

Canon

imageRUNNER

1750i / 1740i / 1730i / 1730

Remote UI Guide



Please read this guide before operating this product.
After you finish reading this guide, store it in a safe place for future reference.

ENG

imageRUNNER
1750i/1740i
1730i/1730
Remote UI Guide



Manuals for the Machine

The manuals for this machine are organized as shown below. Please refer to them for detailed information. Some manuals may not be needed for certain system configurations and products purchased.
















Guides with this symbol are printed manuals.



Guides with this symbol are PDF manuals included on the accompanying CD-ROM.

- **Installation of the Machine**
- **Legal Notices**
- **Setup Instructions**
- **Quick Reference for Basic Operations**
- **Basic Operations**
- **Troubleshooting**
- **Copying Instructions**
- **Sending and Fax Instructions**
- **Remote User Interface Instructions**
- **Network Connectivity**
- **Security Management**
- **Color Network ScanGear Instructions**
- **USB Memory Media Printing Instructions**
- **PS/PCL/UFRII LT Printer Instructions**
- **Windows Printer Driver Instructions**
- **Windows Fax Driver Instructions**
- **Macintosh Printer Driver Instructions**

Starter Guide	
User's Guide	
Easy Operation Guide	
Reference Guide	
Copying Guide	
Sending and Facsimile Guide	
Remote UI Guide (This Document)	
System Settings Guide	
Network ScanGear Guide	
Printer Guide	
Windows Printer Driver Guide	
Windows Fax Driver Guide	
Mac Printer Driver Guide	



How This Manual Is Organized

Chapter 1 Introduction to the Remote UI

Chapter 2 Managing Jobs and Machine Data

Chapter 3 Specifying Department ID and User Management

Chapter 4 Customizing Settings

Chapter 5 Appendix

Includes the glossary and index.

Contents

Preface	vi
How to Use This Manual	vi
Symbols Used in This Manual	vi
Keys and Buttons Used in This Manual	vi
Displays Used in This Manual	vii
Abbreviations Used in This Manual	viii
Trademarks	viii
Availability of the Optional Equipment	viii
Legal Notices	ix
Copyright	ix
Disclaimers	ix

Chapter 1 Introduction to the Remote UI

Overview of the Remote UI	1-2
Functions of the Remote UI	1-3
The Top Page of the Remote UI	1-4
Logon Modes of the Remote UI	1-5
Buttons on the Remote UI	1-6
System Requirements	1-7
Before Using the Remote UI	1-8
Starting the Remote UI	1-9
Viewing the Machine Status and Information	1-14

Chapter 2 Managing Jobs and Machine Data

Managing Jobs	2-2
Managing the Print Jobs	2-2
Viewing the Job Logs	2-4
Managing the Address Book	2-5
Editing the Destinations	2-6
Importing and Exporting Data	2-11
Exporting Address Book Data	2-12
Importing Address Book Data	2-13
Exporting User Management Data	2-14
Importing User Management Data	2-15
Resetting Imported User Management Data	2-17
Exporting Additional Functions Setting Data	2-21
Importing Additional Functions Setting Data	2-23

Managing Key Pairs and Digital Certificates from a Web Browser	2-25
Installing and Registering a Key and Certificate	2-26
Deleting a Key and Certificate	2-30
Installing and Registering a CA Certificate	2-32
Deleting a CA Certificate	2-35

Chapter 3 Specifying Department ID and User Management

Managing the Department IDs and User IDs	3-2
Enabling Department ID Management and User Management	3-2
Managing the Department IDs	3-6
Managing the User IDs	3-10

Chapter 4 Customizing Settings

Customizing the System Settings	4-2
Editing the LDAP Server Settings	4-10
Editing the Forwarding Settings	4-14
Specifying the Authorized Send Settings	4-17
Customizing the Machine Settings	4-26
Specifying the SNMPv3 Settings	4-29
Enabling SNMPv3	4-30
Specifying the User Information for SNMPv3	4-31
Specifying the Context Settings for SNMPv3	4-34
Verifying SSL Server Certificates	4-37

Chapter 5 Appendix

Glossary	5-2
Index	5-6


Preface


Thank you for purchasing the Canon imageRUNNER 1750i/1740i/1730i/1730. Please read this manual thoroughly before operating the machine to familiarize yourself with its capabilities, and to make the most of its many functions. After reading this manual, store it in a safe place for future reference.

How to Use This Manual

Symbols Used in This Manual

The following symbols are used in this manual to explain procedures, restrictions, handling precautions, and instructions that should be observed for safety.


 **IMPORTANT** Indicates operational requirements and restrictions. Be sure to read these items carefully to operate the machine correctly, and avoid damage to the machine or property.

 **NOTE** Indicates a clarification of an operation, or contains additional explanations for a procedure. Reading these notes is highly recommended.


Keys and Buttons Used in This Manual

The following tables provide a few examples of how keys, buttons, and other user interfaces such as icons displayed on the screen are expressed in this manual:

- Keys on the machine's control panel and touch panel display:

	Keys	Example
Control Panel	Key icon + (Key Name)	 (Additional Functions)
Touch Panel Display	[Key Name]	[OK], [Cancel], etc.
	[Key Icon]	[▼], [▲], etc.

- Buttons, icons and other user interfaces on computer operation screens:


Buttons and Other Objects	Example
[Button Name]	[OK]
[Name] + icon, menu, etc.	[CD-ROM] icon, [Start] menu, etc.
[Icon] + (Icon Name).	 (New)

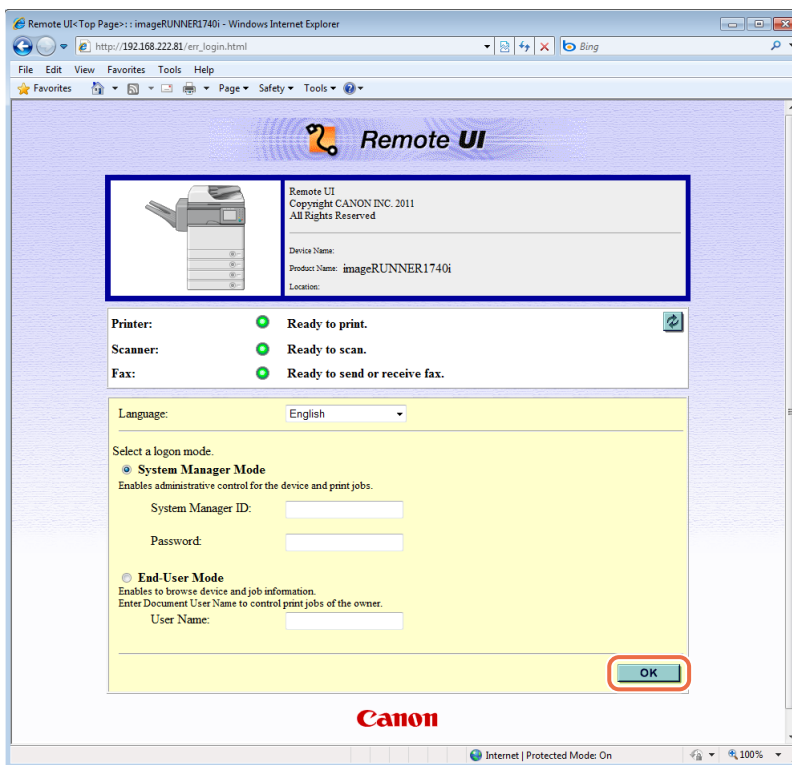
Displays Used in This Manual

Unless otherwise noted, the screen shots used in this manual are taken from the imageRUNNER 1740i with the following optional equipment: Staple Finisher-H1, Cassette Module-Y1 (triple-tiered), Super G3 Fax Board-AJ1, PCL Printer Kit-AL1, and PS Printer Kit-AL1.

Functions that are unavailable due to a particular combination of accessories and optional equipment are not displayed in the web browser. Therefore, the screen shots of the Remote UI used in this manual may differ from the ones you actually see on your web browser, depending on the model or options you have installed or activated.

The IP addresses shown in the screen shots and text in this manual are for illustrative purposes only.

The buttons and other objects that are related to operations during the procedure are marked with a , as shown in the example below.



Abbreviations Used in This Manual

In this manual, product names are abbreviated as follows:

Microsoft Windows 2000 operating system:	Windows 2000
Microsoft Windows XP operating system:	Windows XP
Microsoft Windows Vista operating system:	Windows Vista
Microsoft Windows 7 operating system:	Windows 7
Microsoft Windows operating system:	Windows

Trademarks

Macintosh and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Microsoft, Windows, Windows Vista, and Internet Explorer are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names herein may be the trademarks of their respective owners.

Availability of the Optional Equipment

Of the optional equipment described in the manuals, the Copy Card Reader-F1 may not be available depending on the country or region of purchase. For more information on the optional equipment, see Chapter 4, “Optional Equipment,” in the *Reference Guide*.

Legal Notices

Copyright

Copyright 2012 by Canon Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system without the prior written permission of Canon Inc.

Disclaimers

The information in this document is subject to change without notice.

CANON INC. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, EITHER EXPRESS OR IMPLIED, EXCEPT AS PROVIDED HEREIN, INCLUDING WITHOUT LIMITATION, THEREOF, WARRANTIES AS TO MARKETABILITY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE OR NON-INFRINGEMENT. CANON INC. SHALL NOT BE LIABLE FOR ANY DIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY NATURE, OR LOSSES OR EXPENSES RESULTING FROM THE USE OF THIS MATERIAL.

Introduction to the Remote UI

1

CHAPTER

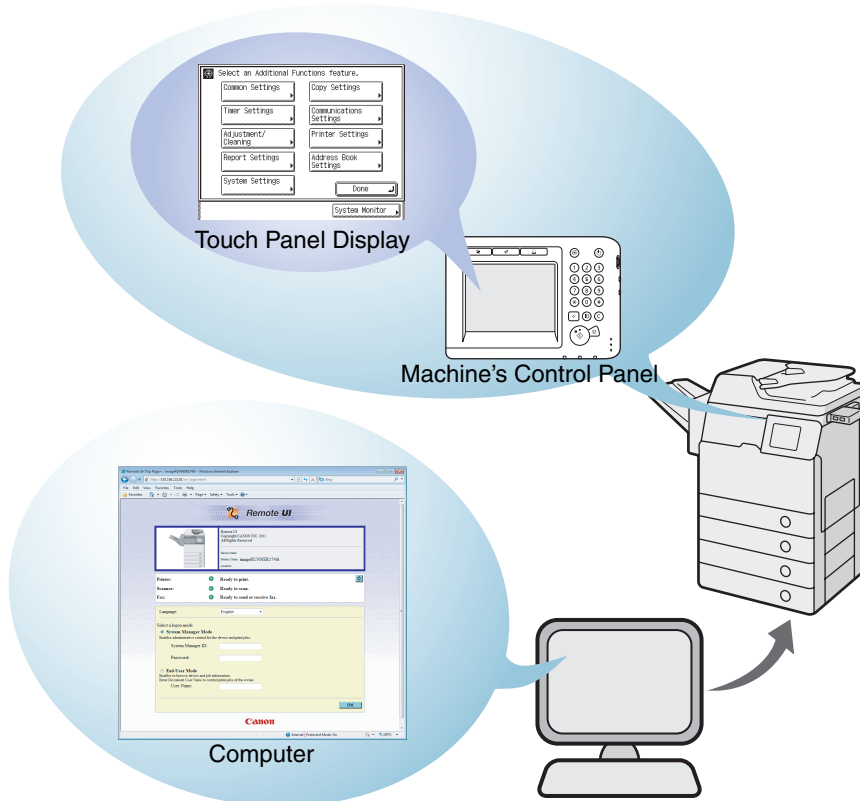
This chapter describes the functionality of the Remote UI and how to start it.

Overview of the Remote UI	1-2
Functions of the Remote UI	1-3
The Top Page of the Remote UI	1-4
Logon Modes of the Remote UI	1-5
Buttons on the Remote UI	1-6
System Requirements	1-7
Before Using the Remote UI	1-8
Starting the Remote UI	1-9
Viewing the Machine Status and Information	1-14

Overview of the Remote UI

The Remote UI (Remote User Interface) software comes preinstalled in the machine and enables you to access the machine's functions by using a web browser. For example, the Remote UI enables you to check the job status, delete jobs, and edit various settings. To use the Remote UI, all you need is a web browser and a network connection between your computer and the machine.

First set the IP (Internet Protocol) address for the machine from the machine's control panel and set up the necessary network connection. Then start your web browser and enter the IP address of the machine. The Remote UI top page is displayed on your computer screen and is ready for you to log in.



You can operate the machine both with the control panel and from the Remote UI.

The major functions available on the Remote UI are as follows:

■ Viewing the machine status

You can view the current status of the machine, such as the remaining paper or toner amount, on your computer screen.

(See “Viewing the Machine Status and Information,” on p. 1-14.)

■ Managing jobs and job logs

You can view the current status of the jobs and the job logs processed by the machine on your computer screen. You can also delete the jobs when you log in to the Remote UI as the System Manager or can delete your own jobs when you log in as an End User.

(See “Managing Jobs,” on p. 2-2.)



NOTE

For the End Users to delete their own jobs, the Permit End-user's Job Operation setting must be enabled. (See “To specify the System Manager ID and System Password:,” on p. 4-9.)

■ Importing and exporting the machine data

You can save and load the machine data such as Address Book data or the Additional Functions setting data.

(See “Importing and Exporting Data,” on p. 2-11.)

■ Managing key pairs and digital certificates

You can install and register key pairs and digital certificates.

(See “Managing Key Pairs and Digital Certificates from a Web Browser,” on p. 2-25.)

■ Specifying the Department ID Management and User Management

You can manage the Department IDs and User IDs. User IDs can be registered, edited, or deleted only on the Remote UI, while the Department IDs can be managed both on the machine's control panel and on the Remote UI.


(See “Managing the Department IDs and User IDs,” on p. 3-2.)

■ Specifying the Authorized Send settings

You can specify the Authorized Send settings only on the Remote UI.

(See “Specifying the Authorized Send Settings,” on p. 4-17.)

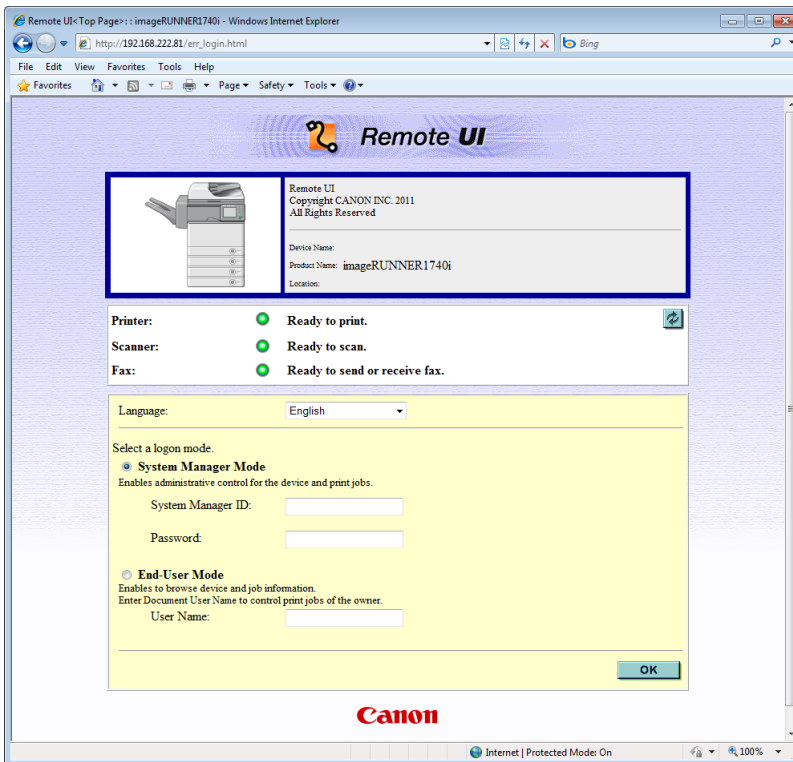
■ Customizing the Additional Functions settings

You can edit the Additional Functions settings on the Remote UI as you can by pressing  (Additional Functions) on the machine's control panel.

(See “Customizing Settings,” on p. 4-1.)

The Top Page of the Remote UI

When you enter the IP address of the machine on your web browser and press the [ENTER] key on your computer keyboard, the Remote UI top page is displayed.



NOTE

- The appearance of the Remote UI top page depends on the management mode applied to the machine. For more information, see “Enabling Department ID Management and User Management,” on p. 3-2.
- For instructions on how to log in to the Remote UI, see “Starting the Remote UI,” on p. 1-9.

Logon Modes of the Remote UI

When you log in to the Remote UI by entering the System Manager ID and System Password or the User ID registered as the System Manager and its password, the authority of the System Manager is applied to the Remote UI, and other users (End Users) cannot edit the System Settings and other settings restricted to the System Manager.

■ System Manager Mode

You can access the Remote UI functions with no restrictions.

■ End-User Mode

You can access all Remote UI functions except those restricted to the System Manager. Major functions open to End Users and the System Manager are:

- Checking the machine status such as paper or toner amount
- Checking the job status and deleting their own jobs

NOTE

For the End Users to delete their own jobs, the Permit End-user's Job Operation setting must be enabled. (See "To specify the System Manager ID and System Password;" on p. 4-9.)

- Registering or editing the addresses for the Send/Fax functions

NOTE

The Address Book can be protected by setting a password in the Restrict Send Function page. (See "To specify the Restrict the Send Function settings;" on p. 4-8.)

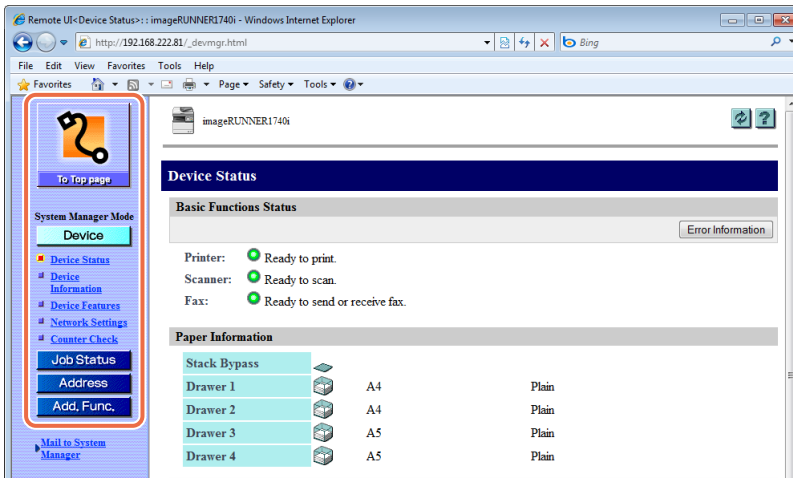
- Customizing the Additional Functions settings except those restricted to the System Manager, such as the System Settings.

Buttons on the Remote UI

After you have logged in to the Remote UI, the Device Status page is displayed. The left frame of the page displays the buttons listed below, which allow you to access and perform operations on other Remote UI pages.

1

Introduction to the Remote UI



Click to return to the Remote UI top page.



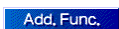
Click to display the machine status and various setting information.




Click to display the status of the jobs and the logs of the jobs processed by the machine.



Click to manage the Address Book of the machine.



Click to specify or change various settings on the machine. This button works similarly as the  (Additional Functions) key on the machine's control panel.



Click to update or refresh the current page with the latest information.



Click to display the online help for the Remote UI.



Click to return to the top of the page.



Click to return to the previous page.

System Requirements

The Remote UI has been confirmed to work in the following system environments.

■ Windows

- OS (Operating Systems)
 - Windows 2000
 - Windows XP
 - Windows Vista
 - Windows 7
- Web Browser
 - Microsoft Internet Explorer 6.0 or later

■ Macintosh

- OS (Operating System)
 - Mac OS X 10.3 or later, except Classic Environment
- Web Browser
 - Safari 2.0.3 or later
 - Safari 1.3.2 on Mac OS X 10.3.x is also supported.



NOTE

Other than the software listed above, no other software, such as a web server, is necessary. (There is already a web server inside the machine.)

Before Using the Remote UI


Before you start using the Remote UI, specify or check the following settings.

■ Specifying the Network Settings on the machine

- Specify or check the Network Settings to obtain or find out the IP address of the machine.
- Confirm that the Use HTTP setting is set to 'On'.



NOTE

- You can find the Network Settings including the Use HTTP setting by pressing  (Additional Functions) → [System Settings].
- If you cannot find out the IP address of the machine, consult your network administrator or see the *System Settings Guide*.

■ Enabling the Remote UI and specifying the device name

- Confirm that the Remote UI On/Off setting is set to 'On'. If you want to establish a more secure communication by using SSL, set the Use SSL setting to 'On'. Make sure to generate and specify the default SSL key pair. (See Chapter 3, "Setting up the Machine for Your Network Environment," in the *System Settings Guide*.)
- Specify the name of the device in the Device Info Settings to identify the machine you operate from the Remote UI by the specified name.




IMPORTANT

- Connection via a proxy server is not possible. If your system environment has a proxy server, specify the IP address of the machine as an proxy exception on your web browser. (Set your web browser not to access the IP address of the machine through a proxy server.) Setting procedures vary depending on the system environment. Consult your network administrator.
- Enable all cookies and use Java Script on your web browser. Otherwise, you will not be able to change the machine's settings using the Remote UI.
- If multiple Remote UIs are running simultaneously, the latest setting is enabled.



NOTE

You can find the Remote UI On/Off setting and Device Info Settings by pressing  (Additional Functions) → [System Settings]. For more information on the Remote UI On/Off setting, see Chapter 6, "Protecting the Machine from Unauthorized Access," in the *System Settings Guide*. For more information on the Device Info Settings, see Chapter 7, "Other System Settings," in the *System Settings Guide*.

Starting the Remote UI

To start the Remote UI, follow the procedure below.



IMPORTANT

- The IP addresses shown in the screen shots and text in this manual are for illustrative purposes only.
- If the Language Switch setting is set to 'On', some characters are restricted and cannot be entered. To enter all characters, set the Language Switch setting to 'Off'. (See Chapter 3, "Configuring the Machine's Basic Settings," in the *Reference Guide*.)
- If you change the language on the Remote UI, the characters of the displayed language can be entered. However, if the displayed language is different from the language used on the touch panel display of the machine, the language may not be displayed correctly.
- To enter characters from a web browser, use the characters that you can enter from the machine's control panel. If you use other characters, they may not be displayed or recognized properly on the machine.

1 Start your web browser.

2 Enter the appropriate URL into [Address] or [Location] bar in the web browser → press the [ENTER] key on your computer keyboard.

```
http://<the IP address of the machine>/
```

If you do not know the appropriate URL, consult your network administrator.

The Remote UI top page is displayed.



IMPORTANT

If the machine's SSL communication is enabled, a security alert may be displayed regarding the security certificate. In this case, check that the correct URL is entered, and then proceed to display the Remote UI top page. For more information on the SSL communication, see Chapter 3, "Setting up the Machine for Your Network Environment," in the *System Settings Guide*.



NOTE

You can change the language displayed on the Remote UI top page by clicking the [Language] drop-down list box and selecting the desired language, regardless of the language used on the touch panel display of the machine.

3 Enter your ID and password depending on the management mode applied to the machine.

The required ID and password vary depending on the management mode (Department ID/User Management) applied to the machine. For more information, see “Enabling Department ID Management and User Management,” on p. 3-2.

● When Department ID Management and User Management are disabled:

- ❑ Select the logon mode and enter the System Manager ID and System Password, or user name.
 - To log in to the Remote UI in the System Manager Mode, select the option button for [System Manager Mode] → enter the System Manager ID and System Password.

