in the administrator mode.
- Depending on the status of this machine, you may not be able to log in to the administrator mode.

The registered user with administrator authority logs in as the administrator

- ✓ A pre-setting is required to allow the registered user to log in with administrator privileges. For details, refer to page 10-17.

- 1 Select [Registered User] in [User Type].

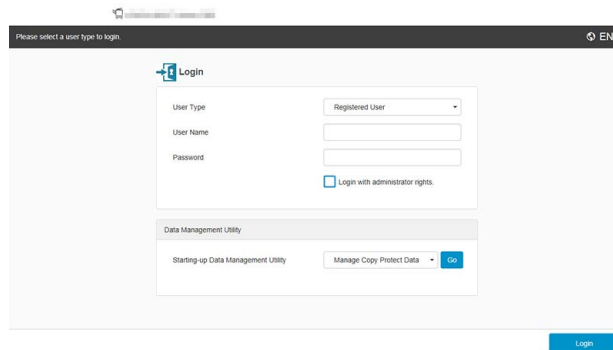
- 2 Enter the user name and password.
- 3 Set [Login with administrator rights.] to ON.
- 4 Click [Login].
The administrator mode window appears.
- 5 After a target operation is completed, click [Logout].
- 6 Click [OK] in the logout confirmation window.

Tips

- You can log in to the administrator mode to change settings of this machine even when a job is running or an error or paper jam is occurring on this machine. However, setting change that affects an active job will not be immediately reflected. To check whether settings have been reflected, select [Maintenance] - [Confirm update settings for Held Jobs.] in the administrator mode.
- Depending on the status of this machine, you may not be able to log in to the administrator mode.

Logging in as a registered user

- 1 Select [Registered User] in [User Type].
→ When the administrator of this machine wants to log in to the user mode, select [Administrator (User Mode)] in [User Type].



The screenshot shows a web browser window with the title "Please select a user type to login". The main content area is titled "Login" and contains a form with the following fields and options:

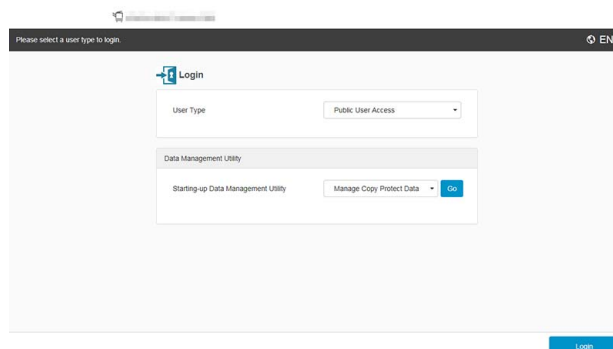
- User Type:** A dropdown menu currently set to "Registered User".
- User Name:** An empty text input field.
- Password:** An empty password input field.
- Login with administrator rights.

Below the login form is a section titled "Data Management Utility" with a sub-section "Starting-up Data Management Utility" containing a "Manage Copy Protect Data" button with a "Go" sub-button. A "Login" button is located at the bottom right of the page.

- 2 Enter the user name and password.
→ If you select [Administrator (User Mode)] in step 1, enter the administrator password.
- 3 When [Server Name] is displayed, select the server to perform authentication.
- 4 Click [Login].
The page in user mode is displayed.
- 5 After a target operation is completed, click [Logout].
- 6 Click [OK] in the logout confirmation window.

Logging in as a public user

- 1 Select [Public User] in [User Type].

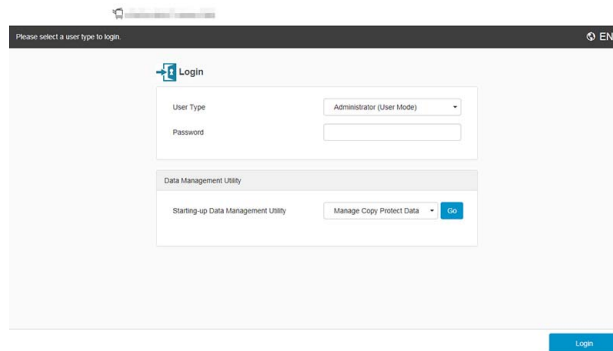


The screenshot shows the same "Login" page as above, but with the "User Type" dropdown menu set to "Public User Access". All other elements, including the "Data Management Utility" section and the "Login" button, remain the same.

- 2 Click [Login].
The page in user mode is displayed.
- 3 After a target operation is completed, click [Logout].
- 4 Click [OK] in the logout confirmation window.

Logging in as a administrator user

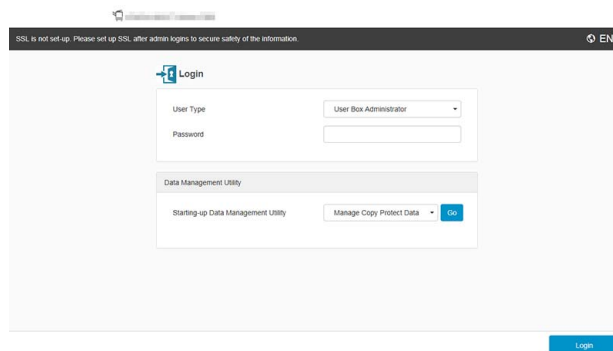
- 1 Select [Administrator (User Mode)] in [User Type].



- 2 Enter the administrator password for this machine.
- 3 Click [Login].
The page in user mode is displayed.
- 4 After a target operation is completed, click [Logout].
- 5 Click [OK] in the logout confirmation window.

Logging in as the User Box administrator

- 1 Select [User Box Administrator] in [User Type].



- 2 Enter the password of the User Box administrator.
- 3 Click [Login].
The page in user mode is displayed.
- 4 After a target operation is completed, click [Logout].
- 5 Click [OK] in the logout confirmation window.

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

2.3 Available Operations in User Mode

The user can confirm the status of this machine, use the files in the User Box, perform Direct Print, register an address, and other functions of this machine. Also, you can change the defaults or screen displays of the copy, scan/fax, or print function in a user-friendly manner to suit your environment.

Menu	Description
[Information]	Enables you to check the device status, device configuration, consumable information, meter counts, eco information, and authorization function list view.
[Job]	Enables you to check the job currently being performed and the job log.
[System Settings]	Configure the operating environment of this machine.
[Box]	Enables you to create a User Box on this machine, print a file from the User Box, and send a file.
[Copier Settings]	Configure settings for copy operations.
[Printer Settings]	Configure settings for printer operations.
[Store Address]	Enables you to register frequently-used destinations and edit the registration content.
[Scan/Fax Settings]	Configure settings for fax and scan operations.
[Fax Settings]	Configure settings for fax operations.
[Direct Print]	Allows you to directly send a file on your computer or in an SMB sharing folder to this machine and print it.
[Customize]	Allows you to customize the screen of the classic style.

2.4 Available Operations in Administrator Mode

You can specify the initial operations of the copy, print, fax, or User Box function, power saving function, and network function to suit your environment. Also, you can manage the usage status of this machine or prevent information leakage by specifying the authentication or security function.

Menu	Description
[Maintenance]	Set the status of this machine, for example, the counter information notification setting.
[System Settings]	Configure the operating environment of this machine such as the functional operations and screen display.
[Security]	Configure the security function of this machine such as password setting or data management method.
[User Auth/Account Track]	Configure user authentication and account track. This function allows you to restrict users who can use this machine or manage the usage status of this machine. Specify the authentication method, or register user information or account track information.
[Network]	Configure the network function such as setting up TCP/IP and configuring your environment for Scan TX.
[Box]	Allows you to register or delete all User Boxes.
[Printer Settings]	Specify the time-out time to limit a communication between this machine and a computer, or configure settings of a communication with the printer driver.
[Store Address]	Enables you to register frequently-used destinations and edit the registration content.
[Fax Settings]	Configure the operating environment of the fax or network fax function.
[Copier Settings]	Configure settings for copy operations.



Configuring Basic Information Settings of this Machine

3 Configuring Basic Information Settings of this Machine

3.1 Registering information of this machine

Register device information of this machine such as the name, installation location, and information about the administrator.

Select [System Settings] - [Machine Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Device Location]	Enter the location where to install this machine (using up to 255 characters).
[Administrator Registration]	<p>Register the name, E-mail address and extension number of the administrator of this machine.</p> <ul style="list-style-type: none"> • [Administrator Name]: Enter the administrator name of this machine (using up to 20 characters). • [E-mail Address]: Enter the E-mail address of the administrator of this machine (using up to 128 characters, excluding spaces). To use the E-mail TX function, it settings are required. • [Extension No.]: Enter the extension number of the administrator of this machine (using up to eight digits). • [Company Name]: Enter the company name (using up to 80 characters). • [Department Name]: Enter the department name (using up to 80 characters).
[Input Machine Address]	<p>Register the device name and E-mail address of this machine.</p> <ul style="list-style-type: none"> • [Device Name]: Enter the name of this machine (using up to 80 characters). The file name automatically assigned in scanning and sending incorporates the name specified for [Device Name]. • [E-mail Address]: Enter the E-mail address of this machine (using up to 320 characters, excluding spaces). To use the Internet fax function or E-mail RX print function, it settings are required.

Tips

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

3.2 Registering support information

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

Select [System Settings] - [Register Support Information] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Contact Name]	Enter the contact name of this machine (using up to 63 characters).
[Contact Information]	Enter the contact information of this machine such as the phone number or URL (using up to 127 characters).
[Product Help URL]	Enter the Product Help URL of this machine (using up to 127 characters).
[Corporate URL]	Enter the URL of the Web page for the manufacturer of this machine (using up to 127 characters).
[Supplies and Accessories]	Enter consumables supplier information (using up to 127 characters).
[Online Help URL]	Enter the Web Connection online help URL (using up to 127 characters).
[Driver URL]	Enter the URL of the place where the driver of this machine is stored (using up to 127 characters). Enter an appropriate URL to suit your environment.
[Engine Serial Number]	Enables you to confirm the serial number of this machine.

Tips

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

3.3 Setting the date and time for the machine

Manually configuring settings

Specify the current date and time and time zone of this machine.

Select [Maintenance] - [Date/Time Setting] - [Manual Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Date]	Specify the current date of this machine. <ul style="list-style-type: none"> • [Year]: Enter the year. • [Month]: Enter the month. • [Day]: Enter the day.
[Time]	Specify the current time of this machine. <ul style="list-style-type: none"> • [Hour]: Enter the hour. • [Minute]: Enter the minute.
[Time Zone]	Select the time zone (time difference from the world standard time) to suit your environment.

Automatically configuring settings using NTP

Configure settings to automatically adjust the date and time of this machine using the NTP (Network Time Protocol) server.

✓ This machine must be connected to the network.

1 Select [Maintenance] - [Date/Time Setting] - [Manual Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and specify [Time Zone].

→ For details on how to specify [Time Zone] setting, refer to page 3-4.

2 Select [Maintenance] - [Date/Time Setting] - [Time Adjustment Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Time Adjustment Setting]	When connecting to the NTP server to adjust the date and time of this machine, set this option to ON (default: OFF).
[Auto IPv6 Retrieval]	When automatically specifying the NTP server address using DHCPv6, set this option to ON (default: ON).
[NTP Server Address]	Enter the NTP server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the NTP server port number (default: [123]).
[Auto Time Adjustment]	When connecting to the NTP server to automatically adjust the date and time of this machine, set this option to ON (default: OFF). <ul style="list-style-type: none"> • [Polling Interval]: Specify an interval to automatically adjust the date and time (default: [24] hours).

3 Click [Adjust].

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

3.4 Configuring the daylight saving time settings

Configure settings to apply the daylight savings time to this machine.

Select [Maintenance] - [Daylight Saving Time] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Daylight Saving Time]	When applying daylight savings time to this machine, set this option to ON (default: OFF). Also, enter the time to move the clocks forward for daylight saving time. The current time is moved forward to reflect daylight saving time.
[Specify Method]	Select the method to specify the date and time to start daylight saving time and the date and time to end it. <ul style="list-style-type: none">• [Weekly]: Specify the start date or end date using the week or a day of the week.• [Day]: Specify the start date and the end date using the date.
[Start Date/Time]/[End Date/Time]	Respectively select the date and time to start daylight saving time and the date and time to end it.



Configuring Network Environment Settings

4 Configuring Network Environment Settings

4.1 Network Settings

Setting flow

- 1 Checking that TCP/IP is enabled (page 4-2)
- 2 Setting the IP address to this machine
 - Specifying the IPv4 address (page 4-2)
 - Specifying the IPv6 address (page 4-3)
- 3 Configuring settings to suit your environment
 - Registering the DNS server (page 4-3)
 - Registering the host name (page 4-3)
 - Registering the domain name (page 4-4)

Enabling TCP/IP

Check that TCP/IP is enabled.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TCP/IP]	When enabling TCP/IP, set this option to ON (default: ON).
[Network Speed]	Select the network speed according to your environment (default: [Auto (10M/100M/1Gbps)]).

Specifying IPv4 address

When connecting this machine to the IPv4 environment, specify the IPv4 address. The IP address is compatible with IPv4 and IPv6, which can be used simultaneously.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [IPv4] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IP Address Setting Method]	Select the method to specify the IP address to this machine according to your environment (default: [Auto Setting]). To manually specify the IP address, select [Manual Setting]. To automatically specify the IP address using DHCP, select [Auto Setting], and specify the automatic setting method.
[IP Address]	Enter the fixed IP address assigned to the machine when manually specifying the IP address.
[Subnet Mask]	Enter the subnet mask when manually specifying it.
[Default Gateway]	Enter the default gateway when manually specifying it.

Specifying IPv6 address

When connecting this machine to the IPv6 environment, specify the IPv6 address. The IP address is compatible with IPv4 and IPv6, which can be used simultaneously.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [IPv6] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IPv6]	When using IPv6, set this option to ON (default: ON).
[Auto IPv6 Setting]	When automatically specifying the IPv6 global address, set this option to ON (default: ON). The IPv6 global address is automatically set based on the prefix length notified from the router and the MAC address of this machine.
[DHCPv6 Setting]	When automatically specifying the IPv6 global address using DHCPv6, set this option to ON (default: ON).
[Link-Local Address]	Displays the link-local address. The link-local address is automatically specified from the MAC address of this machine.
[Global Address]	Enter the IPv6 global address when manually specifying it.
[Prefix Length]	Enter the prefix length of the IPv6 global address between 1 and 128 when manually specifying it.
[Gateway Address]	Enter the gateway address when manually specifying it.

Registering the DNS server

When DNS is installed in your environment, register the DNS server.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [DNS Server Setting(IPv4)] or [DNS Server Setting(IPv6)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[DNS Server Auto Obtain]	When automatically specifying the DNS server address using DHCP, set this option to ON (default: ON).
[Primary DNS Server]	Enter the primary DNS server address when manually specifying it.
[Secondary DNS Server1] or [Secondary DNS Server2]	Enter the secondary DNS server address when manually specifying it.

Registering the host name

When using the host name to connect to this machine, register the host name of this machine.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [DNS Host] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[DNS Host Name]	Enter the host name of this machine (using up to 63 characters, 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.
[Dynamic DNS Setting]	When using the Dynamic DNS function, set this option to ON (default: OFF). If your DNS server supports the Dynamic DNS function, the set host name can be automatically registered to the DNS server or changes can be automatically updated.
[LLMNR Setting]	When using LLMNR, set this option to ON (default: ON). Using LLMNR enables you to resolve the name even in an environment that does not have a DNS server. This option is only compatible with Windows computers. It is useful to resolve the name in the IPv6 environment.

Registering the domain name

Register the name of a domain this machine joins.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [DNS Domain Name Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[DNS Domain Auto Obtain]	When automatically specifying the domain name using DHCP, set this option to ON (default: ON).
[DNS Search Domain Name Auto Retrieval]	When automatically specifying the search domain name using DHCP, set this option to ON (default: ON).
[DNS Default Domain Name]	When manually specifying the domain name, enter the default domain name of this machine (using up to 253 bytes, including the host name, - and . for symbol marks).
[DNS Search Domain Name1] to [DNS Search Domain Name3]	When manually specifying, enter the search domain name (using up to 63 characters, including only - and . for symbol marks).

4.2 Displaying on the Windows Network Map

Using LLTD (Link Layer Topology Discovery) allows you to display this machine on the network map of a Windows computer.

Select [Network] - [LLTD Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LLTD Setting]	When enabling LLTD, set this option to ON (default: ON).

4.3 Displaying the network error code on the screen of this machine

When an error occurs on the network, the network error code can be viewed on the screen of this machine. You can check the action to take as well as a description of the error by referring to the code in the error code list.

Select [Maintenance] - [Network Error Code Display Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Error Code Display]	When displaying the error code, set this option to ON (default: ON).



Reference

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



Configuring the Scan Transmission Environment

5 Configuring the Scan Transmission Environment

5.1 Configuring the Scan to E-mail Environment

Setting flow

The Scan to E-mail is a function that sends 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 the LDAP server or Active Directory is used for user management, you can search for or specify an E-mail address from the server.

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for Scan to E-mail (page 5-2)
- 3 Configuring settings to suit your environment
 - Establishing SSL/TLS communication (page 5-4)
 - Using SMTP authentication (page 5-4)
 - Using POP before SMTP authentication (page 5-5)
 - Using S/MIME (page 5-6)
 - Using the Scan to Me function (page 5-8)
 - Using the Scan to URL function (page 5-8)

Configuring Basic Settings for Scan to E-mail

Configure the settings to send an E-mail from this machine.

- 1 Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail TX Setting]	When sending E-mails from this machine, set this option to ON (default: ON).
[E-Mail Send]	When using the Scan to E-mail function, set this option to ON (default: ON). Using this function allows you to send the scanned original data as an E-mail attachment.
[E-mail Notification]	When using the E-mail notification function, set this option to ON (default: ON). If a warning occurs on this machine that instructs the user to add paper, replace toner, or resolve a paper jam, it can be sent to a registered E-mail address. For details on the E-mail Notification function, refer to page 12-11.
[Total Counter Notification]	When using the total counter notification function, set this option to ON (default: ON). Using this function allows you to send counter information managed by this machine to the registered E-mail address. For details on the Total Counter Notification function, refer to page 12-10.
[SMTP Server Address]	Enter the address of the E-mail server (SMTP). Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the port number of the E-mail server (SMTP) (default: [25]).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (SMTP) (default: [60] sec.).

Setting	Description
[Server load reduction transmission method]	<p>Select the sending method to reduce the load of the E-mail server (SMTP) (default: [OFF]).</p> <ul style="list-style-type: none"> • [Binary Division]: Divides an E-mail with the specified size. [Binary division Size]: Enter the size to divide an E-mail. • [Stop Scan TX when maximum limit is exceeded]: Stops sending an E-mail when its size exceeds the specified maximum value. When specifying the maximum value, select [Limit] in [Max Mail Size], then enter the maximum E-mail size allowable for the E-mail server (SMTP) in [Server Capacity limit]. • [Scan TX by Download URL method only when maximum limit is exceeded]: Notifies the E-mail address specified as the destination of the download URL without attaching files when the E-mail size exceeds the specified maximum value. When specifying the maximum value, select [Limit] in [Max Mail Size], then enter the maximum E-mail size allowable for the E-mail server (SMTP) in [Server Capacity limit]. • [Always Scan TX by Download URL method]: Notifies the E-mail address specified as the destination of the download URL without attaching files.

- 2** Select [System Settings] - [Machine Setting] - [Administrator Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and enter the E-mail address of the administrator of this machine into [E-mail Address] (using up to 128 characters, excluding spaces).

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

Tips

- You can change the sender address on the screen of this machine before sending E-mail.
- If user authentication is installed on this machine, the E-mail address of the login user is used as the sender's E-mail address.

Using an SSL/TLS communication

When SSL/TLS is installed in your environment, specify the method to encrypt communications with the mail server (SMTP).

Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SSL/TLS Settings]	Select the method to encrypt communications with the E-mail server (SMTP) (default: [OFF]). This option supports SMTP over SSL and Start TLS.
[Port No.(SSL)]	If necessary, change the port number for SSL communication (default: [465]). This option is available when [SMTP over SSL] is selected for [SSL/TLS Settings].
[Certificate Verification Level Settings]	To validate the certificate during SSL communication, select items to be verified. <ul style="list-style-type: none"> [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).



Reference

Verifying the Peer's Certificate (page 11-20)

Using SMTP authentication

The SMTP authentication is a function that verifies the user using the user ID and password when sending an E-mail.

When SMTP authentication is installed in your environment, configure settings to use SMTP authentication.

Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)] - [Detail Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMTP Authentication]	When using SMTP authentication, set this option to ON (default: OFF).
[SMTP Authentication Method]	Set the SMTP authentication method to ON.
[User ID]	Enter the user ID for SMTP authentication (using up to 64 characters).
[Password]	Enter the password for SMTP authentication (using up to 64 characters, excluding ").
[Domain Name]	When the SMTP authentication method is Digest-MD5, enter the domain name (realm) (using up to 253 characters). When there are two or more domains (realm), enter the domain name. When there is only one domain (realm), no entry is required. The domain name is notified from the E-mail server (SMTP) at the initial communication, and communication is automatically performed using that domain name.

Setting	Description
[Authentication Setting]	<p>Select whether to synchronize the SMTP authentication with the user authentication of this machine (default: [Set Value]). This item is necessary when the user authentication is installed on this machine.</p> <ul style="list-style-type: none"> [User Authentication]: Uses the registered user's user authentication of this machine as authentication information for SMTP authentication. [Set Value]: Uses values entered at [User ID] and [Password]. If SMTP authentication fails because the user who sends an E-mail does not match the user specified in [User ID], set [Envelope-From Setting] to ON, then enter the E-mail address to be applied to Envelope-From in [From Address]. When [Envelope-From Setting] is set to OFF, the E-mail address of the administrator of this machine is applied to Envelope-From.

Using the POP before SMTP authentication

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

When POP before SMTP authentication is installed in your environment, configure settings to use POP before SMTP authentication.

- 1 Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)] - [Detail Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[POP Before SMTP]	<p>When using POP before SMTP, set this option to ON (default: OFF).</p> <ul style="list-style-type: none"> [POP Before SMTP Time]: If necessary, change the waiting time until starting E-mail transmission after the POP authentication is successful (default: [5] sec.). Depending on your environment, it may take time before the E-mail transmission is allowed after the POP authentication is successful. In that case, if an insufficient time period is specified, E-mail transmission may fail.

- 2 Select [Network] - [E-mail Setting] - [E-mail RX (POP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail RX Setting]	When receiving E-mails on this machine, set this option to ON (default: ON).
[POP Server Address]	<p>Enter the address of your E-mail server (POP). Use one of the following formats.</p> <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name used for POP authentication (using up to 63 characters).
[Password]	Enter the password for POP authentication (using up to 15 characters).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (POP) (default: [30] sec.).
[Port Number]	If necessary, change the port number of the E-mail server (POP) (default: [110]).

- 3 Configure the POP over SSL and APOP settings to suit your environment. Select [Network] - [E-mail Setting] - [E-mail RX (POP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[APOP Authentication]	When using APOP Authentication, set this option to ON (default: OFF).
[Enable SSL]	<p>When using SSL communications, set this option to ON (default: OFF).</p> <ul style="list-style-type: none"> [Port No.(SSL)]: If necessary, change the port number for SSL communication (default: [995]).

Setting	Description
[Certificate Verification Level Settings]	<p>To validate the certificate during SSL communication, select items to be verified.</p> <ul style="list-style-type: none"> • [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). • [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). • [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). • [Chain]: Confirm whether there is a problem in the certificate chain (certificate path). The chain is validated by referencing the external certificates managed on this machine (default: OFF). • [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).



Reference

Verifying the Peer's Certificate (page 11-20)

Using S/MIME

S/MIME is one of the E-mail encryption schemes. Using S/MIME encrypts an E-mail sent from this machine, preventing an interception by third parties during sending. Furthermore, adding a digital signature to an E-mail provides assurance regarding the authenticity of the sender, and certifies that the E-mail has not been falsified.

If S/MIME is installed in your environment, configure settings to use S/MIME.

- 1 Register a certificate used for E-mail encryption to the destination of E-mail transmission (page 13-2).
- 2 Register the certificate of this machine to be added to E-mails as digital signature (page 11-4).
- 3 Select [Network] - [E-mail Setting] - [S/MIME] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[S/MIME Comm.Setting]	<p>When using S/MIME, set this option to ON (default: OFF). To set to ON, the E-mail address of the certificate of this machine must match the E-mail address of the administrator.</p>
[Digital Signature]	<p>To add digital signature when sending E-mails, select a method to add it (default: [Do not add signature]).</p> <ul style="list-style-type: none"> • [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 to add digital signature before sending an E-mail.
[Digital Signature Type]	<p>To add a digital signature when sending E-mails, select its authentication method (default: [SHA-1]).</p>
[E-Mail Text Encrypt. Method]	<p>Select the method to encrypt the E-mail text (default: [3DES]).</p>
[Automatically Obtain Certificates]	<p>Select whether to automatically obtain the digital signature (user certificate) from the E-mail received on this machine (default: [OFF]). The obtained certificate is additionally registered in the E-mail address that matches the E-mail address described in the certificate.</p>
[Print S/MIME information]	<p>Select whether to print S/MIME information when this machine receives an S/MIME E-mail (default: [OFF]).</p>

Setting	Description
[Certificate Verification Level Settings]	<p>When verifying the obtained certificate while [Automatically Obtain Certificates] is set to [ON], select an item to be verified.</p> <ul style="list-style-type: none">• [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON).• [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF).• [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine.• [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

 **Tips**

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- 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.

Using the Scan to Me function

To use the Scan to Me function, register an E-mail address in the user's registration information.

This option is available when the MFP authentication or external server authentication is installed on this machine.

Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail Address]	Enter the user's E-mail address (using up to 320 characters, excluding spaces).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- If Active Directory is used as an authentication server, register the user's E-mail address in Active Directory.

Reference

Sending to your Address (Scan to Me) ("User's Guide[Scan Operations]/[Sending Original Data as an E-mail Attachment (Scan to E-mail)]")

Using the Scan to URL function

Configure the settings to use the Scan to URL function.

This option is available when the MFP authentication or external server authentication is installed on this machine.

- 1 Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail Address]	Enter the user's E-mail address (using up to 320 characters, excluding spaces).

- 2 Select [User Auth/Account Track] - [User Authentication Setting] - [URL display enable setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[URL display enable setting]	When using the Scan to URL function, set this option to ON (default: ON).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Reference

Sending the Download URL to your Address (Scan to URL) ("User's Guide[Scan Operations]/[Using Scan Sending Functions in Classic Style]")

5.2 Configuring the SMB Send environment

Setting flow

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

When the DNS server or WINS server is installed for name resolution, register each server.

Using LLMNR (Link-local Multicast Name Resolution) enables you to perform name resolution even in an environment that does not contain a DNS server or WINS server. This option is only compatible with Windows computers. It is useful to resolve the name in the IPv6 environment.

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

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring basic settings for SMB transmission (page 5-9)
- 3** Configuring settings to suit your environment
 - Using the WINS server (page 5-10)
 - Registering the DNS server (page 4-3)
 - Performing name resolution with LLMNR (page 5-10)
 - Using in DFS environment (page 5-10)
 - Using the Scan to Home function (page 5-11)
 - Constructing a single sign-on environment for SMB transmission (page 5-11)
 - Using the Scan to Authorized Folder function (page 5-12)
 - Checking whether there are sub folders when searching for an SMB sharing folder (page 5-13)



Tips

- 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, WINS, or LLMNR.
To perform name resolution with DNS, a destination computer can be specified with the "computer name (host name)" (example: host1) or "full computer name (FQDN)" (example: host1.test.local).
To perform name resolution with WINS or LLMNR, a destination computer can be specified only with a "computer name (host name)" (example: host1).

Configure basic settings for the SMB transmission

Configure the settings for using the SMB Send function.

Select [Network] - [SMB Setting] - [Client Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMB TX Setting]	When using the SMB TX function, set this option to ON (default: ON).
[SMB Authentication Setting]	Select an authentication method for SMB transmission according to your environment (default: [NTLM v1/v2]). <ul style="list-style-type: none"> • [NTLM v1]: Performs the NTLM v1 authentication. This option is available in the NT domain environment. • [NTLM v2]: Performs NTLM v2 authentication. This option is available in the NT domain environment. • [NTLM v1/v2]: Performs NTLM v1 authentication when NTLM v2 authentication fails. This option is available in the NT domain environment or Mac OS environment. • [Kerberos]: Performs Kerberos authentication. This option is available in the Active Directory domain environment.

Setting	Description
[SMB security Signature Setting]	<p>Select whether to enable the SMB signature of this machine to suit your environment (default: [When requested]).</p> <ul style="list-style-type: none"> [Disable]: Disables the SMB signature of this machine. [When requested]: Enables the SMB signature of this machine (client) only when the SMB signature is requested from the server side. If the SMB signature is not requested from the server side, operations are performed while the SMB signature of this machine (client) remains disabled, and a connection is possible even when the SMB signature on the server side is disabled. [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the server side. If the SMB signature in the server side is disabled, it will not be possible to make a connection.

Using the WINS server

When WINS is installed in your environment, register the WINS server.

Select [Network] - [SMB Setting] - [WINS/NetBIOS Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[WINS/NetBIOS]	When using the WINS server, set this option to ON (default: ON).
[Auto Obtain Setting]	When automatically specifying the WINS server address using DHCP, set this option to ON (default: ON).
[WINS Server Address1]/[WINS Server Address2]	<p>Enter the WINS server address when manually specifying it. Use the following entry formats.</p> <ul style="list-style-type: none"> Example of entry: "192.168.1.1"
[Node Type Setting]	<p>Select the name resolution method (default: [H Node]).</p> <ul style="list-style-type: none"> [B Node]: Makes inquires 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.

Resolving the name using LLMNR

Using LLMNR (Link-local Multicast Name Resolution) enables you to resolve the name even in an environment that does not have a DNS server. This option is only compatible with Windows computers. It is useful to resolve the name in the IPv6 environment.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting1] - [DNS Host] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LLMNR Setting]	When using LLMNR, set this option to ON (default: ON).

Using in the DFS environment

If DFS (Distributed File System) is installed in your environment, enable DFS.

Select [Network] - [SMB Setting] - [Client Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[DFS Setting]	When using DFS, set this option to ON (default: ON).

Using the Scan to Home function

Configure the settings to use the Scan to Home function.

This function is available when the user's home folder is registered in Active Directory while user authentication by Active Directory is installed on this machine.

Select [User Auth/Account Track] - [User Authentication Setting] - [Scan to Home Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Scan to Home Settings]	When using the Scan to Home function, set this option to ON (default: OFF).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Reference

Sending to Your Computer (Scan to Home) ("User's Guide[Scan Operations]/[Sending a File to a Shared Folder of a Computer (SMB Send)]")

Constructing a single sign-on environment for the SMB transmission

When user authentication by Active Directory is enabled, single sign-on can be set on this machine.

Select [Network] - [SMB Setting] - [Client Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMB TX Setting]	When using the SMB TX function, set this option to ON (default: ON).
[SMB Authentication Setting]	To use the single sign-on function, select [Kerberos] (default: [NTLM v1/v2]).
[Authentication Setting if Kerberos Fails]	If [Kerberos] is selected in [SMB Authentication Setting], select whether to perform NTLM authentication when Kerberos authentication has failed (default: [Disable NTLM]). <ul style="list-style-type: none"> • [Enable NTLM v1/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. • [Disable NTLM]: Assumes that authentication fails when Kerberos authentication has failed.

Setting	Description
[Single Sign-On Setting]	<p>Configure the single sign-on function for SMB transmission. By using the user authentication information (login name and password) of this machine as SMB destination authentication information (user ID and password), you can reduce the number of steps required to specify SMB destination authentication information, enabling you to configure a single sign-on environment for SMB transmission.</p> <ul style="list-style-type: none"> [Default Domain Name]: When a server other than Active Directory is used for external server authentication or external server authentication is not used, specify the name of the domain to which the destination host belongs at SMB transmission (using up to 64 characters). When Active Directory is used for external server authentication, the value specified in this step is ignored, and the domain name of the login destination for external server authentication is used instead. If [Kerberos] is selected in [SMB Authentication Setting], entry is required. [SMB User Credential Setting]: When using the user authentication information (login name and password) of this machine as SMB destination authentication information (user ID and password), set this option to ON (default: OFF). [Edit SMB User Credentials]: This option is available when [SMB User Credential Setting] is set to ON (default: OFF). Setting to OFF (Restrict) registers SMB destinations, excluding the user ID and password specified at login. However, using Web Connection, an SMB destination is registered, including the user ID and password. Setting to ON (Allow) enables you to select whether to register SMB destinations, including the user ID and password. Selecting [Reg. excl. ID and Password] automatically adds the user ID and password at SMB transmission.
[User Authentication(NTLM)]	When using single sign-on, set this option to ON (default: ON).
[SMB security Signature Setting]	<p>Select whether to enable the SMB signature of this machine to suit your environment (default: [When requested]).</p> <ul style="list-style-type: none"> [Disable]: Disables the SMB signature of this machine. [When requested]: Enables the SMB signature of this machine (client) only when the SMB signature is requested from the server side. If the SMB signature is not requested from the server side, operations are performed while the SMB signature of this machine (client) remains disabled, and a connection is possible even when the SMB signature on the server side is disabled. [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the server side. If the SMB signature in the server side is disabled, it will not be possible to make a connection.

Using the Scan to Authorized Folder function

Configure the settings to use the Scan to Authorized Folder function.

Using the Scan to Authorized Folder function allows you to limit SMB transmission destinations only to computers that can be connected using user authentication information.

Select [User Auth/Account Track] - [Scan to Authorized Folder Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Scan to Authorized Folder Settings]	<p>When restricting the available destinations, set this option to ON (default: OFF). If [Scan to Authorized Folder Settings] is set to ON, the following restrictions will be applied:</p> <ul style="list-style-type: none"> Addresses cannot be specified by direct input for scan transmission. Users cannot save files to User Boxes. Users cannot send files from User Boxes. Users cannot use annotation User Boxes. Users cannot select addresses from transmission log. Users cannot use the URL notification function.

To use Scan to Authorized Folder, configure the following settings in addition to [Scan to Authorized Folder Settings].

Setting	Description
User Authentication	Enable user authentication.
SMB Send	Enable the SMB send function.
SMB Registration	Register the SMB destinations. <ul style="list-style-type: none"> Addresses other than SMB cannot be used concurrently with Scan to Authorized Folder. If address book, group, and program data other than SMB are registered, delete all of them. The [User ID] of the registered SMB address must be left blank.
Limit user's registration/change of address	Disable user's registration/change of address.
Limit Public User Function	When access by public users is allowed, disable the scan function for public users.
Delete LDAP server registration	If the LDAP server is not used, delete the registration information of the LDAP server from this machine.

Checking whether there are sub folders when searching for an SMB sharing folder

Specify whether to check if there are sub folders when this machine searches for an SMB sharing folder on the network.

Select [Network] - [SMB Setting] - [SMB Browsing setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMB Browsing setting]	Select whether to check if there are sub folders when searching for an SMB sharing folder on the network (default: [Disable Sub search]). <ul style="list-style-type: none"> [Enable Sub search]: Checks whether there are sub folders. If there are sub folders, "+" is displayed on the parent folder icon. [Disable Sub search]: Does not check whether there are sub folders. Select this option to shorten the time required to display the result when searching for a folder.

5.3 Configuring the operating environment for FTP Send

Setting flow

The FTP transmission is a function that sends 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 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for FTP transmission (page 5-14)
- 3 Configuring settings to suit your environment
 - Using the proxy server (page 5-14)

Configuring basic settings for the FTP transmission

Configure the settings for using the FTP Send function.

Select [Network] - [FTP Setting] - [FTP TX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[FTP TX]	When using the FTP Send function, set this option to ON (default: ON).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the FTP server (default: [60] sec.).
[Port No.]	If necessary, change the FTP server port number (default: [21]).

Using a proxy server

When a proxy server is installed in your environment, register the proxy server.

Select [Network] - [FTP Setting] - [FTP TX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number (default: [21]).

5.4 Configuring the WebDAV transmission environment

Setting flow

The WebDAV transmission is a function that sends 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 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for WebDAV transmission (page 5-15)
- 3 Configuring settings to suit your environment
 - Using the proxy server (page 5-15)
 - Establishing SSL communication (page 5-16)

Configure basic settings for the WebDAV transmission

Configure the settings for using the WebDAV Send function.

Select [Network] - [WebDAV Settings] - [WebDAV Client Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[WebDAV TX Setting]	When using the WebDAV TX function, set this option to ON (default: ON).
[Chunk Transmission]	When sending data by dividing it into some chunks, set this option to ON (default: OFF). Configure the setting if your WebDAV server supports chunk transmission.
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the WebDAV server (default: [60] sec.).
[Server Authentication Character Code]	Select a character code to perform the authentication under the WebDAV server (default: [UTF-8]). You can use this setting when [Japanese] is specified for the language to be displayed on the screen of this machine.
[HTTP Version Setting]	Select the version of the protocol for HTTP communication (default: [HTTP/1.1]). <ul style="list-style-type: none"> • [HTTP/1.1]: Uses HTTP/1.1 only. • [HTTP/2, HTTP/1.1]: Uses HTTP/2 when connected to HTTP/2. In other cases, HTTP/1.1 is used.

Using a proxy server

When a proxy server is installed in your environment, register the proxy server.

Select [Network] - [WebDAV Settings] - [WebDAV Client Settings] - [Proxy Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number (default: [8080]).
[User Name]	Enter the user name used for proxy authentication (using up to 63 characters).
[Password]	Enter the password used for proxy authentication (using up to 63 characters).

Using SSL communication

If SSL is installed in your environment, enable SSL.

- 1 Select [Store Address] - [Address Book] - [WebDAV] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and set [SSL Settings] to ON (default: OFF).
→ To directly enter a destination WebDAV server, configure SSL setting when entering the destination.
- 2 Select [Network] - [WebDAV Settings] - [WebDAV Client Settings] - [Certificate Verification Level Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and specify the certificate verification method.

Setting	Description
[Expiration Date]	Confirm whether the certificate is still valid (default: ON).
[CN]	Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF).
[Key Usage]	Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF).
[Chain]	Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine.
[Expiration Date Confirmation]	Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).



Reference

Verifying the Peer's Certificate (page 11-20)

5.5 Configuring the WSD scan environment

Setting flow

WSD (Web Service for Device) is a function to search for a WSD-compatible device on the network.

WSD Scan enables you to instruct scanning from a computer and import the original data without configuring tiresome environmental settings. This option is only compatible with Windows computers.

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

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

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring basic settings for WSD Scan (page 5-17)
- 3** Configuring settings to suit your environment
 - Using the proxy server (page 5-18)
 - Establishing SSL communication (page 5-18)
- 4** Configuring your computer ("User's Guide[Scan Operations]/[Using Scan Sending Functions in Classic Style]")

Configuring basic settings for WSD Scan

Configure the settings to use the WSD Scan function.

- 1** Select [Network] - [DPWS Settings] - [DPWS Common Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Friendly Name]	Enter the name of this machine to be displayed when being searched using the Web service from the computer (using up to 62 characters).
[Publication Service]	When using this machine in either one of the following environments, set this option to ON (default: ON). <ul style="list-style-type: none"> • Environment where NetBIOS is disabled on Windows computer • Environment constructed so that only communications using IPv6 are allowed Up to 512 destinations can be detected in Publication Service (including detection counts by NetBIOS).

- 2** Select [Network] - [DPWS Settings] - [Scanner Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Scan Function]	When using the WSD scan function, set this option to ON (default: OFF).
[Scanner Name]	Enter the name of this machine when using it as the WSD scanner (using up to 63 characters).
[Scanner Location]	Enter a scanner location if necessary (using up to 63 characters).
[Scanner Information]	Enter scanner information if necessary (using up to 63 characters).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the computer (default: [120] sec.).

Using a proxy server

Configure settings to establish communications in the environment where the multicast communication is restricted using the discovery proxy defined by WS-Discovery. Configure the setting if your environment requires the discovery proxy server.

In normal circumstances, the computer must be connected at a location where multicast communication is available for this machine. However, installing the discovery proxy server at a location where unicast communication is available for this machine enables communications even in environment with multicast communication restricted.

Select [Network] - [DPWS Settings] - [DPWS Extension Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable Proxy]	When using discovery proxy, set this option to ON (default: OFF).
[Proxy1] to [Proxy3]	Register the discovery proxy server. <ul style="list-style-type: none"> [Proxy Server Address]: Enter the discovery proxy server address. Use one of the following formats. Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" [File Path]: Enter the service name at the path of the URL where the WS-Discovery service is published in the discovery proxy server (using up to 255 characters). [Enable SSL]: When using SSL communications, set this option to ON (default: OFF). [Proxy Server Port Number]: If necessary, change the port number of the discovery proxy server (default: [80]/[443] (in use of SSL)).

Using SSL communication

Configure settings to encrypt communications between this machine and the computer using SSL.

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

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

Select [Network] - [DPWS Settings] - [DPWS Common Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SSL Setting]	When using SSL communications, set this option to ON (default: OFF).
[Certificate Verification Level Settings]	To validate the certificate during SSL communication, select items to be verified. <ul style="list-style-type: none"> [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

Tips

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



Reference

Verifying the Peer's Certificate (page 11-20)

5.6 Configuring the TWAIN scan environment

Setting flow

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

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for TWAIN Scan (page 5-20)
- 3 Configuring settings to suit your environment
 - Changing the operation lock time (page 5-20)

Configuring the basic settings for the TWAIN scan

Configure the settings to use the TWAIN Scan function.

- 1 Select [Network] - [SNMP Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SNMP]	When using the TWAIN scan function, set this option to ON (default: ON). Select the check box of the SNMP version you use.
[UDP Port Setting]	If necessary, change the UDP port number (default: [161]).

- 2 Select [Network] - [TCP Socket Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TCP Socket]	When using the TWAIN scan function, set this option to ON (default: ON).
[Port No.]	If necessary, change the TCP Socket port number (default: [59158]).

Changing the operation lock time

While the TWAIN scan is running, **Control Panel** operations are locked. If necessary, change the time period before the control panel is unlocked.

Select [System Settings] - [Network TWAIN] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine), and configure the following settings.

Setting	Description
[TWAIN Lock Time]	Change the time until the operation lock is released (default: [120] seconds).

5.7 Configuring Settings to Search for a Destination via the LDAP Server

Setting flow

If the LDAP server or the Active Directory of Windows Server is used for user management, you can search for (LDAP Search) destination information registered in the server and specify the desired destination.

