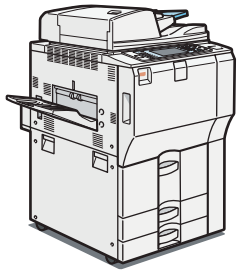
Notes for Security Functions



Read this manual carefully before you use this product and keep it handy for future reference.

Important

Contents of this manual are subject to change without prior notice. In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the machine.

Some illustrations in this manual might be slightly different from the machine.

Certain options might not be available in some countries. For details, please contact your local dealer.

Modifications For Improved Operational Security

To improve the operational security of this machine, we have modified the machine's security-related specifications. This booklet explains those modifications and contains errata for the manuals provided with the machine. Before using the machine, be sure to read carefully the manuals provided in conjunction with this booklet.

❖ How to use this booklet

- When referring to the "Security Reference" manual, refer also to the errata contained in this booklet. The errata for this manual can be found on p.2 “Security Reference Errata”, p.15 “Setting Up the Machine”, and in subsequent sections of this booklet.
- When referring to the "Copy and Document Server Reference" manual, refer also to the errata contained in this booklet. The errata for this manual can be found on p.11 “Copy and Document Server Reference Errata” of this booklet.
- When referring to the "Network and System Settings Guide" manual, refer also to the errata contained in this booklet. The errata for this manual can be found on p.12 “Network and System Settings Guide Errata” of this booklet.
- When referring to the "Facsimile Reference" manual, refer also to the errata contained in this booklet. The errata for this manual can be found on p.13 “Facsimile Reference Errata” of this booklet.
- When referring to the "Scanner Reference" manual, refer also to the errata contained in this booklet. The errata for this manual can be found on p.14 “Scanner Reference Errata” of this booklet.

Security Reference Errata

This chapter corrects errors in the supplied Security Reference. Please refer to it when reading the Security Reference.

Topic	Additional Description
Getting Started >Before Using the Security Functions	【Error】 **Important** ❒ If the security settings are not specified, the machine may be damaged by malicious attackers. 【Corrections】 **Important** ❒ If the security settings are not configured, the data in the machine is vulnerable to attack.
Getting Started >Setting Up the Machine	Some details in this section have been changed. Replace this section with p.15 “Setting Up the Machine” in this booklet.
Configuring Administrator Authentication >Enabling Administrator Authentication >Registering the Administrator	Delete the following: **Note** ❒ Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters when entering the login user name or password. If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor.
	【Error】 **Note** ❒ You can use up to 32 alphanumeric characters and symbols when registering login user names and login passwords. Keep in mind that passwords are case-sensitive. ❒ User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank. 【Corrections】 **Note** ❒ When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive. User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank. For details about what characters the password can contain, see p.8 “Characters that can be used in passwords” in this booklet.

Topic	Additional Description
Configuring Administrator Authentication >Enabling Administrator Authentication >Logging on Using Administrator Authentication	【Error】 **Note** ❒ If you log on using a login user name with the authority of more than one administrator, "Administrator" appears. 【Corrections】 **Note** ❒ If the user name entered at login has multiple administrator privileges, any administrator name with administrator privileges will be displayed.
Configuring Administrator Authentication >Enabling Administrator Authentication >Logging on Using Administrator Authentication Step 5	Add the following: When the administrator is making settings for the first time, a password is not required; the administrator can simply press **[OK]** to proceed.
Configuring Administrator Authentication >Enabling Administrator Authentication >Changing the Administrator	Add the following: **Note** ❒ An administrator's privileges can be changed only by an administrator who has the privileges of the administrator concerned. ❒ Administrator privileges cannot be revoked by any single administrator.
Configuring User Authentication >Basic Authentication >Specifying Basic Authentication >Specifying Login User Names and Passwords	Add the following: **Note** ❒ The administrator must inform general users concerning the number of characters that passwords can contain. ❒ Do not use Japanese, Traditional Chinese, Simplified Chinese, or Hangul double-byte characters. If you use multi-byte characters when entering the login user name or password, you cannot authenticate using Web Image Monitor. For details about what characters the password can contain, see p.8 “Characters that can be used in passwords” in this booklet.
Configuring User Authentication >If User Authentication is Specified	【Error】 When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. Unless a valid user name and password are entered, operations are not possible with the machine. 【Corrections】 When user authentication (User Code Authentication, Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server Authentication) is set, the authentication screen is displayed. To use the machine’s security functions, each user must enter a valid user name and password.

Topic	Additional Description
Configuring User Authentication >If User Authentication is Specified >If Basic, Windows, LDAP or Integration Server Authentication is Specified >Logging on Using the Printer Driver	Extra details about specifying the authentication settings required for logging on have been added. For details about specifying the LAN-Fax driver properties, see p.17 “Specifying the LAN-Fax Driver Properties” in this booklet. For details about specifying the printer driver properties, see p.18 “Specifying the Printer Driver Properties” in this booklet.
Configuring User Authentication >If User Authentication is Specified >User Lockout Function >Specifying the User Lockout Function Step 7	【Error】 7 Set the "Lockout Release Timer" to **[Active]**. 【Corrections】 7 After lockout, if you want to cancel lockout after a specified time elapses, set the "Lockout Release Timer" to **[Active]**.
Configuring User Authentication >If User Authentication is Specified >User Lockout Function >Unlocking a Locked User Account	Change of Title 【Error】 Unlocking a Locked User Account 【Corrections】 Canceling Password Lockout
	Add the following: **Note** ❒ The administrator and supervisor password lockout can be canceled by switching the main power off and then back on again.
Protecting Data from Information Leaks >Preventing Unauthorized Copying >Configuring Unauthorized Copy Prevention and Data Security for Copying >Specifying Data Security for Copying from the Printer Driver After Step 6	【Error】 6 Click **[OK]**. 【Corrections】 6 If you want to embed text in the printed copy, enter the text in the **[Text:]** box in the **[Unauthorized copy prevention: Text]** group. Also, specify **[Font:]**, **[Font style:]**, and Size. 7 Click **[OK]**.
Protecting Data from Information Leaks >Printing a Confidential Document >Changing the Password of a Locked Print File Step 8	Delete the following: The password entry screen does not appear if the file administrator is logged in.

Topic	Additional Description
Protecting Data from Information Leaks >Configuring Access Permissions for Stored Files	Add the following: **Note** ❒ The file administrator can also delete stored files. For details, see "Deleting a Stored Document", Copy and Document Server Reference.
Protecting Data from Information Leaks >Configuring Access Permissions for Stored Files >Specifying User and Access Permissions for Stored Files	Add the following: **Important** ❒ The file administrator can change the owner of a document using the document's **[Change Access Priv.]** setting. This setting also allows the file administrator to change the access privileges of the owner and other users. ❒ To change the access privileges of a document's owner or another user with Full Control privileges for a document, use the **[Change Access Priv.]** setting of the document.
	Add the following: ❖ **Changing the Owner of a Document** Explains how to change the owner of a document. This can be specified by the file administrator. 1 Press the **【Document Server】** key. 2 Select the file. 3 Press **[File Management]**. 4 Press **[Change Access Priv.]**. 5 Under "Owner", press **[Change]**. 6 Select the user you want to register. 7 Press **[Exit]**. 8 Press **[OK]** twice.
Protecting Data from Information Leaks >Configuring Access Permissions for Stored Files >Specifying Access Permissions for Files Stored Using the Scanner and Fax Functions	**【Error】** If user authentication is set for the scanner function, you can specify access privileges for stored files when storing them in the Document Server. You can also change the access privileges for the file. **【Corrections】** If user authentication is set for scanner and fax function, you can specify access privileges for stored files when storing them in the Document Server. You can also change the access privileges for the file.
Securing Information Sent over the Network or Stored on Hard Disk >Protecting the Address Book >Configuring Address Book Access Permissions	Add the following: **Note** ❒ An authenticated user's access to Address Book information is determined by the access permissions granted to that user: "Read-only", "Edit", "Edit / Delete", or "Full Control". Note that granting a user "Edit", "Edit / Delete", or "Full Control" permission allows that user to perform high level operations, which could result in loss of or changes to sensitive information. For this reason, we recommend you grant only the "Read-only" access permission to general users.

Topic	Additional Description
Securing Information Sent over the Network or Stored on Hard Disk >Protecting the Address Book >Encrypting Data in the Address Book	Add the following: **Note** ❒ The backup copy of the address book data stored in the SD card is encrypted. For details about backing up and then restoring the address book using an SD card, see "Administrator Tools", Network and System Settings Guide.
Securing Information Sent over the Network or Stored on Hard Disk >Encrypting Data on the Hard Disk >Enabling the Encryption Settings Securing Information Sent over the Network or Stored on Hard Disk >Encrypting Data on the Hard Disk >Updating the Encryption Key	Add the following: **Important** ❒ If the encryption key update was not completed, the printed encryption key will not be valid.
Managing Access to the Machine >Managing Log Files	Extra details and important notes about downloading log files have been added. For details, see p.20 “Managing Log Files” in this booklet. **Note** ❒ For details about managing log files, see also "Managing Log Files" in the Security Reference.
Enhanced Network Security >Encrypting Transmitted Passwords >Specifying a Driver Encryption Key Step 8	Add the following: For details about specifying the encryption key on the LAN-Fax driver, see the LAN-Fax driver Help.
Enhanced Network Security >Protection Using Encryption >User Settings for SSL (Secure Sockets Layer)	【Error】 If you have installed a device certificate using a self-signed certificate and enabled Secure Sockets Layer (SSL), a warning message may appear when you access the machine using Web Image Monitor or IPP. To stop this message appearing, install the certificate using the procedure for your particular browser. If you are the network administrator, tell your users they must install the certificate to stop the warning message appearing. 【Corrections】 We recommend that after installing the self-signed certificate or device certificate from a private certificate authority on the main unit and enabling SSL (communication encryption), you instruct users to install the certificate on their computers. Installation of the certificate is especially necessary for users who want to print via IPP-SSL from Windows Vista. The network administrator must instruct each user to install the certificate.