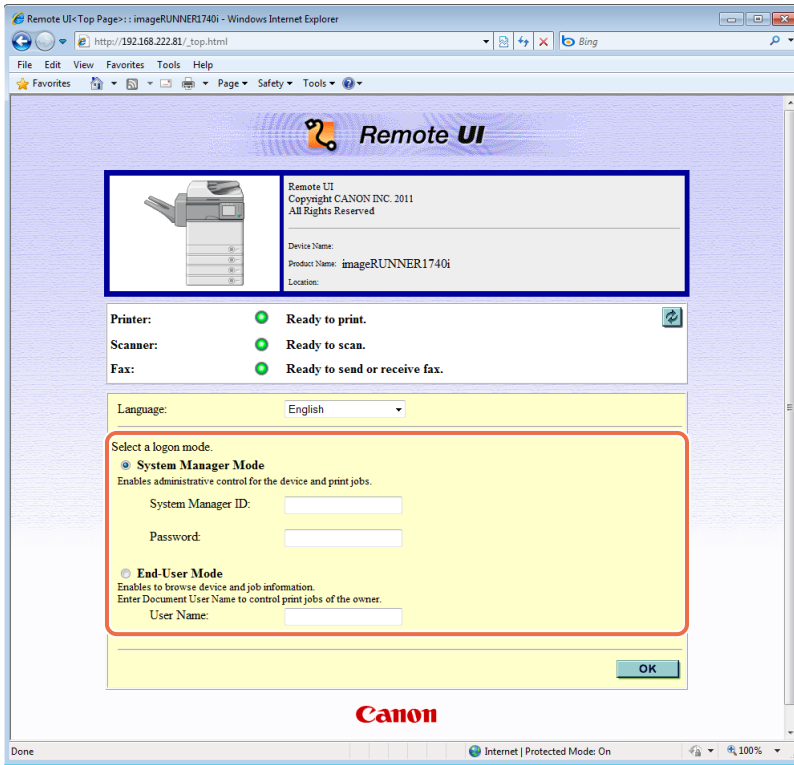
IMPORTANT

The System Manager ID and System Password are both set to ‘7654321’ at purchase. Change them before using the machine. (See “To specify the System Manager ID and System Password:,” on p. 4-9.)

- To log in to the Remote UI in the End-User Mode, select the option button for [End-User Mode] → enter the user name or leave the [User Name] text box blank. (See the note below.)

NOTE

If you are logging in to the Remote UI in the End-User Mode and want to delete your own print job, enter your user name with which you sent the print job (it is usually the user name for your computer). Otherwise, click [OK] to log in to the Remote UI with the [User Name] text box left blank. (See the note on p. 1-5.)



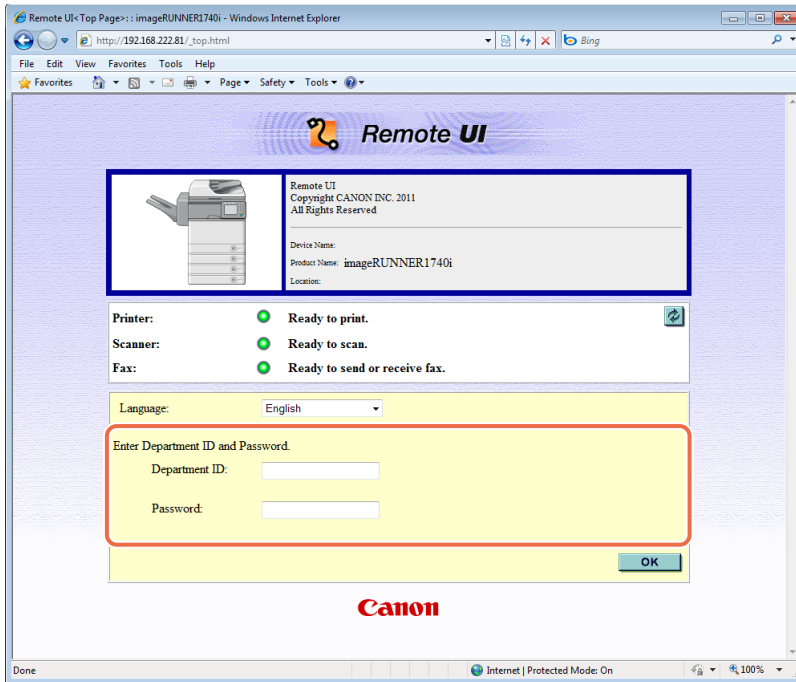
 NOTE

- If the page is not shown correctly, check the following settings:
 - Cache settings on your web browser
 - HTTP port number (default is '80')
- For information on other network connection problems and remedies, see Chapter 8, "Troubleshooting," in the *System Settings Guide* or consult your network administrator.

● When Department ID Management is enabled:

- ❑ Enter the Department ID and password.

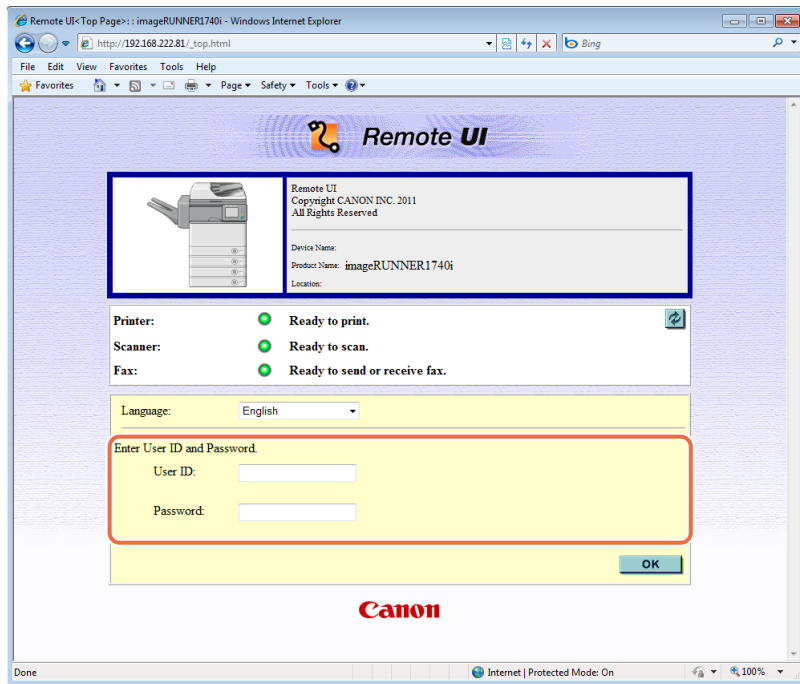
You can log in as the System Manager by entering the System Manager ID in the [Department ID] text box and the System Password in the [Password] text box.



● When User Management is enabled:

- Enter the User ID and password.

You can log in as the System Manager by entering the User ID registered as the System Manager in the [User ID] text box and its password in the [Password] text box.



● When both Department ID Management and User Management are enabled:

NOTE

The same Remote UI top page as shown in “When User Management is enabled;” on p. 1-13 appears.

- Enter the User ID and password.

You can log in as the System Manager by entering the User ID registered as the System Manager in the [User ID] text box and its password in the [Password] text box.

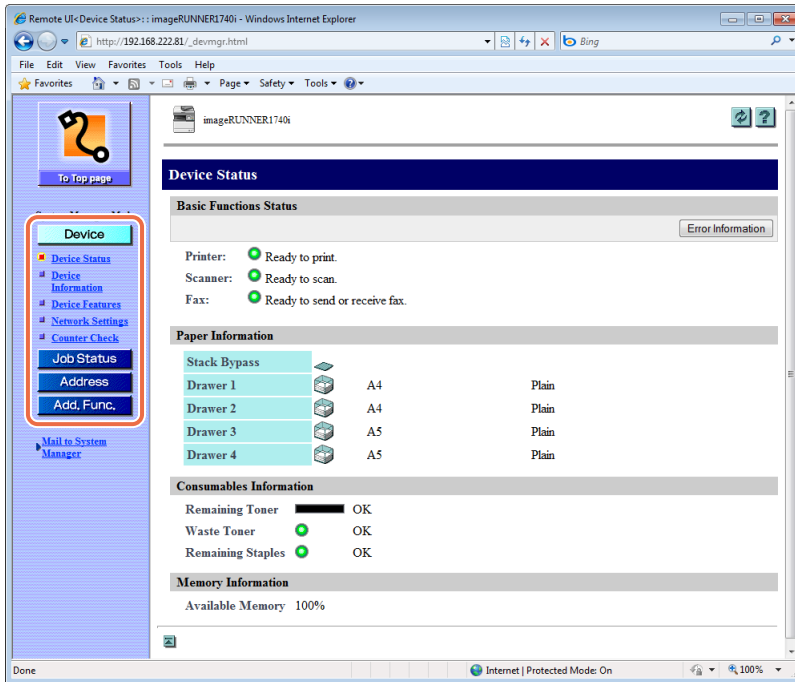
4 Click [OK].

The Device Status page appears. (See “Viewing the Machine Status and Information,” on p. 1-14.)

Viewing the Machine Status and Information

When you successfully log in to the Remote UI, the Device Status page in the [Device] menu is displayed. From the [Device] menu, you can view the current status of the machine, information about the consumables such as paper, and other information about the machine.

- 1 Click [Device] → click the hyperlink to the page you want to display in the [Device] menu.



The information page you selected is displayed.

The pages in the [Device] menu are as follows:

Device Status page:	Displays the machine status such as available memory, availability of consumables, and error information if any. To check the details of the error, click [Error Information].
Device Information page:	Displays the information about the machine, such as the system manager's information and the location where the machine is installed.
Device Features page:	Displays the information about the machine, such as the maximum print speed, the total RAM size, and the number of the drawers attached to the machine.
Network Settings page:	Displays the information about the machine's network settings.
Counter Check page:	Displays page counts such as the total counts and copy counts. The number and types of counters displayed may vary depending on the machine configuration.

Managing Jobs and Machine Data

2

CHAPTER

This chapter describes how to manage jobs, import/export data, and install key pairs and digital certificates by using the Remote UI.

Managing Jobs	2-2
Managing the Print Jobs	2-2
Viewing the Job Logs	2-4
Managing the Address Book	2-5
Editing the Destinations	2-6
Importing and Exporting Data	2-11
Exporting Address Book Data	2-12
Importing Address Book Data	2-13
Exporting User Management Data	2-14
Importing User Management Data	2-15
Resetting Imported User Management Data	2-17
Exporting Additional Functions Setting Data	2-21
Importing Additional Functions Setting Data	2-23
Managing Key Pairs and Digital Certificates from a Web Browser	2-25
Installing and Registering a Key and Certificate	2-26
Deleting a Key and Certificate	2-30
Installing and Registering a CA Certificate	2-32
Deleting a CA Certificate	2-35

Managing Jobs

You can manage the print jobs and view the logs of the jobs processed by the machine. The [Job Status] menu has the following sections:

- Print Job
 - Status
 - Log
- Send/Receive Fax Job
 - Log
- Send/Store/Receive Job
 - Log

Managing the Print Jobs

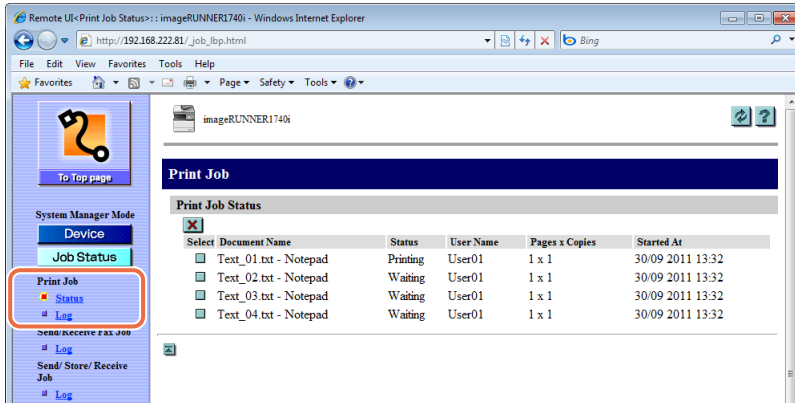
You can manage the print jobs that are being processed or waiting to be processed by the machine.



NOTE

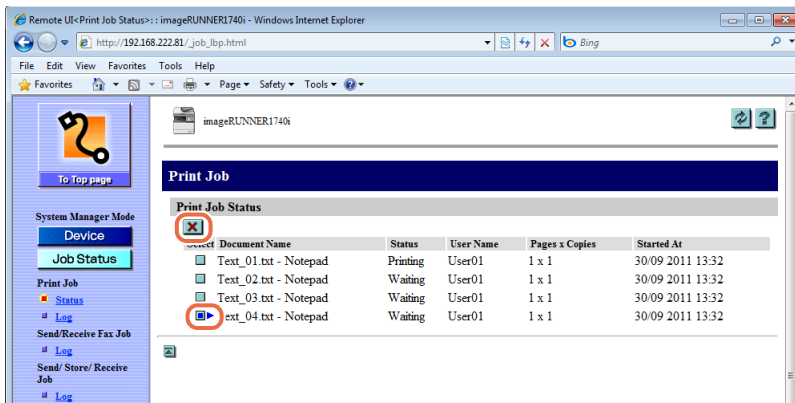
End Users can delete their own print jobs, when the Permit End-user's Job Operation setting is enabled. (See "To specify the System Manager ID and System Password:" on p. 4-9.)

1 Click [Job Status] → [Status] in the [Job Status] menu.



The list of print jobs being processed or waiting to be processed by the machine is displayed.

2 To delete a print job, click [] (Select) next to the job you want to delete → [X] (Delete).



The selected job is deleted.

Viewing the Job Logs

You can view the logs of the jobs processed by the machine. The maximum numbers of the logs displayed are as follows:

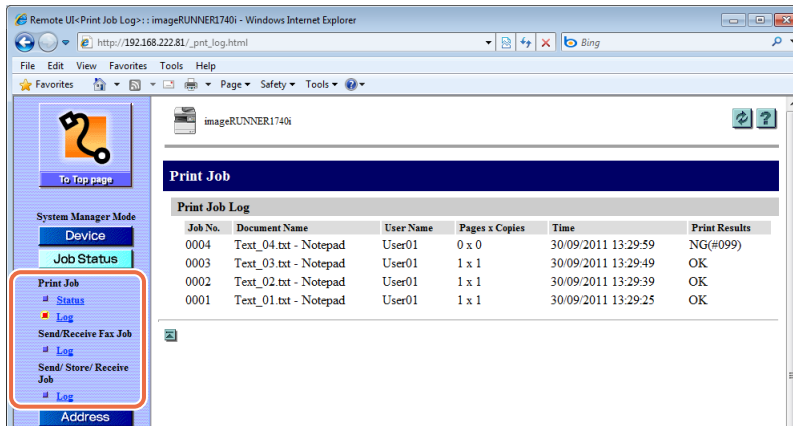
- Print Job Log: the last 128 jobs
- Send/Receive Fax Job Log: the last 45 jobs
- Send/Store/Receive Job Log: the last 128 jobs



IMPORTANT

The Job Logs are displayed only when the Job Log Display setting in the Edit System Settings page is enabled. (See “Customizing the System Settings,” on p. 4-2.)

- 1 Click [Job Status] → [Log] you want to view in the [Job Status] menu.



The screen shot above shows the screen displayed when you select the [Log] of the <Print Job>.

The Print Job page shows a list of the jobs that have already been processed by the machine.

Managing the Address Book

You can manage the Address Book data on the Remote UI as well as on the machine's control panel. The types of addresses are as follows:

■ E-mail Address

You can manage e-mail addresses.

■ I-fax Address

You can manage I-fax addresses.

■ File Server Address

You can manage file server addresses with the information to save scanned documents in a file server, such as the protocol and path name of the destination folder.

■ Fax Number

You can manage fax numbers.

■ Group Address

You can manage group addresses, which enable you to include multiple addresses in a single group.

NOTE

For instructions on how to manage the Address Book on the machine's control panel, see Chapter 4, "Specifying Destinations Easily and Quickly," in the *Sending and Facsimile Guide*.

Editing the Destinations

You can register, edit, or delete the destinations in the Address Book.

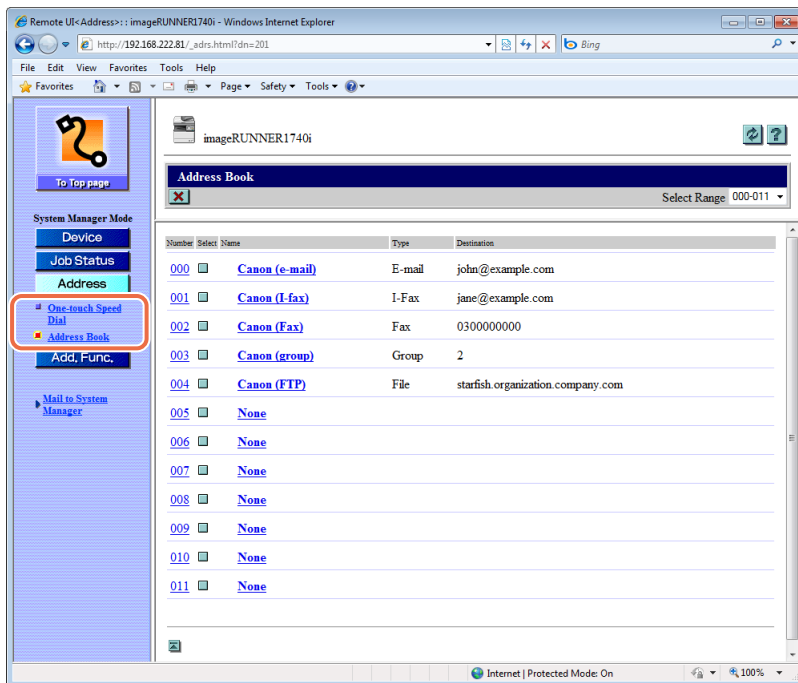
NOTE

The screen shots and procedures in this section are for the Address Book. The Address Book and One-touch Speed Dial use a similar procedure for editing destinations.

2

Managing Jobs and Machine Data

- 1 Click [Address] → [One-touch Speed Dial] or [Address Book] from the menu displayed under [Address].



If the address book is protected by a password, the Enter password page appears. Enter the password → click [OK].

The Address Book page is displayed.

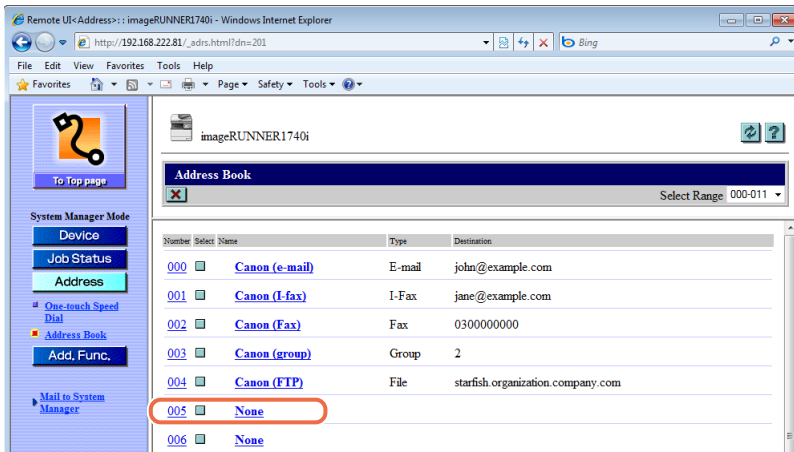
NOTE

You can select the address numbers to display from the [Select Range] drop-down list box.

2 Edit the destinations.

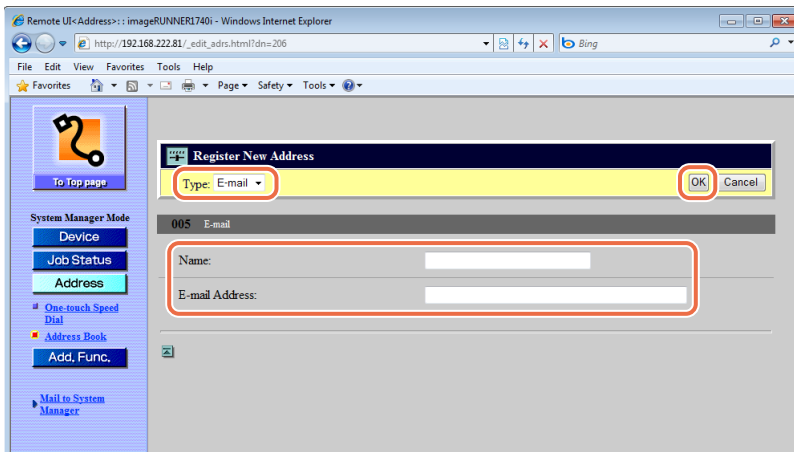
● To register a new destination:

- ❑ Click [None] or any number for which [None] is displayed.



The Register New Address page is displayed.

- ❑ Select the type of the address from the [Type] drop-down list box → specify the necessary settings depending on the type of address you selected → click [OK].



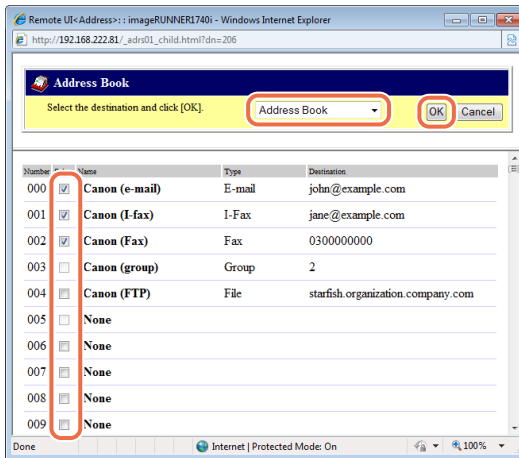
The new address is registered in the machine, and the page returns to the Address Book page.

NOTE

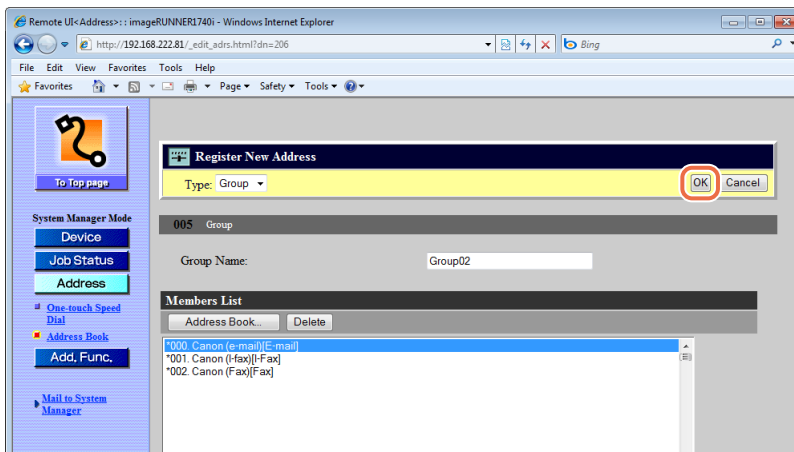
For more information on the address types, see Chapter 4, “Specifying Destinations Easily and Quickly,” in the *Sending and Facsimile Guide*.

● **To register a new group address:**

- Click [None] or any number for which [None] is displayed on the page shown in step 1.
The Register New Address page is displayed.
- Select <Group> from the [Type] drop-down list box.
- Enter the name for the group in the [Group Name] text box.
- Click [Address Book].
The list of addresses registered in the machine is displayed in the new window.
- Specify the type of address from the drop-down list box.
- Select the check boxes next to the addresses you want to include to the group → click [OK].



The selected addresses are displayed in the [Members List].



- Make sure that the addresses you want to add to the group are displayed in the Members List field → click [OK].

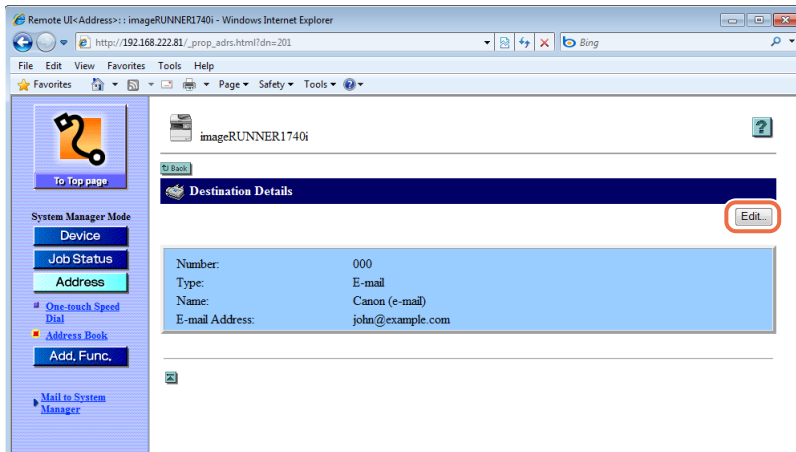
The new group address is registered and the page returns to the Address Book page.

● **To edit the details of the destination:**

- Click the name or any number next to the name on the Address Book page shown in step 1.