When using the LDAP search function, follow the below procedure to configure the settings.

- ✓ To use the LDAP function of the Active Directory server, you must register the DNS server that synchronizes the Active Directory on this machine before starting the procedure. For details on how to register the DNS server, refer to page 4-3.
 - ✓ To use the LDAP function of the Active Directory server, you must match the date and time of this machine and Active Directory. For details on how to set the date and time of this machine, refer to page 3-4.
- 1 Configuring network settings of this machine (page 4-2)
 - 2 Configuring basic settings for LDAP search (page 5-21)
 - 3 Configuring settings to suit your environment
 - Establishing SSL communication (page 5-22)



Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Configure basic settings for the LDAP search

Configure settings to search for destination information registered in the LDAP server.

- 1 Select [Network] - [LDAP Setting] - [LDAP Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enabling LDAP]	To perform LDAP search, select [ON] (default: [OFF]).
[Default Search Result Display Setting]	Select whether an E-mail address, fax number, or Internet fax number is given priority to be displayed as the destination search result when searching for destinations from the LDAP server (default: [E-mail]).

- 2 Select [Network] - [LDAP Setting] - [Setting Up LDAP] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LDAP Server Name]	Enter the name of the LDAP server (using up to 32 characters).
[Server Address]	Enter the LDAP server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number (default: [389]).
[Search Base]	Specify the starting point to search for a destination (using up to 255 characters). The range from the entered origin point, including the following tree structure, is searched. Example of entry: "cn=users,dc=example,dc=com"
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server (default: [60] sec.).
[Max.Search Results]	Change the maximum number of destinations to be displayed as search results, if necessary (default: [100]).

Setting	Description
[General Settings]	Select the authentication method to log in to the LDAP server depending on your environment (default: [anonymous]). <ul style="list-style-type: none"> [Login Name]: Enter the login name used for LDAP authentication (using up to 64 characters). [Password]: Enter the password for LDAP authentication (using up to 64 characters). [Domain Name]: If [GSS-SPNEGO] is selected for [General Settings], enter the domain name of Active Directory (using up to 64 characters).
[Select Server Authentication Method]	Select whether to synchronize the LDAP authentication with the user authentication of this machine (default: [Set Value]). <ul style="list-style-type: none"> [Set Value]: Uses values entered in [Login Name] and [Password]. [User Authentication]: Uses the registered user's user authentication of this machine as authentication information for LDAP authentication. [Dynamic Authentication]: The system prompts you to enter the user name and password at LDAP searching.
[Use Referral]	If necessary, select whether to use the referral function (default: [ON]).
[Search Condition Attributes]	Select attributes to be specified when performing the LDAP search (default: [Name]). The setting can be switched between [Name] (cn) and [Nickname] (displayName).
[Search]	Select whether to display candidate destinations when entering a part of the name to perform LDAP search (default: [OFF]).
[Initial Setting for Search Details]	Specify the default LDAP search conditions for each item (default: [OR]). <ul style="list-style-type: none"> [Search Attributes Authentication]: When enabling Search Attributes Authentication, set this option to ON (default: OFF). Configure this setting when [General Settings] is set to [Simple] and [Select Server Authentication Method] to [Dynamic Authentication]. If enabled, the user does not need to enter all of the DN (Distinguished Name) when performing authentication via the LDAP server. [Search Attribute]: Enter the search attribute to be automatically added before the user name (using up to 64 characters). The attribute must start with an alphabet character (default: [uid]). In normal circumstances, specify "uid" before the user name, however, depending on your environment, you need to specify other attribute such as "cn".


Tips

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

Using SSL communication

If SSL is installed in your environment, enable SSL.

Select [Network] - [LDAP Setting] - [Setting Up LDAP] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable SSL]	When using SSL communications, set this option to ON (default: OFF). <ul style="list-style-type: none"> [Port No.(SSL)]: If necessary, change the port number for SSL communication (default: [636]).

Setting	Description
[Certificate Verification Level Settings]	<p>To validate the certificate during SSL communication, select items to be verified.</p> <ul style="list-style-type: none">• [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON).• [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF).• [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF).• [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine.• [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

**Reference**

Verifying the Peer's Certificate (page 11-20)

5.8 Associating with the distributed scan server

Setting flow

This machine can be associated with the Distributed Scan Management system (scan server) of Windows Server.

This machine converts the scanned original data into a computer compatible file format, and sends its file to a scan server. When receiving the file, the scan server carries out sending to the SMB folder, E-mail address, or Microsoft Office SharePoint Server based on the registered scan process.

✓ This machine must join the Active Directory domain in advance.

1 Enable WSD scan and configure the SSL communication settings (page 5-17)

2 Associating with the Distributed Scan Management system (page 5-24)

Associating with the Distributed Scan Management system

Configure settings to associate with the Distributed Scan Management system.

Select [Network] - [Distributed Scan Function Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Distributed Scan Function Settings]	When associating this machine with the Distributed Scan Management system of Windows Server to use the scan function, set this option to ON (default: OFF).



Configuring the Printing Environment

6 Configuring the Printing Environment

6.1 Configuring the LPR printing environment

Setting flow

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

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Enabling LPD (page 6-2)

Enabling LPD

To use the LPR print function, enable LPD (Line Printer Daemon).

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting2] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LPD Setting]	When enabling LPD, set this option to ON (default: ON).

6.2 Configuring the Port9100 printing environment

Setting flow

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

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Changing the RAW port number as needed (page 6-3)

Changing the RAW port number

Specify a RAW port number required for Port9100 printing.

Select [Network] - [TCP/IP Setting] - [TCP/IP Setting2] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[RAW Port Number]	<p>Change the RAW port number to suit your environment. The following shows the default settings.</p> <ul style="list-style-type: none">• [Port 1]: 9100• [Port 2]: 9112• [Port 3]: 9113• [Port 4]: 9114• [Port 5]: 9115• [Port 6]: 9116

6.3 Configuring the SMB printing environment

Setting flow

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

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

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring basic settings for SMB Print (page 6-4)
- 3** Configuring settings to suit your environment
 - Using the WINS server (page 5-10)
 - Performing name resolution with LLMNR (page 5-10)

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Configure basic settings for the SMB printing

Configure settings to use the SMB server.

Select [Network] - [SMB Setting] - [SMB Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMB Server Settings]	When using this machine as the SMB server, set this option to ON (default: OFF).
[SMB Server Common Settings]	<p>Configure common settings to use the machine as an SMB server.</p> <ul style="list-style-type: none"> • [SMB Host Name]: Enter the host name of this machine (using up to 15 characters). • [Workgroup]: Enter the name of the workgroup that contains this machine (using up to 15 characters, excluding ", \, ;, :, *, <, >, , +, =, and ?). • [SMB Authentication Protocol]: Select the SMB authentication protocol to be used in the machine (default: [SMB1.0/SMB2.0/SMB3.0]). • [SMB security Signature Setting]: Select whether to enable the SMB signature of this machine to suit your environment (default: [Only When Requested]). <p>[Disable]: Disables the SMB signature of this machine. [Only When Requested]: Enables the SMB signature of this machine (server) only when the SMB signature is requested from the client side. If the SMB signature is not requested from the client side, operations are performed while the SMB signature of this machine (server) remains disabled, and a connection is possible even when the SMB signature in the client side is disabled. [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the client side. If the SMB signature in the client side is disabled, it will not be possible to make a connection.</p>
[SMB Print Setting]	<p>Configure the settings to use the SMB Print function.</p> <ul style="list-style-type: none"> • [SMB Print]: When using the SMB Print function, set this option to ON (default: OFF). • [Print Service Name]: Enter a print service name in uppercase letters (up to 12 characters, excluding / and \).

6.4 Configuring the IPP printing environment

Setting flow

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

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

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for IPP Print (page 6-5)
- 3 Configuring settings to suit your environment
 - Performing IPP authentication (page 6-5)
 - Establishing SSL communication (IPPS) (page 6-6)

Configuring basic settings for the IPP printing

Configure the settings to use the IPP print function.

Select [Network] - [HTTP Server Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IPP Setting]	When enabling IPP, set this option to ON (default: ON).
[Accept IPP Jobs]	When using the IPP print function, set this option to ON (default: ON).
[IPP HTTP Version Set.]	Select the version of the HTTP protocol for IPP communication (default: [HTTP/1.1]). <ul style="list-style-type: none"> • [HTTP/1.1]: Uses HTTP/1.1 only. • [HTTP/2, HTTP/1.1]: Uses HTTP/2 when connected to HTTP/2. In other cases, HTTP/1.1 is used.
[Support Operation]	Select whether to allow the following IPP operations. <ul style="list-style-type: none"> • [Print Job]: Allows a print job (default: ON). • [Valid Job]: Allows you to check a valid job (default: ON). • [Cancel Job]: Allows you to cancel a job (default: ON). • [Open Job Attributes]: Allows you to obtain job attributes (default: ON). • [Open Job]: Allows you to obtain a list of job attributes (default: ON). • [Open Printer Attributes]: Allows you to obtain printer attributes (default: ON).
[Printer Information]	If necessary, enter the printer information of this machine. <ul style="list-style-type: none"> • [Printer Name]: Enter the printer name of this machine (using up to 127 characters). • [Printer Location]: Enter the location where to install this machine (using up to 127 characters). • [Printer Information]: Enter printer information of this machine (using up to 127 characters). • [Printer URI]: Displays the URI of the printers that can print data using the IPP.

Using the IPP authentication

Configure a setting to use IPP authentication.

Select [Network] - [HTTP Server Setting] - [IPP Authentication Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IPP Authentication Settings]	When using IPP authentication, set this option to ON (default: ON).
[General Settings]	Select an IPP authentication method (default: [requesting-user-name]).

Setting	Description
[User Authentication Synchronization]	When synchronizing IPP authentication and user authentication, set this option to ON (default: OFF). This item is necessary when the user authentication is installed on this machine. If ON is selected, the registered user's authentication information of this machine is used as authentication information for IPP authentication. When [requesting-user-name] is selected in [General Settings], you cannot set this option to ON.
[User Authentication Information for IPP Print]	Select which login information is used for user authentication to manage IPP print jobs on this machine when [User Authentication Synchronization] is set to ON (default: [Prioritize IPP Authentication Information]). <ul style="list-style-type: none"> [Prioritize IPP Authentication Information]: Uses the user name and password for IPP authentication. [Prioritize PJI Information]: Prioritizes the user name and password for PJI, and uses the user name and password for IPP authentication only when there is no PJI description.
[User Name]	Enter the user name used for IPP authentication (using up to 20 characters, excluding colon ":"). This entry is required if you have selected [basic], [digest-MD5], or [digest-SHA2] for [General Settings].
[Password]	Enter the password for IPP authentication (using up to 20 characters). This entry is required if you have selected [basic], [digest-MD5], or [digest-SHA2] for [General Settings].
[realm]	If [digest-MD5] or [digest-SHA2] is selected for [General Settings], enter the domain (realm) (using up to 127 characters).
[Validity Period]	Enter the validity period of IPP authentication information (default: [5] min.). If this value is set to [0] min., authentication information is discarded after authentication has been completed.

Communicating using SSL (IPPS)

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

- 1 Register a certificate for this machine and enable SSL communication (page 11-4).
- 2 Select [Network] - [HTTP Server Setting] - [IPP-SSL Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IPP-SSL Setting]	Select whether to use SSL communication or not (default: [Non-SSL Only]). <ul style="list-style-type: none"> [Non-SSL Only]: Only non-SSL communication is allowed. [SSL Only]: Only SSL communication is allowed. [SSL/Non-SSL]: Both SSL communication and non-SSL communication are allowed.

To perform IPPS printing on a Windows computer, check the following points.

- When using the IPPS to print data on this machine, configure settings for this machine using the following procedure.
 - "https://host name.domain name/ipp"
For the host name and domain name, enter [DNS Host Name] and [DNS Default Domain Name] you specified for [TCP/IP Setting1] of this machine.
- Confirm that the name resolution of this machine is possible using the DNS server from the computer. Register this machine in the DNS server in advance. In addition, configure DNS settings on the computer.
- If the certificate of this machine is not the one issued by the Certificate Authority (CA), you must register the certificate of this machine in [Trusted Root Certification Authorities] of the computer.

6.5 Configuring the WSD printing environment

Setting flow

WSD (Web Service for Device) is a function to search for a WSD-compatible device on the network.

This function allows you to automatically detect the machine connected to the network and easily install it 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 the this machine and the computer enables more secure printing.

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for WSD Print (page 6-7)
- 3 Configuring settings to suit your environment
 - Using the proxy server (page 5-18)
 - Establishing SSL communication (page 5-18)
- 4 Configuring your computer ("User's Guide[Print Operations]/[Printing in the Windows Environment]")



Tips

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

Configuring basic settings for WSD Print

Configure the settings to use the WSD print function.

- 1 Select [Network] - [DPWS Settings] - [DPWS Common Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Friendly Name]	Enter the name of this machine to be displayed when being searched using the Web service from the computer (using up to 62 characters).
[Publication Service]	When using this machine in either one of the following environments, set this option to ON (default: ON). <ul style="list-style-type: none"> • Environment where NetBIOS is disabled on Windows computer • Environment constructed so that only communications using IPv6 are allowed Up to 512 destinations can be detected in Publication Service (including detection counts by NetBIOS).

- 2 Select [Network] - [DPWS Settings] - [Printer Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Print Function]	When using the WSD print function, set this option to ON (default: OFF).
[WSD Print V2.0 Setting]	When using the functions of WSD print version 2.0, set this option to ON (default: ON). When you connect this machine from the computer compatible with version 2.0, you can issue a printing prenotification to this machine, send account information, specify parameters for the advanced device functions, or obtain the device capability and localization information.
[Printer Name]	Enter the name of this machine when using it as the WSD printer (using up to 63 characters).
[Printer Location]	Enter a printer location if necessary (using up to 63 characters).
[Printer Information]	Enter printer information if necessary (using up to 63 characters).

6.6 Configuring the Bonjour printing environment

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

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

Enabling the Bonjour function on this machine enables the computer to automatically detect this networked machine and display it in the list as a printer that can be added.

Select [Network] - [Bonjour Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Bonjour]	When using Bonjour, set this option to ON (default: OFF).
[Bonjour Name]	Enter a Bonjour name that is to be displayed as the name of connected device (using up to 63 characters).
[Wide-Area Bonjour]	When using Wide-Area Bonjour, set this option to ON (default: ON). You can detect this machine across segments from the computer while the machine and computer are connected to different networks. To use Wide-Area Bonjour, you need to specify the DNS server address you are using.

6.7 Configuring the E-mail RX Print environment

Setting flow

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

If you send the E-mail, to which the target file is attached, to the E-mail address of this machine, you can print the file on this machine without using the printer driver. If necessary, you can save an E-mail attachment in a User Box of the machine.

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

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configure the E-mail address of this machine (page 3-2)
- 3 Configure settings to receive E-mails on this machine (page 6-9)
- 4 Configure settings to print a received E-mail attachment (page 6-9)

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Configure settings to receive E-mails on this machine

Configure the settings to enable this machine to receive an E-mail.

Select [Network] - [E-mail Setting] - [E-mail RX (POP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail RX Setting]	When receiving E-mails on this machine, set this option to ON (default: ON).
[POP Server Address]	Enter the address of your E-mail server (POP). Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name used for POP authentication (using up to 63 characters).
[Password]	Enter the password for POP authentication (using up to 15 characters).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (POP) (default: [30] sec.).
[Port No.]	If necessary, change the port number of the E-mail server (POP) (default: [110]).
[Check for New Messages]	When periodically connecting to the E-mail server (POP) to check whether E-mails arrive or not, set this option to ON (default: ON). <ul style="list-style-type: none"> • [Polling Interval]: Specify an interval to check whether E-mails arrive or not (default: [15] min.).

Configure settings to print a received E-mail attachment

Configure a setting to use the E-mail RX Print function.

Select [Network] - [E-mail Setting] - [E-mail RX Print] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail RX Print]	When using the E-mail RX Print function, set this option to ON (default: OFF).
[E-mail RX Permission]	When restricting E-mail addresses that are available for the E-mail RX Print function, set this option to ON (default: OFF). <ul style="list-style-type: none"> • [Permit Address 1] to [Permit Address 10]: Enter the E-mail addresses for which you want to permit the E-mail RX Print function, or enter the E-mail domain.

Setting	Description
[Save in User Box]	<p>When saving all the E-mail attachment files received on this machine to a User Box, set this option to ON (default: OFF).</p> <ul style="list-style-type: none">• In [User Box No.], enter the number of the User Box to save an E-mail attachment in. If the number of the User Box to save the E-mail attachment in is not specified by E-mail, the file is saved in the User Box for which you have entered a number. When you receive an encrypted PDF file as an E-mail attachment, the file is saved in the Password Encrypted PDF User Box.

6.8 Specifying the default print settings for this machine

6.8.1 Specifying the default PCL print settings

To make adjustments, the adjustment value specified here is added to that of the image quality specified in the PCL driver when data is printed from a computer.

Select [Print Setting] - [PCL Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Brightness]	Adjust the brightness to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the brightness specified in the PCL driver.
[Contrast]	Adjust the contrast to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the contrast specified in the PCL driver.
[Saturation]	Adjust the saturation to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the saturation specified in the PCL driver.
[Color Balance]	Adjust the color balance to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the color balance specified in the PCL driver.

6.8.2 Specifying the default PS print settings

To make adjustments, the adjustment value specified here is added to that of the image quality specified in the PS driver when data is printed from a computer.

Select [Print Setting] - [PS Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Brightness]	Adjust the brightness to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the brightness specified in the PS driver.
[Contrast]	Adjust the contrast to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the contrast specified in the PS driver.
[Saturation]	Adjust the saturation to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the saturation specified in the PS driver.
[Color Balance]	Adjust the color balance to print data from a computer (default: [0]). To make adjustments, the adjustment value specified here is added to that of the color balance specified in the PS driver.

6.8.3 Configuring security settings for XPS or OOXML printing

Configuring security settings for XPS or OOXML printing.

Select [Print Setting] - [Security Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Print XPS/OOXML Errors]	To print error information when an error occurs during printing of an XPS or OOXML (docx, xlsx, or pptx) file, set this option to ON (default: ON).

6.9 Specifying the time-out time by interface

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

Select [Print Setting] - [Interface Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Network Timeout]	When this machine is connected via a network to the computer, change the communication time-out time (default: [60] sec.).
[USB Timeout]	When this machine is connected via a USB device to the computer, change the communication time-out time (default: [60] sec.).

6.10 Restricting the Obtainment of Device Information from the Drive Using the Password

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

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

Select [Print Setting] - [Assign Account to Acquire Device Info] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Assign Account to Acquire Device Info]	<p>When restricting the acquirement of device information from the printer driver using the password, set this option to ON (default: OFF).</p> <ul style="list-style-type: none">• [Password]: Enter a password to restrict device information to be obtained (using up to eight characters, excluding spaces and "). Inform users who obtain device information from the printer driver of the password you have entered in this field.

6.11 Printing from the Bypass Tray Using the Paper Settings Configured in the Printer Driver

When printing data from a computer using the **Bypass Tray**, you can put the settings configured in the printer driver ahead of the paper size and paper type for the **Bypass Tray** that are specified on this machine.

Select [System Settings] - [Bypass Tray Overwrite Settings for Print PC] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Bypass Tray Overwrite Settings for Print PC]	When specifying Bypass Tray in the printer driver to make prints, select whether to prioritize the paper setting in the printer driver or that in the main unit (default: [Driver Priority]).

6.12 Changing the Time to Light up the LED of this Machine after Printing

You can change the time to light up the **Print Indicator** after printing was completed.

Select [System Settings] - [Print end notification lamp ON time settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Print end notification lamp ON time settings]	Change the time to light up the Print Indicator after printing was completed (default: [4] sec.).



Configuring the Fax Environment

7 Configuring the Fax Environment

7.1 Configuring basic fax settings

7.1.1 Configuring the Line Usage Settings

Configure the environment to use fax functions on this machine, such as the types of telephone lines (dialing method) and fax receive mode.

Select [Fax Settings] - [Line Parameter Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Dialing Method]	Select the line type according to your environment (default: [PB]).
[Receive Mode]	Select the fax receiving method (default: [Auto RX]). <ul style="list-style-type: none"> [Auto RX]: Automatically start receiving a fax if the call is a fax call. [Manual RX]: Manually request the reception of a fax. Select this mode if a phone is connected to this machine and you expect frequent voice calls.
[Number of RX Call Rings]	If necessary, change the number of times the phone rings before automatically receiving a fax (default: [2] times).
[Number of Redials]	If the machine fails to send a fax successfully, it automatically redials the same destination after a certain period of time has elapsed. If necessary, change the number of redials (default: [3] times).
[Redial Interval]	If necessary, change the redial intervals when you specified a value in [Number of Redials] (the setting range varies according to the local standards).
[Manual RX V34 Setting]	To cancel the V.34 function when manually receiving a fax, set this option to ON (default: OFF).
[Line Monitor Sound]	When monitoring the communication sound on the telephone line during fax communication, set this option to ON (default: OFF).
[Line Monitor Sound Volume (Send)]	Specify the line monitor sound level during fax transmission (default: [3]). When communicating with fax, a monitoring sound is generated even if send or receive monitoring sound of this machine is set to [0] since the sound is generated both on this machine and on the destination side. For setting to mute, set both [Line Monitor Sound Volume (Send)] and [Line Monitor Sound Volume (Receive)] to [0], or set [Line Monitor Sound] to OFF.
[Line Monitor Sound Volume (Receive)]	Specify the line monitor sound level during fax receiving (default: [4]). When monitoring the fax receiving sound, monitor sounds output from the recipient, including switching equipment or TA.
[Pause Time]	If necessary, change the wait time when the pause is entered (default: [1] sec.).

7.1.2 Configuring connection settings for a PBX environment

Configure settings to connect this machine to PBX (private branch exchange).

Select [Fax Settings] - [Function Setting] - [PBX Connection Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[PBX Connection Setting]	When using PBX, set this option to ON (default: OFF).
[Outside Line]	Enter an outside line number (using up to four digits). When a [Outside] key is selected to specify a destination, the outside line entered in this option is added.

Setting	Description
[PBX Dial Tone Detection Settings]	Configure the settings to detect the tone signal for extension connection. To restrict a PBX connection only for a specific line, service settings must be configured by your service representative. For details, contact your service representative.


Tips

- When [PBX Connection Setting] is set, the [Outside] key is displayed on the destination specification screen. When you specify the destination using the [Outside] key, it prevents cancellation of significant digits from occurring to a dialed number, which allows a fax to be sent to the correct destination.
- If you select [Fax Settings] - [Function Setting] - [Function ON/OFF Setting] and also set [Require the use of the External Line key for outside calling] to ON, you can prohibit the user from entering an outside line number without using the [Outside] key.

7.1.3 Registering the sender information

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

Select [Fax Settings] - [Header Information] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Sender Fax No.]	Enter the fax number of this machine (using up to 20 digits, including symbols #, *, +, and spaces). The fax number you entered is printed as the sender information.

To register a new sender name, specify an unregistered number in the sender name list, and select [Edit].

Setting	Description
[No.]	Displays the registration number.
[Sender Name]	Enter the sender name (using up to 30 characters).

7.2 Specifying operations when sending and receiving a fax

7.2.1 Specifying How to Print the Sender Name/Reception Information

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

Select [Fax Settings] - [Header/Footer Position] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Header Position]	Specify the position at which a sender information is printed on a fax (default: [Outside Body Text]). <ul style="list-style-type: none"> [Inside Body Text]: Prints the sender information inside the original image. Part of the original image may be cut off. [Outside Body Text]: Prints the sender information outside the original image. [OFF]: Does not print sender information. [OFF] is not available in the USA and Hong Kong models.
[TTI Print Position and Character Size]	Select the size of characters to print a sender information (default: [Minimal]). <ul style="list-style-type: none"> [Normal]: Prints the sender information in the normal text size. [Minimal]: The character height is half that of the characters in [Normal] size. It is recommended that you select [Minimal] to prevent a fax image from being cut off or to prevent a page from being divided when pages are printed at a receiving machine. If [Normal] is selected for the scanning resolution for sending a fax, it is converted into [Normal] to prevent characters from becoming corrupted and unreadable.
[Print Receiver's Name]	Select whether to print a destination fax number as the sender information (default: [ON]). If [OFF] is selected, the fax number of this machine is printed instead of the fax number of the destination. This item is not displayed in the USA and Hong Kong models.
[Footer Position]	Select the position of receiving information to be printed on the received fax (default: [OFF]). <ul style="list-style-type: none"> [Inside Body Text]: Prints the receiving information inside the original image. Part of the original image may be cut off. [Outside Body Text]: Prints the receiving information outside the original image. [OFF]: Does not print receiving information.

7.2.2 Changing Print Settings When Receiving a Fax

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

Select [Fax Settings] - [TX/RX Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Duplex Print (RX)]	When printing a multi-page fax on both sides of paper, set this option to ON (default: OFF). This item is not available if [Print Separate Fax Pages] is set to ON.
[Letter/Ledger over A4/A3]	When preferentially printing a fax on inch-size paper, set this option to ON (the default value varies depending on the area you are in).
[Print Paper Selection]	Select the criterion of selecting paper for printing a fax (default: [Auto Select]). <ul style="list-style-type: none"> [Priority Size]: Prints a fax on paper specified in [Print Paper Size]. If the machine runs out of specified paper, paper of the next closest size is used. [Fixed Size]: Always prints a fax on paper specified in [Print Paper Size]. [Auto Select]: Prints a fax on paper that is automatically selected to suit the fax received.
[Print Paper Size]	Select size of paper for printing a received fax. The initial value varies depending on the setting for [Letter/Ledger over A4/A3].

Setting	Description
[Incorrect User Box No. Entry]	Select the action taken by the machine if an unregistered User Box is specified for receiving a fax using the machine's User Box (default: [Print]). <ul style="list-style-type: none"> [Print]: Prints a received fax without saving it in a User Box. [Show Error Message]: Handles the fax as a communication error. It is neither saved nor printed. [Auto Create User Box]: Automatically creates a User Box with a specified number and stores documents in it.
[Paper Tray Setting]	Specify the paper tray to print a fax (default: [Auto]).
[Allow Paper Tray Setting]	When [Paper Tray Setting] is set to [Auto], set the tray, which allows fax printing, to ON (default: ON).
[Min. Reduction for RX Print]	Change the reduction ratio when printing a fax (default: [96%]).
[Print Separate Fax Pages]	When printing a fax longer than the standard size on separate pages, set this option to ON (default: OFF). This item is not available if [Duplex Print (RX)] is set to ON.
[File After Polling TX]	Select whether to delete a file after it is sent in response to a polling request if Polling TX is used to register files for polling (default: [Delete]).
[No. of Sets (RX)]	Change the number of copies to print a fax (default: [1] copy).
[RX Document Print Settings]	Select whether to print a received network fax in color or black and white (default: [Full Color/Black]). To restrict the print to only black and white print, select [Black Only].

7.2.3 Canceling stamp setting when sending a fax

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

Select [System Settings] - [Stamp Settings] - [Fax TX Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Cancel stamp settings when sending a fax.]	When canceling the stamp setting to send a fax, set this option to ON (default: ON).

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

Specify how to print a received fax depending on its resolution.

Select [Fax Settings] - [Fax Print Quality Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Low Resolution]	Select whether to give priority to image quality or speed by lowering the skew adjustment level when printing a received fax with a low resolution (default: [Prioritize Quality]). If [Prioritize Quality] is selected, an image is corrected.
[High Resolution]	Select whether to give priority to image quality or speed by lowering the skew adjustment level when printing a received fax with a high resolution (default: [Skew adj. level : Low]). If [Prioritize Quality] is selected, an image is corrected. Note that, for a high resolution fax, image correction is less effective relative to a low resolution fax.

7.3 Specifying useful transmission and reception functions

7.3.1 Enabling/Disabling the Fax Functions

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

Select [Fax Settings] - [Function Setting] - [Function ON/OFF Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[F-Code TX]	When using the F-Code TX function, set this option to ON (default: ON). F-Code TX is a function that send documents to a destination by entering a SUB address and a sender ID (communication password) of a specific User Box. The remote machine must support the F-Code TX/RX. Faxing is possible without specifying a sender ID (communication password). This setting is used for Confidential Communication, Relay Distribution, or PC-Fax RX.
[Relay RX]	When using the Relay RX function, set this option to ON (default: ON). If this machine is used as a relaying station, it is possible to receive a fax from a remote machine and automatically relay it to multiple programmed destinations.
[Relay Printing]	When distributing a received fax and printing it on this machine while this machine is used as a fax relaying machine, set this option to ON (default: OFF).
[Destination Check Display Function]	Configure the settings to use the destination check display function. A list of specified destinations is displayed before fax transmission. <ul style="list-style-type: none"> [Destination Check Display Function]: When using the destination check display function, set this option to ON (default: OFF). [TX Approval Password]: When prompting the user to enter the transmission approval password after a list of specified destinations was displayed, set this option to ON (default: OFF). [Password]: Enter the transmission approval password (using up to 64 characters).
[Confirm Address (TX)]	When requesting the user to enter a fax number twice to send a fax by directly entering the fax number, set this option to ON (default: OFF).
[Confirm Address (Register)]	When requesting the user to enter a fax number twice to register it when, for example, registering a destination or forwarding destination, set this option to ON (default: OFF).
[PIN Code Display Mask Function]	Configure a setting to prevent display of the PIN code in a fax report or job history when adding a personal ID (PIN code) to a fax number in order to send a fax. When masking the PIN code part, set this option to ON (default: OFF). <ul style="list-style-type: none"> [Select Separator]: Select a separator to identify the PIN code. To specify the destination, enclose the PIN code with the separators you selected in this option (default: [-]). When [PIN Code Display Mask Function] is set to ON, the following functions are not available. <ul style="list-style-type: none"> [Fax Settings] - [Function Setting] - [Incomplete TX Hold] [Fax Settings] - [Header/Footer Position] - [Print Receiver's Name]
[Reset the setting value after using other functions.]	To clear the setting value including the address when the scan/fax mode or fax mode is changed to another screen, set this option to ON (default: OFF).
[Require the use of the External Line key for outside calling.]	To prohibit the user from entering an outside line number without using the [Outside] key when directly entering the destination's fax number in PBX environment, set this option to ON (default: ON). If the directly entered number matches the outside line number specified in [PBX Connection Setting] when this option is set to ON, the system prohibits the user from entering the number following the matching number. This setting is displayed when [PBX Connection Setting] (page 7-2) is set to ON.
[Prohibit fax usage while using ext TEL line.]	When prohibiting a fax while the telephone set connected to the TEL port is in use, set this option to ON (default: ON).

7.3.2 Using the Closed Network RX function

Configure the settings for using the Closed Network RX function.

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

Select [Fax Settings] - [Function Setting] - [Closed Network RX] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Closed Network RX Password]	To use the Closed Network RX function, enter the password to restrict peers (using 4 digits). Inform the peer of the password you entered here.

7.3.3 Using the Fax Retransmit function

Configure the settings for using the Fax Retransmit function.

Fax Retransmit is a function that stores a fax that could not be sent by Redial in the machine's User Box for a given period of time. A stored fax job can be resent later by recalling it from the User Box.

Select [Fax Settings] - [Function Setting] - [Incomplete TX Hold] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Incomplete TX Hold]	When using the Incomplete TX Hold function, set this option to ON (default: OFF).
[File Storage Duration]	Specify the time period during which a fax failed to be sent is stored in the machine's User Box (default: [12] hours).

7.3.4 Using the Memory RX function

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

- 1 Select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [Memory RX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].
- 2 In [Memory RX Setting], configure the following settings.

Setting	Description
[Memory RX User Box Password]	Enter the password to restrict accesses to the Memory RX User Box (using up to 64 digits).

Tips

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

7.3.5 Using the Forward TX function

Forward TX is a function that transfers the received fax, Internet fax, IP address Fax, IP fax (SIP) to a pre-specified destination.

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

- 1** Select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [Forward TX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].
- 2** Select the fax function to set the forward fax function (only when Internet fax, IP address fax, or IP fax (SIP) is enabled).
 - To forward a fax or IP fax (SIP) received on this machine, click [Edit] of G3 Fax in [Select Fax Settings].
 - To forward an Internet fax received on this machine, click [Edit] of Internet Fax in [Select Fax Settings].
 - To forward an IP address fax received on this machine, click [Edit] of IP Address Fax in [Select Fax Settings].
- 3** In [Forward TX Setting], configure the following settings.

Setting	Description
[Forward TX Setting]	When using the Forward TX function, set this option to ON (default: OFF).
[Output Method]	Select whether to print a received fax on this machine when forwarding it (default: [Forward & Print]). <ul style="list-style-type: none"> • [Forward & Print]: A received fax is forwarded and printed on this machine. • [Forward & Print (If TX Fails)]: A received fax is printed on this machine only when forwarding has failed.
[Forward Dest.]	Specify a destination to which to forward a received fax. <ul style="list-style-type: none"> • [Select from Address Book]: Forwards a fax to a destination registered in the address book on this machine. • [Select from Group]: Forwards a fax to a group registered on this machine. • [Select from User Box No.]: Forwards a User Box registered on this machine. • [Direct Input]: Forwards a fax to the fax number you enter.
[File Format]	Select the file type to forward a fax (default: [PDF]). You can convert a fax into a file except when the forwarding destination is a fax.
[Page Setting]	Select a filing page unit when a received fax contains multiple pages (default: [Multi Page]). <ul style="list-style-type: none"> • [Multi Page]: Converts all pages to a single file. • [Page Separation]: Select this check box to convert each page to a separate file.
[E-mail Attachment]	You can select the E-mail attachment method when the forward destination is an E-mail address and [Page Setting] is set to [Page Separation] (default: [All Files Sent as one (1) E-mail]). <ul style="list-style-type: none"> • [All Files Sent as one (1) E-mail]: Attaches all files to a single E-mail. • [One (1) File per E-Mail]: Sends one E-mail for each file.

Tips

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

7.3.6 Using the PC-Fax RX Function

PC-Fax RX is a function that automatically saves a received fax to the Compulsory Memory RX User Box or the User Box specified in F-Code (SUB Address). A stored fax job can be read from the User Box into a computer.

- 1 Select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [PC-Fax RX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].
- 2 In [PC-Fax RX Setting], configure the following settings.

Setting	Description
[PC-Fax RX Setting]	Select [Allow] to use the PC-Fax RX function (default: [Restrict]).
[Receiving User Box Destination]	Select either [Memory RX User Box] or [Specified User Box] (a User Box specified in F-Code (SUB Address)) as the location to save received faxes (default: [Memory RX User Box]).
[Print]	When making prints on this machine after receiving a fax, set this option to ON (default: ON).
[Password Check]	To check the communication password (sender ID) when you select [Specified User Box] for [Receiving User Box Destination], set this option to ON (default: OFF). <ul style="list-style-type: none"> • [Communication Password]: Enter the communication password (using up to eight digits, including symbols # and *).

Tips

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

7.3.7 Using the TSI Routing function

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

- 1 Select [Fax Settings] - [Function Setting] - [RX Data Operation Settings] - [TSI User Box Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].
- 2 In [TSI User Box Settings], configure the following settings.

Setting	Description
[TSI User Box Settings]	When using the TSI User Box function, set this option to ON (default: OFF).
[Action when TSI User Box is not set.]	Select the action to be taken by the machine if a fax number (TSI) is not registered and no forwarding destination is received (default: [Automatically Print]). <ul style="list-style-type: none"> • [Automatically Print]: Prints a received fax without saving it in a User Box. • [Memory RX User Box]: Saves received documents in a Memory RX User Box. • [Specified User Box]: Saves received documents in a specified User Box. Click [Search from List], then select the User Box to save the received documents from the list. • [Specified Destination]: Forwards received documents to the specified one-touch destinations. To select the desired forwarding destinations from the address book registered on this machine, click [Search from List]. • [Specified Group]: Forwards received documents to the specified group. To select the desired forwarding destinations from the group registered on this machine, click [Search from List].
[Print]	When making prints on this machine after receiving a fax, set this option to ON (default: OFF).

- 3** Click [Register Forwarding Destination], then click [OK].
- Clicking [Set All] allows you to specify the file type to forward a received fax. The specified file type is applied to all forwarding destinations.
- [TSI User Box List] is displayed.
- 4** In the [TSI User Box List], click [Register], then configure the following settings.

Setting	Description
[Sender (TSI)]	Enter the fax number (TSI) of the sender you want to register the forwarding destination in (using up to 20 digits, including symbols #, *, +, and spaces).
[Forwarding Destination]	Specify a forwarding destination when a fax is received from the fax number entered at [Sender (TSI)]. <ul style="list-style-type: none"> [Select from Address Book]: Forwards a fax to a destination registered in the address book on this machine. [Select from Group]: Forwards a fax to a group registered on this machine. [Select from User Box No.]: Forwards a User Box registered on this machine.
[File Format]	Select the file type to forward a fax (default: [PDF]). You can convert a fax into a file except when the forwarding destination is a fax.
[Page Setting]	Select a filing page unit when a received fax contains multiple pages (default: [Multi Page]). <ul style="list-style-type: none"> [Multi Page]: Converts all pages to a single file. [Page Separation]: Select this check box to convert each page to a separate file.
[E-mail Attachment]	You can select the E-mail attachment method when the forward destination is an E-mail address and [Page Setting] is set to [Page Separation] (default: [All Files Sent as one (1) E-mail]). <ul style="list-style-type: none"> [All Files Sent as one (1) E-mail]: Attaches all files to a single E-mail. [One (1) File per E-Mail]: Sends one E-mail for each file.

Tips

- This function cannot be used together with the following functions.
Forward TX, Memory RX, PC-Fax RX
- To specify the file type when forwarding a fax using the TSI Routing function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

7.3.8 Restricting PC-FAX transmission

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

Select [Fax Settings] - [Function Setting] - [PC-FAX TX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[PC-Fax Permission Setting]	When allowing the PC-FAX TX, set this option to ON (default: ON).

7.4 Specifying fax report print conditions

Specify the conditions for printing fax-related reports.

Select [Fax Settings] - [Report Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TX Result Report]	Select when to print a report containing the results of fax transmission (default: [If TX Fails]). <ul style="list-style-type: none"> • [Always]: The report is printed every time a fax has been sent. • [If TX Fails]: The report is printed if a fax transmission has failed. • [OFF]: The report is not printed.
[Tx Result Report Print Confirmation Screen]	Select whether to display a screen that asks if you want to print a TX Result Report each time a fax is sent (default: [OFF]).
[Sequential TX Report]	When printing a report containing results of faxes sent by polling and broadcast, select [ON] (default: [ON]).
[Broadcast Result Report]	Select whether to combine results of broadcast on all destinations involved or list them for each destination (default: [All Destinations]).
[Bulletin TX Report]	When printing a report containing records of faxes registered with the bulletin for being received by polling, select [ON] (default: [ON]).
[Relay TX Result Report]	When printing a report containing results of faxes sent by relay distribution, select [ON] (default: [ON]).
[Tx Result Report Print Settings]	Select the method to output a TX result report (TX result report, broadcast result report, polling TX result report, replay TX result report, or bulletin board polling TX result report) (default: [Print]). <ul style="list-style-type: none"> • [Print]: Prints a TX result report on this machine. • [E-mail Notification]: Sends a TX result report to any destination by E-mail. E-mail settings are required in advance. If [E-mail Notification] is selected, configure the following items. <ul style="list-style-type: none"> • [Notification Address]: Enter the E-mail address of the destination (using up to 320 characters, excluding spaces). • [Notification Address Priority Setting]: Select a notification destination when User Authentication is enabled (default: [Notification Address]). Selecting [User Address] issues a notification to the E-mail address of the user who logs in to this machine and sends a fax. If the user's E-mail address is not registered, a notification is issued to the destinations registered in [Notification Address]. If [Notification Address] is selected, a notification is always issued to the destination registered in [Notification Address]. • [Report File Attachment]: Select whether to convert a TX result report to a file and attach it to an E-mail (default: [Attach]). • [Report Image Setting]: Select whether to display the first page of the sent original on a TX result report (default: [With image]). • [Report File Format]: Select the file type to attach a TX result report to an E-mail (default: [PDF]).
[Activity Report]	Select the timing to print an activity report (default: [Every 100 Comm.]). <ul style="list-style-type: none"> • [OFF]: Does not print an activity report. • [Daily]: Prints an activity report at the time specified in [Output Time Settings] every day. • [Every 100 Comm.]: Prints an activity report every 100 communications. • [100/Daily]: Prints an activity report at the time specified in [Output Time Settings] every day. In addition, a report is printed every 100 communications.
[Relay Request Report]	When printing a report when receiving a fax as a relay station, select [ON] (default: [ON]).
[PC-Fax TX Error Report]	To print a report when a PC-Fax TX job cannot be normally received from the computer using the fax driver, select [ON] (default: [OFF]).
[Timer Reservation TX Report]	When printing a report when transmission is reserved using the Timer TX function, select [ON] (default: [ON]).
[Confidential Rx Report]	When printing a report containing results of a confidential receiving fax, select [ON] (default: [ON]).

Setting	Description
[Remark Column Print Setup]	Specify whether to print user or account name in the remarks column of the activity report if user authentication or account track is enabled on this machine (default: [Normal Printing]). <ul style="list-style-type: none"> • [Normal Printing]: The line status or sending setting will be printed. • [User Name Printing]: The user name for user authentication will be printed. • [Account Name Printing]: The account name for user authentication will be printed.
[Network Fax RX Error Report]	To print a report when the machine has failed to receive an Internet fax or IP address fax, select [ON] (default: [ON]).
[Print Job Number]	Select [ON] to display a job number on a report to be printed (default: [OFF]). The following reports are targeted for this processing. <ul style="list-style-type: none"> • Activity Report • TX Report • RX Report • TX Result Report • Broadcast Result Report
[MDN Message]	When printing a report notifying that an Internet fax has been sent to the recipient machine, select [ON] (default: [ON]).
[DSN Message]	When printing a report notifying that an Internet fax has been sent to the mail server of the recipient machine, select [ON] (default: [OFF]).
[Print E-mail Message Body]	Select whether to print a report notifying that an Internet fax has been successfully received after it was received (default: [Print]). The report has the subject and message body of an Internet fax.
[Legend display Settings]	Select [ON] to display an explanatory note on a report to be printed (default: [ON]). If an explanatory note is omitted, the image of the sent original can be displayed on a larger area.

7.5 Restricting Deletions of Received Faxes

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

Two methods are available to restrict deletions.