<table>
<tr><th>Topic</th><th>Additional Description</th></tr>
<tr><td>Enhanced Network Security >Transmission Using IPsec >IPsec Settings

❖ Encryption Key Auto Exchange / Manual Settings - Shared Settings</td><td>
【Error】
<table>
<tr><th>Setting</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>IPsec</td><td>Specify whether to enable or disable IPsec.</td><td>・ Active
・ Inactive</td></tr>
</table>
BZA004S

【Corrections】
<table>
<tr><th>Setting</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>IPsec*1</td><td>Specify whether to enable or disable IPsec.</td><td>・ Active
・ Inactive</td></tr>
</table>
BZA005S

*1 The [IPsec] setting can also be made from the control panel.
</td></tr>
<tr><td>Enhanced Network Security >Transmission Using IPsec >IPsec Settings

❖ Encryption Key Auto Exchange Setting Items</td><td>
【Error】
<table>
<tr><th>Settings</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>Encapsulation Mode</td><td>Specify the encapsulation mode.
(auto setting)</td><td>・Transport
・Tunnel
(Tunnel beginning address -Tunnel ending address)
If you specify "Tunnel", you must then specify the "Tunnel End Points", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".</td></tr>
</table>
BUS013S

【Corrections】
<table>
<tr><th>Settings</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>Encapsulation Mode</td><td>Specify the encapsulation mode.
(auto setting)</td><td>・Transport
・Tunnel
(Tunnel beginning address -Tunnel ending address)
Select the transport mode (this has no bearing on the security level).
If you specify "Tunnel", you must then specify the "Tunnel End Point", which are the beginning and ending IP addresses. Set the same address for the beginning point as you set in "Local Address".</td></tr>
</table>
BZA003S
</td></tr>
</table>

<table>
<tr><th>Topic</th><th>Additional Description</th></tr>
<tr><td>Enhanced Network Security >Transmission Using IPsec >IPsec Settings

❖ Encryption Key Auto Exchange Setting Items</td><td>
【Error】
<table>
<tr><th>Settings</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>Authentication Method</td><td>Specify the method for authenticating transmission partners. (auto setting)</td><td>・PSK
・Certificate
If you specify PSK, you must then set the PSK text (using ASCII characters).
If you specify Certificate, the certificate for IPsec must be installed and specified before it can be used.</td></tr>
</table>
BUS011S

【Corrections】
<table>
<tr><th>Settings</th><th>Description</th><th>Setting Value</th></tr>
<tr><td>Authentication Method</td><td>Specify the method for authenticating transmission partners. (auto setting)</td><td>・PSK
・Certificate
If you specify PSK, you must then set the PSK text (using ASCII characters).
If you are using "PSK", specify a PSK password using up to 32 ASCII characters.
If you specify Certificate, the certificate for IPsec must be installed and specified before it can be used.</td></tr>
</table>
BUS012S
</td></tr>
<tr><td>Specifying the Extended Security Functions >Specifying the Extended Security Functions >Extended Security Settings

❖ Password Policy</td><td>
Add the following:
Characters that can be used in passwords
Passwords can contain the following characters:
• Upper case letters: A to Z (26 characters)
• Lower case letters: a to z (26 characters)
• Numbers: 0 to 9 (10 characters)
• Symbols: (space) ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } (33 characters)

Note
❒ Some characters are not available, regardless of whether their codes are entered using the keyboard or the control panel.
</td></tr>
<tr><td>Specifying the Extended Security Functions >Other Security Functions >Fax Function</td><td>
Add the following:

❖ Specifying Automatic Deletion of Incoming Faxes when an Error Occurs
In [Facsimile Features], you can configure the machine to automatically delete incoming faxes by setting "Switch 10, Bit 7" in [Parameter Setting] under [Initial Settings]. If you make this setting, the machine will delete every incoming fax when an error occurs, even if you have configured the machine to only store incoming faxes. Errors can be caused by corruption of the hard disk, memory overload, or lack of storage for incoming faxes. Each deletion is recorded and will appear on the incoming fax deletion report. By preventing incoming faxes printing out unexpectedly, this function makes fax reception more secure. For details about Parameter Setting, see "Facsimile Features", Facsimile Reference.
</td></tr>
</table>

Topic	Additional Description
Specifying the Extended Security Functions >Limiting Machine Operations to Customers Only >Settings >Canceling Service Mode Lock	【Error】 To enable a service representative to inspect or repair this machine, the machine administrator must log on and cancel the service mode lock beforehand. 【Corrections】 Before the customer engineer can carry out an inspection or repair in service mode, the machine administrator must first log on to the machine, release the service mode lock, and then call the customer engineer. After the inspection or repair is completed, the service mode lock must be reapplied.
Specifying the Extended Security Functions >Additional Information for Enhanced Security	Some details in this section have been changed. Replace this section with p.38 “Additional Information for Enhanced Security” in this booklet.
Appendix >Supervisor Operations	【Error】 **Important** ❒ When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive. 【Corrections】 **Important** ❒ When registering login user names and login passwords, you can specify up to 32 alphanumeric characters and symbols. Keep in mind that user names and passwords are case-sensitive. User names cannot contain numbers only, a space, colon (:), or quotation mark ("), nor can they be left blank. For details about what characters the password can contain, see p.8 “Characters that can be used in passwords” in this booklet.
Appendix >Supervisor Operations >Logging on as the Supervisor Step 5	Add the following: When the supervisor is making settings for the first time, a password is not required; the supervisor can simply press **[OK]** to proceed.
Appendix >Supervisor Operations >Resetting an Administrator's Password	【Error】 This section describes how to reset the administrators' passwords. 【Corrections】 This section describes how to reset the administrators' passwords. Administrator login names cannot be changed.
Appendix >Machine Administrator Settings	Some details in this section have been changed. Replace this section with p.46 “Machine Administrator Settings” in this booklet.
Appendix >Network Administrator Settings	Some details in this section have been changed. Replace this section with p.58 “Network Administrator Settings” in this booklet.

Topic	Additional Description
Appendix >File Administrator Settings	Some details in this section have been changed. Replace this section with p.63 “File Administrator Settings” in this booklet.
Appendix >User Administrator Settings	Some details in this section have been changed. Replace this section with p.65 “User Administrator Settings” in this booklet.
Appendix >The Privilege for User Account Settings in the Address Book	Some details in this section have been changed. Replace this section with p.43 “The Privilege for User Account Settings in the Address Book” in this booklet.

Copy and Document Server Reference Errata

This chapter corrects errors in the supplied Copy and Document Server Reference. Please refer to it when reading the Copy and Document Server Reference.

Topic	Additional Description
Document Server >Using the Document Server>Downloading Stored Documents with Web Image Monitor	【Error】 **Important** ❒ When downloading a document stored with the copy feature, the optional file format converter is required. **Note** ❒ You cannot select **[Multi-page: TIFF]** for a document being stored with the copy or printer. ❒ When downloading a document with **[Multi-page: TIFF]**, you must prepare the file format converter. 【Corrections】 **Important** ❒ File Format Converter is required if you want to download documents saved under the copy or printer function. **Note** ❒ Files stored using the scanner function cannot be downloaded as multi-page TIFF files in the following cases: • If the originals were scanned in full color or gray scale with **[Compression (Gray Scale / Full Colour)]** in **[Scanner Features]** set to **[On]**. • If the originals contained full-color images and were scanned with **[Compression (Gray Scale / Full Colour)]** set to **[On]** and **[Scan Settings]** set to **[Auto Colour Select]** in **[Scanner Features]**. ❒ **[JPEG]** can only be selected for files stored using the scanner function. However, JPEG files cannot be downloaded in the following cases: • If the originals were scanned in black and white. • If the originals were scanned with **[Compression (Gray Scale / Full Colour)]** in **[Scanner Features]** set to **[Off]**.
Document Server >Using the Document Server>Downloading Stored Documents with Web Image Monitor After Step 5	【Error】 5 Select **[PDF]**, **[Multi-page: TIFF]**, or **[JPEG]** for the file format. The data will be downloaded. 6 Click **[OK]**. 【Corrections】 5 Select **[PDF]**, **[Multi-page: TIFF]**, or **[JPEG]** for the file format, and then click **[Download]**. The data will be downloaded. 6 Click **[OK]**.

Network and System Settings Guide Errata

This chapter corrects errors in the supplied Network and System Settings Guide. Please refer to it when reading the Network and System Settings Guide.

Topic	Additional Description
System Settings >Administrator Tools ❖ **Back Up / Restore Address Book**	Add the following: Backup requires a removable SD card to be installed in this machine. For details about installing and removing the SD card, contact your sales or service representative.

Facsimile Reference Errata

This chapter corrects errors in the supplied Facsimile Reference.
Please refer to it when reading the Facsimile Reference.

Topic	Additional Description
Fax via Computer >Sending Fax Documents from Computers >Installing Individual Applications	Add the following: ❖ **Using the TCP/IP Port** Use SmartDeviceMonitor for Client in DeskTopBinder to specify the TCP/IP port. 1 Click **[TCP/IP]**. 2 Click **[Search]**. A list of printers using TCP/IP appears. 3 Select the machine you want to use. Only machines that respond to a broadcast from the computer appear. To use a machine not listed here, click **[Specify Address]**, and then enter the IP address or host name of the machine. 4 Click **[OK]**. ❖ **Using the IPP Port** Use SmartDeviceMonitor for Client in DeskTopBinder to specify the IPP port. 1 Click **[IPP]**. 2 In the **[Printer URL]** box, enter "http://machine's IP address/printer" as the machine's address. 3 Enter a name for identifying the machine in **[IPP Port Name]**. Use a name different from the one of any existing ports. If a name is not specified here, the address entered in the **[Printer URL]** box becomes the IPP port name. 4 Click **[Detailed Settings]** to make necessary settings. For details about the settings, see SmartDeviceMonitor for Client Help. 5 Click **[OK]**. **Note** ❒ For details about each setting, see the Help on the CD-ROM.

Scanner Reference Errata

This chapter corrects errors in the supplied Scanner Reference.
Please refer to it when reading the Scanner Reference.

Topic	Additional Description
Sending Scan Files by E-mail >Simultaneous Storage and Sending by E-mail	【Error】 **Note** ❒ If a file is sent and stored simultaneously with **[Security]** set, the e-mail will be encrypted and the signature applied, but the stored file will not be changed. 【Corrections】 **Note** ❒ If a file is sent and stored simultaneously with **[Security]** set, the e-mail will be encrypted and the signature applied, but the stored file will not be changed. Encryption of stored files is possible only when the optional HDD Encryption unit is installed. For details about encrypting stored files, see "Encrypting Data on the Hard Disk", Security Reference.
Sending Scan Files by E-mail >Security Settings to E-mails >Sending Encrypted E-mail	【Error】 **Note** ❒ If you selected **[Store to HDD + Send]**, the e-mail will be encrypted, but the stored file will not be encrypted. 【Corrections】 **Note** ❒ If you select **[Store to HDD + Send]**, only the sent e-mail will be encrypted and the stored file will not. However, encryption of stored files is possible only when the optional HDD Encryption unit is installed. For details about encryption of stored files, see "Encrypting Data on the Hard Disk", Security Reference.
Sending Scan Files to Folders >Before Sending Files by Scan to Folder >Preparation for Sending by Scan to Folder	Add the following: **Note** ❒ Scan to Folder is not supported in IPv6 environments.

Setting Up the Machine

Use this section in place of "Setting Up the Machine" in the Security Reference.

This section explains how to enable encryption of transmitted data and configure the administrator account. If you want a high level of security, make the following setting before using the machine.

❖ Enabling security

① Turn the machine on.

② Press the **【User Tools】** key.

③ Press **[System Settings]**.

④ Press **[Interface Settings]**.

⑤ Specify IPv4 Address.
For details on how to specify the IPv4 address, see "Interface Settings", Network and System Settings Guide.

⑥ Be sure to connect this machine to a network that only administrators can access.

⑦ Start Web Image Monitor, and then log on to the machine as the administrator.
For details about logging on to Web Image Monitor as an administrator, see "Using Web Image Monitor to Configure Administrator Authentication".

⑧ Click **[Configuration]**, and then click **[E-mail]** under "Device Settings".
The "E-mail" page appears.

⑨ Enter the machine administrator's e-mail address in **[Administrator E-mail Address]**, and then, click **[OK]**.

⑩ Install the device certificate.
For information on how to install the device certificate, see "Protection Using Encryption".

⑪ Enable secure sockets layer (SSL).
For details about enabling SSL, see "Enabling SSL".

⑫ Change the administrator's user name and password.
To enable higher security, proceed to step 2 in the following "Enabling enhanced security".

⑬ Log off, and then quit Web Image Monitor.

⑭ Disconnect the machine from the administrators-only network, and then connect it to the general use network.

❖ Enabling enhanced security

① Configure the security settings for the machine by following steps 1 to 12 in the previous section, "Enabling security".