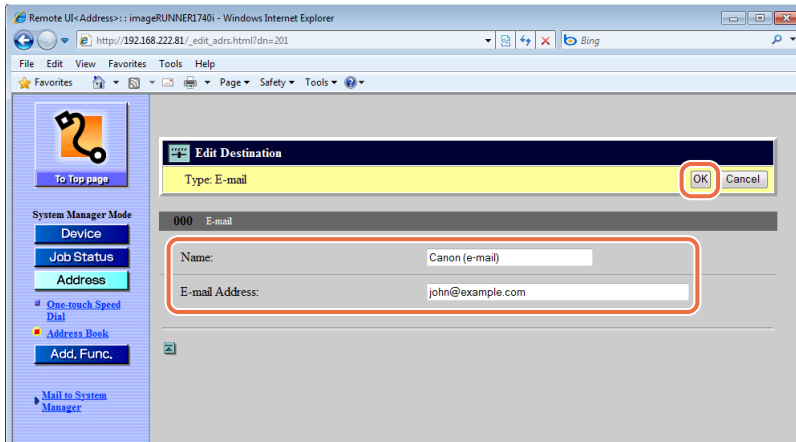
The Destination Details page appears.

- Click [Edit].



The Edit Destination page is displayed.

- ❑ Edit the settings as necessary → click [OK].



The page returns to the Address Book page.

- **To delete the destination:**

- ❑ On the Address Book page shown in step 1, click [] (Select) next to the address you want to delete → [] (Delete).

The selected destination is deleted.

Importing and Exporting Data

You can save (export) setting information such as the Address Book and Additional Functions setting data as a file. You can store the exported file as a backup and load (import) the data into the machine when necessary.



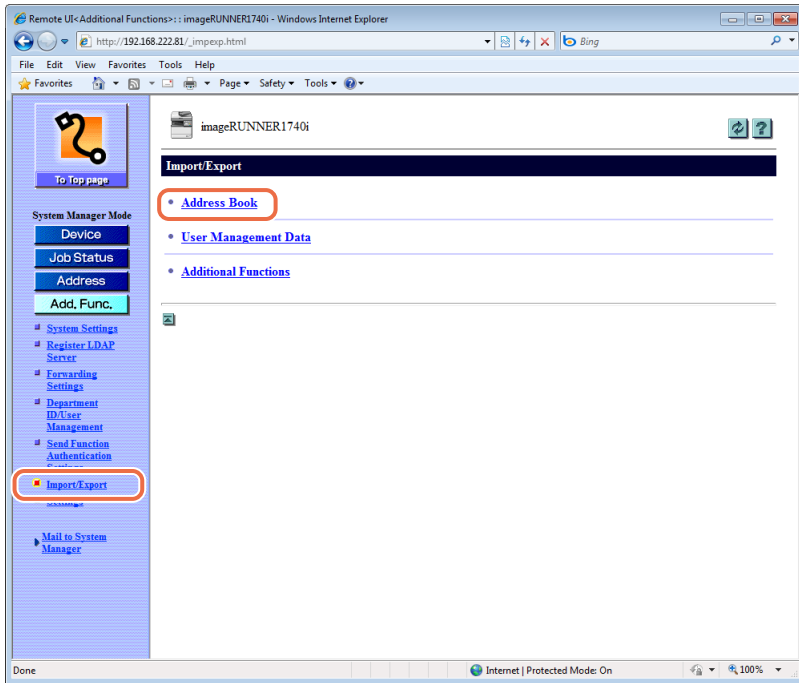
IMPORTANT

- The importing/exporting operation may take a few minutes to complete. Do not turn the machine's main power OFF until the operation is complete. Otherwise, the machine may malfunction.
- During an exporting operation, the page does not change until the operation is complete. Do not click [Start Export] while the computer indicates that the operation is still being processed.
- The Import/Export function is available only when the Remote UI is in the System Manager Mode.
- The importing/exporting operation is performed based on the language displayed on the touch panel display of the machine. For example, if the language displayed on the touch panel display and the language of the Address Book data to import do not match, the importing operation cannot be properly performed.

Exporting Address Book Data

You can save (export) the Address Book data stored in the machine as a file.

1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

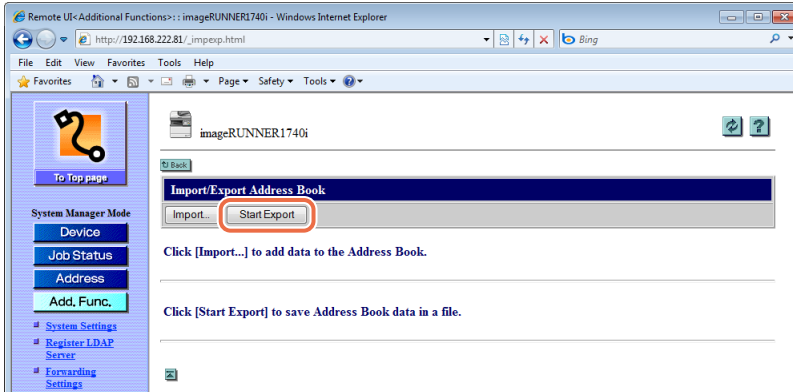


The Import/Export page is displayed.

2 Click [Address Book] on the page shown in step 1.

The Import/Export Address Book page is displayed.

3 Click [Start Export].



4 Follow the instructions on the computer screen to specify the location to save the file.

The file is saved in the specified location.

Importing Address Book Data

You can load (import) the Address Book data into the machine from a saved (exported) file.

IMPORTANT

- When you load (import) the Address Book data, the addresses registered in the machine are overwritten by the new data.
- The machine imports/exports the Address Book data based on the index numbers displayed on the address list on the Address Book page on the Remote UI. An address entry is overwritten if the imported Address Book data contains an address entry with the same index number.
- Do not load the Address Book when the machine has Delayed Send jobs.
- If the machine is in the Sleep mode, press the machine's control panel power switch to clear the Sleep mode before performing an Import operation.

1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in "Exporting Address Book Data," on p. 2-12.

The Import/Export page is displayed.

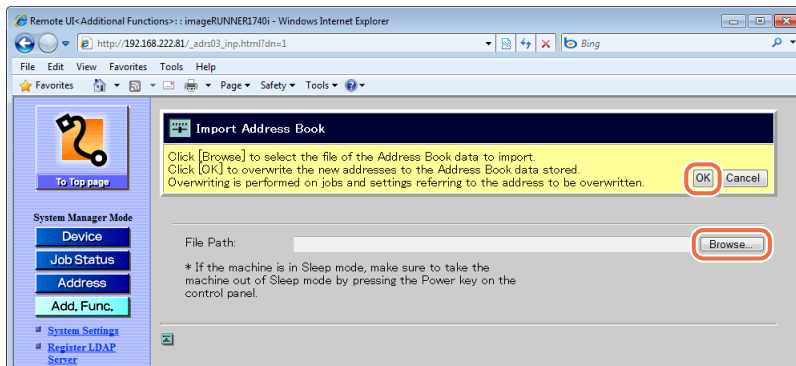
2 Click [Address Book].

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.
The Import/Export Address Book page is displayed.

3 Click [Import].

For help, see the screen shot in step 3 in “Exporting Address Book Data,” on p. 2-12.
The Import Address Book page is displayed.

4 Click [Browse] → select the file to import → click [OK].



The Remote UI starts importing the data and when it is complete, the page returns to the Import/Export Address Book page.



IMPORTANT

Do not import any files while the machine is processing other jobs.

Exporting User Management Data

You can save (export) the User Management data stored in the machine as a file.



IMPORTANT

All the User IDs are exported as ‘User’ (End User).

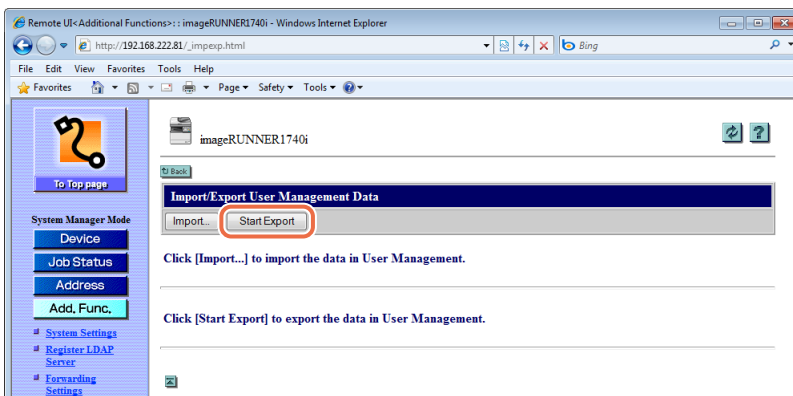
1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.
The Import/Export page is displayed.

2 Click [User Management Data].

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12. The Import/Export User Management Data page is displayed.

3 Click [Start Export].



4 Follow the instructions on the computer screen to specify the location to save the file.

The file is saved in the specified location.

Importing User Management Data

You can load (import) the User Management data into the machine from a saved (exported) file.

IMPORTANT

- Be sure to disable the Department ID Management and User Management before importing the User Management data. (See “Enabling Department ID Management and User Management,” on p. 3-2.)
- All the User IDs are registered or overwritten as ‘User’ (End User) when the machine imports the User ID data and their passwords are cleared. You must reset the passwords for the User IDs and for Department IDs each User ID belongs to after importing. (See “Resetting Imported User Management Data,” on p. 2-17.)
- If the machine is in the Sleep mode, press the machine’s control panel power switch to clear the Sleep mode before importing the data.

1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.
The Import/Export page is displayed.

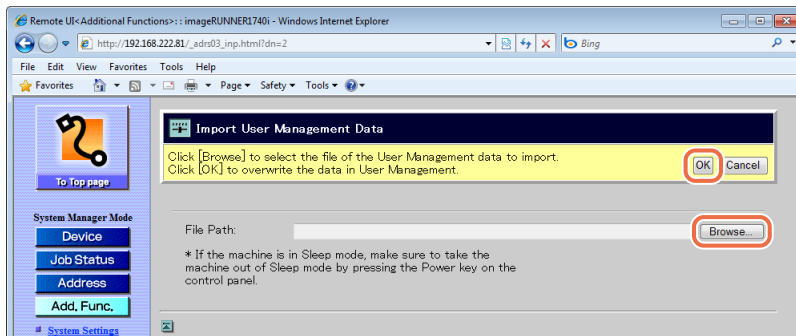
2 Click [User Management Data].

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.
The Import/Export User Management Data page is displayed.

3 Click [Import].

For help, see the screen shot in step 3 in “Exporting User Management Data,” on p. 2-14.
The Import User Management Data page is displayed.

4 Click [Browse] → select the file to import → click [OK].



The Remote UI starts importing the data and when it is complete, the page returns to the Import/Export User Management Data page.



IMPORTANT

Do not import any files while the machine is processing jobs.

Resetting Imported User Management Data

For security reasons, the loaded (imported) User Management data does not contain the passwords for User IDs and for Department IDs each User ID belongs to. You must follow the procedure below to reset the passwords after loading (importing) the User Management data.



IMPORTANT

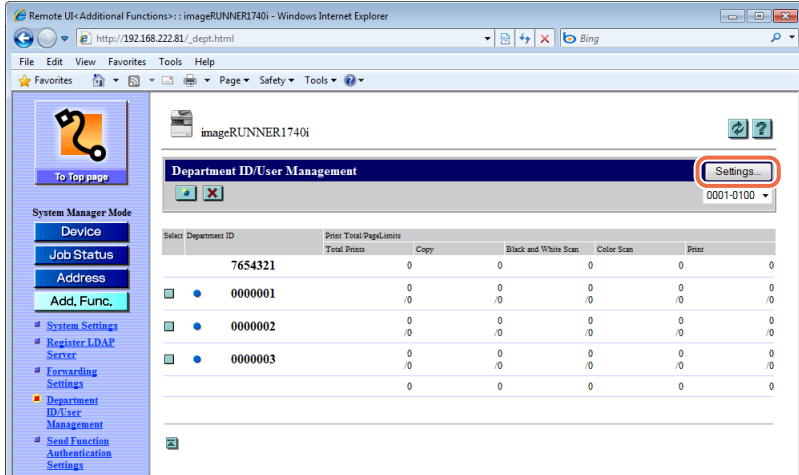
- Before you enable Department ID Management and User Management, be sure to reset the passwords for User IDs as directed in the procedure below.
- To reset the passwords, log in to the Remote UI in the System Manager mode. (See “When Department ID Management and User Management are disabled:,” on p. 1-10.)

- 1 Click [Add.Func.] → [Department ID/User Management] in the [Add.Func.] menu.

Select	Department ID	Print Total Page Limits Total Prints	Copy	Black and White Scan	Color Scan	Print
	7654321	0	0	0	0	0
<input type="checkbox"/>	0000001	0 /0	0 /0	0 /0	0 /0	0 /0
<input type="checkbox"/>	0000002	0 /0	0 /0	0 /0	0 /0	0 /0
<input type="checkbox"/>	0000003	0 /0	0 /0	0 /0	0 /0	0 /0

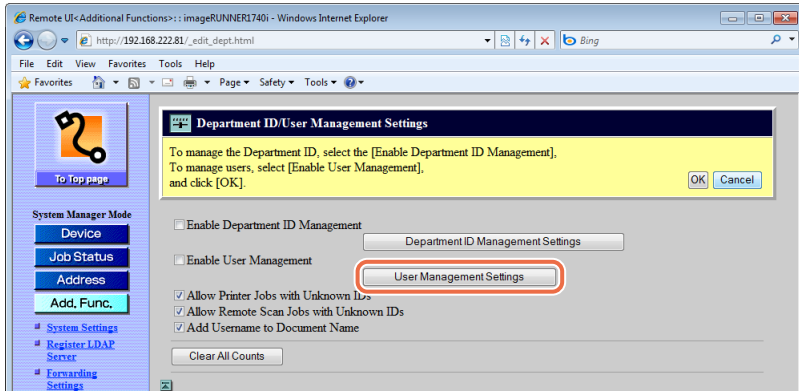
The [Department ID/User Management] page is displayed.

2 Click [Settings].



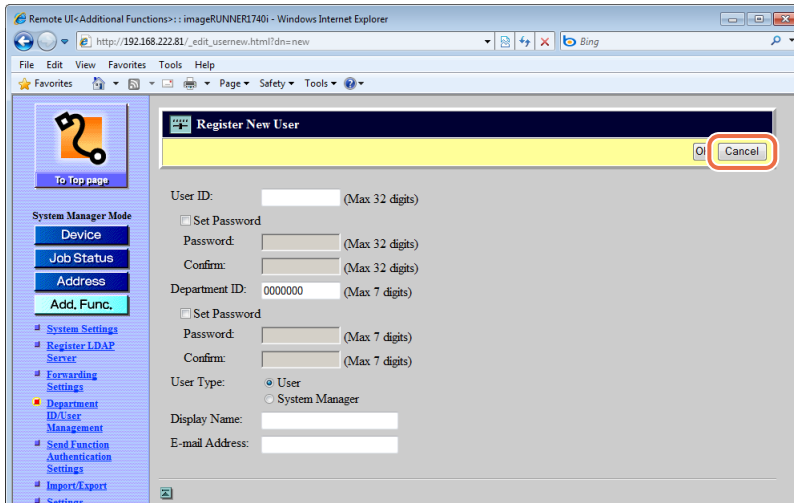
The [Department ID/User Management Settings] page is displayed.

3 Click [User Management Settings].



The [Register New User] page is displayed.

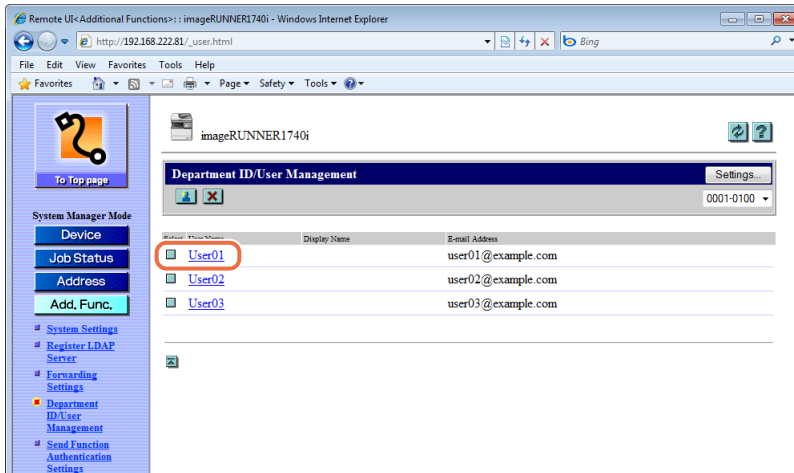
4 Click [Cancel] on the [Register New User] page.



Specifying the new user information is not required in this step.

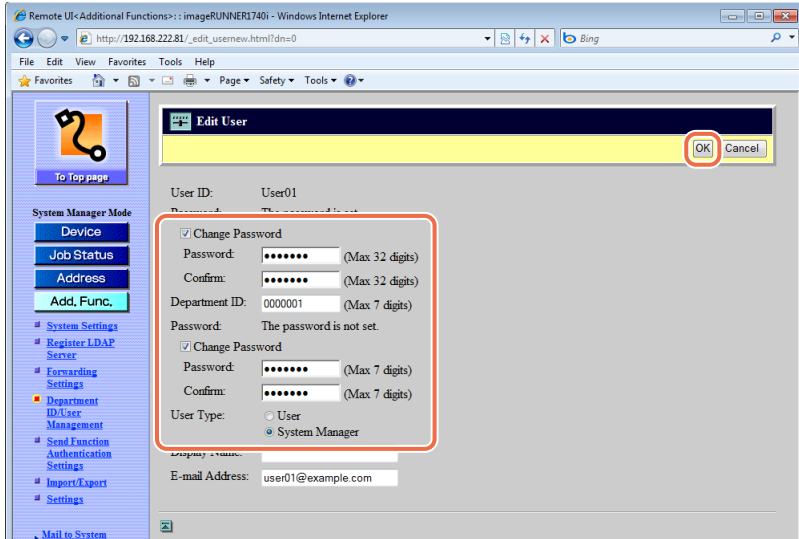
The User IDs registered in the machine are displayed.

5 Click the User ID to reset the passwords.



The [Edit User] page is displayed.

6 Reset the passwords → click [OK].



Change Password: Select this check box and enter the password for the User ID in (for the User ID) the [Password] and [Confirm] text box.

NOTE

You can enter the new password for the User ID instead of entering the old (before importing) password.

Change Password: Select this check box and enter the password for the (for the Department ID) Department ID the User ID belongs to in the [Password] and [Confirm] text box.

User Type: Specify the User Type by selecting the [User] (End User) or [System Manager] option button.

IMPORTANT

All the User IDs are registered or overwritten as 'User' (End User) when the machine imports User Management data, so you may need to reset the User Types. If the User Types of all the User IDs are set to 'User' (End User), every user is regarded as the System Manager and will be able to log in to the machine and the Remote UI in the System Manager Mode.

7 Repeat steps 5 and 6 to reset the passwords of the other User IDs.

8 Enable Department ID Management and/or User Management as necessary after resetting the passwords for all the User IDs.

For more information, see “Enabling Department ID Management and User Management,” on p. 3-2.

 **NOTE**

To switch from the User ID list to the Department ID list, click [Department ID Management Settings] on the [Department ID/User Management Settings] page shown in step 3, and click [Cancel] on the [Register New Department] page. To display the list of the User IDs again, follow steps 1 to 4.

Exporting Additional Functions Setting Data

You can save (export) the Additional Functions setting data stored in the machine as a file.

 **NOTE**

The Additional Functions settings you can export are displayed on the page shown in step 3.

1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.

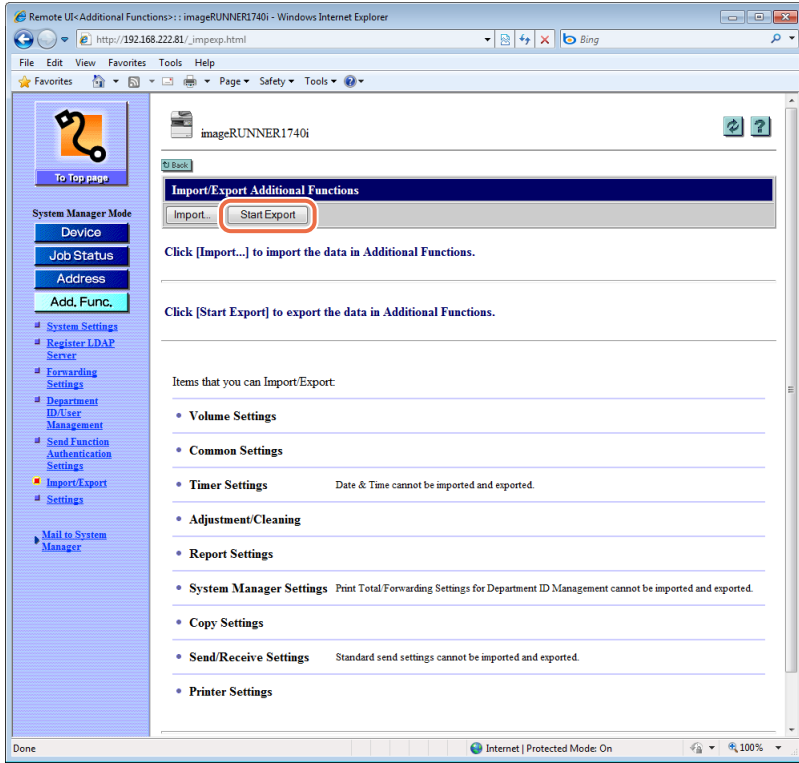
The Import/Export page is displayed.

2 Click [Additional Functions].

For help, see the screen shot in step 1 in “Exporting Address Book Data,” on p. 2-12.

The Import/Export Additional Functions page including the list of the Additional Functions settings to be exported is displayed.

3 Click [Start Export].



4 Follow the instructions on the computer screen to specify the location to save the file.

The file is saved in the specified location.

Importing Additional Functions Setting Data

You can load (import) the Additional Functions setting data into the machine from a saved (exported) file.



IMPORTANT

If the machine is in the Sleep mode, press the machine's control panel power switch to clear the Sleep mode before performing an Import operation.



NOTE

The Additional Functions settings you can import are displayed on the page shown in step 3 in "Exporting Additional Functions Setting Data," on p. 2-21.

1 Click [Add.Func.] → [Import/Export] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in "Exporting Address Book Data," on p. 2-12.

The Import/Export page is displayed.

2 Click [Additional Functions].

For help, see the screen shot in step 1 in "Exporting Address Book Data," on p. 2-12.

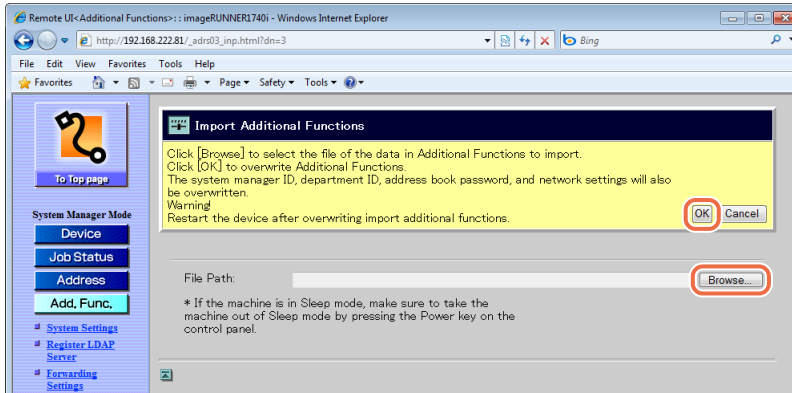
The Import/Export Additional Functions page including the list of the Additional Functions settings to be imported is displayed.

3 Click [Import].

For help, see the screen shot in step 3 in "Exporting Additional Functions Setting Data," on p. 2-21.

The Import Additional Functions page is displayed.

4 Click [Browse] → select the file to import → click [OK].



The Remote UI starts importing the data and when it is complete, the page returns to the Import/Export Additional Functions page.



IMPORTANT

Do not import any files while the machine is processing other jobs.

5

Restart the machine to enable the imported settings.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.



IMPORTANT

- When Additional Functions settings data is imported, the System Manager ID, Department IDs, Address Book password, and network settings are automatically overwritten.
- The Remote UI cannot be used to perform other operations until the machine is restarted.
- Do not import any files while the machine is processing other jobs.

