RICOH

RICOH Streamline NX

Operating Instructions

Administrator's Guide

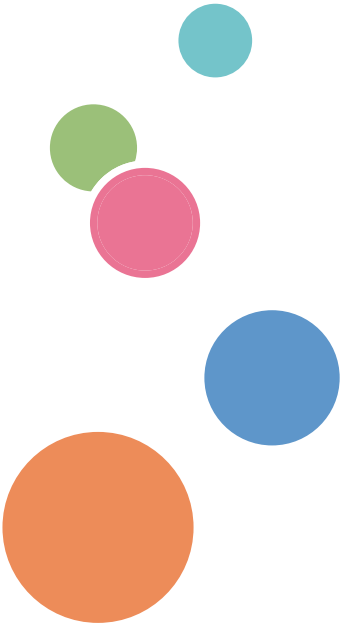


TABLE OF CONTENTS

3. Managing Devices

4. Managing Authentication Information

5. Managing Printing Functions

6. Managing Document Delivery Functions

7. Using RICOH Streamline NX on a Mobile Device

8. Managing Servers

9. Managing System Operation and Logs

10. List of Setting Items

11. Appendix

Guides for This Solution

The following guides are available for RICOH Streamline NX:

Installation Guide (PDF)

This guide is for the administrator. It describes how to install, uninstall, and activate the system and how to configure the database. It also describes how to install RICOH Streamline NX PC Client.

Administrator's Guide (PDF/HTML)

This guide is for the administrator. It describes the system workflow and how to operate the Management Console. The following functions are described:

- Device management
- User management
- Print management
- Capture management
- Server management
- Log management

User's Guide (PDF/HTML)

This guide is for general users. It describes how to scan a document using the operation screen of the device. It also describes the Send to Email, Send to Folder, and Send to FTP functions and how to use the mobile app.

RICOH Streamline NX PC Client Operation Guide (PDF/HTML)

This guide is for general users. It describes how to configure RICOH Streamline NX PC Client installed on a client computer and how to perform Client Secure Print and Dynamic Delegation Print.

Reporting and Dashboards Guide (PDF/HTML)

This guide is for administrators and general users. It describes the report settings and report types that can be generated within the Management Console.

Important Information about Device Configuration (PDF)

This guide is for administrators. It describes the management extension function for device settings.

Migration Guide: For Device Manager NX (PDF)

This guide is for the administrators. It describes how to execute the migration of data from the existing product to RICOH Streamline NX.

How to Read This Manual

Symbols

This manual uses the following symbols:

Important

Indicates points to pay attention to when using the machine, and explanations of likely causes of paper misfeeds, damage to originals, or loss of data. Be sure to read these explanations.

Note

Indicates supplementary explanations of the machine's functions, and instructions on resolving user errors.

[ ]

Indicates the names of keys on the machine's display or control panels.

Important

To the maximum extent permitted by applicable laws, in no event will the manufacturer be liable for any damages whatsoever arising out of failures of this product, losses of documents or data, or the use or non-use of this product and operation manuals provided with it.

Make sure that you always copy or have backups of important documents or data. Documents or data might be erased due to your operational errors or malfunctions of the machine. Also, you are responsible for taking protective measures against computer viruses, worms, and other harmful software.

In no event will the manufacturer be responsible for any documents created by you using this product or any results from the data executed by you.

Contents of this manual are subject to change without prior notice.

Revision History

Date	Revision No.	Revision Details
6/26/2017	1.0.0	First release of document
11/6/2017	1.0.1	Document for 3.0.2 software release
12/22/2017	1.1.0	Document for 3.1.0 software release

Terminology

This section describes the terms used in this guide.

Authentication

The devices (MFPs and laser printers) that are compatible with RICOH Streamline NX support user authentication. The user must log in to the device when authentication is enabled by the administrator.

Client computer

This is a computer other than a server that uses the RICOH Streamline NX system. It accesses the Management Console using a web browser, manages printing using RICOH Streamline NX PC Client, and manages USB-connected devices using USB Agent.

Workflow

A workflow is created by the system administrator and represents the flow of various processes that are related to scanning and delivery of documents. The methods of conversion and delivery are configured according to the document process requirements that are specified by the administrator. For example, a user in the sales department can use the Send to Email function to send a proposal document to a potential client via e-mail. Another user in the legal department can use the Send to Folder function to keep a record of the communication data with a customer and store it in an archive.

Core Server

RICOH Streamline NX consists of a Core Server and Delegation Servers. The Core Server is the server at the center of the RICOH Streamline NX system. It manages the Delegation Servers.

Delegation Server

The Delegation Server processes the printing, document delivery, and device management functions. Depending on the size of the system and how the various functions are used, multiple Delegation Servers can be created to distribute the load.

MIE Server

This server is required to use a mobile app and submitting a print job from a mobile device.

The MIE server connects to a Delegation Server and links with mobile devices.

RICOH Software Server

This refers to the server that is operated by RICOH and can be accessed via the Internet. From RICOH Software Server, the user can download the suitable Device Application or SDK Platform and install it on the device being used by the user.

Access account

This refers to the information required to allow or restrict access to the device. Depending on the type of the account, a user ID and password are required. To manage devices in RICOH Streamline NX, use the following access accounts:

- SNMP account: Use this account to search for a device or obtain information from a device.
- Device administrator account: Use this account to modify the configuration of a device.
- SDK account: Use this account to manage the software that is installed on a device.

Administrator

This refers to the administrator who configures the devices or manages the related information. Depending on the device that is being used, there are different types of administrators, such as a device administrator who configures the devices or a user administrator who manages the user information. In this guide, these are all referred to as the “administrator” in general. Read the word as the appropriate administrator according to the device in use or the configuration context.

Device

This refers to a printer or MFP on the network. In this guide, printers and MFPs are referred to as "devices".

To use the printing and document delivery functions of RICOH Streamline NX, select a Ricoh MFP or printer. For a list of supported models, see "List of Supported Models and Functions", Administrator's Guide.

Discovery

This function performs a search over a network for a device that matches the specified criteria and registers the discovered device in RICOH Streamline NX.

Polling

This function obtains the information such as the device status and remaining amount of consumables from the device that has been discovered over a network.

User

This refers to a user who uses the device to perform operations such as printing and scanning.

Smart Operation Panel

Smart Operation Panel is a 10.1-inch full-color touch panel which allows you to operate the device by touching, flicking and dragging on the operation panel. For the models purchased in Japan, it is called "MultiLink-Panel".

Streamline NX Embedded application

This refers to the RICOH Streamline NX specific embedded application.

Device Application

This refers to the Device Application except RICOH Streamline NX specific embedded application.

Trademarks

Adobe, Acrobat, PostScript, and PostScript 3 are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Gmail, Google Drive, G Suite, and Android are trademarks of Google Inc.

AppleTalk, iPad, iPhone, iPod, iPod touch, Macintosh, OS X, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries.

AirPrint and the AirPrint logo are trademarks of Apple Inc.

Dropbox is a trademark of Dropbox, Inc.

Entrust® is a trademark of Entrust, Inc.

Ethernet 241 is a trademark of RF IDeas, Inc.

Firefox® is a registered trademark of the Mozilla Foundation.

FMAudit™ is a trademark of eCommerce Industries, Inc.

LRS is a registered trademark of Levi, Ray & Shoup, Inc.

Microsoft, Windows, Windows Server, Windows Vista, Windows Phone, SharePoint, Office 365, Internet Explorer, Excel, and SQL Server are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

Netware, IPX, IPX/SPX, are trademarks of Novell Inc.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

PCL® is a registered trademark of Hewlett-Packard Company.

RightFax is a trademark of OpenText Corporation.

Thawte® is a trademark of Symantec Corporation or its affiliates in the U.S. and other countries.

VeriSign™ is a trademark of VeriSign, Inc.

The proper names of the Windows operating systems are as follows:

- The product names of Windows Vista are as follows:

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

  Microsoft® Windows Vista® Home Basic

  Microsoft® Windows Vista® Enterprise
- The product names of Windows 7 are as follows:

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

Microsoft® Windows® 7 Enterprise

- The product names of Windows 8.1 are as follows:

  Microsoft® Windows® 8.1

  Microsoft® Windows® 8.1 Pro

  Microsoft® Windows® 8.1 Enterprise

- The product names of Windows 10 are as follows:

  Microsoft® Windows® 10 Home

  Microsoft® Windows® 10 Pro

  Microsoft® Windows® 10 Mobile

  Microsoft® Windows® 10 Enterprise

  Microsoft® Windows® 10 Education

  Microsoft® Windows® 10 Mobile Enterprise

- The product names of Windows Server 2008 R2 are as follows:

  Microsoft® Windows Server® 2008 R2 Standard

  Microsoft® Windows Server® 2008 R2 Enterprise

  Microsoft® Windows Server® 2008 R2 Datacenter

- The product names of Windows Server 2012 are as follows:

  Microsoft® Windows Server® 2012 Essentials

  Microsoft® Windows Server® 2012 Standard

  Microsoft® Windows Server® 2012 Datacenter

- The product names of Windows Server 2012 R2 are as follows:

  Microsoft® Windows Server® 2012 R2 Essentials

  Microsoft® Windows Server® 2012 R2 Standard

  Microsoft® Windows Server® 2012 R2 Datacenter

- The product names of Windows Server 2016 are as follows:

  Microsoft® Windows Server® 2016 Datacenter

  Microsoft® Windows Server® 2016 Standard

  Microsoft® Windows Server® 2016 Essentials

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

Introduction

Thank you for purchasing RICOH Streamline NX.

RICOH Streamline NX offers a total solution for secure and large-scale, integrated management of devices. In addition to providing remote management of device settings, monitoring of devices, and output of reports, RICOH Streamline NX can also expand the print and scan functionality of devices.

The expanded functionality of the devices can improve user convenience and administrator operation efficiency for management cost savings. The RICOH Streamline NX system also offers the use of cards, PINs, and other personal authentication functions to strengthen the security of devices and reduce the risk of information leaks.

In addition, RICOH Streamline NX can be used to monitor and manage network devices. The system can immediately detect a problem on a connected device located anywhere around the world to help minimize downtime. In addition, the system can apply initial settings collectively and remotely on a large scale to newly installed devices.

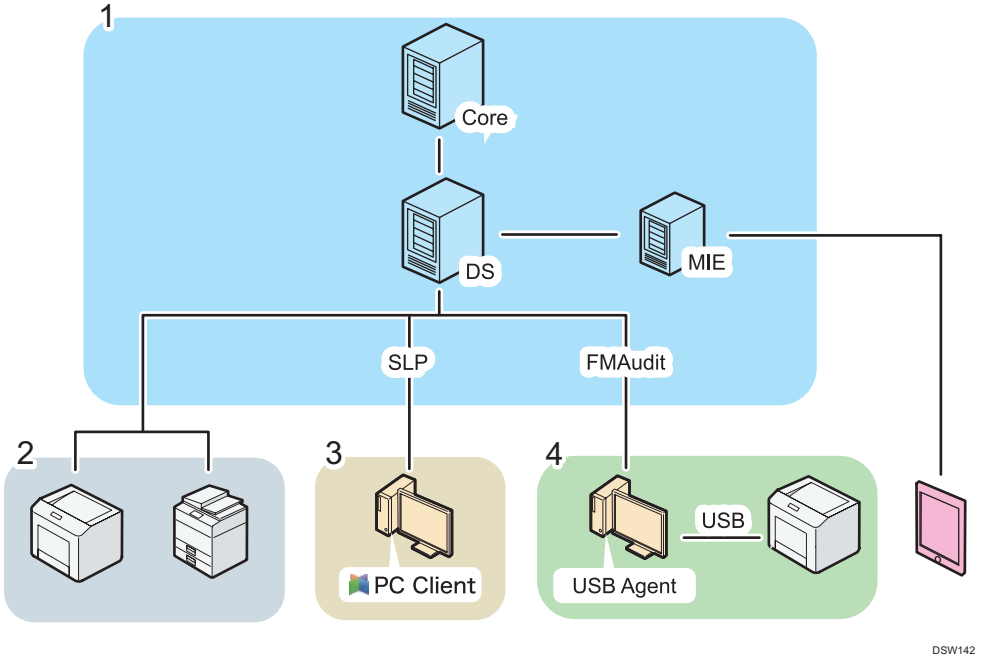
Administrators can manage all connected devices centrally through a unified web interface without having to install special software to the client computer.

Note

- @Remote is a system in which Ricoh manages your devices. Activation of a @Remote license can further reduce internal device management costs.
- RICOH Streamline NX requires internet access to communicate with the RICOH Software Server to obtain software and firmware updates and to the RICOH Activation Server to perform product activation. If necessary for security purposes, you can restrict the use of RICOH Streamline NX so that it does not access the internet beyond the firewall.

Installation Workflow Summary

The RICOH Streamline NX system consists of servers, devices, and client computers. This section describes an overview of the system and the workflow for starting operations.



1. **RICOH Streamline NX servers**

   There are three types of servers in this system: a Core Server, Delegation Servers, and MIE servers.

   Core Server

   This server is at the center of the RICOH Streamline NX system. The administrator accesses the Core Server from a client computer to manage the entire system.

   Delegation Server (DS)

   These servers are managed by the Core Server. The Delegation Servers are directly responsible for all processing related to the devices, including processing of print jobs, image conversion and delivery of scanned documents, and processing of information obtained from the devices.

   You can install a Delegation Server separately so as not to reside with other functions.

   In addition, SLP enables the RICOH Streamline NX PC Client to detect Delegation Servers.

   MIE server

   This server is required to use a mobile app and submitting a print job from a mobile device. The MIE server connects to a Delegation Server and links with mobile devices.

2. **Managed devices**

   You can install the Device Applications to Ricoh devices only.

   To ensure stronger security via user authentication and enable advanced printing and capturing functions, install the Device Applications to compatible Ricoh devices.

Note

- For a list of models that support the Device Applications, see page 23 "List of Supported Models and Functions".
- For details, see page 109 "Managing Device Applications".

3. **RICOH Streamline NX PC Client**

   Installing RICOH Streamline NX PC Client on a client computer enables the user to store secure print jobs to a client computer and collect accounting information to the server.

4. **FMAudit**

   If you select the FMAudit device monitoring engine option when installing the Delegation Server, you can manage USB-connected devices.

Note

- To print from a smart device, the PCL emulation must be supported on the printing device.
- The number of devices that can be processed by one Core Server or Delegation Server varies depending on server performance and processing load. The following is a guide. For details, contact your service representative.
  - Core Server: A single Core Server can manage up to approx. 100,000 devices, and up to 250 Delegation Servers.
  - Delegation Server: Each Delegation Server can perform processing for the following number of devices:
  - Polling: approximately 10,000 devices
  - Device management: 5,000 devices
  - Capturing and printing: 1,000 devices

List of Supported Models and Functions

RICOH Streamline NX identifies devices by MAC address, serial number, and vendor name (converted from model name). Detected devices are displayed on the device list with an icon according to the type of device. For the relationship between the device icons and the supported functions, see the tables below.

Type of Device	Device Icon	Supported Functions
RICOH Device (2012 models and later)		• Device monitoring, device configuration management*1 • Device authentication*2 • Secure printing using Device Application*2 • Document scanning using Device Application*2 • Direct printing • Client Accounting printing
RICOH Device (2007-2011 models)		
RICOH device (2000-2006 models)		• Device monitoring*1 • Secure printing using mobile app • Direct printing • Client Accounting printing
RICOH GelJet device		
Other RICOH device		
RICOH device (Model with external controller)		
Non-RICOH device		
USB-connected device		• Device monitoring*1 • Direct printing • Client Accounting printing

*1 For details on supported functions, see the table below.

*2 Devices with SDK-J are supported.

Note

- Depending on the models, you may not be able to use some functions listed in the "Supported Functions" column. For details, contact a RICOH service representative.

Functions Supporting Device Monitoring and Device Configuration Management

Type of Device	Device Icon	Supported Functions
RICOH device (2012 models and later)		• Discovery • Get basic information of device • Counter Polling • Detailed Counter Polling • Detailed User Counter Polling • Basic device settings • Advanced device settings • Address book settings • Energy saver mode settings
RICOH device (2007-2011 models)		• Discovery • Get basic information of device • Counter Polling • Detailed counter • User counter • Basic device settings • Address book settings • Energy saver mode settings
RICOH MFP (2000-2006 models)		• Discovery • Get basic information of device • Counter Polling • Detailed counter
RICOH GelJet device		• Discovery • Get basic information of device (partial support) • Detailed counter
Other RICOH device		• Discovery • Get basic information of device (partial support) • Detailed counter

Type of Device	Device Icon	Supported Functions
RICOH device (model with external controller)		• Discovery • Get basic information of device (partial support) • Counter Polling (partial support)
Non-RICOH device		• Discovery • Get basic information of device (partial support) • Detailed counter (partial support)

List of Licenses and Functions

To use the RICOH Streamline NX functions, you must purchase a license. Choose from the base license (required) for use of the basic functions or the advanced license (optional) for activation of other functions. Purchase and activate the license to best suit your needs.

Important

- **In addition to a base or advanced license, you are also required to have a maintenance service license with an annual subscription.**

List of Licenses

The tables below show the supported system functions according to the license type.

- Base License

License Type	Supported Functions	License Unit
Base	• Device List • System Setup • Discovery • Report • Dashboard • Driver distribution (Basic)	Device

- Advanced License

License Type	Supported Functions	License Unit
Print Management	• Direct printing • Secure printing	Device
Scan & Capture Device	• Document scanning and delivery • Destination Connectors	Device
Scan & Capture Input Connector	• Monitor Folder • Mobile	Core server
Scan & Capture Process Connector	• Barcode Separator/Index • Zone OCR	Core server

License Type	Supported Functions	License Unit
RICOH Streamline NX PC Client	• Print rules • Secure printing • Delegation printing • Client Accounting	Client computer
@Remote Connector	• @Remote service	Device
Driver Distribution	• Driver distribution (Advanced)	Device
Extended Item Setting	• SLNX Management Extension	Device
Trial	• All functions	Unlimited

Supported Functions Reference

For details on the system functions that can be activated with the base and advanced licenses, see the reference pages below.

Supported Functions	Reference
Device List	page 53 "Managing Devices"
System Setup	page 518 "Server Settings"
Discovery	page 76 "Adding a Device to the Device List"
Report	page 633 "Reports"
Dashboard	page 577 "Dashboards"
Direct printing	page 182 "Device Direct Printing"
Secure printing	page 180 "The Secure Printing Function"
Document scanning and delivery	page 219 "Managing Document Delivery Functions"
Destination Connectors	page 222 "Available Destination Connectors"
Monitor Folder	page 186 "Features of Secure Printing Functions"
All Process Connectors	page 224 "Available Process Connectors"

Supported Functions	Reference
Print rules	page 199 "Configuring Print Rules"
Delegation printing	page 186 "Features of Secure Printing Functions"
Client Accounting	page 184 "Client Accounting"
@Remote service	page 128 "Monitoring Devices Using the @Remote Function"
Driver distribution	page 133 "Distributing Printer Drivers"
Advanced device settings	page 102 "Managing the Device Settings"

1. Workflow

RICOH Streamline NX is an integrated management system comprising servers and devices. With RICOH Streamline NX, you can monitor and manage devices, scan and deliver documents, and use advanced printing functions to manage information and costs securely in a network environment.

Workflow for Configuring the Initial Settings

After the installation of RICOH Streamline NX is completed, configure the basic system settings as shown below.

1. ▶ **Activating RICOH Streamline NX**

   Use the product keys of RICOH Streamline NX to activate the product. The activation can be performed either online or offline.

   Note

   - For details, see “Activating RICOH Streamline NX”, Installation Guide.

2. ▶ **page 154 "Configuring an External Authentication Server"**

   Configure the authentication profile to communicate with the external LDAP or Kerberos database. This allows the creation, synchronization, and group searches of external user accounts in the database.

3. ▶ **page 160 "Managing User Roles and Privileges"**

   To ensure efficient operations of a large-scale system, assign each user an appropriate role and limit the operations the user can perform according to his or her job duties. For example, the Device Admin role can read and write all information related to a device, but the Report User role can only generate and display reports.

   Use roles and privileges to configure which functions of RICOH Streamline NX each user can access.

4. ▶ **Specifying the Destination E-mail Address of Notifications**

   Register the destination e-mail addresses for delivery of notification messages.

   Note

   - For details, see page 535 "Email Address".

5. ▶ **Configuring the Network Settings**

Configure the proxy server, SSL communication, e-mail server, recipients of the system warnings, and FTP/SFTP service.

Note

- For details about the setting items, see page 522 "Networking".

6. ▶ **Configuring the Management Settings of the System Data**

Configure the settings related to system data storage such as the data storage period, notification when the available space is low, and grace period before data is deleted.

Note

- For details about the setting items, see page 527 "System Data Management".

Note

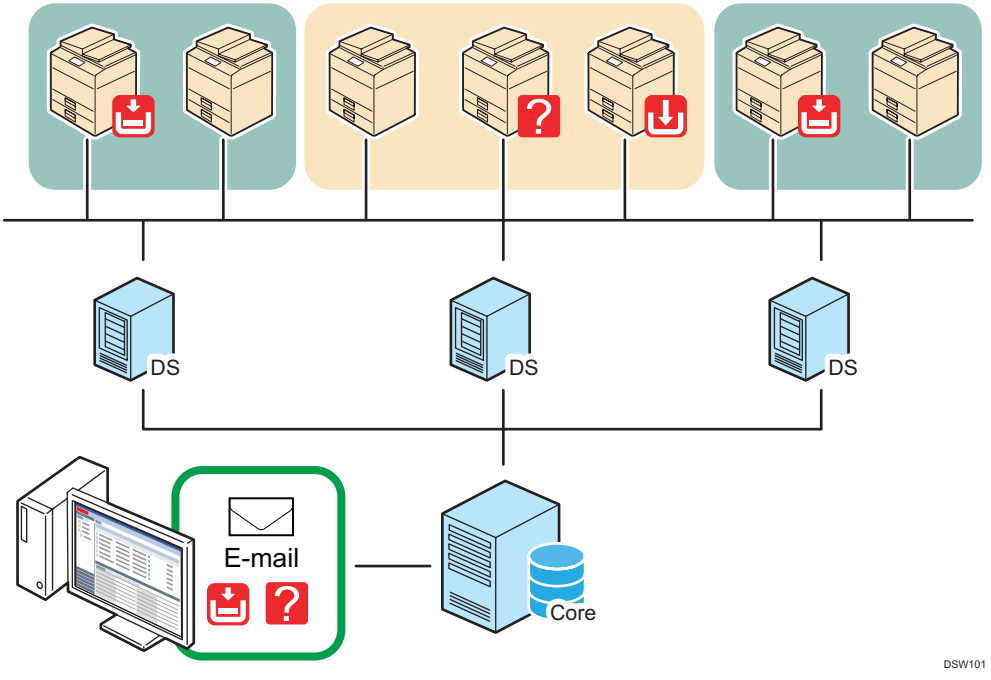
- By using the Configuration Wizard, you can display each configuration screen from the Management Console. For details about the Configuration Wizard, see page 48 "Screen Configuration of the Management Console".