② Click **[Configuration]**, and then click **[Network Security]** under "Security".
The "Network Security" page appears.

③ To use only the ports that have high security, set "Network Security" to **[Level 2]**.
If "Network Security" is set to **[Level 2]**, some functions will be unavailable. For details, see "Status of Functions under each Network Security Level" and "Enabling and Disabling Protocols".

④ Set both "FTP" with high security risk and "SNMPv3 Function" to **[Inactive]**, and then click **[OK]** twice.
For details about the functions that will be unavailable if "FTP" and "SNMPv3" are set to **[Inactive]**, see "Enabling and Disabling Protocols".

⑤ Log off, and then quit Web Image Monitor.

⑥ Press the **【User Tools】** key on the control panel.

⑦ Press **[System Settings]**.

⑧ Press **[Administrator Tools]**.

⑨ Press **[Extended Security]**.
If the setting to be specified does not appear, press **[▼Next]** to scroll down to other settings.

⑩ Set **[@Remote Service]** to **[Prohibit]**.
For details about "Update Firmware", see the following "Firmware Update Cautions".

⑪ Press **[OK]**.

⑫ Press **[Exit]**.

⑬ Press the **【User Tools】** key.

⑭ Disconnect the machine from the administrators-only network, and then connect it to the general use network.

❖ Firmware Update Cautions

If "IPsec" is enabled, all information on the network will be encrypted. This allows you to perform firmware updates securely.
If "IPsec" is not enabled, the information on the network may not be encrypted depending on the protocol. If you want to perform a firmware update when "IPsec" is not enabled, be sure to do so only if your network environment is protected against electronic eavesdropping and similar security threats.

Reference

"Using Web Image Monitor to Configure Administrator Authentication", Security Reference

"Protection Using Encryption", Security Reference

"Enabling SSL", Security Reference

"Status of Functions under each Network Security Level", Security Reference

"Enabling and Disabling Protocols", Security Reference

Specifying the LAN-Fax Driver Properties

Add the following information and procedure to Security Reference >Configuring User Authentication >If User Authentication is Specified >If Basic, Windows, LDAP or Integration Server Authentication is Specified >Logging on Using the Printer Driver.

If the user authentication settings are made on the machine, make sure the user authentication settings are made on the LAN-Fax driver also.

With user authentication, only users registered in the machine or server can send and/or print faxes using the machine. Make sure the user's login user name and login password settings are entered on the LAN-Fax driver to enable that user to send and/or print. Users not registered on the machine cannot use the machine for sending and/or printing.

1. **Open the LAN-Fax driver properties dialog box, and then click the [Advanced Options] tab.**
2. **Select the [General user authentication] check box.**
3. **If you want to encrypt the login password, select the [Encryption] check box.**
   If you do not want to encrypt the login password, skip to Step 5.
4. **Enter the driver encryption key already set on the machine.**
5. **Click [OK] to close the LAN-Fax driver properties dialog box.**
6. **Open the document you want to send from an application.**
7. **Select [LAN-Fax] as the printer and then start the print job.**
   The **[LAN-Fax]** dialog box appears.
8. **Click [User Settings].**
   [User Settings] dialog box appears.
9. **Enter the login user name and login password already set on the machine or server for user authentication.**
   Be sure to enter the same login user name and login password that is registered on the machine or the server.
   If you enter an invalid login user name and login password, sending and/or printing does not start.
10. **Click [OK] to close the dialog box.**

Note

- **[User code:]** and **[Specify sender]** settings on the **[User Settings]** dialog box are invalid when you use the user authentication function.

Specifying the Printer Driver Properties

Add the following information and procedure to Security Reference >Configuring User Authentication >If User Authentication is Specified >If Basic, Windows, LDAP or Integration Server Authentication is Specified >Logging on Using the Printer Driver.

If the user authentication settings have been made on the machine, you also need to make the user authentication settings on the printer driver.

With user authentication, only users who are registered on the machine or the server can print using the machine. You need to make the login user name and login password settings for a user to enable that user to print. Users who are not registered on the machine printer or the server cannot use the machine for printing.

The following procedure explains how to configure the printer driver under Windows XP.

1. **Open the printer properties dialog box, and then click the [Advanced Options] tab.**
2. **Select the [Confirm authentication information when printing] check box.**
3. **If you want to encrypt the login password, select the [Encrypt] check box.**
   If you do not want to encrypt the login password, skip to Step 7.
4. **Enter the driver encryption key already set on the machine.**
5. **Click [OK].**
   [Confirm Driver Encryption Key] dialog box appears.
6. **Reenter the encryption key.**
7. **Click [OK] to close the printer properties dialog box.**
8. **From the [Printers and Faxes] window, open the printing preferences dialog box.**
9. **If the dialog box type is "Custom Setting", click [Printer Configuration] on the [Print Settings] tab.**
   If the dialog box type is "Multi-tab", click the **[Printer Configuration]** tab.
10. **Click [User Authentication].**
11. **Enter a login user name and login password already set on the machine or the server for user authentication.**
    Be sure to enter the same login user name and login password that is registered on the machine or the server.
    If you do not enter a valid login user name and login password, printing will not start.
12. **Click [OK].**
    [Confirm Login Password] dialog box appears.

⓭ Reenter the login password.

⓮ Click [OK].

⓯ If the dialog box type is "Custom Setting", click [OK] to close the [Printer Configuration] dialog box.

⓰ Click [OK] to close the printing preferences dialog box.

Note

❒ When you use the user authentication function, user code setting becomes invalid.

❒ Depending on the applications, the settings you make here may not be used as the default settings.

Reference

For details about the printer properties dialog box type, see "Two Dialog Box Types", Printer Reference.

Managing Log Files

Add the following information to the section "Managing Log Files" in the Security Reference.

The logs created by this machine allow you to track access to the machine, identities of users, and usage of the machine's various functions. For security, you can encrypt the logs.

The logs can be viewed using Web Image Monitor. Collected logs can be downloaded all at once from Web Image Monitor as CSV files. You cannot download the log files directly from the hard disk.

Also, login information is cross-checked even when Web SmartDeviceMonitor is in use. For details, see the operating instructions supplied with Web SmartDeviceMonitor.

❖ Log Types

This machine creates two types of log: the job log and the access log.

- Job Log
  Stores details of user file-related operations such as saving files in the document server, copying, printing, sending faxes and scanning; and control panel operations such as printing reports (the configuration list, for instance).
- Access Log
  Stores details about the following: login/logout activity; stored file operations such as creating, editing, and deleting; administrator operations such as specifying log collection level, deletions of all logs, and specifying log encryption; customer engineer operations such as hard disk formatting; system operations such as viewing the results of log transfers and specifying copy protection settings; and security operations such as specifying encryption settings, detection of unauthorized access attempts, user lockouts, and firmware authentication.

Note

❒ The log setting can be specified in **[Logs]** under **[Configuration]** in Web Image Monitor.

Download Logs

The logs collected on this machine are in CSV format, so can be batch-downloaded.

1 Open a Web browser.

2 In the Web browser's address bar, enter "http://(the machine's IP address or host name)/ " to access the machine.

When entering an IPv4 address, do not begin segments with zeros. For example: if the address is "192.168.001.010", you must enter it as "192.168.1.10" to connect to the machine. If you enter it as "192.168.001.010", you cannot access the machine.

The top page of Web Image Monitor appears.

3 Click [Login].

The machine administrator can log on.

Log in using an administrator's user name and password.

4 Click [Configuration], and then click [Download Logs] under "Device Settings".

The "Download Logs" page appears.

5 Click [Download].

6 Specify the folder in which you want to save the file.

7 Click [Back].

8 Click [Logout].

Note

- ❒ Only the jobs that were completed before **[Download]** was clicked are recorded in the log. The "Result" field of the log entry for uncompleted jobs will be blank.
- ❒ Download time may vary depending on the number of logs.
- ❒ If an error occurs while the CSV file is downloading or being created, the download is canceled and details of the error are included at the end of the file.
- ❒ If a log is downloaded successfully, "Log data download is completed!!" will appear in the last line of the log file.
- ❒ For details about saving CSV log files, see your browser's Help.
- ❒ Downloaded log files use UTF-8 character encoding. To view a log file, open it using an application that supports UTF-8.
- ❒ To collect logs, set "Collect Job Logs" and "Collect Access Logs" to "Active". This setting can be specified in **[Logs]** under **[Configuration]** in Web Image Monitor.
- ❒ For details about the items in the logs, see p.30 "Attributes of Logs you can Download" in this booklet.

Note Concerning Downloading Logs

When the number of stored logs reaches the maximum, the oldest logs will be overwritten by newer logs. This applies to both job and access logs and occurs regardless of whether or not the logs have been downloaded.

Overwritten old logs will not be included in downloaded log files.

For this reason, we recommend you take note of the information in the table below and perform regular log management using Web Image Monitor.

❖ Maximum number of logs that can be stored in the machine

Job Logs	Access Logs
2,000	6,000

❖ Estimated number of logs created per day

Job Logs	Access Logs
100 (100 logs per day)	300 This figure is based on 100 operations such as initialization and access operations over the Web and 200 access log entries (two entries per job: one login and one logout).

If the daily estimates are not exceeded, the machine can store logs for 20 days without having to overwrite older logs. However, we recommend that you download the logs every 10 days. This will prevent unwanted overwriting and ensure all logs are preserved, even if the daily estimate is exceeded.

It is the responsibility of the machine administrator to deal downloaded log files appropriately.

Note

❒ If you change the **[Collect]** / **[Do not Collect]** setting for log collection, you must perform a batch deletion of the logs.

❒ After downloading the logs, perform a batch deletion of the logs.

❒ Logs processed during log downloads might not be recorded, so do not perform operations on logs during log downloads.

❒ Batch deletion of logs can be performed from the control panel or through Web Image Monitor.

Notes on Operation when the Number of Log Entries Reaches Maximum

The machine reads the number of access and job logs and begins overwriting the oldest log entries to make space for the new logs as they arrive.

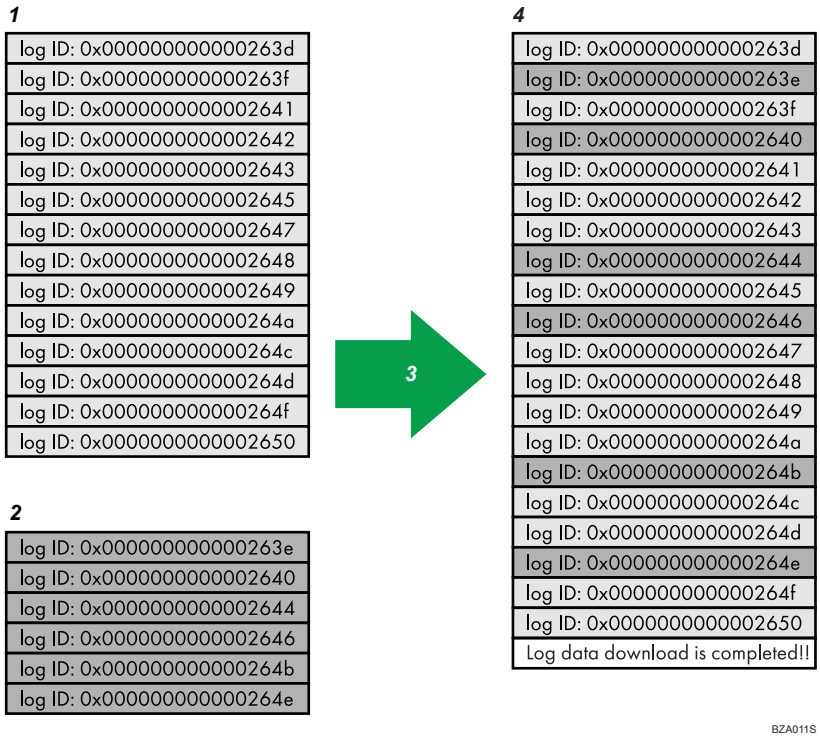
Downloaded log files include both access and job logs, with some log entries incomplete.