Managing Key Pairs and Digital Certificates from a Web Browser

Key pairs and digital certificates can be used for security purposes, such as IEEE802.1X port-based authentication and SSL communication.

You can manage key pairs and digital certificates from the Remote UI by dividing them into the following types:

■ Key and Certificate

In IEEE802.1X port-based authentication, a key pair (or a private key and certificate) in PKCS#12 format is required for enabling the EAP-TLS method on the client device. If you want to access the machine securely from a web browser (Remote UI), generate a key pair and set it for SSL communications. Up to three key pairs can be registered.

■ CA Certificate

CA certificates are used for verifying the digital certificates sent from other devices, such as servers, client computers, etc. Up to 10 CA certificates (including the pre-installed CA certificates) can be registered.

This section focuses on how to install and register key pairs and digital certificates from a computer on the network. For instructions on how to generate a key pair for SSL communications, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.



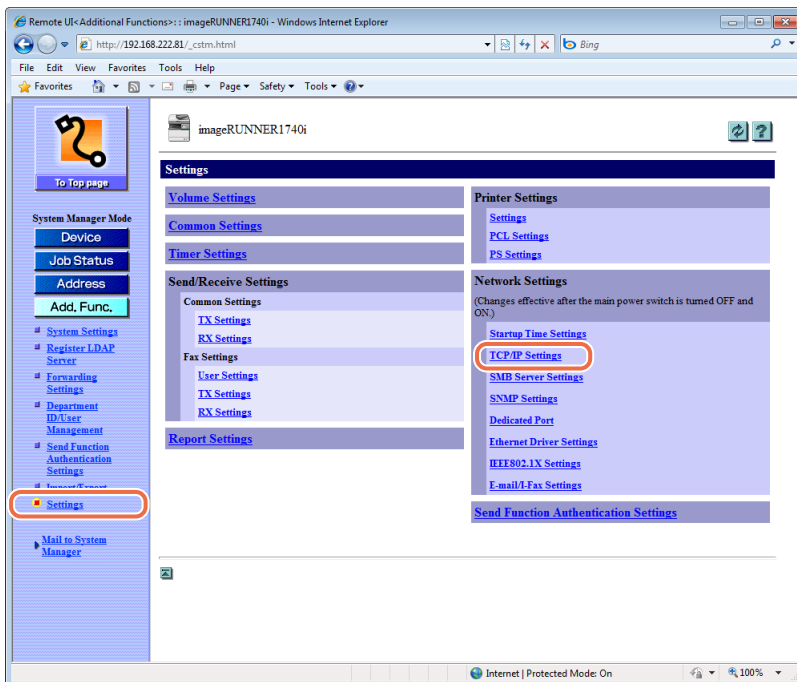
IMPORTANT

- Certificates must meet the following requirements:
 - Format: X.509 version 1 or version 3 (DER encoded binary)
 - Signature algorithm: SHA1-RSA, SHA256-RSA, SHA384-RSA*, SHA512-RSA*, MD5-RSA, or MD2-RSA (For CA certificates, SHA1-DSA is also allowed.)
 - Key length: 512, 1024, 2048, or 4096 bits (RSA)/2048 or 3072 bits (DSA)
 - File extension: ‘.p12’ or ‘.pfx’ (for key pair files)/‘.cer’ or ‘.der’ (for CA certificate files)
 - * SHA384-RSA and SHA512-RSA are supported only when the key length is 1024 bits or more.
- The machine does not use certificate revocation list (CRL) for verifying digital certificates.
- The Certificate Settings are available only when the Remote UI is in the System Manager Mode.

Installing and Registering a Key and Certificate

Install a key pair (or a private key and certificate) in the machine as described below. You can also register the key pair or delete unnecessary key pair files.

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

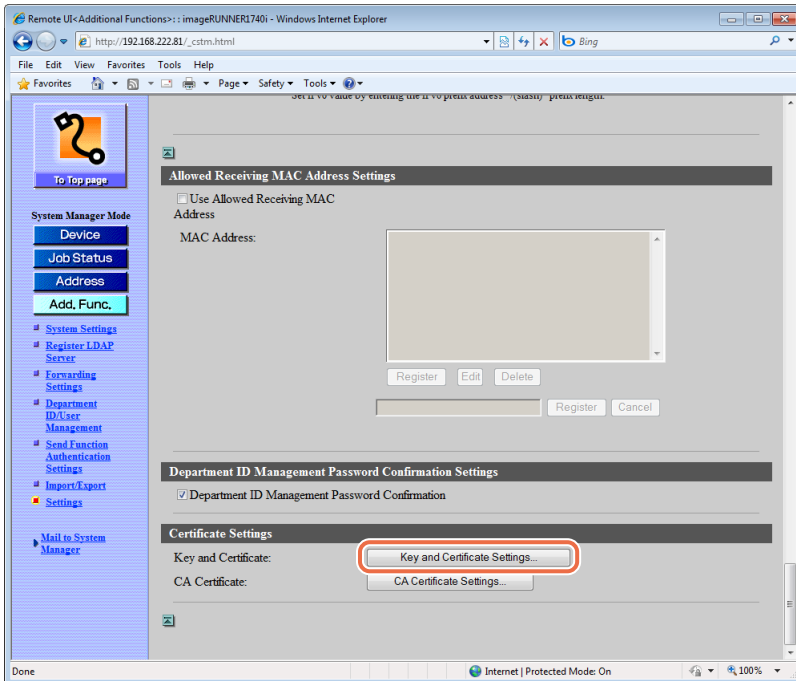


The Settings page is displayed.

2 Click [TCP/IP Settings] on the page shown in step 1.

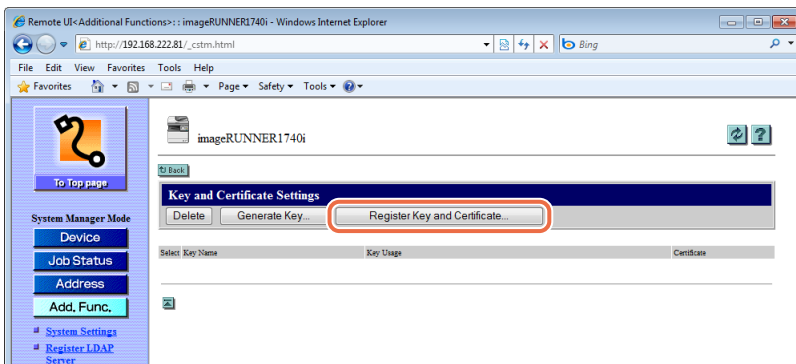
The TCP/IP Settings page is displayed.

3 Scroll the page until [Certificate Settings] appears → click [Key and Certificate Settings].



The Key and Certificate Settings page is displayed.

4 Click [Register Key and Certificate].



The Register Key and Certificate page is displayed.

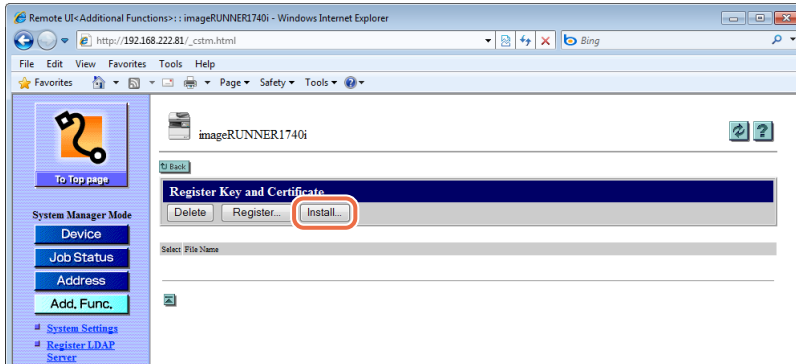
NOTE

If you want to generate an SSL key pair with the machine, click [Generate Key] → enter the required information on the page that appears → click [OK]. For more information, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.

5 Select the function.

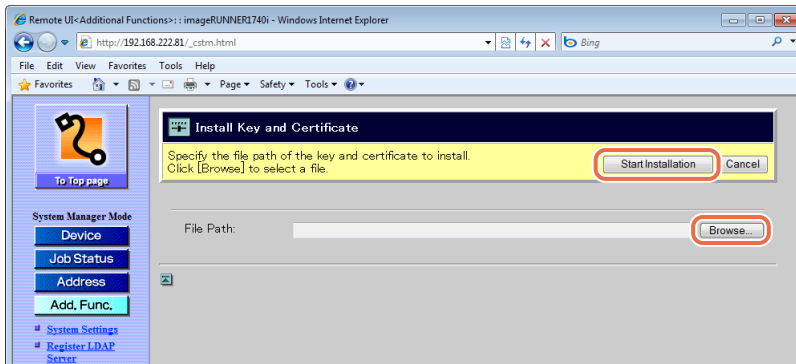
● To install a new key and certificate:

- Click [Install].



The Install Key and Certificate page is displayed.

- Click [Browse] → select the key pair file to install → click [Start Installation].



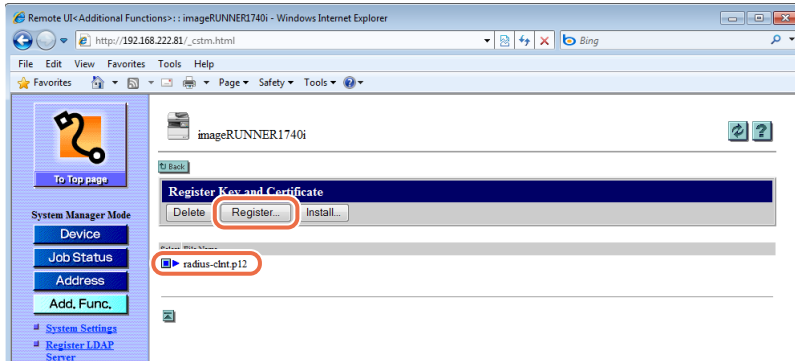
The Remote UI starts installing the key and certificate and when it is complete, the page returns to the Register Key and Certificate page.

IMPORTANT

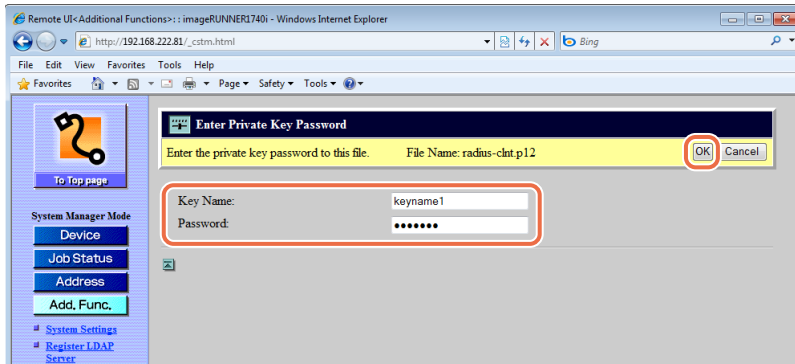
The maximum number of characters that you can enter for the file name is 24 (including the file extension ‘.p12’ or ‘.pfx’).

- **To register the key and certificate:**

- Click (Select) next to the key pair file you want to register → [Register].




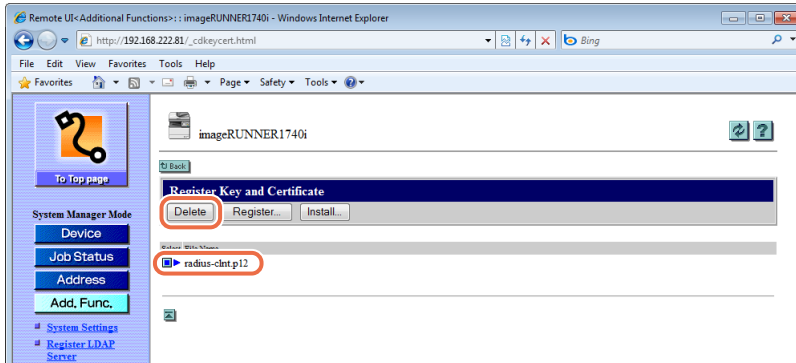
- Enter the key name and password (up to 24 characters respectively) → click [OK].



The Remote UI starts registering the key and certificate and when it is complete, the page returns to the Register Key and Certificate page.

- **To delete the installed (but not registered) key and certificate:**

- Click [] (Select) next to the file you want to delete → [Delete].



The selected file is deleted.

6 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

Deleting a Key and Certificate

Key pairs become invalid when the certificate expires or when the file becomes corrupted. If this happens, delete unnecessary key pair files as described below.

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in "Installing and Registering a Key and Certificate," on p. 2-26.

The Settings page is displayed.

2 Click [TCP/IP Settings] on the page shown in step 1.

For help, see the screen shot in step 1 in "Installing and Registering a Key and Certificate," on p. 2-26.

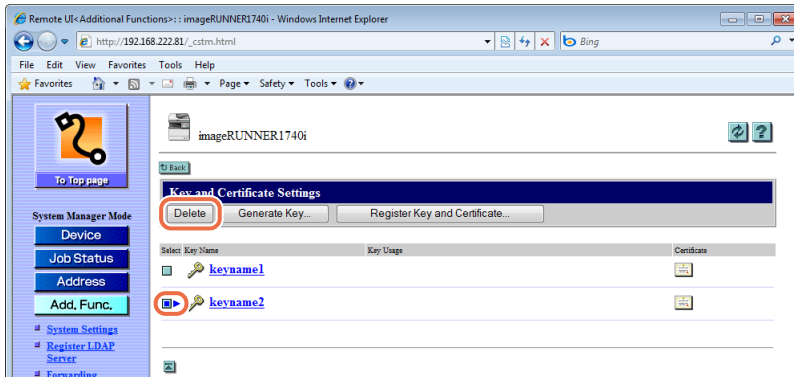
The TCP/IP Settings page is displayed.

3 Scroll the page until [Certificate Settings] appears → click [Key and Certificate Settings].

For help, see the screen shot in step 3 in “Installing and Registering a Key and Certificate,” on p. 2-26.

The Key and Certificate Settings page is displayed.

4 Click [] (Select) next to the key pair you want to delete → [Delete].



The selected key pair is deleted.

NOTE

- If you want to display the details of a certificate, click [] (Certificate).
- You may not be able to delete a key pair. In this case, check what the key pair is being used for (indicated under <Key Usage>) and perform the following:
 - If the key pair is used for SSL, disable the SSL settings for e-mails/I-faxes and the Remote UI. (See Chapter 3, “Setting up the Machine for Your Network Environment,” and Chapter 6, “Protecting the Machine from Unauthorized Access,” in the *System Settings Guide*.)
 - If the key pair is used for IEEE802.1X authentication, register a new key pair and set it as the default key. (See Chapter 2, “Connecting the Machine to a TCP/IP Network,” in the *System Settings Guide*.) The key pair reset to ‘Off’ can be deleted.

5 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

Installing and Registering a CA Certificate

Install a CA certificate in the machine as described below. You can also register the CA certificate or delete unnecessary certificate files.

2

Managing Jobs and Machine Data

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Installing and Registering a Key and Certificate,” on p. 2-26.

The Settings page is displayed.

2 Click [TCP/IP Settings] on the page shown in step 1.

For help, see the screen shot in step 1 in “Installing and Registering a Key and Certificate,” on p. 2-26.

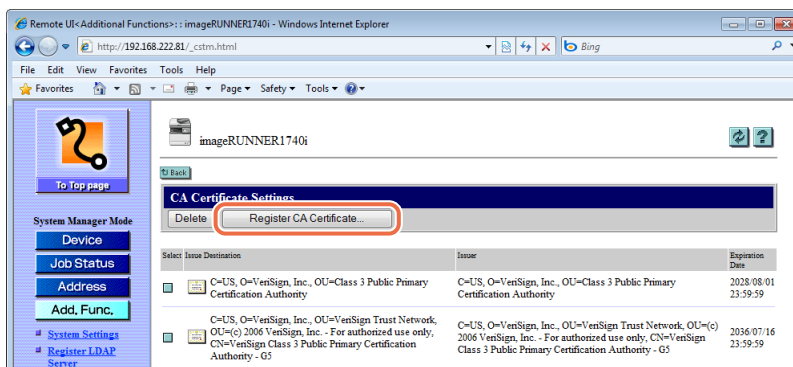
The TCP/IP Settings page is displayed.

3 Scroll the page until [Certificate Settings] appears → click [CA Certificate Settings].

For help, see the screen shot in step 3 in “Installing and Registering a Key and Certificate,” on p. 2-26.

The CA Certificate Settings page is displayed.

4 Click [Register CA Certificate].

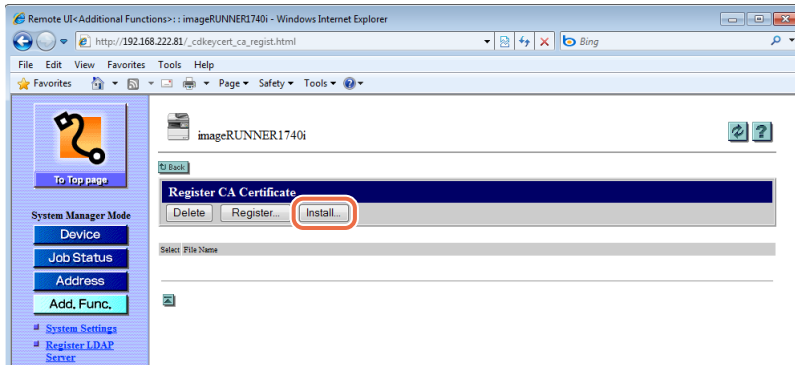


The Register CA Certificate page is displayed.

5 Select the function.

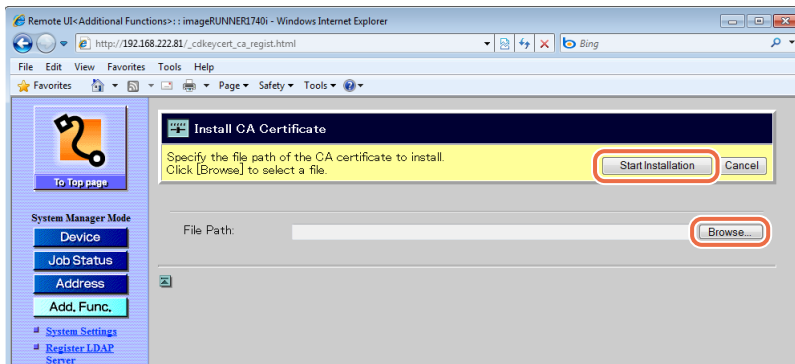
● To install a new CA certificate:

- Click [Install].



The Install CA Certificate page is displayed.

- Click [Browse] → select the CA certificate file to install → click [Start Installation].



The Remote UI starts installing the CA certificate and when it is complete, the page returns to the Register CA Certificate page.

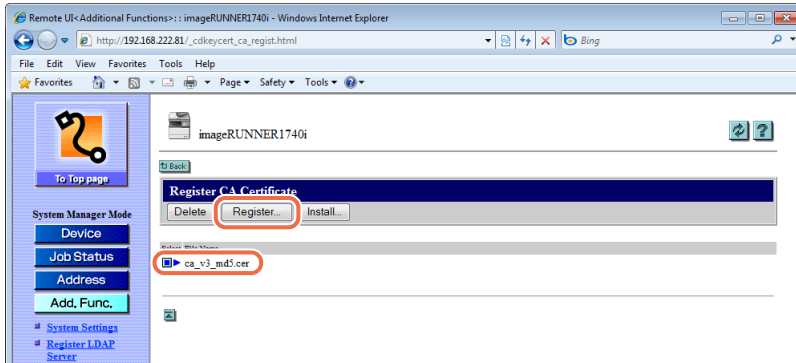


IMPORTANT

The maximum number of characters that you can enter for the file name is 24 (including the file extension '.cer' or '.der').


● **To register the CA certificate:**

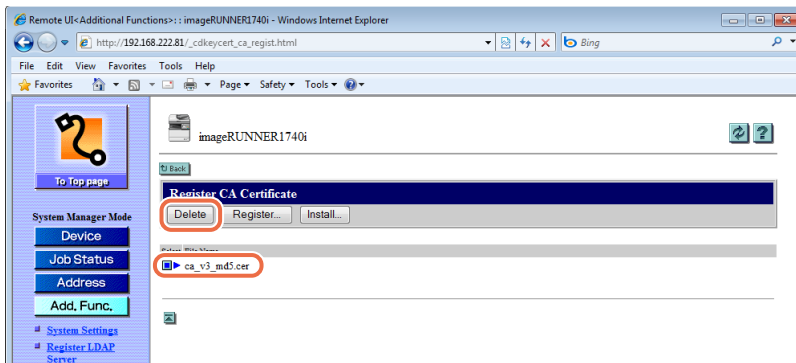
- ❑ Click [] (Select) next to the CA certificate file you want to register → [Register].



The Remote UI starts registering the CA certificate and when it is complete, the page returns to the CA Certificate Settings page.

● **To delete the installed (but not registered) CA certificate:**

- ❑ Click [] (Select) next to the file you want to delete → [Delete].



The selected file is deleted.

6 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

Deleting a CA Certificate

CA certificates become invalid when the certificate expires or when the file becomes corrupted. If this happens, delete unnecessary files as described below.

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Installing and Registering a Key and Certificate,” on p. 2-26.

The Settings page is displayed.

2 Click [TCP/IP Settings] on the page shown in step 1.

For help, see the screen shot in step 1 in “Installing and Registering a Key and Certificate,” on p. 2-26.

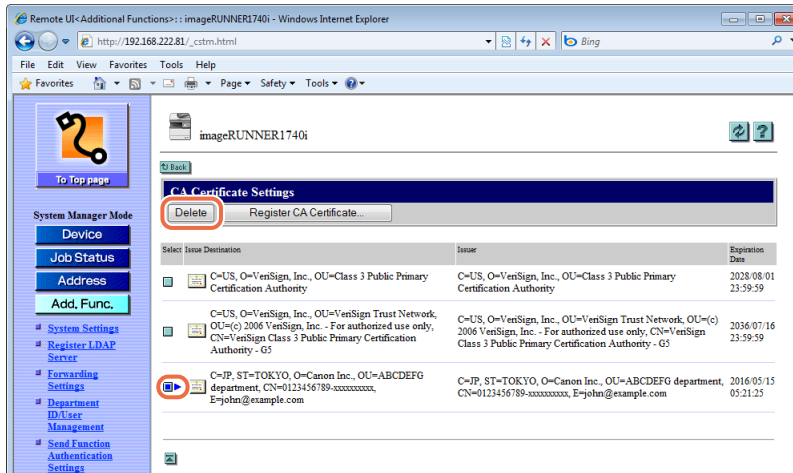
The TCP/IP Settings page is displayed.

3 Scroll the page until [Certificate Settings] appears → click [CA Certificate Settings].

For help, see the screen shot in step 3 in “Installing and Registering a Key and Certificate,” on p. 2-26.


The CA Certificate Settings page is displayed.

4 Click [] (Select) next to the CA certificate you want to delete → [Delete].



The selected CA certificate is deleted.

NOTE

If you want to display the details of a certificate, click [] (Certificate).

5 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

Specifying Department ID and User Management

3

CHAPTER

This chapter describes how to specify the Department ID Management and User Management settings by using the Remote UI.

Managing the Department IDs and User IDs	3-2
Enabling Department ID Management and User Management.	3-2
Managing the Department IDs.	3-6
Managing the User IDs	3-10

Managing the Department IDs and User IDs

You can specify the Department ID Management and User Management settings on the Remote UI.

IMPORTANT

- Be sure to disable User Management when the optional Copy Card Reader-F1 is attached to the machine.
- Specifying the Department ID Management and User Management settings are available only when the Remote UI is in the System Manager Mode.

Enabling Department ID Management and User Management

You can enable either or both the Department ID management and User Management, depending on your needs.