Device Management Function Workflow

Monitoring the Device Status

With RICOH Streamline NX, you can monitor the status of devices over a network. You can obtain information such as the current device status, various logs, and the remaining amount of consumables from the devices that are being monitored.

You can also receive a notification via e-mail and have a program executed if a device error occurs or a device status changes. In addition, you can collect logs of these events.



1. ▶ **page 71 "Organizing the Device List"**

Configure the access account to enable RICOH Streamline NX to obtain information from devices or apply settings to devices. Use the access account that is registered to RICOH Streamline NX to search for devices in a network and then add the discovered devices to the device list.

2. **page 76 "Adding a Device to the Device List"**

Devices are automatically grouped by IP address, host name, manufacturer, or model. You can also organize devices into categories or groups manually, such as by floor or department. Group devices by the installation locations or organizational units for easier device management.

3. **page 89 "Checking the Device Status"**

By obtaining the device information and monitoring devices regularly, you can track the device status and be notified when errors occur and when the amount of consumables is low.

4. **page 94 "Notifying the Device Status by E-mail"**

You can receive a notification by e-mail when the status of a device changes or any new device is detected.

5. **page 114 "Managing Device Logs"**

The device logs are collected for tracking and understanding the operational status of the devices.

6. **page 120 "Managing the Power Status of Devices"**

You can change the energy saver mode of a device according to a configured schedule. For example, you can configure a schedule on a device to enter the energy saver mode at 7:00 PM every night and recover from the energy saver mode at 6:00 AM every morning.

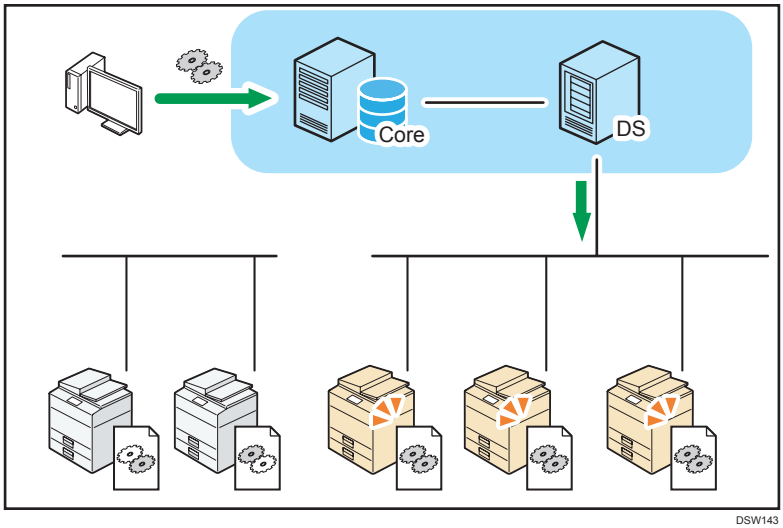
Note

- By using the Configuration Wizard, you can display each configuration screen from the Management Console. For details about the Configuration Wizard, see page 48 "Screen Configuration of the Management Console".

Managing the Address Book and Settings of Devices in a Batch

When adding a new device, you must configure the address book, network, paper, printer and other settings. On standalone devices, you would have to use Web Image Monitor or the device operation screen to configure each of the settings.

With RICOH Streamline NX, you can apply the required operational settings to multiple devices. For example, when multiple devices are added at various locations, the company headquarters in charge of managing the devices can apply the settings for all devices over the network at the same time. This enables quick and efficient device management.



1. ▶ **Creating a Template**

A template is a standard file that contains the setting values to be applied to a device. There are several types of templates each with a different purpose. For details, see the following:

page 102 "Managing the Device Settings"

page 106 "Updating the Firmware"

page 112 "Managing the Address Book"

page 114 "Managing Device Logs"

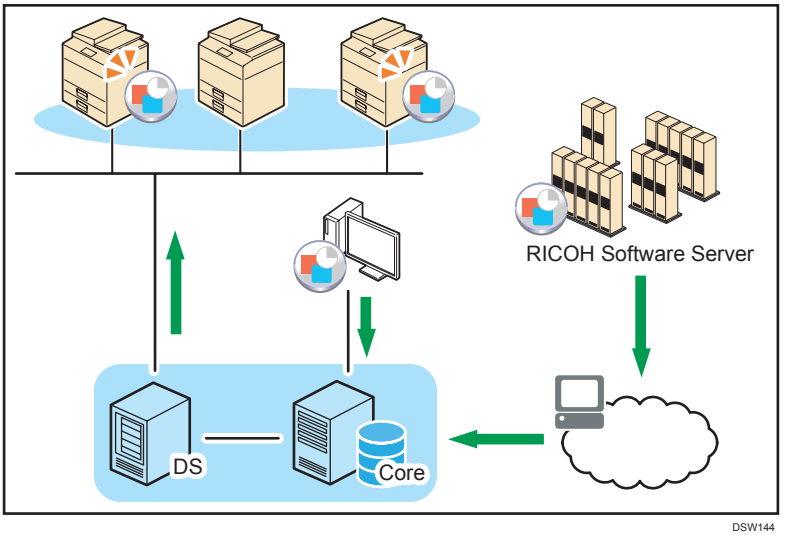
2. ▶ **page 116 "Registering a Template to a Task"**

Register the schedule, method, and target device to which to apply the created template as tasks. A template can be executed only after it is registered as a task. There are several types of tasks each with a different purpose. For details, see the following:

- page 116 "Registering a Template to a Task"

Managing the Embedded Functions of the Device

Use RICOH Streamline NX to manage the applications used for advanced device functions. Upload the Device Applications to the RICOH Streamline NX server, and then install them on a device, or download the latest version of an application from the server and update the applications on the device.



1. ▶ **Creating a Template**

A template is a standard file that contains the setting values to be applied to a device. Specify the type of extended application to be applied to the device and the method of obtaining the Device Applications. For details, see the following:

- page 109 "Managing Device Applications"
- page 108 "Managing the SDK/J Platform"

2. ▶ **page 116 "Registering a Template to a Task"**

Register the schedule, method, and target device to which to apply the created template as tasks. A template can be executed only after it is registered as a task. There are several types of tasks each with a different purpose. For details, see the following:

- page 116 "Registering a Template to a Task"

Note

- Configuration templates are very effective when used in combination with discovery tasks. For example, if you run a scheduled task that discovers new devices, then run a task that automatically moves the new devices to a particular category or group (based upon defined characteristics), you can then run a task that automatically applies a Standard Device Preferences template to the discovered devices. The template can contain location-specific information such as SMTP server address, LDAP server address and global fleet-specific settings. The template can also contain device function settings (print, scan, fax, copy), etc.

Installing a New Device or Relocating/Replacing a Device

This section describes the workflow for installing new devices or relocating or replacing existing devices.

Note

- When replacing an old device with a new one, perform the operation described in "Disposing of a Device", and then "Installing a New Device".

Installing a new device

1. **Connecting the Device to the Network**

   Specify the IP address of the device and connect the device to the hub using an Ethernet cable so that RICOH Streamline NX can detect the device.

   For details, see the operation manual of the device, or contact a RICOH service representative.

2. **page 76 "Adding a Device to the Device List"**

   Configure the access account to enable RICOH Streamline NX to obtain information from devices or apply settings to devices. Use the access account that is registered to RICOH Streamline NX to search for devices in a network and then add the discovered devices to the device list.

3. **Installing Streamline NX Embedded Applications on the Device**

   Create a task for Streamline NX Embedded Applications.

   The template for installing Streamline NX Embedded Applications is preset in the system. Register the template and perform the task.

   For details, see page 116 "Registering a Template to a Task".

4. **Confirming the Device Operations**

   Make sure that you can log in to the device from the control panel of the device. As necessary, make sure that the printing and document delivery functions work as intended.

Relocating the device

1. ▶ **Changing the IP Address of a Device**

   If it is necessary to change the IP address of the device on relocating, change the IP address from the control panel of the device after relocation is conducted.

   For details, see page 387 "Changing the IP Address of a Server or Device", or contact a RICOH service representative.

2. ▶ **Registering the New IP Address of the Device in the System**

   In the device list on the Management Console, perform Discovery or edit the IP address to register the new IP address of the device. For details, see the following:

   - page 77 "Searching for Devices"
   - page 80 "Adding a Device to the Device List"

3. ▶ **Confirming the Device Operations**

   Make sure that you can log in to the device from the control panel of the device. As necessary, make sure that the printing and document delivery functions work as intended.

Disposing of a device

Important

- **Streamline NX Embedded Application license is disabled and can be used on another device only when the Device Application is uninstalled using the following procedure. The license becomes invalid when the Device Application is uninstalled from Web Image Monitor or the device operation panel.**

1. ▶ **Preparing to Uninstall Streamline NX Embedded Applications**

   Create a template to uninstall Streamline NX Embedded Applications.

   For details, see page 109 "Managing Device Applications".

2. ▶ **Uninstalling Streamline NX Embedded Applications**

   Create a task for the template created in Step 1 and execute the task against the device to be deleted.

   For details, see page 116 "Registering a Template to a Task".

3. ▶ **page 82 "Deleting a Device from the Device List"**

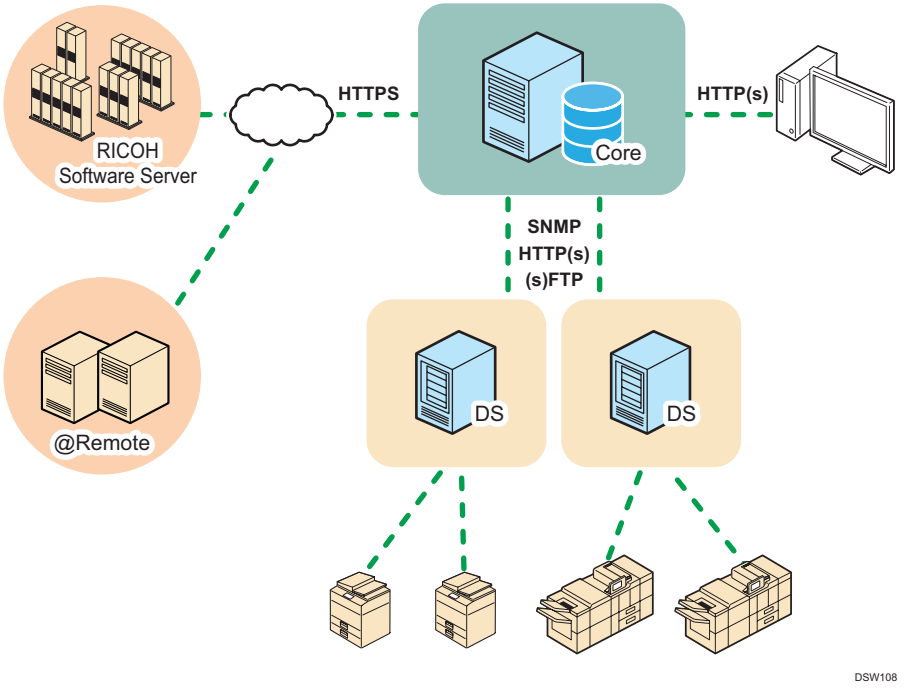
Delete the device from the device list on the Management Console.

4. ▶ **Disposing of a Device**

Dispose of the device according to the procedure specified in laws or regulations or follow the necessary procedures for recycling. For details, contact a RICOH service representative.

Using the @Remote Function

@Remote is an optional function that connects to @Remote Center via the Internet and monitors the status of devices on a network in real-time.



1. ▶ **Use the advanced license product key to activate the @Remote function**

Use the product key of the advanced license to activate the @Remote function. Perform the activation either online or offline.

Note

- For details about activating the product, see “Activating RICOH Streamline NX”, Installation Guide.

2. **▶ page 128 "Configuring the Connection Settings between @Remote Center and Delegation Servers"**

Configure the settings for connecting to @Remote center.

3. **▶ page 128 "Selecting the Information to Be Sent to @Remote Center"**

Select the information to be transmitted to @Remote center.

4. **▶ page 129 "Configuring the Method and Frequency to Send Information to @Remote Center"**

Configure the method for transmitting the device list information to @Remote center and the update interval.

Managing the Users

All functions in RICOH Streamline NX use authentication to identify the user. By properly configuring the user authentication function, you can better manage the operational cost of the devices and improve your business efficiency.

For example, you can set the limit on the number of color prints or prohibit use of the scanner function, thereby reducing print costs and preventing the risk of information leaks.

1. **▶ page 157 "Creating and Importing Users"**

It is necessary to connect to the external server using LDAP or Kerberos protocol to manage users in an external server. In addition, you can create local user accounts when local authentication is available.

2. **▶ page 172 "Managing User Information"**

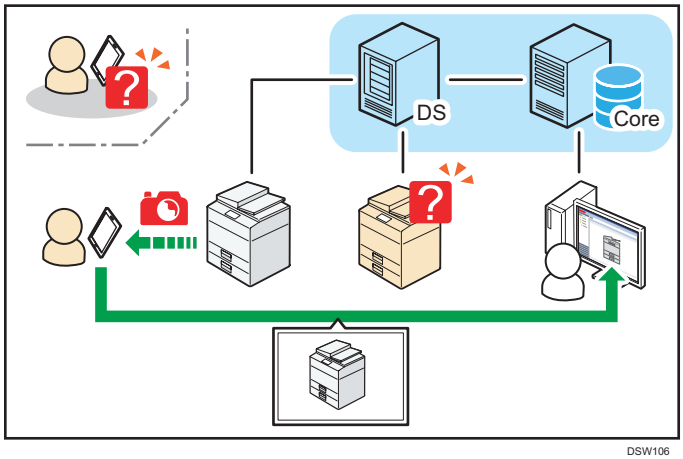
Associate the items that are required for operating the system, such as the group, department, and card information, with each user.

Note

- By using the Configuration Wizard, you can display each configuration screen from the Management Console. For details about the Configuration Wizard, see page 48 "Screen Configuration of the Management Console".

Monitoring Devices with a Mobile App

RICOH Streamline NX has a device management application for iOS, Android, and Windows Phone. The RICOH Streamline NX Device Manager app can be downloaded from the app store. With the device manager app, the administrator can search for devices and monitor the device status (device errors, out of toner, out of paper). The mobile app can also be used to register photos taken by the camera in the device properties. The device management app also supports SSL to ensure secure communication with devices.



Note

- Before starting to use the mobile app, be sure to register devices using the workflow described in page 31 "Monitoring the Device Status".

1. **page 374 "Configure the Initial Settings of the RICOH Streamline NX Device Manager App"**

   Start the mobile app and configure the initial settings such as the destination server and port number.

2. **page 375 "Logging in to the RICOH Streamline NX Device Manager App"**

   Log in to a device from the mobile app, and check the device status.

Document Delivery Function Workflow

This section describes the workflow to set up the system so that users can use the document delivery function.

Sending Scanned Documents and Received Faxes over a Network

You can deliver to a specified destination the document that has been a scanned document or a received fax on a device. You can also convert documents to image, PDF, Word, and Excel files, and send them by e-mail, and store to a shared folder. Use these functions for the following:

- Streamlining the operational workflow for improved productivity
- Digitizing paper documents and sending them over a network to promote paperless operations, and thereby reducing paper consumption and storage costs
- Digitizing documents to distribute important information immediately

1. **Using the Advanced License for Activation**

   Activate the software with a Capture License to enable scanning and delivery functions. This can be done online or offline.

   Note

   - For details about how to activate RICOH Streamline NX, see "Activating RICOH Streamline NX", Installation Guide.

2. **page 227 "Creating a Workflow"**

   Configure the methods for delivering scanned documents and converting images, and save the settings as a workflow.

3. **page 319 "Configuring Device Applications"**

   Configure the items to be displayed on the operation screen of the device.

4. **page 321 "Configuring a Workflow Profile"**

   Create a workflow profile that associates a workflow with a device or Monitor Folder.

5. **page 329 "Configuring a Profile Task"**

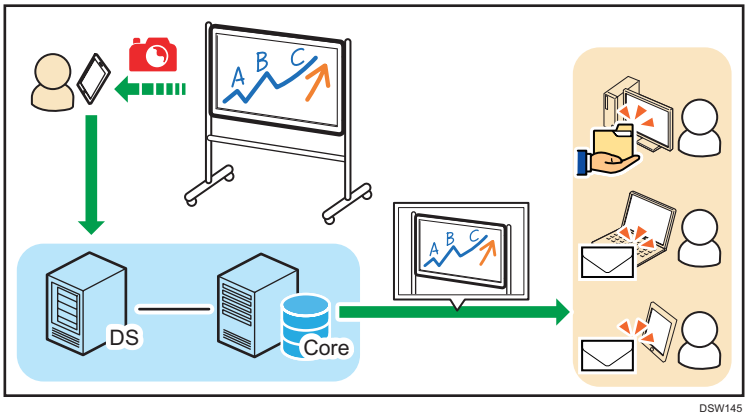
   Configure a schedule for syncing the configured workflow profile with a device or Delegation Server.

Note

- By using the Configuration Wizard, you can display each configuration screen from the Management Console. For details about the Configuration Wizard, see page 48 "Screen Configuration of the Management Console".

Sending Photos Taken with the Camera from a Mobile Device

Use the user-based mobile app to send images taken with a camera on a mobile device to the server. For example, you can share photos of notes written on a whiteboard in a meeting or share photos from a business trip to ensure more accurate information sharing.



1. ▶ **Confirming the capture function configuration**

   To use the mobile app, activate the capture function and create workflows. Make sure that Steps 1 and 2 of page 40 "Sending Scanned Documents and Received Faxes over a Network" are completed.

   Note

   - Create a mobile workflow as necessary.

2. ▶ **page 381 "Configuring a Workflow Profile Associated with a Mobile Device"**

   To use the delivery function or printing function for secure print documents on a mobile device, create a workflow in the Management Console, and then configure a workflow profile that associates the workflow with a mobile device.

3. ▶ **page 329 "Configuring a Profile Task"**

   Configure the schedule for syncing the configured workflow profile with Delegation Servers.

Print Function Workflow

1

Enhanced Security and Convenience of Printer Function

When the RICOH Streamline NX server is linked with devices, the user can manage documents to be printed on the server, and the administrator manages the print function of the devices. For example, the administrator can configure the print function to only allow printing of monochrome prints or to store documents on the server and allow printing to be performed from a remote location. In addition, integrating the management of logs and histories related to print jobs can help in analyzing print costs and creating statistical data.

For an overview of the print function, see page 179 "Overview of the Printing Functions".

Print Functions of RICOH Streamline NX

The following types of print functions are available in RICOH Streamline NX:

- Print Rules Function
- Secure Print Function
- Direct Print Function
- Client Direct Print Function

Secure Print Function

The Secure Print Function allows only identified users to perform secure printing from devices that have Embedded Client installed.

1. ▶ **Using the Advanced License for Activation**

Activate the software with a Print License to enable printing functions. This can be done online or offline.

Note

- Once you activate the license for the print function, all print functions are enabled.
- For details about activating the product, see “Activating RICOH Streamline NX”, Installation Guide.

2. ▶ **Checking the Types of Secure Print**

View the special features and the available types of Secure Print. Two types of Secure Print are available: Server Secure Print and Client Secure Print. For details, see page 186 "Configuring Secure Printing".

3. ▶ **page 190 "Settings to Use Secure Printing"**

Check the settings that are required to use the Server Secure Print and Client Secure Print functions.

Direct Print Function

When a user sends a print job, authentication and application of the print rules are performed on the Delegation Server or client computer with RICOH Streamline NX PC Client, and the job is immediately printed from the specified device.

1. ▶ **Using the Advanced License for Activation**

Activate the software with a Print License to enable printing functions. This can be done online or offline.

Note

- Once you activate the license for the print function, all print functions are enabled.
- For details about activating the product, see "Activating RICOH Streamline NX", Installation Guide.

2. ▶ **Checking the Types of Direct Printing**

Three types of direct printing are available: Server Direct Print, Client Direct Print and Device Direct Print. For details, see page 195 "Configuring Direct Printing".

3. ▶ **page 196 "Configuring the Settings to Use Direct Printing"**

Check the settings that are required to use the Direct Print function.

Device Direct Printing Function

With the device direct printing function, a user can send a print job from a computer to a device and have it printed without going through the Delegation Server. You can print documents only if the printer driver for the device is installed on your computer, and there is no need to install RICOH Streamline NX PC Client.

Print Rules Function

In the Print Rules function, the administrator creates print rules in advance according to the operation purpose, and when the user performs printing, the settings specified in the print rules are automatically applied.

1. ▶ **Using the Advanced License for Activation**

   Activate the software with a Print License to enable printing functions. This can be done online or offline.

   Note

   - Once you activate the license for the print function, all print functions are enabled.
   - For details about activating the product, see “Activating RICOH Streamline NX”, Installation Guide.

2. ▶ **page 199 "Configuring Print Rules"**

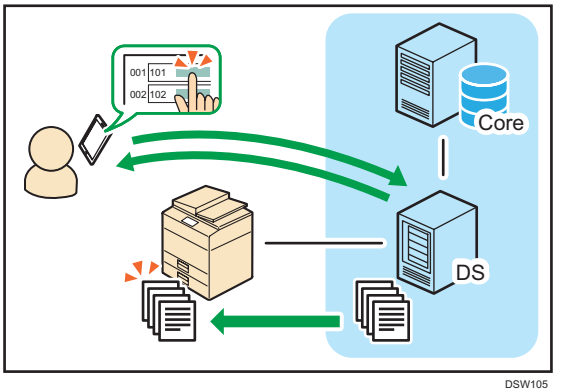
   Confirm the details of Print Rules Function.

3. ▶ **page 200 "Creating Print Rules"**

   Create the print rules such as the criteria and actions to be applied to print jobs and the target users.

Enabling the Mobile App for Print Functions

Use the mobile app to print or view print jobs stored in the server. You can release print jobs to a printer without having to log on at the device.



DSW105

1. **▶ page 374 "Configure the Initial Settings of the RICOH Streamline NX Device Manager App"**

Configure the user name and password to log in to the server.

Note

- For details, see “Configuring the Default Settings of the RICOH Streamline NX Mobile App”, User's Guide.

2. How to Use the Management Console

Use a web browser application to display the Management Console of RICOH Streamline NX.