The following illustration shows an example in which logs are downloaded during access log overwriting.

In this example, some of the access log entries are incomplete.

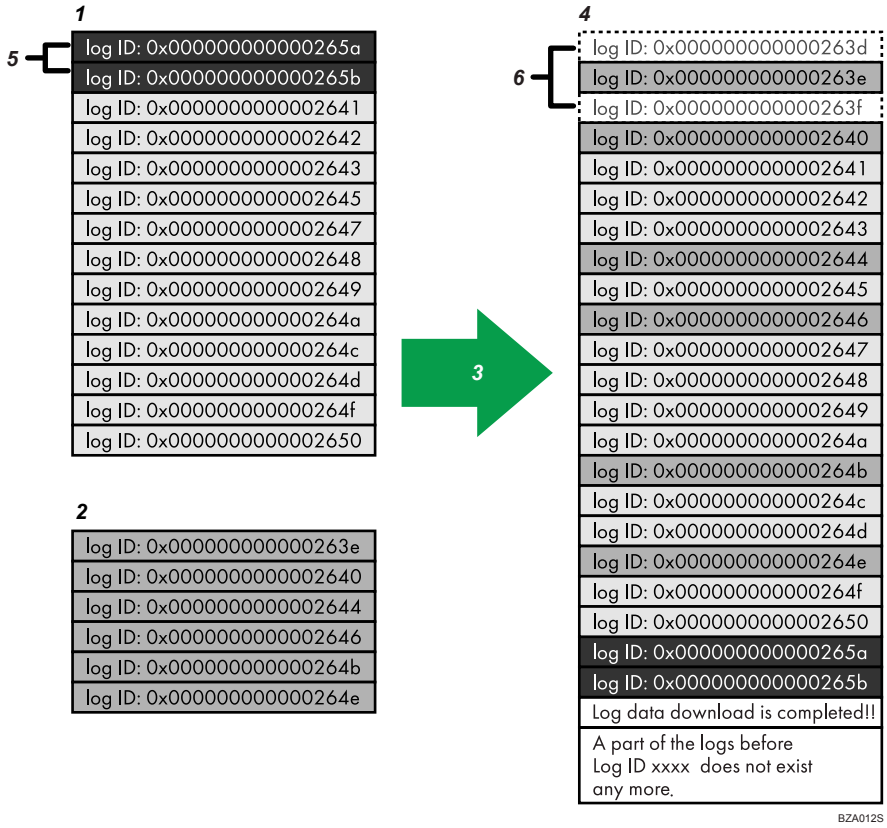
Logs are overwritten in reverse priority order, meaning logs of lowest priority are overwritten first and logs of highest priority are overwritten last. This way, if the overwrite is canceled, there is a chance that logs of higher priority will still be available.

❖ If logs are downloaded without overwriting



1. **Access Log**
2. **Job Log**
3. **Download**
4. **Downloaded Logs**

❖ If logs are downloaded during overwriting



1. **Access Log**
2. **Job Log**
3. **Download**
4. **Downloaded Logs**
5. **Overwriting**
6. **Deleted by Overwriting**

To determine whether or not overwriting occurred while the logs were downloading, check the message in the last line of the downloaded logs.

- If overwriting did not occur, the last line will contain the following message:
  Log data download is completed!!
- If overwriting did occur, the last line will contain the following message:
  Log data download is completed!!
  A part of the logs before Log ID xxxx does not exist any more.

Note

❒ Examine logs following "Log ID xxxx".

Detailed Explanation of Print Job-Related Log Entries

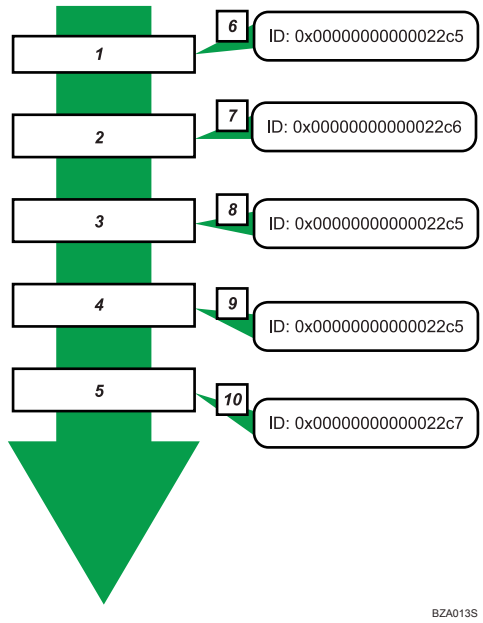
Print Log entries are made before the login entry is made in the Access Log.

Details of series of jobs (including reception, processing, and output of the jobs' data) are combined into single entries.

When the machine receives a print job, it creates an ID for the job and records this in the job log. The machine then creates a login ID for the print job and records this in the access log. It then creates a job log entry detailing the job's processing and outputting (under the same login ID). When the machine has finished processing the job, it creates a logout entry and places this in the access log.

Entries detailing the reception, processing, and output of a series of print jobs are created in the job log first, and then the login and logout details of those jobs are recorded in the access log.

❖ Print Job Flowchart



1. **Print job data is received.**

2. **Authentication (login) data is received.**

3. **Print job is processed.**

4. **Print job is output.**

5. **Authentication (login) data is received.**

6. **An ID is assigned to the print job and recorded as an entry in the Job Log.**

7. **Authentication (login) data is recorded as an entry in the Access Log.**

8. **Information about the processing of the print job is recorded as an entry in the Job Log (using the same ID).**

9. **Information about the outputting of the print job is recorded as an entry in the Job Log (using the same ID).**

10. **Authentication (logout) data is recorded as an entry in the Access Log.**

Logs that can be Collected

The following tables explain the items in the job log and access log that the machine creates when you enable log collection using Web Image Monitor. If you require log collection, use Web Image Monitor to configure it. This setting can be specified in **[Logs]** under **[Configuration]** in Web Image Monitor.

❖ Job Log Information Items

Job Log Item	Log Type Attribute	Content
Copier: Copying	Copier: Copying	Details of normal and Sample Copy jobs.
Copier: Copying and Storing	Copier: Copying and Storing	Details of files stored in Document Server that were also copied at the time of storage.
Document Server: Storing	Document Server: Storing	Details of files stored using the Document Server screen.
Document Server: Stored File Downloading	Document Server: Stored File Downloading	Details of files stored in Document Server and downloaded using Web Image Monitor or DeskTopBinder.
Utility: Storing	Utility: Storing	Details of files stored in Document Server using Desk Top Editor For Production.
Stored File Printing	Stored File Printing	Details of files printed using the Document Server screen.
Scanner: Sending	Scanner: Sending	Details of sent scan files.
Scanner: URL Link Sending and Storing	Scanner: URL Link Sending and Storing	Details of scan files stored in Document Server and whose URLs were sent by e-mail at the time of storage.
Scanner: Sending and Storing	Scanner: Sending and Storing	Details of scan files stored in Document Server that were also sent at the time of storage.
Scanner: Storing	Scanner: Storing	Details of scan files stored in Document Server.
Scanner: Stored File Downloading	Scanner: Stored File Downloading	Details of scan files stored in Document Server and downloaded using Web Image Monitor, DeskTopBinder or Desk Top Editor For Production.
Scanner: Stored File Sending	Scanner: Stored File Sending	Details of stored scan files that were also sent.
Scanner: Stored File URL Link Sending	Scanner: Stored File URL Link Sending	Details of stored scan files whose URLs were sent by e-mail.
Printer: Printing	Printer: Printing	Details of normal print jobs.
Printer: Locked Print (Incomplete)	Printer: Locked Print (Incomplete)	Log showing Locked Print documents temporarily stored on the machine.

Job Log Item	Log Type Attribute	Content
Printer: Locked Print	Printer: Locked Print	Log showing Locked Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Sample Print (Incomplete)	Printer: Sample Print (Incomplete)	Log showing Sample Print documents temporarily stored on the machine.
Printer: Sample Print	Printer: Sample Print	Log showing Sample Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Hold Print (Incomplete)	Printer: Hold Print (Incomplete)	Log showing Hold Print documents temporarily stored on the machine.
Printer: Hold Print	Printer: Hold Print	Log showing Hold Print documents temporarily stored on the machine and then printed from the control panel or through Web Image Monitor.
Printer: Stored Print	Printer: Stored Print	Details of Stored Print files stored on the machine.
Printer: Store and Normal Print	Printer: Store and Normal Print	Details of Stored Print files that were printed at the time of storage (when "Job type:" in printer properties was set to "Store and Normal Print").
Printer: Stored File Printing	Printer: Stored File Printing	Details of Stored Print files printed from the control panel or Web Image Monitor.
Printer: Document Server Sending	Printer: Document Server Sending	Details of files stored in Document Server (when "Job type:" in printer properties was set to "Send to Document Server").
Report Printing	Report Printing	Details of reports printed from the control panel.
Result Report Printing/E-mailing	Result Report Printing/E-mailing	Details of job results printed from the control panel or notified by e-mail.
Scanner: TWAIN Driver Scanning	Scanner: TWAIN Driver Scanning	Details of stored scan files that were sent using Network TWAIN Scanner.
Fax: Sending	Fax: Sending	Details of sent fax files.
Fax: LAN-Fax Sending	Fax: LAN-Fax Sending	Details of a fax sent from the computer.
Fax: Storing	Fax: Storing	Details of stored fax files.

Job Log Item	Log Type Attribute	Content
Fax: Stored File Printing	Fax: Stored File Printing	Details of fax files stored on the machine and printed using the facsimile function.
Fax: Stored File Downloading	Fax: Stored File Downloading	Details of the Document Server's stored files downloaded via Web Image Monitor or DeskTopBinder.
Fax: Receiving	Fax: Receiving	Details of storage of received fax files.
Fax: Receiving and Delivering	Fax: Receiving and Delivering	Details of fax files stored on the machine and printed using the facsimile function. Details of faxes that received and delivered by the machine.
Fax: Receiving and Storing	Fax: Receiving and Storing	Details of fax files that received and stored by the machine.

❖ Access Log Information Items

Access Log Item	Log Type Attribute	Content
Login *1	Login	Times of login and identity of logged in users.
Logout	Logout	Times of logout and identity of logged out users.
File Storing	File Storing	Details of files stored in Document Server.
Stored File Deletion	Stored File Deletion	Details of files deleted from Document server.
All Stored Files Deletion	All Stored Files Deletion	Details of deletions of all Document Server files.
HDD Format *2	HDD Format	Details of hard disk formatting.
Unauthorized Copying	Unauthorized Copying	Details of documents scanned with "Data Security for Copying".
All Logs Deletion	All Logs Deletion	Details of deletions of all logs.
Log Setting Change	Log Setting Change	Details of changes made to log settings.
Transfer Log Error	Transfer Log Error	Details of an error during log transfer to Web SmartDeviceMonitor.
Log Collection Item Change	Log Collection Item Change	Details of changes made to log settings.
Collect Encrypted Communication Logs	Collect Encrypted Communication Logs	Details of changes to job log collection levels, access log collection levels, and types of log collected.
Access Violation *3	Access Violation	Details of failed access attempts.
Lockout	Lockout	Details of lockout activation.
Firmware: Update	Firmware: Update	Details of firmware updates.