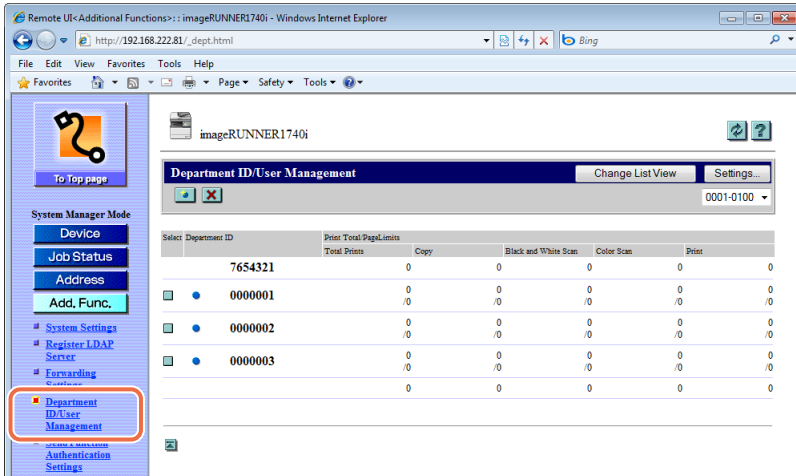
IMPORTANT

- Be sure to confirm the System Manager ID and System Password are properly set to log in to the Remote UI in the System Manager Mode before enabling Department ID Management. (See “To specify the System Manager ID and System Password;” on p. 4-9.)
- Before enabling Department ID/User Management, register at least one Department ID/User ID beforehand. (See “Managing the Department IDs,” on p. 3-6 and “Managing the User IDs,” on p. 3-10.)
- First register a User ID as the System Manager, and then register other User IDs as the End Users before enabling User Management. (See “To register a new User ID;” on p. 3-10.)

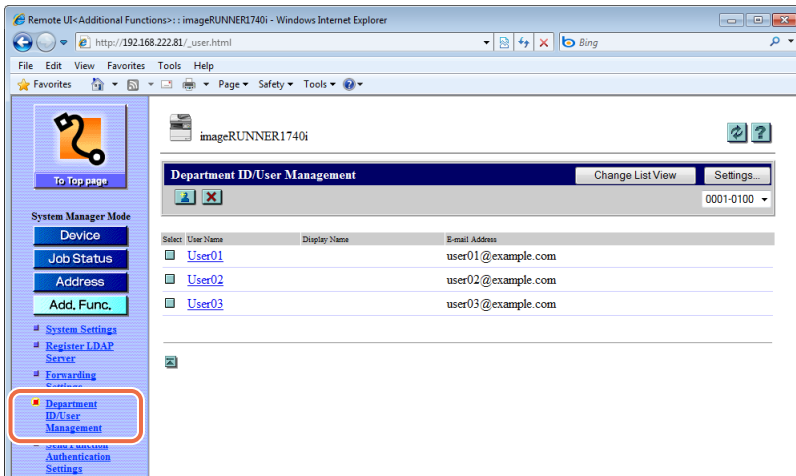
1 Click [Add.Func.] → [Department ID/User Management] in the [Add.Func.] menu.

NOTE

The list of the Department IDs switches to the list of the User IDs by clicking [Change List View]. The [Change List View] button appears when both Department ID Management and User Management are enabled and at least one ID is registered for each mode.



The page above displays the list of the Department IDs.

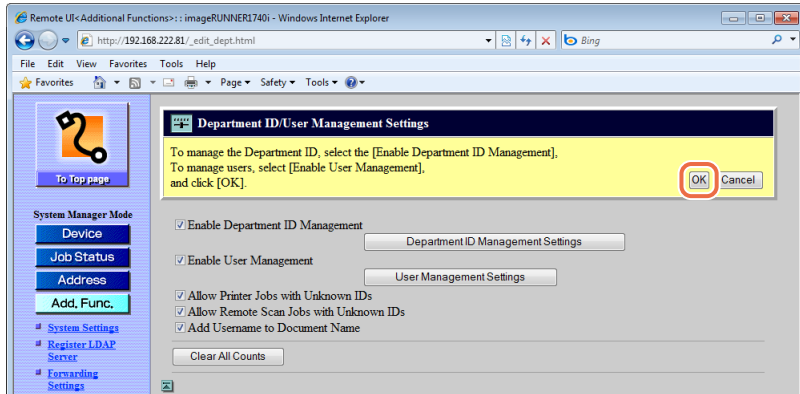


The page above displays the list of the User IDs.

2 Click [Settings] on the page shown in step 1.

The Department ID/User Management Settings page appears.

3 Select the [Enable Department ID Management] and/or [Enable User Management] check box, and specify the necessary settings → click [OK].



The settings are as follows:

Enable Department ID Management: Select this check box to enable Department ID Management. When it is enabled, the users must enter their Department ID and password (when it is set) to log in to the machine and the Remote UI.

IMPORTANT

Before selecting this check box, make sure that at least one Department ID is registered.

Department ID Management Settings: Click this button to register a Department ID. (See “Managing the Department IDs,” on p. 3-6.)

Enable User Management: Select this check box to enable User Management. When it is enabled, the users must enter their User ID and password (when it is set) to log in to the machine and the Remote UI.

IMPORTANT

Before selecting this check box, make sure that at least one User ID is registered.

User Management Settings:	Click this button to register a User ID. (See “Managing the User IDs,” on p. 3-10.)
Allow Printer Jobs with Unknown IDs:	Select this check box to allow the machine to accept print jobs from unknown IDs.
Allow Remote Scan Jobs with Unknown IDs:	Select this check box to allow the machine to accept remote scan jobs from unknown IDs.
Add Username to Document Name:	Select this check box to add the User ID to the name of the sent document.
Clear All Counts:	Click this button to reset the counters to zero for all Department IDs.



NOTE

For instructions on how to specify the settings above on the machine’s control panel, see Chapter 6, “Protecting the Machine from Unauthorized Access,” in the *System Settings Guide*.

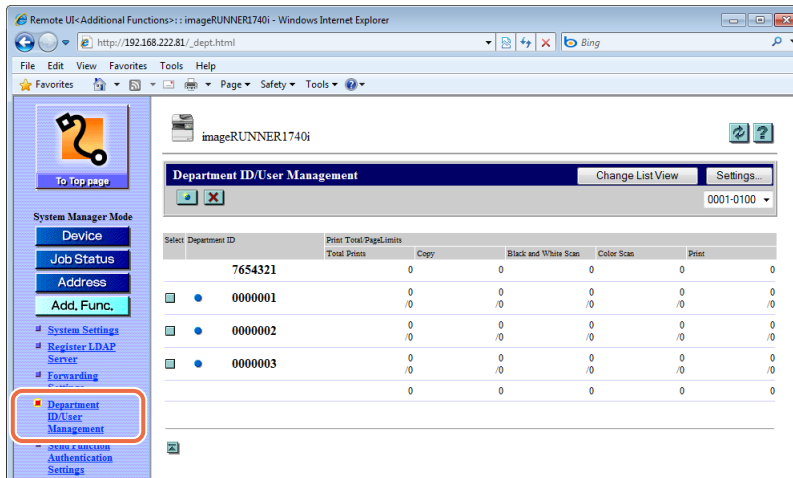
Managing the Department IDs

You can register, edit, or delete the Department IDs.

- 1 Click [Add.Func.] → [Department ID/User Management] in the [Add.Func.] menu.

NOTE

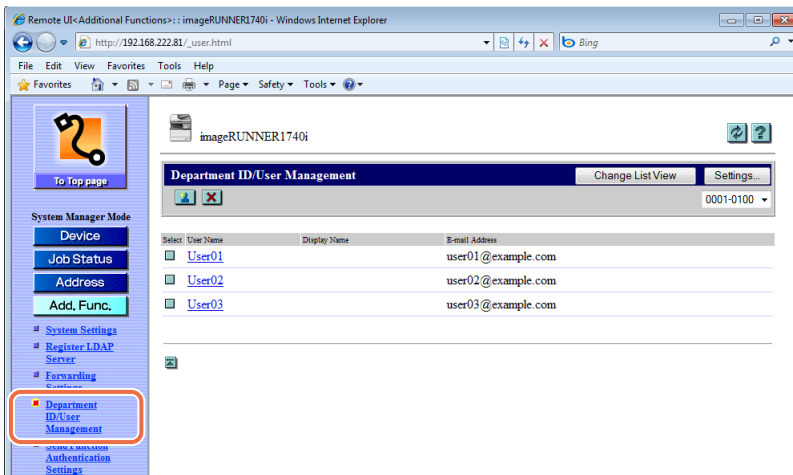
The list of the Department IDs switches to the list of the User IDs by clicking [Change List View]. The [Change List View] button appears when both the Department ID Management and the User Management are enabled and at least one ID is registered for each mode.



The screenshot shows a web browser window displaying the 'Department ID/User Management' page for 'imageRUNNER1740i'. The page includes a 'Change List View' button and a 'Settings...' button. A table lists Department IDs and their associated limits. The 'Add.Func.' menu item in the left sidebar is highlighted with a red box.

Select	Department ID	Print Total Page Limits	Copy	Black and White Scan	Color Scan	Print
	7654321	Total Pages	0	0	0	0
<input type="checkbox"/>	0000001	/0	0	0	0	0
<input type="checkbox"/>	0000002	/0	0	0	0	0
<input type="checkbox"/>	0000003	/0	0	0	0	0
			0	0	0	0

The page above displays the list of the Department IDs.



The page above displays the list of the User IDs.

2 Edit the Department IDs.

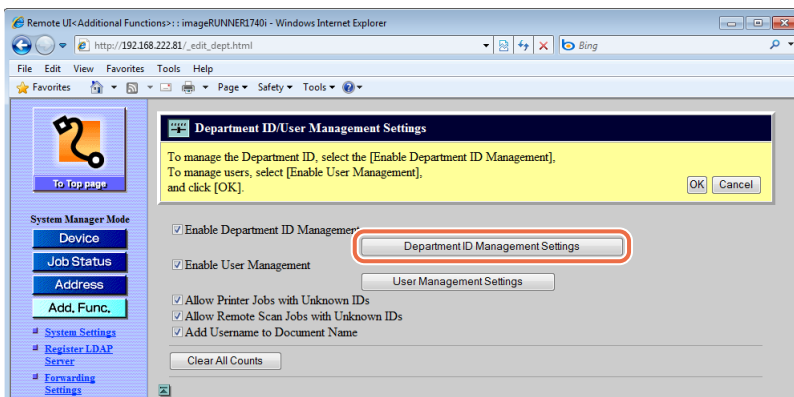
● To register a new Department ID:




NOTE

You can register up to 1,000 Department IDs.

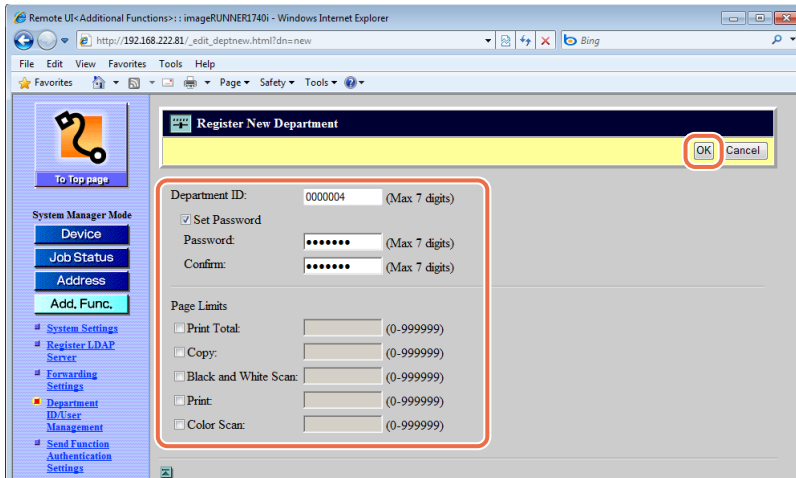
- Click [Settings] on the page shown in step 1.
The Department ID/User Management Settings page is displayed.
- Click [Department ID Management Settings].



The Register New Department page is displayed.

You can also display the Register New Department page by clicking [] (New) on the list of the Department IDs shown in step 1.

- Specify the necessary settings on the Register New Department page → click [OK].



The settings are as follows:

- Department ID: Enter a numeric ID (seven digits maximum).
- Set Password: Select this check box to set the password.
- Password: Enter a numeric password (seven digits maximum).
- Confirm: Enter the password again to confirm it.
- Page Limits: Select each check box to enter the maximum number of prints, copies, or scans that the department is allowed to make (0 - 999999).


IMPORTANT

When the optional Copy Card Reader-F1 is attached to the machine, do not register a new Department ID.

NOTE

- For instructions on how to specify the settings above on the machine's control panel, see Chapter 6, "Protecting the Machine from Unauthorized Access," in the *System Settings Guide*.
- The maximum number of digits you can register for the Department ID is seven. If you enter fewer than seven digits, the machine automatically adds zeros to the beginning.
Example: If <321> is entered, the Department ID will be displayed as <0000321>.
- <Print Total> is the sum of <Copy> and <Print>.



● To edit the Department ID:

- On the Department ID list shown in step 1, click [] (Edit) next to the Department ID you want to edit.

The Edit Department ID page is displayed.

- Edit the settings as necessary → click [OK].

● To delete the Department ID:

- On the Department ID list shown in step 1, click [] (Select) next to the Department ID you want to delete → [] (Delete).

Select	Department ID	Print Total	Page Limits	Copy	Black and White Scan	Color Scan	Print
	7654321	0		0	0	0	0
<input type="checkbox"/>	0000001	0		0	0	0	0
<input checked="" type="checkbox"/>	0000002	0		0	0	0	0
<input type="checkbox"/>	0000003	0	6000	2000	0	0	4000
<input type="checkbox"/>	0000004	0		0	0	0	0
		0		0	0	0	0

The selected Department ID is deleted.



IMPORTANT

When the optional Copy Card Reader-F1 is attached to the machine, do not delete a Department ID.

Managing the User IDs

You can register, edit, or delete the User IDs.



IMPORTANT

- First register a User ID as the System Manager, and then register other User IDs as the End Users before enabling User Management.
- If the User Types of all the User IDs are set to 'User' (End User), every user is regarded as the System Manager and will be able to log in to the machine and the Remote UI in the System Manager Mode.
- If you enable both Department ID Management and User Management, be sure to assign a Department ID (and the password for the Department ID) to each User ID. Users can log in to the machine and the Remote UI by entering the User ID that belongs to a Department ID.
- User IDs can be registered, edited, or deleted only on the Remote UI, while User Management can be enabled and disabled both on the machine's control panel and on the Remote UI.

1 Click [Add.Func.] → [Department ID/User Management] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in "Managing the Department IDs," on p. 3-6.

2 Edit the User IDs.

● To register a new User ID:



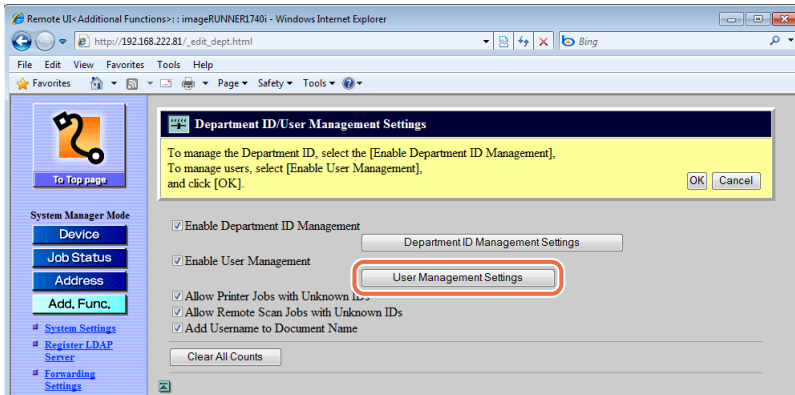
NOTE

You can register up to 1,000 User IDs.


- Click [Settings] on the page shown in step 1 in "Managing the Department IDs," on p. 3-6.

The Department ID/User Management Settings page is displayed.

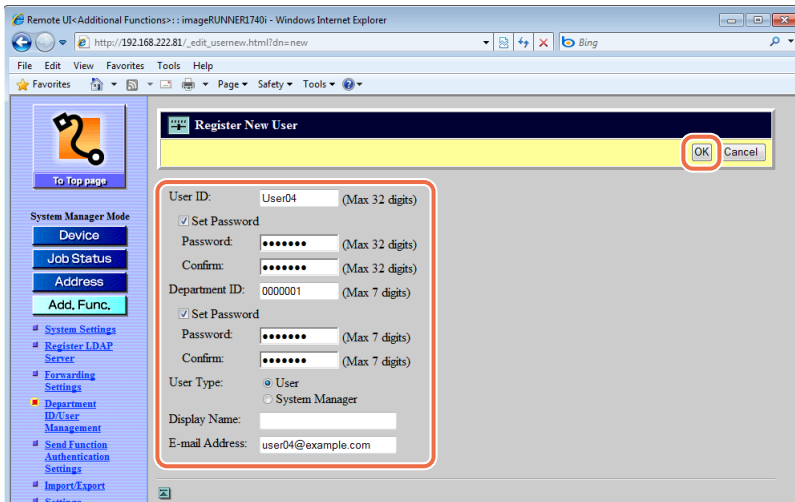
- Click [User Management Settings].



The Register New User page is displayed.

You can also display the Register New User page by clicking [] (New) on the list of the User IDs shown in step 1 in “Managing the Department IDs,” on p. 3-6.

- Specify the necessary settings on the Register New User page → click [OK].



The settings are as follows:

User ID:	Enter a User ID (a log-in name) (32 characters maximum).
Set Password:	Select this check box to set a password for the User ID.
Password:	Enter the password (32 characters maximum).
Confirm:	Enter the password again to confirm it.
Department ID:	Enter the Department ID the User ID belongs to (seven digits maximum).
Set Password:	Select this check box to set a password for the Department ID.
Password:	Enter the password (seven digits maximum).
Confirm:	Enter the password again to confirm it.



IMPORTANT

If you enable both Department ID Management and User Management, be sure to assign a Department ID (and the password for the Department ID) to each User ID. Users can log in to the machine and the Remote UI by entering their User ID that belongs to a Department ID.

User Type:	Specify the User Type by selecting the [User] (End User) or [System Manager] option button.
Display Name:	Enter the user name to display (32 characters maximum).
E-mail Address:	Enter the e-mail address of the user (120 characters maximum).



IMPORTANT

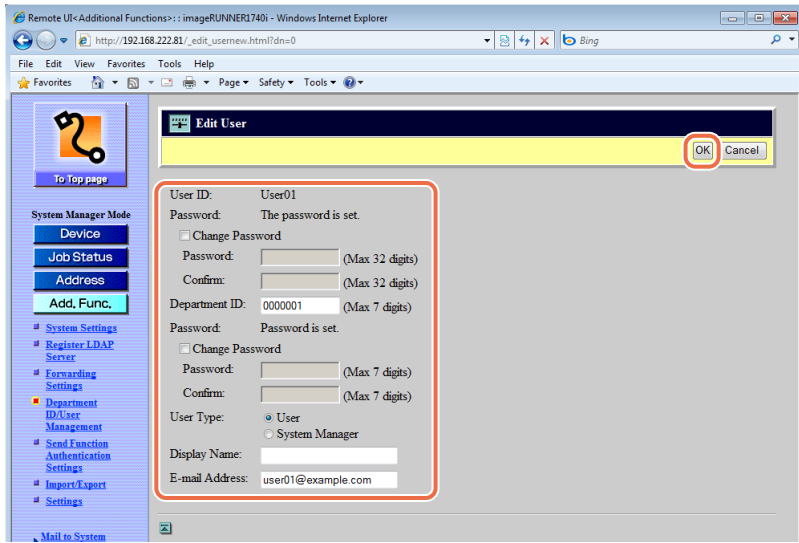
- When the optional Copy Card Reader-F1 is attached to the machine, do not register a new User ID.
- The settings above can be specified only on the Remote UI.

● **To edit the User ID:**

- ❑ Click the User ID you want to edit on the list of the User IDs shown in step 1 in “Managing the Department IDs,” on p. 3-6.

The Edit User page is displayed.

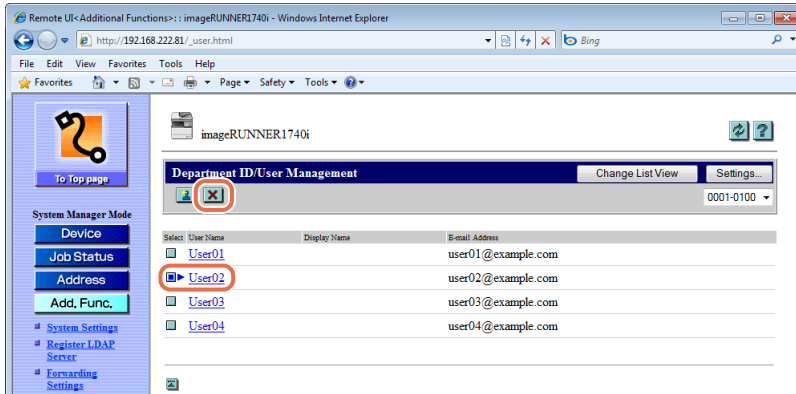
- ❑ Edit the settings as necessary → click [OK].



● To delete the User ID:

- ❑ Click (Select) next to the User ID you want to delete → (Delete).

For help, see the screen shot in step 1 in “Managing the Department IDs,” on p. 3-6.



The selected User ID is deleted.

👤 IMPORTANT

When the optional Copy Card Reader-F1 is attached to the machine, do not delete a User ID.

Customizing Settings

4


CHAPTER

This chapter describes how to customize the machine settings by using the Remote UI.

Customizing the System Settings	4-2
Editing the LDAP Server Settings	4-10
Editing the Forwarding Settings	4-14
Specifying the Authorized Send Settings	4-17
Customizing the Machine Settings	4-26
Specifying the SNMPv3 Settings	4-29
Enabling SNMPv3	4-30
Specifying the User Information for SNMPv3	4-31
Specifying the Context Settings for SNMPv3	4-34
Verifying SSL Server Certificates	4-37

Customizing the System Settings

In the System Settings page in the [Add.Func.] (Additional Functions) menu, you can specify the System Settings of the machine. Although many of the settings can be specified both on the Remote UI and on the machine's control panel, some settings can be specified only on the machine.

You can find the System Settings on the machine's control panel by pressing  (Additional Functions). For more information, see the *System Settings Guide*.



IMPORTANT

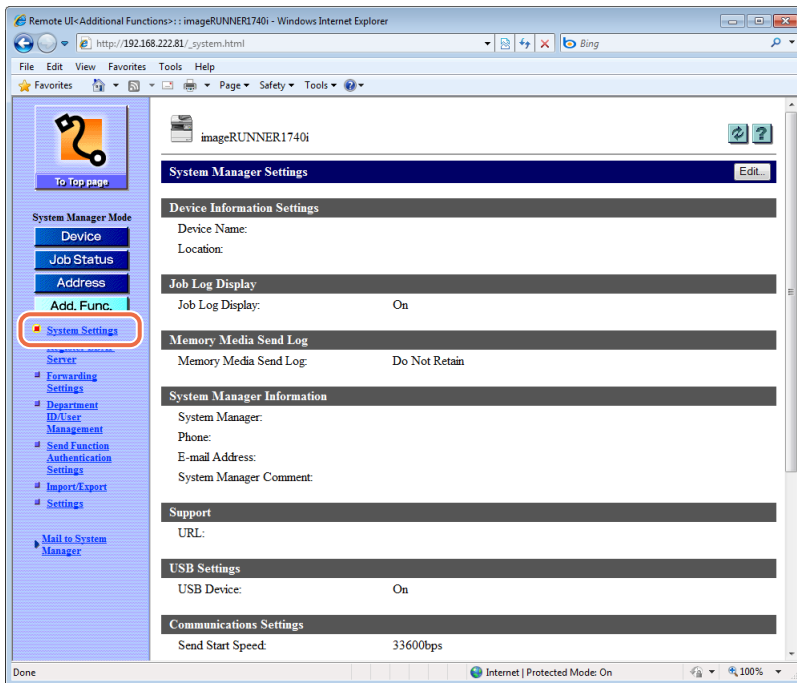
You can edit the System Settings on the Remote UI only when it is in the System Manager Mode.