Logging In to the Management Console

Use the Management Console to obtain the status of monitored devices, change the device settings, and perform all other operations for the entire system.

1. **In a web browser, access the URL shown below and display the login screen.**
   - When SSL is not used

     http://(IP-address-or-hostname-of-Core-Server):(port-number)/index.html
   - When SSL is used

     https://(IP-address-or-hostname-of-Core-Server):(port-number)/index.html
2. **Select a [Profile].**

   To log in as a local user, select [Default (Internal)].

   To login as an externally identified user registered to an LDAP server or other server, select the authentication profile for connecting to an external authentication server.
3. **Enter the user name and password.**

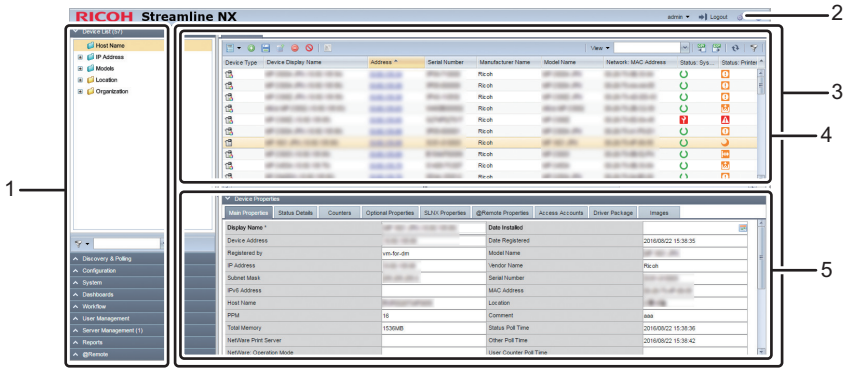
   Use the correct case in the password.
4. **Select the language to be displayed on the screen.**
5. **Click [Login].**

Note

- The Management Console is designed to meet the needs of various system personnel. For example, the appropriate permission to allow use of only the required functions can be assigned to various people in charge including the system administrator, field superintendent in need of reports, and person in charge of issuing guest accounts.
- For roles that can be configured in the Management Console, see page 160 "Managing User Roles and Privileges".

Screen Configuration of the Management Console

This describes the basic configuration of the screen in the Management Console using the device list screen as an example.



DSW601

1. **Navigation tree**

   The navigation tree is divided into different functions. To display a detailed item in tree view, click a category title.

2. **Configuration Wizard**

   Click the configuration wizard to display the links to various setting screens. You can configure the settings for different purposes by following the instructions on the screen.

3. **Tab area**

   To add a new tab and display the operation screen, click a detailed item in the navigation tree. Click tabs to switch between different operation screens. To close multiple tabs at once, right-click a tab and select [Close All but Current] or [Close All].

4. **List area**

   Various lists such as the device list and task list are displayed above the tab area. Various icons are displayed in the toolbar in the list area. Use these icons to perform operations such as creating a new setting item or importing/exporting the setting items. The displayed icons may differ depending on the function.

5. **Properties area**

   When an item is selected in the list area, detailed information of that item is displayed below the tab area. Use the properties area to configure the settings of the item.

   Click the title bar of the properties area to open or close the area. Drag the title bar to change the size (height) of the area.

Bookmarks and Page Navigation

As a browser-based application, RICOH Streamline NX offers the ability to bookmark particular pages that you use often. Navigate to a tab that you want to bookmark, and use your browser's bookmark feature to bookmark the tab. If you log out of RICOH Streamline NX and then load the bookmark, you must enter your credentials on the log in screen, after which the browser will load the bookmarked tab.

You can also use the browser's forward and back buttons to page through the tabs you have loaded previously.

Time and Time zones

Within RICOH Streamline NX, time is handled in different ways based on the following:

- All times for device activity stored in the Core Server database is reported in the Core Server's local time.
- Time displayed in the RICOH Streamline NX management interface is based on the browser settings.
- Tasks are run according to the Delegation Server's local time. If you create a task that will be applied to all devices, and the devices are managed by two different Delegation Servers, the task will run at different times if the servers are in different time zones.

Changing Your Password

You can change your password for local user accounts only. If your user account is managed by LDAP or Kerberos, you cannot change your password within RICOH Streamline NX. Follow these instructions if logging in with a local account only.

1. **Click the user name at the top right of the Management Console.**
2. **Click [Change Password].**
3. **Enter the current password and a new password in the dialog box that appears, and then click [OK].**

Changing the Display Settings

Specify the country where the product is used, the custom properties, and the display format of the date and time in the display settings of the Management Console.

Note

- For details about the setting items, see page 519 "Display".

Changing the Default Country Setting

The region setting of the operating system installed on the Core Server is set by default as the country setting in the Management Console. When the system is being operated in more than one country, it is recommended to specify the country where the number of the devices to be managed is the largest for the default setting. The country information is requested in the following cases:

Activating the License

Activation must be performed after the country setting has been configured correctly to the target country.

Using RICOH Software Server

To obtain the list of Device Applications from RICOH Software Server, the country setting in the template must be configured correctly.

Also, the correct country information is required to activate Device Applications.

1. **Click the following items in the navigation tree to open the [Display] tab.**

   [System] ▶ [Server Settings] ▶ [Display]

2. **In [Country Setting], select a country.**
3. **Click [Save].**

Configuring the Custom Properties

Configure Custom Properties to save device specific information as a device property. For example, you can create an item name such as control number or asset number and save the value of the created item on each device.

Note

- The custom properties are displayed on the [Optional Properties] tab in [Device Properties]. To configure a value in the Custom Properties, select a device in the device list, and then click [Optional Properties] ▶ [Custom Property].
- A device administrator can enter the actual values for each device in the custom fields.

1. **Click the following items in the navigation tree to open the [Display] tab.**

   [System] ▶ [Server Settings] ▶ [Display]

2. **In [Custom Property 1], enter an item name.**

   You can configure up to 10 custom properties.

3. **Click [Save].**

3. Managing Devices

To manage a device, first search for the device on the network and register the discovered device in the Device List.

Once you register a device in the Device List, you can then obtain the status information, configure the settings, and install Device Applications.

Once a device is registered in the Device List, operations such as obtaining the status information, configuring the settings, or installing Device Applications can be performed.

Viewing the Device List

This section describes the icons displayed in the device list and the items in the device properties.

Note

- For details about registering devices in the device list, see page 76 "Adding a Device to the Device List".
- For details about obtaining the device status, see page 89 "Checking the Device Status".
- Only the devices within the screen display range are read from the server and displayed in the device list. When you use the scroll bar to scroll through the list quickly, the devices being scrolled through are not read from the server, and they cannot be displayed.

Icons Displayed in the Device List

All operation icons and device icons displayed in the device list are described in the tables as shown below. Some operation icons may not be displayed depending on the function.

Operation icons

Icon	Description
	Displays the following menu items in the device list: • Add Device: Adds a device to the list. See page 80 "Adding a Device to the Device List". • Move Devices to New Delegation Server: Changes the Delegation Server assigned to the device. This operation is available only when multiple Delegation Servers are installed. • Delete: Deletes a device from the list. See page 82 "Deleting a Device from the Device List". • Ignore Devices: Hides the device in the list. • Notifications: Displays the notification settings applied to the device. • Request Polling: Obtains the status of the selected device. • User Counter: Displays the user counter of the selected device. • History: Displays the status and counter history of the selected device.

Icon	Description

Note
• When the following functions are performed, users assigned a user codes between 90000000 and 90000019 displayed on [User Counter] are treated as temporary users registered to the device address book by RICOH Streamline NX:
  • Secure Printing from devices installed with the Streamline NX Embedded Application.
  • Server Direct Printing
  • Client Direct Printing
• The following are not moved to a new Delegation Server when [Move Devices to New Delegation Server] is executed:
  • Scan history
  • Scan jobs
  • Print jobs
  • Device Job Log
  • Device Access Log
• After executing [Move Devices to New Delegation Server], it is necessary to uninstall and re-install Streamline NX Embedded Application on devices. if the old Delegation Server is eliminated and does not belong to any group in [Delegation Server Failover/Load Balancing Groups].
• These users can be safely deleted while the device address book is being configured.
When any of the above functions are performed after the users are deleted, the user codes between 90000000 and 90000019 are automatically registered again.
• Select (Delete) to exclude the machine from the output report. When you are using the report function, select (Ignore Devices) instead of (Delete). Also, the machine with (Ignore Devices) that is selected will not be counted as a machine that is managed under Basic license.
• Select (Delete) to reduce the size of the database. However, the machine with (Delete) that is selected will be excluded from the output report.	

	Adds the device in the device list. It also deletes the device registered in the device list. For details about adding or deleting devices, see page 80 "Adding a Device to the Device List" or page 82 "Deleting a Device from the Device List".
	Saves the edited device information.

Icon	Description
	Hides the devices to be temporarily excluded from the subject of management. The hidden devices can be displayed again from the right-click menu of the navigation tree.
	Changes the Delegation Server assigned to the device. This operation is available only when multiple Delegation Servers are installed.
	Displays the current location of the device on a map. This operation is available only when the map information is registered to the device.

	Saves and enables selection of the current view setting of the list.
	• Save: Saves the following settings as a view. You can register up to five views.
	  • Sort order
	  • Column width
	  • Displayed columns
	  • Fixed column
	  • Calculated column
	  • Column display items
	  • Sorting status of each column
	• Save as: Saves the view as new.
	• Delete: Deletes a registered view.
	To switch to a different view, select a registered view in the list.

	Exports or imports the list information as a CSV file. Up to 5000 devices can be imported at one time. The device properties such as the display name and device installation date can also be specified. For details, see page 759 "Format of a Device Information CSV File".
	Updates the list information.
	Filters the list information. Click this to display the input/select area above the item name in the list. Select or enter the search key and click  on the right side of the input area or press the Enter key to display the corresponding address book.
	Displays the help contents explaining the setting item and how to perform operations on the displayed screen.

Note

- For details about the column operation and map function, see page 83 "Customizing the Device List Display".

Device icons

Icon	Description
	Ricoh Digital Full Color MFP*
	Ricoh Digital Monochrome MFP*
	Ricoh Color Laser Printer*
	Ricoh Monochrome Laser Printer*
	Ricoh GELJET Printer MFP
	Ricoh GELJET Printer
	Other-Ricoh color/monochrome MFP or printer
	Non-Ricoh color/monochrome MFP or printer
	USB-connected device

* The displayed device icon differs depending on the device used.

Device Properties

The items that are displayed vary depending on the device.

Main Properties

This displays the device information obtained via polling.

- Device Name

  Displays the name of the device. Change this item as needed. The old device name is retained even after the device is detected again by discovery.

- Date Installed

  Displays the installation date and time of the device. Change this item as needed.

- Address

  Displays the IP address or host name of the device. Change this item as needed.

- Date Registered

Displays the date and time the device was registered in the list.

- Registered by

  Displays the login user name if the device was registered manually. Displays the Delegation Server name if the device was registered by discovery.

- Model Name
- IP Address
- Host Name
- Subnet Mask
- Vendor Name
- IPv6 Address
- Serial Number
- MAC Address
- WIM Location

  Displays the install location specified in the device.

- Comment

  Displays the comment specified in the device.

- PPM

  Displays the number of pages that can be printed per minute.

- Total Memory
- Status Poll Time
- NetWare Print Server
- Other Poll Time
- NetWare: Operation Mode
- User Counter Poll Time
- DS Free Space
- Counter Poll Time
- Document Server Capacity
- Supply Poll Time
- DOSS Last Auto Delete Date
- Detailed Counter Poll Time
- DOSS Auto Delete Enabled
- DOSS Auto Delete Method
- DOSS Auto Delete Count

- HDD Encryption
- Last Communication Time
- Last Received Time of Device Job Log
- Last Received Time of Device Access Log
- Last Received Time of Device Eco Log
- Disable DMNX Management Extension for Configuration Templates

  The setting items marked with a dagger mark can no longer be read or written when this check box is selected. Also, the device properties that are related to DOSS cannot be obtained on some devices.
- Display Message

  Enter the message to be displayed on the operation screen of the device.
- Device Type
- Operation Panel

  Displays "Smart" or "Standard" depending on the type of the selected device. When the information cannot be obtained from the device, this item is left blank.
- SOP: Interface Settings
- SOP: Wi-Fi Connection

Note

- For Ricoh MFPs and printers, the contents configured in Web Image Monitor are displayed in “WIM Location” and “Comment”.
- The last communication time is updated when a poll or task is successfully completed.

Status Details

This displays the detailed device status. Select one of the following tabs to view each status: [Printer Status], [Paper Tray], [Toner/Ink], and [Output Tray].

Printer status

Displays the status of the printer function. To display detailed information, place the mouse cursor over the icon. When more than one status has occurred at the same time, the status with higher priority is displayed.

In the table shown below, the icons are described in the order of higher priority.

Icon	System	Printer	Copier	Fax	Scanner	Description
	✓	✓	✓	✓	✓	The device is not responding.

Icon	System	Printer	Copier	Fax	Scanner	Description
	✓	N/A	✓	✓	✓	A service code has occurred.
	✓	N/A	N/A	N/A	N/A	Replace or replenish the consumable.
	✓	✓	✓	✓	N/A	The toner/ink has run out.
	✓	✓	✓	✓	N/A	A paper jam has occurred.
	✓	✓	✓	✓	N/A	Paper has run out.
	✓	N/A	N/A	✓	N/A	Maintenance is in process.
	✓	N/A	N/A	✓	N/A	A fax communication error has occurred.
	✓	N/A	✓	✓	✓	A paper jam has occurred in the ADF.
	✓	✓	✓	✓	✓	A cover is open.
	✓	✓	✓	✓	✓	An error has occurred.
	✓	N/A	N/A	N/A	N/A	Access violation has been detected.
	N/A	✓	N/A	N/A	N/A	The device is offline.
	N/A	✓	✓	✓	N/A	The device is warming up.
	N/A	✓	✓	✓	✓	The device is busy.
	N/A	✓	✓	✓	N/A	The toner/ink is almost empty.
	N/A	✓	N/A	N/A	N/A	The paper is almost empty.
	N/A	✓	✓	✓	✓	Caution.
	N/A	✓	✓	✓	✓	The device is in Energy Saver Mode.

Icon	System	Printer	Copier	Fax	Scanner	Description
	✓	✓	✓	✓	✓	The device is ready to use.

Input Tray

This displays the paper tray types and the paper orientation, size, type, and amount of remaining paper for each tray.

 : Indicates the paper orientation in relation to the paper feed direction.

Paper tray icon	Paper role icon	Description
		Paper has run out.
		0–20%*
		20–40%
		40–60%
		60–80%
		80–100%

* "20 %" is the default value for a device. The actual threshold varies depending on the device.

Toner/Ink

This displays the colors of the toner/inks and the remaining amount of each toner/ink. For devices that do not support the detection of the remaining amount of toner/ink and for some monochrome MFPs, this item may be displayed as "Unknown".

The remaining amount of toner/ink indicated by the indicator is shown below. The color of the indicator is the same as that of the corresponding toner/ink. Black is used as an example in the table shown below.

Icon	Description
	The toner/ink has run out.
	The toner/ink is almost empty.
	0–20%
	20–40%

Icon	Description
	40–60%
	60–80%
	80–100%

Note

- In the device properties of a RICOH device (2012 models and later), the serial number, replacement date, and counter of the toner/ink can also be displayed.

Output Tray

This displays the types of output trays and the status of each tray.

The status of the output tray indicated by each icon is as follows:

Icon	Description
	The output tray is full with paper.
	There is paper remaining on the output tray.
	An error has occurred.
(Nothing is displayed)	The output tray is in the normal state.

Counter

This displays the counter information such as the number of prints made in color and monochrome and the number of pages sent via fax.

- Device Counter Total

  Indicates the total value of the counters for the copier, printer, and fax functions.

  The Total counter provides the sum of all toner usage on this devices, and is a cumulative total of monochrome and color toner usage (if applicable).

- Copier: B&W, Full Color, Two-color, Single Color

  Indicates the counter values for the copier function.

- Printer Black, Full Color, Two-color

  Indicates the counter values for the printer function.

- Printer Color Mono
- Economy Color

- Fax Prints: B&W
- Fax

  Indicates the counter values for the fax function.
- A2
- A3/DLT
- Duplex Print
- Send/TX Total: Color, B&W

  Indicates the total value of the counters for the scanner send and fax send functions.
- Fax Send
- Scanner Send Color, B&W

  Indicates the counter value for the scanner send function.
- Total Mono
- Total Color
- Internal Counters: Color Copies, B&W Copies
- Internal Counters: Color Prints, B&W Prints
- Internal Counters: Full Color Sheets Total, B&W Sheets Total
- Internal Counters: Full Color Sheets Prints, B&W Prints
- Internal Counters: Full Color Sheets A3/DLT and up, Full Color Sheets Under A3/DLT
- Internal Counters: Full Color Economy Prints, B&W Economy Prints
- Coverage Color Pages, Percentage

  Coverage is the total toner usage (in units of 1%) per sheet of A4 page. For example, when an entire A4 sheet is filled with solid black, black toner coverage is 100%.
- Coverage B&W Pages, Percentage
- Color 1, 2, 3

  Indicates the counter values categorized in Low, Med, and High for coverage of color pages. The unit of the counter is side(s). The default thresholds for each coverage category are as follows:
  - Color 1 (Low): Lower than 5 %
  - Color 2 (Mid): 5 to lower than 20 %
  - Color 3 (High): 20 % or higher
- Activate

  Indicates the counter value of the total running time of the device. The unit of the counter is minute(s).
- Idle

Indicates the counter value of the total inactive time of the device. The unit of the counter is minute(s).

- Preheat

  Indicates the counter value of the time the device was in preheating mode. The unit of the counter is minute(s).

- Sleep

  Indicates the counter value of the time the device was in sleep mode. The unit of the counter is minute(s).

- OffMode

  Indicates the counter value of the time the device was in off mode. The unit of the counter is minute(s).

Detailed Counter

For Ricoh devices with the device icons  , the following detailed counter information can be viewed.

Number of pages in a job

Records the number of pages in a job. The counter unit is jobs.

- Jobs per Pages:Total:1 Sheet
- Jobs per Pages:Total:2 Sheets
- Jobs per Pages:Total:3 Sheets
- Jobs per Pages:Total:4 Sheets
- Jobs per Pages:Total:5 Sheets
- Jobs per Pages:Total:6-10 Sheets
- Jobs per Pages:Total:11-20 Sheets
- Jobs per Pages:Total:21-50 Sheets
- Jobs per Pages:Total:51-100 Sheets
- Jobs per Pages:Total:101-300 Sheets
- Jobs per Pages:Total:301-500 Sheets
- Jobs per Pages:Total:501-700 Sheets
- Jobs per Pages:Total:701-1000 Sheets
- Jobs per Pages:Total:1001 Sheets

2 Sided/Combine

Records the number of pages printed on two sides of a sheet of paper using the combine and binding functions. The counter unit is pages.

- Duplex/Pages per Sheet:Total:2in1
- Duplex/Pages per Sheet:Total:4in1

- Duplex/Pages per Sheet:Total:6in1
- Duplex/Pages per Sheet:Total:8in1
- Duplex/Pages per Sheet:Total:9in1
- Duplex/Pages per Sheet:Total:16in1
- Duplex/Pages Per Sheet:Total:Single->Duplex
- Duplex/Pages Per Sheet:Total:Duplex->Duplex
- Duplex/Pages Per Sheet:Total:Spread->Duplex
- Duplex/Pages Per Sheet:Total:Single
- Duplex/Pages Per Sheet:Total:Duplex
- Duplex/Pages Per Sheet:Total:Mini-book
- Duplex/Pages Per Sheet:Total:Magazine Binding
- Duplex/Pages Per Sheet:Total:2in1+Mini-book
- Duplex/Pages Per Sheet:Total:4in1+Mini-book
- Duplex/Pages Per Sheet:Total:6in1+Mini-book
- Duplex/Pages Per Sheet:Total:8in1+Mini-book
- Duplex/Pages Per Sheet:Total9in1+Mini-book
- Duplex/Pages Per Sheet:Total:2in1+Magazine Binding
- Duplex/Pages Per Sheet:Total:4in1+Magazine Binding
- Duplex/Pages Per Sheet:Total:6in1+Magazine Binding
- Duplex/Pages Per Sheet:Total:8in1+Magazine Binding
- Duplex/Pages Per Sheet:Total:9in1+Magazine Binding
- Duplex/Pages Per Sheet:Total:16in1+Magazine Binding

Paper size

Records the size of printed paper. The counter unit is pages.

- Paper Size:Total:A3
- Paper Size:Total:A4
- Paper Size:Total:A5
- Paper Size:Total:B4
- Paper Size:Total:B5
- Paper Size:Total:DLT
- Paper Size:Total:LG
- Paper Size:Total:LT
- Paper Size:Total:HLT

- Paper Size:Total:Spread Paper
- Paper Size:Total:A2
- Paper Size:Total:B3
- Paper Size:Total:Other(Regular Size)
- Paper Size:Total:Other(Long/Custom Size)
- Paper Size:Total:A1
- Paper Size:Total:A0
- Paper Size:Total:B1
- Paper Size:Total:B2
- Paper Size:Total:30inchx42inch
- Paper Size:Total:34inchx44inch
- Paper Size:Total:22inchx34inch
- Paper Size:Total:17inchx22inch
- Paper Size:Total:A0(Custom Size)(A0 and Larger)
- Paper Size:Total:A0(Custom Size)(Smaller than A0)
- Paper Size:Total:A1(Custom Size)
- Paper Size:Total:A2(Custom Size)
- Paper Size:Total:A3(Custom Size)
- Paper Size:Total:A4(Custom Size)
- Paper Size:Total:B1(Custom Size)
- Paper Size:Total:B2(Custom Size)
- Paper Size:Total:B3(Custom Size)
- Paper Size:Total:B4(Custom Size)
- Paper Size:Total:A(Custom Size)
- Paper Size:Total:B(Custom Size)
- Paper Size:Total:C(Custom Size)
- Paper Size:Total:D(Custom Size)
- Paper Size:Total:E(Custom Size)

Paper type

Records the type of printed paper. The counter unit is pages.

- Paper Type:Total:Plain paper
- Paper Type:Total:Recycled paper
- Paper Type:Total:Special paper

- Paper Type:Total:Thick paper
- Paper Type:Total:Plain paper(back side)
- Paper Type:Total:Thick paper(back side)
- Paper Type:Total:OHP
- Paper Type:Total:Other

Printer Language

Records the printer language executing printing. The counter unit is pages.