Access Log Item	Log Type Attribute	Content
Firmware: Structure Change	Firmware: Structure Change	Details of structure changes that occurred when an SD card was inserted or removed, or when an unsupported SD card was inserted.
Firmware: Structure	Firmware: Structure	Details of checks for changes to firmware module structure made at times such as when the machine was switched on.
Machine Data Encryption Key Change	Machine Data Encryption Key Change	Details of changes made to encryption keys using the Machine Data Encryption setting.
Firmware: Invalid	Firmware: Invalid	Details of checks for firmware validity made at times such as when the machine was switched on.
Date/Time Change	Date/Time Change	Details of changes made to date and time settings.
File Access Privilege Change	File Access Privilege Change	Log for changing the access privilege to the stored files.
Password Change	Password Change	Details of changes made to the login password.
Administrator Change	Administrator Change	Details of changes of administrator.
Address Book Change	Address Book Change	Details of changes made to address book entries.
Capture Error	Capture Error	Details of file capture errors.

*1 There is no "Login" log made for SNMPv3.
*2 If the hard disk is formatted, all the log entries up to the format are deleted and a log entry indicating the completion of the format is made.
*3 An "Access Violation" indicates the system has experienced frequent remote DoS attacks involving logon attempts through user authentication.

Note

❒ If "Job Log Collect Level" is set to "Level 1", all job logs are collected.

❒ If "Access Log Collect Level" is set to "Level 1", the following information items are recorded in the access log:

- HDD Format
- All Logs Deletion
- Log Setting Change
- Log Collection Item Change

❒ If "Access Log Collect Level" is set to "Level 2", all access logs are collected.

❒ The first log made following power on is the "Firmware: Structure" log.

Attributes of Logs you can Download

If you use Web Image Monitor to download logs, a CSV file containing the information items shown in the following table is produced.

Note that a blank field indicates an item is not featured in a log.

❖ File Output Format

- Character Code Set: UTF-8
- Output Format: CSV (Comma-Separated Values)
- File Name: "Device Name + _log.csv"

❖ Order of Log Entries

Log entries are printed in ascending order according to Log ID.

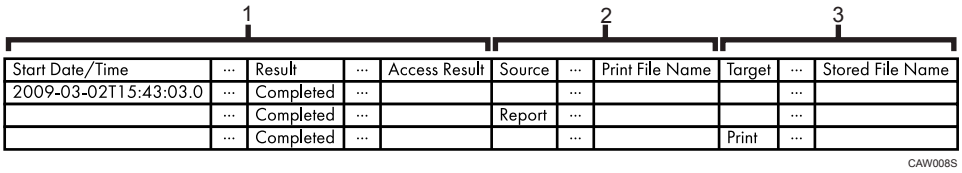
❖ File Structure

The data title is printed in the first line (header line) of the file.

❖ The Difference between the Output Format of Access Log and Job Log

The output format of the access log and job log are different.

- Access log
  Items in the list and access log entries appear on separate lines.
- Job log
  Multiple lines appear in the order of All, Source (job input data), and Target (job output data). The same log ID is assigned to all lines corresponding to a single job log entry.



1 All	Each item in the list is displayed on a separate line.
2 Source	Displays the "Result" and "Status" of Job and Access Log items in the list. Also displays information about the job log input. If there are multiple sources, multiple lines are displayed.
3 Target	Displays the "Result" and "Status" of Job and Access Log items in the list. Also displays information about the job log output. If there are multiple targets, multiple lines are displayed.

❖ Job and Access Log Information Items

Item	Content
Start Date/Time	For a job log entry, indicates the start date and time of the operation. If the job has not been completed, this is blank. For an access log entry, indicates the same date and time as shown by "End Date/Time". This is in Item 1 of the CSV file.
End Date/Time	For a job log entry, indicates the end date and time of the operation. If the operation is still in progress, this will be blank. For an access log entry, indicates the same date and time as shown by "Result". This is Item 2 of the CSV file.
Log Type	Details of the log type. Access logs are classified under "Access Log Type". For details about the information items contained in each type of log, see "Logs that can be Collected". This is Item 3 of the CSV file.
Result [*1]	Indicates the result of an operation or event: • If "Succeeded" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful. If the operation is still in progress, this will be blank. • If "Succeeded" is displayed for an access log entry, the event completed successfully; "Failed" indicates the event was unsuccessful.
Status	Indicates the status of an operation or event: • If "Completed" is displayed for a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress. • If "Completed" is displayed for "Source" or "Target" in a job log entry, the operation completed successfully; "Failed" indicates the operation was unsuccessful; "Processing" indicates the operation is still in progress; "Error" indicates an error occurred; "Suspended" indicates the operation is currently suspended. • If "Succeeded" is displayed for an access log entry, the operation completed successfully; if any of the following are displayed, the operation was unsuccessful: "Password Mismatch", "User Not Programmed", "Other Failures", "User Locked Out", "File Password Mismatch", "No Privileges", "Failed to Access File", "File Limit Exceeded", "Transfer Canceled", "Power Failure", "Lost File", "Functional Problem", "Communication Failure", or "Communication Result Unknown".

Item	Content
User Entry ID	Indicates the user's entry ID. This is a hexadecimal ID that identifies users who performed job or access log-related operations: For supervisors, only "0xffffff86" is available; for administrators, "0xffffff87", "0xffffff88", "0xffffff89", and "0xffffff8a" are available. For general users, any value between "0x00000001" and "0xfffffeff" is available. "0x00000000", "0xffffff80", and "0xffffff81" indicate system operations related to user authentication. IDs "0xffffff80" and "0xffffff81" indicate system operations related to stored files and the address book; "0x00000000" indicates other operations. "0xffffff80" indicates operations related to deleting Hold Print, Locked Print, and Stored Print jobs, or to changing their access permissions. Displays Address Book updates when Auto registration of users is enabled through Windows Authentication, LDAP Authentication, or another authentication system. ID "0xffffff81" indicates operations related to creating Hold Print, Locked Print, and Stored Print jobs that can be deleted using system operations. "0x00000000" and "0xffffff81" indicate operations that do not require user authentication (such as copying and scanning) and that were performed by non-authenticated users. ID "0xffffff81" indicates operations related to stored files , the address book and job logs; "0x00000000" indicates other operations.
User Code/User Name	Identifies the user code or user name of the user who performed the operation. If an administrator performed the operation, this ID will contain the login name of that administrator.
Log ID	Identifies the ID that is assigned to the log. This is a hexadecimal ID that identifies the log.

*1 The following log items are recorded only when the logged operations are executed successfully: "Document Server: Stored File Downloading", "Stored File Printing", "Scanner: Storing", "Scanner: Stored File Sending", "Printer: Stored File Printing", and "Fax: Stored File Downloading" (Job logs) and "File Storing" and "Stored File Deletion" (Access logs).

❖ Access Log Information Items

Item	Content
Access Log Type	Indicates the type of access: "Authentication" indicates a user authentication access. "System" indicates a system access. "Stored File" indicates a stored file access. "Network Attack Detection/Encrypted Communication" indicates a network attack or encrypted communication access. "Firmware" indicates a firmware verification access. "Address Book" indicates an address book access.
Logout Mode	Mode of logout. The remark "Manual Logout" indicates manual logout by the user; "Auto Logout" indicates automatic logout following a timeout.
Login Method	Identifies the method of login (authorization): "Control Panel" indicates the login was performed through the control panel; "via Network" indicates the login was performed remotely through a network computer; and "Others" indicates the login was performed through another method.
Login User Type	Indicates the type of login user: "User" indicates the logged in user was a registered general user. "Guest" indicates the logged in user was a guest user. "User Administrator" indicates the logged in user was a registered user administrator. "File Administrator" indicates the logged in user was a registered file administrator. "Machine Administrator" indicates the logged in user was a registered machine administrator. "Network Administrator" indicates the logged in user was a registered network administrator. "Supervisor" indicates the logged in user was a registered supervisor. "Customer Engineer (Service Mode)" indicates the logged in user was a customer engineer. "Others" indicates the logged in user did not belong to any of the above types of user.
Target User Entry ID	Indicates the entry ID of the target user: This is a hexadecimal ID that indicates users to whom the following settings are applied: • Lockout • Password Change
Target User Code/User Name	User code or user name of the user whose data was accessed. If the administrator's data was accessed, the administrator's user name is logged.
Lockout/Release	The mode of operation access. "Lockout" indicates activation of password lockout; "Release" indicates deactivation of password lockout.

Item	Content
Lockout/Release Method	"Manual" is recorded if the machine is unlocked manually. "Auto" is recorded if the machine is unlocked by the lockout release timer.
Stored File ID	Identifies a created or deleted file. This is a hexadecimal ID that indicates created or deleted stored files.
Stored File Name	Name of a created or deleted file.
File Location	Location of all file deletion. "Document Server" indicates deletion of all files on the hard disk. "Fax Memory" indicates deletion of all files in the fax memory.
Collect Job Logs	Indicates the status of the job log collection setting: "Active" indicates job log collection is enabled. "Inactive" indicates job log collection is disabled. "Not Changed" indicates no changes have been made to the job log collection setting.
Collect Access Logs	Indicates the status of the access log collection setting: "Active" indicates access log collection is enabled. "Inactive" indicates access log collection is disabled. "Not Changed" indicates no changes have been made to the access log collection setting.
Transfer Logs	Indicates the status of the log transfer setting: "Active" indicates log transfer is enabled. "Inactive" indicates log transfer is disabled. "Not Changed" indicates no changes have been made to the log transfer setting.
Encrypt Logs	Indicates the status of the log encryption setting: "Active" indicates log encryption is enabled. "Inactive" indicates log encryption is disabled. "Not Changed" indicates no changes have been made to the log encryption setting.
Log Type	Indicates the type of log whose collection level has been changed. "Job Log" indicates the Job Log's collection level has been changed. "Access Log" indicates the Access Log's collection level has been changed. This is Item 24 of the CSV file.
Log Collect Level	Indicates the level of log collection: "Level 1", "Level 2", or "User Settings".
Encryption/Cleartext	Indicates whether communication encryption is enabled or disabled: "Encryption Communication" indicates encryption is enabled; "Cleartext Communication" indicates encryption is disabled.
Machine Port No.	Indicates the machine's port number.

Item	Content
Protocol	Destination protocol. "TCP" indicates the destination's protocol is TCP; "UDP" indicates the destination's protocol is UDP; "Unknown" indicates the destination's protocol could not be identified.
IP Address	Destination IP address.
Port No.	Destination port number. This is in decimal.
MAC Address	Destination MAC (physical) address.
Primary Communication Protocol	Indicates the primary communication protocol.
Secondary Communication Protocol	Indicates the secondary communication protocol.
Encryption Protocol	Indicates the protocol used to encrypt the communication.
Communication Direction	Indicates the direction of communication: "Communication Start Request Receiver (In)" indicates the machine received a request to start communication; "Communication Start Request Sender (Out)" indicates the machine sent a request to start communication.
Communication Start Log ID	Indicates the log ID for the communication start time. This is a hexadecimal ID that indicates the time at which the communication started.
Communication Start/End	Indicates the times at which the communication started and ended.
Network Attack Status	Indicates the attack status of the network: "Violation Detected" indicates an attack on the network was detected. "Recovered from Violation" indicates the network recovered from an attack. "Max. Host Capacity Reached" indicates the machine became inoperable due to the volume of incoming data reaching the maximum host capacity. "Recovered from Max. Host Capacity" indicates that the machine became operable again following reduction of the volume of incoming data.
Network Attack Type	Identifies the type of network attack as either "Password Entry Violation" or "Device Access Violation".
Network Attack Type Details	Indicates details about the type of network attack: "Authentication Error" or "Encryption Error".
Network Attack Route	Identifies the route of the network attack as either "Attack from Control Panel" or "Attack from Other than Control Panel".
Login User Name used for Network Attack	Identifies the login user name that the network attack was performed under.