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

Select [Fax Settings] - [Function Setting] - [RX Data Deletion Restriction Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[RX Data Deletion Restriction Settings]	When restricting deletion of the received fax, set this option to ON (default: OFF).
[Password Deletion]	To restrict deletion of received faxes with a password, enter the password (using up to eight digits).
[Administrator User Box Deletion]	Makes a restriction to delete received faxes only when a user logs in with User Box administrator or administrator privileges. [Administrator User Box Deletion] is displayed when User Authentication or Account Track is enabled and User Box Administrator is specified.

7.6 Registering the number to prohibit its entry

Register the numbers of which the entry is prohibited as a fax sending destination. When the specified fax number matches the number registered here at the time of fax sending or address registration, its entry is prohibited.

Select [Store Address] - [Register address input prohibition rule.] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[No.]	Displays the automatically assigned number at the time of registration.
[Rule name]	Enter the rule name.
[Fax number (Match previous number)]	Enter the number to prohibit its entry. The number is judged by prefix match.
[Apply setting]	When applying the rule to prohibit the entry, set this option to ON (default: OFF).



Configuring the Network Fax Environment

8 Configuring the Network Fax Environment

8.1 Configuring the Internet fax environment

Setting flow

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

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

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

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

- ✓ To use the Internet Fax function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- ✓ To use the Internet Fax function, ask your service representative to configure settings. For details, contact your service representative.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configure basic settings for sending and receiving an Internet fax (page 8-2)
- 3 Configuring settings to suit your environment
 - Checking a fax reception (page 8-4)
 - Specifying the reception ability of this machine (page 8-4)
 - Specifying the default compression type for transmission in black and white (page 8-5)
 - Configuring default compression type setting for transmission in color (page 8-5)
 - Establishing SSL/TLS communication (page 5-4)
 - Using SMTP authentication (page 5-4)
 - Using POP before SMTP authentication (page 5-5)

Tips

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

Configure basic settings for sending and receiving an Internet fax

Configure the settings to use the Internet fax function.

- 1 Select [Network] - [Network Fax Setting] - [Network Fax Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[I-Fax Function Setting]	When using Internet Fax, set this option to ON (default: OFF).

- 2** Select [System Settings] - [Machine Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Input Machine Address]	Register the device name and E-mail address of this machine. <ul style="list-style-type: none"> [Device Name]: Enter the name of this machine (using up to 80 characters). The file name automatically assigned in scanning and sending incorporates the name specified for [Device Name]. [E-mail Address]: Enter the E-mail address of this machine (using up to 320 characters, excluding spaces). To use the Internet fax function or E-mail RX print function, it settings are required.

- 3** Select [Fax Settings] - [Header Information] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Default]	Select the default setting for the sender name. The sender name, which is specified by default, is automatically added when a fax is sent.
[Sender Name]	Displays registered sender names.
[Edit]	You can register up to 20 sender names. Use this option to use different sender names depending on the destination. <ul style="list-style-type: none"> [No.]: Displays the registration number. [Sender Name]: Enter the sender name (using up to 30 characters).
[Delete]	Deletes the registered sender name.

- 4** Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail TX Setting]	When sending E-mails from this machine, set this option to ON (default: ON).
[E-Mail Send]	When using Internet Fax, set this option to ON (default: ON).
[SMTP Server Address]	Enter the address of the E-mail server (SMTP). Use one of the following formats. <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the port number of the E-mail server (SMTP) (default: [25]).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (SMTP) (default: [60] sec.).
[Server load reduction transmission method]	Select the sending method to reduce the load of the E-mail server (SMTP) (default: [OFF]). <ul style="list-style-type: none"> [Binary Division]: Divides an E-mail with the specified size. [Binary division Size]: Enter the size to divide an E-mail. [Stop Scan TX when maximum limit is exceeded]: Stops sending an E-mail when its size exceeds the specified maximum value. When specifying the maximum value, select [Limit] in [Max Mail Size], then enter the maximum E-mail size allowable for the E-mail server (SMTP) in [Server Capacity limit]. [Scan TX by Download URL method only when maximum limit is exceeded]: Notifies the E-mail address specified as the destination of the download URL without attaching files when the E-mail size exceeds the specified maximum value. When specifying the maximum value, select [Limit] in [Max Mail Size], then enter the maximum E-mail size allowable for the E-mail server (SMTP) in [Server Capacity limit]. [Always Scan TX by Download URL method]: Notifies the E-mail address specified as the destination of the download URL without attaching files.

- 5** Select [Network] - [E-mail Setting] - [E-mail RX (POP)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[E-mail RX Setting]	When receiving E-mails on this machine, set this option to ON (default: ON).
[POP Server Address]	Enter the address of your E-mail server (POP). Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Login Name]	Enter the login name used for POP authentication (using up to 63 characters).
[Password]	Enter the password for POP authentication (using up to 15 characters).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (POP) (default: [30] sec.).
[Port No.]	If necessary, change the port number of the E-mail server (POP) (default: [110]).
[Check for New Messages]	When periodically connecting to the E-mail server (POP) to check whether E-mails arrive or not, set this option to ON (default: ON). <ul style="list-style-type: none"> • [Polling Interval]: Specify an interval to check whether E-mails arrive or not (default: [15] min.).

Checking a fax reception

Configure settings for Internet fax reception confirmation (MDN/DSN).

Select [Fax Settings] - [Network Fax Setting] - [I-Fax Advanced Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[MDN Request]	When requesting the sender to confirm a fax reception (MDN Request), set this option to ON (default: ON). 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.
[DSN Request]	When requesting the destination E-mail server to check a fax arrival (DSN request), set this option to ON (default: OFF). When [MDN Request] is set to ON, priority is given to the MDN request.
[MDN Response]	To return a response message when the machine receives an MDN request, set this option to ON (default: ON).
[MDN/DSN Response Monitoring Setting]	To specify the waiting time for a response from the destination after a MDN request or DSN request is sent by this machine, set this option to ON. <ul style="list-style-type: none"> • [Monitoring Time]: Change the waiting time for a response from the destination (default: [24] Time). If a response message is received after the specified wait period has elapsed, the machine ignores the message.
[Maximum Resolution]	If necessary, switch the maximum resolution that this machine can support (default: [Ultra Fine]).
[Add Content-Type Information]	To add Content-Type information to an Internet fax when sending it, set this option to ON (default: OFF). If ON is selected, "application=faxbw" is added to the Content-Type header of MIME as a sub type.

Specifying the reception ability of this machine

Specify the Internet fax receiving ability of this machine. The peer is notified of the specified receiving ability by a response to an MDN request received on this machine.

Select [Fax Settings] - [Network Fax Setting] - [Internet Fax RX Ability] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

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

Specifying the default compression type for transmission in black and white

Change the default compression type to send image data in black and white.

Select [Fax Settings] - [Network Fax Setting] - [Black Compression Level] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Black Compression Level]	Change the default compression type to send image data in black and white (default: [MMR]). <ul style="list-style-type: none"> • [MMR]: The data size is the smallest. • [MR]: The data size is intermediate between [MH] and [MMR]. • [MH]: The data size is larger than [MMR].

Configuring default compression type setting for transmission in color

Change the default compression type to send image data in full color or gray scale.

Select [Fax Settings] - [Network Fax Setting] - [Color/Grayscale Multi-Value Compression Method] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Color/Grayscale Multi-Value Compression Method]	Change the default compression type to send image data in full color or gray scale (default: [JPEG (Color)]). <ul style="list-style-type: none"> • [JPEG (Color)]: Compresses image data in color JPEG format. • [JPEG (Gray Scale)]: Compresses image data in black and white JPEG format. • [Unset]: Compress data according to the compression type specified in [Black Compression Level]. You cannot send data in color or gray scale. Whichever file format you specify, data is converted to the TIFF format.

8.2 Configuring the IP address fax environment

Setting flow

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

The SMTP protocol is used to send and receive IP address faxes. Communications are established using the E-mail server (SMTP) function of this machine; therefore, no server is required to specify the destination's IP address for communications.

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

- ✓ To use the IP Address Fax function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- ✓ To use the IP Address Fax function, ask your service representative to configure settings. For details, contact your service representative.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configure basic settings for sending and receiving faxes using IP address fax (page 8-6)
- 3 Configuring settings to suit your environment
 - Specifying the default compression type for transmission in black and white (page 8-5)
 - Configuring default compression type setting for transmission in color (page 8-5)

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

Configure the settings for using the IP Address Fax function.

- 1 Select [Network] - [Network Fax Setting] - [Network Fax Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IP Address Fax Function Settings]	When using the IP address fax function, set this option to ON (default: OFF).

- 2 Select [Network] - [Network Fax Setting] - [SMTP TX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Port No.]	If necessary, change the port number of the E-mail server (SMTP) (default: [25]).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (SMTP) (default: [60] sec.).

- 3 Select [Network] - [Network Fax Setting] - [SMTP RX Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMTP RX]	When using the SMTP reception function, set this option to ON (default: OFF).
[Port No.]	If necessary, change the port number of the E-mail server (SMTP) (default: [25]).
[Connection Timeout]	If necessary, change the time-out time to limit a communication with the E-mail server (SMTP) (default: [300] sec.).

- 4** Select [Fax Settings] - [Header Information] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Default]	Select the default setting for the sender name. The sender name, which is specified by default, is automatically added when a fax is sent.
[Sender Name]	Displays registered sender names.
[Edit]	You can register up to 20 sender names. Use this option to use different sender names depending on the destination. <ul style="list-style-type: none"> [No.]: Displays the registration number. [Sender Name]: Enter the sender name (using up to 30 characters).
[Delete]	Deletes the registered sender name.

- 5** Select [Fax Settings] - [Network Fax Setting] - [IP Address Fax Operation Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Operating Mode]	Select an operation mode of IP address fax according to your environment (default: [Mode 1]). <ul style="list-style-type: none"> [Mode 1]: This mode allows communications between our models that support IP address fax communications and between models that comply with the Direct SMTP standard. However, because a unique method developed by our company is used to send a color fax, only our company's models can receive such a color fax. [Mode 2]: This mode allows communications between our models that support IP address fax communications and between models that comply with the Direct SMTP standard. The method compatible with the Direct SMTP standard (Profile-C format) is used to send a color fax.
[Sending Colored Documents]	Select whether or not to accept sending of color faxes when selecting [Mode 2] for [Operating Mode] (default: [Allow]). To send a fax to a machine that does not support color reception based on the Direct SMTP standard, select [Restrict].

8.3 Configuring the IP fax (SIP) operating environment

Setting flow

IP fax (SIP) is a function that enables the real-time sending/receiving via the intranet and Internet. It is possible to send and receive with less delay compared to Internet fax that spools jobs in the mail server. Also, this function provides a lower communication costs than a fax using a telephone line.

IP fax (SIP) uses the SIP server to call a destination. The SIP server centrally manages the association between the identifiers (SIP-URI) and IP addresses of SIP-compatible devices, and intermediates the establishment of a connection between devices.

- ✓ To use the IP fax (SIP) function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- ✓ To use the IP fax (SIP) function, ask your service representative to configure settings. For details, contact your service representative.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring the basic settings for IP fax (SIP) sending and receiving (page 8-8)
- 3 Configuring settings to suit your environment
 - Configuring the setting to connect to the SIP server (page 8-9)
 - Configuring the setting to automatically acquire SIP configuration information (IPv4) (page 8-9)
 - Configuring the setting to automatically acquire SIP configuration information (IPv6) (page 8-9)

Configuring the basic settings for IP fax (SIP) sending and receiving

- 1 Select [Network] - [Network Fax Setting] - [Network Fax Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IP-FAX(T38) Function Setting]	When using the IP fax (SIP) function, set this option to ON (default: OFF).

- 2 Select [Network] - [Network Fax Setting] - [IP-FAX(T38) Detail Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Port Number]	Enter the port number depending on the number of lines used (default: [10000] to [10003]). Specify the port numbers by the number of available lines.
[Timeout]	Change the communication timeout period as needed (default: [60] sec.).

- 3 Select [Network] - [SIP setting] - [SIP Basic Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SIP setting]	When [IP-FAX(T38) Function Setting] is set to ON in step 1, this option is set to ON synchronously.
[User ID]	Enter the SIP user ID of this machine.
[Domain Name]	Enter the name of the SIP domain which this machine joins.
[Transport Mode]	Select the transport protocol (default: [UDP]).
[Port Number]	If necessary, change the port number (default: [5060]).
[Keep-alive interval value]	Enter the session update interval (default: [1800]).
[Request retransmission interval value]	Enter the packet resending interval (default: [500]).

Configuring the setting to connect to the SIP server

Configure the setting to connect to the SIP server.

Select [Network] - [SIP setting] - [SIP Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Priority proxy setting]	Configure the setting to connect to the priority SIP proxy server. <ul style="list-style-type: none"> • [Destination type]: Enter the server address. • [Port Number]: If necessary, change the port number (default: [5060]). • [User Name]: Enter the user name used to log in to the server. • [Password]: Enter the password used to log in to the server.
[Alternate proxy setting]	Configure the setting to connect to the alternate SIP proxy server. <ul style="list-style-type: none"> • [Destination type]: Enter the server address. • [Port Number]: If necessary, change the port number (default: [5060]). • [User Name]: Enter the user name used to log in to the server. • [Password]: Enter the password used to log in to the server.
[Register Setting]	Configure the setting to connect to the SIP registrar server. <ul style="list-style-type: none"> • [Destination type]: Enter the server address. • [Port Number]: If necessary, change the port number (default: [5060]). • [User Name]: Enter the user name used to log in to the server. • [Password]: Enter the password used to log in to the server.
[SIP Server connection check]	Check whether the server connection is possible with the current setting.

Configuring the setting to automatically acquire SIP configuration information (IPv4)

Configure the setting to automatically acquire SIP configuration information using DHCP in IPv4 environment.

Select [Network] - [SIP setting] - [SIP Automatic Retrieval Settings(IPv4)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Auto acquisition of proxy address]	When automatically acquiring the address of the SIP proxy server, set this option to ON (default: ON).
[Domain Name Auto Retrieval]	When automatically acquiring the SIP domain name, set this option to ON (default: ON).

Configuring the setting to automatically acquire SIP configuration information (IPv6)

Configure the setting to automatically acquire SIP configuration information using DHCP in IPv6 environment.

Select [Network] - [SIP setting] - [SIP Automatic Retrieval Settings(IPv6)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Auto acquisition of proxy address]	When automatically acquiring the address of the SIP proxy server, set this option to ON (default: ON).
[Domain Name Auto Retrieval]	When automatically acquiring the SIP domain name, set this option to ON (default: ON).



Configuring the User Box Environment

9 Configuring the User Box Environment

9.1 Registering and editing a User Box

9.1.1 Registering and editing a User Box

Register a Public, Personal, or Group User Box.

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

Select [Box] - [User Box List] - [New Registration] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine), and configure the following settings.

Setting	Description
[User Box Number]	Registration number of the User Box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters).
[Assign User Box Password]	To restrict usage of the User Box with the password, set this setting on. <ul style="list-style-type: none"> • [User Box Password]: Enter the User Box password (using up to 64 characters, excluding double quotation marks ").
[Index]	Select an index using the registered name.
[Type]	When user authentication or account track is enabled, select the User Box type. If [Personal] is selected, specify the owner user. If [Group] is selected, specify the owner account.
[Auto Delete Document]	Specify the period from the date/time when a file was saved in a User Box; the date/time when a file was last printed; or the date/time when a file was sent from a User Box, to the date/time when a file is to be deleted automatically. <ul style="list-style-type: none"> • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[User Box Expansion Function]	Configure the User Box expansion function as needed.
[Confidential RX]	Set to ON when adding the confidential RX function to the User Box (default: OFF). <ul style="list-style-type: none"> • [Communication Password]: Enter the password for confidential RX (using up to eight characters). The password entered here is required to send a fax to this machine using Confidential TX. Inform the sender of the password you entered here.
[Auto Save Document to MFP Shared Folder]	Set to ON when using the Auto Save Document to MFP Shared Folder function (default: OFF). In [SMB Communication Encryption], select whether to encrypt SMB communications with a client device. To use the encryption function, the password must be specified for the User Box. Enabling the encryption function permits only accesses from client devices of SMB 3.0 or later. This setting is available when the following conditions are satisfied. <ul style="list-style-type: none"> • [Type] is set to [Public]. • [Confidential RX] is set to OFF. • [SMB Server Settings] and [Share SMB File Setting] are set to ON in [SMB Server Settings] (page 9-8).
[Web Connection Download Settings]	Select whether to download a file in a User Box at high speed (default: [Normal Download]). The following types of documents are not targeted for this setting. <ul style="list-style-type: none"> • Document stored in a User Box by the print function of the computer • Document stored from USB memory to User Box • Document stored in a User Box using the F code function


Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- To edit or delete a registered User Box, specify the target one in the User Box list, and select [Edit] or [Delete].

9.1.2 Registering and editing a Bulletin Board User Box

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

If announcement and other fax documents are stored in Bulletin Board User Boxes on purpose and if recipients are notified of the related User Box numbers, the users can select the required fax documents and they can be polled.

Select [Box] - [System User Box List] - [New Registration] - [Bulletin Board User Box] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine), and configure the following settings.

Setting	Description
[User Box Number]	Registration number of the User Box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters).
[Assign User Box Password]	To restrict usage of the User Box with the password, set this setting on. <ul style="list-style-type: none"> • [User Box Password]: Enter the User Box password (using up to 64 characters, excluding double quotation marks ").
[Type]	When user authentication or account track is enabled, select the User Box type. If [Personal] is selected, specify the owner user. If [Group] is selected, specify the owner account.
[Auto Delete Document]	Specify the period from the date/time when a file was saved in a User Box; the date/time when a file was last printed; or the date/time when a file was sent from a User Box, to the date/time when a file is to be deleted automatically. <ul style="list-style-type: none"> • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.


Tips

- To edit or delete a registered User Box, specify the target one in the User Box list, and select [Edit] or [Delete].

9.1.3 Registering and editing a Relay User Box

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

When you send a fax to the relay machine using the relay distribution function, the relay machine sends the received fax to all recipients pre-registered in the Relay User Box.

Using the Relay User Box, you can reduce the total communication cost via the relay machine, for example, when you want to broadcast to distant places.

Select [Box] - [System User Box List] - [New Registration] - [Relay User Box] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine), and configure the following settings.

Setting	Description
[User Box Number]	Registration number of the User Box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters).

Setting	Description
[Relay Address]	Select [Search from List], and select a group destination in which fax destinations are registered. Fax addresses must be included in the group destination to be registered as a relay destination.
[Relay TX Password]	Enter the relay password (using up to eight characters, including symbols # and *). The entered password is required when you issue a relay request to this machine. Inform the sender of the password you entered here.


Tips

- To edit or delete a registered User Box, specify the target one in the User Box list, and select [Edit] or [Delete].

9.1.4 Registering and editing an Annotation User Box

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

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

Select [Box] - [System User Box List] - [New Registration] - [Annotation User Box] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Box Number]	Registration number of the User Box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters).
[Assign User Box Password]	To restrict usage of the User Box with the password, set this setting on. <ul style="list-style-type: none"> • [User Box Password]: Enter the User Box password (using up to 64 characters, excluding double quotation marks ").
[Auto Delete Document]	Specify the period from the date/time when a file was saved in a User Box; the date/time when a file was last printed; or the date/time when a file was sent from a User Box, to the date/time when a file is to be deleted automatically. <ul style="list-style-type: none"> • [Do Not Delete]: Keeps the file in the User Box. • [Do Not Keep]: Select this option to use a document to give an annotation only without saving or using it for copying. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[Count Up]	Select the unit for adding a number to a file from By Job and By Page. <ul style="list-style-type: none"> • [By Job]: Adds a number for each file. Even if a file has multiple pages, a same number is added to the file as one job. • [By Page]: Adds a number for each page.
[Stamp Elements]	Specify the fixed text, date and time, and print position to be added to a file. <ul style="list-style-type: none"> • [Primary Field]: Add any text (using up to 40 characters). • [Secondary Field]: Add any text at the beginning of the annotation (using up to 20 characters). • [Date/Time Setting]: Select the format for the date and time. • [Print Position]: Select a position to print the annotation at. • [Density]: Select the density of characters of the date and time and annotation to be printed. • [Number Type]: Select the digit number of annotation.


Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

- To edit or delete a registered User Box, specify the target one in the User Box list, and select [Edit] or [Delete].

9.2 Managing User Boxes

9.2.1 Managing User Boxes

Specifying the maximum number of User Boxes

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

Select [User Auth/Account Track] - [Public User Box Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Set the maximum number of User Boxes]	<p>When specifying the maximum number of User Boxes, set this option to ON (default: OFF).</p> <ul style="list-style-type: none"> [Maximum Number of User Boxes]: Enter the maximum number of Public User Boxes that can be registered in this machine by the user (unit: User Box).

Deleting all empty User Boxes

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

Select [System Settings] - [User Box Setting] - [Delete Unused User Box] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [OK].

Disabling the user to register or edit a User Box

You can enable or disable each user's ability to create, edit, and delete a User Box.

Select [System Settings] - [User Box Setting] - [User Box Operation] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Allow/Restrict User Box]	When permitting the user to register, edit, and delete a User Box, set this option to ON (default: ON).

9.2.2 Managing files in a User Box

Automatically deleting files from a User Box

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

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

Select [System Settings] - [User Box Setting] - [Document Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Delete Setting]	<p>Select whether the administrator collectively specifies the file deletion times for all the User Boxes (default: [Set by User.]).</p> <p>If [Set by Administrator.] is selected, the user cannot specify the file deletion time for each User Box when creating a User Box.</p>
[Delete Time Setting]	<p>Specify the time required to automatically delete files from a User Box (default: [1] day).</p> <ul style="list-style-type: none"> [Do Not Delete]: Keeps the file in the User Box. [Specify days]: Select the number of days until the file is automatically deleted. [Specify Time]: Enter the time period before the file is automatically deleted.

Holding files in a User Box

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

Select [System Settings] - [User Box Setting] - [Document Hold Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Automatic deletion when retrieving documents.]	When holding a file in a User Box after printing or sending a file in a User Box, set this option to ON (default: ON).
[Delete confirmation screen.]	When displaying the deletion confirmation screen after printing or sending a file in a User Box, set this option to ON (default: OFF). You can prompt the user to select whether to hold a file in a User Box.

Automatically deleting files saved in a User Box using the Scan to URL function

Specify the period from the date and time when files are saved in a User Box on this machine to the time when they are deleted automatically using the Scan to URL function.

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

Select [System Settings] - [URL Document Management Setting] - [URL Document Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Delete Time Setting]	Specify the time required to automatically delete files from a User Box (default: [3] days). <ul style="list-style-type: none"> [Specify days]: Select the number of days until the file is automatically deleted. [Specify Time]: Enter the time period before the file is automatically deleted.

Deleting all files saved in a User Box using the Scan to URL function

Delete all files saved in a User Box on this machine using the Scan to URL function.

Select [System Settings] - [URL Document Management Setting] - [URL Delete Document] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [OK].

9.2.3 Sharing files in a User Box via SMB

Setting flow

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

If files are saved in the Public User Box, they are also saved in the corresponding SMB folder automatically. The files saved in the SMB folder via the Public User Box can be extracted easily by accessing the SMB folder on the network from a computer.

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

- 1** Configuring the SMB server (page 9-8)
- 2** Creating a Public User Box to share files (page 9-8)
- 3** Configuring settings to suit your environment
 - Automatically deleting files from the SMB folder (page 9-9)
 - Deleting all files from the SMB folder (page 9-9)

Configuring the SMB server

Configure settings to use the SMB server.

Select [Network] - [SMB Setting] - [SMB Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SMB Server Settings]	When using this machine as the SMB server, set this option to ON (default: OFF).
[SMB Server Common Settings]	<p>Configure common settings to use the machine as an SMB server.</p> <ul style="list-style-type: none"> • [SMB Host Name]: Enter the host name of this machine (using up to 15 characters). • [Workgroup]: Enter the name of the workgroup that contains this machine (using up to 15 characters, excluding ", \, ;, :, *, <, >, , +, =, and ?). • [SMB Authentication Protocol]: Select the SMB authentication protocol to be used in the machine (default: [SMB1.0/SMB2.0/SMB3.0]). • [SMB security Signature Setting]: Select whether to enable the SMB signature of this machine to suit your environment (default: [Only When Requested]). [Disable]: Disables the SMB signature of this machine. [Only When Requested]: Enables the SMB signature of this machine (server) only when the SMB signature is requested from the client side. If the SMB signature is not requested from the client side, operations are performed while the SMB signature of this machine (server) remains disabled, and a connection is possible even when the SMB signature in the client side is disabled. [Required]: Enables the SMB signature of this machine. To establish a connection, the SMB signature is also required in the client side. If the SMB signature in the client side is disabled, it will not be possible to make a connection.
[Share SMB File Setting]	When using the SMB file sharing function, set this option to ON (default: OFF).

Creating a Public User Box to share files

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

Select [Box] - [User Box List] - [New Registration] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine), and configure the following settings.

Setting	Description
[User Box Number]	Registration number of the User Box. Select [Use opening number] to automatically assign the smallest available number. When specifying a number, select [Input directly], and enter a value between 1 and 999999999.
[User Box Name]	Enter the User Box name (using up to 20 characters).
[Assign User Box Password]	To restrict usage of the User Box with the password, set this setting on. <ul style="list-style-type: none"> • [User Box Password]: Enter the User Box password (using up to 64 characters, excluding double quotation marks ").
[Index]	Select an index using the registered name.
[Type]	Select [Public] to use the Share SMB File function.
[Auto Delete Document]	<p>Specify the period from the date/time when a file was saved in a User Box; the date/time when a file was last printed; or the date/time when a file was sent from a User Box, to the date/time when a file is to be deleted automatically.</p> <ul style="list-style-type: none"> • [Do Not Delete]: Keeps the file in the User Box. • [Specify days]: Select the number of days until the file is automatically deleted. • [Specify Time]: Enter the time period before the file is automatically deleted.
[User Box Expansion Function]	Configure the User Box expansion function as needed.

Setting	Description
[Auto Save Document to MFP Shared Folder]	Set to ON when using the Auto Save Document to MFP Shared Folder function (default: OFF). In [SMB Communication Encryption], select whether to encrypt SMB communications with a client device. To use the encryption function, the password must be specified for the User Box. Enabling the encryption function permits only accesses from client devices of SMB 3.0 or later.


Tips

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

Automatically deleting files from the SMB folder

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

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

Select [System Settings] - [User Box Setting] - [Document in MFP Shared Folder Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Document in MFP Shared Folder Delete Time Setting]	When collectively specifying the file deletion time to be applied to all the SMB folders, set this option to ON (default: ON).
[Document in MFP Shared Folder Delete Time]	Specify the time required to automatically delete files from the SMB folder (default: [1] day).

Deleting all files from the SMB folder

Delete all the files saved in the SMB folder.

Select [System Settings] - [User Box Setting] - [Delete all in SMB folder] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [OK].

9.2.4 Managing files in a Secure Print User Box

Deleting all secure documents

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

Select [System Settings] - [User Box Setting] - [Delete Secure Print File] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [OK].

Automatically deleting all secure documents

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

Select [System Settings] - [User Box Setting] - [Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Auto Delete Secure Document]	<p>When automatically deleting files saved in the Secure Print User Box, set this option to ON (default: ON). Also, specify the time required to automatically delete such a file (default: [1] day).</p> <ul style="list-style-type: none"> [Specify days]: Select the number of days until the file is automatically deleted. [Specify Time]: Enter the time period before the file is automatically deleted.

Specifying the simple print function for secure document

Configure settings to use the simple print function for secure document.

Select [System Settings] - [User Box Setting] - [Security Document Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Security Document Setting]	<p>Select whether to enable simple printing for secure document (default: [Do Not Release Secure Print]).</p> <p>If you select [Release Secure Print], the computer login name is used as the document ID for Secure Print, so you can skip the entry of the document ID. Also, when making prints on the machine, the user can display a list of document IDs on the screen of this machine and easily specify the target document ID.</p>

9.2.5 Managing files in a ID & Print User Box

Automatically deleting all ID & Print documents

Specify the time to automatically delete documents in the ID & Print User Box, from the date/time the document was saved or the date/time they were last printed.

Select [System Settings] - [User Box Setting] - [Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[ID & Print Delete Time]	<p>When automatically deleting files saved in the ID & Print User Box, set this option to ON (default: ON). Also, specify the time required to automatically delete such a file (default: [1] day).</p> <ul style="list-style-type: none"> [Specify days]: Select the number of days until the file is automatically deleted. [Specify Time]: Enter the time period before the file is automatically deleted.

Specifying processing after printing ID & Print documents

Specify processing to be performed after ID & Print documents were printed.

Select [System Settings] - [User Box Setting] - [ID & Print Delete Time] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Delete after Print]	<p>Select whether to ask the user if they want to delete the file from the ID & Print User Box after it is printed, or to always delete the file after it is printed without requesting confirmation (default: [Confirm with User]).</p>

9.2.6 Managing files in a Password Encrypted PDF User Box

Automatically deleting a Password Encrypted PDF file

Specify the period from the date/time when a file was saved in a Password Encrypted PDF User Box or last printed to the date/time when it is to be deleted automatically.

Select [System Settings] - [User Box Setting] - [Delete Time Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Encrypted PDF Delete Time Setting]	<p>When automatically deleting files saved in the Password Encrypted PDF User Box, set this option to ON (default: ON). Also, specify the time required to automatically delete such a file (default: [1] day).</p> <ul style="list-style-type: none"> [Specify days]: Select the number of days until the file is automatically deleted. [Specify Time]: Enter the time period before the file is automatically deleted.

9.2.7 Backing up files in a User Box

Specify the User Box to be backed up.

Select [Maintenance] - [User Box Document Backup] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Box Document Backup]	Set the backup User Box to ON (default: OFF).

9.3 Configuring the USB Memory Device settings

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

Select [System Settings] - [User Box Setting] - [USB flash drive function settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Save Document]	When permitting the user to save a file in a USB flash drive, set this option to ON (default: OFF).
[Print Document]	When permitting the user to print a file from a USB flash drive, set this option to ON (default: ON).
[USB to User Box]	When permitting the user to save a file read from a USB flash drive in a User Box, set this option to ON (default: OFF).

Tips

- When user authentication is enabled, select [User Registration] (page 10-20) and configure settings to use a USB flash drive for each registered user.

10

Restricting Users from Using this Device

10 Restricting Users from Using this Device

10.1 Overview of User Authentication and Account Track

About user authentication

Employing User Authentication enables you to manage users who can use this machine. It also enables security- and cost-conscious advanced operations of this machine. By employing User Authentication, you can use the following functions to users of this machine.



Function	Description
Identification	This function allows you to restrict users of this machine by identifying them.
Allow	<p>You can set privileges to restrict usage of the functions of this machine by user.</p> <ul style="list-style-type: none"> For example, you can configure settings to make printing available for a specific user but not for other users. Also, you can configure settings to restrict printing by users who are not identified by this machine (public users). You can also limit access to destinations for each user. Based on the degree of importance of the address and relationship with users, you can set it up so that specific users can access all destinations but other users can only access some of the destinations. <p>Configuring settings according to the business requirements of users provides you with added security measures and reduced costs simultaneously.</p>
Accounting	<p>You can record the usage status of this machine by user. Analyzing it by user enables this machine to be operated more efficiently. For example, depending on the usage status of this machine, you can manage the maximum number of sheets each user can print. This encourages users to develop an awareness of costs, contributing to cost reductions.</p>

The user authentication methods are classified into three types: MFP authentication, external server authentication, and MFP authentication + External Server Authentication.

Authentication Method	Description
MFP authentication	<p>The method to manage users of this machine using the authentication function of this machine.</p> <p>Since user information is managed inside this machine, you can use it simply by registering it.</p> <p>For details, refer to page 10-5.</p>
External server authentication	<p>The method to manage users of this machine by synchronizing it with Active Directory or LDAP server.</p> <p>When Active Directory or LDAP server is used for user management in your environment, you can use user information managed using the server.</p> <p>This machine supports the following server types.</p> <ul style="list-style-type: none"> Active Directory: For details, refer to page 10-8. NTLM: For details, refer to page 10-12. LDAP: For details, refer to page 10-13.

Authentication Method	Description
MFP authentication + External server authentication	The method comprising a combination of the authentication function of this machine and authentication by an external server. Even if some sort of problem occurs on the external authentication server, you can use this machine by using its authentication function.

Tips

- You can also manage users of this machine by associating with the enhanced server. To associate with the enhanced server, "Enhanced Server Authentication" and "ON (MFP) + ON (Enhanced Server)" are supported in addition to the above authentication method.

About account track

Employing the Account Track function enables you to manage multiple users by account. Account authentication information is managed internally by this machine.

A password can be set by account to restrict users from using this machine. Also, this function allows you to restrict available functions or manage the usage status of this machine by account.

For details on how to configure account track settings, refer to page 10-6.



Combining user authentication and account track

You can use a combination of user authentication and account track to manage each user for each department. To combine user authentication and account track, specify whether to synchronize account information with users according to your environment.

Relationship between users and accounts	Description
When the user and account is in one-to-one relation	By synchronizing account information with a user, you can associate the user with an account on a one-to-one basis. For example, you can allow a company staff member belonging to a certain department to print but not allow another member belonging to another department to print. Also, you can count the number of printed sheets by department to encourage each department to develop an awareness of costs. If you specify the department of a user when registering him/her, you can log in to the account simply by logging in as the user.
When a user joins multiple accounts	To manage the usage status not only by actual department but also by project, do not synchronize the user with an account. For example, for a project across multiple departments, you can analyze the usage status of this machine by project as well as by company staff member or department. To log in to this machine, enter the user name, then specify the account.

 **Tips**

When switching between synchronization and non-synchronization of user authentication and account authentication depending on the business status, configure the following settings to allow each user to select whether to perform synchronization.

- Select [User Auth/Account Track] - [Authentication Type], then set [Synchronize User Authentication / Account Track] to [Synchronize by User].
- Select [Security] - [Restrict User Access], then set [Synchronize User Authentication / Account Track By User] to ON.

10.2 Installing User Authentication/Account Track

10.2.1 MFP authentication setting

Setting flow

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 usage status of this machine.

When employing the MFP authentication, follow the below procedure to configure the settings.

- 1** Configuring basic settings for the user authentication (page 10-5)
- 2** Configuring settings to suit your environment
 - Configuring a setting so that a user can log in to this machine using administrator privileges (page 10-17)
 - Restricting available functions for each user (page 10-20)
 - Restricting the accessible destinations (page 10-22)
 - Managing the maximum number of copies by user (page 10-25)

Configure basic settings for the user authentication

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

- 1** Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Authentication]	Select [ON (MFP)] to employ the MFP authentication.
[Public User Access]	Select whether to allow use of an unregistered user (public user) (default: [Restrict]). <ul style="list-style-type: none"> • [Restrict]: Restricts a use of a public user. • [ON (With Login)]: Allows that public users to use this machine. When a public user uses this machine, select [Used by public user] on the Login screen. • [ON (Without Login)]: Allows that public users to use this machine. 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.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed (default: [Skip Job]). <ul style="list-style-type: none"> • [Skip Job]: Stops the job currently running, and starts printing the next job. • [Stop Job]: Stops all jobs. • [Delete Job]: Deletes the active job.

- 2** Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [New Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[No.]	Specify the user's registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.

Setting	Description
[User Name]	Enter the user name (using up to 64 characters). You cannot configure the same user name as an the one that has already been assigned to a registered user. Once a user name is registered, it cannot be changed.
[E-mail Address]	Enter the user's E-mail address (using up to 320 characters, excluding spaces). If the E-mail address is registered, the Scan to Me function and the Scan to URL function are available.
[User Password]	Enter the password to log in to this machine (using up to 64 characters).
[Function Permission]	Restricts functions available to the user if necessary. For details, refer to page 10-20.
[Max. Allowance Set]	Sets the maximum number of sheets the user can print and User Boxes they can register. For details, refer to page 10-25.
[Limiting Access to Destinations]	Restricts destinations the user can access if necessary. For details, refer to page 10-22.
[Permission Setting]	Assigns administrator privileges or User Box administrator privileges to a user as required. For details, refer to page 10-17.

Tips

- If you click [Continue Registration] after registering a user, you can register another user successively without going back to the user list screen.
- If you set [Temporarily stop use] to ON, you can temporarily disable the registered user.
- If the user authentication and account track functions are synchronized, [Account Name] is displayed. At [Account Name], you can specify the account name of the user.
- If you click [Counter] in the list of registered users, you can confirm the number of used sheets for each user.

10.2.2 Account track setting

Setting flow

Installing Account Track enables you to collectively manage multiple users on an account basis. Account authentication information is managed internally by this machine.

A password can be set by account to restrict users from using this machine. Also, this function allows you to restrict available functions or manage the usage status of this machine by account.

You can use a combination of user authentication and account track to manage each user for each department. For example, you can allow a company staff member belonging to a certain department to print but not allow another member belonging to another department to print. Also, you can count the number of printed sheets by department to encourage each department to develop an awareness of costs. You can log in to this machine simply by entering the user name. There is no need to specify the account.

When employing Account Track, follow the below procedure to configure the settings.

- 1 Configuring basic account track settings (page 10-6)
- 2 Configuring settings to suit your environment
 - Restricting available functions for each account (page 10-21)
 - Managing the maximum number of copies by account (page 10-25)

Configure basic account track settings

Enable the account track function. Also register the account.

- 1** Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Account Track]	When enabling account track, set this option to ON (default: OFF).
[Account Track Input Method]	When enabling account track, select the account track method (default: [Account Name & Password]). <ul style="list-style-type: none"> [Account Name & Password]: Enter the account name and password to log in. When using user authentication and account track in combination, the setting cannot be changed from [Account Name & Password]. [Password Only]: Enter only the password to log in.
[Synchronize User Authentication / Account Track]	When using user authentication and account track in conjunction, select whether to synchronize user authentication and account track (default: [Synchronize]). <ul style="list-style-type: none"> [Synchronize]: Select this option when the user and account is in one-to-one relation. If you specify the department of a user when registering him/her, you can log in to the account simply by logging in as the user. [Do Not Synchronize]: Select this option when the user joins multiple accounts. To log in to this machine, enter the user name, then specify the account. [Synchronize by User]: Enables the user to select whether to synchronize the user authentication and account authentication.
[Number of Counters Assigned]	When using user authentication and account track in conjunction, enter the number of counters to be assigned to the user. Up to 1000 counters can be assigned to the user and account collectively. For example, if you assign 950 user counters, you can assign up to 50 account track counters.
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each account can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed (default: [Skip Job]). <ul style="list-style-type: none"> [Skip Job]: Stops the job currently running, and starts printing the next job. [Stop Job]: Stops all jobs. [Delete Job]: Deletes the active job.

- 2** Select [User Auth/Account Track] - [Account Track Settings] - [New Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[No.]	Specify the account's registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Account Name]	Enter the account name (using up to eight characters). This entry is required if you have selected [Account Name & Password] at [Account Track Input Method] in step 1.
[Password]	Enter the password to log in to this machine (using up to 64 characters).
[Function Permission]	Restricts functions available to the account if necessary. For details, refer to page 10-21.
[Max. Allowance Set]	Sets the maximum number of sheets the account can print and User Boxes it can register. For details, refer to page 10-25.

Tips

- If you click [Continue Registration] after registering an account, you can register another account successively without going back to the account list screen.
- If you set [Temporarily stop use] to ON, you can temporarily disable the registered account.
- If you click [Counter] in the list of registered accounts, you can confirm the number of used sheets for each account.

10.2.3 Active Directory authentication setting

Setting flow

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 usage status of this machine.

When employing the Active Directory authentication, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Specifying the date and time of this machine (page 3-4)
- 3 Configuring basic settings for Active Directory authentication (page 10-8)
- 4 Configuring settings to suit your environment
 - Using the single sign-on (page 10-10)
 - Reinforcing authentication processing when using Active Directory (page 10-10)

Configuring basic settings for the Active Directory authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

- 1 Select [User Auth/Account Track] - [External Server Settings] - [External Server Settings] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine).
- 2 Click [Edit] of [1st Server], and configure the following settings.

Setting	Description
[External Server Name]	Enter the name of the authentication server (using up to 32 characters).
[External Server Type]	Select [Active Directory].
[Active Directory]	Register server information when Active Directory is used as the authentication server. <ul style="list-style-type: none"> • [Default Domain Name]: Enter the default domain name of your authentication server (using up to 64 characters). • [Timeout]: Change the timeout interval for communication with Active Directory, if required (default: [60] sec.).

- 3 Click [Edit] of [2nd Server] as needed, and configure the following settings.

Setting	Description
[2nd Server Setting]	When using the secondary server, set this option to ON (default: OFF).
[Round Robin function]	When using the round-robin function, set this option to ON (default: OFF). If you select round-robin function, you can alternately connect the primary and secondary servers to distribute the server load.

Setting	Description
[Reconnection Settings]	<p>Configure a setting to connect to the secondary server when the machine cannot be connected to the primary server (default: [Set Reconnect Interval]). When the round-robin function is enabled, this setting can also be used to connect to the primary server when the machine cannot be connected to the secondary server.</p> <ul style="list-style-type: none"> [Reconnect for every login]: Connects to the primary server each time authentication is carried out on this machine. If the primary server is shutting down, this machine is connected to the secondary server. [Set Reconnect Interval]: Connects to the secondary server when the primary server is shutting down at the time the machine is being authenticated. After this, this machine is connected to the secondary server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary server when machine authentication is occurring.
[External Server Type]	Select the type of the authentication server and set required information. For details, refer to the registration contents of the primary server.

- 4** Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Authentication]	<p>When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)].</p> <p>If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].</p>
[Default Authentication Method]	If [User Authentication] is set to [ON (MFP + External Server)], select the preferential authentication method (default: [ON (External Server)]).
[Ticket Hold Time Setting (Active Directory)]	Change the retention time for a Kerberos authentication ticket if Active Directory is used as an authentication server (default: [5] min.).
[When Number of Jobs Reach Maximum]	<p>Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed (default: [Skip Job]).</p> <ul style="list-style-type: none"> [Skip Job]: Stops the job currently running, and starts printing the next job. [Stop Job]: Stops all jobs. [Delete Job]: Deletes the active job.
[External Authentication server setting]	<p>Set server authentication operations.</p> <ul style="list-style-type: none"> [Temporarily Save Authentication Information]: To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, set this option to ON (default: OFF). [Reconnection Settings]: Specify the timing to reconnect to the authentication server (default: [Set Reconnect Interval]). [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Expiration Date Settings]: When specifying the validity period to the temporarily saved authentication information, set this option to ON (default: OFF). Also, enter the expiration date. [Overwrite User Info]: When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case (default: [Restrict]). If you select [Allow], the oldest authenticated user information is erased and the new user is registered.


Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Authentication Server Connection status] - [External Server Authentication]. If [Connection Enabled] is displayed, you can connect to both the primary and secondary authentication servers.

Using the single sign-on

When user authentication by Active Directory is enabled, single sign-on can be set on this machine.

- Select [Network] - [Single Sign-On Setting] - [Domain Login Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Permission Setting]	When using Single Sign-On, set this option to ON (default: OFF).
[Host Name]	Enter the host name of this machine (using up to 253 characters). Enter the host name you specified in [TCP/IP Setting1] - [DNS Host].
[Domain Name]	Enter the domain name of Active Directory (using up to 64 characters).
[Account Name]	Enter the administrator's account name of the Active Directory domain (using up to 64 characters).
[Password]	Enter the administrator's password of the Active Directory domain (using up to 64 characters).
[Timeout]	Change the time-out time of domain joining processing if necessary (default: [30] sec.).

- After entering required information in step 1, click [OK].
The domain joining processing is executed.
- Select [Network] - [Single Sign-On Setting] - [Auto Log Out Time] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Auto Log Out Time]	When the user uses services of this machine in the Active Directory domain, change the time to hold the user's authentication information on this machine (default: [1 hour]). Since the user can reuse authentication information while it is held on this machine, they can use the services of this machine without performing authentication again.


Tips

- You can select [Network] - [Single Sign-On Setting] - [Applications and Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine) to view the list of services of this machine that joins the Active Directory domain.

Reinforcing authentication processing when using Active Directory

Specify whether to verify authentication information (ticket) obtained from Active Directory on this machine when logging in to this machine while Active Directory is used as the authentication server.

- Select [User Auth/Account Track] - [Self-Verification Setting in AD Authentication] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Self-Verification Setting in AD Authentication]	When verifying authentication information (ticket) obtained from Active Directory on this machine, set this option to ON (default: OFF).
[Host Name]	Enter the host name of this machine (using up to 253 characters).

Setting	Description
[Domain Name]	Enter the domain name of Active Directory (using up to 64 characters).
[Account Name]	Enter the administrator's account name of the Active Directory domain (using up to 64 characters).
[Password]	Enter the administrator's password of the Active Directory domain (using up to 64 characters).
[Timeout]	Change the time-out time of domain joining processing if necessary (default: [30] sec.).

2 Click [OK].

The domain joining processing is executed.

 **Tips**

- If you change [Host Name] or [Domain Name] and click [OK] while Active Directory's single sign-on is enabled on this machine, [Network] - [Single Sign-On Setting] - [Domain Login Setting] - [Permission Setting] is changed to OFF.

10.2.4 NTLM authentication setting

Setting flow

When you use Active Directory of Windows Server (NT-compatible domain environment) for user management, you can restrict users of this machine by authentication using NTLM.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the usage status of this machine.

When employing the NTLM authentication function, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for NTLM authentication (page 10-12)
- 3 Configuring settings to suit your environment
 - Using the WINS server (page 5-10)

Configure basic settings for the NTLM authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

- 1 Select [User Auth/Account Track] - [External Server Settings] - [External Server Settings] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine).
- 2 Click [Edit] of [1st Server], and configure the following settings.

Setting	Description
[External Server Name]	Enter the name of the authentication server (using up to 32 characters).
[External Server Type]	Select [NTLM v1] or [NTLM v2].
[NTLM]	Register server information when NTLM is used as the authentication server. <ul style="list-style-type: none"> • [Default Domain Name]: Enter the default domain name of your authentication server (using up to 64 characters).

- 3 Click [Edit] of [2nd Server] as needed, and configure the following settings.

Setting	Description
[2nd Server Setting]	When using the secondary server, set this option to ON (default: OFF).
[Round Robin function]	When using the round-robin function, set this option to ON (default: OFF). If you select round-robin function, you can alternately connect the primary and secondary servers to distribute the server load.
[Reconnection Settings]	Configure a setting to connect to the secondary server when the machine cannot be connected to the primary server (default: [Set Reconnect Interval]). When the round-robin function is enabled, this setting can also be used to connect to the primary server when the machine cannot be connected to the secondary server. <ul style="list-style-type: none"> • [Reconnect for every login]: Connects to the primary server each time authentication is carried out on this machine. If the primary server is shutting down, this machine is connected to the secondary server. • [Set Reconnect Interval]: Connects to the secondary server when the primary server is shutting down at the time the machine is being authenticated. After this, this machine is connected to the secondary server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary server when machine authentication is occurring.
[External Server Type]	Select the type of the authentication server and set required information. For details, refer to the registration contents of the primary server.

- 4** Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Authentication]	When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)]. If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].
[Default Authentication Method]	If [User Authentication] is set to [ON (MFP + External Server)], select the preferential authentication method (default: [ON (External Server)]).
[When Number of Jobs Reach Maximum]	Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed (default: [Skip Job]). <ul style="list-style-type: none"> [Skip Job]: Stops the job currently running, and starts printing the next job. [Stop Job]: Stops all jobs. [Delete Job]: Deletes the active job.
[External Authentication server setting]	Set server authentication operations. <ul style="list-style-type: none"> [Temporarily Save Authentication Information]: To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, set this option to ON (default: OFF). [Reconnection Settings]: Specify the timing to reconnect to the authentication server (default: [Set Reconnect Interval]). [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Expiration Date Settings]: When specifying the validity period to the temporarily saved authentication information, set this option to ON (default: OFF). Also, enter the expiration date. [Overwrite User Info]: When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case (default: [Restrict]). If you select [Allow], the oldest authenticated user information is erased and the new user is registered.

Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Authentication Server Connection status] - [External Server Authentication]. If [Connection Enabled] is displayed, you can connect to both the primary and secondary authentication servers.

10.2.5 LDAP authentication setting

Setting flow

When you use the LDAP server for user management, you can restrict users of this machine by authentication using LDAP.

Employing the user authentication enables security- and cost-conscious advanced operations such as restricting users from accessing this machine, restricting users from using the functions by user, and managing the usage status of this machine.

When employing the LDAP authentication function, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)

- 2 Configuring basic settings for LDAP authentication (page 10-14)
- 3 Configuring settings to suit your environment
 - Establishing SSL communication (page 10-17)

Configure basic settings for the LDAP authentication

Register your authentication server on this machine. In addition, change the authentication method of this machine so that authentication is performed using the registered authentication server.

- 1 Select [User Auth/Account Track] - [External Server Settings] - [External Server Settings] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine).
- 2 Click [Edit] of [1st Server], and configure the following settings.

Setting	Description
[External Server Name]	Enter the name of the authentication server (using up to 32 characters).
[External Server Type]	Select [LDAP].
[LDAP]	<p>Register server information when LDAP is used as the authentication server.</p> <ul style="list-style-type: none"> • [Server Address]: Enter your LDAP server address. • [Port No.]: If necessary, change the LDAP server port number (default: [389]). • [Search Base 1] to [Search Base 3]: Specify the starting point and range to search a user to be authenticated. [Search Base]: Specify the starting point to search for a target (using up to 255 characters). Example of entry: "cn=users,dc=example,dc=com" [Search Range]: Select a tree search range (default: [Full Tree]). [Full Tree]: Makes a search, including the tree structure under the entered starting point. [Next hierarchy only]: Searches for only one level directly beneath the entered starting point. In this case, the level at the starting point is not included as a search target. • [Timeout]: Change the timeout interval for communication with the LDAP server, if required (default: [60] sec.). • [Authentication Type]: Select the authentication method to log in to the LDAP server depending on your environment (default: [Simple]). • [Search Attribute]: Enter the search attribute used in user account search (using up to 64 characters). The attribute must start with an alphabet character (default: [uid]). • [Search Attributes Authentication]: To automatically generate DN (Distinguished Name) required for authentication by the LDAP server on this machine when [Simple] is selected for [Authentication Type], set this option to ON (default: OFF). Also, enter authentication information used for logging in to the LDAP server in order to search for the user ID.
[Search Directory Service]	If you select [Active Directory], you can limit a search target for authentication to users (default: [Other]). However, when a search target for authentication is limited to users, search target identification processing occurs on the server side, so the authentication time may be delayed. This function is available when the authentication server is set to Active Directory.

- 3 Click [Edit] of [2nd Server] as needed, and configure the following settings.

Setting	Description
[2nd Server Setting]	When using the secondary server, set this option to ON (default: OFF).
[Round Robin function]	When using the round-robin function, set this option to ON (default: OFF). If you select round-robin function, you can alternately connect the primary and secondary servers to distribute the server load.

Setting	Description
[Reconnection Settings]	<p>Configure a setting to connect to the secondary server when the machine cannot be connected to the primary server (default: [Set Reconnect Interval]). When the round-robin function is enabled, this setting can also be used to connect to the primary server when the machine cannot be connected to the secondary server.</p> <ul style="list-style-type: none"> [Reconnect for every login]: Connects to the primary server each time authentication is carried out on this machine. If the primary server is shutting down, this machine is connected to the secondary server. [Set Reconnect Interval]: Connects to the secondary server when the primary server is shutting down at the time the machine is being authenticated. After this, this machine is connected to the secondary server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary server when machine authentication is occurring.
[External Server Type]	Select the type of the authentication server and set required information. For details, refer to the registration contents of the primary server.

- 4** Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Authentication]	<p>When performing authentication using an external authentication server, select [ON (External Server)] or [ON (MFP + External Server)].</p> <p>If you want to configure setting so that you can log in to this machine using its authentication function in consideration of an occurrence of some sort of problem on the external authentication server, select [ON (MFP + External Server)].</p>
[Default Authentication Method]	If [User Authentication] is set to [ON (MFP + External Server)], select the preferential authentication method (default: [ON (External Server)]).
[Ticket Hold Time Setting (Active Directory)]	Change the retention time for a Kerberos authentication ticket if Active Directory is used as an authentication server (default: [5] min.).
[When Number of Jobs Reach Maximum]	<p>Sets the maximum number of sheets that each user can print. Here, select an operation if the number of sheets exceeds the maximum number of sheets that can be printed (default: [Skip Job]).</p> <ul style="list-style-type: none"> [Skip Job]: Stops the job currently running, and starts printing the next job. [Stop Job]: Stops all jobs. [Delete Job]: Deletes the active job.
[External Authentication server setting]	<p>Set server authentication operations.</p> <ul style="list-style-type: none"> [Temporarily Save Authentication Information]: To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, set this option to ON (default: OFF). [Reconnection Settings]: Specify the timing to reconnect to the authentication server (default: [Set Reconnect Interval]). [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. [Expiration Date Settings]: When specifying the validity period to the temporarily saved authentication information, set this option to ON (default: OFF). Also, enter the expiration date. [Overwrite User Info]: When the external server authentication is used, authenticated user information is also managed on this machine. If the number of users who have executed the external server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. Select whether to allow the user to overwrite registered user information for that case (default: [Restrict]). If you select [Allow], the oldest authenticated user information is erased and the new user is registered.

Setting	Description
[External Server DN Cache]	Select whether to save DN (Distinguished Name) information on the machine to speed up the LDAP server authentication (default: [OFF]). If [ON] is selected, information related to the user's DN is saved on the machine when authentication succeeds in the LDAP server. At the next authentication, a user search is performed using the saved information.

 **Tips**

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Authentication Server Connection status] - [External Server Authentication]. If [Connection Enabled] is displayed, you can connect to both the primary and secondary authentication servers.

Using SSL communication

If SSL is installed in your environment, enable SSL.

Select [User Auth/Account Track] - [External Server Settings] - [External Server Settings] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LDAP]	Configure settings to establish a communication via SSL. <ul style="list-style-type: none"> [Enable SSL]: When using SSL communications, set this option to ON (default: OFF). [Port No.(SSL)]: If necessary, change the port number for SSL communication (default: [636]).

10.2.6 Configuring a setting so that a user can log in to this machine using administrator privileges

You can configure a setting so that a registered user can log in to this machine using administrator privileges.

- 1 Select [User Auth/Account Track] - [User Authentication Setting] - [Administrative Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Login Allowed with Administrative Rights]	When allowing the user to log in with administrator or User Box administrator privileges, set this option to ON (default: OFF).

- 2 Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Permission Setting]	Assigns administrator privileges to the user. Select [All Users] to apply this setting to all users. Specify whether to assign each of the following privileges to the user. <ul style="list-style-type: none"> [Administrative Rights] (default: OFF) [User Box Administrator Rights] (default: OFF)

10.2.7 Extending the number of users to be authenticated

Using the advanced user database, you can extend the number of user information items, which can be registered on the machine, to 50000. This option is available when [ON (MFP)] or [ON (MFP + External Server)] is selected in [User Authentication].

Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Extended User DB]	Select whether to extend the number of users to be authenticated on the machine using the advanced user database (default: [OFF]).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

10.2.8 Using the MFP authentication together against in the case where an enhanced server has shut down

To manage users who use this machine via the enhanced server, you can use the MFP authentication together against in the case where an enhanced server has shut down.

Using the enhanced server authentication and MFP authentication together, you can use the authentication information temporarily saved on the machine to log in and use the machine even if the enhanced server has shut down.

- 1 Select [User Auth/Account Track] - [Authentication Type] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[User Authentication]	To use enhanced server authentication and MFP authentication together, select [ON (MFP + Enhanced Server)].
[Update Billing Information]	Select whether to overwrite existing billing information if the billing information that can be managed on this machine reached the upper limit when the enhanced server shut down (default: [Restrict]).
[Default Authentication Method]	If [User Authentication] is set to [ON (MFP + Enhanced Server)], select the preferential authentication method (default: [Enhanced Server Authentication]).
[Number of Counters Assigned]	If you have selected [ON (MFP + Enhanced Server)] in [User Authentication], assign a counter area to temporarily save information against in the case where an enhanced server has shut down. Up to 1000 counter areas can be specified combined with [User Counter].
[External Authentication server setting]	Set server authentication operations. <ul style="list-style-type: none"> • [Temporarily Save Authentication Information]: To temporarily save authentication information in the main unit against a case where an external authentication server shuts down, set this option to ON (default: OFF). • [Reconnection Settings]: Specify the timing to reconnect to the authentication server (default: [Set Reconnect Interval]). [Reconnect for every login]: Connects to the authentication server at the time authentication is carried out on this machine. If the authentication server is in the shutdown state at the time authentication is carried out on this machine, first confirm that the authentication server is down, and use the temporarily saved authentication information to log in to this machine. [Set Reconnect Interval]: Connect to the authentication server at the time specified in [Reconnection Time], and check the status of the authentication server. If the authentication server is in the shutdown state, use the authentication information temporarily saved in the main unit to log in. • [Expiration Date Settings]: When specifying the validity period to the temporarily saved authentication information, set this option to ON (default: OFF). Also, enter the expiration date. • [Overwrite User Info]: If [ON (MFP + Enhanced Server)] is selected in [User Authentication], [Allow] is specified forcibly. When the enhanced server authentication is used, the authenticated user information is also managed on this machine. If the number of users who have executed the enhanced server authentication reaches the maximum number of users this machine can manage, authentication of any new users will not be permitted. In this case, registered user information is overwritten.

- 2 Select [User Auth/Account Track] - [Max. Allowance Setting when Enhanced Server down] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

- [Max. Allowance Setting when Enhanced Server down] is displayed when [Temporarily Save Authentication Information] is set to ON in step 1.

Setting	Description
[Max. Allowance Setting when Enhanced Server down]	When managing the maximum allowance for the number of printed sheets or the number of registered User Boxes on this machine when the enhanced server has shut down, set this option to ON (default: ON).
[Print(Total)]/[Print(Color)]/[Print(Black)]	To manage the maximum allowance for the number of printed sheets, specify the maximum allowance.

Setting	Description
[Personal User Box Allowance]	To manage the maximum allowance for the number of registered Personal User Boxes, specify the maximum allowance.
[Billing Allowance]	To manage the maximum allowance for accounting, specify the maximum allowance.

 **Tips**

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

10.3 Managing a Use of this Machine by User or Account

10.3.1 Restricting available functions

Restricting available functions for each user

Installing user authentication allows you to restrict available functions for each user.

For example, you can set it up so that specific users can print, but other users can not print. Configuring settings according to the business requirements of users provides you with added security measures and reduced costs simultaneously.

Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Function Permission] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Function	Description
[Copy]	Select whether to allow use of the copy function (default: [Full Color/Black]). [Black Only] allows black and white copying only.
[Scan]	Select whether to allow use of the scan function (default: [Full Color/Black]). [Black Only] allows scanning in black and white only.
[Save to USB flash drive]	Select whether to allow users to save files on a USB memory (default: OFF). This option is available when saving files on a USB memory device is enabled on this machine.
[Scan documents to USB flash drive]	Select whether to allow scanning of files from a USB memory device (default: OFF). This option is available when scanning files from a USB memory device is enabled on this machine.
[Fax]	Select whether to allow use of the fax or network fax function (default: [Full Color/Black]). [Black Only] allows black and white transmission only.
[Print]	Select whether to allow printing by the print function (default: [Full Color/Black]). [Black Only] allows black and white printing only.
[User Box]	Select whether to allow use of files saved in the User Box (default: ON).
[TX Document Print]	Select whether to allow printing of scan transmission or fax transmission data (default: [Full Color/Black]). [Black Only] allows black and white printing only. If you select [Restrict], you cannot print transmission data during scan and fax transmissions. In addition, you cannot print transmission data saved in the following User Boxes. However, you can print data saved in a User Box from a USB flash drive. <ul style="list-style-type: none"> • Scan transmission data in Public, Personal, and Group User Box • Fax transmission data in Bulletin Board User Box, Polling TX User Box, and Fax Retransmit User Box
[Manual Destination Input]	Select whether to allow the user to directly enter a destination (default: [Allow]). [Allow Fax Only] allows direct input of a fax number only.
[Web Browser]	Select whether to allow use of the Web browser function (default: [Allow All]). This function is available when the Web browser function is enabled. <ul style="list-style-type: none"> • [File Upload]: Select whether to allow file uploading (default: ON). • [File Download]: Select whether to allow file downloading (default: ON).
[Biometric/IC Card Information Registration]	Select whether to allow registration of bio authentication information and IC card authentication information (default: OFF).

Tips

- To use the external authentication server, user information is registered once you execute authentication. To restrict functions accessible by users, edit user information registered on this machine.

Restricting available functions by account track

Installing account track allows you to restrict available functions by account track.

For example, you can set it up so that specific accounts can print, but other accounts cannot print. Configuring settings according to the business requirements of accounts provides you with added security measures and reduced costs simultaneously.

Select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration] - [Edit] - [Function Permission] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Function	Description
[Copy]	Select whether to allow use of the copy function (default: [Full Color/Black]). [Black Only] allows black and white copying only.
[Scan]	Select whether to allow use of the scan function (default: [Full Color/Black]). [Black Only] allows scanning in black and white only.
[Fax]	Select whether to allow use of the fax or network fax function (default: [Full Color/Black]). [Black Only] allows black and white transmission only.
[Print]	Select whether to allow printing by the print function (default: [Full Color/Black]). [Black Only] allows black and white printing only.
[TX Document Print]	Select whether to allow printing of scan transmission or fax transmission data (default: [Full Color/Black]). [Black Only] allows black and white printing only. If you select [Restrict], you cannot print transmission data during scan and fax transmissions. In addition, you cannot print transmission data saved in the following User Boxes. However, you can print data saved in a User Box from a USB flash drive. <ul style="list-style-type: none"> • Scan transmission data in Public, Personal, and Group User Box • Fax transmission data in Bulletin Board User Box, Polling TX User Box, and Fax Retransmit User Box

Configuring the default settings of the functions available for users of external server 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.

Select [User Auth/Account Track] - [User Authentication Setting] - [Default Function Permission] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then configure the default function permission setting when using an external authentication server.

Tips

- To use the external authentication server, user information is registered once you execute authentication. To restrict functions accessible by users, edit user information registered on this machine.

10.3.2 Limiting the accessible destinations

Methods to limit access to destinations

You can limit accessible destinations for each user on this machine. The following three methods are available to limit accessible destinations.

Method to limit access	Description
Managing based on the reference allowed level	Sorts destinations depending on the importance level, and set the upper limit of the access level for each user.
Managing based on the reference allowed group	Sorts destinations into groups. A user can only access permitted destinations in the group.
Managing based on a combination of the reference allowed level and the reference allowed group	Set the access range based on a combination of the important level of a destination and the relationship between the destination and the user.

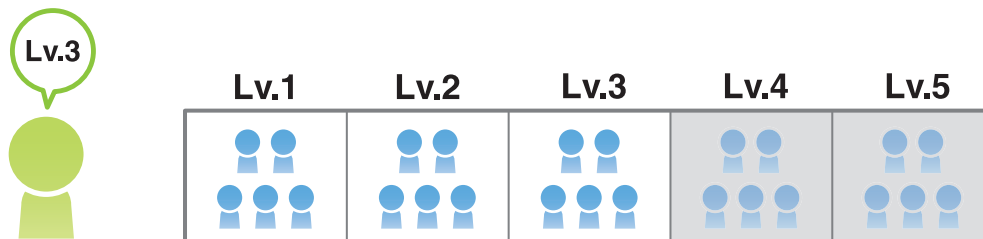
Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Setting the reference allowed level

This function sorts out destinations registered in this machine from Level 0 to Level 5 in order of importance to set the upper limit of the access level (allowed level) for each user.

For example, assume that Level 3 is set for a certain user as a reference allowed level. In this case, that user can access destinations in Reference Allowed Level 1 to 3, but cannot access destinations in Reference Allowed Level 4 and 5.



- 1 Select [Store Address] - [Address Book] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), select [Set direct Reference Allowed Level], then set the reference allowed level for the address book.
- 2 Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and set [Access Allowed Level] to ON to specify the reference allowed level.

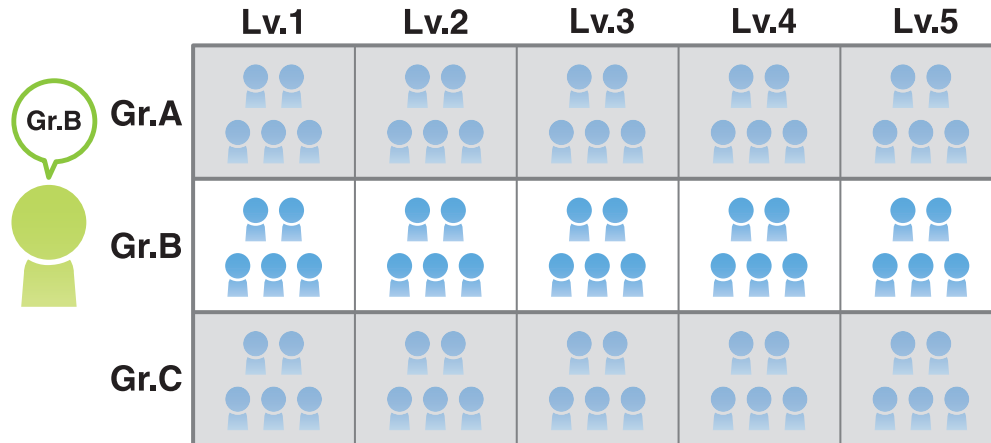
Tips

- The reference allowed level set for the user is "Level 0" by default. Level-0 users can only access the destinations at level 0.

Assigning a 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.



Register a reference allowed group on this machine. In addition, assign a reference allowed group to the destination and user.

- 1 Select [Security] - [Limiting Access to Destinations] - [Store Group] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and register the reference allowed group.

Setting	Description
[Group Name]	Enter the name of the group (using up to 24 characters).
[Access Allowed Level]	To manage the address book by combining the reference allowed level and reference allowed group, select a reference allowed level of the reference allowed group (default: [Level 0]).

- 2 Select [Store Address] - [Address Book] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), select [Search from Reference Allowed Group], then assign the reference allowed group to the registered destination.
- 3 Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and set [Reference Allowed Group] to ON to assign the reference allowed group to the registered user.

Simultaneously setting a reference allowed level and reference allowed group

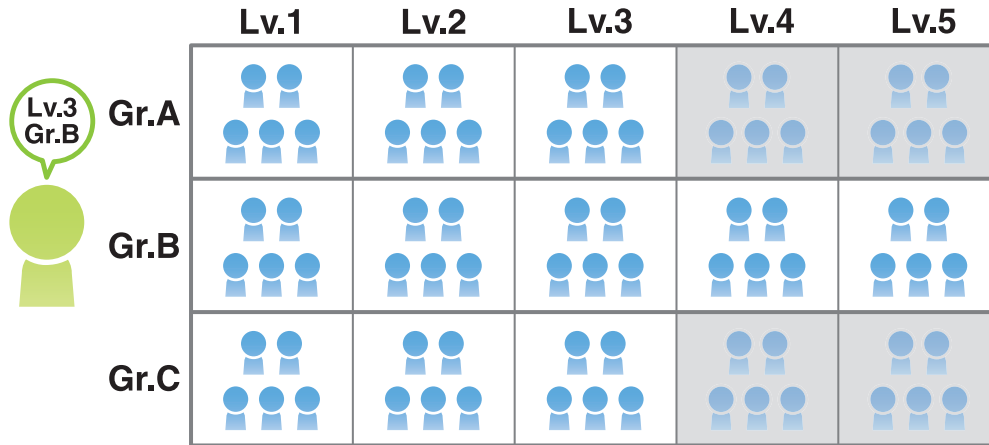
A combination of the reference allowed level and reference allowed group provides more flexible management.

For example, assume that Level 3 is set as a reference allowed level and Group B is set as a reference allowed group for a certain user.

In this case, destinations the user can access are as follows.

- Destinations of Reference Allowed Level 1 to 3: A1 to A3, B1 to B3, C1 to C3

- Destinations belonging to Reference Allowed Group B: B1 to B5



Set both a reference allowed level and reference allowed group for a user.

To manage the address book by combining the reference allowed level and reference allowed group, register a reference allowed group for which a reference allowed level is set, and assign it to the address book.

- 1 Select [Security] - [Limiting Access to Destinations] - [Store Group] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and register the reference allowed group.

Setting	Description
[Group Name]	Enter the name of the group (using up to 24 characters).
[Access Allowed Level]	To manage the address book by combining the reference allowed level and reference allowed group, select a reference allowed level of the reference allowed group (default: [Level 0]).

- 2 Select [Store Address] - [Address Book] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), set the reference allowed group or level to the registered destination.

→ To manage the address book by combining the reference allowed level and reference allowed group, assign a reference allowed group for which a reference allowed level is set to the address book.

- 3 Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and set the reference allowed group and level to the registered user respectively.

→ To specify a reference allowed group for a registered user means that you specify a reference allowed group itself. Therefore, even if a reference allowed level has been set for the selected reference allowed group, that setting of reference allowed level is not applied here.

Tips

- You can specify the reference allowed level of each reference allowed group. If you assign a reference allowed group for which a reference allowed level is set to the address book, you can manage destinations by using both the reference allowed level and reference allowed group.

10.3.3 Managing the maximum number of printable pages

Managing the maximum number of printable pages by user

Employing User Authentication enables you to specify the maximum number of printable pages by user. Also, you can set the upper limit of the number of User Boxes that can be registered.

Management of the upper limit of copies by user depending on the usage status of this machine encourages users to develop an awareness of costs and also contributes to cost reduction.

Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Max. Allowance Set] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Function	Description
[Total Allowance]	Set the total number of printable pages (default: OFF).
[Individual Allowance]	Specify the number of printable pages separately for [Color] and [Black] (default: OFF).
[Box Administration]	Specify the number of registerable User Boxes (default: OFF).

Tips

- To use the external authentication server, user information is registered once you execute authentication. To set the upper limit, edit user information registered on this machine.

Managing the maximum number of printable pages by account

Employing Account Track enables you to specify the maximum number of printable pages by account. Also, you can set the upper limit of the number of User Boxes that can be registered.

Management of the upper limit of printable pages by account depending on the usage status of this machine encourages accounts to develop an awareness of costs and also contributes to cost reduction.

Select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration] - [Edit] - [Max. Allowance Set] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Function	Description
[Total Allowance]	Set the total number of printable pages (default: OFF).
[Individual Allowance]	Specify the number of printable pages separately for [Color] and [Black] (default: OFF).
[Box Administration]	Specify the number of registerable User Boxes (default: OFF).

10.3.4 Managing a use by a public user

Restrict the functions or destinations public users can use or access.

Select [User Auth/Account Track] - [User Authentication Setting] - [Public User] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Function Permission]	<p>Restrict the functions public users can use. Specify whether to restrict the following functions, respectively:</p> <ul style="list-style-type: none"> • [Copy] (default: [Full Color/Black]) • [Scan] (default: [Full Color/Black]) • [Save to USB flash drive] (default: OFF) • [Scan documents to USB flash drive] (default: OFF) • [Fax] (default: [Full Color/Black]) • [Print] (default: [Full Color/Black]) • [User Box] (default: ON) • [TX Document Print] (default: [Full Color/Black]) • [Manual Destination Input] (default: [Allow]) • [Web Browser] (default: ON) • [Biometric/IC Card Information Registration] (default: OFF)
[Limiting Access to Destinations]	<p>Restricts destinations public users can access.</p> <ul style="list-style-type: none"> • [Reference Allowed Group]: Assign a reference allowed group to a public user (default: OFF). • [Access Allowed Level]: Assign a reference allowed level to a public user (default: [Level 0]).

Tips

- When a public user attempts to use a restricted function, the login screen appears to switch the user. For example, if color scan is restricted for public users, the Login screen appears when a public user attempts a color scan operation. In this case, the user can log in to this machine as another user for whom color scan is allowed, and use the color scan function. To display the login screen when you select a function restricted for a public user, select [User Auth/Account Track] - [Prohibited Function Login Setting], and set [Prohibited Function Login Setting] to ON.

10.3.5 Changing the function key to be displayed on the classic style screen

Setting flow

This machine provides three display patterns to display or hide function keys in each mode.

If user authentication or account track is installed on this machine, you can select a display pattern of function keys to be displayed in each mode screen for each user or account track.

For example, you can configure settings so that only basic functions are normally displayed on the screen and all functions are displayed on the screen when a specific user or account logs in to this machine. If you select a display pattern according to your environment, you can increase productivity when using this machine.

To select a function key display pattern for each user or account, follow the below procedure to configure the settings.

- 1 Allowing changing the function key display pattern by user or account (page 10-26)
- 2 Selecting a function key display pattern by user or account
 - To change the function key display pattern by user, refer to page 10-27.
 - To change the function key display pattern by account, refer to page 10-27.

Allowing changing the function key display pattern by user or account

Configure setting to select a display pattern of the function keys to be displayed on the screen in each mode for each user or account track.

Select [System Settings] - [Custom Function Profile User/Account] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Custom Function Profile User/Account]	When permitting the user to change the display pattern of function keys in the Copy, Scan/Fax and User Box modes of classic style for each user or account, set this option to ON (default: OFF).

Selecting a function key display pattern by user

Change the display pattern of function keys in the Copy, Scan/Fax and User Box modes of classic style, respectively.

Select [User Auth/Account Track] - [User Authentication Setting] - [User Registration] - [Edit] - [Custom Function Profile User/Account] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Copy/Print Screen]	Select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard].
[Send/Save Screen]	Select a display pattern of function keys to be displayed on the send and save settings screens in Scan/Fax and User Box modes (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard].

Tips

- To check the functions available for each pattern setting, select [System Settings] - [Custom Function Pattern Selection], then click [Details].
- A function key display pattern can be added to suit your requirements. For details, contact your service representative.

Selecting a function key display pattern by account

Change the display pattern of function keys in the Copy, Scan/Fax and User Box modes of classic style, respectively.

Select [User Auth/Account Track] - [Account Track Settings] - [Account Track Registration] - [Edit] - [Custom Function Profile by Account] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Copy/Print Screen]	Select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard].
[Send/Save Screen]	Select a display pattern of function keys to be displayed on the send and save settings screens in Scan/Fax and User Box modes (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard].

Tips

- To check the functions available for each pattern setting, select [System Settings] - [Custom Function Pattern Selection], then click [Details].
- A function key display pattern can be added to suit your requirements. For details, contact your service representative.

10.3.6 Configuring common settings for user authentication and account track

Configure common settings in user authentication/account track to display the confirmation screen when logging out.

Select [User Auth/Account Track] - [User/Account Common Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Single Color / 2 Color Output Management]	Switch settings for single color or 2-color printing between options to handle it as either color or black-and-white printing (default: [Color]). <ul style="list-style-type: none">• [Color]: Manages single color and 2-color printing as color print.• [Black]: Manages single color and 2-color printing as black print. Select this option to manage full-color printing alone as color print.
[Logout Confirmation Display Setting]	Specify whether to display the logout confirmation screen when you log out from the login mode (Recipient User or Public User) (default: [ON]).

10.4 Configuring Print Operations in User Authentication Environment

10.4.1 Specifying the operations of the ID & Print function

Specify the operations of the ID & Print function. Also, specify the action that this machine takes when it receives a print job from a public user or a print job without authentication information.

Select [User Auth/Account Track] - [User Authentication Setting] - [Administrative Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine).

Setting	Description
[ID & Print]	When handling jobs normally printed from the printer driver as ID & Print jobs, set this option to ON (default: OFF).
[Public User]	Select the process performed when a public user job or a job without user authentication information is received (default: [Print Immediately]). <ul style="list-style-type: none"> [Print Immediately]: Prints the job without saving it in the ID & Print User Box. [Save]: Saves the job in the ID & Print User Box.
[ID & Print Operation Settings]	Select the processing method when using the ID & Print function in Authentication Unit (default: [Print All Jobs]). <ul style="list-style-type: none"> [Print All Jobs]: One successful authentication session allows the user to print all jobs. [Print Each Job]: One successful authentication session allows the user to print one job.
[Change to Basic Screen after ID & Print]	Select whether to display the screen after login when ID & Print was executed (default: [Restrict]). If [ON] is selected, [Login after Print] is displayed in [ID & Print] on the login page.
[Auth. Operation Setting when print Documents are Stored]	Select the default value for the operation that is performed after authentication in the login window. <ul style="list-style-type: none"> [Logout after Print]: Automatically logs out after data printing. [Login without Print]: Logs out without printing data. [Login after Print]: Logs in after data printing. This setting is available when [ON] is selected for [Change to Basic Screen after ID & Print].



Tips

- To use ID & Print, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

10.4.2 Restricting print jobs without authentication information

Select whether to permit printing of a job without authentication information when User Auth/Account Track is enabled.

To print data without adding authentication information using the printer driver, for example, when you want to directly send jobs from the mission-critical system such as ERP (Enterprise Resource Planning) to the machine and make prints, permit printing of a job without authentication information.

Select [User Auth/Account Track] - [Print without Authentication] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Print without Authentication]	Select whether to permit printing of a job without authentication information (default: [Restrict]). <ul style="list-style-type: none"> [Full Color/Black]: Allows both color and black and white printing. Print jobs are counted as public user jobs. [Black Only]: Allows black and white printing only. Color printing jobs are also printed in black and white. Print jobs are counted as public user jobs. [Restrict]: Printing is restricted. Canceling [Restrict] allows everybody to perform printing. Select [Restrict] to control user access and ensure security.

Setting	Description
[IP Filtering (Permit Access)]	To restrict printable computers using the IP address when you select [Full Color/Black] or [Black Only] in [Print without Authentication], set this option to ON (default: OFF). <ul style="list-style-type: none"> [IP Address]: Enter the range of IP address of the printable computers. Example to enter [Set1] to [Set5]: "192.168.1.1 - 192.168.1.10" To allow access from a single IP address, you can only enter the address in one side of the range.


Tips

- If print jobs without authentication information are allowed, they are counted as public user jobs.

10.4.3 Printing with authentication by user name only (quick authentication)

Setting flow

When quick authentication is allowed while user authentication is enabled, you can print with authentication by user name only (without a password) when making prints using the printer driver.

When using the quick authentication, follow the below procedure to configure the settings.

- 1 Permitting quick authentication (page 10-30)
- 2 Configuring settings to suit your environment
 - Registering the quick authentication server (page 10-30)
 - Establishing SSL communication (page 10-32)

Permitting quick authentication

Specify whether to allow quick authentication.

Select [User Auth/Account Track] - [Simple Authentication setting] - [Simple Authentication setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Function	Description
[Simple Authentication setting]	When allowing the quick authentication, set this option to ON (default: OFF).


Tips

- To permit the quick authentication, the login user name for this machine for MFP authentication, external server authentication, and enhanced server authentication must match the Windows login ID.

Registering the quick authentication server

You must inquire the LDAP server about the user name to obtain permission to access this machine in an environment where external server authentication is employed. This LDAP server is called the quick authentication server.

- 1 Select [User Auth/Account Track] - [Simple Authentication setting] - [Register Simple Authentication Server] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine).
- 2 Click [Edit] of [1st Server], and configure the following settings.

Setting	Description
[Simple Authentication Server Name]	Enter the name of the authentication server (using up to 32 characters).

Setting	Description
[External Authentication Server]	Select the external authentication server used to associate the quick authentication (default: [No Selection]). When authentication succeeds, user authentication information is registered on the machine to manage users on the machine. This authentication information includes the user name and external authentication server name. The external authentication server name selected here is registered on the machine together with the user name.
[Server Address]	Enter the LDAP server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number (default: [389]).
[Search Base 1] to [Search Base 3]	Specify the starting point and range to search for a user to be authenticated. <ul style="list-style-type: none"> • [Search Base]: Specify the starting point to search for a target (using up to 255 characters). Example of entry: "cn=users,dc=example,dc=com" • [Search Range]: Select a tree search range (default: [Full Tree]). [Full Tree]: Makes a search, including the tree structure under the entered starting point. [Next hierarchy only]: Searches for only one level directly beneath the entered starting point. In this case, the level at the starting point is not included as a search target.
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server (default: [60] sec.).
[Authentication Type]	Select the authentication method to log in to the LDAP server depending on your environment (default: [Simple]). <ul style="list-style-type: none"> • [Login Name]: Enter the login name used for LDAP authentication (using up to 64 characters). • [Password]: Enter the password for LDAP authentication (using up to 64 characters). • [Domain Name]: If [GSS-SPNEGO] is selected for [Authentication Type], enter the domain name of Active Directory (using up to 64 characters).
[Use Referral]	Select whether to use the referral function (default: [ON]).
[Search Attribute]	When performing LDAP search, enter the search attribute to be automatically added before the user name (using up to 64 characters). The attribute must start with an alphabet character (default: [uid]).
[Search Directory Service]	If you select [Active Directory], you can limit a search target for authentication to users (default: [Other]). However, when a search target for authentication is limited to users, search target identification processing occurs on the server side, so the authentication time may be delayed. This function is available when the authentication server is set to Active Directory.

3 Click [Edit] of [2nd Server] as needed, and configure the following settings.

Setting	Description
[2nd Server Setting]	When using the secondary server, set this option to ON (default: OFF).
[Round Robin function]	When using the round-robin function, set this option to ON (default: OFF). If you select round-robin function, you can alternately connect the primary and secondary servers to distribute the server load.

Setting	Description
[Reconnection Settings]	<p>Configure a setting to connect to the secondary server when the machine cannot be connected to the primary server (default: [Set Reconnect Interval]). When the round-robin function is enabled, this setting can also be used to connect to the primary server when the machine cannot be connected to the secondary server.</p> <ul style="list-style-type: none"> [Reconnect for every login]: Connects to the primary server each time authentication is carried out on this machine. If the primary server is shutting down, this machine is connected to the secondary server. [Set Reconnect Interval]: Connects to the secondary server when the primary server is shutting down at the time the machine is being authenticated. After this, this machine is connected to the secondary server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary server when machine authentication is occurring.
Secondary Server Information	<p>Register the secondary server. For details, refer to the registration contents of the primary server. To extract the primary server setting and configure the secondary server setting, tap [Same as 1st Server].</p>



Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Authentication Server Connection status] - [Simple Auth.]. If [Connection Enabled] is displayed, you can connect to both the primary and secondary authentication servers.

Using SSL communication

If SSL is installed in your environment, enable SSL.

Select [User Auth/Account Track] - [Simple Authentication setting] - [Register Simple Authentication Server] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable SSL]	<p>When using SSL communications, set this option to ON (default: OFF).</p> <ul style="list-style-type: none"> [Port No.(SSL)]: If necessary, change the port number for SSL communication (default: [636]).
[Certificate Verification Level Settings]	<p>To validate the certificate during SSL communication, select items to be verified.</p> <ul style="list-style-type: none"> [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

10.5 Installing IC Card Authentication or Biometric Authentication

10.5.1 Setting biometric authentication operations

When using the optional **Biometric Authentication Unit**, set biometric authentication operations.

Select [User Auth/Account Track] - [Authentication Device Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Bio Authentication]	Set biometric authentication operations. <ul style="list-style-type: none"> [Beep Sound]: To output a "blip" sound when the finger vein pattern is scanned successfully, set this option to ON (default: ON). Select how to log in to this machine (default: [1-to-many authentication]). <ul style="list-style-type: none"> [1-to-many authentication]: Simply place his or her finger to log in. [1-to-1 authentication]: Enter the user name and position his or her finger to log in. [1 to many authentication PIN code authentication]: Enter the PIN Code and place the user's finger to log in. This setting is displayed when VLAN is set.
[Logoff Settings]	When automatically logging out after scanning the original, set this option to ON (default: OFF).

10.5.2 Authenticating in the LDAP server using the authentication card (LDAP-IC Card Authentication)

Setting flow

You can configure settings so that authentication is performed in the LDAP server using the card ID registered in the authentication card (LDAP-IC Card Authentication).

Authentication is completed simply by placing the IC card. This enhances security without damaging users' ability to easily operate the machine.

To perform authentication using the authentication card, follow the below procedure to configure the settings.

- 1 Enabling use of **IC Card Authentication Unit** on this machine ("User's Guide[Advanced Function Operations]/[Installing IC Card Authentication]")
- 2 Configuring basic settings for LDAP-IC card authentication (page 10-33)
- 3 Configuring settings to suit your environment
 - Establishing SSL communication (page 10-36)

Configuring basic settings for the LDAP-IC card authentication

- 1 Select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [LDAP-IC Card Authentication Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[LDAP-IC Card Authentication Setting]	When performing authentication via the LDAP server using the card ID registered on authentication card, set this option to ON (default: OFF).