- Emulation:Total:RPCS
- Emulation:Total:RPDL
- Emulation:Total:PS3
- Emulation:Total:R98
- Emulation:Total:R16
- Emulation:Total:GL
- Emulation:Total:R55
- Emulation:Total:RTIFF
- Emulation:Total:PDF
- Emulation:Total:PCL5
- Emulation:Total:PCLXL
- Emulation:Total:IPDLC
- Emulation:Total:BM-Links
- Emulation:Total:IPDS
- Emulation:Total:Other

Finishing

Records the number of pages printed using the finishing functions. The counter unit is pages.

- Finishing:Total:Sort
- Finishing:Total:Stack
- Finishing:Total:Staple
- Finishing:Total:Stapling(Center)
- Finishing:Total:Z Booklet
- Finishing:Total:Punch
- Finishing:Total:Booklet(Center)
- Finishing:Total:Booklet(In, Triple)
- Finishing:Total:Booklet(Out, Triple)

- Finishing:Total:Booklet(Simple, 4 times)
- Finishing:Total:Booklet(double doors)
- Finishing:Total:Perfect Binding
- Finishing:Total:Ring Binding
- Finishing:Total:Other

Total number of pages

Records the total number of printed pages by function and the device function The counter unit is pages.

- Total Printouts : Total
- Total Printouts : Copier
- Total Printouts : Fax
- Total Printouts : Printer
- Total Printouts : Scanner
- Total Printouts : Local Storage
- Total Printouts : Other

Optional Properties

Switch between the [Custom Properties], [Installed Applications], [Firmware and Platform], and [Functions] tabs to display the corresponding information.

Custom Properties

Displays an additional properties that configured by a device administrator. For the configuration procedure, see page 50 "Configuring the Custom Properties".

Installed Applications

Displays the list of applications that are installed on the device.

The user can view the application name, version, product ID, application type, activation status, license type, and expiration date.

Firmware and Platform

Displays the device firmware version, SDK/J platform version, SmartSDK version, heap side and stack size.

Function

Displays the functions and printer language that are supported by the device.

- Function

  This displays the functions supported by the device such as bypass tray feed, duplex print, and thick paper print.

- Printer Language

  This displays the printer languages supported by the device.

SLNX Properties

Embedded Settings

Displays the embedded settings on the device.

Note

- For details about the setting items, see page 511 "Embedded Setting".

Workflow Profile

Displays the workflow profiles that can be used on the device.

@Remote Properties

Use this item to check information such as inquiries to @Remote Center. Activate @Remote license to display this information.

- Device ID
- Cutoff Date
- Service Depot
- Service Depot Phone No
- Supply Order From
- Supply Order Phone No
- Encryption Length

Access Account Settings

Use this item to check the access account profiles that were used to access the device. In addition, change the profile of the access account for each device.

For details about configuring the access account, see page 76 "Configuring an Access Account".

For details about the access account items, see page 474 "Access Profiles".

Driver Package

The driver that has been uploaded to the repository on Core Server can be associated with a device.

Note

- For details, see page 133 "Distributing Printer Drivers".

Images

Image files in png, jpg, or gif format can be registered. The number of images that can be registered differs depending on the size of the database. For details about manage the system capacity, see page 395 "Managing the System Capacity",

Item	Function
Description	Enter or view the description of the device image.
Capture Date	Displays registration date of the device image.
Captured by	Displays the name of the user who registered the device image.
[Update] button	Click to update the information after [Description] has been updated.
[Set Primary] button	Click to select the device image to be displayed first. When this setting is not specified, the device images are displayed in chronological order.
[Add] button	Click to show the [Add Map] dialog box for adding a device image. • [Description]: Enter the description of the device image. • [Image File]: Click the [Browse] button and select the device image to be added. The following file formats are supported: • PNG • JPG • GIF
[Delete] button	Deletes all registered device images.

Organizing the Device List

To manage a large number of devices efficiently, classify the devices according to the device management operational structure. For example, when devices are divided into categories or groups that have been created for various regions or organizations of a company, you can combine multiple devices into a single unit and change device settings or impose restrictions on user access for multiple devices at one time.

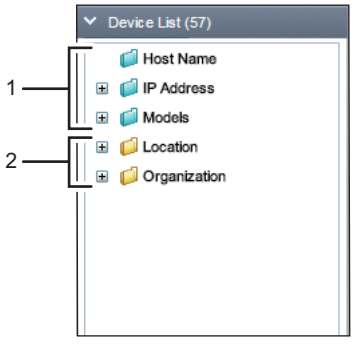
It is recommended to categorize devices and organize the device list, such as by examining the network configuration and organizational structure.

Overview of Categories and Groups

You can perform operations related to device categories in [Device List] in the navigation tree.

The folder icons displayed on the first hierarchy in [Device List] are called “categories”, and the folder icons on the second and later hierarchies are called “groups”.

There are two types of categories: system categories, which are preset in the Management Console, and custom categories, which the administrator can create.



DSW602

1. **System Category/System Group**

   A system category is indicated by a blue folder icon. System categories can be further classified into the following three types:

   - Host Name

     Devices are classified according to the domain hierarchy. Regardless of whether the domain hierarchy is an actual domain or not, the domain hierarchies are divided into groups by separating each hierarchy by a dot.

   - IP Address

     Devices are classified into groups by subnet of IPv4 addresses. Devices that have no assigned IPv4 address are categorized in the "N/A" group.

   - Models

Devices are classified into groups by manufacturer. These devices are further divided into groups by model names.

2. **Custom Category/Custom Group**

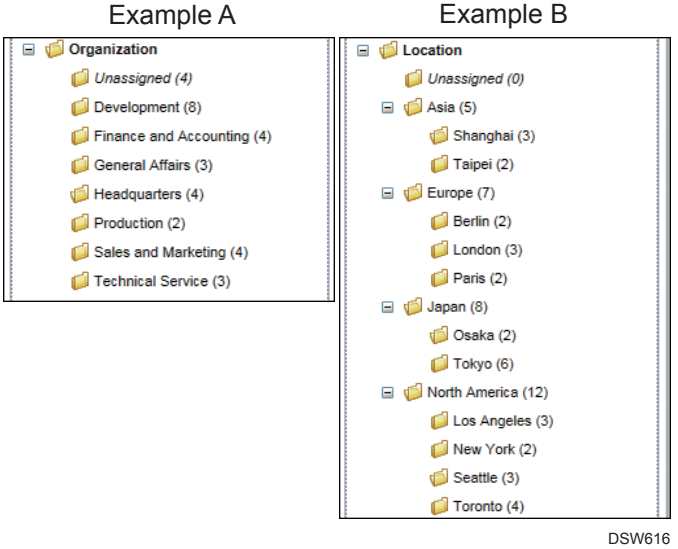
   A custom category is indicated by a yellow folder icon. You can create up to 5,000 categories or groups. If there are too many devices to manage under System Category alone, create custom categories to manage them efficiently according to the operational structure. You can filter devices to be grouped while creating a custom category or custom group.

Organization Strategies

The best strategy is to organize the list into categories and groups that make sense based on the organization of your fleet BEFORE you populate the list. To implement this organization, RICOH Streamline NX supports the creation of up to 5000 custom categories and groups to suit your organizational needs. For example, you might prefer to group your devices by location or by organization (subsidiaries, divisions, departments, etc.).

To develop your own organization strategy, consider the following:

- A category is a method of classifying the devices within your organization. For example, you might categorize based on location (country, city, building, floor, etc.), by department (Accounting, Engineering, Marketing, etc.), or by cost center, etc.



DSW616

- You can use the structure to associate security roles with custom groups. For example, if you organize the structure based on Location, then create groups for various continents, and create further subgroups for countries and cities, your structure might look similar to Example B on the right. If multiple device administrators are responsible for devices within each country, you can associate Security Context Groups with the country groups in this structure, thereby allowing each device admin to view or modify only the devices in their location.

In Example A, the structure is based on the organization of the business into groups such as accounting, engineering, etc. Using this structure, you can produce reports and/or set up security based on function. However, it is important to note that Security Context Groups can be applied to one custom category only, so ensure you plan your groups accordingly.

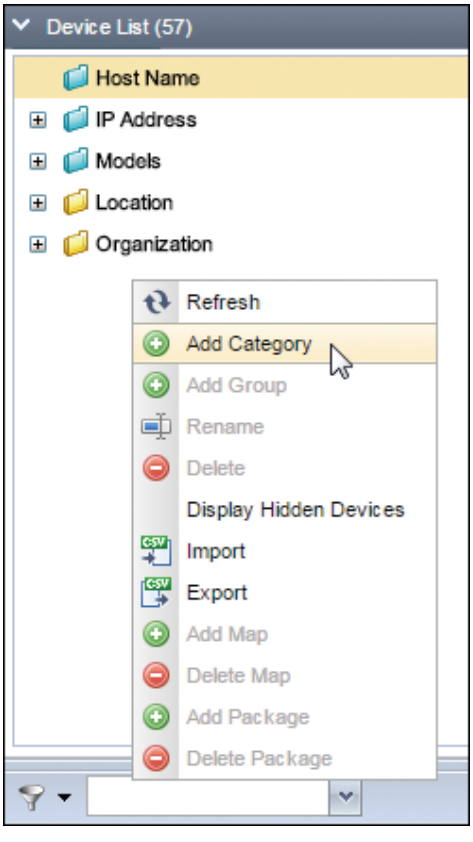
By organizing before importing or performing discovery, you can establish filtering rules that will place imported or discovered devices in the correct category or group automatically. This initial planning will save you a significant amount of time overall.

The possibilities for organization are boundless, and it is up to you to use the information and instructions in this section as a guideline for establishing your own organization scheme.

The examples in this section create categories based on geographical location and require several subgroups per location.

Creating a Custom Category and Custom Group

1. **Click [Device List] in the navigation tree to expand the system category.**
2. **Right-click the blank space in the navigation tree, and select [Add Category].**



3. **Enter the category name, and click [OK].**

4. **Right-click the created category, and select [Add Group].**

- Assign the existing devices matched by filter criteria

  Only the registered devices in the device list are included in the group.

- Assign new or unassigned devices using filter criteria

  The registered devices in the device list and newly discovered devices are included in the group.

- Filter Criteria

  [Filter Criteria] can be used when either of two items shown above is selected.

  Specify the matching condition, device property item, comparative operator, and reference value for the criteria to narrow down devices.

  - Matching condition: Select from the following items:

    Match All, Match Any, or Match None

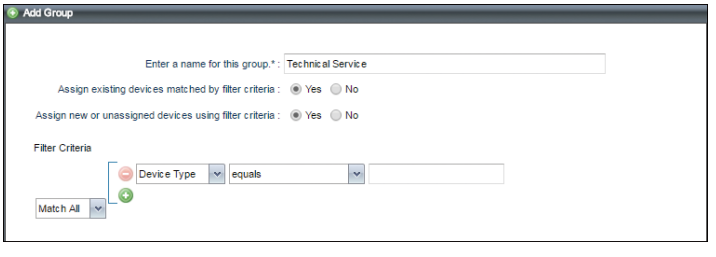
  - Device property item: Select a property item that can be retrieved from the device.
  - Comparative operator: Select from the following items:

    including, excluding, larger than, equal to, starting with, ending with

  - Reference value: Enter the value to be used as a reference.

To specify more than one matching criteria, click the button.

5. **Enter a group name.**
6. **Specify the target range of the device to be categorized in a group.**



7. **Click [Select Device], and check that the result is as you intended.**
8. **Click [OK].**

   To edit multiple category names or group names at one time, select the categories or groups in the navigation tree, and then press the F2 key.

9. **To add an individual device to a group, drag the device from the device list and drop it in the group.**

   To select more than one device, select the devices while pressing the SHIFT or CTRL key.

Note

- For the operations that can be performed on the navigation tree, see page 457 "Device List".

- Although you can perform a task on a device belonging to the "Unassigned" group, it is recommended to leave no device in the "Unassigned" group to make management easier.
- Click  to import or export categories or groups in a CSV file. For the format of CSV files, see page 760 "Format of a Device Group Information CSV File".
- When [Assign new or unassigned devices using filter criteria] is selected, it may take up to 5 minutes to assign the corresponding device to a group.

Adding a Device to the Device List

To add a device to the device list, specify the criteria such as the network search range.

1. ▶ **page 76 "Configuring an Access Account".**

   Configure the account information to enable the Management Console to connect to the device.

2. ▶ **page 77 "Searching for Devices".**

   Configure the Discovery setting such as search method, network range, and schedule for detect the devices on a network.

   You can also add a device by importing a CSV file containing the device information.

Note

- When only a small number of devices is being added, the devices can be added by specifying the device IP addresses individually. See page 80 "Adding a Device to the Device List".

Configuring an Access Account

"Access account" is the account information that is used by the Management Console to communicate with the device. Configure an access account to search for and communicate with a device.

There are three types of access accounts as follows:

- Web Service Account Setting
- SNMP
- SDK/J Platform

More than one access account can be specified at one time, and the accounts are used in the specified order to access devices when you perform discovery. Accounts that have successfully accessed the device are stored in the device properties, and the recorded device access account is used thereafter.

One access account is configured by default for each of Device Administrator, SNMP and SDK/J Platform. The default access account can be edited, but not deleted.

Important

- **To manage a device using the discovery, polling, and template functions, make sure that the authentication information of the access account matches the authentication information configured on the device.**
- **The authentication information of the device administrator must be the same as that of the administrator who has all administrative privileges (Device Administrator, User Management, File Administrator, and Network Administrator).**

1. **Click the following items in the navigation tree to open the tab that corresponds to the type of the access account.**

   - [Discovery & Polling] ▶ [Access Accounts] ▶ [Device Administrator]
   - [Discovery & Polling] ▶ [Access Accounts] ▶ [SNMP]
   - [Discovery & Polling] ▶ [Access Accounts] ▶ [SDK/J Platform]

2. **Click (Add).**
3. **Enter the [Profile Name], [User Name], and other information.**

   For details about the setting values, see page 474 "Access Profiles".

4. **Select the Security Group Context.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

5. **Click (Save) when the configuration is complete.**

Note

- SNMP read access is required to allow RICOH Streamline NX to discover and monitor the device. Communication with USB-connected local devices also uses SNMP v1/v2. Ensure the RICOH Streamline NX USB Agent is installed on each local computer (which has a USB-connected device) prior to completing these instructions. For details, see Installation Guide.

Searching for Devices

The process of searching for devices on a network and detecting the devices to be monitored and managed is called “discovery”.

To perform discovery, specify an IP address range, subnet mask, or other settings for search condition. The time required to perform discovery can be shortened and the traffic load on the network lessened by limiting the range to perform the search. Select the best timing and method that least affects your business when performing discovery.

The following two methods of discovery are available:

Network Search

A network search sends an SNMP authentication message to devices within a specified IP range.

Broadcast

A broadcast search sends an SNMP authentication message to every client on the network at the same time, or to a specified subnet.

Important

- If attempting to reach external network segments other than the segment to which the Delegation Server belongs, modify your router settings to enable broadcast.
- Discovery can detect devices that support Printer MIB v2 (RFC 3805), Printer MIB (RFC 1759), MIB-II (RFC 1213), or Host Resource MIB (RFC 2790).

1. **Click the following items in the navigation tree to open the [Broadcast] or [Network Search] tab.**

   [Discovery & Polling] ▶ [Discovery] ▶ [Network Search] or [Broadcast]

2. **Click (Add).**
3. **Enter the task name and description on the [General] tab.**
4. **Select the Delegation Server to be the target of discovery.**
5. **When performing reverse DNS lookup to identify the host name of the device, select the [Perform Reverse DNS Lookup] option.**
6. **Select the Security Group Context.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

7. **Add the account to be used for accessing the device to [Assigned Account] on the [Access Accounts] tab.**

   Up to 10 accounts each can be registered for Device Administrator, SNMP, and SDK/J Platform.

8. **Configure the range to search for devices by entering information such as the IP address or subnet mask on the [Discovery Range (Network Search)] or [Discovery Range (Broadcast)] tab.**

   The hostname is only used if [One Host Name] is selected and a hostname is entered in the [Host Name] field in the [Range Type].

   - To specify the search range manually:

     1. Click (Add).
     2. Specify the search range.
     3. Click (Save).

     Note

     - To specify another IP range, click (Add), and set the parameters for the next range. You can add as many search parameters as needed, but remember to click (Save) to save each new search.

- To import a CSV file that specifies the search range:

  1. Click (Imports data from CSV files.).
  2. Click [Browse...].
  3. Specify the CSV file to be imported, and click [Open].
  4. Click [Upload].
  5. Click [OK].

Note

- If you do not save on this tab, you will see an error message when you try to save the Discovery profile indicating that parameters are missing.
- The items that can be specified differ depending on whether [Network Search] or [Broadcast] is selected. To export the search range as a CSV file, click (Export data as a CSV file).

9. Configure the schedule to perform device discovery on the [Schedule] tab.

When [Disable Schedule] is checked, this Discovery profile will not run as per the set schedule. Use this feature to temporarily disable the Discovery profile. Use the (Delete) button on the tool bar to remove the Discovery profile completely.

10. Configure the settings for SNMP Trap and Device Log Collection on the [Auto Settings] tab.

11. Click (Save) when the configuration is complete.

The registered discovery task in the list is displayed. To immediately perform discovery, click (Run Immediately).

Note

- You need to perform discovery again in the following cases:
  - To add a newly installed device to the device list
  - To update the device list for the changes in the device IP address or host name
- The devices are identified by the serial numbers or MAC addresses. Even when the IP address or host name of the device is changed, the device information is caries over if the device is determined to be the same device.
- For details about the setting items on each tab, see page 461 "Discovery".
- For the format of CSV files, see page 761 "Format of a Discovery Range CSV File".

Modifying the Connection Port Behavior

By default, RICOH Streamline NX attempts to connect to devices via port 80. When the port 80 is closed on devices, it is necessary to modify the connection port behavior so that the Delegation Server can access the device via port 443.

Follow the procedure below to modify the setting to redirect the connection if necessary.

1. **Log-in to the Management Console using a user account that has the @RemoteCE Privilege.**
2. **Click [System] ▶ [Server Settings] ▶ [Advanced System Settings Editor].**
3. **Click [View] ▶ [Delegation Server Settings].**
4. **When applying this change on all Delegation Servers, select [Global Settings]. When applying this change to a specific Delegation Server, select the target Delegation Server.**
5. **Find the "dm.protocol.device.webservice" key, and set the option to either 0 or 1 as follows:**

   0: RICOH Streamline NX tries to connect to port 80 first if port 80 is open on the device. If the device returns a response indicating redirection to port 443, RICOH Streamline NX connects to port 443. If port 80 is closed, no redirection occurs and the connection will fail.

   1: RICOH Streamline NX connects only to port 443.
6. **Restart RICOH SLNX Delegation Server Service on each applied Delegation Server.**

Adding a Device to the Device List

This section describes how to add a device to the device list by specifying the IP address or host name of the device.

Note

- When changing the IP address or host name of the device already registered in the list, you can change the IP address or host name directly from the device properties.

Adding a device from the "Add Device" screen

Adds a device to the device list manually.

1. **In the navigation tree, click [Device List], and select a category, group, or power filter.**
2. **Click (Add device).**
3. **Select the Delegation Server to assign to the device to be added, and then enter the IP address or host name of the device.**
4. **Specify the account to be used to access the device.**

5. **Click [OK].**

Note

- If the added device matches the filter criteria of a custom group, the device is categorized in the group that the criteria matches. If there is not group that the criteria matches, the device is categorized in the "Unassigned" group.

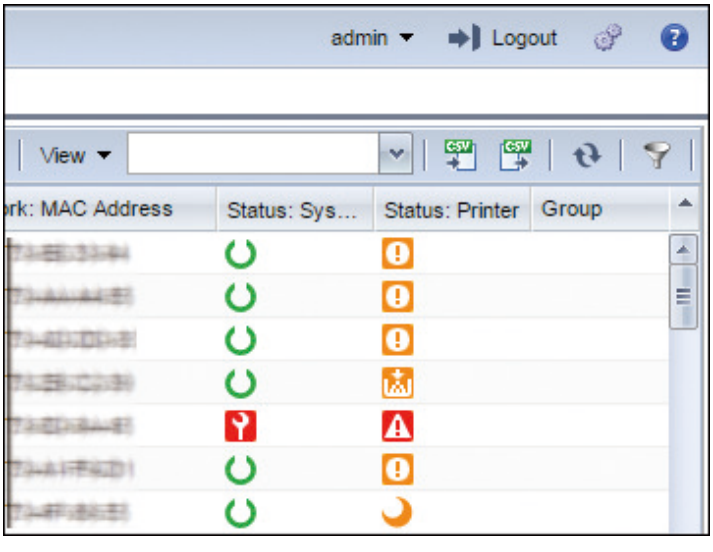
Importing devices from a CSV file

Use a CSV file to add a large number of devices at one time. You can add a device even when the device is turned off or not reachable over the network.

For the format of CSV files, see page 759 "Format of a Device Information CSV File".

A sample CSV file can be downloaded from the import screen.

1. **In the navigation tree, click [Device List], and select a category, group, or power filter.**
2. **Click (Import).**



3. **Click [Browse...] on the Import Devices screen, and then select a CSV file.**

   If you have not yet created the CSV file, click [Download Sample File] to download a sample CSV file to be used as a template.

4. **Click [Upload], and then click [OK].**

   The information imported into the device list is displayed.

Note

- The default profile that is pre-registered in the system is applied to the access account to be used to establish a connection to the device that was imported from the CSV file.

- If the device information could not be obtained while the device was being imported, the information is obtained at the timing that a connection is established by performing polling. For details about Polling, see page 89 "Checking the Device Status".

Deleting a Device from the Device List

1. **In the navigation tree, click [Device List].**
2. **Click the category or group to be deleted.**
3. **Select the device to be deleted in the list and click (Delete devices), or right-click the device and select [Delete Devices].**

   To select more than one device, select the devices while pressing the SHIFT or CTRL key.
4. **Click [Yes].**

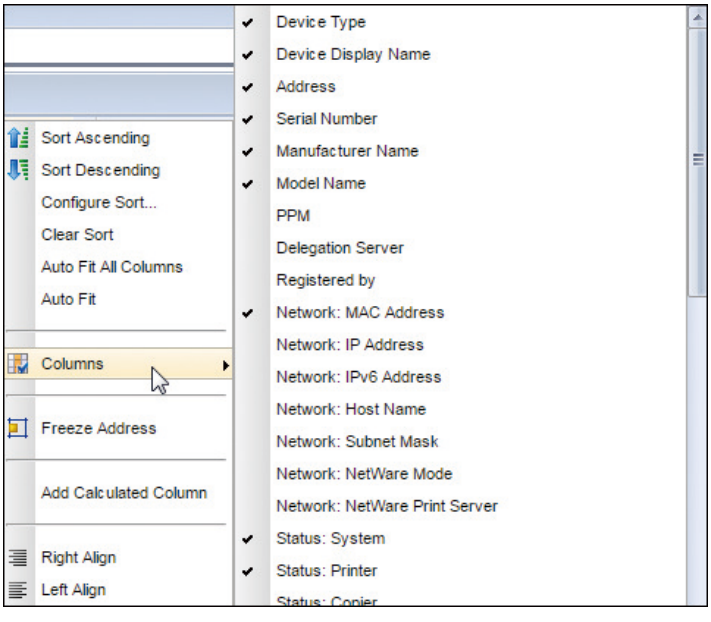
Customizing the Device List Display

You can change the displayed content of the device list according to your purpose. In addition to adding or changing columns, you can display devices on a map and use Quick Filter and Power Filter to filter devices.