Item	Content
Add/Update/Delete Firmware	Indicates the method used to add, update, or delete the machine's firmware: "Updated with SD Card" indicates an SD card was used to perform the firmware update. "Added with SD Card" indicates an SD card was used to add the firmware. "Deleted with SD Card" indicates an SD card was used to delete the firmware. "Moved to Another SD Card" indicates the firmware update was moved to another SD card. "Updated via Remote" indicates the firmware update was updated remotely from a computer. "Updated for Other Reasons" indicates the firmware updated was performed using a method other than any of the above.
Module Name	Firmware module name.
Parts Number	Firmware module part number.
Version	Firmware version.
Machine Data Encryption Key Operation	Indicates the type of encryption key operation performed: "Back Up Machine Data Encryption Key" indicates an encryption key backup was performed. "Restore Machine Data Encryption Key" indicates an encryption key was restored. "Clear NVRAM" indicates the NVRAM was cleared. "Start Updating Machine Data Encryption Key" indicates an encryption key update was started. "Finish Updating Machine Data Encryption Key" indicates an encryption key update was finished.
Machine Data Encryption Key Type	Identifies the type of the encryption key as "Encryption Key for Hard Disk", "Encryption Key for NVRAM", or "Device Certificate".
Validity Error File Name	Indicates the name of the file in which a validity error was detected.
Access Result	Indicates the results of logged operations: "Completed" indicates an operation completed successfully; "Failed" indicates an operation completed unsuccessfully.

❖ Job Log Information Items

❖ Input Information

Item	Content
Source	Indicates the source of the job file: "Scan File" indicates the job file was scanned in; "Stored File" indicates the job file was stored on the machine; "Printer" indicates the job file was sent from the printer driver; "Received File" indicates the job file was received over the network; "Report" indicates the job file was a printed report.
Start Date/Time	Dates and times "Scan File", "Received File" and "Printer" operations started. This is Item 52 of the CSV file.
End Date/Time	Dates and times "Scan File", "Received File" and "Printer" operations ended. This is Item 53 of the CSV file.
Stored File Name	Names of "Stored File" files.
Stored File ID	Indicates the ID of data that is output as a stored file. This is a decimal ID that identifies the stored file.
Print File Name	Name of "Printer" files.

❖ Output Information

Item	Content
Target	Type of the job target. "Print" indicates a print file; "Store" indicates a stored file; "Send" indicates a sent file.
Start Date/Time	Dates and times "Print", "Store", and "Send" operations started. This is Item 58 of the CSV file.
End Date/Time	Dates and times "Print", "Store", and "Send" operations ended. This is Item 59 of the CSV file.
Destination Name	Names of "Send" destinations.
Destination Address	IP address, path, e-mail address, or fax number of the "Send" destinations.
Stored File ID *1	Indicates the ID of data that is output as a store file. This is a decimal ID that identifies the stored file.
Stored File Name *2	If the Target type is "Store", the file name of the stored file is recorded.

Printing stored faxes from the Fax screen before transmission will not be recorded in the job log.

*1 Stored File IDs are not logged for documents processed using fax functions.

*2 Stored File Names are not logged for documents processed using fax functions.

Additional Information for Enhanced Security

Use this section in place of "Additional Information Enhanced Security" in the Security Reference.

This section explains the settings that you can configure to enhance the machine's security.

Control panel security settings

If the security settings are not configured, the data in the machine is vulnerable to attack. Use the control panel to configure the security settings as shown in the following table.

Menu	Tab	Item	Setting
System Settings	Timer Settings	Auto Logout Timer	**[On]**: 180 seconds or less
System Settings	Administrator Tools	Administrator Authentication Management/User Management	Select **[On]**, and then select **[Administrator Tools]** for "Available Settings".
System Settings	Administrator Tools	Administrator Authentication Management/Machine Management	Select **[On]**, and then select **[Timer Settings]**, **[Interface Settings]**, **[File Transfer]**, and **[Administrator Tools]** for "Available Settings".
System Settings	Administrator Tools	Administrator Authentication Management/Network Management	Select **[On]**, and then select **[Interface Settings]**, **[File Transfer]**, and **[Administrator Tools]** for "Available Settings".
System Settings	Administrator Tools	Administrator Authentication Management/File Management	Select **[On]**, and then select **[Administrator Tools]** for "Available Settings".
System Settings	Administrator Tools	Extended Security/Settings by SNMPv1, v2	**[Prohibit]**
System Settings	Administrator Tools	Extended Security/Restrict Use of Simple Encryption	**[Off]**
System Settings	Administrator Tools	Extended Security/Authenticate Current Job	**[Access Privilege]**
System Settings	Administrator Tools	Extended Security/Password Policy	"Complexity Setting": **[Level 1]** or higher, "Minimum Character No.": 8 or higher

Menu	Tab	Item	Setting
System Settings	Administrator Tools	Network Security Level	**[Level 2]** To acquire the machine status through printer driver or Web Image Monitor, set "SNMP" to "Active" on Web Image Monitor.
System Settings	Administrator Tools	Service Mode Lock	**[On]**
System Settings	Administrator Tools	Machine Data Encryption Settings	Select **[Encrypt]**, and then select **[All Data]** for "Carry over all data or file system data only (without formatting), or format all data.".
Scanner Features	Initial Settings	Menu Protect	**[Level 2]**

Note

❒ The SNMP setting can be specified in **[SNMP]** under **[Configuration]** in Web Image Monitor.

Reference

For details about auto logout timer settings, see "Auto Logout", Security Reference. You cannot specify the Web Image Monitor auto-logout time with Auto Logout Timer.

For details about basic authentication settings, see "Basic Authentication", Security Reference.

For details about administrator authentication settings, see "Enabling Administrator Authentication", Security Reference.

For details about extended security settings, see "Specifying the Extended Security Functions", Security Reference.

For details about network security level settings, see "Specifying Network Security Level", Security Reference.

For details about service mode lock settings, see "Limiting Machine Operations to Customers Only", Security Reference.

For details about machine data encryption settings, see "Encrypting Data on the Hard Disk", Security Reference. If **[Encrypt]** is already selected, further encryption settings are not necessary.

For details about the menu protect setting, see "Menu Protect", Security Reference.

Setting items using Web Image Monitor

Use Web Image Monitor to configure the security settings shown in the following table.

Category	Item	Setting
Device Settings/Logs	Collect Job Logs	Active
Device Settings/Logs	Collect Access Logs	Active
Security/User Lockout Policy	Lockout	Active
Security/User Lockout Policy	Number of Attempts before Lockout	5 times or less
Security/Network Security	FTP	Inactive Before specifying this setting, set "Network Security Level" to **[Level 2]** on the control panel.
Security	S/MIME	"Encryption Algorithm": 3DES-168 bit You must register the user certificate in order to use S/MIME.
Address Book/E-mail	User Certificate	You must register the user certificate in order to use S/MIME.

Reference

For details about the user lockout policy, see "User Lockout Function", Security Reference.

For details about specifying an S/MIME encryption algorithm and registering a user certificate, see "Using S/MIME to Protect E-mail Transmission", Security Reference.

Settings when IPsec is Available/Unavailable

All communication to and from machines on which IPsec is enabled is encrypted.

If your network supports IPsec, we recommend you enable it.

Settings when IPsec is available

If IPsec is available, configure the settings shown in the following table to enhance the security of the data travelling on your network.

❖ Control panel settings

Menu	Tab	Item	Setting
System Settings	Interface Settings	IPsec *1	**[Active]**
System Settings	Interface Settings	Permit SSL / TLS Communication *1	**[Ciphertext Only]**

*1 This function can also be configured using Web Image Monitor.

❖ Web Image Monitor settings

Category	Item	Setting
Security/ IPsec	Encryption Key Manual Settings	Inactive
Security/ IPsec	Encryption Key Auto Exchange Settings/ Security Level	Authentication and High Level Encryption

Settings when IPsec is not available

If IPsec is not available, configure the settings shown in the following table to enhance the security of the data travelling on your network.

❖ Setting items using the control panel

Menu	Tab	Item	Setting
System Settings	Interface Settings	IPsec *1	**[Inactive]**
System Settings	Interface Settings	Permit SSL / TLS Communication *1	**[Ciphertext Only]**

*1 This function can also be configured using Web Image Monitor.

❖ Management when IPsec is inactive

The following procedures make user data more secure when IPsec is unavailable. Administrators must inform users to carry out these procedures.

- Fax
  When sending faxes, specify destinations by fax number, Internet Fax destination, e-mail address, or folder destination. Do not specify destinations by IP-Fax destination. For details about specifying fax destinations, see "Specifying a Destination", Facsimile Reference.
- Printer
  To use the printer functions, specify "SFTP" as the protocol, or specify "IPP" and select "Active" for "SSL".
  For details about SFTP, see "Special Operations under Windows", Network and System Settings Guide.
  For details about IPP settings, see "Installing the Printer Driver", Printer Reference.
  For details about SSL settings, see "Protection Using Encryption", Security Reference.
- Scanner
  Sends the URL of the scanned files to destinations instead of sending the actual scanned files. This can be done by changing **[Stored File E-mail Method]** to **[Send URL Link]** in **[Send Settings]** in **[Scanner Features]**. Use Web Image Monitor through your network to view, delete, send, and download scanned files.
  When sending scanned files attached to e-mail, protect them by applying an S/MIME certificate. To do this, configure the "Security" settings prior to sending. For details about sending e-mail from the scanner, see "Sending Scan Files by E-mail", Scanner Reference.

Reference

For details about enabling and disabling IPsec from the control panel, see "System Settings", Network and System Settings Guide.

For details about the setting for permitting SSL/TLS communication, see "Setting the SSL/TLS Encryption Mode", Security Reference.

For details about specifying the IPsec setting via Web Image Monitor, see "Transmission Using IPsec", Security Reference.

The Privilege for User Account Settings in the Address Book

Use this section in place of "The Privilege for User Account Settings in the Address Book" in the Security Reference.

User privileges for the address book are specified as follows:

R/W, R, and N/A below indicate user privileges specified for the operations.

- Abbreviations in the table heads
  Read-only (User) = This is a user assigned "Read-only" privilege.
  Edit (User) = This is a user assigned "Edit" privilege.
  Edit / Delete (User) = This is a user assigned "Edit / Delete" privilege.
  User Admin. = This is the user administrator.
  Registered User = This is a user that has personal information registered in the Address Book and has a login password and user name.
  Full Control = This is a user granted full control.
- Abbreviations in the table columns
  R/W (Read and Write) = Both reading and modifying the setting are available.
  R (Read) = Reading only.
  N/A (Not Applicable) = Neither reading nor modifying the setting is available.