- 2 Select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Server Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

3 Click [Edit] of [1st Server], and configure the following settings.

Setting	Description
[LDAP-IC Card Authentication Server Name]	Enter the name of the authentication server (using up to 32 characters).
[External Authentication Server]	Select the external authentication server used to associate the LDAP-IC card authentication (default: [No Selection]). When authentication succeeds, user authentication information is registered on the machine to manage users on the machine. This authentication information includes the user name and external authentication server name. The external authentication server name selected here is registered on the machine together with the user name.
[Card Information Registration Settings]	When authentication is performed on the machine using an IC card not registered in the LDAP server, select whether to register the card information in the LDAP server (default: [OFF]). <ul style="list-style-type: none"> [Sequential Server Card Registration]: Specify the server to register card information in. If you select [Primary Server for Card Registration], card information is registered in the server with authentication succeeded among the primary and secondary servers. [User Name Attribute]: Specify the attribute to be searched as the user name.
[Card Information Character Type During Search]	Select the search string conversion method to search for the card ID via the LDAP server (default: [Uppercase Letters/ Lowercase Letters]). When the target card attribute information on the server is unified into upper and lower case letters, in some cases, you can convert the character type of the search string and subsequently reduce the search speed. <ul style="list-style-type: none"> [Uppercase Letters/ Lowercase Letters]: Converts the card ID into upper or lower case letters to carry out a search. [Uppercase Letters]: Converts the card ID to uppercase letters to carry out a search. [Lowercase Letters]: Converts the card ID to lowercase letters to carry out a search.
[Server Address]	Enter the LDAP server address. Use one of the following formats. <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the LDAP server port number (default: [389]).
[Search Base 1] to [Search Base 3]	Specify the starting point and range to search for a user to be authenticated. <ul style="list-style-type: none"> [Search Base]: Specify the starting point to search for a target (using up to 255 characters). Example of entry: "cn=users,dc=example,dc=com" [Search Range]: Select a tree search range (default: [Full Tree]). [Full Tree]: Makes a search, including the tree structure under the entered starting point. [Next hierarchy only]: Searches for only one level directly beneath the entered starting point. In this case, the level at the starting point is not included as a search target.
[Timeout]	If necessary, change the time-out time to limit a communication with the LDAP server (default: [60] sec.).
[Authentication Type]	Select the authentication method to log in to the LDAP server depending on your environment (default: [Simple]). <ul style="list-style-type: none"> [Login Name]: Enter the login name used for LDAP authentication (using up to 64 characters). In this step, enter the user (name) that belongs to a specific administrator group on the LDAP server. [Password]: Enter the password for LDAP authentication (using up to 64 characters). [Domain Name]: If [GSS-SPNEGO] is selected for [Authentication Type], enter the domain name of Active Directory (using up to 64 characters).
[Use Referral]	Select whether to use the referral function (default: [ON]).
[Search Attribute]	When performing LDAP search, enter the search attribute to be automatically added before the user name (using up to 64 characters). The attribute must start with an alphabet character (default: [uid]).

Setting	Description
[User Name]	Select how to obtain the user name when logging in to this machine (default: [Use Card ID]). If [ON] is selected in [Card Information Registration Settings], [Acquiring] is selected, and any change cannot be made. <ul style="list-style-type: none"> [Use Card ID]: Select this option when only IC card information is registered on the server. Uses the card ID in the IC card as the user name. [Acquiring]: Select this option when user information other than IC card information is registered on the server. Uses the user name obtained from the server. Enter the attribute to be searched as the user name ("uid") at [User Name Attribute].
[Search Directory Service]	If you select [Active Directory], you can limit a search target for authentication to users (default: [Other]). However, when a search target for authentication is limited to users, search target identification processing occurs on the server side, so the authentication time may be delayed. This function is available when the authentication server is set to Active Directory.

4 Click [Edit] of [2nd Server] as needed, and configure the following settings.

Setting	Description
[2nd Server Setting]	When using the secondary server, set this option to ON (default: OFF).
[Round Robin function]	When using the round-robin function, set this option to ON (default: OFF). If you select round-robin function, you can alternately connect the primary and secondary servers to distribute the server load.
[Reconnection Settings]	Configure a setting to connect to the secondary server when the machine cannot be connected to the primary server (default: [Set Reconnect Interval]). When the round-robin function is enabled, this setting can also be used to connect to the primary server when the machine cannot be connected to the secondary server. <ul style="list-style-type: none"> [Reconnect for every login]: Connects to the primary server each time authentication is carried out on this machine. If the primary server is shutting down, this machine is connected to the secondary server. [Set Reconnect Interval]: Connects to the secondary server when the primary server is shutting down at the time the machine is being authenticated. After this, this machine is connected to the secondary server when machine authentication is occurring until the time specified in [Reconnection Time] lapses. After the time specified in [Reconnection Time] has lapsed, this machine is reconnected to the primary server when machine authentication is occurring.
[Card Information Registration Settings]	When authentication is performed on the machine using an IC card not registered in the LDAP server, select whether to register the card information in the LDAP server. <ul style="list-style-type: none"> [Same as 1st Server]: Select [Enable] when using the same setting as for the primary server. When using a setting different from that of the primary server, select [Disable], then specify the attribute that is to be searched as the user name in [User Name Attribute].
Secondary Server Information	Register the secondary server. For details, refer to the registration contents of the primary server. To extract the primary server setting and configure the secondary server setting, tap [Same as 1st Server].

Tips

- To check the status of the connection of the primary authentication server and the secondary authentication server, select [User Auth/Account Track] - [Authentication Server Connection status] - [LDAP-IC Card Authentication]. If [Connection Enabled] is displayed, you can connect to both the primary and secondary authentication servers.

Using SSL communication

If SSL is installed in your environment, enable SSL.

Select [User Auth/Account Track] - [LDAP-IC Card Authentication Setting] - [Server Registration] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable SSL]	<p>When using SSL communications, set this option to ON (default: OFF).</p> <ul style="list-style-type: none"> [Port No.(SSL)]: If necessary, change the port number for SSL communication (default: [636]).
[Certificate Verification Level Settings]	<p>To validate the certificate during SSL communication, select items to be verified.</p> <ul style="list-style-type: none"> [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).



Reinforcing Security

11 Reinforcing Security

11.1 Changing Security Settings

11.1.1 Enhancing the security by simple operation

[Quick Security Setting] summarizes settings to enhance the security level of this machine. We recommend that you change settings in order to use this machine more securely.

Select [Security] - [Quick Security Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Quick IP Filtering]	<p>Allows you to restrict the devices that can access this machine using the IP address (IPv4/IPv6). The range of IP addresses for which access is to be restricted is specified automatically.</p> <p>Select the method to specify the IP address for which access is restricted. [Synchronize IP Address] is specified by default. In some areas, [No Filtering] is specified by default.</p> <ul style="list-style-type: none"> • [Synchronize IP Address]: For the IPv4 address, this option only permits access for the IPv4 address set to this machine, and the IPv4 addresses of which the high-order 3 bytes are the same. Example: When the IPv4 address of this machine is set to "192.168.0.134", the range of IPv4 addresses that allow access is as follows. 192.168.0.0 to 192.168.0.255 For the IPv6 address, this option only permits access for the global unicast address (2000::/3). Also, this option only permits access for the IPv6 address set to this machine, and the IPv6 addresses of which the high-order 64 bits are the same. Example: When the IPv6 address of this machine is set to "2345:1:2:3:4:5:6:7", the range of IPv6 addresses that allow access is as follows. 2345:1:2:3::0 to 2345:1:2:3:FFFF:FFFF:FFFF:FFFF • [Synchronize Subnet Mask]: For the IPv4 address, this option only permits access for IPv4 addresses that belong to the same network using the IPv4 address set to this machine and subnet mask. If no subnet mask is set or "0.0.0.0" is specified, this option permits the IPv4 address set to this machine, and the IPv4 addresses each of which only the suffix is different. This results in the same operation as for [Synchronize IP Address]. Example: When the IPv4 address of this machine is set to "192.168.17.134" and the subnet mask is set to "255.255.252.0", the range of IPv4 addresses that allow access is as follows. 192.168.16.** to 192.168.19.** For the IPv6 address, this option only permits access for the global unicast address (2000::/3). Also, filtering is carried out using the global IPv6 address set to this machine and prefix. If the prefix is not specified, filtering is carried out in the same way as when the 64-bit prefix is specified. Example: When the IPv6 address of this machine is set to "2345:1:2:3:4:5:6:7" and Prefix is set to "/64", the range of IPv6 addresses that allow access is as follows. 2345:1:2:3::0 to 2345:1:2:3:FFFF:FFFF:FFFF:FFFF • [No Filtering]: Does not use the filtering function.
[Security Warning Display Setting]	<p>To display the security warning screen if the administrator password remains set to the default or if password rules are not satisfied, set this option to ON. ON is specified by default. In some areas, OFF is specified by default.</p>

Setting	Description
[USB flash drive function settings]	<p>Specify whether to permit a function that requires the USB Port.</p> <ul style="list-style-type: none">• [Save Document]: When permitting the user to save a file in a USB flash drive, set this option to ON (default: OFF).• [Print Document]: When permitting the user to print a file from a USB flash drive, set this option to ON (default: ON).• [Scan documents to USB flash drive]: When permitting the user to save a file read from a USB flash drive in a User Box, set this option to ON (default: OFF).• [Print]: When allowing the user to print files from a USB-connected computer, set this option to ON (default: ON).

11.1.2 Changing the administrator password

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

✓ To display this page, select [Security] - [PKI Settings] - [SSL Setting] in the administrator mode to encrypt communications between your computer and **Web Connection** using SSL. For details, refer to page 11-4.

1 Select [Security] - [Administrator Password Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and enter a new administrator password (using up to 64 characters, excluding ").

2 Click [OK].

The administrator password is changed.

11.2 Encrypting Communications

11.2.1 Using an SSL/TLS communication

About the certificate of this machine

Communication between this machine and the computer can be encrypted with SSL to enhance security.

A certificate for this machine is used for the SSL communication between the machine and the computer. As a certificate was registered on this machine upon shipment, you can only enable SSL/TLS on the machine to start the SSL encrypted communication immediately after setup.

This machine can manage multiple certificates and use different certificates depending on the application (protocol). You can self-create a new certificate or install a certificate issued by the Certificate Authority (CA).

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

Usage	Description
Using the certificate registered upon shipment	The certificate that was registered on this machine upon shipment can be used as it is.
Using a self-created certificate	Create a certificate with this machine. The Certificate Authority (CA) is not required for a self-created certificate, and it can be used simply after entering necessary information for creating the certificate.
Using a certificate issued by the Certificate Authority (CA)	Create certificate signing request data in this machine, and request a trusted Certificate Authority (CA) for issuing a certificate for the machine. When the data is returned from the Certificate Authority after its review, register the data with this machine.



Reference

Importing a certificate (page 11-19)

Using different certificates depending on the application (page 11-17)

Using the certificate registered upon shipment

Select a login mode to enable SSL communication. Also select the SSL encryption strength.

Select [Security] - [PKI Settings] - [SSL Setting] in administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Mode using SSL/TLS]	Select a login mode to establish SSL communications (default: [None]). <ul style="list-style-type: none"> [Admin. Mode]: Establishes SSL communications in the administrator mode only. [Admin. Mode and User Mode]: Establishes SSL communications in both the administrator mode and user mode. [None]: Does not establish SSL communications.
[Encryption Strength]	Select the SSL encryption strength (default: [AES-256, 3DES-168, RC4-128]).
[SSL/TLS Version Setting]	Select the version of the SSL to be used.

Self-creating a certificate

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

- 1 Select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Create and install a self-signed Certificate.] in administrator mode of **Web Connection**, and enter information required for creating a certificate, then click [OK].

The certificate is created and installed on this machine. It may take several minutes to create a certificate.

Setting	Description
[Common Name]	Displays the IP address of this machine.
[Department]	Enter an organization or association name (using up to 63 ASCII characters).
[Account Name]	Enter the organization unit name (using up to 63 ASCII characters). You can also specify a null.
[Locality]	Enter the locality name (using up to 127 ASCII characters).
[State/Province]	Enter the state or province name (using up to 127 ASCII characters).
[Country]	Enter the country name. As the country name, specify a country code defined in ISO03166 (using up to two ASCII characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU
[Admin. E-mail Address]	Enter the E-mail address of the administrator of this machine (using up to 128 characters, excluding spaces). If the E-mail address of the administrator was already registered from [System Settings] - [Machine Setting], this field displays the registered E-mail address.
[Validity Start Date]	Displays the starting date of the certificate validity period. Displays the date and time of this machine when this screen is displayed.
[Validity Period]	Enter the validity period of a certificate with the number of days that have elapsed since the starting date.
[Encryption Key Type]	Select a type of encryption key.

- 2 When the certificate has been installed, enable SSL communication (page 11-4).

Requesting the Certificate Authority for issuing a certificate

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

- 1 Select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Request a Certificate] in administrator mode of **Web Connection**, and enter information required for issuing a certificate, then click [OK].

The certificate signing request data to be sent to the Certificate Authority is created.

Setting	Description
[Common Name]	Displays the IP address of this machine.
[Department]	Enter an organization or association name (using up to 63 ASCII characters).
[Account Name]	Enter the organization unit name (using up to 63 ASCII characters). You can also specify a null.
[Locality]	Enter the locality name (using up to 127 ASCII characters).
[State/Province]	Enter the state or province name (using up to 127 ASCII characters).
[Country]	Enter the country name. As the country name, specify a country code defined in ISO03166 (using up to two ASCII characters). United States: US, Great Britain: GB, Italy: IT, Australia: AU, The Netherlands: NL, Canada: CA, Spain: ES, Czech Republic: CZ, China: CN, Denmark: DK, Germany: DE, Japan: JP, France: FR, Belgium: BE, Russia: RU
[Admin. E-mail Address]	Enter the E-mail address of the administrator of this machine (using up to 128 characters, excluding spaces). If the E-mail address of the administrator was already registered from [System Settings] - [Machine Setting], this field displays the registered E-mail address.

Setting	Description
[Encryption Key Type]	Select a type of encryption key.

- 2** Click [Save].
→ Click this button to save certificate signing request data on your computer as a file.
- 3** Send the certificate signing request data to the Certificate Authority.
When the data is returned from the Certificate Authority after its review, register the data with this machine.
- 4** Select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Install a Certificate] in administrator mode of **Web Connection**, and paste the text data sent from the Certificate Authority (CA), and then click [Install].
- 5** When the certificate has been installed, enable SSL communication (page 11-4).

11.2.2 Using IPsec communication

Configure the setting if your environment requires IPsec.

The IPsec technology prevents the falsification or leakage of data on the IP packet basis by using encryption technology. As IPsec encrypts data in the network layer, secure communication is ensured even if you use protocols in an upper layer or applications that do not support encryption.

- 1** Select [Network] - [TCP/IP Setting] - [IPsec] - [IPsec Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].
- 2** Click [Edit] from [IKEv1] or [IKEv2] in [IPsec Setting], then configure the following settings.

Setting	Description
[Encryption Algorithm]	Select the encryption algorithm to create a common key used for communication.
[Authentication Algorithm]	Select the authentication algorithm to create a common key used for communication.
[Encryption Key Validity Period]	Specify the validity period of a common key to securely create a common key used to encrypt communications (default: [28800] sec.). When this period has expired, a new key is created. This can secure the communication.
[Diffie-Hellman Group]	Select the Diffie-Hellman group (default: [Group 2]).
[Negotiation Mode]	Select the negotiation mode (default: [Main Mode]). This option is not available in [IKEv2].

- 3** From [SA] in [IPsec Setting], click [Registration] and register the Security Association (SA).
→ Up to 10 groups can be registered for the SA.

Setting	Description
[Name]	Enter the SA name (using 1 to 10 characters, excluding ").
[Encapsulation Mode]	Select the IPsec operation mode (default: [Transport]).
[Security Protocol]	Select a security protocol.
[Key Exchange Method]	Select the key replacement method to securely create a common key used to encrypt communications (default: [IKEv1]).
[Tunnel End Point]	If [Tunnel] is selected in [Encapsulation Mode], enter the IP address of the IPsec gateway that is used as a peer.
[Lifetime After Establishing SA]	Enter the lifetime of a common key used to encrypt communications (default: [3600] sec.).

Setting	Description
[IKE Setting]	<p>Configure IKE settings used for this SA. This is required when [IKEv1] or [IKEv2] is selected in [Key Exchange Method].</p> <ul style="list-style-type: none"> • [Authentication Method]: Select the authentication method. • [Local Authentication Method]: Select the authentication method of this machine when [IKEv2] is selected in [Key Exchange Method]. • [Peer Authentication Method]: Select the peer authentication method when [IKEv2] is selected in [Key Exchange Method]. • [ESN]: When applying the 64-bit extended sequence number, set this option to ON. • [Replay Detection]: When enabling replay defense, set this option to ON. • [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]: When increasing the IKE intensity, set this option to ON. Setting to ON increases the time spent for communication.

4 From [Peer] in [IPsec Setting], click [Registration] and register peers of this machine.

→ Up to 10 peers can be registered.

Setting	Description
[Peer]	When registering a peer, set this option to ON (default: OFF).
[Name]	Enter the peer name (using 1 to 10 characters, excluding ").
[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 a peer using up to 128 ASCII characters or up to 256 hexadecimal characters. Specify the same text as that for the peer.
[Key-ID String]	Enter the Key-ID to be specified for the Pre-Shared Key (using up to 128 bytes).

5 From [Protocol Setting] in [IPsec Setting], click [Registration] and specify the protocol used for IPsec communication.

→ Up to 10 protocols can be specified.

Setting	Description
[Protocol Setting]	When registering the protocol setting, set this option to ON (default: OFF).
[Name]	Enter the group name with the protocol specified (using 1 to 10 characters, excluding ").
[Protocol Identification Setting]	Select a protocol used for IPsec communication (default: [No Selection]).
[Port No.]	If [TCP] or [UDP] has been selected in [Protocol Identification Setting], specify the port number used for IPsec communication.
[ICMP Message Type]	Specify the ICMP message type when [ICMP] is selected in [Protocol Identification Setting].
[ICMPv6 Message Type]	Specify the ICMP message type when [ICMPv6] is selected in [Protocol Identification Setting].

6 Select [Network] - [TCP/IP Setting] - [IPsec] - [Enable IPsec] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].

7 In [Enable IPsec], configure the following settings.

Setting	Description
[IPsec]	When using IPsec, set this option to ON (default: OFF).

Setting	Description
[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 (default: [15] sec.).
[Cookies]	Select whether to enable the defense using Cookies against denial-of-service attacks (default: [Disable]).
[ICMP Pass]	Select whether to apply IPsec to the Internet Control Message Protocol (ICMP) (default: [Disable]). Select [Enable] to allow the ICMP packets to pass without applying IPsec to the ICMP.
[ICMPv6 Pass]	Select whether to apply IPsec to the Internet Control Message Protocol for IPv6 (ICMPv6) (default: [Disable]). Select [Enable] to allow the ICMPv6 packets to pass without applying IPsec to the ICMPv6.
[Default Action]	Select an action to be taken if no settings meet the [IPsec Policy] while IPsec communication is enabled (default: [Allow]). Select [Deny] to discard IP packets that do not meet the [IPsec Policy] settings.
[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. <ul style="list-style-type: none"> • [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). • [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). • [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. • [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

8 From [IPsec Policy] in [Enable IPsec], click [Registration], then configure the following settings.

→ IP packet conditions can be specified to pass or allow the IP packets that meet each of the conditions.

Setting	Description
[IPsec Policy]	Select whether to use the IPsec policy (default: [OFF]).
[Name]	Enter the IPsec policy name (using 1 to 10 characters, excluding ").
[Peer]	Select a peer setting. Select the setting from those registered in [Peer] in [IPsec Setting].
[Protocol Setting]	Select a protocol. Select the setting from those registered in [Protocol Setting] in [IPsec Setting].
[IPsec Setting]	Select an SA setting. Select the setting from those registered in [SA] in [IPsec Setting].
[Communication Type]	Select a direction of IPsec communication.
[Action]	Select the operation for the IP packet that matches the specified condition. <ul style="list-style-type: none"> • [Protected]: Protect the IP packets that met the conditions. • [Allow]: Do not protect the IP packets that met the conditions. • [Deny]: Discard the IP packets that met the conditions. • [Cancel]: Refuse the IP packets that met the conditions.

9 Select [IPsec] - [Communication Check], then check that a connection with a peer can be established normally by the configured setting.

→ Enter the peer's IP address into [IP Address], then click [Check Connection].

11.3 Restricting Communications

11.3.1 Restricting external accesses using the IP address

Automatically specifying the IP Address to restrict accesses

Restrict devices that can access this machine depending on the range of IP addresses.

- 1 Select [Network] - [TCP/IP Setting] - [IP Address Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IPv4 Filtering (Permit Access)]	<p>Specify an IPv4 address to allow access to this machine.</p> <ul style="list-style-type: none"> • [IPv4 Filtering (Permit Access)]: When specifying the IPv4 address that allow access, set this option to ON (default: OFF). • Range 1 to Range 5: Enter the range of IPv4 addresses that allow access using the following format. Entry example: "192.168.1.1 - 192.168.1.10" If a single IPv4 address is allowed to access, you can only enter the address in one side of the range.
[IPv4 Filtering (Deny Access)]	<p>Specify an IPv4 address to deny access to this machine.</p> <ul style="list-style-type: none"> • [IPv4 Filtering (Deny Access)]: When specifying the IPv4 address that deny access, set this option to ON (default: OFF). • Range 1 to Range 5: Enter the range of IPv4 addresses that deny access using the following format. Entry example: "192.168.1.1 - 192.168.1.10" To deny access from a single IPv4 address, you can only enter the address in one side of the range.
[IPv6 Filtering (Permit Access)]	<p>Specify an IPv6 address to allow access to this machine.</p> <ul style="list-style-type: none"> • [IPv6 Filtering (Permit Access)]: When specifying the IPv6 address that allow access, set this option to ON (default: OFF). • Range 1 to Range 5: Enter the IPv6 address and prefix length to specify the range of IPv6 addresses that allow access.
[IPv6 Filtering (Deny Access)]	<p>Specify an IPv6 address to deny access to this machine.</p> <ul style="list-style-type: none"> • [IPv6 Filtering (Deny Access)]: When specifying the IPv6 address that deny access, set this option to ON (default: OFF). • Range 1 to Range 5: Enter the IPv6 address and prefix length to specify the range of IPv6 addresses that deny access.

- 2 Select [Network] - [TCP/IP Setting] - [Filtering Type] - [IP Address Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].

Automatically Auto the IP Address to restrict accesses

If the quick IP filtering function is employed, the range of the IP addresses accessible to this machine is set automatically, enabling you to quickly specify access restrictions.

- 1 Select [Network] - [TCP/IP Setting] - [Quick IP Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Quick IP Filtering]	<p>Select the method to specify the IP address for which access is restricted (default: [Synchronize IP Address]).</p> <ul style="list-style-type: none"> • [Synchronize IP Address]: For the IPv4 address, this option only permits access for the IPv4 address set to this machine, and the IPv4 addresses of which the high-order 3 bytes are the same. Example: When the IPv4 address of this machine is set to "192.168.0.134", the range of IPv4 addresses that allow access is as follows. 192.168.0.0 to 192.168.0.255 For the IPv6 address, this option only permits access for the global unicast address (2000::/3). Also, this option only permits access for the IPv6 address set to this machine, and the IPv6 addresses of which the high-order 64 bits are the same. Example: When the IPv6 address of this machine is set to "2345:1:2:3:4:5:6:7", the range of IPv6 addresses that allow access is as follows. 2345:1:2:3::0 to 2345:1:2:3:FFFF:FFFF:FFFF:FFFF • [Synchronize Subnet Mask]: For the IPv4 address, this option only permits access for IPv4 addresses that belong to the same network using the IPv4 address set to this machine and subnet mask. If no subnet mask is set or "0.0.0.0" is specified, this option permits the IPv4 address set to this machine, and the IPv4 addresses each of which only the suffix is different. This results in the same operation as for [Synchronize IP Address]. Example: When the IPv4 address of this machine is set to "192.168.17.134" and the subnet mask is set to "255.255.252.0", the range of IPv4 addresses that allow access is as follows. 192.168.16.** to 192.168.19.** For the IPv6 address, this option only permits access for the global unicast address (2000::/3). Also, filtering is carried out using the global IPv6 address set to this machine and prefix. If the prefix is not specified, filtering is carried out in the same way as when the 64-bit prefix is specified. Example: When the IPv6 address of this machine is set to "2345:1:2:3:4:5:6:7" and Prefix is set to "/64", the range of IPv6 addresses that allow access is as follows. 2345:1:2:3::0 to 2345:1:2:3:FFFF:FFFF:FFFF:FFFF • [No Filtering]: Does not use the filtering function.

- 2 Select [Network] - [TCP/IP Setting] - [Filtering Type] - [Quick IP Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].

Tips

- If the quick IP filtering function is used, the range of IP addresses for which access is to be restricted is specified automatically. To manually specify the range of IP addresses for which access is to be restricted, set [Network] - [TCP/IP Setting] - [IP Address Filtering] or [Packet Filtering] instead of using [Quick IP Filtering].

11.3.2 Restricting Packet Transfer

Registering filter

Restrict a reception of packets sent to the machine depending on the source address. This function also restricts sending depending on the destination address.

- 1 Select [Network] - [TCP/IP Setting] - [Packet Filtering] - [Registration] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Address Type]	Select the address type for the target packet.
[Start Address]	<p>Specify the range of addresses to be filtered.</p> <ul style="list-style-type: none"> • If you select [IPv4] in [Address Type], specify the starting address of the IPv4 address range. You can specify the broadcast address or multicast address as needed. Format: "*. *.*.*" For "*", specify the value between 0 and 255. If necessary, you can specify the address range depending on the IPv4 address and prefix length. In this case, the address range that matches bits in the prefix part is targeted for filtering. Format: "*. *.*.*@" For "*", specify the value between 0 and 255. For "@", specify the value between 1 and 31. • If you select [IPv6] in [Address Type], specify the address range depending on the IPv6 and prefix length. You can specify the multicast address as needed. Format: "*****.*****.*****.*****.*****.*****.*****.*****@" For "*", specify a hexadecimal number. For "@", specify the value between 1 and 127. • If you select [MAC Address] in [Address Type], specify the MAC address. In this case, only a single address is targeted for filtering. You cannot specify the address range. Format: "*****.*****.*****.*****" For "*", specify a hexadecimal number.
[Finish Address]	<p>When you select IPv4 in [Address Type], specify the ending address of the IPv4 address range to be filtered. If you skip [Finish Address], only the address specified in [Start Address] is targeted for filtering. Format: "*. *.*.*" For "*", specify the value between 0 and 255. When you specify the prefix length of the IPv4 address in [Start Address], you cannot specify the ending address.</p>
[Receive/Send]	<p>Select the communication direction of the target packet.</p> <ul style="list-style-type: none"> • [Receive]: Restricts packets received by the machine depending on the source address. • [Send]: Restricts packets sent by the machine depending on the destination address. <p>If you select [MAC Address] in [Address Type], you cannot set to [Send].</p>
[Allow/Denied]	Select whether to allow or reject a communication of the target packet.

- 2 Select [Network] - [TCP/IP Setting] - [Packet Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TX/RX address out of range]	Select whether to allow sending or receiving a packet to which the registered filter is not applied (default: [Allow]).

- 3 Select [Network] - [TCP/IP Setting] - [Filtering Type] - [Packet Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [OK].

NOTICE

*Note that this machine cannot be connected using **Web Connection** from your computer if sending or receiving is not allowed for your computer's address.*

Exporting filter

Export packet filtering settings to a file.

This function is available when you want to edit filter settings on a computer.

1 Select [Network] - [TCP/IP Setting] - [Packet Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [Export].

2 Click [Start].

This starts exporting of the configuration file.

Importing filter

Import packet filtering settings from a file.

This option is available to edit filter settings exported from the machine on the computer before importing them.

1 Select [Network] - [TCP/IP Setting] - [Packet Filtering] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [Import].

2 Specify the configuration file to import.

3 Click [Start].

The import result is displayed.

Recording logs

You can acquire logs of packets for which receiving or sending is rejected by filtering.

Select [Network] - [TCP/IP Setting] - [Packet Filtering] - [Log settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Log Setting]	Select whether to record packet filtering logs (default: [Disable]).

Downloading logs

Write packet filtering logs to a USB flash drive.

1 Select [Network] - [TCP/IP Setting] - [Packet Filtering] - [Log settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Number of Lines]	Specify the number of logs to be written (default: [1000]).

2 Click [Start].

3 Click [OK].

4 Click [Download].

This starts downloading of the log file.

11.3.3 Restricting E-mail recipients using the domain

Restrict the domain of the recipient to send an E-mail, Internet fax, or IP address fax.

Security enhancement is realized by restricting a transmission from this machine to an external device.

Select [Network] - [Domain Send Operation Restriction Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Domain Send Operation Restriction Setting]	Select whether to limit the recipient domain (default: [Do Not Limit]).
[Limit Type]	Select a method to restrict the recipient domain. <ul style="list-style-type: none"> To specify a domain to be permitted, select [Permitted TX]. To specify a domain to be rejected, select [Send Deny].
[Permitted TX List]	Specify the domain to be permitted as the recipient when [Permitted TX] is selected in [Limit Type]. Select a recipient domain key, then enter the IP address or domain name of the domain (using up to 255 bytes). <ul style="list-style-type: none"> Symbol "?" is recognized as any one character. Symbol "*" is recognized as any characters of 0 or more.
[Send Deny List]	Specify the domain to be rejected as the recipient when [Send Deny] is selected in [Limit Type]. Select a recipient domain key, then enter the IP address or domain name of the domain (using up to 255 bytes). <ul style="list-style-type: none"> Symbol "?" is recognized as any one character. Symbol "*" is recognized as any characters of 0 or more.
[Limitation check of Shared address]	Check whether destinations with transmission disabled are included in the destinations registered on this machine.

Tips

- If [Permitted TX] is selected in [Limit Type], the setting of [Send Deny List] is deleted.
- If [Send Deny] is selected in [Limit Type], the setting of [Permitted TX List] is deleted.

11.4 Restricting network or USB connections

11.4.1 Connecting this machine to IEEE802.1X authentication environment

When IEEE802.1X authentication is installed in your environment, configure settings to use IEEE802.1X authentication on this machine.

Using IEEE802.1X authentication enables you to only connect devices authorized by administrators to the LAN environment. Devices that are not authenticated will not be allowed to even join the network, and this ensures rigid security.

Select [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IEEE802.1X Authentication Setting]	When using IEEE802.1X authentication, set this option to ON (default: OFF).
[Supplicant Setting]	Configure settings to operate this machine as a supplicant (client to be authenticated). For details on settings, refer to the settings of [Supplicant Setting] shown below.

Settings of [Supplicant Setting]

Setting	Description
[User ID]	Enter a user ID (using up to 128 characters). This user ID is used for all EAP-Type options.
[Password]	Enter a password (using up to 128 characters). The password is used for all EAP-Type options other than [EAP-TLS].
[EAP-Type]	Select the EAP authentication method (default: [OFF]). <ul style="list-style-type: none"> [Depend on Server]: The EAP-Type provided by the authentication server will be used for authentication. Configure the supplicant settings as required for this machine according to the EAP-Type provided by the authentication server. Do not select [OFF].
[EAP-TTLS]	Configure the EAP-TTLS settings if [EAP-Type] is set to [EAP-TTLS] or [Depend on Server]. <ul style="list-style-type: none"> [anonymous]: Enter the user ID used for EAP-TTLS authentication (using up to 128 characters). [Inner Authentication Protocol]: Select an internal authentication protocol for EAP-TTLS.
[Server ID]	To verify CN of the certificate, enter the server ID (using up to 64 characters).
[Client Certificates]	Select whether to encrypt the authentication information using a certificate for this machine. This setting can be configured if the following conditions are satisfied: <ul style="list-style-type: none"> The certificate is registered on this machine [EAP-TLS], [EAP-TTLS], [PEAP], or [Depend on Server] is selected from [EAP-Type].
[Encryption Strength]	If [EAP-TLS], [EAP-TTLS], [PEAP], or [Depend on Server] is selected from [EAP-Type], select an encryption strength for encryption by TLS. <ul style="list-style-type: none"> [Mid]: Keys that are more than 56 bits in length are used for communication. [High]: Keys that are more than 128 bits in length are used for communication.
[Certificate Verification Level Settings]	To verify the certificate, select items to be verified. <ul style="list-style-type: none"> [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine.

Setting	Description
[Network Stop Time]	When specifying the delay time between the start of an authentication process and the end of network communication, set this option to ON (default: OFF). <ul style="list-style-type: none"> [Stop Time]: Enter the delay time (sec.). If an authentication process does not succeed within the specified time, all network communication will stop. To restart the authentication process after network communication stopped, reboot this machine.

Tips

- You can select [Network] - [IEEE802.1X Authentication Setting] - [IEEE802.1X Authentication Trial] to confirm the current authentication status. The authentication process can be activated for the authentication server.
- This setting is not displayed on **Web Connection** when [Network I/F Configuration] is set to [Wireless Only]. In a wireless-only environment, if [WPA-EAP(AES)] or [WPA2-EAP(AES)] is selected in [Wireless Network Setting] - [Authentication/Encryption Algorithm], select [Utility] - [Administrator] - [Network] - [IEEE802.1x Setting] on the screen of this machine, and configure the supplicant settings.

11.4.2 Restricting functions using the USB port

Specify whether to permit a function that requires the **USB Port**.

Select [Security] - [USB port connection permission setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Set All]	Select whether to restrict all the functions using the USB Port , or configure a setting for each function (default: [Detail Setting]).

If [Detail Setting] is selected in [Set All], configure the following settings.

Setting	Description
[Authentication Device]	When allowing a connection with the Authentication Unit , select [Allow] (default: [Allow]).
[External Keyboard]	When allowing the user to connect an external keyboard, set this option to ON (default: ON).
[USB flash drive (User)]	Specify whether to allow the use of USB memory for functions to be used by the user (default: [Individual Settings]). <ul style="list-style-type: none"> [Save Document]: When permitting the user to save a file in a USB flash drive, set this option to ON (default: OFF). [Print Document]: When permitting the user to print a file from a USB flash drive, set this option to ON (default: ON). [Scan documents to USB flash drive]: When permitting the user to save a file read from a USB flash drive in a User Box, set this option to ON (default: OFF).
[USB flash drive (Administrator)]	Specify whether to allow the use of USB memory for functions to be used by the administrator (default: [Individual Settings]). <ul style="list-style-type: none"> [Write the Configuration from USB]: When allowing the user to change the settings of this machine by loading the configuration file saved in a USB flash drive, set this option to ON (default: ON).
[USB flash drive (Service)]	Specify whether to allow the use of USB memory for functions to be used by the service engineer (default: [Individual Settings]). <ul style="list-style-type: none"> [Firmware Update]: When allowing firmware updating using a USB flash drive, set this option to ON (default: ON). [Storage data backup]: When allowing the backup or restoration of the storage on this machine, set this option to ON (default: OFF).
[PC Connect]	Specify whether to enable to print files from a USB-connected computer (default: [Individual Settings]). <ul style="list-style-type: none"> [Print]: When allowing the user to print files from a USB-connected computer, set this option to ON (default: ON).


Tips

- If [USB flash drive (Administrator)] is set to OFF, [TPM Key Backup] is set to OFF in addition to the functions that can be set in [Individual Settings]. Also, USB memory is not available for the following functions. [TX Operation Log Output], [Main Menu Display Settings], [License Settings], [Authorization function Setting], import, export, or log storage of [Packet Filtering] in the main unit, import or export of **Web Connection** via the Web browser of the main unit
- If [USB flash drive (Service)] is set to OFF, some functions are restricted in addition to the functions that can be set in [Individual Settings].

11.4.3 Restricting the firmware update using a USB memory with a password

Configure settings to restrict the service representative's firmware update using a USB flash drive.

Select [Security] - [Firmware Update (USB) Permission Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[USB Update]	<p>Select the method to allow the service engineer to update firmware using a USB flash drive (default: [USB port connection permission preference setting]).</p> <ul style="list-style-type: none"> • [Password Priority]: Prompts the user to enter the password. Enter the required password in [Password] (using up to 20 characters). When the entered password matches the password specified here, firmware update is permitted. • [USB port connection permission preference setting]: Follows the Allow or Restrict setting that is selected in [USB flash drive (Service)] - [Firmware Update] of [Security] - [USB port connection permission setting].

11.5 Managing the certificates for this machine

11.5.1 Using Different Certificates Depending on the Application

This machine can manage multiple certificates and use different certificates depending on the application (protocol).

Click [Security] - [PKI Settings] - [Protocol Setting] - [Register] in administrator mode of **Web Connection**, then select a certificate to be used for the protocol.

Protocol	Application
[SSL]: [http Server]	If this machine is used as an http server, it encrypts transmission from a client to the machine. For example, it is used for the following application. <ul style="list-style-type: none"> • Accessing Web Connection via HTTPS • Printing via IPPS
[SSL]: [E-Mail Transmission (SMTP)]	If this machine is used as an SMTP client, it submits a certificate of the machine according to a request from the E-mail server (SMTP).
[SSL]: [E-mail RX (POP)]	If this machine is used as an POP client, it submits a certificate of the machine according to a request from the E-mail server (POP).
[SSL]: [TCP Socket]	If this machine is used as a TCP Socket client, it submits a certificate of the machine according to a request by the TCP Socket server.
[SSL]: [LDAP]	If this machine is used as an LDAP client, it submits a certificate of the machine according to a request by the LDAP server.
[SSL]: [WebDAV Client]	If this machine is used as a WebDAV client, it submits a certificate of the machine according to a request by the WebDAV server.
[SSL]: [OpenAPI]	If this machine is used as an OpenAPI server, it encrypts transmission from an OpenAPI client to the machine.
[SSL]: [Web Service]	If this machine is used as a Web service server, it encrypts transmission from a client to the machine. This option is used when your Windows computer accesses the machine via HTTPS.
[IEEE802.1X]	If this machine is used as an IEEE802.1X authentication client, it is used for the following applications: <ul style="list-style-type: none"> • Encrypting communication if this machine is authenticated by the IEEE802.1X server via EAP-TLS. • Submitting a certificate of this machine upon request by the server via EAP-TTLS or EAP-PEAP.
[S/MIME]	When sending an S/MIME E-mail, it attaches a certificate of this machine to ensure the sender of the E-mail.
[SSL]: [IPsec]	Used to activate IPsec communication on this machine.
[SSL]: [Remote Panel]	When the screen of this machine is operated remotely with the dedicated software, it is used for the following applications: <ul style="list-style-type: none"> • Submitting a certificate of this machine, in the client settings, according to a request by the server on which the dedicated software has been installed. • Encrypting communication, in the server settings, from a client viewing the screen of this machine to the machine.
[SSL]: [ThinPrint]	If this machine is used as a ThinPrint client, it submits a certificate of the machine according to a request by the ThinPrint server (.print Engine). After this machine validates the certificate, the ThinPrint server performs encrypted communication. Specify the certificate of this machine to use for communication that is issued by the Certificate Authority (CA).

Tips

- If the certificate to be used was registered, a "*" mark appears for the protocol.
- Clicking [Edit] changes the registered certificate or check details of the certificate.
- Clicking [Delete] deletes the registration information.

11.5.2 Exporting a certificate

Exporting information to your computer

The certificate for this machine can be exported to your computer. You can export the certificate if you wish to manage it on the computer or transfer it to other device.

- 1** Select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Export Certificate] in administrator mode of **Web Connection**, then click [OK].
- 2** In [Export Destination], select [Export to PC].
- 3** Enter the password (using up to 32 characters), then click [OK].
 - The entered password is required for importing the certificate.
- 4** Click [Download].
 - The certificate for this machine is saved to the computer.

Exporting information to an SMB sharing folder

The certificate for this machine can be exported to an SMB sharing folder. You can export the certificate if you wish to manage it on the computer or transfer it to other device.

- 1** Select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Export Certificate] in administrator mode of **Web Connection**, then click [OK].
- 2** In [Export Destination], select [Export to SMB].
- 3** Enter the password (using up to 32 characters), then click [OK].
 - The entered password is required for importing the certificate.
- 4** Enter the information to connect to the SMB server.

Setting	Description
[Server Address]	Enter the SMB server address. Example of entry: "192.168.1.1"
[User Name]	Enter the user name to log in to the SMB server (using up to 64 characters).
[Password]	Enter the password to log in to the SMB server (using up to 64 characters).

- 5** Click [Connection].
 - The folder selection page is displayed.
- 6** Select a folder to export a certificate from, then click [OK].
 - The certificate of this machine is saved in the selected SMB sharing folder.

11.5.3 Importing a certificate

Importing information from your computer

The exported certificate can be imported on this machine.

- 1 Select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Import Certificate] in administrator mode of **Web Connection**, then click [OK].
- 2 Select [Select from PC], and specify the certificate to import.
- 3 Enter the password (using up to 32 characters), then click [OK].
 - Enter the password specified when exporting the certificate.
 The import result is displayed.

Importing information from an SMB sharing folder

The exported certificate can be imported on this machine.

- 1 Select [Security] - [PKI Settings] - [Device Certificate Setting] - [New Registration] - [Import Certificate] in administrator mode of **Web Connection**, then click [OK].
- 2 Select [Select from SMB List], then click [SMB List].
- 3 Enter the information to connect to the SMB server.

Setting	Description
[Server Address]	Enter the SMB server address. Example of entry: "192.168.1.1"
[User Name]	Enter the user name to log in to the SMB server (using up to 64 characters).
[Password]	Enter the password to log in to the SMB server (using up to 64 characters).

- 4 Click [Connection].
The folder selection page is displayed.
- 5 Specify the certificate to be imported, then click [OK].
- 6 Enter the password (using up to 32 characters), then click [OK].
 - Enter the password specified when exporting the certificate.
 The import result is displayed.

11.5.4 Deleting a certificate

A certificate for this machine can be deleted if necessary.

Select [Security] - [PKI Settings] - [Device Certificate Setting] - [Setting] - [Remove a Certificate] in administrator mode of **Web Connection**, then click [OK].

Tips

- The certificate specified as default cannot be deleted. Before deleting it, specify another certificate as default.

11.5.5 Verifying a certificate for peer

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

To check the expiration of certificate, register the URL of the Online Certificate Status Protocol (OCSP) service.