Adding a Display Column

1. **In the navigation tree, click [Device List], and select a category, group, or power filter.**
2. **Right-click any column and point the cursor to [Column].**

   A list of items that can appear as columns is displayed. A check mark appears for the columns that are already displayed.



3. **Select the check boxes of the items to add as columns.**

   Clear the check box to hide the column.

Note

- To sort devices with the values displayed in the columns as reference, right-click the column, and select [Sort by Ascending Order], [Sort by Descending Order], or [Configure Sort]. When clicking [Configure Sort], you can sort devices by priority with multiple columns as reference.
- Click the [Views] menu item to save the customized display.
- You cannot share a saved view with another user.

Adding a Calculated Column

You can apply a calculating formula specified to the contents of an existing column and create a column to obtain a new value. Use this function, for example, to create a [Color Print] column to obtain the ratio of color printing from the Total and Total Color values.

1. **In the navigation tree, click [Device List], and select a category, group, or power filter.**
2. **Right-click any column, and select [Add Calculated Column].**
3. **Enter the name of the column.**
4. **Enter the formula in the [Calculation] field.**

   Specify the formula by combining the following keys and numerical expressions (+, -, *, /):

Key	Source field
A	Device Counter Total
B	Copy Black
C	Copy Color Full
D	Copy Color Twin
E	Copy Color Mono
F	Printer Black
G	Printer Color Full
H	Printer Color Twin
I	Printer Color Mono
J	Economy Color Counter
K	Fax Black
L	Fax Color Mono
M	A2
N	A3/DLT
O	Duplex Print
P	Send Color
Q	Send Mono

Key	Source field
R	Fax Send
S	Scanner Send Color
T	Scanner Send Mono
U	Total Mono
V	Total Color

For example, to obtain the total number of printers, enter [F+G+H].

Similarly, to obtain the output ratio of [Copy Black] and [Printer Black], enter [B+F].

5. **Click [OK] to save the column.**

A new column is added.

Note

- When the column appears in the [Devices] tab, the Calculated Column name is displayed in italics to distinguish it from a regular column. There are ten calculation fields available.
- To delete or edit a calculated column, right-click on the Column name and select either [Edit Calculated Column] or [Delete Calculated Column] from the menu.

Displaying Devices in a Map

You can add a map image to a group in the navigation tree and place device icons at any position on the map image. For example, use an office floor image to create a map that is visually easy to understand the location of installed devices.

Use a jpg, gif, or png file for the map image.

Adding a map

1. **In the navigation tree, click [Device List], and select a group to be added to the map.**
2. **Right-click the group name, and select [Add Map].**
3. **On the Add Map screen, click [Browse...], select a map image, and then click [Upload].**

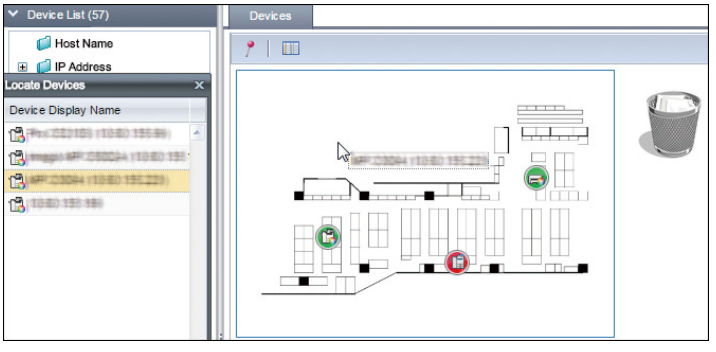
When you have successfully uploaded an image, a map icon is displayed next to the group name in the navigation tree.

To display the map, click (Map).

Locating devices on the map

1. **In the navigation tree, click [Device List], and select a group with a registered map.**
2. **Click (Map).**
3. **Click (Locate Devices).**

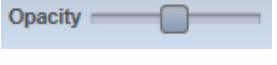
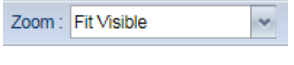
   A list of devices that belong to the group is displayed.
4. **Drag and drop the devices to be added to the map.**



5. **Click (Locate Devices) when the positioning of devices is complete.**

   Click (Device List) to return to the Device List screen.

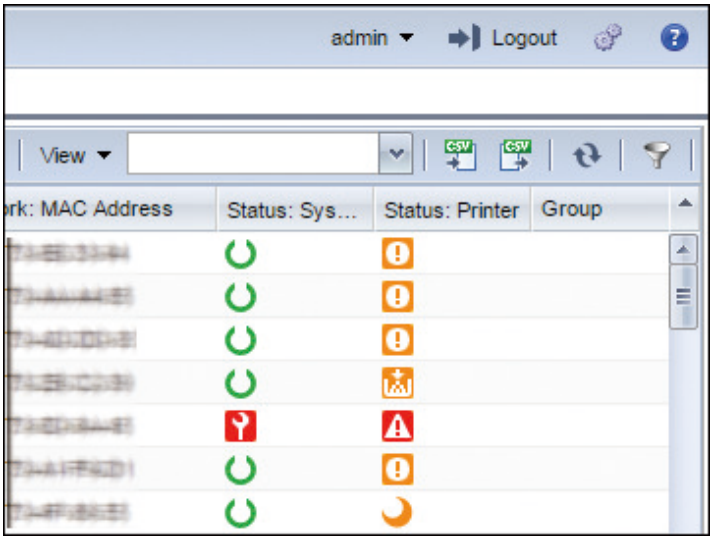
Operation icons

Icon	Description
	A device is represented by a circular icon on the map. The icon color indicates the following states: • Green: Normal • Yellow: Warning • Red: Error or offline in a state of warning / error • Gray: Offline
	Use the slider to adjust the opacity of the map image. Left: Raises the opacity of the map image. Right: Lowers the opacity of the map image.
	Specify the magnification ratio and method of the map image. • Scaling factor: 25 %, 50 %, 75 %, 100 %, 150 %, 300 % • Magnification method: Fit to page width, show entire page

Using Quick Filters

Use quick filters to enter conditions for each column and filter devices that are displayed on the device list.

1. **In the navigation tree, click [Device List], and select a category or group.**
2. **Click (Filters).**



3. **Enter the filter condition in the input field displayed above the column.**

   Depending on the column item, you can click the drop-down list and select a value as the filter condition.

4. **Click (Filters).**

   Only those devices that match the specified value are displayed.

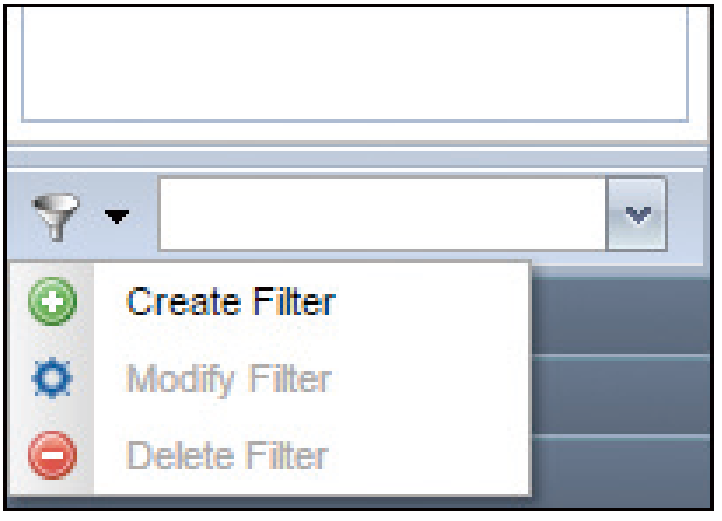
   Enter filter values into the other columns to further filter the devices that are displayed.

Using Power Filter

Use a power filter to filter all devices in the device list by specific values. Create and save a power filter to display only those devices that match a specified value in the navigation tree with one click. For example, you can display only the devices with an error as the printer status or only the devices with a counter that exceeds a specific value.

1. **In the navigation tree, click [Device List].**

2. **Click (Manage Filters) at the bottom left of the navigation tree, and select [Create Filter].**



3. **On the Create Filter screen, click [Filter Blocks], and select the type of filter condition.**
4. **Check a filter condition item from the displayed list.**

   To add another filter condition, repeat Steps 3 and 4.

   If the standard Filter Blocks do not produce the results you want, select [Custom Criteria] from the Filter Blocks list to set your own criteria.
5. **When specification of filter conditions are complete, enter the name of the power filter, and click (Save Filter).**

   The device list is updated, and only those devices that match the configured power filter are displayed.
6. **To apply a power filter, select the power filter name from the drop-down list below [Device List] in the navigation tree.**

Note

- To change the filter condition of a power filter, select the name of the power filter you want to change from the Power Filter drop-down list, click (Manage Filters), and select [Modify Filter].
- You cannot share a saved power filter with another user.

Checking the Device Status

Polling is the process of a server accessing a device to obtain the device status. Perform polling regularly and monitor the device to keep track of the device status.

To check the device status, the administrator can perform regular or period polling to obtain the following device information:

Polling type	Description	Default polling interval
Status Polling	Obtains the system status and the status of the printer, copier, scanner, and fax functions.	Every 1 hours
Supplies Polling	Obtains the status of the toner, source tray, and output tray. Although the device will be woken from energy-saving mode during this poll type, energy-saving is not canceled.	Every 3 hours
Counter Polling	Obtains the counter information such as the number of prints and copies made on the device. Although the device will be woken from energy-saving mode during this poll type, energy-saving is not canceled.	Every 6 hours
Other Polling	Obtains the device firmware and the types of Device Applications installed on the device. The Mac address or serial numbers will be refreshed upon Other polling.	Every 7 days
User Counter Polling	Obtains the counter information registered to the device for each user and the counter information of anonymous users not registered to the device. Although the device will be woken from energy-saving mode during this poll type, energy-saving is not canceled. This polling type is enabled only the RICOH devices (2005-2011 models and 2012 models and later). For details, see page 23 "List of Supported Models and Functions".	Disable

Polling type	Description	Default polling interval
Detailed Counter Polling	Obtains the itemized counter information such as the number of prints and copies made on the device. For example, you can obtain the counter information categorized in the followings: • Number of pages per job • Number of job in which duplex or booklet printing is combined with N-up printing • Number of output pages by paper type and paper size • Number of output pages by printer language and finishing function • Total number of output pages on a device and the number by function Although the device will be woken from energy-saving mode during this poll type, energy-saving is not canceled.	Disable
Error Polling	Performs Status Polling on the device in which an error is occurring, and obtains the device status.	Disable

Note

- A polling task for all devices (default) is pre-registered in the system. The default Start Date and Time is set based on the RICOH Streamline NX system installed date and time.
- Ensure you create notifications to receive warning when a device problem is detected, including toner outages. For details, see page 94 "Notifying the Device Status by E-mail".

Creating a Polling Task

Create a polling task to monitor the device status regularly.

The types of polling that can be performed in a polling task are as follows:

- Status Polling
- Supplies Polling
- Counter Polling

- Other Polling
- User Counter Polling
- Detailed Counter Polling

For details about Error Polling, see page 92 "Creating an Error Polling Task".

1. **Click the following items in the navigation tree to open the [Polling] tab.**

   [Discovery & Polling] ▶ [Polling]

2. **Click (Add).**
3. **Enter the task name and description on the [General] tab.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **On the [Target Devices/Groups] tab, specify the devices or groups for which to obtain the device information.**

   1. Click (Add Device) or (Add Group).
   2. Select the target device or group.
   3. Click [OK].

5. **On each polling tab, configure the execution schedule.**

   If there are specific times when you do not want to use network resources to run the poll, click [Advanced Settings] then set the times when the poll will not occur. For example, if your network is particularly busy between 9 and 11 am, enter 9:00 as the start time and 11:00 as the finish time to prevent the profile from running within this timeframe.

6. **Click (Save) when the settings are complete.**

   A profile for obtaining the device information is added to the list. To perform polling immediately, click ▶ (Immediately).

Note

- For details about the setting items on each tab, see page 469 "Polling".
- A device in energy saver mode recovers from the energy saving state when Other Polling is performed on the device.
- In cases where a single device is targeted for multiple polling tasks that are scheduled at the same time, polling is performed only once, and the required poll types are obtained all at once.
- If polling starts before the prohibited time, the in-process polling continues.

Creating an Error Polling Task

When an error occurs on a device, it will be notified from the device by SNMP Trap. However, whether the error has been resolved or not needs to be notified by Status Polling.

Use an error polling task to perform status polling only on the devices in which errors occurred. For example, you can monitor the error status more accurately by specifying an interval that is shorter than the interval specified for a normal status polling for the error polling task.

1. **Click the following items in the navigation tree to open the [Error Polling] tab.**

   [Discovery & Polling] ▶ [Error Polling]

2. **Click (Add).**
3. **Enter the task name and description on the [General] tab.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **On the [Target Devices/Groups] tab, specify the devices or groups for which to obtain the device information.**

   1. Click (Add Device) or (Add Group).
   2. Select the target device or group.
   3. Click [OK].

5. **Select the type of the error information to be obtained on the [Triggers] tab.**
6. **Configure the schedule to execute Error Polling on the [Schedule] tab.**
7. **Click (Save) when the settings are complete.**

Note

- For details about the setting items on each tab, see page 469 "Polling".

Performing Polling Immediately from the Device List

1. **Select the target device in the device list.**

   To specify more than one device, select the devices while pressing the SHIFT or CTRL key.

2. **Right-click the selected device, and select [Request Polling].**
3. **Select the types of information to be obtained, and click [OK].**

   The polling result is applied to the target device.

Note

- A device in energy saver mode recovers from the energy saving state when Other Polling is performed on the device.

View Polling Times

You can view the last polling time for a device if you show the Polling Columns in the [Devices] tab. This information is a good indicator of how long the device has been in the current status.

1. **Select a category or group from the [Device List] to populate the [Devices] tab.**
2. **Right-click on any column name in the [Devices] tab, and select [Columns] from the menu.**
3. **Scroll down the list of available columns until you reach the Date/Time poll options.**
4. **Select the poll options that you want to appear in the [Devices] tab.**

   Selected options show a checkmark to the left of the option.
5. **Click away from the menu to close it and update the column display in the [Devices] tab.**

   You can hover your mouse over any poll time to view a tooltip showing complete details.

Notifying the Device Status by E-mail

The system can be configured to send a notification by e-mail such as when a new device is discovered on the network or device error information is obtained. There are two types of notifications: discovery notification and polling notification.

Discovery notification

Configure a discovery notification if you want to be notified when the conditions to send a notification are fulfilled by discovery.

Polling notification

Configure a polling notification if you want to be notified when the conditions to send a notification are fulfilled by polling.

Configuration notification

Configure a configuration notification if you want to be notified when the conditions to send a notification are fulfilled by configuration task.

1. **page 95 "Configuring the E-mail Server"**

To send notification messages, configure the SMTP server information.

2. **page 95 "Creating a Destination"**

Register the destination e-mail addresses. In addition, specify the application to process the notification.

Note

- You can register multiple e-mail addresses to the address list under the [System] [Server Settings]. For details, see page 535 "Email Address".

3. **Creating a Notification Policy**

Notification Policy is a group of settings that include the conditions to send notifications, the message contents, and the target devices. There are two types of notification policy: discovery notification policy and polling notification policy.

- page 96 "Creating a Polling Notification Policy"
- page 98 "Creating a Discovery Notification Policy"
- page 100 "Creating a Configuration Alert Policy"

Configuring the E-mail Server

1. **Click the following items in the navigation tree to open the [Networking] tab.**

   [System] ▶ [System Settings] ▶ [Networking]

2. **Configure the e-mail server to deliver notifications.**

   In "Email Server Setting", specify the SMTP Server Address and other required information. For details about the setting items, see page 522 "Networking".

3. **Click [Save].**

Creating a Destination

Notification destinations must be registered to create a notification policy. There are two kinds of notification destinations as follows:

E-mail

Specify the e-mail address to deliver the message.

Application

Select the application to be executed.

1. **Click the following items in the navigation tree to open the [Destinations] tab.**

   [System] ▶ [Notifications] ▶ [Destinations]

2. **Click (Add).**
3. **In [Destination Name], enter the destination name.**

   When creating Discovery or Polling profiles, you are required to pick from the list of the Destinations, so ensure the destination name reflects the contents of the destination.

4. **In [Notification Type], select either [Email] or [Execute an application].**
5. **Specify the destination.**
   - When [Email] is selected in [Notification Type], specify an e-mail address. Click [Address List] to select the e-mail address, or enter the e-mail address manually. To enter more than one e-mail address, separate each address by a comma (,).
   - When [Execute an application] is selected in [Notification Type], enter the file path of the application to be executed.
6. **Select [Language].**
7. **Select the Security Group Context.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

For the security group context, see page 167 "Configuring Group Restrictions".

8. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 568 "Destinations".

Creating a Polling Notification Policy

Configure the settings to send a notification when a device is in a certain status. Notification Policy also includes the settings for the notification destinations, the message contents, and the target devices.

1. **Click the following items in the navigation tree to open the [Policies] tab.**

   [System] ▶ [Notifications] ▶ [Policies]

2. **Click (Add).**

   The dialog box for specifying the policy type is displayed.

3. **Enter the policy name.**

4. **Select [Type] in the [Polling] menu.**

   You will not be given the opportunity to change the Definition Type once you set it here, so ensure you select the right type before clicking Save.

5. **Select [Destination].**

   If the destination list is empty, complete the instructions in page 95 "Creating a Destination", then return to these instructions.

6. **Click [Save].**

   The name of the policy entered in Step 3 is displayed in the list.

7. **Select the destination on the [General] tab.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

8. **Specify the device status for sending a notification on the [Triggers] tab.**

   The statuses such as [Paper Misfeed] and [Service Code] can be specified. For details about the setting items, see page 563 "Policies".

   Note

   - You can enable the [Advanced Criteria] checkbox if you prefer to combine various status (Printer, Copier, Fax, Scanner or System), or to set an alert on advanced options such as Total Device Counters, Input/Output Tray level or status, toner level, etc. If you enable the

checkbox, you will see a warning message informing you that continuing will erase all simple criteria selections made thus far.

9. **Specify the conditions for sending notification on the [Conditions] tab as necessary.**

   You do not have to make any selection on this tab. For example, you can specify the device status selected on the previous tab must be present for one hour before the notification is sent.

   For details about the setting items, see page 563 "Policies".

10. **Configure the message to be sent as necessary.**

    When a language other than English is specified for the destination language, create a message that corresponds to the destination language. A message in English is sent to the destination even when you have not created a message in the same language as the destination language.

    To create a message, use the following procedure:

    1. Click (Add) on the [Messages] tab.
    2. Select the [Language] of the message to be sent, and enter the [Subject] and [Body].

       Right-click the [Subject] or [Body] input field to display the list of usable variables. The following items are available as usable variables:

Variable	
Device Status*	Input Tray Status
Controller Version	Notification Name
Copier Status*	Output Tray Capacity
Device Counters Total*	Output Tray Name
IP Address	Output Tray Status
MAC Address	Printer Status*
Device Display Name	Printer Version
Device Polling Date*	Scanner Status*
Device Serial Number*	Server Date
Device URL	System Country
Device Display Name (list)	System Status*
Discovered Devices Count	System Version
Delegation Server Name	Toner Details
Fax Status*	Toner Level

Variable	
Input Tray Capacity	
Input Tray Name	

* The state at, or just before the time the notification is sent

Note

- Within polling notifications the Discovered Device Count variable always returns a value of 0.If you add the $[discovery_devicecount]$ variable to the message body within a polling notification, the value will therefore be displayed as 0. However, within discovery notifications the Discovered Device Count is equal to the number of discovered devices. If you add the $[discovery_devicecount]$ variable to the message body you will see the actual number of discovered devices.

3. To create a message in another language, change [Language] and repeat Steps 1 and 2.
4. Click (Save).

11. Configure the devices or groups to be monitored on the [Monitored Devices] tab.

12. Click (Save) when the settings are complete.

Creating a Discovery Notification Policy

Create a discovery notification policy to send a notification when a new device is added to the device list in the Management Console.

1. Click the following items in the navigation tree to open the [Policies] tab.

[System] ▶ [Notifications] ▶ [Policies]

2. Click (Add).

The dialog box for specifying the policy type is displayed.

3. Enter the policy name.

4. Select [Discovery] in the [Type] menu.

You will not be given the opportunity to change the Definition Type once you set it here, so ensure you select the right type before clicking Save.

5. Select [Destination].

If the destination list is empty, complete the instructions in page 95 "Creating a Destination", then return to these instructions.

6. Click [Save].

The name of the policy entered in Step 3 is displayed in the list.

7. **Select the destination on the [General] tab.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

8. **Specify the device status for which to send notification on the [Triggers] tab as necessary.**

   Device statuses such as [Paper Misfeed] and [Service Code] can be specified. When a device status is specified, a notification is sent only when the status of the newly discovered device matches the specified status.

   If no device status is specified, a notification is sent regardless of the status of the newly discovered device.

   For example, the notification will be sent when 10 or more new devices are discovered, select the [Advanced Criteria] check box, and configure as follows:

Variable	Conditions	Value
Discovered Device Count	greater than	9

9. **Configure the message to be sent as necessary.**

   When a language other than English is specified for the destination language, create a message that corresponds to the destination language. A message in English is sent to the destination even when you have not created a message in the same language as the destination language.

   To create a message, use the following procedure:

   1. Click (Add) on the [Messages] tab.
   2. Select the [Language] of the message to be sent, and enter the [Subject] and [Body].