System Settings on the Machine	Menus or Buttons on the Remote UI to access the settings listed left
System Manager Settings (System Manager's name and other information)	[Add.Func.] → [System Settings] → [Edit] (See p. 4-5)
System Manager Settings (System Manager ID and System Password)	[Add.Func.] → [System Settings] → [Edit] → [Register ID and Password] (See p. 4-9)
Device Info Settings	[Add.Func.] → [System Settings] → [Edit]
Department ID Management	[Add.Func.] → [Department ID/User Management] (See p. 3-6)
User ID Management	[Add.Func.] → [Department ID/User Management] (See p. 3-10)
Network Settings	[Add.Func.] → [Settings] → [Network Settings]
Communications Settings	[Add.Func.] → [System Settings] → [Edit]
Forwarding Settings	[Add.Func.] → [Forwarding Settings] (See p. 4-14)
Store/Print When Forwarding	[Add.Func.] → [System Settings] → [Edit]
Use SSL (under the Remote UI On/Off setting)	[Add.Func.] → [System Settings] → [Edit] (The Remote UI On/Off setting is available only on the machine's control panel.)
Restrict the Send Function	[Add.Func.] → [System Settings] → [Edit] → [Restrict the Send Function] (See p. 4-8)

System Settings on the Machine	Menus or Buttons on the Remote UI to access the settings listed left
Register LDAP Server	[Add.Func.] → [Register LDAP Server] (See p. 4-10)
Job Log Display	[Add.Func.] → [System Settings] → [Edit]
Memory Media Send Log*	[Add.Func.] → [System Settings] → [Edit]
Use USB Device	[Add.Func.] → [System Settings] → [Edit]
PDL Selection (Plug-n-Play)	[Add.Func.] → [System Settings] → [Edit]
Memory Media Settings	[Add.Func.] → [System Settings] → [Edit]
Secure Print Settings	[Add.Func.] → [System Settings] → [Edit]
Mem. Used When Warning Displayed	[Add.Func.] → [System Settings] → [Edit]
Other Settings	Available only on the machine's control panel.

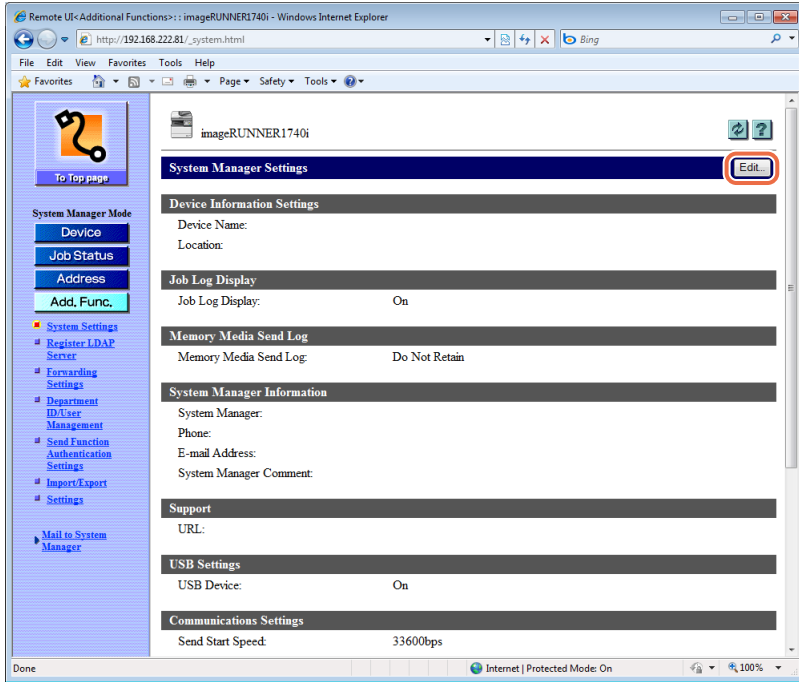
* [Memory Media Send Log] is displayed only when the Use Scan to Memory Media setting in Memory Media Settings is set to 'On'.

1 Click [Add.Func.] → [System Settings] in the [Add.Func.] menu.



The System Manager Settings page is displayed.

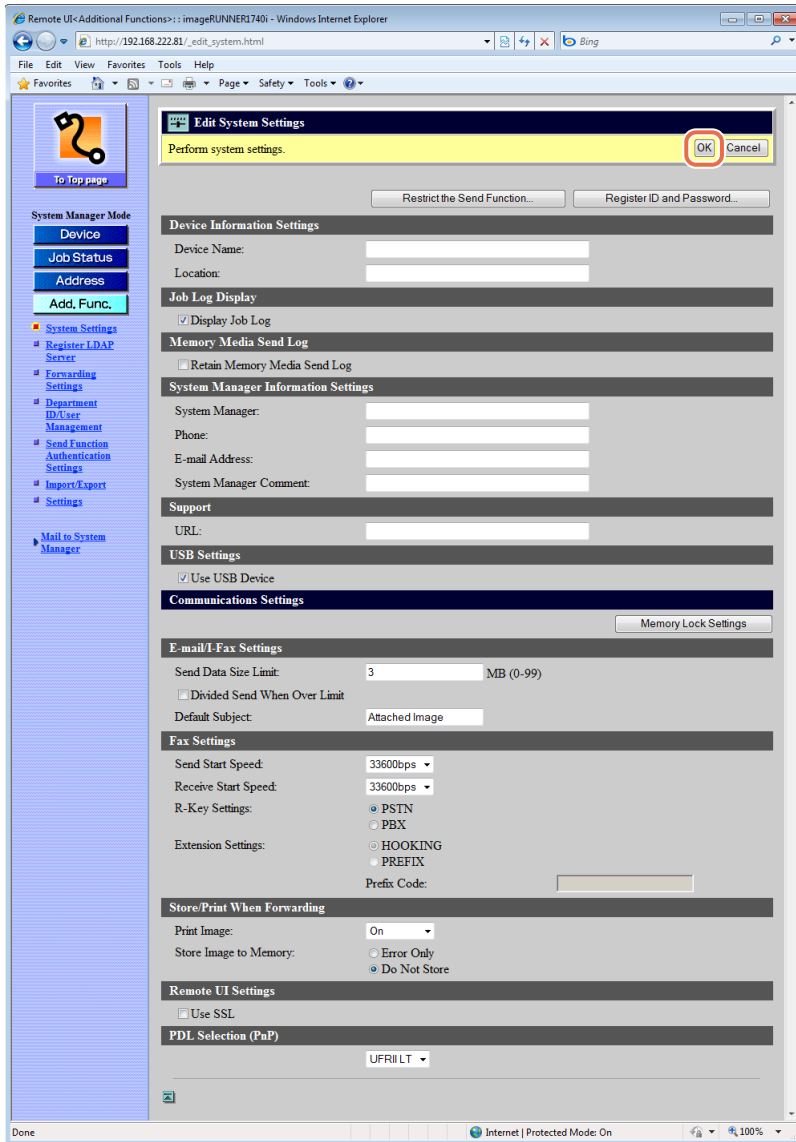
2 Click [Edit].



The Edit System Settings page is displayed.

● To specify the System Settings:

- Specify the necessary settings → click [OK].



The settings are as follows:

<System Manager Information Settings>

- System Manager: Enter the name of the System Manager (32 characters maximum).
- Phone: Enter the contact information of the System Manager (64 characters maximum).
- E-mail Address: Enter the e-mail address of the System Manager (64 characters maximum).
- System Manager Comment: Enter the comments from the System Manager (64 characters maximum).



IMPORTANT

<Phone>, <E-mail Address>, and <System Manager Comment> can be specified only on the Remote UI.



NOTE

For instructions on how to specify the System Manager ID and System Password, see “To specify the System Manager ID and System Password:” on p. 4-9.

<Support>

URL: Enter the URL for supporting the users as necessary.



IMPORTANT

<Support> can be specified only on the Remote UI.



NOTE

For information on the settings except described above, see the following chapters in the *System Settings Guide*:

Device Information Chapter 7, "Other System Settings"

Settings:

Job Log Display: Chapter 6, "Protecting the Machine from Unauthorized Access"

Memory Media Chapter 7, "Other System Settings"

Send Log:

System Manager Chapter 1, "Before You Start"

Information Settings:

USB Settings: Chapter 7, "Other System Settings"

Communications Chapter 4, "Setting the Send Function"

Settings:

E-Mail/I-Fax Chapter 4, "Setting the Send Function"

Settings:

Fax Settings: Chapter 4, "Setting the Send Function"

Store/Print When Chapter 4, "Setting the Send Function"

Forwarding:

Remote UI Settings: Chapter 6, "Protecting the Machine from Unauthorized Access"

PDL Selection (PnP): Chapter 7, "Other System Settings"

Memory Media Chapter 4, "Setting the Send Function" and

Settings: Chapter 7, "Other System Settings"

Secured Print Chapter 7, "Other System Settings"

Settings:

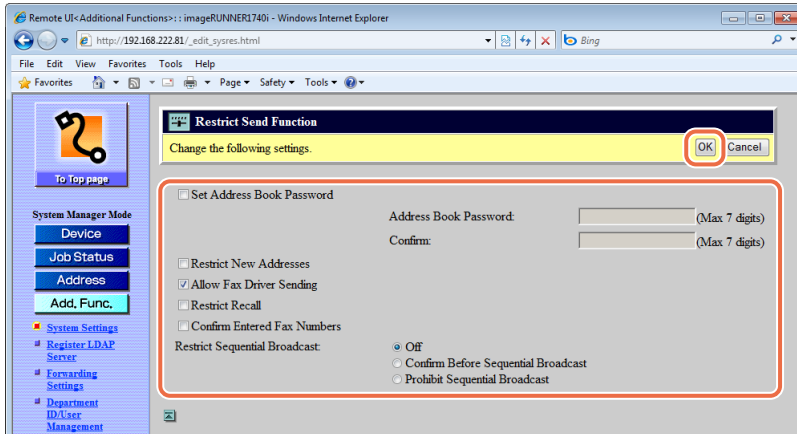
Memory Used When Chapter 7, "Other System Settings"

Warning Message is

Displayed:

● **To specify the Restrict the Send Function settings:**

- ❑ Click [Restrict the Send Function] displayed on the Edit System Settings page.
For help, see the screen shot in “To specify the System Settings,” on p. 4-5.
The Restrict Send Function page is displayed.
- ❑ Specify the necessary settings → click [OK].

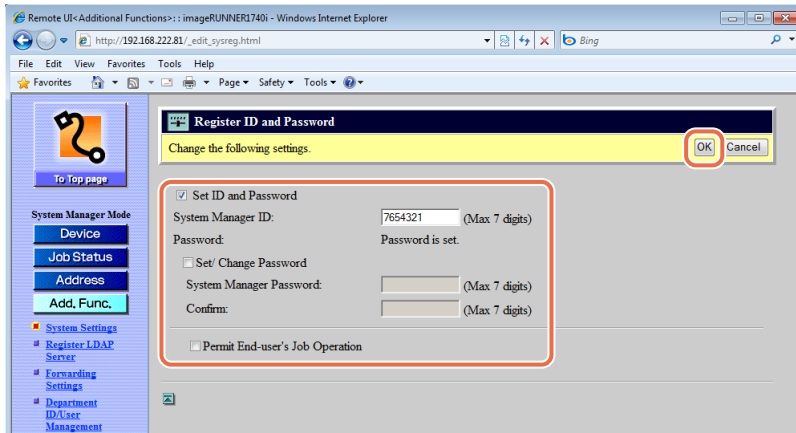


NOTE

For information on the settings, see Chapter 4, “Setting the Send Function,” in the *System Settings Guide*.

● **To specify the System Manager ID and System Password:**

- ❑ Click [Register ID and Password] on the Edit System Settings page.
For help, see the screen shot in “To specify the System Settings:,” on p. 4-5.
The Register ID and Password page is displayed.
- ❑ Specify the necessary settings → click [OK].



The settings are as follows:

- | | |
|--------------------------|---|
| Set ID and Password: | Select this check box to set the System Manager ID and System Password. |
| System Manager ID: | Enter the System Manager ID (seven digits maximum). |
| Set/Change Password: | Select this check box to set or change the System Password. |
| System Manager Password: | Enter the System Password (seven digits maximum). |
| Confirm: | Enter again the password to confirm it. |

 **IMPORTANT**

The System Manager ID and System Password are both set to '7654321' at purchase. Change them before using the machine.

- | | |
|----------------------------------|--|
| Permit End-user's Job Operation: | When this check box is selected, print jobs can be deleted in the End-User Mode under the user name entered when logging in. |
|----------------------------------|--|

 **IMPORTANT**

<Permit End-user's Job Operation> can be specified only on the Remote UI.

Editing the LDAP Server Settings

You can manage the LDAP server settings.



IMPORTANT

Specifying the LDAP server settings is available only when the Remote UI is in the System Manager Mode.



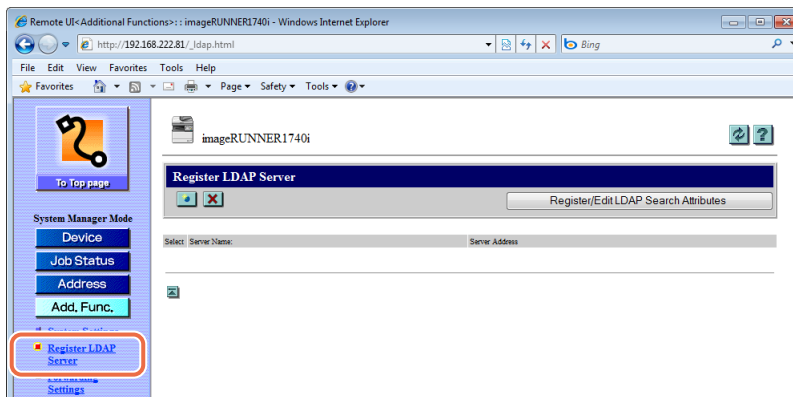
NOTE

For instructions on how to edit the LDAP server settings on the machine's control panel, see Chapter 3, "Setting up the Machine for Your Network Environment," in the *System Settings Guide*.

4

Customizing Settings


- 1 Click [Add.Func.] → [Register LDAP Server] in the [Add.Func.] menu.



The Register LDAP Server page is displayed.

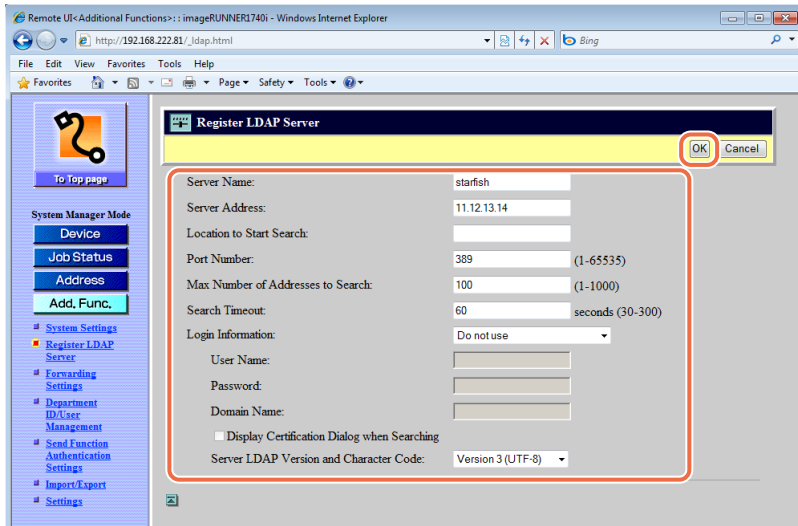
2 Edit the LDAP server settings.

● To register a new LDAP server:

- ❑ Click [] (Register) on the page shown in step 1.

The Register LDAP Server (or Register LDAP Search Server) page is displayed.

- ❑ Specify the necessary settings → click [OK].



The screenshot shows a web browser window displaying the 'Register LDAP Server' page. The page has a navigation menu on the left with options like 'System Manager Mode', 'Device', 'Job Status', 'Address', 'Add, Func.', 'System Settings', 'Register LDAP Server', 'Forwarding Settings', 'Department ID/User Management', 'Send Function Authentication Settings', 'Import/Export', and 'Settings'. The main content area contains a form with the following fields:

Server Name:	starfish
Server Address:	11.12.13.14
Location to Start Search:	
Port Number:	389 (1-65535)
Max Number of Addresses to Search:	100 (1-1000)
Search Timeout:	60 seconds (30-300)
Login Information:	Do not use
User Name:	
Password:	
Domain Name:	
<input type="checkbox"/> Display Certification Dialog when Searching	
Server LDAP Version and Character Code:	Version 3 (UTF-8)

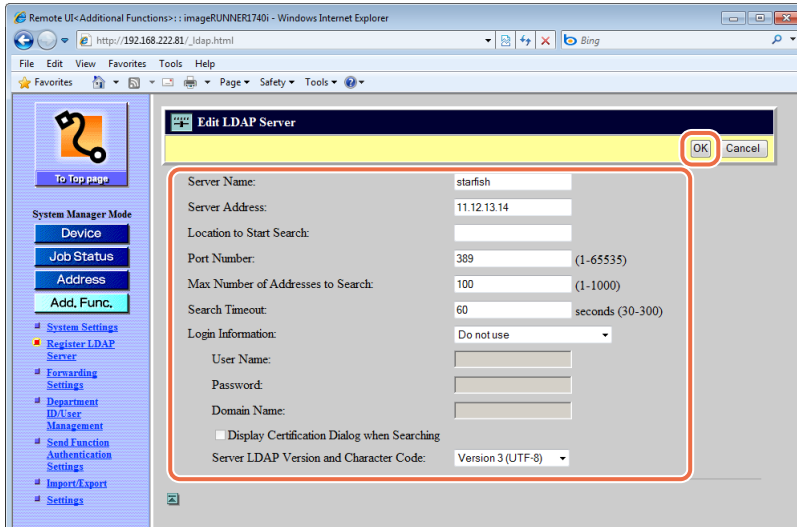
Buttons for 'OK' and 'Cancel' are located at the top right of the form area.

NOTE

- For information on the settings, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.
- If Authorized Send is activated, <Authentication Method> appears on this page. Specify whether to carry over the login information (user name and password) from Authorized Send to the authentication information used when users search for e-mail addresses and fax numbers via the LDAP server. To use the same user name and password for LDAP search authentication, select [Assume the same authentication information as when operation to send was started]. If not, select [Use device-specific authentication information].

● **To edit the LDAP server:**

- ❑ Click the LDAP server name you want to edit on the page shown in step 1.
The Edit LDAP Server (or Edit LDAP Search Server) page is displayed.
- ❑ Edit the settings as necessary → click [OK].

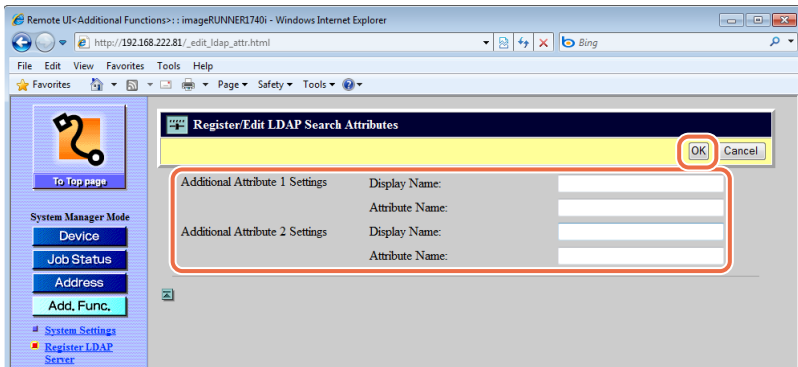


● **To delete the LDAP server:**

- ❑ On the page shown in step 1, click [] (Select) next to the LDAP server you want to delete → [X] (Delete).
The selected LDAP server is deleted.

● **To register or edit the LDAP search attributes:**

- ❑ Click [Register/Edit LDAP Search Attributes] on the page shown in step 1.
The Register/Edit LDAP Search Attributes page is displayed.
- ❑ Specify or edit the necessary settings → click [OK].



NOTE

For information on the settings, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.

Editing the Forwarding Settings

You can register, edit, or delete the conditions for forwarding received documents.



IMPORTANT

Specifying the Forwarding Settings is available only when the Remote UI is in the System Manager Mode.



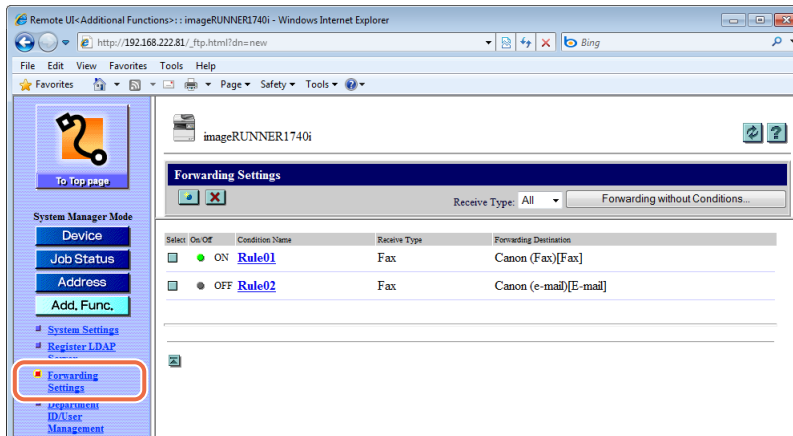
NOTE

For instructions on how to edit the forwarding settings on the machine's control panel, see Chapter 4, "Setting the Send Function," in the *System Settings Guide*.

4

Customizing Settings


- 1 Click [Add.Func.] → [Forwarding Settings] in the [Add.Func.] menu.

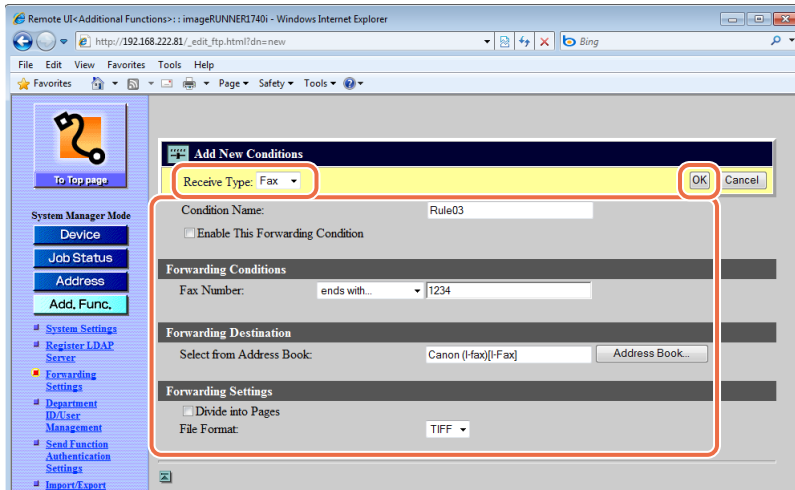


The Forwarding Settings page is displayed.

- 2 Edit the forwarding settings.

- **To register a new forwarding condition:**

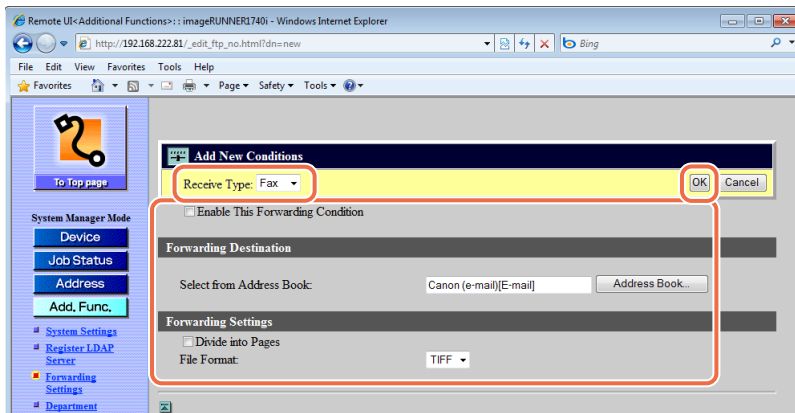
- Click [] (Add New Conditions) on the page shown in step 1.
The Add New Conditions page is displayed.
- Specify the necessary settings → click [OK].

**NOTE**

For information on the settings, see Chapter 4, “Setting the Send Function,” in the *System Settings Guide*.

● To forward all received documents without specific conditions:

- Click [Forwarding without Conditions] on the page shown in step 1. The Add New Conditions page is displayed.
- Specify the necessary settings → click [OK].

**NOTE**

For information on the settings, see Chapter 4, “Setting the Send Function,” in the *System Settings Guide*.