❖ Tab Name: Names

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Registration No.	R	R/W	R/W	R/W	R/W	R/W
Key Display	R	R/W	R/W	R/W	R/W	R/W
Name	R	R/W	R/W	R/W	R/W	R/W
Select Title	R	R/W	R/W	R/W	R/W	R/W

❖ Tab Name: Auth. Info

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
User Code	N/A	N/A	N/A	N/A	N/A	R/W
Login User Name	N/A	N/A	N/A	N/A	R	R/W
Login Password	N/A	N/A	N/A	N/A	R/W *1	R/W *1
SMTP Authentication	N/A	N/A	N/A	N/A	R/W *1	R/W *1
Folder Authentication	R	R/W *1	R/W *1	R/W *1	R/W *1	R/W *1
LDAP Authentication	N/A	N/A	N/A	N/A	R/W *1	R/W *1
Available Functions	N/A	N/A	N/A	N/A	R	R/W

*1 The password for "Login Password", "SMTP Authentication", "Folder Authentication" or "LDAP Authentication" can be entered or changed but not displayed.

❖ Tab Name: Protection

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Use Name as	R	R/W	R/W	R/W	R/W	R/W
Protection Code	N/A	N/A	N/A	R/W *1	R/W *1	R/W *1
Protection Object	N/A	R/W	R/W	R/W	R/W	R/W
Protect Destination: Permissions for Users / Groups	N/A	N/A	N/A	R/W	R/W	R/W
Protect File(s): Permissions for Users / Groups	N/A	N/A	N/A	R/W	R/W	R/W

*1 The code for "Protection Code" can be entered or changed but not displayed.

❖ Tab Name: Fax Dest.

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Fax Destination	R	R/W	R/W	R/W	R/W	R/W
Select Line	R	R/W	R/W	R/W	R/W	R/W
International TX Mode	R	R/W	R/W	R/W	R/W	R/W
Adv. Features	R	R/W	R/W	R/W	R/W	R/W
Fax Header	R	R/W	R/W	R/W	R/W	R/W
Label Insertion	R	R/W	R/W	R/W	R/W	R/W

❖ Tab Name: E-mail

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
E-mail Address	R	R/W	R/W	R/W	R/W	R/W
Use E-mail Address for	R	R/W	R/W	R/W	R/W	R/W
Send via SMTP Server	R	R/W	R/W	R/W	R/W	R/W

❖ Tab Name: Folder

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
SMB/FTP/NCP	R	R/W	R/W	R/W	R/W	R/W
SMB: Path	R	R/W	R/W	R/W	R/W	R/W
FTP: Port Number	R	R/W	R/W	R/W	R/W	R/W
FTP: Server Name	R	R/W	R/W	R/W	R/W	R/W
FTP: Path	R	R/W	R/W	R/W	R/W	R/W
NCP: Path	R	R/W	R/W	R/W	R/W	R/W
NCP: Connection Type	R	R/W	R/W	R/W	R/W	R/W

❖ Tab Name: Add to Group

Settings	Read-only (User)	Edit (User)	Edit / Delete (User)	Full Control	Registered User	User Admin.
Add to Group	R	R/W	R/W	R/W	R/W	R/W

Machine Administrator Settings

Use this section in place of "Machine Administrator Settings" in the Security Reference.

The machine administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ **General Features**
All the settings can be specified.

❖ **Tray Paper Settings**
All the settings can be specified.

❖ **Timer Settings**
All the settings can be specified.

❖ **Interface Settings**
The following settings can be specified.

- Network
  DNS Configuration
  You can perform a connection test.
- Parallel Interface
  Parallel Timing
  Parallel Communication Speed
  Selection Signal Status
  Input Prime
  Bidirectional Communication
  Signal Control

❖ **File Transfer**
The following settings can be specified.

- Delivery Option
- Capture Server IPv4 Address
- Fax RX File Transmission
- SMTP Authentication
  SMTP Authentication
  User Name
  E-mail Address
  Password
  Encryption
- POP before SMTP
  Wait Time after Authent.
  User Name
  E-mail Address
  Password

- Reception Protocol
- POP3 / IMAP4 Settings
  Server Name
  Encryption
  Connection Test
- Administrator's E-mail Address
- Default User Name / Password (Send)
  SMB User Name / SMB Password
  FTP User Name / FTP Password
  NCP User Name / NCP Password
- Program / Change / Delete E-mail Message
- Fax E-mail Account
  Account
  E-mail Address
  User Name
  Password

❖ **Administrator Tools**

The following settings can be specified.

- Address Book Management
  Search
  Switch Title
- Address Book: Program / Change / Delete Group
  Search
  Switch Title
- Display / Print Counter
  Print Counter List
- Display / Clear / Print Counter per User
  All Users
  Per User
- User Authentication Management
  You can specify which authentication to use.
  You can also edit the settings for each function.
- Enhanced Authentication Management
- Administrator Authentication Management
  Machine Management
- Program / Change Administrator
  Machine Administrator
- Key Counter Management
- External Charge Unit Management
- Enhanced External Charge Unit Management

- Extended Security
  Restrict Display of User Information
  Transfer to Fax Receiver
  Authenticate Current Job
  @Remote Service
  Update Firmware
  Change Firmware Structure
- Capture Priority
- Capture: Delete All Unsent Files
- Capture: Ownership
- Capture: Public Priority
- Capture: Owner Defaults
- Program / Change / Delete LDAP Server
  Name
  Server Name
  Search Base
  Port Number
  Use Secure Connection (SSL)
  Authentication
  User Name
  Password
  Realm Name
  Connection Test
  Search Conditions
  Search Options
- LDAP Search
- Program / Change / Delete Realm
  Realm Name
  KDC Server Name
  Domain Name
- AOF (Always On)
- Service Mode Lock
- Delete All Logs
- Auto Erase Memory Setting
- Erase All Memory
- Transfer Log Setting
- Data Security for Copying
- Print Backup: Delete All Files
- Print Backup: Compression
- Print Backup: Default Format
- Print Backup: Default Resolution
- Fixed USB Port
- Machine Data Encryption Settings

Note

- ❒ The "Parallel Interface" setting is available only if the optional IEEE 1284 interface board is installed.
- ❒ The "Capture Server IPv4 Address" setting appears only when the optional File Format Converter is installed and the capture function is being used by the ScanRouter delivery software.
- ❒ The "Fax RX File Transmission" setting is displayed only when the ScanRouter delivery software is using the delivery function.
- ❒ "Auto Erase Memory Setting" and the "Erase All Memory" setting are available only if the optional DataOverwriteSecurity unit is installed.
- ❒ The following settings are available only if the optional File Format Converter is installed: "Capture Priority", "Capture: Delete All Unsent Files", "Capture: Ownership", "Capture: Public Priority", "Capture: Owner Defaults", "Print Backup: Delete All Files", "Print Backup: Compression", "Print Backup: Default Format", "Print Backup: Default Resolution".
- ❒ The "Data Security for Copying" setting is available only if the optional Copy Data Security unit is installed.
- ❒ "Machine Data Encryption Settings" are available only if the optional HDD Encryption unit is installed.

Copier / Document Server Features

The following settings can be specified.

❖ **General Features**
All the settings can be specified.

❖ **Reproduction Ratio**
All the settings can be specified.

❖ **Edit**
All the settings can be specified.

❖ **Stamp**
All the settings can be specified.

❖ **Input / Output**
All the settings can be specified.

❖ **Administrator Tools**
All the settings can be specified.

Facsimile Features

The following settings can be specified.

❖ **General Settings**
All the settings can be specified.

❖ **Scan Settings**
All the settings can be specified.

❖ **Send Settings**
The following settings can be specified.
- Program / Change / Delete Standard Message
- Backup File TX Setting

❖ **Reception Settings**
The following settings can be specified.
- Switch Reception Mode
- Program Special Sender
- Program Special Sender: Print List
- Forwarding
- Reception File Setting
- SMTP RX File Delivery Settings
- 2 Sided Print
- Checkered Mark
- Centre Mark
- Print Reception Time
- Reception File Print Quantity
- Paper Tray
- Specify Tray for Lines
- Folder Transfer Result Report
- Memory Lock Reception

❖ **Initial Settings**
The following settings can be specified.
- Parameter Setting
- Parameter Setting: Print List
- Program Closed Network Code
- Program Memory Lock ID
- Internet Fax Setting
- Select Dial / Push Phone
- Program Fax Information
- Menu Protect

- E-mail Setting
- Folder Setting

Printer Features

The following settings can be specified.

❖ **List / Test Print**
All the settings can be specified.

❖ **Maintenance**
The following settings can be specified.
- Menu Protect
- List / Test Print Lock
- Reset IPDS Fonts

❖ **System**
The following settings can be specified.
- Print Error Report
- Auto Continue
- Memory Overflow
- Job Separation
- Rotate by 180 Degrees
- Initial Print Job List
- Print Compressed Data
- Memory Usage
- Duplex
- Copies
- Blank Page Print
- Edge Smoothing
- Toner Saving
- Spool Image
- Reserved Job Waiting Time
- Printer Language
- Sub Paper Size
- Page Size
- Letterhead Setting
- Bypass Tray Setting Priority
- Edge to Edge Print
- Default Printer Language
- Tray Switching
- Extended Auto Tray Switching

❖ **Host Interface**
All the settings can be specified.

❖ **PCL Menu**
All the settings can be specified.

❖ **PS Menu**
All the settings can be specified.

❖ **PDF Menu**
All the settings can be specified.

❖ **IPDS Menu**
All the settings can be specified.

Note

❒ The "Job Separation" function is available only when the optional finisher is installed.

❒ The "Reset IPDS Fonts" setting is available only if the optional IPDS unit is installed.

❒ PS or PDF menu settings are available only if the optional PostScript 3 unit is installed.

❒ IPDS menu settings are available only if the optional IPDS unit is installed.

Scanner Features

The following settings can be specified.

❖ **General Settings**

- Switch Title
- Update Delivery Server Destination List
- Search Destination
- TWAIN Standby Time
- Destination List Display Priority 1
- Destination List Display Priority 2
- Print & Delete Scanner Journal
- Print Scanner Journal
- Delete Scanner Journal

❖ **Scan Settings**
All the settings can be specified.

❖ **Send Settings**

The following settings can be specified.

- Compression (Black & White)
- Compression (Gray Scale / Full Colour)
- High Compression PDF Level
- Insert Additional E-mail Info
- No. of Digits for Single Page Files
- Stored File E-mail Method
- Default E-mail Subject

❖ **Initial Settings**

All the settings can be specified.

Settings via Web Image Monitor

The following settings can be specified.

❖ **Home**

- Reset Device
- Reset Printer Job

❖ **Job**

All the settings can be specified.

❖ **Device Settings**

- System
  Spool Printing
  Protect Printer Display Panel
  Print Priority
  Function Reset Timer
  Permit Firmware Update
  Permit Firmware Structure Change
  Display IP Address on Device Display Panel
  Output Tray
  Paper Tray Priority
  Front Cover Sheet Tray
  Back Cover Sheet Tray
  Slip Sheet Tray
  Designation Sheet 1 Tray
  Designation Sheet 2 Tray
- Paper
  All the settings can be specified.
- Date/Time
  All the settings can be specified.
- Timer
  All the settings can be specified.