      Right-click the [Subject] or [Body] input field to display the list of usable variables. The following items are available as usable variables:

Variable	
Device Status*	Input Tray Status
Controller Version	Notification Name
Copier Status*	Output Tray Capacity
Device Counters Total*	Output Tray Name
IP Address	Output Tray Status
MAC Address	Printer Status*
Device Display Name	Printer Version

Variable	
Device Polling Date*	Scanner Status*
Device Serial Number*	Server Date
Device URL	System Country
Device Display Name (list)	System Status*
Discovered Devices Count	System Version
Delegation Server Name	Toner Details
Fax Status*	Toner Level
Input Tray Capacity	
Input Tray Name	

* Current or Previous

Note

- Within discovery notifications the Discovered Device Count is equal to the number of discovered devices. If you add the $[discovery_devicecount]$ variable to the message body you will see a real number of the discovered devices.

3. To create a message in another language, change [Language] and repeat Steps 1 and 2.
4. Click (Save).

10. Configure the groups to be monitored on the [Monitored Devices] tab.

11. Click (Save) when the settings are complete.

Creating a Configuration Alert Policy

Create a configuration alert policy to send a notification when the device settings have been modified by a configuration task.

Note

- Your user access role must have DeviceAdvancedRead permissions to view this feature, and DeviceAdvancedWrite permissions to add, update, or remove Configuration Alert policies. For information on permissions, see page 160 "Managing User Roles and Privileges".

1. Click the following items in the navigation tree to open the [Configuration Alerts] tab.

[System] ▶ [Notifications] ▶ [Configuration Alerts]

2. **Click (Add).**
3. **Enter the policy name.**
4. **Click either [Input Email Address Manually] or [Select Destination].**

   If you selected [Input Email Address Manually], enter the e-mail address of the recipient and specify the language.

   If you selected [Select Destination], select a destination from the [Destinations] drop-down menu.
5. **Select the Security Group Context.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".
6. **Select the check box of the device setting to be used as the notification criteria on the [Attributes].**
7. **Configure the devices or groups to be monitored on the [Monitored Devices] tab.**
8. **Click (Save) when the settings are complete.**

Managing the Device Settings

Use the device preferences templates to configure the device settings such as time zone and function settings on multiple devices at one time. There are two types of device settings templates as follows:

Important

- **To use the device settings template, the access accounts of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.**

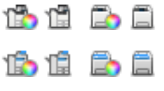
Standard Device Preferences template

You can edit the setting items as required. This template is useful for updating general setting items that do not depend on the model. Secure information such as password and SNMP community name cannot be obtained when the settings are retrieved from the device.

Device-Specific Preferences template

While you cannot edit the setting items, you can copy device settings to devices with the same model, configuration, and region (North America/Europe/Asia). This template is useful for configuring a large number of the same model devices using the standard settings. You can obtain secure information such as password and SNMP community name, but such information is not displayed in the Management Console to prevent the information from being leaked or tampered.

Use the device icons to identify the supported template types.

Description	Device-Specific Preferences template	Standard Device Preferences template
Device icon		
Retrieval of device secure information	Yes	No
Viewing of secure information	No	No
Applying of secure information of the device	Yes	Yes
Editing of obtained setting values	No	Yes
Retrieval of an image for use on the home screen	Yes	No

Note

- You can configure the items marked with a dagger mark (†) in the device preferences template after you activating the advanced license. For details about the configuration items, see page 643 "List of Device Preference Setting Items".

Creating a Standard Device Preferences Template

Create a new standard device preferences template, and configure the device settings. You can obtain the setting values from a specific device or import them from a CSV file.

1. **Click the following items in the navigation tree to open the [Standard Device Preferences] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Standard Device Preferences]

2. **Click (Add).**
3. **Enter the template name and description on the [General] tab.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the method of creating the template.**

   Create Blank Template

   Creates a template by specifying new setting values.

   Get Data from Device

   Obtains the settings from a specified device. Secure information such as passwords and security settings cannot be obtained.

   1. Click [Select Device].
   2. Select the device from which to obtain the settings, and click [OK].

   Import CSV File

   Imports the template CSV file.

   1. Click [Browse...].
   2. Specify the CSV file to be imported, and click [Open].

5. **Click [OK].**
6. **Configure the required items on the [Standard Device Preferences] tab.**
7. **Click (Save) when the settings are complete.**

Note

- For details about the configuration items, see page 643 "List of Device Preference Setting Items".
- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".

Creating a Device-specific Preferences Template

Specify a device and directly obtain its current configuration, or import the configuration file exported from the device to create a device-specific preferences template.

1. **Click the following items in the navigation tree to open the [Configuration Templates] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Device-specific Preferences]

2. **Click (Add).**
3. **Enter the [Template Name] and [Description].**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the method of creating the template.**

   Get Encrypted Settings from Device

   Obtains the current setting values from the device. Secure information such as passwords and security settings can be obtained.

   1. Click [Select Device].
   2. Select the device from which to obtain the settings, and click [OK].
   3. Enter a password.

      The entered password is used to encrypt and decrypt the settings data obtained from the device.
   4. To obtain the logo image on the home screen configured on the device, select the [Logo File] check box.

   Import Encrypted Settings from File

   Imports the settings file exported from the device and stored on the computer.

1. Enter the password that was specified when the settings file was created.
2. Click [Browse] under [Settings File] to specify the setting file.
3. To import a logo image to be displayed on the home screen, click [Browse] under [Logo Image], and then specify the image file.

Get Smart Operation Panel Settings from Device

Obtains the current setting values from the device equipped with Smart Operation Panel.

1. Click [Select Device].
2. Select the device from which to obtain the settings, and click [OK].

5. **Click [OK].**

Importing of the data starts. It may take a few minutes until importing is completed.

6. **Click (Save) when the settings are complete.**

Note

- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".

Updating the Firmware

Use the firmware template to update the firmware of the devices.

Important

- **To use the firmware template, the access accounts of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.**

1. **Click the following items in the navigation tree to open the [Firmware] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Firmware]

2. **Click (Add).**
3. **Enter the [Template Name] and [Description].**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the software selection method.**

   Download from RICOH Software Server

   Downloads the firmware from the Ricoh server. The firmware can be updated to the latest version supported by the device.

   Note

   - The device model is not specified and the firmware will not be downloaded at the time of template creation. Instead, the device model is sent to the RICOH Software Server and the firmware is downloaded whenever the template is applied to a specific MFP. As a result, each different model may receive different firmware from the RICOH Software Server. In this case, the firmware license agreement will be a general binding agreement. In addition, partial firmware upgrades are not possible using this method – use local firmware packages upgrades instead.

   Use File in Repository

   Select the firmware from the repository. Select the firmware to be used for updating from the list.

   Upload New File to Repository

   This method is used only to update custom-made firmware by RICOH, and it is not normally used.

   Uploads the firmware to the repository. Select the uploaded firmware from the list.

5. **Click [OK].**

Note

- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".

Managing the SDK/J Platform

Use the SDK/J Platform template to update the SDK/J platform installed on the device.

Important

- **To use the SDK/J platform template, the access accounts of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.**

1. **Click the following items in the navigation tree to open the [SDK/J Platform] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [SDK/J Platform]

2. **Click (Add).**
3. **Enter the template name and description.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the method for selecting the SDK/J platform.**

   Download from RICOH Software Server

   You can update to the latest SDK/J Platform by connecting to RICOH Software Server via the Internet.

   Select your country or the closest country in the [Country] list.

   Use File in Repository

   In the list, select the SDK/J platform package to be included in the template. The supported model names for each package are displayed in the list.

   Use the Ricoh server to manage the Device Applications.

   Upload New File to Repository

   Uploads the SDK/J platform file to the repository. You can select uploaded file in the list. This method is used only to apply a custom package, and it is not used normally.

5. **Click [OK].**

Managing Device Applications

Use the Device Applications template to install, activate, update, or uninstall the Device Applications on the device.

Important

- To use the SDK/J platform template, the access accounts of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.
- Streamline NX Embedded Applications cannot be installed on devices without HDD even if they are listed in the table on page 23 "List of Supported Models and Functions".
- Streamline NX Embedded Applications cannot be managed using RICOH Software Server. Use the "SLNX3.X Embedded Install" template that is registered in the system to install Streamline NX Embedded Applications.
- When installing a Streamline NX Embedded Applications, configure the Streamline NX Embedded Applications in advance before executing the Device Applications template. Follow the steps in to apply the settings on the device page 122 "Managing the Streamline NX Embedded Settings".

1. **Click the following items in the navigation tree to open the [Device Applications] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Device Applications]

2. **Click (Add).**
3. **Enter the [Template Name] and [Description].**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the method for selecting the Device Application.**

   RICOH Software Server

   Use RICOH Software Server to manage Device Applications. You can obtain the latest Device Application by connecting to RICOH Software Server via the Internet.

1. Select one of the following operations to perform on the Device Application.
   - [Download from RICOH Software Server]
   - [Uninstallation]
   - [Activate]
2. Select your country or the closest country in the [Country] list.
3. Enter the product key of the Device Application.
4. Click [Retrieve Application List], and select the Device Application to be included in the template.

RICOH Software Server cannot be selected depending on the type of the Device Application.

Local File

Use the repository to manage Device Applications. Upload the Device Applications manually to the repository

This method is used to manage non-RICOH Device Applications or Device Applications that are not registered to RICOH Software Server.

- [Use File in Repository]

  Select the Device Application to be included in the template in the list.

- [Uninstallation]

  Select the Device Application to be uninstalled from the [Application Name (Product ID)] menu.

  The list of applications obtained from the device information is displayed for the selection items in the menu.

- [Upload New File to Repository]

  Uploads the file of the Device Application to the repository. You can select the uploaded file in the list. This method is used only to apply a custom package, and it is not normally used.

5. Click [OK].

Note

- If the selected application is compatible with Smart Operation Panel models only, the application is applied to Smart Operation Panel models and all other models will be skipped.
- If the available free space on the machine to install an SDK application is insufficient, the SDK application will not work properly. If error code "277" appears in the task log, delete SDK applications that are not necessary from the machine to allocate sufficient free space. If allocating sufficient free space is still not possible, contact your RICOH service representative.
- On 2015 models and later, use the following procedure to check the available free space on the machine:

1. Log in to Web Image Monitor of the machine with the administrator privileges.

   For details about the login procedure, see the operation manual of the machine.

2. From the top screen of Web Image Monitor, open the following menu screen:

   [Device Management] ▶ [Configuration] ▶ [Extended Feature Settings] ▶ [Administrator Tools]

3. Check “Remaining Free Space”.

- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".

Managing the Address Book

Use the Address Book template to manage the user information to be registered to the device address book. You can also specify whether to collect or reset the counter per user before applying the Address Book template.

Important

- **To use the Address Book template, the access account of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.**
- **If your Address Book data is encrypted, it may take longer or possibly result in failure when creating the template (when the Address Book data is exported from the device) or when executing the task (when the Address Book data is imported between RICOH Streamline NX and the device). Refer to the device's security guide (refer to the section concerning Preventing Leakage of Information from Machines) for detailed information about how to configure the Address Book data encryption and the Machine Data encryption.**

1. **Click the following items in the navigation tree to open the [Address Book] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Address Book]

2. **Click (Add).**
3. **Enter the template name and description.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Specify the method for creating the template.**

   Create Blank Template

   Creates user information by editing the information directly. Select one of the following methods for authenticating the user information to be registered.

   - [User Code]/[None]
   - [Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Server]

   Get Editable Settings from Device

   Obtains the address book information from a device. Click [Select Device] to select the device from which to obtain the address book.

   Get Encrypted Settings from Device

   Obtains the address book information after it is encrypted. Click [Select Device] to select the device from which to import the address book. The encrypted user information cannot be edited in the Management Console.

Import Editable Data from File

Imports the data file of the address book. Secure information such as passwords cannot be imported. Click [Browse] to specify the file path.

Note

- When you import the CSV file which you edited, please surround the value with "[" and "]" in the file. Because the spreadsheet application (Microsoft EXCEL, etc.) treats the string value such as FAX numbers as a numerical value, the application may automatically delete the head of "0"s from the string value. In this case, the settings in the CSV file cannot be imported normally.

Import Encrypted Data from File

Imports the data file (udf format) of the encrypted address book. Click [Browse] to specify the file path. The encrypted user information cannot be edited in the Management Console.

Import Data from SmartDeviceMonitor for Admin/Ridoc IO Analyzer

Imports the data file of SmartDeviceMonitor for Admin/Ridoc IO Analyzer. Click [Browse] for [File Path (Address Management Tool)] and [File Path (User Management Tool)] to specify the file path.

5. **Click [OK].**
6. **Click the [Settings] tab, and configure the setting items required to apply the template.**

   Specify whether or not to reset the volume use counter and delete the address book registered to a device.
7. **Click the [Entry List] tab, and configure the user information.**

   For details about the setting items, see page 487 "Address Book".

   The Address Book contents cannot be edited depending on the method the template was created. If the Address Book can be edited, you can include secure information such as password in the Address Book template to be applied on a device. However, it is impossible to check whether the secure information specified in the Address Book template is the same as the information already specified in the Address Book of the device.
8. **When the settings are completed, click (Save) on the [Entry List] tab, and then click (Save) on the [Address Book] tab.**

Note

- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".

Managing Device Logs

Information such as the usage of device features and changes in the device status is recorded and stored in each device. This information is called a device log.

Use the Log Collection template to change the type of device logs to be collected. You can also delete the log data stored in a device.

For details about the device logs, see "Managing Logs", Security Guide that is provided with the device.

Important

- **To use the device log template, the access accounts of SNMP, Device Administrator, and SDK/J are required. The template may not be executed properly when the access account are not configured.**

1. **Click the following items in the navigation tree to open the [Log Collection] tab.**

   [Configuration] ▶ [Configuration Templates] ▶ [Log Collection]

2. **Click (Add).**
3. **Enter the template name and description.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".
4. **Click [OK].**
5. **Configure the settings related to the device log on the [Log Collection] tab.**

   Delete Log data in Device

   Deletes all the log data stored in a device.

   Log Transfer Settings

   Specify whether or not to encrypt the device log upon transferring, and also select the type of the device log to be collected.
6. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 498 "Log Collection".
- To execute a template, register the template to a task first. For details, see page 116 "Registering a Template to a Task".
- You can manage the device log collection function and export the device logs from [System] ▶ [Server Settings] ▶ [Device Log Management] in the navigation tree. For details, see page 533 "Device Log Management".

- Depending on the job contents, the device log records general information, source information, and destination information.
  If the job log that is written in a CSV file has a job that contains the source and destination information, the destination information is copied to the source information.
  Therefore, make sure that the destination information is not copied repeatedly when the device status is obtained from the destination information in the CSV file.
  - For example, when the following three files are stored in the document box, three sheets will be printed when you select and print documents A, B, and C:
    - Document A: 1 page (source information 1)
    - Document B: 1 page (source information 2)
    - Document C: 1 page (source information 3)
  - When you output the log and export it to a CSV file, a total of nine copies are output including the three-line destination information. (Plot ping pages)
    - Document A: 3 (destination information 1)
    - Document B: 3 (destination information 1)
    - Document C: 3 (destination information 1)

Registering a Template to a Task

You can execute a created template against devices by registering the created template to a task. Register the template to be added to a task, a target device, or execution schedule as a task. The procedure to create a task is the same for all [Configuration Templates].

1. **Click the following items in the navigation tree to open the [Configuration Tasks] tab.**

   [Configuration] ▶ [Configuration Tasks]

2. **Click (Add).**
3. **On the [General] tab, enter the name and description.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **Select [Check] or [Apply] as the method for executing the template.**

   Check

   The configuration in the template is compared with that of the target device, and the result is recorded in a log. No change is made to the target device.

   Apply

   The configuration in the template is applied to the target device.

5. **Click (Select Target Template) on the [Template] tab.**
6. **Select the template to be registered to the task in the [Target Template] list, and click [OK].**

   Select the [Switch into Energy Saver Mode after Execute Template] or [Force Reboot after Template Execution] check box as necessary.

   For example, you can use [Force Reboot after Template Execution] to check the device configuration and reboot the devices periodically.

7. **On the [Target Devices/Groups] tab, specify the devices or groups that are the target of the task.**

   1. Click (Add group) or (Add Devices).
   2. Add the target devices or groups to the [Target Device] or [Target Groups] list, and then click [OK].

8. **On the [Schedule] tab, configure the date, time, and interval to perform the task.**

   When [Disable Schedule] is checked, this task will not run as per the set schedule. Use this feature to temporarily disable the task, or use the (Delete) button to remove the task.

If you select [Once Only] as the schedule type, the task will run when you click the (Save) button.

To specify a time period that is exempt from the task, select the [Advanced Settings] check box.

9. **On the [Notification] tab, specify whether or not to receive a notification when a task is completed.**
10. **Click (Save) when the settings are complete.**

Click (Run) to execute the task immediately.

Note

- For details about the setting items, see page 501 "Configuration Tasks".
- To display the list of registered tasks, select [System] [Scheduled Tasks] in the navigation tree.
- Execute a configuration task at times other than business hours whenever possible.
- If 213 and 214 errors occur in the task log after executing a configuration task, reboot the corresponding device immediately.

Rebooting a Device

You can create a task to reboot a device according to a preset schedule.

Important

- To execute a reboot, the following access account is required according to the target device.
  - Device Administrator Account: Ricoh devices of models 2007 to 2011 or 2012 and later
  - SNMP account: Devices other than above
- For the device models, see page 23 "List of Supported Models and Functions".

1. **Click the following items in the navigation tree to open the [Configuration Tasks] tab:**

   [Configuration] ▶ [Configuration Tasks]

2. **Click (Add).**
3. **On the [General] tab, enter the name and description.**

   When Group Restrictions is enabled in the security settings, the Security Group Context item is displayed, and restrictions are applied to the device group that is the target of the template.

   For details about Security Group Context, see page 167 "Configuring Group Restrictions".

4. **Select [Reboot] for the type of operation.**

   You cannot run a Reboot task and configuration templates at the same time. Therefore, when you select [Reboot], the [Template] tab is disabled and removed from view.

5. **Specify the devices or groups to be rebooted on the [Target Devices/Groups] tab.**

   1. Click (Add Group) or (Add Device).
   2. Select and add the target devices or groups to the [Target Device] or [Target Groups] list, and then click [OK].

6. **On the [Schedule] tab, configure the date, time, and interval to reboot the device.**

   If you select [Once Only] as the schedule type, the task will run when you click the (Save) button.

   To specify a time period that is exempt from the task, select the [Advanced Settings] check box.

7. **On the [Notification] tab, specify whether or not to receive a notification when a task is completed.**

   Specify either Input Email Address Manually or Select Destination.

   You can select the destination from the e-mail destinations configured in [System] ▶ [Notifications] ▶ [Notify to]. For details, see page 95 "Creating a Destination".

8. **Click (Save) when the settings are completed.**

   Click ▶ (Run Immediately) to execute the task immediately.

Note

- Execute a configuration task at times other than business hours whenever possible.
- If 213 and 214 errors occur in the task log after executing a configuration task, reboot the corresponding device immediately.

Managing the Power Status of Devices

You can create tasks for changing the device status. These tasks can be executed on a configured schedule indicating when the device enters or recovers from energy saver mode.

For example, configure two tasks for the device to enter energy saving mode at 7:00 PM every night and recover from energy saver mode at 6:00 AM every morning as shown below:

- Task to set the device in energy saver mode
- Task to recover the device from energy saver mode and enter standby mode

Important

- **To execute an energy saver mode task, the SNMP access account is required.**

1. **Click the following items in the navigation tree to open the [Configuration Tasks] tab.**

   [Configuration] ▶ [Configuration Tasks]

2. **Click (Add).**
3. **On the [General] tab, enter the name and description.**

   The security group items are displayed when the group restriction function is enabled in the security settings, and you can restrict the device group to be specified for the template target.

   For the security group context, see page 167 "Configuring Group Restrictions".

4. **For the operation type, select [Energy Saver Mode] or [Cancel Energy Saver Mode].**
5. **Specify the devices or groups for which to change the Energy Saver Mode on the [Target Devices/Groups] tab.**

   1. Click (Add Group) or (Add Device).
   2. Select and add the target devices or groups to the [Target Device] or [Target Groups]list, and then click [OK].

6. **On the [Schedule] tab, configure the date, time, and interval to change the Energy Saver Mode of the device.**

   If you select [Once Only] as the schedule type, the task will run when you click the (Save) button.

   To specify a time period that is exempt from the task, select the [Advanced Settings] check box.

7. **Specify whether or not to receive a notification when a task is completed on the [Notification] tab.**

   Specify either Input Email Address Manually or Select Destination.

   You can select the destination from the e-mail destinations configured in [System] ▶ [Notifications] ▶ [Destination Address]. For details, see page 95 "Creating a Destination".

8. **Click (Save) when the settings are complete.**

   Click (Run Immediately) to execute the task immediately.

Note

- Execute a configuration task at times other than business hours whenever possible.
- If 213 and 214 errors occur in the task log after executing a configuration task, reboot the corresponding device immediately.

Managing the Streamline NX Embedded Settings

You can manage the settings related to authentication and printing for devices with RICOH Streamline NX specific Embedded Applications installed. You can configure the following item types:

- The settings of the login screen displayed on a device
- The operational settings of a device when user authentication is performed
- The priority setting of user authentication
- The settings of print job display method

You can also specify the Delegation Server for performing authentication, printing, and delivery functions.

Combine these settings to create a device template, and apply the template to the device running the RICOH Streamline NX-specific Embedded Applications.

Important

- **The access accounts of SNMP, Device Administrator, and SDK/J Platform are required to manage Streamline NX Embedded Applications.**
- **Before installing Streamline NX Embedded Application on a device, configure the device settings by following the procedure described below.**

1. **page 123 "Configuring the Login Screen of a Device"**

   Customize the screen image and buttons displayed when a user logs in to a device. You can also select from preset login screens.

2. **page 124 "Configuring the Device Operations when Authenticating Users"**

   Configure the card reader settings and login method.

3. **page 124 "Configuring the Priority Order of User Authentication"**

   Create a list of priority order for authentication profiles. A user performs authentication on a device, starting with the authentication profile with the highest order of priority.

4. **page 125 "Configuring the Display Method of Print Jobs"**

   Configure the settings such as the sort order of the jobs to be displayed on the print screen.

5. ▶ page 511 "Embedded Setting"

Combine the settings configured in Steps 1 through 4 to configure a template. You can also specify the Delegation Server for performing authentication, printing, and delivery functions. To apply the configured settings to a device, save the settings and specify the target device.

Note

- For details about the document delivery application of RICOH Streamline NX, see page 219 "Managing Document Delivery Functions".
- When a Delegation Server (Delegation Server Failover/Load Balancing Groups) is not specified in [Embedded Setting], the Delegation Server with the installed Streamline NX Embedded Application performs authentication, printing, and delivery functions.
- To specify a Delegation Server (Delegation Server Failover/Load Balancing Groups) in [Embedded Setting], create a group in [Server Management] ▶ [Delegation Server Failover/Load Balancing Groups]. For details, see page 383 "Balancing the Workload among Servers".
- To uninstall a Streamline NX Embedded Applications from a device, use the Device Applications template to perform uninstallation. For details, see page 109 "Managing Device Applications".