Select [Security] - [Certificate Verification Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Certificate Verification Settings]	When verifying the reliability of the peer's certificate, set this option to ON (default: ON).
[Timeout]	Change the time-out time of certificate expiration confirmation if necessary (default: [30] sec.).
[OCSP Service]	Using the Online Certificate Status Protocol (OCSP) enables you to check online whether or not the certificate is expired. When using the OCSP service, set this option to ON. Also, enter the URL of the OCSP service (using up to 511 characters). If [URL] is left blank, the URL of the OCSP service embedded in the certificate will be used.
[Proxy Settings]	When a proxy server is installed in your environment, register the proxy server. <ul style="list-style-type: none"> [Proxy Server Address]: Enter the proxy server address. Use one of the following formats. Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" [Proxy Server Port Number]: If necessary, change the proxy server port number (default: [8080]). [User Name]: Enter the user name used for proxy authentication (using up to 63 characters). [Password]: Enter the password for proxy authentication (using up to 63 characters). [Address not using Proxy Server]: Enter an address that does not use the proxy server as needed.

11.5.6 Importing external certificates used for validating the chain

Types of external certificates that can be imported

Import external certificates used for validating the certificate chain (certificate path) in this machine.

The following certificates can be imported on this machine.

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

How to import

Import external certificates used for validating the certificate chain (certificate path) in this machine.

- 1** Select [Security] - [PKI Settings] - [External Certificate Setting] in administrator mode of **Web Connection**, then click [New Registration].
 - To change certificates to be shown in the list, select a certificate you wish to change, and click [Changes the display].
 - To delete the registered certificate, click [Delete].
- 2** Select a certificate to be imported from your computer or the SMB sharing folder.
 - [Select from PC]: Select a certificate to be imported from your computer.
 - [Select from SMB List]: Click [SMB List], then select a certificate to be imported from the SMB sharing folder.
- 3** Click [OK].

The import result is displayed.

11.6 Monitoring or Restricting User Operations

11.6.1 Disabling user's registration/change operations

Configure settings to restrict change or deletion operations for users.

Select [Security] - [Restrict User Access] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Registering and Changing Addresses]	Select whether to allow the user to register or change destinations (default: [Allow]).
[Biometric/IC Card Information Registration]	When allowing the user to register or when deleting the user's biometric or card information, set this option to ON (default: OFF).
[Changing the "From" Address]	Select whether to allow the user to change the sender E-mail address ("From" address) (default: [Allow] (without user authentication), [Login User Address] (with user authentication)). <ul style="list-style-type: none"> [Allow]: Allows the user to change the "From" address. [Admin. E-mail Address]: Prohibit the change of "From" address and use the administrator's E-mail address. [Login User Address]: Prohibit changing of the "From" address and use user's E-mail address. Administrator's E-mail address is used if the user's E-mail address has not been registered.
[Synchronize User Authentication / Account Track By User]	When allowing the user to change the setting for synchronization between user authentication and account track, set this option to ON (default: ON). This setting is displayed when [User Auth/Account Track] - [Authentication Type] - [Synchronize User Authentication / Account Track] is set to [Synchronize by User].
[Restrict Program Function Setting]	When prohibiting users from using the copy program or scan/fax program, set this option to ON (default: OFF).
[Prohibit continuous selection of broadcast destinations.]	When displaying the confirmation screen to successively select destinations, set this option to ON (default: ON). This setting is available when [Utility] - [Administrator] - [Security] - [Restrict User Access] - [Multiple Addresses Restriction Setting] is set to OFF on the screen of this machine.
[Allow full selection of group destinations.]	When displaying the [Select All] button on the Group destination specification screen, set this option to ON (default: OFF). This setting is available when [Utility] - [Administrator] - [Security] - [Restrict User Access] - [Multiple Addresses Restriction Setting] is set to OFF on the screen of this machine and the [Prohibit continuous selection of broadcast destinations.] to ON.
[Changing Job Priority]	When allowing the user to change the job priority order, set this option to ON (default: ON).
[Delete Other User Jobs]	When allowing the user to delete another user's job, set this option to ON (default: OFF).
[Changing Zoom Ratio]	When allowing the user to change the registered zoom ratio, set this option to ON (default: ON).
[Register and Change Overlay]	When allowing the user to overwrite or delete a registered overlay image, set this option to ON (default: ON).

11.6.2 Restricting user's Web browser setting operations

Specify whether to allow the user to change user data settings on the Web browser.

Select [Security] - [Security Details] - [Web browser setting change] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Web browser setting change]	Specify the type of the user who can change the user data setting of the Web browser (default: [Administrator only]). Selecting [Administrator + User] allows you to configure the following Web browser settings using the registered user's privileges. <ul style="list-style-type: none"> • Home page • Start up • Web data (Cookie, Web Storage, or Indexed Database) • Authentication information

Tips

- This function is available when the Web browser function is enabled.

11.6.3 Saving the operation log of the control panel

Configure settings to obtain an operation log when scanning or sending a fax as a send operation log. This helps to analyze a security issue if one occurs.

Select [Security] - [TX Operation Log Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TX Operation Log Setting]	Select whether to acquire transmission logs (default: [Do Not Save]).
[TX Operation Log Erase]	Erases the accumulated TX operation logs.

Tips

- To print the saved sending operation logs or save them in a USB flash drive, select [Utility] - [Administrator] - [System Settings] - [List/Counter] - [TX Operation Log Output] on the screen of this machine.

12 **Managing the Machine Status**

12 Managing the Machine Status

12.1 Managing the machine power for power saving

12.1.1 Setting the Power key/Power save function

Configure the settings on how to use the **Power** key and the machine action in Power Save mode.

Select [Maintenance] - [Timer Setting] - [Power Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Low Power Mode Setting]	Change the time required to automatically shift to the Low Power mode after you did not operate this machine (default: [15] minutes, available range: [2] to [60] minutes). In the Low Power mode, the display of the Touch Panel is turned off to reduce power consumption.
[Sleep Mode Setting]	Change the time required to automatically shift to the Sleep mode after you did not operate this machine (default: [15] minutes, available range: [2] to [60] minutes). Sleep mode provides a greater power saving effect than the Low Power mode. However, the time required to return to the normal mode is longer than the time required to recover from the Low Power mode.
[Power Consumption in Sleep Mode]	Select whether to reduce the power consumption in the Sleep mode (default: [High]). <ul style="list-style-type: none"> [High]: Further reduces the power consumption in the Sleep mode. However, this machine cannot be returned from the Sleep mode when the door of the main unit is opened or closed or when the original is loaded. [Enabled]: Reduces the power consumption in the Sleep mode. [Disabled]: Select this option when a smooth network communication is not established while [High] or [Enabled] is enabled.
[Power Save Settings]	Select the power save mode (Low Power or Sleep) to be switched when the Power key on the Control Panel is pressed (default: [Low Power]).
[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 (default: [Power Save]). <ul style="list-style-type: none"> [Sub Power OFF]: Press the Power key briefly to turn the sub power off. If the Power key is held down, the power save mode is switched to the ErP Auto Power Off mode (similar to main power off mode), which provides a greater power saving effect than when the sub power is turned off. [Power Save]: Press the Power key briefly to shift to the Power Save mode. Hold down the Power key to turn the sub power off.
[Enter Power Save Mode]	When this machine receives a print job from a fax machine or computer in the Power Save mode, select the timing to switch to the Power Save mode after the print job has ended (default: [Immediately]). <ul style="list-style-type: none"> [Normal]: Switches to the Power Save mode based on the time specified in [Low Power Mode Setting] or [Sleep Mode Setting]. [Immediately]: Switches to the Power Save mode immediately after a print job has ended.
[Power Saving Fax/Scan]	Select whether to give priority to the power saving when returning from the Sleep or sub power off mode to a mode other than the copy mode (default: [Standard]). When returning to a mode that does not involve printing, such as scan/fax mode, power consumption can be reduced by not adjusting the temperature of the Fusing Unit on this machine. This option is available when an item other than [Copy] is selected in [Screen to display after Reset] of [System auto reset] ("User's Guide[Descriptions of Functions/Utility Keys]/[Administrator]"). <ul style="list-style-type: none"> [Power Save]: The temperature of Fusing Unit is not adjusted when the machine returns to the normal mode. [Standard]: The temperature of Fusing Unit is adjusted when the machine returns to the normal mode.

**Reference**

Switching to Power Save Mode Using the **Power** Key ("User's Guide[Introduction]/[Turning the Power On or Off]")

12.1.2 Switching to Power Save mode at specified time (Weekly Timer)

Configure settings to automatically switch between power save and normal mode using the weekly timer function.

To use the weekly timer, specify the schedule for switching between power save and normal modes. Optionally, you can use the tracking function that automatically sets a schedule to fit your office usage.

Select [Maintenance] - [Timer Setting] - [Weekly Timer Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Use Weekly Timer]	<p>Configure the settings to use the weekly timer function.</p> <ul style="list-style-type: none"> [Use Weekly Timer]: When using the weekly timer function, set this option to ON (default: ON). [Power Save Mode Setting]: Select the power save mode to which the machine enters based on the weekly timer (default: [ErP Auto Power OFF]). [ErP Auto Power OFF]: A mode that provides a higher more effective power saving effect. In this mode, you cannot receive all jobs. [Sleep]: This mode has a lower power saving effect than the [ErP Auto Power OFF] mode; however, it allows you to receive print jobs from a fax machine or computer. The received jobs are printed when the machine returns to the normal mode. [Date Setting]: Configure the day to apply the weekly timer on. Specify the year and month to display the calendar, and select the desired day. Optionally, you can collectively configure the appropriate days for each day of the week with [Daily Setting]. [Work Time Setting]: Specify the time for switching to the power save mode ([OFF Time]) and the time for returning to the normal mode ([ON Time]) for each day of the week.
[Use Power Save]	<p>When this machine is in normal mode to set the weekly timer, specify the time zone to temporarily switch the machine to sleep mode.</p> <ul style="list-style-type: none"> [Use Power Save]: When specifying the time zone to temporarily switch the machine to sleep mode, set this option to ON (default: OFF). [Power Save Start Time]: Specify the time for the machine to enter the sleep mode. [Power Save End Time]: Specify the time to return the machine to the normal mode.
[Use Overtime Password]	<p>Configure the setting for prompting the machine's user to enter the overtime password when this machine is shifting to power save mode by the weekly timer.</p> <ul style="list-style-type: none"> [Use Overtime Password]: When prompting the user to enter the overtime password, set this option to ON (default: OFF). Also, enter the overtime password to be requested to the machine's user (using up to eight characters).

Setting	Description
[Enable Tracking Function]	<p>Configure the setting to use the tracking function that automatically adjusts the weekly timer On or Off time to fit the user's operating conditions or office usage status. When the tracking function is used, the inactive rate is calculated for each time zone based on the machine usage status over the past four weeks. Based on the inactive rate thus calculated, the (inactive) time zone in which the machine is not operating is determined, and the result is reflected to the weekly timer On or Off time.</p> <ul style="list-style-type: none"> [Enable Tracking Function]: When using the tracking function, set this option to ON (default: ON). [Auto Standby Adjustment Level]: Select the judgment criteria for non-operation, which is defined to be less than the minimum active rate requirement of the machine based on the calculated inactive rate (default: [Level 3]). If the inactive rate exceeds the selected value in a certain time zone, it is judged that the machine is inactive for the time zone. You can select the [Auto Standby Adjustment Level] from the following five levels. The higher the level, the more likely it is that the machine will be judged to be inactive. <ul style="list-style-type: none"> [Level 1]: The inactive rate is 71% or more. [Level 2]: The inactive rate is 51% or more. [Level 3]: The inactive rate is 41% or more. [Level 4]: The inactive rate is 31% or more. [Level 5]: The inactive rate is 10% or more. [Display ON/OFF Time]: Displays the switching times to enter the power save mode ([OFF Time]) and to the normal mode ([ON Time]) set by the tracking function. [Clear Usage Data]: Deletes data related to the usage status of this machine and resets the values for [OFF Time] and [ON Time] that have been automatically set.

12.1.3 Recovering this machine from ErP Auto Power Off mode

Configure the setting to recover the machine from the ErP Auto Power Off mode via the network when the machine is connected to a mobile terminal.

Select [Network] - [Awake from ErP] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Awake from ErP]	<p>Select the method to return the machine from the ErP Auto Power Off mode (default: [Awake with Magic Packet]).</p> <ul style="list-style-type: none"> [Awake with Magic Packet]: The machine returns from the ErP Auto Power Off mode when receiving a magic packet. [Awake with ARP + Unicast Communication]: The machine returns from the ErP Auto Power Off mode when receiving a unicast communication packet.

Tips

- This function is not available when the machine is used in the IPv6 environment.
- This function is not available when [Network] - [Network I/F Configuration] is set to [Wireless Only].
- To recover the machine from the ErP Auto Power Off mode using **Remote Access** on a mobile terminal, connect this machine to the mobile terminal once in advance.

12.2 Customizing the Control Panel environment

12.2.1 Changing the default operation screen

Change the default operation screen to be displayed when this machine is started.

Select [System Settings] - [Def. operation mode set.] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Def. operation mode set.]	Select the default operation screen to be applied when this machine is started (default: [Basic Style]). <ul style="list-style-type: none"> [Basic Style]: Standard operation screen. This mode provides the simple screen layout and instinctive operability. [Classic Style]: Operation screen adopted in the previous models. Some functions are available only in classic style.
[Press Menu key to access Style]	Select the operation screen that is displayed when the home key is tapped (default: [Default setting of Style]).

Tips

- If Enhanced Security Mode is enabled, the initial operation screen is set to the classic style, and this setting is not displayed.

12.2.2 Changing the order to sort the communication list on the Job History screen

Configure settings to display the job history screen.

Select [System Settings] - [Job History Display Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Communication history sort method]	Specify the sort order of [Comm. List] on the [Job List] screen. Select whether to sort in the order of which the registration date/time is earlier or later (default: [New]).

12.2.3 Changing the functions to be assigned to the classic-style side menu

Change the functions to be assigned to the classic-style side menu.

Select [System Settings] - [Registered Key Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and select the functions to assign.

The following shows the default settings.

- [Register Key 1]: [Enlarge Display]
- [Register Key 2]: [Guidance]
- [Register Key 3]: [Interrupt]
- [Register Key 4]: [Preview]
- [Register Key 5]: [OFF]

12.2.4 Selecting functions to be displayed in the main menu of classic style

Configure shortcut keys that are displayed in the main menu of classic style.

- 1 Select [System Settings] - [Main Menu Default (Classic style)] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), select [Assignment No.] for the main menu key to assign a shortcut key to, then click [Edit].
 - [Assignment No.] 1 to 11 are assigned to the first screen of the main menu. These keys should be assigned to frequently used functions.
- 2 Select a function to be assigned to a shortcut key.

Setting	Description
[Function Name]	Select a category of function to be assigned to a shortcut key. <ul style="list-style-type: none"> • [Not Set]: Do not create any shortcut key. • [Function]: Create a shortcut key to the main screen such as Copy mode or Scan/Fax mode. • [Copy Function Settings]: Create a shortcut key to the setting screen for the copy function. • [Scan/Fax Function Settings]: Create a shortcut key to the setting screen for scan/fax function. • [Copy Program]: Create a shortcut key to a copy program. This option is available when copy programs are registered on this machine. • [Scan/Fax Program]: Create a shortcut key to a scan/fax program. This option is available when scan/fax programs are registered on this machine. • [System User Box]: Create a shortcut key to the System User Box. • [Eco Function Settings]: Create a shortcut key to the Eco-related function. • [Widget Settings]: Create a shortcut key to the widget setting screen. • [Quick Security Settings]: Create a shortcut key to the simple security setting screen. • [QR Code Display]: Create a shortcut key to the QR code display screen. • [Address book]: Create a shortcut key to the address book.
[Shortcut Key]	Select a function to be assigned to a shortcut key. The available functions vary depending on the category selected in [Function Name].
[Scan/Fax Program Shortcut Key]	Select a program to be displayed from the list when a shortcut key to a scan/fax program is created.
[Specify Icon]	Select an icon to be displayed on the main menu, if necessary, when a shortcut key is created for a copy program or scan/fax program.

Tips

- If the OpenAPI application is registered on this machine, you can arrange keys for the registered applications or registered application groups in the main menu. For details, contact your service representative.

12.2.5 Changing the theme of the classic-style main menu

Change the background color, etc. for the main menu of classic style as desired.

Select [System Settings] - [Main Menu Display Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Main Menu Display Settings]	Select the theme to be applied to the main menu of classic style (default: [Theme 1]).
[Register]	Connects the USB flash drive, which contains the image you want to use as the theme of the main menu, to this machine, and registers it as the user theme. Up to three files can be registered as images.
[Delete]	Deletes the registered user theme.

12.2.6 Selecting function keys to be displayed in each classic-style mode (using a display pattern)

Change the display pattern of function keys in the Copy, Scan/Fax and User Box modes of classic style, respectively.

Select [System Settings] - [Custom Function Pattern Selection] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Copy/Print Screen Pattern]	Select a display pattern of function keys to be displayed in the print settings screen in Copy or User Box mode (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. You can select [Details] to check the details of each display pattern.
[Send/Save Screen Pattern]	Select a display pattern of function keys to be displayed on the send and save settings screens in Scan/Fax and User Box modes (default: [Full]). <ul style="list-style-type: none"> • [Full]: Displays all the function keys. • [Standard] (Not displayed in some areas): Displays commonly used function keys. • [Basic]: Displays the more basic function keys than [Standard]. You can select [Details] to check the details of each display pattern.

12.2.7 Selecting function keys to be displayed in each classic-style mode (Individual specification)

Setting flow

You can change the type or layout of function keys to be displayed in the main screen in each mode of classic style.

You can arrange the frequently used function keys in the main screen or hide unused function keys depending on function key usage conditions.

To change function keys to be displayed on the screen in each mode, take the following procedure to configure the settings.

- 1** Allowing the change of functions keys in each mode (page 12-7)
- 2** Changing function keys to be displayed on the screen in each mode
 - Changing function keys in copy mode (page 12-8)
 - Changing function keys in scan/fax mode (page 12-8)
 - Changing function keys in fax mode (page 12-8)

Allowing the change of functions keys in each mode

Select whether to allow users to change the function keys to be displayed in each mode of classic style.

Select [System Settings] - [Function Display Key Permission Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Copy/Print]	When permitting the user to change the function key to be displayed in the main screen in copy mode and the print settings screen in User Box mode, set this option to ON (default: OFF).
[Send/Save]	When permitting the user to change the function key to be displayed in the main screen in scan/fax mode and the send and save settings screens in User Box mode, set this option to ON (default: OFF).

Changing function keys in copy mode

Change the function key to be displayed on the main screen in copy mode of classic style and the print settings screen in User Box mode.

- 1 Select [Customize] - [Function Display Key Permission Setting] - [Copy/Print] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine) to select the number of the function key for which you wish to change the setting, then click [Edit].
 - Keys No.1 to No.7 are assigned to basic function 1, and No.8 to No.14 are to basic function 2. It is recommended that you assign frequently-used functions to No.1 to No.7.
- 2 Select a function to be assigned to a shortcut key.
 - Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

Changing function keys in scan/fax mode

Change the function key to be displayed on the main screen in scan/fax mode of classic style and the send and save settings screens in User Box mode.

- 1 Select [Customize] - [Function Display Key Permission Setting] - [Send/Save] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine) to select the number of the function key for which you wish to change the setting, then click [Edit].
- 2 Select a function to be assigned to a shortcut key.
 - Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

Changing function keys in fax mode

Change the function key to be displayed on the main screen in fax mode of classic style.

- 1 Select [Customize] - [Function Display Key Permission Setting] - [Fax TX] in user mode of **Web Connection** (or in [Utility] - [Utility] of this machine) to select the number of the function key for which you wish to change the setting, then click [Edit].
- 2 Select a function to be assigned to a shortcut key.
 - Functions are grouped by category. Click [Display] to display the functions in each category, enabling you to select a target.

12.2.8 Allowing the user to change the language to be displayed on the screen of this machine

Allow the user to temporarily change the language to be displayed on the screen of this machine.

Select [System Settings] - [Temporarily Change Language] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Temporarily Change Language]	When you allow the user to temporarily change the language to be displayed on the screen of this machine, set this option to ON (default: OFF). Setting to ON displays the [Language] key on the home screen or main screen.

12.2.9 Changing the Keypad display when entering number of sets

You can always display the keypad on the screen of classic style, on which you can enter the number of copies.

Select [System Settings] - [Display 10 Keypad when entering Number of Sets] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Display 10 Keypad when entering Number of Sets]	Select whether to always display the keypad on the screen of classic style, on which you can enter the number of copies, only when you have selected the Copies key (default: [When Number of Sets is pressed]).

12.2.10 Arranging widgets on the classic-style screen

You can place texts, icons, GIF animation, or other items as widgets at the desired positions on the classic-style main menu or the copy-mode screen. By arranging widgets on frequently used screens, important information can be highlighted.

Select [System Settings] - [Widget Function Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Widget Function Settings]	When using the widget function, set this option to ON (default: ON).

12.2.11 Displaying the default registration menu on the screen of basic style

Specify whether to display the menu, which is used to register the user-defined value as the default, on each mode screen of basic style.

Select [System Settings] - [Change Permission for Default Value Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Change Permission for Default Value]	When displaying the default registration menu, set this option to ON (default: OFF).

12.3 Monitoring and Checking the Status of this Machine

12.3.1 Checking the ROM version

Check the ROM version of this machine.

Select [Maintenance] - [ROM Version] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and check the ROM version of this machine.

12.3.2 Checking the counter of this machine

You can check the information of various types of counters such as the total counter and counters for respective functions.

Select [Maintenance] - [Meter Count] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and check counter information of this machine.

12.3.3 Notifying counter information by E-mail

Setting flow

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

To send the counter information via E-mail, follow the below procedure to configure the settings.

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring the Scan to E-mail Environment (page 5-2)
 - Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and set [Total Counter Notification] to ON.
- 3** Configuring the counter notification settings (page 12-10)

Configuring the counter notification settings

Register destination E-mail addresses. Up to three destination E-mail addresses can be registered. Also set the notification schedule.

Select [Maintenance] - [Total Counter Notification Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Total Counter Notification Setting]	Enter a model name to be included in the notification mail message (using up to 20 characters).
[Schedule Setting]	Specify the notification schedule by [Daily], [Weekly], or [Monthly]. Up to two schedules can be registered. You can use different schedules for different purposes.
[Register Notification Address]	Register destination E-mail addresses. Also, select a notification schedule to be applied. <ul style="list-style-type: none"> • [E-mail Address]: Enter the E-mail address of the destination (using up to 320 characters, excluding spaces). • [Eco-Related Information Notification]: When notifying of Eco information, set this option to ON (default: ON). • [Notifies by Schedule1] or [Notifies by Schedule2]: Select a schedule to be applied to a destination from the schedules registered in [Schedule Setting].
[Test Notice]	When issuing a test notification, set [Send notice after setting complete] to ON (default: OFF).


Tips

- If [Send notice after setting complete] is set to ON, a test notification is sent to the E-mail addresses that are registered after settings were completed.

12.3.4 Notifying a warning occurrence or consumables replacement period by E-mail

Setting flow

If a warning occurs on this machine that instructs the user to add paper, replace toner, or resolve a paper jam, it can be sent to a registered E-mail address.

To send the machine status via E-mail, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring the Scan to E-mail Environment (page 5-2)
 - Select [Network] - [E-mail Setting] - [E-mail TX (SMTP)], and [E-mail Notification] to ON.
- 3 Configuring the machine status notification settings (page 12-11)

Configuring the machine status notification settings

Register destination E-mail addresses. Up to 10 destination E-mail addresses can be registered. Also select warnings to send a notification when any of them occurs.

Select [Maintenance] - [Status Notification Setting] - [E-mail Address] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Notification Address]	Enter the E-mail address of the destination (using up to 320 characters, excluding spaces).
[Alert]	Select items to be notified automatically. Select the check boxes of items to be notified.

12.3.5 Managing the machine via SNMP

Setting flow

If you manage network devices using Simple Network Management Protocol (SNMP), you can acquire the information of this machine and monitor it via the network. This machine supports the TCP/IP environment.

Using the SNMP TRAP function also enables you to notify the specified IP address of a warning that occurred on this machine.

To manage this machine via SNMP, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring the settings for using SNMP (page 12-11)

Configuring the settings for using SNMP

Configure the settings to obtain information of this machine or to monitor the machine using Simple Network Management Protocol (SNMP).

- 1** Select [Network] - [SNMP Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SNMP Setting]	<p>When enabling SNMP, set this option to ON (default: ON).</p> <ul style="list-style-type: none"> [SNMP v1/v2c(IP)]: When using SNMP v1 or SNMP v2, set this option to ON (default: ON). [SNMP v3(IP)]: When using SNMP v3, set this option to ON (default: ON).
[UDP Port Setting]	If necessary, change the UDP port number (default: [161]).
[SNMP v1/v2c Setting]	<p>Configure SNMP v1/v2c settings.</p> <ul style="list-style-type: none"> [Read Community Name]: Enter a read-only community name (using 1 to 15 characters, excluding spaces, \, ', ", and #) (default: [public]). [Write Community Name]: When allowing reading and writing, set this option to ON (default: ON). Also enter a community name used for reading and writing (using 1 to 15 characters, excluding spaces, \, ', ", and #) (default: [private]).
[SNMP v3 Setting]	<p>Configure SNMP v3 settings.</p> <ul style="list-style-type: none"> [Context Name]: Enter the context name (using up to 63 characters, excluding spaces, \, ', ", and #). [Discovery User Name]: When allowing the detection user, set this option to ON (default: ON). Also, enter a user name for detection (using 1 to 32 characters, excluding spaces, \, ', ", and #) (default: [public]). [Read User Name]: Enter a read-only user name (using up to 32 characters, excluding spaces, \, ', ", and #) (default: [initial]). [Security Level]: Select a security level of the user in the read-write enable state (default: [auth-password/priv-password]). [auth-password]: If [auth-password] or [auth-password/priv-password] is selected from [Security Level], enter an authentication password for the read-only user (using 8 to 32 characters, excluding spaces, \, ', ", and #). [priv-password]: If [auth-password/priv-password] is selected from [Security Level], enter a password used for privacy (encryption) of the read-only user (using 8 to 32 characters, excluding spaces, \, ', ", and #). [Write User Name]: Enter the user name of the user in the read-write enable state (using up to 32 characters) (default: [restrict]). [Security Level]: Select a security level of the user in the read-write enable state (default: [auth-password/priv-password]). [auth-password]: If [auth-password] or [auth-password/priv-password] is selected from [Security Level], enter an authentication password for the read-write enabled user (using 8 to 32 characters, excluding spaces, \, ', ", and #) (default: MAC address of this machine (Alphabetic characters are all in capitals, excluding colons (:))). [priv-password]: If [auth-password/priv-password] is selected from [Security Level], enter a password used for privacy (encryption) of the read-write enabled user (using 8 to 32 characters, excluding spaces, \, ', ", and #) (default: MAC address of this machine (Alphabetic characters are all in capitals, excluding colons (:))). [Encryption Algorithm]: Select an encryption algorithm (default: [DES]). [Authentication Method]: Select an authentication algorithm (default: [MD5]).
[TRAP Setting]	<p>Configure settings for the SNMP TRAP function.</p> <ul style="list-style-type: none"> [Allow Setting]: When allowing a notification of the status of this machine using the SNMP TRAP function, set this option to ON (default: ON). [Trap Setting when Authentication Fails]: When performing TRAP TX due to an authentication failure, set this option to ON (default: OFF).
[Administrator Information]	<p>Enter information of this machine.</p> <ul style="list-style-type: none"> [Device Name]: Enter the name (MIB sysName) of this machine (using up to 255 characters). [Device Location]: Enter the location where to install this machine (MIB sysLocation) (using up to 255 characters). [Administrator Name]: Enter the administrator name (MIB sysContact) (using up to 255 characters).

- 2** To notify of the machine status using SNMP TRAP function, select [Maintenance] - [Status Notification Setting] - [IP Address] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then configure the following settings.

Setting	Description
[Notification Address]	Enter the E-mail address of the destination (using up to 253 characters). Use one of the following formats. Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6b::fe10:2f16"
[Port No.]	If necessary, change the port number.
[Community Name]	Enter the community name (using up to 15 characters) (default: [public]).
[Alert]	Select items to be notified automatically. Select the check boxes of items to be notified.

12.3.6 Outputting job logs

Specifying the job log acquisition method

Configure the settings to obtain job logs. After you have changed these settings, the job log is obtained when you restart this machine.

You can check usage, paper usage, operations and job history for each user or account in the job log. For details on how to viewing the output job logs, contact your service representative.

Select [Security] - [Job Log Settings] - [Job Log Usage Set.] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable Settings]	When obtaining job logs, set this option to ON (default: OFF).
[Obtain Log Type]	Select whether to obtain job logs for each type. <ul style="list-style-type: none"> [Accounting Log]: Enables you to obtain information relevant to paper consumption for each user or account (default: ON). [Counting Log]: Enables you to obtain information about paper consumption and the reduction rate of paper used for printing (default: ON). [Audit Log]: Enables you to obtain user operation or job history (default: ON). You can track unauthorized actions or the leakage of information.
[Transmission Method]	Select the method to send job logs to the server (default: [Manual (External Transmission Method)]). <ul style="list-style-type: none"> [Manual (External Transmission Method)]: Sends job logs when a manual operation or external instruction is triggered. [Auto]: Automatically sends job logs based on the specified conditions. To configure the automatic send setting, select [Job Log Settings] - [Auto Distribution Setting]. [syslog]: Sends job logs in syslog format. To configure the log sending setting, select [Job Log Settings] - [syslog TX settings].
[Overwrite]	To allow the user to overwrite the oldest job log with a new job log when the free space of the storage on the machine runs out, set this option to ON (default: ON).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Downloading job logs

- 1** Select [Maintenance] - [Job Log] - [Create Job Log] in administrator mode of **Web Connection**, then click [OK].
 - If any job logs have not been obtained, download them before creating new job log data. The job logs that have not been obtained are deleted when the new job log data is created.This starts creating job log data.

- 2** Select [Maintenance] - [Job Log] - [Download Job Log] in administrator mode of **Web Connection**, then select the location to download job log data.
 - [Download to PC]: Download job log data to your computer.
 - [Download to SMB]: Download job log data to the SMB sharing folder.

- 3** Click [OK].
 - If you select [Download to PC], click [Download].
 - If you select [Download to SMB], select the SMB sharing folder to download data to.This starts downloading the job log.

12.4 Managing the setting information

12.4.1 Importing configuration information

Types of information that can be imported

Various types of setting information, which are exported from this machine to your computer or the SMB sharing folder can be imported to this machine. You can migrate setting information that is exported from other device of the same model to exchange the device.

The following information can be imported on this machine.

Item	Description
[Device Setting]	Various settings of this machine. To import setting information, enter the password that is specified when exporting it.
[Authentication Information]	Authentication information to be managed by this machine. To import the authentication information, enter the password that was specified for export.
[Address]	The information of addresses registered on this machine. To import the address information, enter the password that was specified for export.
[Copy Protect/Stamp]	The registration information of copy protect or stamp.
[Restriction Code List]	This is a list of restriction codes for the OpenAPI connection application.
[Copy Program]	Copy program registration information.

Tips

- To import address information, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Importing information from your computer

- 1 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be imported, then click [Import].
- 2 Configure the required settings depending on the information to be imported.
 - To import the [Device Setting], [Authentication Information], or [Address], enter the password that was specified for export.
 - To import [Authentication Information], select whether to import the backup file for all authentication data, or to only import the user's registration information.
 - To import [Address], select whether to import the backup file for all address data, or to import the individually exported address file.
 - When importing [Address], if you select [Updates containing only Registration number, leave the original data of the address and Registration Number.], address information, in a file to be imported, containing only a registration number, is not registered in the machine. If you select [Updates containing only Registration number, delete the original data of the address and Registration Number.], address information containing only a registration number is deleted from the machine.
- 3 Select [Select from PC], then click [Browse...].
- 4 Select the file you want to import, and click [OK].
The import confirmation dialog box is displayed.
- 5 Click [Import].
 - If the information currently registered on this machine is different from [Authentication Information] and [Address] to be imported, [Difference] is displayed. Clicking [Difference] allows you to select whether to apply the information registered on this machine or the information to be imported.


Tips

- The counter information cannot be imported.
- For details on the list of inhibited codes, contact your service representative.

Importing information from an SMB sharing folder

- 1 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be imported, then click [Import].
- 2 Configure the required settings depending on the information to be imported.
 - To import the [Device Setting], [Authentication Information], or [Address], enter the password that was specified for export.
 - To import [Authentication Information], select whether to import the backup file for all authentication data, or to only import the user's registration information.
 - To import [Address], select whether to import the backup file for all address data, or to import the individually exported address file.
 - When importing [Address], if you select [Updates containing only Registration number, leave the original data of the address and Registration Number.], address information, in a file to be imported, containing only a registration number, is not registered in the machine. If you select [Updates containing only Registration number, delete the original data of the address and Registration Number.], address information containing only a registration number is deleted from the machine.
- 3 Select [Select from SMB List], then click [SMB List].
- 4 Enter the information to connect to the SMB server.

Setting	Description
[Server Address]	Enter the SMB server address. Example of entry: "192.168.1.1"
[User Name]	Enter the user name to log in to the SMB server (using up to 64 characters).
[Password]	Enter the password to log in to the SMB server (using up to 64 characters).

- 5 Click [Connection].
The folder selection page is displayed.
- 6 Select the file you want to import, and click [OK].
The import confirmation dialog box is displayed.
- 7 Click [Import].
 - If the information currently registered on this machine is different from [Authentication Information] and [Address] to be imported, [Difference] is displayed. Clicking [Difference] allows you to select whether to apply the information registered on this machine or the information to be imported.


Tips

- The counter information cannot be imported.
- For details on the list of inhibited codes, contact your service representative.

Importing information from a USB flash drive

If you access an MFP connected to the network via the Web browser on this machine, you can import configuration information to the destination MFP using a USB flash drive.

- 1 Connect the USB flash drive with configuration information saved to the MFP you want to import configuration information to.

- 2 Open the Web browser on this machine, then specify the IP address of the MFP you want to import configuration information to.
 - For details on the operation procedure, refer to "User's Guide[Advanced Function Operations]/[Using Web Browser on the Touch Panel]".
 This displays the **Web Connection** page of the accessed MFP on the Web browser screen.
- 3 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be imported, then click [Import].
- 4 Configure the required settings depending on the information to be imported.
 - To import the [Device Setting], [Authentication Information], or [Address], enter the password that was specified for export.
 - To import [Authentication Information], select whether to import the backup file for all authentication data, or to only import the user's registration information.
 - To import [Address], select whether to import the backup file for all address data, or to import the individually exported address file.
 - When importing [Address], if you select [Updates containing only Registration number, leave the original data of the address and Registration Number.], address information, in a file to be imported, containing only a registration number, is not registered in the machine. If you select [Updates containing only Registration number, delete the original data of the address and Registration Number.], address information containing only a registration number is deleted from the machine.
- 5 Select [Select from the USB connected to MFP], then click [OK].
- 6 Click [OK].

Tips

- The counter information cannot be imported.
- For details on the list of inhibited codes, contact your service representative.

12.4.2 Exporting configuration information

Types of information that can be exported

Various types of setting information of this machine can be exported to your computer or the SMB sharing folder. Use this function to back up various types of setting information of this machine or copy setting information.

The following information can be exported from this machine.

Item	Description
[Device Setting]	Various settings of this machine. If necessary, the configuration file to be exported can be encrypted using a password.
[Meter Count]	Information of various types of counters on this machine. Select counter information to be exported from counters for respective users or accounts, and others.
[Authentication Information]	Authentication information to be managed by this machine. Select whether to export all authentication information or only user registration information. If necessary, the authentication information file to be exported can be encrypted using password.
[Address]	The information of addresses registered on this machine. Select information to be exported from all address information, address book, group, program, and E-mail subject/body. If necessary, the address information file to be exported can be encrypted using password.
[Copy Protect/Stamp]	The registration information of copy protect or stamp.
[Restriction Code List]	The restriction codes list of our depreciated the OpenAPI connection application.

Item	Description
[Copy Program]	Copy program registration information.

Tips

- To export address information, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Exporting information to your computer

- 1 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be exported, then click [Export].
- 2 Configure the required settings depending on the information to be exported.
 - If [Device Setting] is selected, select the export purpose from [Copy Settings] or [Backup Settings]. If you select [Copy Settings], select the type of the setting to be copied.
 - If you select [Device Setting], [Authentication Information], or [Address], enter the password as required.
 - If you select [Meter Count], select the type of the counter to be exported.
 - If you select [Authentication Information] or [Address], select whether to export all information.
 - If you select [Authentication Information] or [Address], select the format of the file to save data in. To edit information using the spreadsheet software, select [CSV File].
- 3 In [Export Destination], select [Export to PC].
- 4 Click [OK].
The file is saved on the computer.

Tips

- When an E-mail address with a registered certificate is exported, the certificate is not exported. Register the certificate again after importing the address on this machine.
- For details on the list of inhibited codes, contact your service representative.

Exporting information to an SMB sharing folder

- 1 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be exported, then click [Export].
- 2 Configure the required settings depending on the information to be exported.
 - If [Device Setting] is selected, select the export purpose from [Copy Settings] or [Backup Settings]. If you select [Copy Settings], select the type of the setting to be copied.
 - If you select [Device Setting], [Authentication Information], or [Address], enter the password as required.
 - If you select [Meter Count], select the type of the counter to be exported.
 - If you select [Authentication Information] or [Address], select whether to export all information.
 - If you select [Authentication Information] or [Address], select the format of the file to save data in. To edit information using the spreadsheet software, select [CSV File].
- 3 In [Export Destination], select [Export to SMB].
- 4 Click [OK].
- 5 Enter the information to connect to the SMB server.

Setting	Description
[Server Address]	Enter the SMB server address. Example of entry: "192.168.1.1"

Setting	Description
[User Name]	Enter the user name to log in to the SMB server (using up to 64 characters).
[Password]	Enter the password to log in to the SMB server (using up to 64 characters).

6 Click [Connection].

The folder selection page is displayed.

7 Select a folder to export the target file to, then click [OK].

The file is saved in the selected SMB sharing folder.

Exporting information to a USB flash drive

If you access an MFP connected to the network via the Web browser on this machine, you can export configuration information from the destination MFP to a USB flash drive.

1 Connect the USB flash drive to the MFP you want to export configuration information from.

2 Open the Web browser on this machine, then specify the IP address of the MFP you want to export configuration information from.

→ For details on the operation procedure, refer to "User's Guide[Advanced Function Operations]/[Using Web Browser on the Touch Panel]".

This displays the **Web Connection** page of the accessed MFP on the Web browser screen.

3 Select [Maintenance] - [Import/Export] in administrator mode of **Web Connection** to select the information to be exported, then click [Export].

4 Configure the required settings depending on the information to be exported.

→ If [Device Setting] is selected, select the export purpose from [Copy Settings] or [Backup Settings]. If you select [Copy Settings], select the type of the setting to be copied.

→ If you select [Device Setting], [Authentication Information], or [Address], enter the password as required.

→ If you select [Counter], select the type of the counter to be exported.

→ If you select [Authentication Information] or [Address], select whether to export all information.

→ If you select [Authentication Information] or [Address], select the format of the file to save data in. To edit information using the spreadsheet software, select [CSV File].

5 Select [Export to the USB connected to MFP], then click [OK].

6 Click [OK].

Tips

- When an E-mail address with a registered certificate is exported, the certificate is not exported. Register the certificate again after importing the address on this machine.
- For details on the list of inhibited codes, contact your service representative.

12.4.3 Importing configuration information of other device

You can export configuration information from other device on the network and import it to the currently displayed device.

- 1 Select [Search surrounding MFPs] from the device search icon.
 - For details on the device search icon, refer to page 1-4.
 When a device search is completed, the [Search surrounding MFPs] window is displayed.
- 2 Select the device to export configuration information from, and click [Import/Export].
The [Import/Export] page is displayed.
- 3 Select the tab of the information to be exported.
- 4 Configure the required settings depending on the information to be exported.
 - If you select [Device Setting], select the type of the configuration information to be exported.
 - If you select [Device Setting], [Authentication Information], or [Address], enter the password as required.
 - If you select [Authentication Information] or [Address], select whether to export all information.
 - If you select [Authentication Information] or [Address], select the format of the file to save data in. To edit information using the spreadsheet software, select [CSV File].
- 5 Clicking [Next] starts export processing.
When export processing is completed, the import destination confirmation dialog box is displayed.
- 6 Enter the administrator password of the device to import information to.
 - When SSL communication is enabled on the import destination device, set [Use SSL/TLS] to ON.
- 7 Click [OK].

12.4.4 Backing up configuration information

Backing up data to the server

Configure settings to back up setting data of this machine to the server.

Select [Maintenance] - [Backup Setting Information] - [Server BackUp Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Backup Function Usage Setting]	When backing up setting data to the server, set this option to ON (default: OFF).
[TX Protocol]	Select the protocol to communicate with the server, then specify parameters. <ul style="list-style-type: none"> • [SMB]: Select this item to back up data to the SMB server. In [SMB Setting], enter the host name of the server and the path of the sharing folder as well as the user name and password of the user with access rights. • [HTTP]: Select this item to back up data to the WebDAV server. In [HTTP Settings], enter the URL of the WebDAV folder as well as the user name and password of the user with access rights. Also, select whether to use a proxy server.
[Auto Backup Settings]	Configure a setting to periodically make a backup copy. <ul style="list-style-type: none"> • [Auto Backup Settings]: Select whether to periodically make a backup copy (default: [OFF]). • [Interval of Day(s)]: Specify the interval of days to make a backup copy, and specify the time in [Backup Time] (default: [1] day, [0] hour [0] min.). • [Weekly Frequency]: Specify a day of the week to make a backup copy, and specify the time in [Backup Time] (default: [Sun] day of the week, [0] hour [0] min.).
[Backup Target]	Select backup data.

Setting	Description
[Password is changed.]	Select whether to change the password. <ul style="list-style-type: none"> [Encryption Password]: Enter the password to encrypt backup data (using up to 64 characters).
[Last backup date]	Displays the latest date when server backup has been performed. Also, the backup result history is displayed.
[Immediate backup]	Manually execute server backup.

**Tips**

- The backed-up data can be restored by selecting [Maintenance] - [Backup Setting Information] - [Restore from Server].

12.4.5 Initializing configuration information

Resetting the network settings

Return the network settings of this machine to the factory default status.

Select [Maintenance] - [Reset] - [Network Setting Clear] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [Clear].

Deleting all address information

Collectively delete destination information registered on this machine.

Select [Maintenance] - [Reset] - [Format All Destination] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and click [Format].