- Logs
  Job Log
  Access Log
  Transfer Logs (Can be changed to **[Inactive]** only.)
  Encrypt Logs
  Classification Code
  Delete All Logs
- Download Logs
- E-mail
  All the settings can be specified.
- Auto E-mail Notification
  All the settings can be specified.
- On-demand E-mail Notification
  All the settings can be specified.
- File Transfer
  All the settings can be specified.
- User Authentication Management
  All the settings can be specified.
- Administrator Authentication Management
  Machine Administrator Authentication
  Available Settings for Machine Administrator
- Program/Change Administrator
  You can specify the following administrator settings as the machine administrator.
  Login User Name
  Login Password
  Encryption Password
- LDAP Server
  All the settings can be specified.
- Firmware Update
  All the settings can be specified.
- Program/Change Realm
  All the settings can be specified.

❖ **Printer**

- System
  Print Error Report
  Auto Continue
  Memory Overflow
  Job Separation
  Initial Print Job List
  Rotate by 180 Degrees
  Print Compressed Data
  Memory Usage
  Duplex
  Copies
  Blank Page Print
  Edge Smoothing

Toner Saving
Spool Image
Reserved Job Waiting Time
Printer Language
Sub Paper Size
Page Size
Letterhead Setting
Bypass Tray Setting Priority
Edge to Edge Print
Default Printer Language
Tray Switching
Extended Auto Tray Switching
Virtual Printer

- Host Interface
  All the settings can be specified.
- PCL Menu
  All the settings can be specified.
- PS Menu
  All the settings can be specified.
- PDF Menu
  All the settings can be specified.
- IPDS Menu
  All the settings can be specified.
- Tray Parameters (PCL)
  All the settings can be specified.
- Tray Parameters (PS)
  All the settings can be specified.
- PDF Group Password
  All the settings can be specified.
- PDF Fixed Password
  All the settings can be specified.
- Virtual Printer Settings
  All the settings can be specified.
- IPDS Form List
  All the settings can be specified.
- Reset IPDS Fonts
  All the settings can be specified.

❖ **Fax**

- Initial Settings
  All the settings can be specified.
- Send / Reception Settings
  Switch Reception Mode
  SMTP RX File Delivery Settings
  Duplex
  Checkered Mark
  Center Mark
  Print Reception Time
  Reception File Print Quantity
  Paper Tray
  Memory Lock Reception
- Parameter Settings
  All the settings can be specified.

❖ **Scanner**

- General Settings
  All the settings can be specified.
- Scan Settings
  All the settings can be specified.
- Send Settings
  Compression (Black & White)
  Compression (Gray Scale/Full Color)
  High Compression PDF Level
  Insert Additional E-mail Info
  No. of Digits for Single Page Files
  Stored File E-mail Method
  Default E-mail Subject
- Initial Settings
  All the settings can be specified.
- Default Settings for Normal Screens on Device
  All the settings can be specified.
- Default Settings for Simplified Screens on Device
  All the settings can be specified.

❖ **Interface**

- USB

❖ **Network**

- SNMPv3
  Account(Machine Administrator)

❖ **Security**

- User Lockout Policy
  All the settings can be specified.

❖ **RC Gate**

All the settings can be specified.

❖ **Webpage**

- Webpage
  Download Help File

❖ **Extended Feature Settings**
All the settings can be specified.

Note

❒ The "Job Separation" function is available only when the optional finisher is installed.

❒ The following settings are available only if the optional IPDS unit is installed: "IPDS Menu", "IPDS Form List", and "Reset IPDS Fonts".

❒ The following settings are available only if the optional PostScript 3 unit is installed: "PS Menu", "PDF Menu", "Tray Parameters (PS)", "PDF Group Password", and "PDF Fixed Password".

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Device Properties**

- Reset Device
- Reset Current Job
- Reset All Jobs

❖ **User Management Tool**

- Export User Statistics List
- Edit CSV File Format of the User Statistics List
- Open CSV File with Program
- Restrict Access To Device
- Find User

Network Administrator Settings

Use this section in place of "Network Administrator Settings" in the Security Reference.

The network administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ **Interface Settings**

If DHCP is set to On, the settings that are automatically obtained via DHCP cannot be specified.

- Print List
- Network
  Machine IPv4 Address
  IPv4 Gateway Address
  IPv6 Stateless Address Autoconfiguration
  DNS Configuration
  DDNS Configuration
  IPsec
  Domain Name
  WINS Configuration
  Effective Protocol
  NCP Delivery Protocol
  NW Frame Type
  SMB Computer Name
  SMB Work Group
  Ethernet Speed
  IEEE 802.1X Authentication for Ethernet
  Restore IEEE 802.1X Authentication to Defaults
  LAN Type
  Ping Command
  Permit SNMPv3 Communication
  Permit SSL / TLS Communication
  Host Name
  Machine Name
- Wireless LAN
  All the settings can be specified.

❖ **File Transfer**

- SMTP Server
  Server Name
  Port No.
  Connection Test
- E-mail Communication Port
  All the settings can be specified.
- E-mail Reception Interval

- Max. Reception E-mail Size
- E-mail Storage in Server
- Auto Specify Sender Name
- Scanner Resend Interval Time
- Number of Scanner Resends

❖ Administrator Tools

- Address Book Management
  Search
  Switch Title
- Address Book: Program / Change / Delete Group
  Search
  Switch Title
- Administrator Authentication Management
  Network Management
- Program / Change Administrator
  Network Administrator
- Extended Security
  Driver Encryption Key
  Settings by SNMPv1, v2
  Restrict Use of Simple Encryption
- Network Security Level

Note

❒ The "Wireless LAN" setting is available only if the optional Wireless LAN interface unit is installed.

Facsimile Features

The following settings can be specified.

❖ Send Settings

- Max. E-mail Size

❖ Initial Settings

- Enable H.323
- Enable SIP
- H.323 Settings
- SIP Settings
- Program / Change / Delete Gateway

Printer Features

The following settings can be specified.

❖ System

- Print Compressed Data

Scanner Features

The following settings can be specified.

❖ Send Settings

- Max. E-mail Size
- Divide & Send E-mail

Settings via Web Image Monitor

The following settings can be specified.

❖ Device Settings

- System
  Device Name
  Comment
  Location
- E-mail
  Reception
  SMTP
  E-mail Communication Port
- Auto E-mail Notification
  You can select groups to notify.
- Administrator Authentication Management
  Network Administrator Authentication
  Available Settings for Network Administrator
- Program/Change Administrator
  You can specify the following administrator settings for the network administrator.
  Login User Name
  Login Password
  Encryption Password

❖ Printer

- System
  Print Compressed Data

❖ Fax

- Send / Reception Settings
  Maximum E-mail Size
- IP-Fax Settings
  All the settings can be specified.
- IP-Fax Gateway Settings
  All the settings can be specified.

❖ Scanner

- Send Settings
  Max. E-mail Size
  Divide & Send E-mail

❖ Interface

- Interface Settings
  LAN Type
  Ethernet Security
  Ethernet Speed
- Wireless LAN Settings
  LAN Type
  Communication Mode
  SSID
  Channel
  Security Method
  WEP Authentication
  WEP Key Number
  WEP Key
  WPA Encryption Method
  WPA Authentication Method
  WPA-PSK
- Bluetooth
  Operation Mode

❖ Network

- IPv4
  All the settings can be specified.
- IPv6
  All the settings can be specified.
- NetWare
  All the settings can be specified.
- AppleTalk
  All the settings can be specified.
- SMB
  All the settings can be specified.
- SNMP
  All the settings can be specified.
- SNMPv3
  All the settings can be specified.

- SSDP
  All the settings can be specified.
- Bonjour
  All the settings can be specified.

❖ **Security**

- Network Security
  All the settings can be specified.
- Access Control
  All the settings can be specified.
- IPP Authentication
  All the settings can be specified.
- SSL/TLS
  All the settings can be specified.
- ssh
  All the settings can be specified.
- Site Certificate
  All the settings can be specified.
- Device Certificate
  All the settings can be specified.
- IPsec
  All the settings can be specified.
- IEEE 802.1X (WPA/WPA2)
  All the settings can be specified.
- S/MIME
  All the settings can be specified.

❖ **Webpage**

All the settings can be specified.

Note

❒ "Wireless LAN Settings" are available only if the optional Wireless LAN interface unit is installed.

❒ The "Bluetooth" setting is available only if the optional Bluetooth interface unit is installed.

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **NIB Setup Tool**

All the settings can be specified.

File Administrator Settings

Use this section in place of "File Administrator Settings" in the Security Reference.

The file administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ Interface Settings

- Network
  DNS Configuration
  You can perform a connection test.

❖ Administrator Tools

- Address Book Management
  Search
  Switch Title
- Address Book: Program / Change / Delete Group
  Search
  Switch Title
- Administrator Authentication Management
  File Management
- Program / Change Administrator
  File Administrator
- Extended Security
  Enhance File Protection
- Auto Delete File in Document Server
- Delete All Files in Document Server

Facsimile Features

The following settings can be specified.

❖ Reception Settings

- Stored Reception File User Setting

Printer Features

The following settings can be specified.

❖ **Maintenance**

- Delete All Temporary Print Jobs
- Delete All Stored Print Jobs

❖ **System**

- Auto Delete Temporary Print Jobs
- Auto Delete Stored Print Jobs

Settings via Web Image Monitor

The following settings can be specified.

❖ **Document Server**
All the settings can be specified.

❖ **Printer: Print Jobs**
All the settings can be specified.

❖ **Device Settings**

- Auto E-mail Notification
  You can select groups to notify.
- Administrator Authentication Management
  File Administrator Authentication
  Available Settings for File Administrator
- Program/Change Administrator
  You can specify the following administrator settings for the file administrator.
  Login User Name
  Login Password
  Encryption Password

❖ **Printer**

- System
  Auto Delete Temporary Print Jobs
  Auto Delete Stored Print Jobs

❖ **Webpage**

- Webpage
  Download Help File

User Administrator Settings

Use this section in place of "User Administrator Settings" in the Security Reference.

The user administrator settings that can be specified are as follows:

System Settings

The following settings can be specified.

❖ Interface Settings

- Network
  DNS Configuration
  You can perform a connection test.

❖ Administrator Tools

- Address Book Management
- Address Book: Program / Change / Delete Group
- Address Book: Change Order
- Print Address Book: Destination List
- Address Book: Edit Title
- Address Book: Switch Title
- Back Up / Restore Address Book
- Data Carry-over Setting for Address Book Auto-program
- Display / Clear / Print Counter per User
  All Users: Clear
  Per User: Clear
- Administrator Authentication Management
  User Management
- Program / Change Administrator
  User Administrator
- Extended Security
  Encrypt Address Book
  Restrict Use of Destinations
  Restrict Adding of User Destinations
  Password Policy

Settings via Web Image Monitor

The following settings can be specified.

❖ **Address Book**
All the settings can be specified.

❖ **Device Settings**

- Auto E-mail Notification
  You can select groups to notify.
- Administrator Authentication Management
  User Administrator Authentication
  Available Settings for User Administrator
- Program/Change Administrator
  The user administrator settings that can be specified are as follows:
  Login User Name
  Login Password
  Encryption Password

❖ **Webpage**

- Webpage
  Download Help File

Settings via SmartDeviceMonitor for Admin

The following settings can be specified.

❖ **Address Management Tool**
All the settings can be specified.

❖ **User Management Tool**

- Export User Statistics List
- Edit CSV File Format of the User Statistics List
- Open CSV File with Program
- Export User Information
- Import User Information
- Reset User Counters
- Find User
- Add New User
- Delete User
- User Properties

Notes for Security Functions

EN GB
EN US
EN AU D062-7156