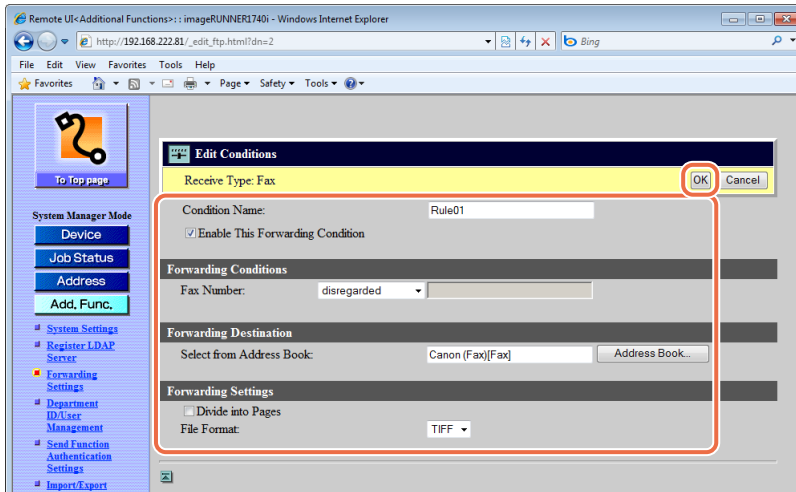
● To edit the forwarding condition:

- Click the name of the forwarding condition that you want to edit on the page shown in step 1.

If you select [All] in the [Receive Type] drop-down list box, all the forwarding settings registered in the machine are displayed.

The Edit Conditions page is displayed.

- Edit the settings as necessary → click [OK].

**● To delete the forwarding condition:**

- On the Forwarding Settings page shown in step 1, click [] (Select) next to the forwarding condition that you want to delete → [X] (Delete the Selected Conditions).

The selected forwarding condition is deleted.

Specifying the Authorized Send Settings

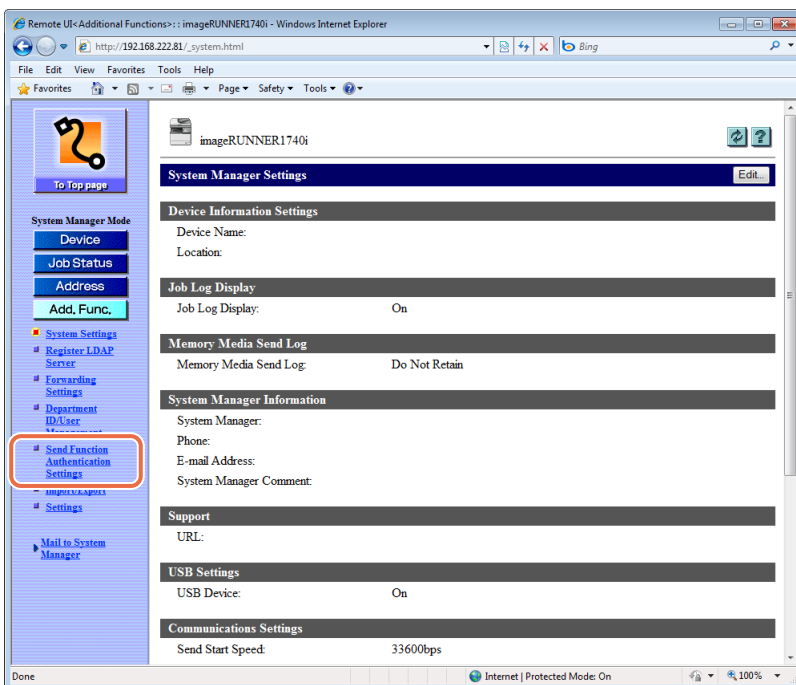
You can specify the Authorized Send settings on the Remote UI only.



IMPORTANT

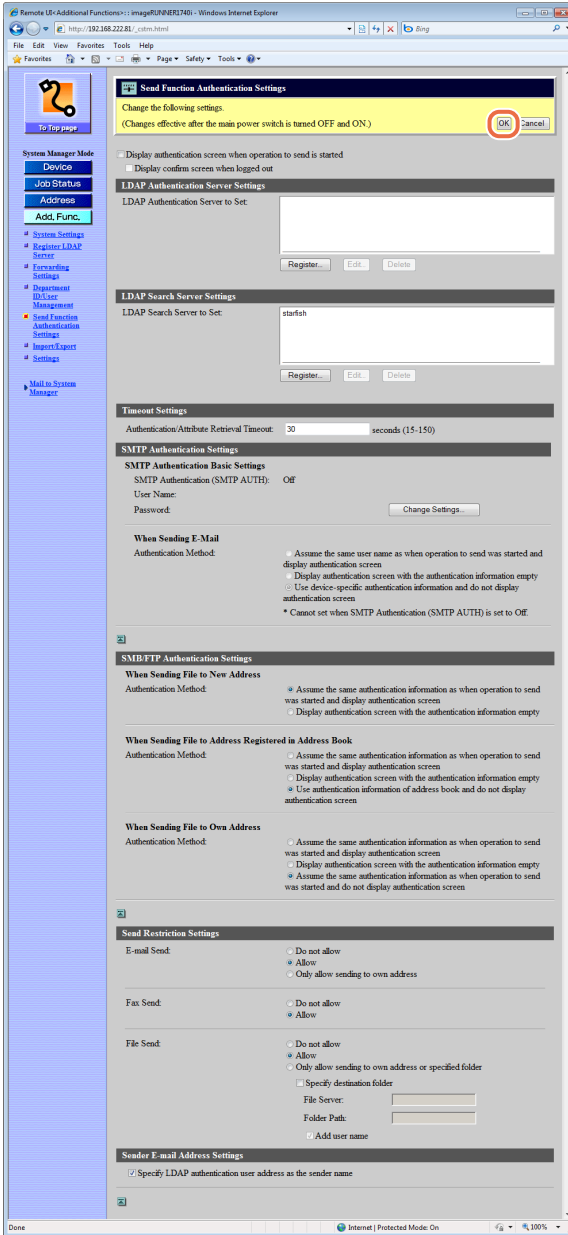
Specifying the Authorized Send settings is available only when the Remote UI is in the System Manager Mode.

- 1 Click [Add.Func.] → [Send Function Authentication Settings] in the [Add.Func.] menu.



The Send Function Authentication Settings page is displayed.

2 Specify the necessary settings → click [OK].



4

Customizing Settings

The setting descriptions are as follows:

- | | |
|---|--|
| <p>Display authentication screen when operation to send is started:</p> | <p>Select this check box to activate Authorized Send and authenticate users who send documents from the machine. To enable the settings in the Send Function Authentication Settings page, this check box must be selected.</p> |
| <p>Display confirm screen when logged out:</p> | <p>Select this check box to display the confirmation screen when a user logs out of Authorized Send. The log out options are [Send] and [Device]. (See Chapter 2, "Sending Documents," in the <i>Sending and Facsimile Guide</i>.)</p> <ul style="list-style-type: none"> • [Send]: Logs out of Authorized Send only. • [Device]: Simultaneously logs out of other security features such as Department ID Management. |



IMPORTANT

The confirmation screen appears only if the machine is locked with security features such as Department ID Management. If the machine is locked with security features and [Display confirm screen when logged out] is not selected, the machine works as if [Device] is pressed when the user logs out of Authorized Send.

<LDAP Authentication Server Settings>

Press [Register] and specify the authentication server settings in the machine, according to the server used. Up to five authentication servers can be registered. To change or delete the registered server settings, select the desired server name and press [Edit] or [Delete].

Server Name:	Enter the name of the authentication server.
Server Address:	Specify the IP address or DNS name of the authentication server. If log in to an authentication server uses the Kerberos authentication method, the DNS name needs to be in a Fully Qualified Domain Name (FQDN) format.
Location to Start Search:	Specify the location of the directory tree to start searching for user entries.
Port Number:	Specify the port number for accessing the authentication server. The default port number is '389' (non-SSL) or '636' (SSL).
Attribute of User Name:	Specify the user attribute name such as 'sAMAccountName' and 'uid'. The specified attribute is used to validate the user name entered when the user logs in to Authorized Send.
Attribute of E-mail Address:	Specify the mail attribute name such as 'mail'. The specified attribute is used to obtain the currently logged on user's e-mail address from the authentication server. The obtained address is specified as destination when the user presses [Send Mail To Self]. (See Chapter 2, "Sending Documents," in the <i>Sending and Facsimile Guide</i> .)
Login Information:	Specify the authentication method used when the machine communicates with the authentication server. Select [Use] to use the Simple authentication method, or [Use (Security Authentication)] to use the Kerberos authentication method. The Kerberos authentication method is available for Active Directory.
Domain Name:	If you select [Use (Security Authentication)] for <Login Information>, enter the directory tree name of the Active Directory, such as <team1.salesdept.canon.co.jp>.
Use System Manager ID:	This setting is available only when [Use] is selected from [Login Information] as the authentication method. Select this check box to use the administrator's ID and password for the authentication server when performing the first bind of the simple binding process. If you use anonymous binding, deselect this check box.
User Name:	This text box is available only when [Use System Manager ID] is selected. Enter the administrator's user name.
Password:	This text box is available only when [Use System Manager ID] is selected. Enter the administrator's login password.
Use SSL:	This setting is available only when [Use] is selected from [Login Information] as the authentication method. Select this check box to use the Secure Sockets Layer (SSL) protocol when the machine communicates with the authentication server. If you select this check box, the value for <Port Number> automatically changes to '636'.



IMPORTANT

- For your network server settings, consult your network administrator.
- <Location to Start Search> can be left blank. In this case, the value of the defaultNamingContext attribute is retrieved and used as the location of the directory tree to start searching. When no value is available, the attribute value with the shortest length in the namingContexts attributes is selected instead. If this fails, <Location to Start Search> is left blank.
- <Attribute of User Name> cannot be specified when the Kerberos authentication method is selected in <Login Information>. If this method is selected or <Attribute of User Name> is left blank, 'sAMAccountName' is automatically used as the user attribute name.
- If <Attribute of E-mail Address> is left blank, 'mail' is automatically used as the mail attribute name.

<LDAP Search Server Settings>

Press [Register] and specify the search server settings in the machine, according to the server used. Up to five search servers can be registered.

To change or delete the registered server settings, select the desired server name and press [Edit] or [Delete].

The screenshot shows a web browser window displaying the 'Register LDAP Search Server' dialog box. The dialog has a title bar with 'OK' and 'Cancel' buttons. The main area contains the following fields and options:

- Server Name: [Text input field]
- Server Address: [Text input field]
- Location to Start Search: [Text input field]
- Port Number: 389 (1-65535)
- Max Number of Addresses to Search: 100 (1-1000)
- Search Timeout: 60 seconds (30-300)
- Login Information: Do not use (dropdown menu)
- Domain Name: [Text input field]
- Server LDAP Version and Character Code: Version 3 (UTF-8) (dropdown menu)
- Authentication Method:
 - Assume the same authentication information as when operation to send was started
 - Use device-specific authentication information
- User Name: [Text input field]
- Password: [Text input field]
- Display Certification Dialog when Searching

For information on the settings other than the one below, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.

Authentication Method: This setting is available only when Authorized Send is activated. Specify whether to carry over the login information (user name and password) from Authorized Send to the authentication information used when users search for e-mail addresses and fax numbers via the LDAP server. To use the same user name and password for LDAP search authentication, select [Assume the same authentication information as when operation to send was started]. If not, select [Use device-specific authentication information].



IMPORTANT

For your network server settings, consult your network administrator.

<Timeout Settings>

Authentication/Attribute Retrieval Timeout: Specify the time that the machine takes to authenticate a user against the authentication server and to retrieve attributes about the user from the server.



IMPORTANT

Depending on the conditions such as authentication methods you are using, the timeout time may be shorter than designated.

<SMTP Authentication Settings>

SMTP Authentication Basic Settings: To edit the SMTP authentication settings, press [Change Settings]. For instructions on how to specify the SMTP authentication settings, see Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*.

Authentication Method: You can specify whether to carry over the login information (user name only) from Authorized Send to SMTP authentication. Select the desired option from the following:

- [Assume the same user name as when operation to send was started and display authentication screen]: Displays the authentication screen with the user name for Authorized Send automatically inserted in the [User Name] text box of the SMTP authentication screen.
- [Display authentication screen with the authentication information empty]: Displays the authentication screen with no entries in the [User Name] text box of the SMTP authentication screen. Users need to enter the user name each time they send e-mails and I-faxes.
- [Use device-specific authentication information and do not display authentication screen]: Does not display the authentication screen. The user name and password specified for the machine are used as the login information.

<SMB/FTP Authentication Settings>

You can specify whether to carry over the login information (user name and password) from Authorized Send to the authentication information used when users send documents to a file server. Specify the settings below to suit your needs.

When Sending File to New Address: This setting is used when users specify the destination by pressing [File] on the top screen (Send) and specifying the file server address manually. Select the desired option from the following:

- [Assume the same authentication information as when operation to send was started and display authentication screen]: Displays the authentication screen with the user name and password for Authorized Send automatically inserted in the [User] text box and the [Password] text box of the screen.
- [Display authentication screen with the authentication information empty]: Displays the authentication screen with no entries in the [User] text box and the [Password] text box of the screen. Users need to enter the user name and password each time they send documents to a file server.

When Sending File to Address Registered in Address Book: This setting is used when users specify the destination by selecting the file server address from the Address Book list. Select the desired option from the following:

- [Assume the same authentication information as when operation to send was started and display authentication screen]: Displays the authentication screen with the user name and password for Authorized Send automatically inserted in the [User] text box and the [Password] text box of the screen.
- [Display authentication screen with the authentication information empty]: Displays the authentication screen with no entries in the [User] text box and the [Password] text box of the screen. Users need to enter the user name and password each time they send documents to a file server.
- [Use authentication information of address book and do not display authentication screen]: Does not display the authentication screen. The user name and password of each address in the Address Book are used as the login information.

- When Sending File to Own Address: This setting is used when users specify the destination by pressing [Send File To Self] on the top screen (Send). Select the desired option from the following:
- [Assume the same authentication information as when operation to send was started and display authentication screen]: Displays the authentication screen with the user name and password for Authorized Send automatically inserted in the [User] text box and the [Password] text box of the screen.
 - [Display authentication screen with the authentication information empty]: Displays the authentication screen with no entries in the [User] text box and the [Password] text box of the screen. Users need to enter the user name and password each time they send documents to a file server.
 - [Assume the same authentication information as when operation to send was started and do not display authentication screen]: Does not display the authentication screen. The user name and password for Authorized Send is used as the login information.

<Send Restriction Settings>

You can enable and disable sending functionalities. Specify the settings below to suit your needs.

- E-mail Send:
- [Do not allow]: Disables user from sending e-mails and I-faxes from the machine.
 - [Allow]: Enables user to send e-mails and I-faxes from the machine.
 - [Only allow sending to own address]: Restricts the destination of sending documents to the e-mail address of a logged on user. With this setting, users also cannot send I-faxes from the machine. For instructions on how to send documents to the e-mail address of a logged on user, see Chapter 2, "Sending Documents," in the *Sending and Facsimile Guide*.
- Fax Send:
- [Do not allow]: Disables user from sending faxes from the machine.
 - [Allow]: Enables user to send faxes from the machine.

- File Send:
- [Do not allow]: Disables user from sending documents to a file server.
 - [Allow]: Enables user to send documents to a file server.
 - [Only allow sending to own address or specified folder]: Restricts the destination of sending documents to the folder of a logged on user or to the specified folder. If Active Directory is used as an authentication server, the home directory (folder) of a logged on user is used as the destination. If not, or you want to manually specify the destination folder, select [Specify destination folder], then enter the name of the file server and the folder name in [File Server] and [Folder Path]. Selecting [Add user name] enables you to use the user name of a logged on user to specify the destination of sending documents under the specified folder. For example, if <share> is entered in [Folder Path] and the user name of a logged on user is 'john', the [john] folder in the [share] folder is specified as the destination. For instructions on how to send documents to the folder of a logged on user, see Chapter 2, "Sending Documents," in the *Sending and Facsimile Guide*.

<Sender E-mail Address Settings>


- Specify LDAP authentication user address as the sender name:
- Select this check box to use the e-mail address of a logged on user as the sender information when sending e-mails or I-faxes. The e-mail address is displayed or printed as the sender information at the recipient's machine, instead of the unit name. (See Chapter 1, "Introduction to Send and Fax Functions," in the *Sending and Facsimile Guide*.)

Customizing the Machine Settings

You can edit the various machine settings on the Settings page in the [Add.Func.] (Additional Functions) menu. Although many of the settings can be made both on the Remote UI and on the machine's control panel, some settings are accessible only on the machine's control panel.

On the Remote UI, the Additional Functions settings are located as shown in the table below.

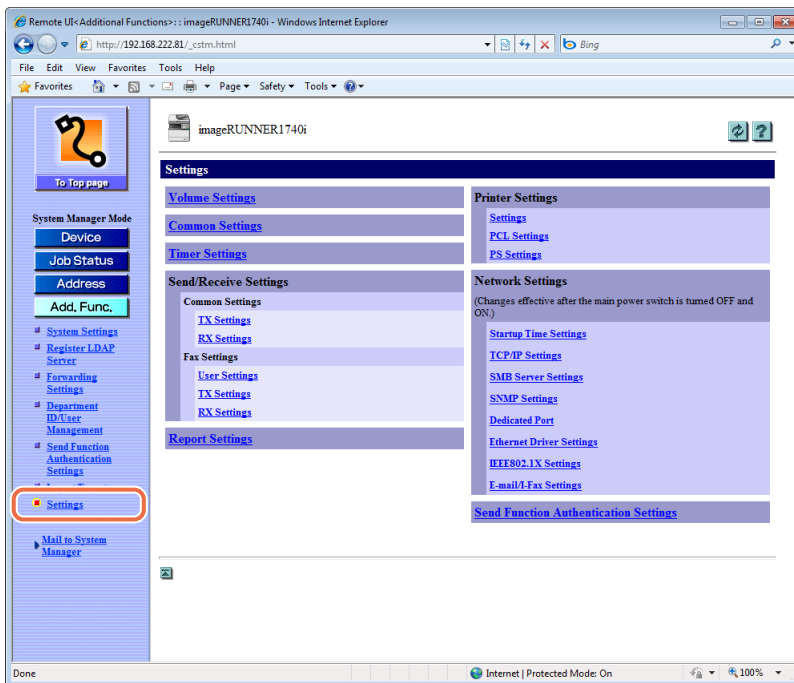
NOTE

- You can access the Additional Functions settings from the machine's control panel by pressing  (Additional Functions).
- For information on the Volume Settings, see Chapter 3, "Configuring the Machine's Basic Settings," in the *Reference Guide*.

Additional Functions menu on the Machine	Menus on the Remote UI	References
Common Settings	[Add.Func.] → [Settings] → [Common Settings]	Chapter 3, "Configuring the Machine's Basic Settings," in the <i>Reference Guide</i>
Copy Settings	Available only on the machine's control panel.	Chapter 4, "Customizing Settings," in the <i>Copying Guide</i>
Timer Settings	[Add.Func.] → [Settings] → [Timer Settings]	Chapter 3, "Configuring the Machine's Basic Settings," in the <i>Reference Guide</i>
Communications Settings	[Add.Func.] → [Settings] → [Send/Receive Settings]	Chapter 7, "Customizing the Machine's Settings," in the <i>Sending and Facsimile Guide</i>
Adjustment/Cleaning	Available only on the machine's control panel.	Chapter 5, "Routine Maintenance," and Chapter 6, "Troubleshooting," in the <i>Reference Guide</i>
Printer Settings	[Add.Func.] → [Settings] → [Printer Settings]	Chapter 4, "Customizing Settings," in the <i>Printer Guide</i>

Additional Functions menu on the Machine	Menus on the Remote UI	References
Report Settings	[Add.Func.] → [Settings] → [Report Settings]	Chapter 8, “Printing Communication Reports and Lists,” in the <i>Sending and Facsimile Guide</i>
Address Book Settings	[Address]	Chapter 4, “Specifying Destinations Easily and Quickly,” in the <i>Sending and Facsimile Guide</i>
System Settings	See the table on p. 4-2.	-

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.



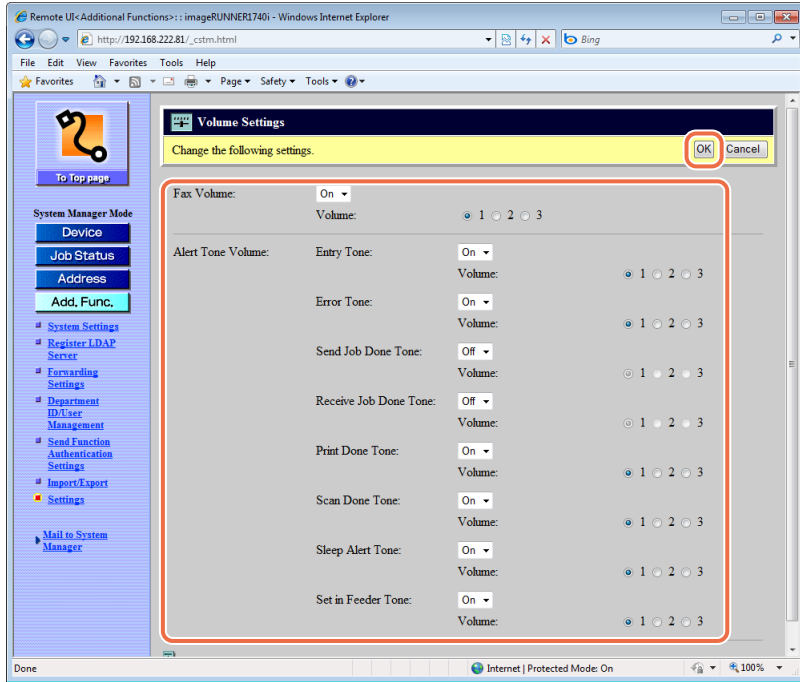
NOTE

The available settings menu varies depending on the models or options you have installed or activated.

2 Click the setting item you want to edit.

The settings page for the selected item is displayed.

3 Edit the settings as necessary → click [OK].



The screen shot above is for the Volume Settings.

NOTE

- For information on the settings, see the other references listed on the table in “Customizing the Machine Settings,” on p. 4-26.
- For information on the settings of [Send Function Authentication Settings], see “Specifying the Authorized Send Settings,” on p. 4-17.

Specifying the SNMPv3 Settings

Specify the settings for SNMPv3 as described below.



IMPORTANT

- Specifying the settings for SNMPv3 is available only when the Remote UI is in the System Manager Mode.
- Specifying the settings for SNMPv3 is available only when SSL communication is enabled. See the following information on the settings for SSL communication.
 - Chapter 3, “Setting up the Machine for Your Network Environment,” in the *System Settings Guide*
 - “Managing Key Pairs and Digital Certificates from a Web Browser,” on p. 2-25



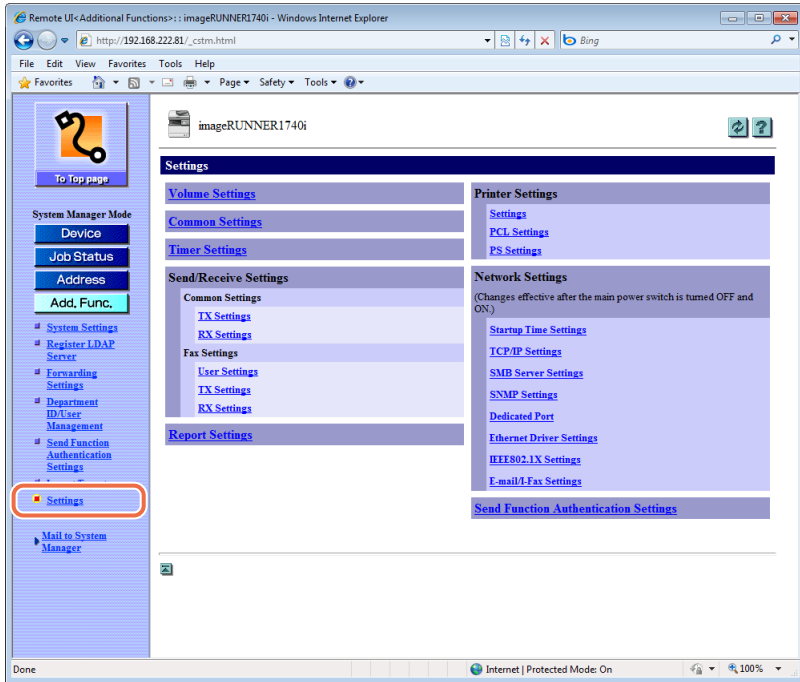
NOTE

The settings for SNMPv3 can be specified only on the Remote UI, while the settings for SNMPv1 can be specified both on the machine’s control panel and the Remote UI. For more information on the settings for SNMPv1, see Chapter 2, “Connecting the Machine to a TCP/IP Network,” in the *System Settings Guide*.