Configuring the Login Screen of a Device

1. **Click the following items in the navigation tree to open the [Embedded Login Screen] tab.**

[Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Embedded Login Screen]

2. **Click (Add).**
3. **Enter the screen name and description on the [General] tab.**
4. **Configure the login screen on the [WVGA], [4.3 inch], or [Smart Operation Panel] tab.**

   Configure the screen background color, message, button style, and other settings.

   To upload a new image file, click [Browse] to select the image file, and then click [Upload].
5. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 504 "Embedded Login Screen".

Configuring the Device Operations when Authenticating Users

1. **Click the following items in the navigation tree to open the [Embedded Authentication] tab.**

   [Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Embedded Authentication]

2. **Click (Add).**
3. **Enter Configuration Name and its description.**
4. **Click the [Card Reader] menu, and specify whether or not to use a card reader, and the type of the card reader to be used.**
5. **Click the [Login Screen] menu, and select the login screen to be displayed on the device.**
6. **Click the [Prioritized Application] menu, and select the screen to be displayed after the user logs in.**
7. **Configure other items as necessary.**
8. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 508 "Embedded Authentication".

Configuring the Priority Order of User Authentication

1. **Click the following items in the navigation tree to open the [Authentication Priority List] tab.**

   [Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Authentication Priority List]

2. **Click (Add).**
3. **Enter Priority List Name and its description.**
4. **Click the [Authentication Order] tab.**
5. **Click (Add) to select an authentication profile, and then click [OK].**
6. **Click (Up) or (Down) to change the priority of the authentication profile.**
7. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 510 "Authentication Priority List".
- When users who have the same user name and password exist in more than one domain, the user to be authenticated is selected in the following order:
  1. The user who is identifiable by the specified domain*1

2. Local user
3. The user who is included in the authentication priority list and registered in the Management Console
4. The user who is included in the authentication priority list but not registered in the Management Console

*1 Add the domain name to the user name in the format of "@domain" to specify the domain for the user (example: user1@domain1). This format is valid only when the authentication profile that has the specified domain included in the authentication priority list.

- For example, if the users who have the same user name and password exist in domain 1, domain 2, and domain 3, and the authentication priority is specified in the order of the user in domain 1 and user in domain 2, and the user in domain 3 is not registered in the authentication priority list, authentication is processed as described below.
  - When any of those users are not registered in the Management Console, authentication is performed according to the authentication priority list, and the user in domain 1 is preferentially authenticated.
  - When both users in domain 1 and domain 2 are registered in the Management Console, authentication is performed according to the authentication priority list, and the user in domain 1 is preferentially authenticated.
  - When only the user in domain 2 is registered in the Management Console, the user in domain 2 is preferentially authenticated because the users registered in the Management Console have priority over the users in the authentication priority list.
  - When the user in domain 1 and local user are registered in the Management Console, the local user is preferentially authenticated.
  - The user in domain 3 who is not registered in the authentication priority list causes a login error even if the user is registered in the Management Console.

Configuring the Display Method of Print Jobs

1. **Click the following items in the navigation tree to open the [Embedded Print] tab.**

   [Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Embedded Print]

2. **Click (Add).**
3. **Enter Configuration Name and its description.**
4. **Specify how to sort the print jobs and the sort order.**
5. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 510 "Embedded Print".

Managing the Streamline NX PC Client Settings

You can configure RICOH Streamline NX PC Client settings using the Management Console and distribute them to RICOH Streamline NX PC Client installed on client computers.

Important

- **This option is only available to users with the SysConfigWrite access privilege. For details about privileges, see page *557* "User Roles".**

Configuring PC Client Global Settings

You can specify if RICOH Streamline NX PC Client users are allowed to switch location profiles for themselves. The users can select a profile from those stored in the Delegation Servers their RICOH Streamline NX PC Clients access.

1. **Click the following items in the navigation tree to open the [PC Client Global Settings] tab.**

   [Configuration] ▶ [Streamline NX PC Client Settings] ▶ [PC Client Global Settings]

2. **Specify whether RICOH Streamline NX PC Client users are allowed to switch location profiles.**
3. **Click (Save).**

Configuring PC Client Location Profiles

You can configure different settings to be applied to RICOH Streamline NX PC Client according to the location it is used.

1. **Click the following items in the navigation tree to open the [PC Client Location Profiles] tab.**

   [Configuration] ▶ [Streamline NX PC Client Settings] ▶ [PC Client Location Profiles]

2. **Click (Add).**
3. **On the [General] tab, enter the profile name and its description.**
4. **Configure other items as necessary.**
5. **On the [Secure Print] tab, configure settings related to the secure printing function.**
6. **On the [Delegation Servers] tab, specify the target Delegation Servers to deploy the location profile.**
7. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 513 "PC Client Location Profiles".
- When the users do not select a profile on RICOH Streamline NX PC Client, the "Default" profile created upon installation of the software is applied. Since the "Default" profile has higher priority over the configurations specified during installation, change the "Default" profile as necessary by selecting the "Default" profile from the profile list displayed in Step 1.

Monitoring Devices Using the @Remote Function

@Remote is a device management service provided by Ricoh. In this service, @Remote Center monitors the devices and Delegation Servers to reduce the in-house cost of managing those devices. To use the @Remote function, @Remote license must be purchased and activated. For details about activating the license, see "Activating RICOH Streamline NX", Installation Guide.

You need the @RemoteCE permission to modify some of the settings. If an item is grayed out and cannot be modified, log in to the system using a user account that has the @RemoteCE permission.

Configuring the Connection Settings between @Remote Center and Delegation Servers

1. **Click the following items in the navigation tree to open the [@Remote Settings] tab.**

   [@Remote] ▶ [@Remote Settings]

2. **In the list, select the server to be connected to @Remote Center.**
3. **On the [Proxy Server] tab, select [On] in [Use Proxy Server].**
4. **Specify the IP address and port number of the proxy server.**
5. **When the proxy server requires authentication, select [On] in [Use Authentication], and specify the user name, password, and domain name.**
6. **Click [Check Connection] to check that a connection can be established between @Remote Center and Delegation Server via the proxy server.**
7. **Click (Save).**

Selecting the Information to Be Sent to @Remote Center

1. **Click the following items in the navigation tree to open the [@Remote Settings] tab.**

   [@Remote] ▶ [@Remote Settings]

2. **In the list, select the server to be connected to @Remote.**
3. **On the [Connector Settings] tab, select the [Send IP addresses] check box.**

   Disabling those items may affect device management on @Remote Center. Contact a RICOH service representative before disabling this item.

4. **Click (Save).**

Registering Connector (Delegation Server) to the Center

1. Click the following items in the navigation tree to open the [@Remote Settings] tab.

   [@Remote] ▶ [@Remote Settings]

2. In the list, select the server to be connected to @Remote Center.
3. In the [Request number] field on the [Connector Settings] tab, enter the request number that has been distributed from a RICOH service representative.
4. Click [Connect].
5. Click [Register].
6. Confirm that [Status] changes to registered.

Note

- Perform this operation for each Delegation Server to be registered.

Allowing the Information to be Sent to @Remote Center

1. Click the following items in the navigation tree to open the [@Remote Settings] tab.

   [@Remote] ▶ [@Remote Settings]

2. In the list, select the server to be connected to @Remote Center.
3. Change [Device List Update] to [Allow] on the [Permission Settings] tab.
4. Click (Save).

Configuring the Method and Frequency to Send Information to @Remote Center

1. Click the following items in the navigation tree to open the [@Remote Settings] tab.

   [@Remote] ▶ [@Remote Settings]

2. In the list, select the server to be connected to @Remote.
3. On the Device List Update tab, configure the method and frequency to send the information.

   Device List Update Method

   Specify settings such as whether to send the device list information to @Remote Center after discovery or after polling.

Device List Update Schedule

Specify the update interval of the device list information to be sent to @Remote Center.

4. **Click (Save) when the settings are complete.**

Note

- For details about the setting items, see page 634 "@Remote Settings".

Managing the Pricing Tables

Create a pricing table to set the cost per page for each function of a device. You can specify a separate cost for individual print conditions such as paper size, color mode, or duplex printing. You can use this information to analyze the operational cost of the device in detail.

There are two types of pricing tables according the device functions as follows:

Built-in Functions

Create a pricing table for the basic functions of a device such as copier, printer, fax and scanner.

Embedded Scan Functions

Create a pricing table for costs associated with workflows of RICOH Streamline NX.

Important

- **A pricing table can be assigned only to a category and groups under the category. Before creating a pricing table, select a category to enable assigning of the pricing table in the following setting item:**
  - **[System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [General] tab ▶ [Target Device Association Category]**
- **When you change the category for which assigning of the pricing table is enabled, the settings related to the pricing table are deleted.**

Creating a Pricing Table for Built-in Functions

1. **Click the following items in the navigation tree to open the [Built-in Functions] tab.**

   [System] ▶ [Pricing Table] ▶ [Built-in Functions]

2. **Click (Add).**
3. **On the [General] tab, enter Pricing Table Name and its description.**
4. **On the [Target Devices/Groups] tab, specify the devices or groups to which to apply the pricing table.**

   1. Click (Add group) or (Add Devices).
   2. Add the target devices or groups to the [Target Device] or [Target Groups] list, and then click [OK].

5. **On the [Cost Per Page] tab, click (Add) to add a line and configure a cost according to the device functions and print conditions.**
6. **Click (Save) when the settings are complete.**

Note

- When [Apply Pricing By] is set to [Users and Departments] in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings], the [Target Users/Departments] tab is displayed instead of the [Devices and Device Groups] tab. In this case, specify the users or departments to which to apply the pricing table in Step 4.
- The pricing table specified for the device/user has priority over the table for the group/department.
- If a pricing table is not specified for a device/user, the table for the group/department to which the device/user belongs is applied.
- If a pricing table is not specified for both the device and group or user and department, the table of the group/department closest to the device/user is applied. For example, the pricing table for the "10.85" group is applied on devices assigned with the IP addresses "10.85.30.xx" when a pricing table is specified for the "10.85" group but not for the "10.85.30" group in the "IP Address" category.
- You can specify only one table for a device, group, user, or department. If you specify a new table for a device, group, user, or department, the existing table is automatically invalidated.

Creating a Pricing Table for Workflow

1. **Click the following items in the navigation tree to open the [Workflows] tab.**

   [System] ▶ [Pricing Table] ▶ [Embedded Scan Functions]

2. **Click (Add).**
3. **On the [General] tab, enter Pricing Table Name and its description.**
4. **On the [Workflows] tab, click (Add) to add the target workflow to the pricing table.**
5. **Specify [Base Rate] and [Page Rate] on the [Cost Per Page] tab.**

   Base Rate

   Counted once each time the workflow is executed.

   Page Rate

   Counted according to the number of pages processed in the workflow.

6. **Click (Save) when the settings are complete.**

Distributing Printer Drivers

The printer driver distribution function enables the administrator to post files such as a printer driver or user's guide to a configured Web page for driver download and enables the user to download and easily install the driver.

Use the driver distribution function to distribute the following files:

- Printer driver packaged with Printer Driver Packager NX/Ridoc Ez Installer NX and uploaded
- Other files (PDF files, third-party drivers, and other file types)
- URL link

Note

- You can enable the driver distribution feature at any time, and you can continue to add drivers to the page as needed. You do not need to disable the feature to add new drivers to the page.
- For details about using Printer Driver Packager NX/Ridoc Ez Installer NX, see the user's guide for Printer Driver Packager NX/Ridoc Ez Installer NX.

Driver Distribution (enhanced) function

The Driver Distribution (basic) function is provided as standard. When you purchase and activate a separate Driver Distribution license, you can use the Driver Distribution (enhanced) function. The Driver Distribution (enhanced) function enables you to use the search function and useful browsing function on the driver download page.

The Driver Distribution (enhanced) function adds the following features to the driver download page:

- User authentication
- Browsing by device category (IP address, hostname, model name, etc.) and by group
- Browsing using a map
- Search using multiple criteria
- Filtering by column (Quick Filter)
- Automatic selection of drivers supported by the operating system
- Sorting by color support, 2 sided printing support, and printing speed

Note

- The Driver Distribution license has a trial period of 60 days. To continue using the license after the trial period, purchase the license. For details about the license, see page 26 "List of Licenses and Functions".

Driver Distribution Workflow

To use the printer driver distribution function, use the following procedure.

1. ▶ **page 134 "Uploading a Driver Package to the Repository"**

   Upload the driver package created in Printer Driver Packager NX/Ridoc Ez Installer NX to the repository on the Core Server. The uploaded driver package can be checked from [Repository Management] in the Management Console.

2. ▶ **page 135 "Associating a Driver Package with a Device or Device Group"**

   Select the intended device or device group of the driver package, and associate the device with the driver package. When registering other files or external links, select and upload an associated device or group.

3. ▶ **page 137 "Enabling Driver Distribution"**

   Enable driver distribution to allow users to access the driver download page.

4. ▶ **page 140 "Accessing the Driver Download Page"**

   Access the driver download page to confirm the contents.

Uploading a Driver Package to the Repository

Upload the driver package created in Printer Driver Packager NX/Ridoc Ez Installer NX to the repository of the Core Server. For details about creating and uploading a package, see the user's guide of Printer Driver Packager NX/Ridoc Ez Installer NX.

Confirming an uploaded driver package

1. **Click the following items in the navigation tree to open the [Repository Management] tab.**

   [System] ▶ [Server Settings] ▶ [Repository Management]

   All driver packages, sets of firmware, SDK/J platforms, and Device Applications files uploaded to the repository are displayed.

   Click the [Type] column to sort the list by data type.

   To delete any external links, files, or driver packages associated with a device or device group, click (Delete).

Associating a Driver Package with a Device or Device Group

To enable the user to download the driver package on the driver download page, associate the uploaded driver package with the supported device or device group.

Another file (PDF, Word, etc.) or external link (vendor Web site, etc.) can also be associated with the device.

1. **Click the following items in the navigation tree to open the [Devices] tab.**

   [Device List] ▶ [Model]

2. **Select the device or device group to be associated with the driver package.**

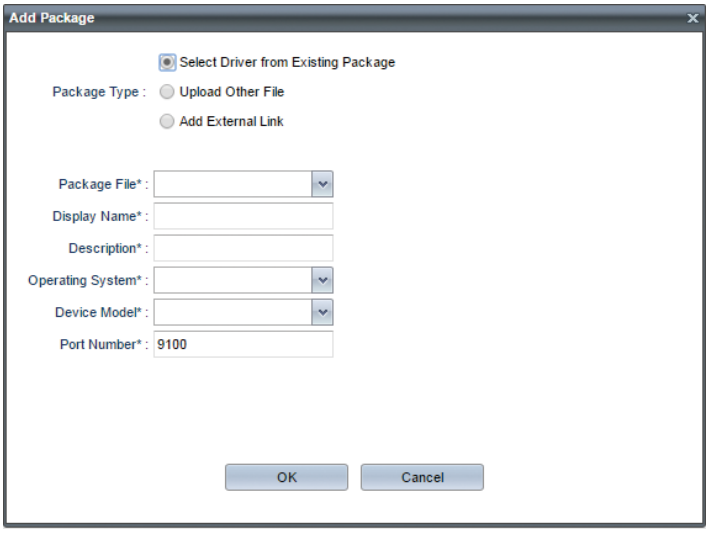
   When associated with a single device

   1. Click the [Driver Package] tab on the [Device Properties] window.
   2. Click (Add).

   When associated with a device group

   1. Right-click Device List and select (Add).

3. **On the [Add Package] window, select [Package Type], and configure the options.**



Options that can be configured vary depending on the selected Package Type. For details, see the following table.

Package Type	Options
Select Driver from Existing Package	• Package File Select a driver package that has been uploaded to the repository from Printer Driver Packager NX/Ridoc Ez Installer NX. • Display Name The name of the uploaded driver package is automatically entered. The name can be changed as necessary. • Operating System These are the operating systems supported by the driver package. The contents of the selected driver package may be automatically set and cannot be changed. • Device Model These are the device models supported by the driver package. The contents of the selected driver package may be automatically set and cannot be changed.
Upload Other File	Upload a file in any format. • Other File Click [Browse], and specify the file to upload. • Display Name The name of the selected file is automatically entered. The name can be changed as necessary. • Description Enter a description for the file • Operating System Select the operating system from the following that supports the driver: [Any], [Any Windows 32-bit], [Any Windows 64-bit], [Windows Vista 32-bit], [Windows Vista 64-bit], [Windows 7 32-bit], [Windows 7 64-bit], [Windows 8 32-bit], [Windows 8 64-bit], [Windows 10 32-bit], [Windows 10 64-bit] **Note** • On the [Driver Package] tab, click (Edit) to edit Display Name, Description, or Operating System.

Package Type	Options
[Add External Link]	Associate a device with an external link. • URL Enter a valid URL. Example: http://www.ricoh.com/ • Display Name The page name of the selected URL is automatically entered (not including the path name). The name can be changed as necessary. • Description Enter the external link description. • Operating System Select the operating system from the following that supports the driver: [Any], [Any Windows 32-bit], [Any Windows 64-bit], [Windows Vista 32-bit], [Windows Vista 64-bit], [Windows 7 32-bit], [Windows 7 64-bit], [Windows 8 32-bit], [Windows 8 64-bit], [Windows 10 32-bit], [Windows 10 64-bit]

4. **Click [OK].**

   A list of driver packages, files, or external links is displayed on the [Driver Package] tab.

Enabling Driver Distribution

After the driver package is uploaded to the repository and the driver package, external link, or another file and device or device group is associated with the device, the driver download page is activated. The user can access this page on the web browser and download and install a released driver to a local computer.

1. **Click the following items in the navigation tree to open the [Driver Distribution] tab.**

   [System] ▶ [Server Settings] ▶ [Driver Distribution]

2. **From the [Enable] drop-down list, select [Basic] or [Advanced].**

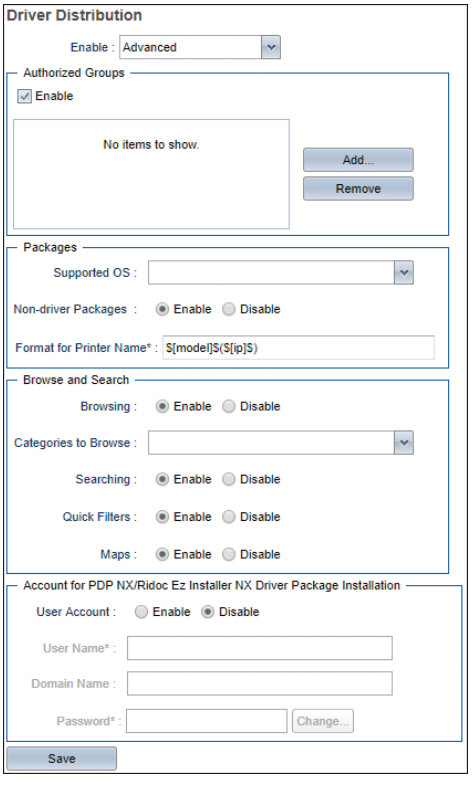
   Note

   - [Advanced] appears only when the Driver Distribution (enhanced) function is enabled.
   - [Advanced] is also displayed during the trial period.

   When [Basic] is selected, proceed to Step 4.

When [Advanced] is selected, proceed to Step 3.

3. Configure the options for the Driver Distribution (enhanced) function.



Item	Description
Authorized Groups	• Enable Select this check box and click [Add...] to specify an LDAP or Active Directory user group to download the driver. When a user of the specified group logs in to the driver download page, the driver download privileges are automatically granted, and the user can then download the driver package. To enable access to the driver download page without authentication, clear the check box.

Item	Description
Packages	• Supported OS Select the appropriate operating system from the following: [Windows Vista 32-bit], [Windows Vista 64-bit], [Windows 7 32-bit], [Windows 7 64-bit], [Windows 8 32-bit], [Windows 8 64-bit], [Windows 10 32-bit], [Windows 10 64-bit] If this setting is not specified, all operating systems can be used. • Non-driver Packages Specify whether to enable or disable the function to browse packages from an external link and download the files.
Browse and Search	• Browsing Select [Enable] to allow the user to perform hierarchical browsing. • Categories to Browse Select the category that the user can browse from the drop-down list. In addition to the default categories of IP address, host name, and model, you can also select from categories defined by the administrator. • Searching Select [Enable] to allow the user to use the search function. • Quick Filters Select [Enable] to allow the user to use the search filter. • Map Select [Enable] to allow the user to use the search map.

4. **Click [Save].**

The user can access the driver download page and download the driver package and other items.

[Account for PDP NX/Ridoc Ez Installer NX Driver Package Installation]

When information about an account with driver installation privileges is specified in [Account for PDP NX/Ridoc Ez Installer NX Driver Package Installation], the account privilege is temporarily granted to install the driver package created using Printer Driver Packager NX/Ridoc Ez Installer NX, and users without driver installation privileges can also install the driver.

When the driver package is downloaded, the installation account is overwritten by the [Account for PDP NX/Ridoc Ez Installer NX Driver Package Installation].

Note

- To use the Printer Driver Packager NX/Ridoc Ez Installer NX settings when the installation account is configured by individual package, do not specify the account in the [Account for PDP NX/Ridoc Ez Installer NX Driver Package Installation].
- To use this function, [Use specified user account] must be configured when a driver package is created in Printer Driver Packager NX/Ridoc Ez Installer NX. For details, see the user's guide of Printer Driver Packager NX/Ridoc Ez Installer NX.

Accessing the Driver Download Page

When the driver distribution is enabled, the user can download the driver package from the driver download page.

1. **In the Web browser URL field, enter "http://(server-IP-address-or-hostname):(port-number)/drivers.html".**

   The Core Server uses port 8080 by default (port 51443 when SSL is enabled). Enter the correct port number if a different port was specified when the Core Server was installed.

   When SSL is enabled, use "https" instead of "http".

2. **The authentication screen is displayed when user authentication is enabled in the Driver Distribution (enhanced) function. Log in with an LDAP or Kerberos profile.**
3. **Click the device.**

   The driver dialog box is displayed.

4. **Click the link in the [Name] column.**

   Click the driver package created in Printer Driver Packager NX/Ridoc Ez Installer NX to start downloading the installer package. Open the downloaded package to install the driver, port, and print queue.

   Click the external link to open the page in a web browser.

   Click another file under “Other” to download a file.

Note

- The devices can be sorted by column header.