**Tips**

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Restarting the network interface

Reset the controller of this machine and restart the network interface.

Select [Maintenance] - [Reset] - [Reset] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [Reset].

12.4.6 Checking whether settings are updated

If settings are changed via **Web Connection** when a job is running, it notifies the administrator that a setting change will not be immediately updated.

In the administrator mode, select [Maintenance] - [Confirm update settings for Held Jobs.] in administrator mode of **Web Connection** to check whether settings are updated.

12.5 Setting the operating environment for this machine

12.5.1 Original/paper setting

Configuring the setting to scan the original from the ADF

Specify the original skew adjustment level of the original when scanning it on the **ADF**.

Select [System Settings] - [ADF original skew adj.setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Skew adj. level]	Select the original skew adjustment level of the original when scanning it on the ADF (default: [High]). <ul style="list-style-type: none"> [High]: Adjusts the skew mechanically and electronically. [Low]: Adjusts the skew mechanically.

Setting the manual staple operation

Set the manual staple operation.

Select [System Settings] - [Manual staple setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Staple start wait time]	Specify the waiting time from the time when paper is loaded into the manual staple slit to the time when stapling is started (default: [1] sec.).
[Setting for Manual Staple]	When not changing to the sleep mode to always make the manual staple available, select [Disable sleep mode] (default: [OFF]).



Tips

- This setting is displayed when the optional **Finisher FS-539** or **Finisher FS-539 SD** is installed in this machine.

12.5.2 Configuring the scan settings

Configuring the preview function display settings

Configure settings related to the preview function of classic style.

Select [System Settings] - [Preview Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Real time preview]	When using the real time preview function, set this option to ON (default: OFF). Display a preview image for each page of an original when it is scanned in scan/fax mode. Each preview image shows the scanned original as is.
[Set key Initial display]	When setting the preview screen with setting keys displayed as the default, set this option to ON (default: OFF).

Printing a stamp on blank pages

Print date/time or stamp on blank pages inserted by the cover sheet or inter sheet function.

Select [System Settings] - [Blank Page Print Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Print Setting]	When printing the date/time or stamp specified by the stamp/page printing function on blank pages inserted by the cover sheet or insert sheet function, set this option to ON (default: OFF). Even if ON is selected, the date/time and stamps are not printed on blank pages inserted with a specified page facing up using the Chapters function.

Configuring the default Compact PDF conversion setting

Select whether to give priority to either the image quality or speed when creating a compact PDF file.

Select [System Settings] - [Compact PDF Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Compact PDF Settings]	Select whether to give priority to either the image quality or speed when creating a compact PDF file (default: [Prioritize Quality]).

Setting the processing accuracy of Outline PDF

When you save data in the Outline PDF format, the text is extracted from the original and converted into a vector image. The following explains how to set the outline processing accuracy of images (figures).

Select [System Settings] - [Outline PDF Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Graphic Outlining]	Select the outline processing accuracy of images (graphics) when saving data in the Outline PDF format (default: [OFF]). The outline processing accuracy is improved in the order of [LOW], [MIDDLE], and [HIGH]. If you select [OFF], outline processing is not performed.

Configuring the default searchable PDF conversion setting

Specify conditions to automatically specify a document name from the OCR character recognition result when creating a searchable PDF file using the searchable PDF function.

Select [System Settings] - [Searchable PDF Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Extract Document name automatically when Searchable PDF is selected]	To automatically specify a document name from the OCR character recognition result when creating a searchable PDF file, set this option to ON (default: ON). <ul style="list-style-type: none"> [Maximum Length of Character Extraction]: Specify the maximum string length when automatically extracting an appropriate character string for a document name from the OCR character recognition result (default: [30 characters]). [Document Name Confirmation Screen]: When displaying the confirmation screen of the document name that is automatically set from the OCR character recognition result, set this option to ON (default: OFF).

Tips

- This setting is displayed when the optional **i-Option LK-105** or **i-Option LK-110** is installed in this machine.

Specifying the default for [PDF Web Optimization]

Change the default of [PDF Web Optimization] that is set to create a PDF file using the scan function.

Select [System Settings] - [PDF Web Optimization Default Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[PDF Web Optimization Default Settings]	Change the default of [PDF Web Optimization] (default: [OFF]).

Tips

- This setting is displayed when the optional **i-Option LK-102** or **i-Option LK-110** is installed in this machine.

Specifying the default for [PDF/A]

Change the default of [PDF/A] that is set to create a PDF file using the scan function (default: [Disable]).

Select [System Settings] - [PDF/A Default Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[PDF/A]	Change the default of [PDF/A] (default: [Disable]).

Tips

- This setting is displayed when the optional **i-Option LK-102** or **i-Option LK-110** is installed in this machine.

Changing the default scan data file name

Change the default file name of scanned original data when saving it.

The file name is: "initial of the function" + "text to be added" + "date" + "sequential number" + "page number" + "file extension".

Select [System Settings] - [Scan File Name Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Function Mode Initial]	Select whether to use an initial of the relevant function as a prefix for the file name (default: [Attach]). The following letters are used as prefixes for file name. C: Copy S: Scan/Fax, User Box P: Print
[Supplementary File Name]	Select whether to add a device name or desired text to the file name (default: [Device Name]). To add desired text, enter it. For the device name, use the name you specified by selecting [Machine Setting] - [Input Machine Address] - [Device Name].

12.5.3 Enlarge display settings

Changing default settings for Normal Display and Enlarge Display collectively

Configure settings to simultaneously change the default values for Normal screen display and Enlarge display at the same time.

Select [System Settings] - [Reset Settings] - [Job Reset] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Default Basic/Enlarge Display Common Setting]	When simultaneously specifying the default values of the normal screen display and enlarged display, set this option to ON (default: OFF). If ON is selected, [Default Enlarge Display Settings] is not displayed. Initial values for each mode that are changed in [Default Copy Settings] or [Default Scan/Fax Settings] are applied to both Normal and Enlarge Display modes.

Setting the action for switching the display to Enlarge Display

Select whether to change the default display of the classic style to the enlarge display mode. Also, set the operation to be taken when the normal screen display is switched to the enlarge display mode.

Select [System Settings] - [Enlarge Display Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Default Enlarge Display Setting]	When changing the default display of the classic style to the enlarge display mode, set this option to ON (default: OFF).
[Enlarge Display Setting]	If [Default Enlarge Display Setting] is set to ON, specify whether to switch to the enlarge display mode when the normal screen display is reset (default: [Normal]).
[Apply Basic Setting to Enlarge Display]	Select whether to inherit the settings configured on the normal screen display when switching the screen from Normal to Enlarge Display (default: [Mode 2]). <ul style="list-style-type: none"> [Mode 1]: Inherit all normal mode settings. [Mode 2]: In Copy mode, only inherit Normal mode settings that can be set in Enlarge Display mode. In Scan/Fax mode, reset the settings.

12.5.4 Support settings

Allowing transmission of the machine usage frequency or function settings information

Information relevant to usage frequency of this machine and the machine function settings can be sent to our company.

Select [System Settings] - [List/Counter] - [Meter Count and Device Confirmation Tx Settings] administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Meter Count and Device Confirmation Tx Settings]	When permitting the user to send information such as the use frequency of the machine and function settings to our company, set this option to ON (default: OFF). The information about this machine will be used by us for the improvement of service and functions in future.

Tips

- Information about IP address and others related to security as well as private information such as address books will not be sent.

12.5.5 Setting the skip job conditions

Specify the printing priority order and whether to skip a job when you cannot perform a printing job immediately.

Select [System Settings] - [Job Priority Operation Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Fax RX Job Priority]	When giving priority to fax printing during copying or printing, set this option to ON (default: OFF).
[Skip Job (Fax)]	To first process the next fax job when printing stops due to a shortage of paper or overloaded output tray, set this option to ON (default: ON).
[Skip Job (Copy, Print)]	To first process the next job other than fax when printing stops due to a shortage of paper or overloaded output tray, set this option to ON (default: ON).

12.5.6 Enabling functions that require the authentication by an external institution

Some functions that require the authentication by an external institution are disabled at product shipment. After authentication has been obtained, enter the target function code to enable the function.

Select [Maintenance] - [Authorization function Setting] - [Install License] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and enter the function code, then click [OK].

Tips

- For details on the functions that require the authentication by an external institution and function codes, contact your service representative.
- Select [Maintenance] - [Authorization function Setting] - [Authorization function list]; you can check the functions that are enabled on this machine.

12.6 Updating firmware or settings of this machine

12.6.1 Acquiring firmware via Internet to update this machine

Setting flow

You can externally download firmware and configuration information of this machine to update them.

You can keep using the machine even while downloading firmware or configuration information.

To externally download firmware and configuration information of this machine and update them, follow the procedure shown below.

- ✓ The firmware and configuration information must be updated by your service representative. For details, contact your service representative.

1 Prepare for downloading a firmware

- Preparing to download firmware via FTP (page 12-27)
- Preparing to download firmware via HTTP (page 12-27)

2 Updating firmware of this machine

- Updating the firmware automatically at the specified time (page 12-28)
- Updating the firmware manually (page 12-28)

Preparing to download firmware via FTP

Configure the setting to use a proxy when downloading firmware to this machine via FTP.

Select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [FTP Server Setting] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[FTP Server Setting]	When using a proxy, set this option to ON (default: OFF).
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number (default: [21]).

Preparing to download firmware via HTTP

Configure the setting to use a proxy when downloading firmware to this machine via HTTP.

Select [Network] - [Machine Update Settings] - [HTTP Proxy Settings] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[HTTP Proxy Settings]	When using a proxy, set this option to ON (default: OFF).
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number to be used for HTTP (default: [80]).
[Proxy Authentication]	Select whether to use Proxy Authentication (default: OFF). <ul style="list-style-type: none"> • [User Name]: Enter the user name used for proxy authentication (using up to 32 characters). • [Password]: Enter the password for proxy authentication (using up to 32 characters).

Updating the firmware automatically at the specified time

This machine can download a firmware automatically at the specified time and update the firmware.

In the administrator mode, select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [Update Firmware at Specified Time] in administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Update Firmware at Specified Time]	When updating firmware automatically at the specified time, set this option to ON (default: OFF).
[Firmware Update Start Time]	Enter the time when this machine should update the firmware automatically.

Updating the firmware manually

Externally download firmware to this machine and update the firmware manually.

You can keep using the machine as usual while downloading a firmware.

However, you cannot use this machine while updating the machine firmware. When the firmware updating process has been completed, this machine reboots automatically.

Select [Network] - [Machine Update Settings] - [Internet ISW Settings] - [Firmware Update Parameters] in administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Firmware Version]	Displays the current firmware version.
[Firmware Download Status]	Displays the status of downloading a firmware. Clicking [Refresh] refreshes the status.
[Firmware Download]	Click this button to download firmware externally.
[Delete Firmware]	Click this button to delete the downloaded firmware.
[Firmware Update Parameters]	Click this button to update the firmware of this machine using the firmware downloaded.

12.6.2 Acquiring the update file from the distribution server to update this machine and other devices

Acquiring the update file to update this machine

This machine can automatically update its firmware and configuration information.

In this step, configure settings so that this machine monitors the firmware update server on the network at periodic intervals to automatically download and update the latest firmware and configuration information.

- 1 Select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Auto Update Settings for This Machine] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Auto Update Settings for This Machine]	When automatically updating firmware of this machine, set this option to ON (default: OFF).
[Download Protocol]	Select a protocol used to obtain firmware from the firmware update server (default: [SMB]).
[SMB Setting]	Configure settings to obtain firmware using the SMB protocol. <ul style="list-style-type: none"> • [Host Name]: Enter the IP address of the firmware update server or the host name (using up to 253 characters, including symbols -, ., and _). • [File Path]: Enter the path of the shared folder that contains firmware (using up to 255 characters). • [User Name]: Enter the user name to connect this machine to the firmware update server (using up to 64 characters). • [Password]: Enter the password to connect to the firmware update server (using up to 64 characters, excluding "). • [Number of Retries]: Specify the number of retries to be executed when a connection with the firmware update server has failed (default: [3] times).

Setting	Description
[HTTP Settings]	Configure settings to obtain firmware using the HTTP protocol (WebDAV). <ul style="list-style-type: none"> [URL]: Enter the URL of the firmware storage location on the firmware update server (using up to 253 characters, excluding spaces). [User Name]: Enter the user name to connect this machine to the firmware update server (using up to 64 characters). [Password]: Enter the password to connect to the firmware update server (using up to 64 characters, excluding "). [Proxy]: When using a proxy server, set this option to ON (default: OFF). [Connection Timeout]: Change the timeout interval for communication with the firmware update server, if required (default: [60] sec.).
[Update Time]	Specify the time to start applying the firmware obtained from the firmware update server to this machine. It is advantageous to specify the time when this machine is not operating such as a break time or night time.
[Polling Settings]	Specify the interval to check whether the latest firmware exists on the firmware update server (default: [60] min.). <ul style="list-style-type: none"> [Set Interval.]: Enter the check interval in hours. [Polling Date/Time]: Specify a day of the week and the time to make a check.
[Retry Interval]	Specify the interval to retry processing when the system failed to check the latest firmware on the firmware update server (default: [5] min.).

2 To automatically update configuration information of this machine, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Machine Update Password] in administrator mode of **Web Connection**, then enter the password to decode the encrypted configuration file (using up to 32 characters).

3 If necessary, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Log TX Settings] in administrator mode of **Web Connection**, then configure a setting to send firmware update logs.

Setting	Description
[Update File Download/Update Log]	When sending firmware update logs of this machine to another location, set this option to ON (default: OFF).
[TX Protocol]	Select a protocol to send log data (default: [SMB]).
[SMB Setting]	Configure settings to send log data using the SMB protocol. <ul style="list-style-type: none"> [Host Name]: Enter the host name of the log sending destination (using up to 253 characters, including symbols -, ., :, and _). [File Path]: Enter the path of the shared folder of the log sending destination (using up to 255 characters). [User Name]: Enter the user name to log in to the log sending destination (using up to 64 characters). [Password]: Enter the password to log in to the log sending destination (using up to 64 characters, excluding ").
[WebDAV Settings]	Configure settings to send log data using the HTTP protocol (WebDAV). <ul style="list-style-type: none"> [URL]: Enter the URL of the log sending destination (using up to 253 characters, excluding spaces). [User Name]: Enter the user name to log in to the log sending destination (using up to 64 characters). [Password]: Enter the password to log in to the log sending destination (using up to 64 characters, excluding "). [Proxy]: When using a proxy server, set this option to ON (default: OFF).

4 Select [Network] - [Machine Update Settings] - [HTTP Proxy Settings] in administrator mode of **Web Connection** as needed, then configure the proxy settings.

Setting	Description
[HTTP Proxy Settings]	When using a proxy, set this option to ON (default: OFF).
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"

Setting	Description
[Proxy Server Port Number]	If necessary, change the proxy server port number to be used for HTTP (default: [80]).
[Proxy Authentication]	Select whether to use Proxy Authentication (default: OFF). <ul style="list-style-type: none"> [User Name]: Enter the user name used for proxy authentication (using up to 32 characters). [Password]: Enter the password for proxy authentication (using up to 32 characters).

Acquiring the update file on this machine to distribute it to other devices

Configure settings to operate this machine as a relay server.

Operating this machine as a relay server allows you to establish a relay between a different firmware update server on the network and other devices to distribute firmware to them.

If this machine monitors a different firmware update server on the network at periodic intervals and checks that the server contains the latest firmware, firmware is downloaded to the firmware storage area of this machine.

Other devices on the network monitor this machine, which is running as a relay server, at periodic intervals. If the latest firmware exists in the firmware storage area of this machine, firmware is downloaded and updated based on the settings of that device.

In this example, configure settings required when this machine monitors a different firmware update server as well as settings required when other devices access the firmware storage area of this machine.

- 1 In the administrator mode, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Relay Server Function Settings] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Update File Download Settings]	When operating this machine as the relay server, set this option to ON (default: OFF). <ul style="list-style-type: none"> [URL]: Enter the URL of the firmware storage location on the firmware update server (using up to 253 characters, excluding spaces). [User Name]: Enter the user name to connect this machine to the firmware update server (using up to 64 characters). [Password]: Enter the password to connect to the firmware update server (using up to 64 characters, excluding "). [Proxy]: When using a proxy server, set this option to ON (default: OFF). [Connection Timeout]: Change the timeout interval for communication with the firmware update server, if required (default: [60] sec.). [Polling Settings]: Specify the interval to check whether the firmware update server contains the latest firmware (default: [60] min.). [Number of Retries]: Specify the number of retries to be executed when the final firmware check for the firmware update server has failed (default: [5] times).
[HTTP Settings]	When allowing another device on the network to access the firmware storage area of this machine using the HTTP protocol (WebDAV), set this option to ON (default: OFF). <ul style="list-style-type: none"> [User Name]: Enter the user name to connect this machine to the firmware update server (using up to 64 characters). [Password]: Enter the password to connect to the firmware update server (using up to 64 characters, excluding ").
[SMB Setting]	When allowing another device on the network to access the firmware storage area of this machine using the SMB protocol, set this option to ON (default: OFF). <ul style="list-style-type: none"> [User Name]: Enter the user name to connect this machine to the firmware update server (using up to 64 characters). [Password]: Enter the password to connect to the firmware update server (using up to 64 characters, excluding "). [Update Log Save Folder]: When saving firmware update log data in the shared folder, set this option to ON (default: OFF). [SMB Communication Encryption]: When encrypting SMB communications with a client machine for the shared folder of this machine, set this option to ON (default: OFF). Setting to ON allows you to access only from client machines of SMB 3.0 or later.

- 2** If necessary, select [Network] - [Machine Update Settings] - [Machine Auto Update Settings] - [Log TX Settings] in administrator mode of **Web Connection**, then configure a setting to send firmware update logs.

Setting	Description
[Relay Update File Download Log]	When sending log data to another location while this machine operates as a relay server, set this option to ON (default: OFF).
[TX Protocol]	Select a protocol to send log data (default: [SMB]).
[SMB Setting]	Configure settings to send log data using the SMB protocol. <ul style="list-style-type: none"> [Host Name]: Enter the host name of the log sending destination (using up to 253 characters, including symbols -, ., :, and _). [File Path]: Enter the path of the shared folder of the log sending destination (using up to 255 characters). [User Name]: Enter the user name to log in to the log sending destination (using up to 64 characters). [Password]: Enter the password to log in to the log sending destination (using up to 64 characters, excluding ").
[WebDAV Settings]	Configure settings to send log data using the HTTP protocol (WebDAV). <ul style="list-style-type: none"> [URL]: Enter the URL of the log sending destination (using up to 253 characters, excluding spaces). [User Name]: Enter the user name to log in to the log sending destination (using up to 64 characters). [Password]: Enter the password to log in to the log sending destination (using up to 64 characters, excluding "). [Proxy]: When using a proxy server, set this option to ON (default: OFF).

- 3** Select [Network] - [Machine Update Settings] - [HTTP Proxy Settings] in administrator mode of **Web Connection** as needed, then configure the proxy settings.

Setting	Description
[HTTP Proxy Settings]	When using a proxy, set this option to ON (default: OFF).
[Proxy Server Address]	Enter the proxy server address. Use one of the following formats. <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Proxy Server Port Number]	If necessary, change the proxy server port number to be used for HTTP (default: [80]).
[Proxy Authentication]	Select whether to use Proxy Authentication (default: OFF). <ul style="list-style-type: none"> [User Name]: Enter the user name used for proxy authentication (using up to 32 characters). [Password]: Enter the password for proxy authentication (using up to 32 characters).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

12.6.3 Connecting the USB flash drive with firmware stored to update this machine

Connect the USB flash drive with firmware stored to this machine to update firmware.

Connect the USB flash drive with firmware stored, select [Network] - [Machine Update Settings] - [Firmware Update Parameters] in administrator mode of **Web Connection**, and click [OK].

12.6.4 Returning the updated firmware to the previous version

Return the firmware of this machine to the previous version.

Select [Network] - [Machine Update Settings] - [Firmware Rollback] in administrator mode of **Web Connection**, then click [Rollback]. Clicking [Rollback] applies the firmware displayed in [Backup File Version] to this machine.

 **Tips**

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

13

Registering Various Types of Information

13 Registering Various Types of Information

13.1 Registering address books

13.1.1 Registering E-mail Address

E-mail addresses can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [E-mail], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[E-mail]	Enter the E-mail address of the destination (using up to 320 characters, excluding spaces).
[Registration of Certification Information]	To encrypt E-mail messages using S/MIME, register the user's certificate. Select a certificate to be registered from your computer or the SMB sharing folder. <ul style="list-style-type: none"> To register the certificate, the E-mail address must be matched between the certificate and the destination to be registered. Only the DER (Distinguished Encoding Rules) format is supported as a file of certificate information.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.2 Registering an FTP Destination

An FTP destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [FTP], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.

Setting	Description
[Host Address]	Enter the destination host name or IP address (using up to 253 bytes). <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[File Path]	Enter the folder name of the host specified in [Host Address] (using up to 127 bytes). When not specifying the folder name, enter only "/". <ul style="list-style-type: none"> • Example to enter the folder name: "scan" • Example to enter the folder name in the folder: "scan/document"
[User ID]	If authentication is required in the FTP server, enter the available user name to log in (using up to 64 characters).
[Password]	Enter the password (using up to 64 characters, excluding double quotation marks ").
[anonymous]	When authentication is not required in the FTP server, set this option to ON (default: OFF).
[PASV Mode]	When the PASV mode is used in your environment, set this option to ON (default: OFF).
[Proxy]	When a proxy server is used in your environment, set this option to ON (default: OFF).
[Port No.]	If necessary, change the port number (default: [21]).
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.


Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.3 Registering an SMB Destination

An SMB destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [SMB], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Specify the index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[Host Address]	Enter the destination computer name (host name) or full computer name (FQDN) (using up to 253 bytes). If you cannot specify the computer name or full computer name, enter the IP address. <ul style="list-style-type: none"> • Example to enter the computer name (host name): "HOME-PC" • Example to enter the full computer name (FQDN): "host1.test.local" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Check Connection]	Check whether or not the host name you specified in [Host Address] exists.
[File Path]	Enter the shared folder name of the host specified in [Host Address] (using up to 255 bytes). <ul style="list-style-type: none"> • Example to enter the folder name: "scan" • Example to enter the folder name in the folder: "scan\document"

Setting	Description
[Host Name Search]	Searches for the host name to be applied to [Host Address]. To search for the host name, specify a group name. <ul style="list-style-type: none"> [Group Name]: Displays the name of the group to which the user belongs by default. To change the group name, select [Edit], and enter the desired group name (using up to 15 characters). After entering the group name, specify search conditions, and start Search. [Host Name]: Enter the target host name (using up to 15 characters). After entering the host name, specify search conditions, and start Search.
[User ID]	Enter the name of a user with folder access rights (using up to 64 characters).
[Password]	Enter the password (using up to 64 characters, excluding double quotation mark ") to access the folder.
[Reference]	Specify the shared folder of the desired computer by reference to the network. When the authentication screen appears, enter the name and password of the user who has privileges to access the shared folder. After authentication, [Host Address] or [File Path] is set automatically. The Reference function may fail under the following conditions. <ul style="list-style-type: none"> 512 or more workgroups or computers are on the network (subnet) connected to this machine. The machine is connected to the IPv6 environment.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.



Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.4 Registering a WebDAV Destination

A WebDAV destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [WebDAV], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[Host Address]	Enter the destination host name or IP address (using up to 253 bytes). <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[File Path]	Enter the folder name of the host specified in [Host Address] (using up to 127 bytes). <ul style="list-style-type: none"> Example to enter the folder name: "scan" Example to enter the folder name in the folder: "scan/document"
[User ID]	Enter the name of a user with folder access rights (using up to 64 characters).
[Password]	Enter the password (using up to 64 characters, excluding double quotation mark ") to access the folder.
[SSL Settings]	When SSL is used in your environment, set this option to ON (default: OFF). Setting this option to ON changes [Port No.] to [443].
[Proxy]	When a proxy server is used in your environment, set this option to ON (default: OFF).

Setting	Description
[Port No.]	If necessary, change the port number (default: [80]).
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.


Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.5 Registering a User Box

A User Box can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [User Box], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[User Box No.]	Select the User Box number of the destination in [Search from List]. If the User Box is already known, you can manually enter the User Box number.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.


Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.6 Registering a Fax Address

A fax address can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [Fax], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.

Setting	Description
[Destination]	Enter the destination fax number (using up to 38 digits, including symbols #, *, -, and characters T, P, and E). <ul style="list-style-type: none"> [T] or [*]: Enter the fax number when issuing a push signal in dial-up line mode (while [Dialing Method] is set to [10pps] or [20pps]). [P]: Enter this when you want to insert a wait time between dials. [-]: Enter this to separate a dial number. It does not affect the dialing of the number. [E-]: Enter the registered outside line number in PBX environment. Enter this when [PBX Connection Setting] (page 7-2) is set to ON.
[Confirm Fax Number]	Enter the fax number again. This option is displayed when [Confirm Address (Register)] (page 7-6) is set to ON.
[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. <ul style="list-style-type: none"> [V34 Off]: V.34 is a communication mode used for super G3 fax communication. When the remote machine or this machine is connected to a telephone line via PBX, however, you may not establish a communication in the super G3 mode depending on telephone line conditions. In this case, it is recommended that you turn the V.34 mode off to send data. [ECM Off]: ECM is an error correction mode defined by ITU-T (International Telecommunication Union - Telecommunication Standardization Sector). Fax machines equipped with the ECM feature communicate with each other, confirming that the sent data is free of errors. This prevents image blurring caused by telephone line noise. The communication time can be reduced by setting ECM to OFF for transmission. However, an image error or communication error may occur depending on the specified communication time value, so change the value to suit conditions. [International Communication]: Used to send a fax to areas where communication conditions are poor. Faxes are sent at a lower speed. [Check Destination]: 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 10-22.


Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.7 Registering an Internet Fax Address

An Internet fax address can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [Internet Fax], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[E-mail]	Enter the E-mail address of the destination (using up to 320 characters, excluding spaces).
[Fax Resolution]	Select the resolution that is available for the recipient machine.
[Paper Size]	Select the paper size that is available for the recipient machine.
[Compression Type]	Select a compression type that is available for the recipient machine.

Setting	Description
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.


Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.8 Registering an IP Address Fax Destination

An IP address fax destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [IP Address Fax], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[Destination Type]	Select the format to specify the destination address (default: [IP Address]).
[Address]	Enter the destination address. <ul style="list-style-type: none"> • If [IP Address] is selected for [Destination Type], enter the destination IP address. Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" • If [Host Name] is selected for [Destination Type], enter the destination host name. Example to enter the host name: "host.example.com" (Include the domain name to enter.) • If [E-mail Address] was selected for [Destination Type], enter the destination E-mail address. To specify a destination with an E-mail address, enter the recipient's IP address following "ipaddrfax@". To enter an IP address, enclose it with brackets []. Example to enter the IP address (IPv4): "ipaddrfax@[192.168.1.1]" Example to enter the IP address (IPv6): "ipaddrfax@[fe80::220:6bff:fe10:2f16]" The host name cannot be entered following symbol "@" of the E-mail address.
[Port No.]	If necessary, change the port number (default: [25]).
[Destination Machine Type]	Select whether the destination machine supports the color mode (default: [Mono Model]).
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.


Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.1.9 Registering an IP Fax (SIP) Destination

An IP fax (SIP) destination can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

Select [Store Address] - [Address Book] - [New Registration] in user mode or administrator mode of **Web Connection**. In [Select Destination], select [IP-FAX(T38)], and configure the following settings.

Setting	Description
[No.]	Destination registration number. Select [Use opening number] to automatically assign the smallest available number. When you want to specify a number, select [Input directly] and then enter a number.
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[Destination Type]	Select the format to specify the destination (default: [Direct method]). <ul style="list-style-type: none"> [Direct method]: Enter the destination's host name or IP address. Select this option when directly calling the destination. [SIP server method]: Specify SIP-URI of the destination. Select this option when calling the destination via the SIP server.
[IP Address (Host Name)]	Enter the destination's host name or IP address. <ul style="list-style-type: none"> Example to enter the host name: "host.example.com" (Include the domain name to enter.) Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the port number (default: [5060]).
[SIP-URI/SIP User Name]	Enter the destination's SIP-URI. Entry example: "sip:abc@example.com" When only the SIP user name is entered, the SIP domain name of this machine is used as the destination's domain name.
[Connection Mode]	Select the transport protocol (default: [UDP]).

Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].

13.2 Registering a Group

A group can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

Select [Store Address] - [Group] - [New Registration] in user mode or administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Name]	Enter the destination name (using up to 24 characters).
[Index]	Select an index to search for a destination using the registered name. For a frequently used destination, select the [Main] check box. The destinations are displayed on the destination selection screen, enabling the user to easily select a destination.
[Scan/Fax Address]	Select the one-touch destinations you want to include in the group from [Search from List]. You can register up to 500 one-touch destinations in a group. If necessary, different types of one-touch destinations can be registered as one group.
[Check Destination]	Allows you to view one-touch destinations registered in a group.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

Tips

- To edit or delete a registered destination, specify the target destination in the destination list, and select [Edit] or [Delete].
- The IP fax (SIP) address cannot be registered in a group with other addresses.

13.3 Registering a program

13.3.1 Registering an E-mail address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the E-mail address program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [E-mail], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination E-mail address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination E-mail address, select [Direct Input] and enter the address. To register certificate information select the [Registration of Certification Information] check box. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.2 Registering an FTP program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the FTP program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [FTP], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination FTP from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination FTP, select [Direct Input] and enter the FTP. <ul style="list-style-type: none"> [Host Address]: Enter the destination host name or IP address (using up to 253 bytes). [File Path]: Enter the folder name of the host specified in [Host Address] (using up to 127 bytes). [User ID]: Enter the available user name to log in (using up to 64 characters) if authentication is required in the FTP server. [Password]: Enter the password (using up to 64 characters, excluding "). [anonymous]: When authentication is not required in the FTP server, set this option to ON (default: OFF). [PASV Mode]: When PASV mode is used in your environment, set this option to ON (default: OFF). [Proxy]: When a proxy server is used in your environment, set this option to ON (default: OFF). [Port No.]: If necessary, change the port number (default: [21]). Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.

Setting	Description
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.3 Registering an SMB program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the SMB program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [SMB], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination SMB from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination SMB, select [Direct Input] and enter the SMB. <ul style="list-style-type: none"> [Host Address]: Enter the destination computer name (host name) or full computer name (FQDN) (using up to 253 bytes). If you cannot specify the computer name or full computer name, enter the IP address. [File Path]: Enter the shared folder name of the host specified in [Host Address] (using up to 255 bytes). [User ID]: Enter the name of a user with folder access rights (using up to 64 characters). [Password]: Enter the password (using up to 64 characters, excluding ") to access the folder. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.4 Registering a WebDAV program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the WebDAV program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [WebDAV], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).

Setting	Description
[Destination Information]	Click [Search from List], and select a destination WebDAV from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination WebDAV, select [Direct Input] and enter the WebDAV. <ul style="list-style-type: none"> [Host Address]: Enter the destination host name or IP address (using up to 253 bytes). [File Path]: Enter the folder name of the host specified in [Host Address] (using up to 255 bytes). [User ID]: Enter the name of a user with folder access rights (using up to 64 characters). [Password]: Enter the password (using up to 64 characters, excluding ") to access the folder. [SSL Settings]: When SSL is used in your environment, set this option to ON (default: OFF). Setting this option to ON changes [Port No.] to [443]. [Proxy]: When a proxy server is used in your environment, set this option to ON (default: OFF). [Port No.]: If necessary, change the port number (default: [80]). Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.5 Registering a User Box program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the User Box program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [User Box], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination User Box from the list. Click [Check Destination] to check registered address books. If you wish to manually specify a destination User Box, select the [Direct Input] option. Click [Search from List], and select a destination User Box from the list. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

13.3.6 Registering a fax address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the fax address program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [Fax], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination fax address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination fax address, select [Direct Input] and enter the address. <ul style="list-style-type: none"> [Destination]: Enter the destination's fax number. [Communication Setting]: As necessary, specify how to send a fax to a destination you wish to register. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the option settings for fax transmission. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.7 Registering an Internet fax address program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the Internet fax address program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [Internet Fax], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination Internet fax address from the list. Click [Check Destination] to check registered address books. If you wish to manually enter a destination Internet fax, select [Direct Input] and enter the FTP. <ul style="list-style-type: none"> [E-mail Address]: Enters the destination E-mail address. [Fax Resolution]/[Paper Size]/[Compression Type]: Select the specifications of original data that the recipient machine can receive. Only one destination can be specified.
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.8 Registering an IP address fax program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the IP address fax program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [IP Address Fax], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	<p>Click [Search from List], and select a destination IP address fax from the list. Click [Check Destination] to check registered address books.</p> <p>If you wish to manually enter a destination IP address fax, select [Direct Input] and enter the IP address fax.</p> <ul style="list-style-type: none"> [Destination Type]: Select the format to specify the destination address (default: [IP Address]). [Address]: Enter the destination address. If [IP Address] is selected for [Destination Type], enter the destination IP address. Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" If [Host Name] is selected for [Destination Type], enter the destination host name. Example to enter the host name: "host.example.com" (Include the domain name to enter.) If [E-mail Address] was selected for [Destination Type], enter the destination E-mail address. To specify a destination with an E-mail address, enter the recipient's IP address following "ipaddrfax@". To enter an IP address, enclose it with brackets []. Example to enter the IP address (IPv4): "ipaddrfax@[192.168.1.1]" Example to enter the IP address (IPv6): "ipaddrfax@[fe80::220:6bff:fe10:2f16]" The host name cannot be entered following symbol "@" of the E-mail address. [Port No.]: If necessary, change the port number (default: [25]). [Destination Machine Type]: Select whether the destination machine supports the color mode (default: [Mono Model]).
[Basic Setting]/[Application Setting]	Configure the Scan option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.9 Registering a group program

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

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

The following describes the group program.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [Group], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Destination Information]	Click [Search from List], and select a destination group from the list. Click [Check Destination] to check registered address books.
[Basic Setting]/[Application Setting]	Configure the scan/fax transmission option settings. For details, refer to page 13-15.

Setting	Description
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.10 Registering a program without destination

A program can be registered or edited using **Web Connection**. Although character input is a difficult process using the **Touch Panel**, it can be carried out easily if you use the computer.

The following describes the program that does not specify a destination. You can only register the scan/fax transmission option settings with the program so that it can apply to various types of destinations.

Select [Store Address] - [Program] - [Registration] in user mode or administrator mode of **Web Connection**. In [Search from Function], select [No Destination], and configure the following settings.

Setting	Description
[Name]	Enter the name of the program (using up to 24 characters).
[Basic Setting]/[Application Setting]	Configure the scan/fax transmission option settings. For details, refer to page 13-15.
[Limiting Access to Destinations]	Limit access to this destination, if necessary. For details, refer to page 10-22.

13.3.11 Configuring the scan/fax transmission option settings

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

In [Basic Setting], configure the basic option settings for the scan/fax mode.

Setting	Description
[Fax Resolution]/[Scan Resolution]	Select a resolution to use to scan the original (default: [Fine]/[300 × 300]).
[File Type]	Select the file type used for saving the scanned original data (default: [Compact PDF]). The available file types are PDF, TIFF, JPEG, XPS, PPTX, DOCX, XLSX, and other types. You should use the password encrypted PDF file format to store important original data.
[Outline PDF]	The text is extracted from the original and converted into a vector image (default: OFF). This can be configured when the [File Type] is set to [Compact PDF].
[PDF Web Optimization]	Optimizes a PDF file to quickly load the first page in the Web browser (default: OFF). This option is available when [File Type] is set to [PDF] or [Compact PDF] while the PDF processing function is enabled.
[PDF/A]	Selecting [PDF/A-1a] or [PDF/A-1b] allows you to create a PDF file based on PDF/A (default: [OFF]). This option is available when [File Type] is set to [PDF] or [Compact PDF] while the PDF processing function is enabled.
[Searchable PDF]	Creates a searchable PDF file using OCR character recognition technology (default: OFF). This option is available when [File Type] is set to [PDF] or [Compact PDF] while the searchable PDF function is enabled. <ul style="list-style-type: none"> [Language Selection]: Select a language for OCR processing. Select the language used in the original to correctly recognize text data. [Adjust Rotation]: Select [Adjust] to automatically perform the rotation adjustment for each page based on the direction of text data detected by OCR processing. [Document Name Auto Extraction]: Select [ON] to automatically extract a character string appropriate for a document name from the OCR character recognition result, and specify it as a document name.

Setting	Description
[Character Recognition]	<p>Creates a searchable file using the OCR character recognition technology (default: [OFF]).</p> <p>This option is available when [File Type] is set to [PPTX], [DOCX], or [XLSX] while the searchable PDF function is enabled.</p> <ul style="list-style-type: none"> [Language Selection]: Select a language for OCR processing. Select the language used in the original to correctly recognize text data. [Adjust Rotation]: Select [Adjust] to automatically perform the rotation adjustment for each page based on the direction of text data detected by OCR processing. [Output Method]: Select how to create a file using the text detected by OCR processing. The selectable output method varies depending on the file type you have selected in [File Type].
[File Name]	If necessary, change the file name of the scanned original.
[Page Setting]	<p>Select a filing page unit when the original consists of multiple pages (default: [Multi Page]).</p> <ul style="list-style-type: none"> [Multi Page]: Converts all pages to a single file. However, if [File Type] is set to [JPEG], you cannot select [Multi Page]. [Page Separation]: Used to convert the specified number of pages as a single file.
[Subject]	Click [Subject List] or select a fixed phrase used as the E-mail subject. If you select [Normal], the subject specified by default will be inserted. When necessary, it can be changed before transmission (default: [Normal]).
[Text]	Click [Text List] or select a fixed phrase used as the E-mail body. If you select [Normal], the body specified by default will be inserted. When necessary, it can be changed before transmission (default: [Normal]).
[File Attachment Setting]	<p>You can select the E-mail attachment method when the destination is an E-mail address and [Page Setting] is set to [Page Separation] (default: [All Files Sent as one (1) E-mail]).</p> <ul style="list-style-type: none"> [All Files Sent as one (1) E-mail]: Attaches all files to a single E-mail. [One (1) File per E-Mail]: Sends one E-mail for each file.
[Simplex/Duplex]	<p>Select whether to scan the front and back sides of an original automatically (default: [1-Sided]). You can only scan a single side of the first page and both sides of the remaining pages automatically.</p> <ul style="list-style-type: none"> [1-Sided]: Scans one side of an original. [2-Sided]: Scans both sides of an original. [Cover Sheet + 2-Sided]: Scans a single side of the first page, and scans both sides of the remaining pages.
[Original Type]	Select the optimum settings for the original to scan it in the optimum image quality (default: [Text Printed Photo]).
[Color]	<p>Select a color mode for scanning originals (default: [Auto]).</p> <p>There are four color modes: [Auto] that fits the original color, [Full Color], [Gray Scale], and [Black and White].</p>
[Separate Scan]	<p>When loading the number of original sheets, which is so large that they cannot be loaded into the ADF at the same time, in several batches and handling them as one job, set this option to ON (default: OFF).</p> <p>You can also scan the original using both ADF and Original Glass alternately.</p>
[Density]	Adjust the density (Dark or Light) to scan the original (default: [0(Standard)]).
[Background Removal]	<p>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 (default: [Bleed Removal]).</p> <ul style="list-style-type: none"> [Bleed Removal]: Select this option to prevent bleeding of the back of the paper when printing a 2-sided original that is so thin that the contents of the back side would be scanned. [Discoloration Adjust]: Select this option to scan an original with the colored background such as a map.
[Scan Size]	Select the size of the original to be scanned (default: [Auto]).

In [Application Setting], configure the application option settings for the scan/fax mode.

Setting	Description
[E-mail Notification]	Send an E-mail, which contains a destination where to save original data, to a specified E-mail address after SMB transmission, FTP transmission, WebDAV transmission, or User Box filing has been ended (default: OFF). Click [Search from List], and select a destination E-mail address from the list. You can manually enter an E-mail address.
[Timer TX]	To set a time to start fax transmission, select [ON] (default: [OFF]). Also specify when to start fax transmission.
[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] (default: [OFF]). Also enter the password.
[F-Code]	Select [Enable] to enable F-Code TX (default: [Disable]). Also enter [SUB Address] and [Password].
[Original Direction]	When scanning a 2-sided original etc., you can specify the original loading direction so that the vertical direction is set correctly (default: [Top]).
[2-Sided Binding Direction]	Select the binding position of original when scanning both sides of the original (default: [Auto]).
[Special Original]	Select an original type when scanning special documents (default: [Not Specified]). <ul style="list-style-type: none"> • [Same Width]: Even for an original with pages of different sizes, when the width of the original to be scanned is the same, by using the ADF, you can scan data while detecting the size of each page. • [Z-Folded Original]: Even folded originals, the original size can be detected accurately. • [Long Original]: Load a long original that cannot be placed on the Original Glass and that is larger in the feeding direction than the full standard size (8-1/2 × 14) into the ADF. There is no need to enter the original size in advance, ADF will detect the size automatically.
[Skip Blank Page(s) During Scan]	When scanning an original that contains blank pages, select whether to exclude blank pages from scanning (default: OFF).
[Book Original]	You can scan two-page spreads such as books and catalogs separately into left and right pages, or scan them as one page (default: OFF). <ul style="list-style-type: none"> • [Method]: Select a method to scan two-page spreads from [Book Spread], [Separation], [Front Cover], and [Front/Back Cover]. • [Center Erase]: Erases the shadow created in the center when the original cover cannot be closed properly due to the thickness of the original. • [Bind Direction]: If [Separation], [Front Cover] or [Front/Back Cover] is selected for [Method], select an output bind position of two-page spreads to be scanned. Select [Left Bind] for originals of left binding, and [Right Bind] for originals of right binding.
[Frame Erase]	Erase four sides of the original to the specified width (default: OFF). You can erase the four sides of the original to different widths.
[Compose(Date/Time)]	When printing on a specified page the date/time that the original was scanned, set this option to ON (default: OFF). You can select a print position in the page and format.
[Compose(Page)]	When printing all the page numbers and chapter numbers, set this option to ON (default: OFF). You can select a print position and format.
[Compose(Header/Footer)]	When printing a text or date/time on the top and bottom margins in a specified page, set this option to ON (default: OFF). Select a content from previously registered ones.
[Compose(Stamp)]	When printing a text such as "PLEASE REPLY" and "DO NOT COPY" on the first page or all pages, set this option to ON (default: OFF). You can select the text to be printed from the registered fix stamps and arbitrary registered stamps.
[Stamp Combine Method]	When combining date/time, page, header/footer, and stamp, select whether to combine them as text or an image (default: [Image]).