Enabling SNMPv3

Enable SNMPv3 as described below.

- 1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

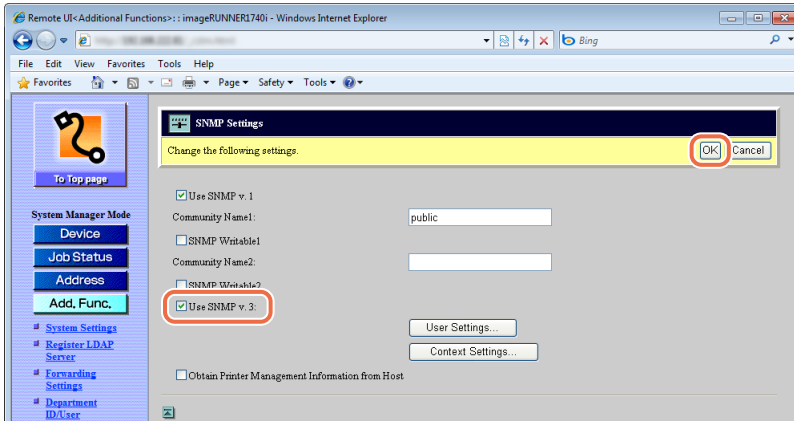


The Settings page is displayed.

- 2 Click [SNMP Settings] on the page shown in step 1.

The SNMP Settings page is displayed.

3 Select the check box for [Use SNMP v. 3] → click [OK].



NOTE

You can enable both SNMPv1 and SNMPv3 at the same time, depending on your needs. For more information on settings for SNMPv1, see Chapter 2, “Connecting the Machine to a TCP/IP Network,” in the *System Settings Guide*.

4 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

IMPORTANT

The setting for [Use SNMP v.3] becomes effective after the machine is restarted, while restarting the machine is not necessary to enable the settings for [User Settings] (p. 4-31) and [Context Settings] (p. 4-34).

Specifying the User Information for SNMPv3

Specify the user information for SNMPv3 as described below.

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

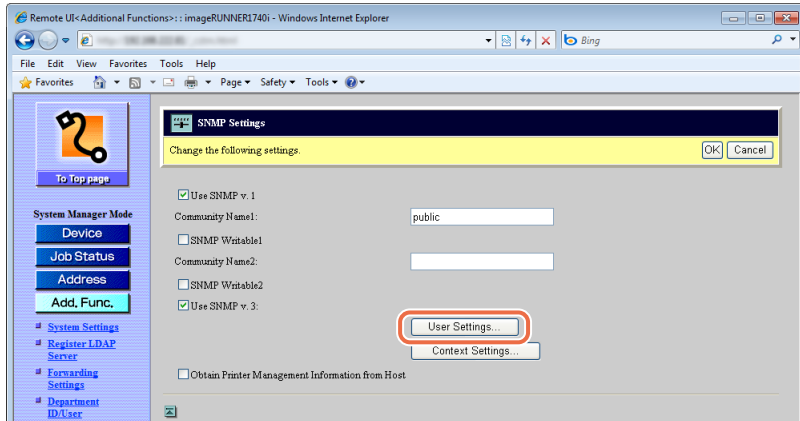
For help, see the screen shot in step 1 in “Enabling SNMPv3,” on p. 4-30.

The Settings page is displayed.

2 Click [SNMP Settings].

For help, see the screen shot in step 1 in “Enabling SNMPv3,” on p. 4-30.
The SNMP Settings page is displayed.

3 Click [User Settings].



The User Settings page is displayed.

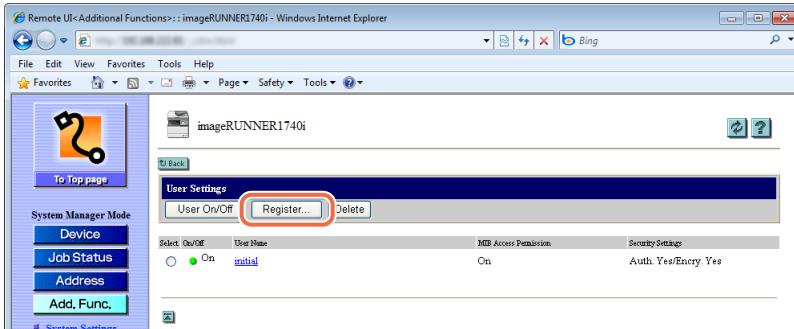
4 Select the function.

● To register a new user:

NOTE

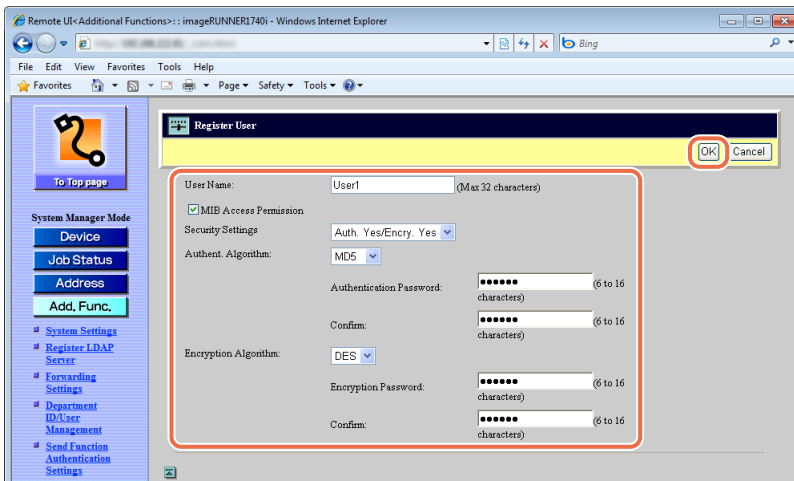
- A default user “initial” is registered. Edit it as necessary.
 - User Name: initial
 - MIB Access Permission: ON
 - Security Settings: Auth. Yes/Encry. Yes
 - Authent. Algorithm: MD5
 - Authentication Password: initial
 - Encryption Algorithm: DES
 - Encryption Password: initial
- You can register up to five users (including the default user “initial”).

❑ Click [Register].



The Register User page is displayed.

❑ Specify the necessary information → click [OK].

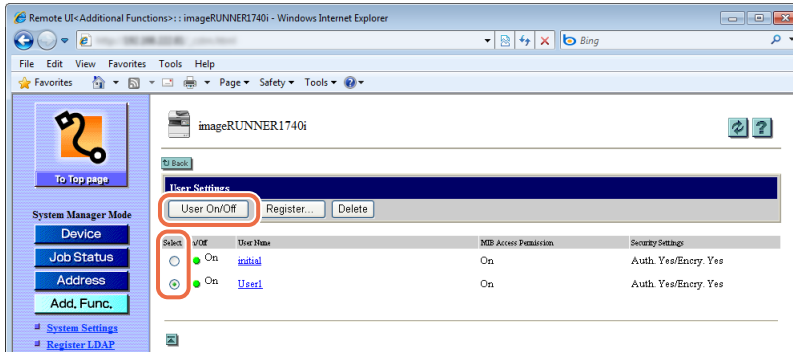


- User Name: Enter the user name (32 alphanumeric characters maximum).
- MIB Access Permission: Select this check box to give read/write permission to the user.
- Security Settings: Select the security setting ([Auth. Yes/Encry. Yes], [Auth. Yes/Encry. No], or [Auth. No/Encrypt. No]). If you select [Auth. Yes/Encry. Yes], for example, both authentication and encryption are enabled.
- Authent. Algorithm: Select the algorithm to be used for authentication ([MD5] or [SHA1]).
- Authentication Password: Enter the password for authentication (6 to 16 alphanumeric characters).
- Confirm: Enter the password again to confirm it.

- Encryption Algorithm: Only [DES] can be selected as the encryption algorithm.
- Encryption Password: Enter the password for encryption (6 to 16 alphanumeric characters).
- Confirm: Enter the password again to confirm it.

● **To enable/disable a user:**

- Select the button for the user you want to enable/disable under <Select> in the user list → click [User On/Off].



● **To edit a user:**

- Click the user name you want to edit in the user list in the User Settings page. The Edit User page is displayed.
- Edit the information as necessary → click [OK].

● **To delete a user:**

- Select the button for the user you want to delete under <Select> in the user list in the User Settings page → click [Delete]. The selected user is deleted.

Specifying the Context Settings for SNMPv3

Specify the context settings for SNMPv3 as described below.

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.

For help, see the screen shot in step 1 in “Enabling SNMPv3,” on p. 4-30.

The Settings page is displayed.

2 Click [SNMP Settings].

For help, see the screen shot in step 1 in “Enabling SNMPv3,” on p. 4-30.
The SNMP Settings page is displayed.

3 Click [Context Settings].

For help, see the screen shot in step 3 in “Specifying the User Information for SNMPv3,” on p. 4-31.
The Context Settings page is displayed.

4 Select the function.

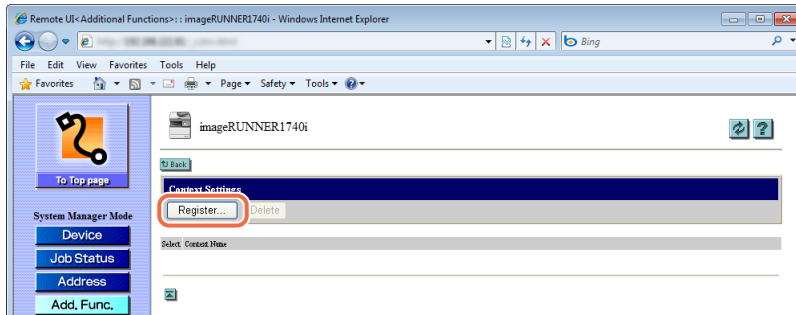
- To register a new context:



NOTE

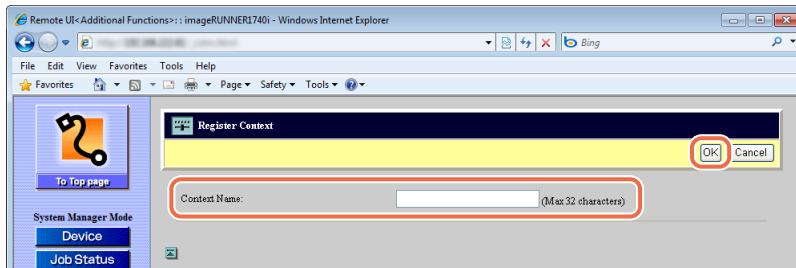
- You can register up to five contexts.
- A default context “NULL” is registered. It is not shown in the context list and cannot be deleted.

- Click [Register].



The Register Context page is displayed.

- Enter the context name up to 32 characters → click [OK].



● To edit a context:

- Click the context name you want to edit in the context list in the Context Settings page.
The Edit Context page is displayed.
- Edit the context name → click [OK].

● To delete a context:

- Select the button for the context you want to delete under <Select> in the context list in the Context Settings page → click [Delete].
The selected context is deleted.

Verifying SSL Server Certificates

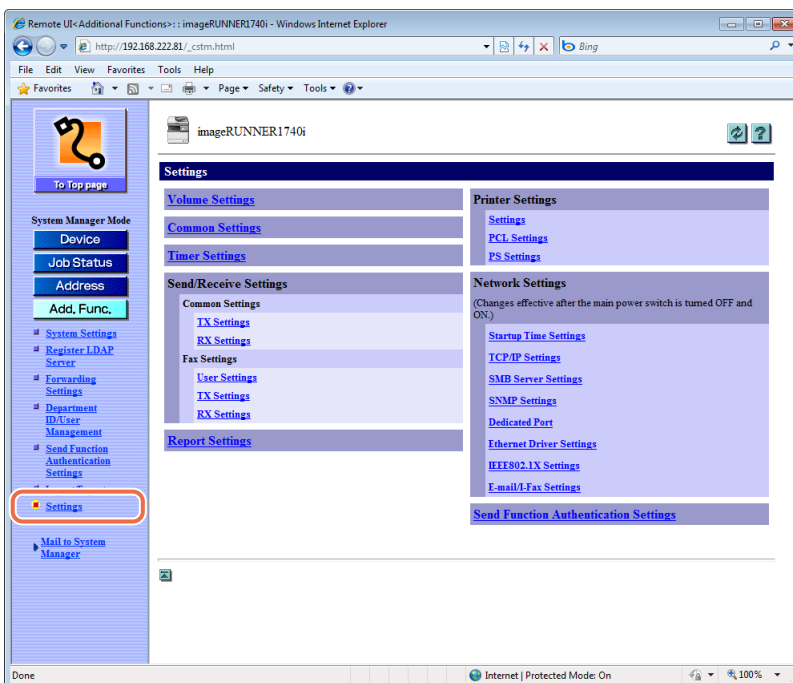
You can set the machine to check the validity of the SSL server certificate when the machine is receiving/sending data with POP/SMTP. The machine verifies the certificate by checking the expiration date, certificate chain, and as well as CN (Common Name).



IMPORTANT

The settings for the SSL server certificate verification are available only on the Remote UI (System Manager Mode).

1 Click [Add.Func.] → [Settings] in the [Add.Func.] menu.



The Settings page is displayed.

2 Click [E-mail/I-Fax Settings] on the page shown in step 1.

The E-mail/I-Fax Settings page is displayed.

3 Select the function.

- To set the machine to verify the SSL server certificate when receiving data with POP:

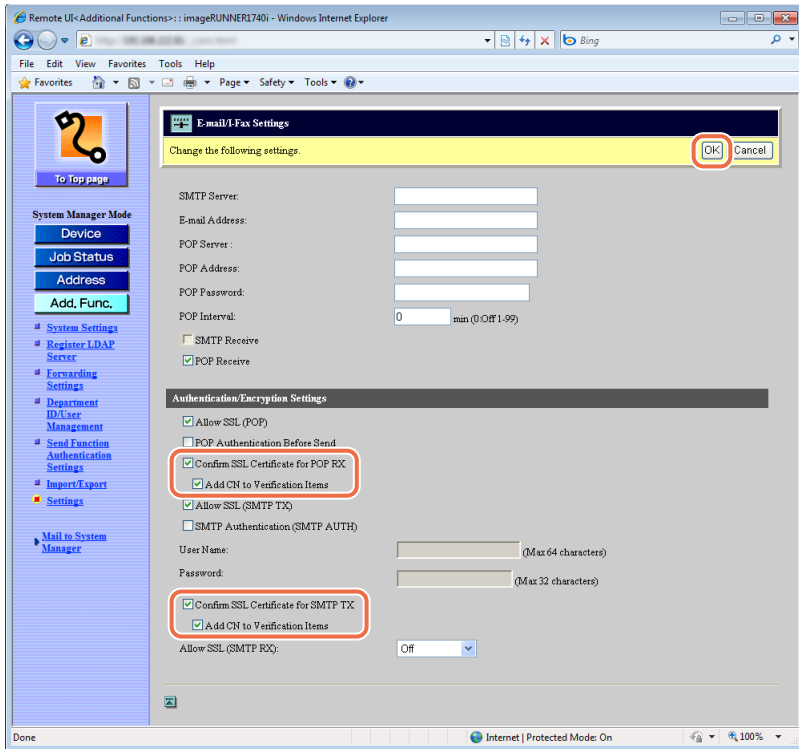
Select the check box for [Confirm SSL Certificate for POP RX].

To include the CN (Common Name) for the verification, select the check box for [Add CN to Verification Items].

- To set the machine to verify the SSL server certificate when sending data with SMTP:

Select the check box for [Confirm SSL Certificate for SMTP TX].

To include the CN (Common Name) for the verification, select the check box for [Add CN to Verification Items].



IMPORTANT

If you do not enable the SSL server certificate verification settings described above, SSL communication may be performed even with an invalid certificate.



NOTE

If the machine detects a problem with the certificate, communication will not be completed and the error message <SSL Error (POP)> or <SSL Error (SMTP Send)> (error code #0842 for the job log) will be displayed.

4 Click [OK] on the page shown in step 3.

5 Restart the machine.

Turn OFF the machine, wait at least 10 seconds, and then turn it ON.

Appendix

5

CHAPTER

This chapter includes the glossary and index.

Glossary	5-2
Index	5-6

Glossary

B

BOOTP

BOOTstrap Protocol. A protocol that enables a client machine to automatically obtain network setup information from a server over a TCP/IP network. BOOTP enables a client to automatically locate such information as the host name, domain name, and IP address, so that it is not necessary to enter these items manually.

bps

Stands for bits per second. The measure of transmission speed used in relationship to networks and communication lines.

C

Cookie

A file left on a user's computer when the user visits a Web site. A cookie allows the Web site to recognize the user on subsequent visits. Cookies are generally used to enable a user to automatically sign on to certain Web sites and to customize the features offered by such sites.

D

DHCP

Dynamic Host Configuration Protocol. A protocol which automatically specifies the network settings of a client on a TCP/IP network. Many of the settings required to set up TCP/IP, which is the standard protocol of the Internet, can be made automatically using DHCP.

F

FTP

File Transfer Protocol. A client-server protocol enabling a user to transfer files on one computer to and from another computer over a TCP/IP network. The File Transfer Protocol also governs the client program with which the user transfers files.

H

HTTP

Hypertext Transfer Protocol. The client-server TCP/IP protocol used on the World Wide Web for the transfer of HTML (Hyper Text Mark-up Language) documents across the Internet.

I

IEEE802.1X authentication

An authentication method that permits only supplicants (devices) authenticated by a RADIUS (Remote Authentication Dial-In User Service) server to connect to the network via an authenticator.

Internet Protocol (IP)

The underlying set of networking rules that describes how data is transmitted across the Internet. Internet Protocol enables data from one computer to be split into packets, and sent to another computer with a specific IP address.

IP address

Internet Protocol address. A network address used by IP (Internet Protocol) to specify a computer or device on the Internet. Currently, two versions of IP are in use: IPv4 and IPv6.

IPv4

Internet Protocol version 4. An IPv4 address is a 32-bit numeric address, usually written as four numbers delimited by periods. For example, '128.121.4.5'.

IPv6

Internet Protocol version 6. An IPv6 address is 128-bit long and consists of eight groups of four hexadecimal digits delimited by colons. For example, '2002:0db6:58b1:02c3:3308:7a2e:6309:2665'. In an IPv6 network, a computer or device can use multiple addresses, as represented by link local address, stateless address, etc.

L

LDAP

Lightweight Directory Access Protocol. A network protocol that enables you to locate organizations, individuals, and other resources, such as files and printers on a network, whether on the public Internet or on a corporate intranet.

P

PDF

Portable Document Format. The page description language used in Adobe Systems' Acrobat document exchange system, which is restricted neither by device nor resolution. PDF displays documents in a way that is independent of the original application software, hardware, and operating system used to create those documents. A PDF document can contain any combination of text, graphics, and images.

Protocol

A set of rules that govern the transmission of data across a network. Examples of protocols are DHCP, BOOTP, RARP, and TCP/IP.

Proxy server

A server that provides a cache of files available on remote servers that are slow or expensive to access. The term "proxy server" normally refers to a World Wide Web server that, upon receiving a URL, tries to supply the requested file from its cache. If the proxy server cannot locate the file in its cache, it obtains the file from the remote server, and saves a copy in its cache so that the next request can be obtained locally.

R

RARP

Reverse Address Resolution Protocol. A protocol which associates a network adapter address (MAC address) with an IP (Internet Protocol) address.

Remote UI

Remote User Interface. The Remote UI is software that enables you to perform operations, which are usually performed on the machine's control panel, using a Web browser (such as Microsoft Internet Explorer or Safari) over a network.

S

SSL

Secure Sockets Layer. A protocol that ensures security and privacy when transmitting private documents over the Internet.

SSL encryption

SSL uses two keys to encrypt data: a public key, which is known to "everyone," and a private or secret key, which is known only to the recipient of the message.

T

TCP/IP

Transmission Control Protocol/Internet Protocol. The protocol used to connect to the Internet or wide area networks.

U

URL

Uniform Resource Locator. A standard way of specifying the location of an object, usually a Web page on the Internet. The URL for a Web page would look something like this: "http://www.w3.org/default.htm". Here, "http:" indicates that a Web page is being accessed, "www.w3.org" is the address of the server containing the Web page, and "default.htm" is the file name under which the Web page is stored on the server.

A

- Add.Func. menu
 - (Additional Functions menu), 4-2, 4-26
- Additional Functions setting data
 - Exporting, 2-21
 - Importing, 2-23
- Address Book, 2-5
 - Deleting the destination, 2-10
 - Editing the destination, 2-9
 - Exporting, 2-12
 - Importing, 2-13
 - Registering a new destination, 2-7
 - Registering a new Group Address, 2-8
- Authorized Send, 4-17

B

- BOOTP, 5-2
- bps, 5-2
- Buttons on the Remote UI, 1-6

C

- CA certificate, 2-25
- Cookie, 5-2

D

- Department ID
 - Deleting, 3-9
 - Editing, 3-9
 - Registering, 3-7
- Department ID Management, 3-2
 - Enabling, 3-2
- DHCP, 5-2

E

- End-User Mode, 1-10

F

- Forwarding Settings, 4-14
 - Deleting the Forwarding Condition, 4-16
 - Editing the Forwarding Condition, 4-16
 - Forwarding Documents without specific conditions, 4-15
 - Registering a Forwarding Condition, 4-14
- FTP, 5-2

H

- HTTP, 5-3

I

- IEEE802.1X authentication, 2-25, 5-3
- Internet Protocol (IP), 5-3
- IP address, 1-4, 1-9, 5-3
- IPv4, 5-3
- IPv6, 5-3

J

- Job Logs, 2-4

K

- Key and certificate, 2-25

L

- LDAP search attributes, 4-13
- LDAP server, 4-10
 - Deleting, 4-12
 - Editing, 4-12
 - Registering, 4-11
- Logon mode, 1-5, 1-10
 - End-User Mode, 1-5
 - System Manager Mode, 1-5

M

- Machine settings, customizing, 4-26

P

- PDF, 5-4
- Print Job, managing, 2-2
- Protocol, 5-4
- Proxy server, 5-4

R

- RARP, 5-4
- Remote UI, 5-4
- Restrict the Send function, specifying, 4-8

S

- SNMPv3, 4-29
- SSL, 5-4
 - SSL encryption, 5-4
 - SSL server certificate, 4-37
- System Manager ID, specifying, 4-9
- System Manager Mode, 1-10
- System Password, specifying, 4-9
- System requirements, 1-7
 - OS (Macintosh), 1-7
 - OS (Windows), 1-7
 - Web browser (Macintosh), 1-7
 - Web browser (Windows), 1-7
- System Settings, specifying, 4-5

T

- TCP/IP, 5-5
- Top page of the Remote UI, 1-4

U

- URL, 1-9, 5-5
- User ID
 - Deleting, 3-14
 - Editing, 3-13
 - Registering, 3-10
- User Management, 3-2
 - Enabling, 3-2
- User Management data
 - Exporting, 2-14
 - Importing, 2-15
 - Resetting, 2-17

W

- Web browser, 1-4, 1-7, 1-9



CANON INC.

30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo 146-8501, Japan

CANON U.S.A., INC.

One Canon Plaza, Lake Success, NY 11042, U.S.A.

CANON CANADA INC.

6390 Dixie Road Mississauga, Ontario L5T 1P7, Canada

CANON EUROPA N.V.

Bovenkerkerweg 59-61 1185 XB Amstelveen, The Netherlands

(See <http://www.canon-europe.com/> for details on your regional dealer)

CANON LATIN AMERICA, INC.

703 Waterford Way Suite 400 Miami, Florida 33126 U.S.A.

CANON AUSTRALIA PTY. LTD

1 Thomas Holt Drive, North Ryde, Sydney, N.S.W. 2113, Australia

CANON CHINA CO., LTD

15F Jinbao Building No.89 Jinbao Street, Dongcheng District, Beijing 100005, China

CANON SINGAPORE PTE. LTD.

1 HarbourFront Avenue #04-01 Keppel Bay Tower, Singapore 098632

CANON HONGKONG CO., LTD

19/F., The Metropolis Tower, 10 Metropolis Drive, Hunghom, Kowloon, Hong Kong