13.4 Registering a temporary one-touch destination

The temporary one-touch function registers a combination of address information and the scan/fax transmission option settings temporarily with this machine.

A temporary one-touch destination is deleted once data is sent to the registered destination or when the machine is turned OFF.

Select [Store Address] - [Temporary One-Touch] in user mode or administrator mode of **Web Connection**, and configure each setting. The temporary one-touch destination to be registered is the same as the registered program address.

 **Tips**

- However, [Registration of Certification Information] and [Limiting Access to Destinations] are not available for temporary programs.

13.5 Registering the subject and body of an E-mail

Registering the subject

Register a fixed subject phrase of the E-mail message. You can register up to 10 subject phrases.

Select [Store Address] - [Subject] - [Edit] in user mode or administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Subject]	Enter a fixed subject phrase (using up to 64 characters).

Tips

- To edit or delete a registered subject, specify the target subject in the subject list, and select [Edit] or [Delete].

Registering the body

Register a fixed message text phrase of the E-mail message. You can register up to 10 message text phrases.

Select [Store Address] - [Text] - [Edit] in user mode or administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Text]	Enter a fixed text phrase (using up to 256 characters).

Tips

- To edit or delete a registered text, specify the target text in the text list, and select [Edit] or [Delete].

13.6 Registering a prefix and suffix of each destination

Register a prefix and suffix of an E-mail address. Using prefix/suffix setting, you can recall the prefix and suffix registered when entering an E-mail address.

Up to 8 prefixes/suffixes can be registered. It is convenient to specify the frequently used prefix or suffix as the default when registering multiple prefixes or suffixes.

- 1 Select [Store Address] - [Prefix/Suffix Setting] in administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[AddressEnport]	When using the prefix/suffix setting function, set this option to ON (default: OFF).

- 2 Select [Store Address] - [Prefix/Suffix] - [Edit] in administrator mode of **Web Connection**, and configure the following settings.

Setting	Description
[Prefix]	Enter the prefix (using up to 20 characters).
[Suffix]	Enter the suffix (using up to 64 characters).

Tips

- To edit or delete a registered prefix or suffix, specify the target one in the prefix/suffix list, and select [Edit] or [Delete].

13.7 Registering the information to be added to header/footer

When printing an original, you can recall the registered header/footer and print it at the top or bottom of a page. Up to 20 headers/footers can be registered.

Select [System Settings] - [Stamp Settings] - [Header/Footer Registration] - [Check/Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Name]	Enter the name of the header or footer to be registered (using up to 16 characters).
[Color]	Select the color of the text to be printed.
[Pages]	Select the range of pages on which the text is printed in the header/footer.
[Size]	Select the size of the text to be printed.
[Text Type]	Select the font of printing texts.
[Date/Time Setting]	Select the display format of date and time if the [Date/Time Setting] of [Header] or [Footer] is set to [Print].
[Distribution Number]	Specify the content of distribution number to be displayed if the [Distribution Number] of [Header] or [Footer] is set to [Print]. <ul style="list-style-type: none"> [Primary Field]: Enter a text to be added to the distribution number for printing (using up to 20 characters). [Output Method]: Select the number of digits. [Start Number Specification]: Specify the number to start distribution numbers.
[Header]/[Footer]	Specify the items to be printed on header/footer. <ul style="list-style-type: none"> [Header String]/[Footer String]: Enter a text to be printed (using up to 40 characters). Select whether to print [Date/Time Setting], [Distribution Number], [Job Number], [Serial Number] (Engineering number of the machine), and [User Name/Account Name].

Tips

- To edit or delete a registered header/footer, specify the target one in the header/footer list, and select [Check/Edit] or [Delete].

13.8 Adding a font/macro

Add a font or macro to this machine. Also delete the registered font or macro.

In the administrator mode, select [Maintenance] - [Edit Font/Macro] - [New Registration] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Type]	Select a type of font or macro to be registered.
[ID]	Enter the ID of the font/macro. This item cannot be configured if the PS font, OOXML font, or PS macro is selected. If you enter an ID that has already been used, the existing ID will be overwritten by it.
[Location]	Select the storage location of the font/macro. Save the OOXML font in the hard disk (HDD).

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- When using any OOXML font not installed on this machine to print an OOXML file using the Direct Print function, you can add the OOXML font to this machine. TrueType and OpenType can be added as the OOXML fonts. For details on the direct print function, refer to "User's Guide[Print Operations]/[Other Printing Method]".

13.9 Registering a paper name and paper type

Register a paper name and paper type as custom paper. Custom paper can be added to the paper type option.

- 1 Select [System Settings] - [Set Paper Name by User] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Set Paper Name by User]	When using custom paper, set this option to ON (default: OFF).

- 2 Select [System Settings] - [Set Paper Name by User] - [Edit Paper Name] - [Edit] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Paper Name]	Enter the paper name (using up to 12 characters) (default: [CUSTOM]).
[Paper Type]	Select the paper type (default: [Plain Paper]).

13.10 Using data management utility

13.10.1 Data Management Utility

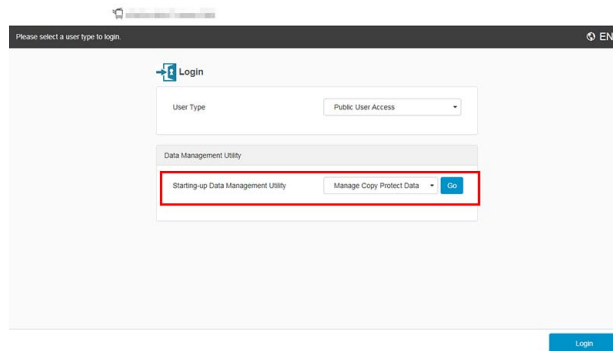
Data Management Utility is a tool capable of managing copy protect data, stamp data, and font/macro data of this machine from a computer on the network.

Start up Data Management Utility from the **Web Connection** login page.

Follow the below procedure to use Data Management Utility.

- ✓ You cannot start up multiple Data Management Utilities at the same time.

- 1 In the **Web Connection** login page, select the Data Management Utility to be started.



- For details on [Manage Copy Protect Data], refer to page 13-24.
- For details on [Manage Stamp Data], refer to page 13-26.
- For details on [Manage Font/Macro], refer to page 13-27.

- 2 Enter the administrator password of this machine, then click [OK].
 - When the registered user who has administrator privileges logs in, select [Registered User], then enter the user name and password.
 Data Management Utility starts up.

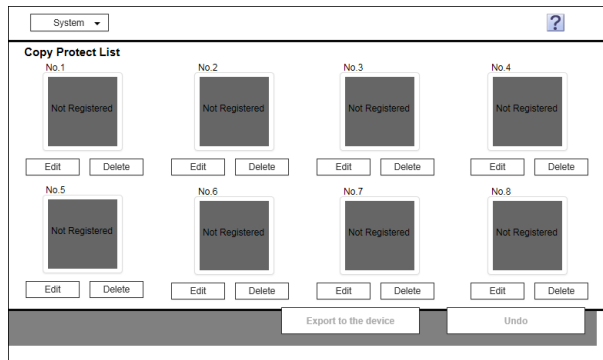
13.10.2 Managing the copy protect data

Copy Protect is a function that prints a text such as "Copy" and "Private" as a concealed text in all pages.

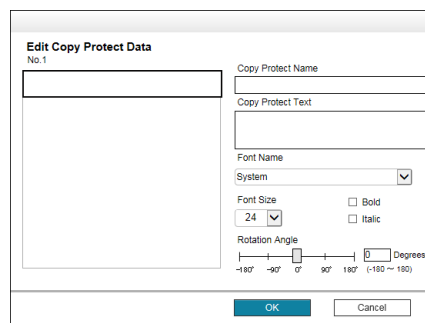
You can register or edit copy protect data using Data Managing Utility. Up to eight units of copy protect data can be managed.

- 1 In the **Web Connection** login page, start the [Manage Copy Protect Data].
The copy protect data list registered on this machine appears.

- 2** To register or edit the copy protect data, click [Edit].
- Clicking [Delete] deletes the registered copy protect data. The copy protect data will not be deleted until you click [Export to the device] and write it to this machine.



- 3** Register or edit the copy protect data, and click [OK].
- You can edit data while checking the result in the preview.



Setting	Description
[Copy Protect Name]	Enter the Copy Protect name (using up to 16 characters).
[Copy Protect Text]	Enter a text to be printed (using up to 32 characters).
[Font Name]	Select the font type of the text.
[Font Size]	Select the size of the text to be printed.
[Bold]	Select this check box to display the text in bold.
[Italic]	Select this check box to display the text in italic.
[Rotation Angle]	Specify the rotation angle of the text. The angle can be adjusted in increments of one degree.

- 4** Click [Export to the device].
- Clicking [Undo] returns to the state before the change.
- The registered or edited copy protect data is written to this machine.

Tips

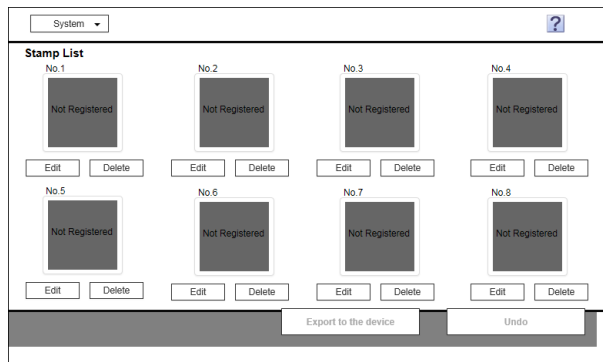
Clicking [System] displays the system menu. The following menu items are available in the system menu.

- [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
- [Export]: Save the data registered on this machine to the computer as a file.
- [Export to SMB]: Save the data registered on this machine to the SMB sharing folder as a file.
- [Import]: Write the data stored in a file to this machine.
- [Exit]: Exit the utility.

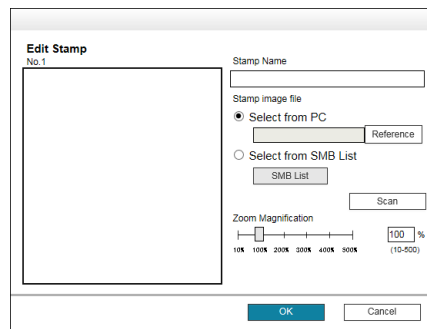
13.10.3 Managing the stamp data

You can register or edit stamp data using Data Managing Utility. Up to eight units of stamp data can be managed. You cannot edit or delete stamp data that was registered on this machine when it was shipped.

- 1 In the **Web Connection** login page, start the [Manage Stamp Data].
The stamp data list registered on this machine appears.
- 2 To register or edit the stamp data, click [Edit].
→ Clicking [Delete] deletes the registered stamp data. The stamp data will not be deleted until you click [Export to the device] and write it to this machine.



- 3 Register or edit the stamp data, and click [OK].
→ You can edit data while checking the result in the preview.



Setting	Description
[Stamp Name]	Enter the stamp name (using up to 16 characters).
[Stamp image file]	Specify the location of the image file (BMP) to be used as a stamp. <ul style="list-style-type: none"> • [Select from PC]: Click [Reference], then select an image file to be imported from your computer. • [Select from SMB List]: Click [SMB List], then select an image file to be imported from the SMB sharing folder.
[Scan]	Enlarges a stamp image. You can check the image details.
[Zoom Magnification]	Specify the zoom ratio of the stamp image. The ratio can be adjusted in increments of 1%.

- 4 Click [Export to the device].
→ Clicking [Undo] returns to the state before the change.
The registered or edited stamp data is written to this machine.

 **Tips**

Clicking [System] displays the system menu. The following menu items are available in the system menu.

- [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
- [Export]: Save the data registered on this machine to the computer as a file.
- [Export to SMB]: Save the data registered on this machine to the SMB sharing folder as a file.
- [Import]: Write the data stored in a file to this machine.
- [Exit]: Exit the utility.

13.10.4 Managing the font/macro data

You can add or delete font/macro data using Data Managing Utility.

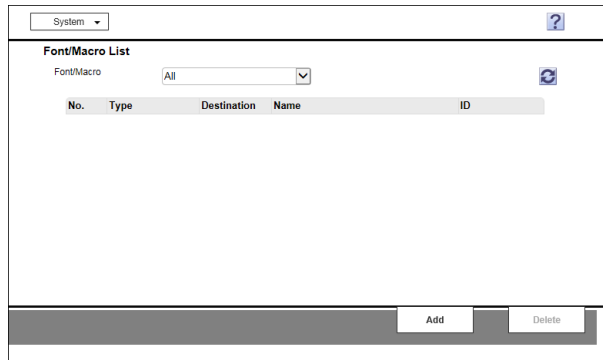
1 In the **Web Connection** login page, start the [Manage Font/Macro].

The font/macro data list registered on this machine appears.

2 To add font or macro data, click [Add].

→ The lists of font and macro can be switched by [Font/Macro].

→ Clicking [Delete] deletes the selected font or macro data.



The screenshot shows a web interface for managing font and macro data. At the top, there is a 'System' dropdown menu and a help icon. Below this, the title 'Font/Macro List' is displayed. Underneath the title, there is a 'Font/Macro' label and a dropdown menu currently set to 'All'. To the right of this dropdown is a refresh icon. Below these elements is a table with the following headers: 'No.', 'Type', 'Destination', 'Name', and 'ID'. The table body is currently empty. At the bottom of the interface, there are two buttons: 'Add' and 'Delete'.

3 Specify the font or macro to be added, and click [OK].

Setting	Description
[Type]	Select a type of font or macro to be added.
[Destination]	Select where to save font or macro. <ul style="list-style-type: none"> • [HDD]: Save data in the storage of this machine. • [RAM]: Save the font or macro to the memory on this machine. When you turn off the power of the machine, the saved font/macro will be erased. To continuously use font or macro data, save it in the storage. Save the OOXML font in the storage.
[ID]	Enter a font or macro ID number for PCL font or PCL macro. If it is not entered, the available ID is assigned automatically.
[Add File]	Select a font file or macro file to be added. <ul style="list-style-type: none"> • [Select from PC]: Click [Reference], then select a file to be added from your computer. • [Select from SMB List]: Click [SMB List], then select a file to be added from the SMB sharing folder.

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".
- Clicking [System] displays the system menu. The following menu items are available in the system menu.
 - [Auto Protect Setting]: Lock the computer screen if a specified amount of time has elapsed without the machine being operated. You can change the time until the screen is locked.
 - [Exit]: Exit the utility.

14

Associating with External Application

14 Associating with External Application

14.1 Using the Web Browser Function

Enabling the Web browser function

Configure the settings to use the Web browser function.

Select [Network] - [Web Browser Setting] - [Web Browser Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Web Browser]	When using the Web browser function, set this option to ON (default: OFF).



Tips

- If the Web browser function is switched to Enable or Disable, this machine restarts automatically.

Restricting file operations on a Web browser

Select whether to allow file operations in the site displayed on the Web browser.

Select [Network] - [Web Browser Setting] - [File Operation Permission Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Upload]	Select whether to upload the data scanned on this machine (default: [ON]). To allow uploading of data to only the specified site, select [Permitted URL Only], then enter the URL of the site to allow uploading of files to (using up to 256 characters).
[Download]	Select whether to download files to this machine (default: [ON]). When you allow downloading of data from only the specified site, select [Permitted URL Only], then enter the URL of the site to allow downloading of files from (using up to 256 characters).

Specifying the operation to be performed when an SSL certificate verification error occurs

Specify the operation to be performed when an SSL certificate verification error occurs in the destination website.

Select [Network] - [Web Browser Setting] - [SSL Certificate Verify error settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Web Browser]	Select the operation to be performed when an SSL certificate verification error occurs in the Web browser (default: [Popup display (Display only once in the same certificate)]). <ul style="list-style-type: none"> • [Connect to the contents]: Connect to the website without displaying a confirmation message. • [Popup display (Display only once in the same certificate)]: Displays a confirmation message only when the first error occurs for each certificate. • [Popup display (Always display)]: Displays a confirmation message each time an error occurs. • [Do not connect to the Contents]: Does not connect to the website in which an error occurs.
[OpenAPI.IWS Application]	Select the operation to be performed when an SSL certificate verification error occurs in the OpenAPI, IWS application.

Configuring settings to display contents

Configure settings to display contents of the Web browser.

Select [System Settings] - [Web Browser Setting] - [General] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Home page]	Enter a URL of a page to be registered as a home page.
[Start up]	Select a page to be displayed when the Web browser has been started (default: [Home page]).
[WebData]	Specify the method to delete web data saved on this machine. <ul style="list-style-type: none"> [Delete All Web Data]: Deletes all the web data (Cookie, Web Storage, and Indexed Database) saved on this machine. [Web Data Delete Schedule]: Select a timing to delete web data (Cookie, Web Storage, and Indexed Database) from this machine (default: [Delete (During Logout/During Timeout)]).
[Authentication Information]	Specify the method to delete authentication information saved on this machine. <ul style="list-style-type: none"> [Delete all Authentication Information]: Deletes all the authentication information saved on this machine. [Delete Auth. Info. Conditions]: Select a timing to delete authentication information from this machine (default: [Delete (During Logout/During Timeout)]).
[Font]	Select a required font when displaying contents with no font specified.

Managing bookmarks

Add or edit a bookmark. To apply the changed contents to this machine, click [Export to the device].

Select [System Settings] - [Web Browser Setting] - [Favorites] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[New Registration]	Select this to add a bookmark to the list. Specify a registration number, then enter the title and URL.
[Delete All]	Select this to delete all bookmarks from the list.
[Edit]	Select this to change the registered contents of a bookmark.
[Delete]	Select this to delete a bookmark from the list.
[Export to the device]	Select this to apply the contents added, edited, or deleted in the list to this machine.
[Undo]	Select this to return the changed contents of the list.

Managing the history

Delete the history of the Web browser. To apply the changed contents to this machine, click [Export to the device].

Select [System Settings] - [Web Browser Setting] - [History] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Delete All]	Select this to delete all histories from the list.
[Search by number.]	Select the range of registration numbers, then click [Go] to change the items displayed in the list.
[Delete]	Select this to delete a history from the list.
[Export to the device]	Select this to apply the contents deleted in the list to this machine.
[Undo]	Select this to return the changed contents of the list.

Setting Web browser operations

Configure settings for Web browser operations.

Select [System Settings] - [Web Browser Setting] - [Detail Settings] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Cache]	Configure the cache function of the Web browser. <ul style="list-style-type: none"> • [Enable Cache]: Select [ON] to use the cache function (default: [ON]). • [Delete Cache]: Select this button to delete all the cache data stored in this machine. • [Delete Cache Conditions]: Select a timing to delete cache data (default: [Do Not Delete]).
[WebData]	[Enable Storage]: Select [Enable] to use Web Storage (default: [Enable]).
[JavaScript]	[Use JavaScript]: Select [Enable] to enable JavaScript embedded in the page (default: [Enable]).
[Software Keyboard]	[Use Software keyboard with priority]: Select [ON] to enter a text using the keyboard displayed on the screen even when an external keyboard is installed on this machine (default: [OFF]).
[Proxy Settings]	Configure the settings to use a proxy server. To use a proxy server, enter its address and port number. When using proxy authentication, enter the account name to log in to the proxy server. In [No Proxy for following domain], you can specify a domain that is not connected via a proxy server. Enter the IP address or domain name of the domain.
[Security Settings]	Configure the settings for SSL communications. <ul style="list-style-type: none"> • [Enable SSL Version]: Select the SSL or TLS version to be used in each of the highest and lowest security levels. • [SSL communication of SHA1 certificate]: Select whether to allow the user to use the certificate signed in the SHA-1 algorithm (default: [Allow with Warning]). Selecting [Allow with Warning] displays a message to check whether to permit an SSL communication based on the SHA-1 certificate.

14.2 Using TCP Socket

Setting flow

To use application that communicates with this machine via TCP Socket, configure the TCP Socket settings of this machine.

If a certificate for this machine is registered, you can encrypt communication between the machine and application using SSL.

To perform the association via TCP Socket, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for TCP Socket (page 14-5)
- 3 Configuring settings to suit your environment
 - Establishing SSL communication (page 14-5)

Tips

- If you installed user authentication using an external authentication server, SSL communication settings are required.

Configuring the basic TCP Socket settings

Configure settings to establish a communication via TCP Socket.

Select [Network] - [TCP Socket Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[TCP Socket]	When using TCP Socket, set this option to ON (default: ON). <ul style="list-style-type: none"> • [Port No.]: If necessary, change the TCP Socket port number (default: [59158]).

Tips

- If you change multiple port numbers collectively in **Web Connection** or on the screen of this machine, a port number duplication error may appear. If a port number duplication error appears, change multiple port numbers one by one instead of changing them collectively.

Using SSL communication

Use SSL to encrypt communication between this machine and application via TCP Socket.

- 1 Register a certificate for this machine and enable SSL communication (page 11-4).
- 2 Select [Network] - [TCP Socket Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Use SSL/TLS]	When using SSL communications, set this option to ON (default: OFF). <ul style="list-style-type: none"> • [Port No.(SSL/TLS)]: If necessary, change the port number for SSL communication (default: [59159]).

14.3 Using OpenAPI

Setting flow

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

If a certificate for this machine is registered, you can use SSL to encrypt communication between this machine and a client when the machine acts as a server.

By using the Simple Service Discovery Protocol (SSDP) function of this machine, you can associate with OpenAPI connection application smoothly.

To perform the association via OpenAPI, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring basic settings for OpenAPI authentication (page 14-6)
- 3 Configuring settings to suit your environment
 - Using the proxy server (page 14-7)
 - Establishing SSL communication (page 14-7)

Configure the basic OpenAPI settings

Configure settings to establish a communication via OpenAPI.

- 1 Select [Network] - [SSDP Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SSDP]	When enabling SSDP, set this option to ON (default: ON). This allows for the following actions: <ul style="list-style-type: none"> • Notifying of OpenAPI service having started on this machine. • Returning a response to a search for OpenAPI service.
[Multicast TTL Setting]	Change TTL (Time To Live) for SSDP multi-cast packet if necessary (default: [1]).

- 2 Select [Network] - [OpenAPI Setting] - [OpenAPI Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Port No.]	If necessary, change the port number for OpenAPI communication (default: [50001]).
[HTTP Version Setting]	Select the version of the protocol for HTTP communication (default: [HTTP/1.1]). <ul style="list-style-type: none"> • [HTTP/1.1]: Uses HTTP/1.1 only. • [HTTP/2, HTTP/1.1]: Uses HTTP/2 when connected to HTTP/2. In other cases, HTTP/1.1 is used.

Tips

- If you change multiple port numbers collectively in **Web Connection** or on the screen of this machine, a port number duplication error may appear. If a port number duplication error appears, change multiple port numbers one by one instead of changing them collectively.

Using a proxy server

When a proxy server is installed in your environment, register the proxy server.

Select [Network] - [OpenAPI Setting] - [OpenAPI Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Proxy Settings]	<p>Register the proxy server to suit your operating environment.</p> <ul style="list-style-type: none"> [Proxy Server Address]: Enter the proxy server address. Use one of the following formats. Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" [Proxy Server Port Number]: If necessary, change the proxy server port number to be used for HTTP (default: [8080]). [Proxy Server Port Number (HTTPS)]: If necessary, change the proxy server port number (default: [8080]). [Proxy Server Port Number (FTP)]: If necessary, change the proxy server port number to be used for FTP (default: [21]). [User Name]: Enter the user name used for proxy authentication (using up to 63 characters). [Password]: Enter the password for proxy authentication (using up to 63 characters).

Using SSL communication

Use SSL to encrypt communication between this machine and application via OpenAPI.

- 1 Register a certificate for this machine and enable SSL communication (page 11-4).
- 2 Select [Network] - [OpenAPI Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SSL/Port Settings]	<p>Select whether to use the SSL for communication or not (default: [Non-SSL Only]).</p> <ul style="list-style-type: none"> [Non-SSL Only]: Only non-SSL communication is allowed. [SSL Only]: Only SSL communication is allowed. [SSL/Non-SSL]: Both SSL communication and non-SSL communication are allowed.
[Port No.(SSL)]	<p>If necessary, change the port number for SSL communication (default: [50003]).</p>
[Certificate Verification Level Settings]	<p>To validate the certificate during SSL communication, select items to be verified.</p> <ul style="list-style-type: none"> [Client Certificates]: Select whether to request a certificate from clients that connect to this machine (default: OFF). [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).



Reference

Verifying the Peer's Certificate (page 11-20)

14.4 Using the FTP Server Function

Setting flow

To use the application that establishes a communication via the FTP server of this machine, set the FTP server function of this machine.

To use the FTP server of this machine for the association, follow the below procedure to configure the settings.

- 1 Configuring network settings of this machine (page 4-2)
- 2 Configuring the FTP server (page 14-8)

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Configuring the FTP server settings

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

Select [Network] - [FTP Setting] - [FTP Server Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[FTP Server]	When using the FTP server function of this machine, set this option to ON (default: OFF).
[Deny Reception Command]	Select a command to deny a receiving job from an FTP client (default: [Allow]). 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.
[PORT Command Enhanced Security]	When enabling the security of this machine against FTP bounce attacks, set this option to ON (default: ON). This option is not available if [Deny Reception Command] is set to [PORT/EPRT]. When a PORT/EPRT command is sent from an FTP client, the data connection is established only if both of the following conditions are satisfied: <ul style="list-style-type: none"> • 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.

14.5 Using the WebDAV Server Function

Setting flow

To use the application that establishes a communication via the WebDAV server of this machine, set the WebDAV server function of this machine.

If a certificate for this machine is registered, you can encrypt communication between the machine and application using SSL.

To use the WebDAV server of this machine for the association, follow the below procedure to configure the settings.

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring the WebDAV server (page 14-9)
- 3** Configuring settings to suit your environment
 - Establishing SSL communication (page 14-9)

Configuring the WebDAV server settings

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

Select [Network] - [WebDAV Settings] - [WebDAV Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[WebDAV Settings]	When using the WebDAV server function of this machine, set this option to ON (default: ON).
[Access Rights Settings]	Specify the password to restrict access to the WebDAV server of this machine (using up to 64 characters) (default: [sysadm]). <ul style="list-style-type: none"> • [Password is changed.]: Returns the password to the default.

Using SSL communication

Encrypt communication between this machine and the WebDAV client with SSL.

- 1** Register a certificate for this machine and enable SSL communication (page 11-4).
- 2** Select [Network] - [WebDAV Settings] - [WebDAV Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[SSL Setting]	Select whether to use the SSL for communication or not (default: [Non-SSL Only]). <ul style="list-style-type: none"> • [Non-SSL Only]: Only non-SSL communication is allowed. • [SSL Only]: Only SSL communication is allowed. • [SSL/Non-SSL]: Both SSL communication and non-SSL communication are allowed.

14.6 Using IWS

Setting flow

Configure the settings to use the IWS (Internal Web Server) function.

- 1** Configuring network settings of this machine (page 4-2)
- 2** Configuring basic settings for IWS authentication (page 14-10)
- 3** Configuring the setting to use **MarketPlace** (page 14-10)
- 4** Configuring the execution environment of the IWS application to operate preferentially (page 14-11)

Configuring the basic IWS settings

Configure the settings to use the IWS (Internal Web Server) function.

Select [Network] - [IWS Settings] - [IWS Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[IWS Settings]	When using the IWS function, set this option to ON (default: ON).
[Port Number (Web Server)]	If necessary, change the port number used to access the Web page contents uploaded to this machine (default: [8090]).
[Port Number (Application Installation)]	If necessary, change the port number to be used for dynamic contents of this machine (default: [8091]).
[Connect IWS Apps to Network]	When allowing the user to externally access the dynamic contents, set this option to ON (default: ON). This option is available when Web page contents uploaded to this machine have dynamic contents such as scripts.
[Communication Between Applications]	Configure settings to operate the IWS application installed on this machine through the IWS application installed on a different device or an external application such as an application on a mobile terminal. <ul style="list-style-type: none"> • [Permit Access for Communication between Applications]: When allowing a communication between an external application and the IWS application of this machine, set this option to ON (default: OFF). • [Authentication]: Configure authentication information for logging in to this machine that is required when an external application operates the IWS application on this machine. [User Name]: Enter the user name used for authentication (using up to eight characters). [Password]: Enter the password for authentication (using up to eight characters). • [Login Information Notification Setting]: When notifying you of the user name and password of the user who is using this machine, when the IWS application on this machine operates that of a different device, set this option to ON (default: OFF).

Configuring the setting to use MarketPlace

Configure the setting to use the application store, **MarketPlace**.

Select [Network] - [IWS Settings] - [MarketPlace Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Enable Settings]	When enabling the MarketPlace application, set this option to ON (default: ON).
[MarketPlace Account Setting]	Set the MarketPlace account to manage this machine. <ul style="list-style-type: none"> • [E-mail Address]: Enter the E-mail address (using up to 320 characters).

Configuring the execution environment of the IWS application to operate preferentially

Select [Network] - [IWS Settings] - [Memory allocation settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and select the execution environment of the IWS application to operate preferentially (default: [Python priority]).

Assign a more memory space to the selected IWS application execution environment.

14.7 Associating with the remote diagnosis system

14.7.1 Registering a proxy server used for remote diagnosis

Configure settings to use the proxy server when communicating with the remote diagnosis system.

Select [Network] - [WebDAV Settings] - [Proxy Setting for Remote Access] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Proxy Setting for Remote Access]	When using a proxy server to communicate with the remote diagnosis system, set this option to ON (default: OFF).
[Proxy Settings]	<p>Register the proxy server to suit your operating environment.</p> <ul style="list-style-type: none"> [Synchronize WebDAV Client Setting]: When using the proxy server registered in [WebDAV Client Settings] as the proxy server for remote diagnosis, set this option to ON (default: ON). [Proxy Server Address]: Enter the proxy server address. Use one of the following formats. Example to enter the host name: "host.example.com" Example to enter the IP address (IPv4): "192.168.1.1" Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16" [Proxy Server Port Number]: If necessary, change the proxy server port number (default: [8080]). [User Name]: Enter the user name used for proxy authentication (using up to 63 characters). [Password]: Enter the password for proxy authentication (using up to 63 characters).

Tips

- This setting is displayed when this machine is managed by the remote diagnosis system. For details on the remote diagnosis system, contact your service representative.

14.7.2 Allowing acquisition of the machine counter

Configure the settings to obtain the counter information of this machine from the remote diagnosis system.

Select [User Auth/Account Track] - [User/Account Common Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Counter Remote Control]	When allowing the user to acquire counter information managed on this machine while the remote diagnosis system is used, set this option to ON (default: OFF).

Tips

- This setting is available if you use the remote diagnosis system, and user authentication and account track is installed on this machine. For details on the remote diagnosis system, contact your service representative.

14.7.3 Sending the machine operating status

Send the operating status of this machine to the remote diagnosis system.

Select [Maintenance] - [Call Remote Center] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), then click [Call Remote Center].

Tips

- This setting is displayed when this machine is managed by the remote diagnosis system. For details on the remote diagnosis system, contact your service representative.

14.7.4 Allowing read and write of the machine setting information

When this machine is managed by the remote diagnosis system, the addresses (address book, group, and program) registered on this machine and authentication information (user authentication and account track) can be imported or exported from/to the remote diagnosis system.

Select [Maintenance] - [Remote Access Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Import/Export User Data]	When permitting the user to rewrite user data from the remote diagnosis system, set this option to ON (default: OFF).

 **Tips**

- This setting is displayed when this machine is managed by the remote diagnosis system. For details on the remote diagnosis system, contact your service representative.

14.8 Associating with the fax server

About association with the fax server

When using a fax server, you can configure the server for registering and using applications.

When using the fax server communicates in the E-mail format, you can configure settings to automatically add a prefix and suffix to a destination number.

Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Registering applications

Register applications and configure a server for using the application.

- 1 Select [Store Address] - [Application Registration] in user mode or administrator mode of **Web Connection** to select the location where you wish to register applications, and click [Registration/Edit].
- 2 Select [Use application template.] and select a template to be used.
 - If you do not use a template, select [Not use application template].
 - For details on template that can be used on this machine, refer to page 14-15.
- 3 Register applications and configure the server settings, then click [Next].

Setting	Description
[Application Setting]	Configure an application to be registered.
[Application Name]	Enter the application name (using up to 16 characters).
[Server Setting]	Configure a server for using the application.
[Host Address]	Enter the host address of the server for using the application (using up to 15 characters, including a period).
[File Path]	Enter the destination file path (using up to 96 characters).
[User ID]	Enter the user ID used to log in to the server (using up to 47 characters).
[Password]	Enter the password of the user name you entered into [User ID] (using up to 31 characters).
[anonymous]	When authentication is not required for the destination server, select ON.
[PASV Mode]	When a PASV server is used in your environment, select ON.
[Proxy]	When a proxy server is used in your environment, select ON.
[Port No.]	If necessary, change the port number.

- 4 Select a custom item you wish to configure, and click [Edit].
- 5 In the [Function Setting] page of the selected custom item, configure the following settings.

Setting	Description
[Button Name]	Enter the button name (using up to 16 characters).
[Function Name]	Select a function name.
[Message on Panel]	Enter the name to be displayed on the screen of this machine (using up to 32 characters).
[Display Method]	Select the method to display information on the screen of this machine.

Setting	Description
[Default Value]	Enter the default value. The number of characters that can be entered differs depending on the function selected in [Function Name]. To hide the default value, select the [Input string shown as ****] check box.
[Keyboard Type]	Select the type of the keyboard to be displayed on the screen of this machine.
[Options]	Set the option according to the function selected in [Function Name].

6 Click [OK].

Application setting templates

Web Connection provides the following templates. Each template provides different custom items predefined for each application.

[WalkUp Fax]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[Sender Name (CS)]	[Name]	[ASCII]	[Walkup]	Not specified.
2	[Fax Number (CS)]	[Personal Fax Number]	[ASCII]	Not specified.	Not specified.
3	[TEL Number (CS)]	[Personal Voice Number]	[ASCII]	Not specified.	Not specified.
4	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
5	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.

[Fax with Account]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Sender Name (CS)]	[Name]	[ASCII]	Not specified.	Not specified.
3	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
4	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
5	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
7	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.
8	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
9	[Hold For Preview]	[Hold For Preview]	Not specified.	Not specified.	[No]

[Secure Docs]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
3	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
4	[Delivery Method]	[Delivery]	Not specified.	Not specified.	[Secure]
5	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
7	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.
8	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
9	[Document PW]	[Document Password]	[ASCII]	Not specified.	Not specified.

[Certified Delivery]

[No.]	[Button Name]	[Function Name]	[Keyboard Type]	[Default Value]	[Options]
1	[User ID]	[ID]	[ASCII]	[Walkup]	Not specified.
2	[Password]	[Password]	[ASCII]	Not specified.	Not specified.
3	[Password Auth#]	[Authentication]	Not specified.	Not specified.	[None]
4	[Subject]	[Subject]	[ASCII]	Not specified.	Not specified.
5	[Billing Code 1]	[BillingCode1]	[ASCII]	Not specified.	Not specified.
6	[Billing Code 2]	[BillingCode2]	[ASCII]	Not specified.	Not specified.
7	[Cover Sheet Type]	[CoverSheet]	Not specified.	Not specified.	Not specified.
8	[Document PW]	[Document Password]	[ASCII]	Not specified.	Not specified.
9	[Delivery Method]	[Delivery]	Not specified.	Not specified.	[Certified]

Associating with the fax server communicating in E-Mail format

When using a fax server that communicates in the E-mail format, a prefix and a suffix can be automatically added to the destination number.

Select [System Settings] - [System Connection Setting] - [System Connection Setting] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Prefix/Suffix Automatic Setting]	To automatically add a prefix or suffix to the destination number when using a fax server that communicates in the E-mail format, set this option to ON (default: OFF). Setting to ON adds the value of registered number 01 in [Store Address] - [Prefix/Suffix].

Tips

If [Prefix/Suffix Automatic Setting] is set to ON, other settings are restricted.

- [Fax Settings] in administrator mode is not available (excluding [Destination Check Display Function], [PC-Fax Permission Setting], [Confirm Address (TX)], [Confirm Address (Register)], and [PIN Code Display Mask Function]).
- [Store Address] - [Application Registration] is not available.
- Bulletin Board User Box, Polling TX User Box, Memory RX User Box, and Fax Retransmit User Box are not available.
- Bulletin Board User Box and Relay User Box cannot be registered.
- Confidential RX is not available.
- The Off-Hook key is not available.
- You cannot configure [Fax Header Settings], [Line Setting], [Quick Memory TX], [Polling TX], [Polling RX], [Timer TX], [Password TX], and [F-Code TX] in the scan/fax mode.
- The network fax function is not available.
- [Outside], [Tone], [Pause], [-], and [Line Settings] are not available when registering a fax destination in the address book.
- No report can be output from the job display screen of this machine.
- Numbers excluding a prefix and suffix are displayed in job history.
- Send job types are handled as E-mail.
- The Fax TX in the counter is not updated.

14.9 Remote-controlling the Screen of this Machine

About operation method

You can remote-control the screen of this machine using a computer connected to the network. There are the following types of operation methods.

Operation method	Description
Using the dedicated software	This method uses the dedicated software that collects screen information of this machine periodically, and operates the screen of this machine from a computer on the network. You must prepare a dedicated remote control software program and server. Despite the burden, this method enables you to control the machine remotely even from a computer located outside the router network.
Accessing the machine directly	This method accesses this machine directly from another computer on the network, and operates the screen of this machine using a Web browser. A dedicated remote control software program is not required, but the computer used for the remote control must be able to access this machine.
Using a Mobile Terminal	This method remotely operates the screen of this machine using a mobile terminal. For details, refer to "User's Guide[Advanced Function Operations]/[Linking with a Mobile Terminal]".

Using the dedicated software

Configure settings to operate the screen of this machine using the dedicated software on a different computer.

Select [Network] - [Remote Panel Settings] - [Remote Panel Client Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Client Setting]	When operating the screen of this machine using the dedicated software on a different computer, set this option to ON (default: OFF).
[Server Address]	Enter the address of the server where the dedicated software was installed. Use one of the following formats. <ul style="list-style-type: none"> • Example to enter the host name: "host.example.com" • Example to enter the IP address (IPv4): "192.168.1.1" • Example to enter the IP address (IPv6): "fe80::220:6bff:fe10:2f16"
[Port No.]	If necessary, change the port number of the server where the dedicated software was installed (default: [443]).
[HTTP Version Setting]	Select the version of the protocol for HTTP communication (default: [HTTP/1.1]). <ul style="list-style-type: none"> • [HTTP/1.1]: Uses HTTP/1.1 only. • [HTTP/2, HTTP/1.1]: Uses HTTP/2 when connected to HTTP/2. In other cases, HTTP/1.1 is used.
[Connection Timeout]	If necessary, change the timeout time of communication with the server where the dedicated software was installed (default: [60] sec.).
[Certificate Verification Level Settings]	To validate the certificate during SSL communication, select items to be verified. <ul style="list-style-type: none"> • [Expiration Date]: Confirm whether the certificate is within the validity period (default: ON). • [CN]: Confirm whether CN (Common Name) of the certificate matches the server address (default: OFF). • [Key Usage]: Confirm whether the certificate is used according to the intended purpose approved by the certificate issuer (default: OFF). • [Chain]: Confirm whether there is a problem in the certificate chain (certificate path) (default: OFF). The chain is validated by referencing the external certificates managed on this machine. • [Expiration Date Confirmation]: Confirm whether the certificate has expired (default: OFF). The expiration date confirmation is performed in the order of OCSP (Online Certificate Status Protocol) service, and CRL (Certificate Revocation List).

Setting	Description
[Synchronize WebDAV Client Setting]	When a proxy server is installed in your environment, register the proxy server. <ul style="list-style-type: none"> [Synchronize]: Use a proxy server registered in [WebDAV Client Settings]. [Proxy Settings]: Register a required proxy server separately from the proxy server registered in [WebDAV Client Settings]. Enter the proxy server address, port number, and the user name and password required to log in to the proxy server.
[Launch Remote Panel from vCare]	When allowing the user to launch the remote panel from the remote diagnosis system, set this option to ON (default: OFF).



Reference

Verifying the Peer's Certificate (page 11-20)

Accessing the machine directly

Configure settings to operate the screen of this machine using the Web browser on a different computer.

Select [Network] - [Remote Panel Settings] - [Remote Panel Server Settings] in administrator mode of **Web Connection** (or in [Utility] - [Administrator] of this machine), and configure the following settings.

Setting	Description
[Server Setting]	When operating the screen of this machine using the Web browser on a different computer, set this option to ON (default: OFF).
[Port No.(SSL)]	If necessary, change the port number (default: [50443]).
[HTTP Version Setting]	Select the version of the protocol for HTTP communication (default: [HTTP/1.1]). <ul style="list-style-type: none"> [HTTP/1.1]: Uses HTTP/1.1 only. [HTTP/2, HTTP/1.1]: Uses HTTP/2 when connected to HTTP/2. In other cases, HTTP/1.1 is used.
[Password Authentication]	When prompting the user to enter the password for connecting to this machine, set this option to ON (default: OFF). <ul style="list-style-type: none"> [Password is changed.]: Enter the required password (using up to 64 characters).
[IP Filtering (Permit Access)]	When restricting computers to which you want to allow access to this machine using IP addresses, set this option to ON (default: OFF). Also, enter the range of IP addresses allowed to access.

14.10 Releasing the association with application

Configure settings to prevent this machine from being connected to the server when an error occurs on the server of the application associated with this machine.

Select [System Settings] - [System Connection Setting] - [System Connection Setting] in administrator mode of **Web Connection**, then configure the following settings.

Setting	Description
[Application Connection Setting]	When disconnecting this machine from an application, set this option to OFF (default: ON).



Tips

- To use this function, an option is required. For details on the required option, refer to "User's Guide[About This Machine]/[List of Functions with Options Required]".

Notice to users

Type	Notice
<ul style="list-style-type: none">• Class A items (Broadcast communications unit for business use)	This class A product is registered in Electromagnetic Compatibility, and User may be required to take adequate measures for other purposes than household use.
<ul style="list-style-type: none">• Class B items (Broadcast communications unit for household use)	This class B product is registered in Electromagnetic compatibility and is for domestic environment and also for general use.

※ This device is in the Class A items in the North America.

※ This device is in the Class B items.