- When the Driver Distribution (enhanced) function is enabled, the search function and browsing by using a map or category or group in the device list can be used.
- When the Driver Distribution (enhanced) function is enabled, only those drivers the current operating system supports are displayed in the download dialog box.

Using the Certificate Management Tool

You can use the Certificate Management Tool to create a self-signed certificate of a device and distribute certificates to devices.

You can use this tool to perform the following tasks:

- Retrieve/Install/Delete certificates
- Install/Delete intermediate certificates
- Create self-signed certificates
- Generate and retrieve Certificate Signing Requests (CSR)
- Associate and Disassociate certificates with an Application

This tool supports the certificate configuration for the following applications on the MFP: SSL/TLS, IEEE 802.1x, S/MIME, IPsec, PDF Digital Certificate, PDF/A Digital Certificate.

Important

- **Only the 2013 models or later of the RICOH devices indicated by the device icons  can be managed by the Certificate Management Tool. Even if the device can be imported from the device list, 2012 models do not support the Certificate Management Tool. An error is displayed when an attempt is made to obtain information from an unsupported device.**

Setup Summary for the Encrypted Communication Path

There are four steps to complete to set up the encrypted communication path with the device certificate:

1. Build the combination of application on each device and certificate entry.
2. Create CSR.
3. Create the certificate/to submit to the certificate authority/to take out the certificate.
4. Install the certificate.

Please refer to the following chapters in the device's manual or security guide for the specific details of each procedure as relates to your device.

- Protecting the Communication Path via a Device Certificate
- Creating the Device Certificate (Issued by a Certificate Authority)
- Installing the Device Certificate (Issued by a Certificate Authority)

In addition, please refer to the following chapter of Web Image Monitor Help for details regarding how to set items on the device:

- Configuration ▶ Security: Device Certificate

The Certificate Management Tool can carry out a series of processing from step two to step four (mentioned above) as a job lot by performing in cooperation with the SCEP server. This tool can also

perform procedure one as a single task. In addition, because this tool has same parameters as those of the device, you can configure them in the same manner as the device configuration.

1. ▶ **page 144 "Set the Configuration Options"**

   Configure the connection settings to connect to the Core Server.

2. ▶ **page 145 "Downloading the Device List"**

   Obtain the device list from the Core Server.

3. ▶ **page 146 "Confirming a Certificate"**

   Configuration status of MFP Certificate can be confirmed in the Certificate Management Tool.

4. ▶ **page 148 "Managing Certificates"**

   You can perform the following operations when managing certificates:

   - Obtaining the certificate settings status on a device
   - Creating a self-signed certificate on a device
   - Creating and obtaining a Certificate Signing Request (CSR)
   - Installing and deleting a certificate or intermediate certificate on a device

   To install a certificate, associate the certificate with CSR and import an intermediate certificate in the Certificate Management Tool in advance.

5. ▶ **page 151 "Assigning an Application"**

   Assign the certificate to the related application of the selected device.

System Requirements of Certificate Management Tool

Install Certificate Management Tool in the following folder on the Core Server:

`(Installation path)\tools\CertificateManagement`

Copy the folder that contains the exe file of Certificate Management Tool to run the tool on a client computer.

Important

- **This tool automates interaction with the Simple Certificate Enrollment Protocol (SCEP) and therefore requires an SCEP interface to your Certificate Authority (CA). If you do not have access to this interface, you must manually request and generate the appropriate certificates.**

To operate Certificate Management Tool on a client computer, establish a network connection from the client computer to the device to which to install the certificate. The Certificate Management Tool is supported on the following operating systems:

- Windows Server 2008 R2 Standard/Enterprise SP1 (64-bit) or later
- Windows Server 2012 Standard/Enterprise (64-bit)
- Windows Server 2012 R2 Standard/Enterprise (64-bit)
- Windows 7 Home Basic/Home Premium/Professional/Enterprise/Ultimate (32/64 bit)
- Windows 8.1 Pro/Enterprise (32/64 bit)
- Windows 10 Home/Pro/Enterprise (32/64 bit)

Set the Configuration Options

Follow these instructions to configure the location of the Core server and the SCEP server.

1. **Open the folder that contains Certificate Management Tool, and then double-click "SLNXCertTool.exe".**
2. **From the [File] menu, select [Options].**
3. **In [Address], enter the IP address or host name of the Core Server.**
4. **In [Port], enter the port number of the Core Server.**

   The port number of the Core Server is "8080" (default).
5. **Select the [SSL Connection] check box to connect to the Core Server via SSL connection.**
6. **To validate the SSL certificate of the Core Server, select the [Validate Certificate] check box.**

   If you are not interfacing with an SCEP server, proceed to Step 11.
7. **In [SCEP Server URL], enter the SCEP server URL.**

   Enter the path name to mscep.dll in full as the SCEP server URL.

   Example:

http(s)://(scep_server_address)/certsrv/mscep/mscep.dll

   Where (scep_server_address) is the address of the SCEP server. When you customize the address of the SCEP server, please change it to match your server environment.
8. **To validate the SSL certificate of the SCEP Server, select the [Validate Certificate] check box.**

9. **Click the [...] button next to [PKCS12 File] to specify a certificate file (.pfx) to be used to connect to the SCEP server.**

Note

- To create the private key certificate for SCEP, perform the following within MMC.
  1. Click [Start], type "mmc" in the [Search programs and files box], and then press the Enter key.
  2. Select [File] ▶ [Add/Remove Snap-in]. Select [Certificates], and then click [Add].
  3. Select [Computer Account], click [Finish], and then click [OK].
  4. Expand [Certificates (Current User)] and select [Personal].
  5. Right click in the main window, select [All Tasks] ▶ [Request New Certificate].
  6. Create a new User certificate.
  7. Select the new certificate, right click, and select [All Tasks] ▶ [Export].
  8. Export with the private key included in PKCS #12 format and password protect it.
  9. Save the file where it can be accessed by the Certificate Management Tool.

10. **In [Password], enter the password of the private key to be used to connect to the SCEP server.**
11. **To allow only SSL connections to the device, select the [Allow only SSL connections] check box.**
12. **To validate the SSL certificate of the device, select the [Validate Certificate] check box.**
13. **Click the [...] button next to [Cache Location:], and then select the folder in which to store the cache file.**

    The information cached in this location includes certificates and information retrieved from devices and from RICOH Streamline NX. The information stored in this folder can be obtained again from the devices or the RICOH Streamline NX as necessary.
14. **Specify whether or not to display the log.**

    [On] is specified by default.
15. **Click [OK].**

Downloading the Device List

Important

- **The following privileges are required to download the device list: DeviceBasicRead, DeviceBasicWrite, DeviceAdvancedRead, DeviceAdvancedWrite, and SysConfigRead.**

1. **From the [File] menu, select [Download device list].**

2. **On the login screen, enter the user name and password.**

   Use the same authentication information that was used to log in to the Management Console.

3. **If authentication is successful, the downloaded device list is displayed.**

Note

- The categories and groups in the downloaded device list cannot be edited.

Confirming a Certificate

The Certificate Management Tool can display information in two different views: "Certificate View (Default)" and "Application-Certificate View". The information displayed in each view differs as shown below.

Changing the Views

There are two views that you can switch between: Certificate view (the default view) and Application-Certificate view. You can use the View menu to switch between the views, or use the View options on the toolbar.

Certificate View ( )

1. **Click Certificate View on the toolbar. This is the default view.**
2. **Click on a device group to view the list of devices within the group. Each device within the group is listed in the middle pane, displaying the following columns:**

Column	Description
Certificate #	Each device can support up to six certificates. This line displays the currently displayed certificate.
Name	Device name obtained from the Core Server
Address	Device IP address or host name
Model Name	Model information obtained from the Core Server
Expiry Date	Expiration date of the installed certificate. This field is left blank when no certificate is installed.
Application	Device Applications associated with the certificate. This field is displayed even when no certificate is installed.
MFP CSR	Indicates that the CSR of the device is stored in the local cache.

Column	Description
MFP Certificate	Indicates that the certificate of a device is stored in the local cache.
MFP Int CA	Indicates that the intermediate certificate of a device is stored in the local cache.
Certificate to be Installed	Indicates that a certificate that can be installed on a device is stored in the local storage.
Int CA to be Installed	Indicates that an intermediate certificate that can be installed on a device is stored in the local storage.

3. **Click on a device to view specific certificate information in the right pane. The default view shows all certificates for the device. To view a particular certificate, select the number from the Show list on the toolbar.**

Application-Certificate View ( )

1. **Click Application-Certificate View on the toolbar.**
2. **Click on a device group to view the list of devices within the group. Each device within the group is listed in the middle pane, displaying the following columns:**

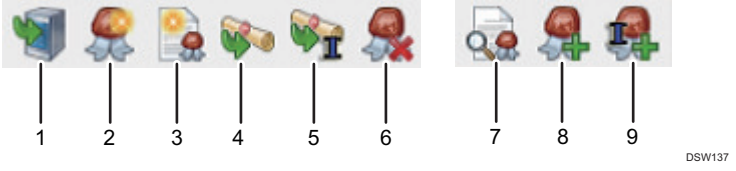
Column	Description
Name	Device name obtained from the Core Server
Address	Device IP address or host name
Model Name	Model information obtained from the Core Server
• SSL/TLS • IEEE 802.1 • S/MIME • IPSEC • PDF DIGITAL CERT • PDF/A DIGITAL CERT	A separate line is available for each application.

Note

- Certificate tasks and applications cannot be assigned in Application-Certificate View.

Managing Certificates

Useful functions for managing certificates are available on the toolbar as listed below. Each option is described in the table shown below.



1. **Retrieve Information**

   Obtains all certificate information from a device.

2. **Create Self Signed Certificate**

   Creates a self-signed certificate. On the Certificate Information screen that is displayed, enter Common Name, Organization, Organizational Unit, E-mail Address, City/Locality, State/Province, Country Code, Effective Date, validity period, and Algorithm Signature.

   Important

   - **Common Name must be unique.**

3. **Create CSR**

   Creates a CSR to be downloaded and stored in the local application cache.

   On the Certificate Signing Request screen that appears, enter Common Name, Organization, Organizational Unit, E-mail Address, City/Locality, State/Province, Country (Country Code), Effective Date, validity period, and Algorithm Signature.

4. **Install Certificate**

   Uploads and installs the local certificate that is associated with the selected device or certificate number to the device.

5. **Install Intermediate Certificate**

   Uploads the local certificate that is associated with the selected device or certificate number.

6. **Delete Certificate**

   Deletes the certificate of the specified certificate number from the selected device.

7. **Display CSR**

   Use this item to copy the displayed value to the certificate generation program.

   This is available when only one device is selected.

   If the selected device or certificate number does not contain CSR data, an error message is displayed.

8. **Associate Certificate to CSR**

   Imports a certificate to be installed to a specified device or certificate number.

   This is available when only one device is selected.

9. **Import Intermediate Certificate**

   Use this item to import an intermediate certificate file when the SCEP server to display the intermediate certificate is unavailable, or use the item to copy the certificate information to the "Import Intermediate Certificate" screen.

Note

- WARNING: A common name is typically the DNS name or IP address of the device. SSL server certificates are specific to the common name that they were issued to, so it is important that the common name is the same as the address that will be used when accessing the device.
- Check whether an execution of the task has succeeded or failed in the "Log" pane.

Assign Certificates

There are two methods available for installing certificates. If SCEP is available, certificates can be generated and installed in one step. Without SCEP, there are multiple steps that need to be taken to create and install a certificate. Select one or more devices that on which you want to generate and install certificates.

Creating and installing certificates via SCEP

Before using SCEP refer to the SCEP Configuration Notes section below to ensure it is configured correctly.

1. **Select one or more device certificate slots that you want to generate and install certificates on.**
2. **From the [Certificate] menu, select [Combination Tasks] ▶ [Generate and Install Certificate].**
3. **In the [Certificate Signing Request] screen, enter a Common Name, Organization, Organizational Unit, Email Address, City/Locale, State/Province, Country Code, and Algorithm Signature.**
4. **Click [OK] to continue. A CSR is generated and enrolled with SCEP to create a certificate, which is then installed on the device.**

Installing certificates without SCEP

To create and install certificates without SCEP, do the following:

1. **Create Certificate Signing Requests (CSR):**

   1. Select one or more device certificate slots that you want to create a CSR on.
   2. From the Certificate menu, select [Create CSR].
   3. In the [Certificate Signing Request] screen, enter a Common Name, Organization, Organization Unit, Email Address, City/Locale, State/Province, Country Code, and Algorithm Signature.
   4. Click OK to continue. A CSR is generated.

2. **Create Certificates:**

   1. Select one device certificate slot where a CSR was generated.
   2. From the Certificate menu, select [Local Tasks] ▶ [Display CSR].
   3. Copy the [Certificate Data] and use it to create a certificate with your Certificate Authority. The certificate must be created Base 64 encoded.

3. **Install the Certificate that was created from the Certificate Authority. There are two mechanisms for associating and installing the certificate:**

   Associate the certificate in two steps:

   1. Select the device certificate slot where the CSR for the generated certificate exists, and then locate the Certificate menu and select [Local Tasks] ▶ [Associate Certificate to CSR].
   2. Import the certificate file, or paste the contents into the [Associate Certificate to CSR] field and click [OK].

      The certificate is now associated with the CSR.
   3. From the [Certificate] menu, select [Install Certificate].

      The certificate is installed.

   Associate and install the certificate in one step. This option also allows you to assign an application at the same time:

   1. Select the device certificate slot where the CSR for the generated certificate exists, and then from the [Certificate] menu, select [Combination Tasks] ▶ [Associate and Install Certificate].
   2. Import the certificate file, or paste the contents into the [Associate Certificate to CSR] field and click [OK].
   3. Choose the application which will be assigned to the certificate. Click OK.

      The certificate is associated with the CSR, the certificate is installed, and the application assignment is completed.

Assigning an Application

There are two methods for assigning applications to certificates. If SCEP is not being used, application assignment can be done at the same time as certificate installation when running the [Combination Tasks] ▶ [Associate and Install Certificate] task. Otherwise, application assignment must be done as a separate step.

1. **Select the device certificate slot where the application will be assigned.**
2. **From the Certificate menu, select [Assign Application to Certificate].**
3. **Select the applications to assign. Click [OK].**

   The applications are assigned to the certificate.

SCEP Server Requirements

This section describes the SCEP server supported by the Certificate Management Tool.

Supported Environment

The Certificate Management Tool can support the Network Device Enrollment Service (NDES) on the following operation systems.

- Windows Server 2008 R2 Standard /Enterprise SP1 or later (64-bit)
- Windows Server 2012 Standard/Datacenter (64-bit)
- Windows Server 2012 R2 Standard/Datacenter (64-bit)

SCEP Configuration Notes

SCEP functionality has been tested with Microsoft's Certificate Authority with Network Device Enrollment Services (NDES) installed. For the SCEP calls to function, you must disable password enforcement by updating the following registry key on the Certificate Authority Server:

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP\EnforcePassword
\EnforcePassword = 0

When creating certificates for the device, they should be created using a webserver certificate template. If the certificate is created with the wrong intended purpose (it should be "Server Authentication"), it will fail to work with the application it is associated with (e.g. not being able to log into the device when a certificate that is not for "Server Authentication" is associated with SSL).

Follow these instructions to configure NDES to hand out WebServer certificates for SCEP requests:

1. **Open Registry Editor on the CA and navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP.**

2. **Change the values of the following registry keys to the name of the template:**
    - EncryptionTemplate
    - GeneralPurposeTemplate
    - SignatureTemplate
3. **The values for these keys should be set to the name of the web server template (do not confuse the web server template name with the web server template display name).**

Configuring the Internet Information Service

By default, IIS *7/7.5* security is too restrictive to permit the devices to enroll via SCEP.

For the Certificate Management Tool, IIS configuration must be updated using the command below (default maxQueryString is 1024):

```
%systemroot%\system32\inetsrv\appcmd.exe set config
/section:system.webServer/security/requestFiltering /
requestLimits.maxQueryString:"3072"
/commit:apphost
```

4. Managing Authentication Information

This chapter describes the functions and settings related to user authentication in RICOH Streamline NX.

Managing the Authentication Settings

All functions in RICOH Streamline NX use user authentication to identify the user. By authenticating users before they print, copy, or scan, you not only secure the devices, but also enable cost management by user.

To register the user information to the Core Server, use the Management Console to connect to an external authentication server, such as LDAP or Kerberos server, and then import the user information. You can add groups, departments, and other information to the imported user information in the Management Console to manage costs by organizational unit.

In addition to cost management, the user authentication function also plays an important role in terms of security. Users without authentication information can be prohibited from using devices, thereby preventing unauthorized access. The configuration items vary depending on the user login method. For example, you need to link the user information and card information when logging in to a device with a card.

Identify the most suitable method for your network environment and policies, configure the settings accordingly.

Synchronizing the password automatically with Active Directory

- Use Active Directory Password Filter in RICOH Streamline NX to link with Active Directory. Installing Password Filter of RICOH Streamline NX to the Active Directory domain controller, you can synchronize the user password with the Core Server database and centralize management.

  Install the following three Password Filter files to the Active Directory domain controller.

  - RicohPwdEvents.dll
  - RicohPwdFilter.dll
  - RicohPwdFilter.ini

  For details about Active Directory Password Filter, see the Microsoft website.

  https://msdn.microsoft.com/library/windows/desktop/ms721882(v=vs.85).aspx
- Password Filter is stored on the installation path (\tools\PasswordChangeNotification). For details about installing Password Filter to the Active Directory domain controller, see the technical information from Microsoft.
- The user password sent from the Password Filter to the Core Server database is encrypted.

Linking with Forefront Identity Manager

- You can link RICOH Streamline NX with Microsoft Forefront Identity Manager. Installing Password Filter of RICOH Streamline NX to the Forefront Identity Manager server, you can synchronize the user password with the Core Server database and centralize management.

  For details about Forefront Identity Manager, see the Microsoft website.

  https://technet.microsoft.com/library/jj590203(v=ws.10).aspx
- Password Filter is stored on the installation path (\tools\PasswordChangeNotification). Install all files on the Forefront Identity Manager server. For details about installing Password Filter to the Forefront Identity Manager server, see the technical information from Microsoft.
- The user password sent from the Password Filter to the Core Server database is encrypted.

Configuring an External Authentication Server

Register the information of the external authentication server, such as LDAP or Kerberos server, as an Authentication Profile, and import the information of the users that use the devices into the Core Server.

Important

- **The LDAP profile is required to configure Kerberos authentication. When configuring Kerberos authentication, configure the LDAP profile also.**

1. **Click the following items in the navigation tree to open the [Authentication Profile] tab.**

   [System] ▶ [Security] ▶ [Authentication Profile]

2. **Click (Add).**
3. **Select [LDAP] from the [Type] menu on the [General] tab, and then enter the authentication profile name in [Name].**
4. **Enter the LDAP server information on the [LDAP] tab.**

   For details about the setting items, see page 551 "Authentication Profiles".
5. **Click (Save).**
6. **Select the name of the authentication profile that has been added to the list, and then click (Check Connection).**
7. **Enter the user name and password, and then click [OK].**
8. **Check that you can connect to the server.**

Note

- The operation flow for configuring the Kerberos server is the same as the LDAP server. In Step 3, select [Kerberos] from the [Type] menu, and enter the information of the Kerberos server.

Authentication Methods

You can use one of several combinations of login methods to log in to a device.

Specify the login method for each device. Select a login method that is suitable for the environment where the device is used.

User Name and Password

Log in by entering a user name and password on the operation screen of the device.

Card

The user logs in by scanning a card on the card reader of the device.

Card and Secondary PIN

The user logs in by scanning a card on the card reader of the device and by entering a secondary PIN on the operation screen.

Card and Password

The user logs in by scanning a card on the card reader of the device and by entering a password on the operation screen.

User PIN

Log in by entering a user PIN on the device operation screen.

Note

- To enhance security, it is recommended to use an authentication method that uses a PIN code combined with a card, or a user name and password to log in to devices, instead of using only PIN.
- For details about configuring user names, passwords, PINs, and cards, see page 172 "Managing User Information".
- For details about the device login methods, see page 122 "Managing the Streamline NX Embedded Settings".

Specifying the Extended Security Functions

Use this function to prevent unauthorized access to the Management Console and devices.

Configuring the Local Password Policy

The administrator can specify an expiry date on the password that is used by the user to log in to the Management Console. You can maintain the security of the administrator account by updating the password regularly. You can also configure the following settings:

- Locking the account when an incorrect password has been entered several times
- Increasing the minimum number of characters in a password
- Requiring the use of uppercase letters and numbers in the password

To enable a local password policy, configure the settings on the screen shown below.

[System] ▶ [Security] ▶ [Password Policy]

Note

- For details about the setting items, see page 562 "Local Password Policy".
- This setting applies only to local users. For details about local users, see page 157 "Creating and Importing Users".
- The LDAP server's password policy, not the one of RICOH Streamline NX, will apply to the externally identified users.

Enabling Account Lockout

You can specify the number of times a user can enter an incorrect password when logging in on the operation screen of the device. When you exceed the specified number of retry times, the account is locked, and you cannot log in to the device.

You can also specify the period to wait before the account is unlocked and can be used for login again.

To enable account lockout, configure [Threshold] and [Lockout Duration] on the screen shown below.

[System] ▶ [Server Settings] ▶ [Delegation Server Settings]

Note

- For details about the setting items, see page 539 "Delegation Server Settings".
- The LDAP server's lockout policy, not the one of RICOH Streamline NX, will apply to the externally identified users.

Disabling Local Authentication

You can specify whether or not to prohibit the creation of local users. By centralizing the management privileges of user information to an external authentication server, you can prevent changes to information that were unintended by the system administrator.

To disable local authentication, change the [Enable Local Authentication] setting on the screen shown below.

[System] ▶ [Server Settings] ▶ [User Management and Accounting Settings]

Note

- For details about the setting items, see page 546 "User Management and Accounting Settings".
- For details about local users, see page 157 "Creating and Importing Users".

Creating and Importing Users

Use the Management Console to manage all user information centrally on the system. There are two types of users: externally identified users and local users.

Externally Identified Users

Externally identified users are managed on an LDAP or Kerberos server. To manage these users, import the user information to the Core Server from the LDAP or Kerberos server.

Local Users

Use the Management Console to create and add local users to the Core Server. Create a local user to manage the user separately from the users on an external authentication server. You can later synchronize the local user created in the Management Console to the external authentication server.

Note

- You can also import the user information from a CSV file. For details, see page 158 "Importing local users from a CSV File".

Importing User Information from the LDAP Server

Import the user information from the LDAP server to the Core Server.

1. **Click the following items in the navigation tree to open the [Users] tab.**

   [User Management] ▶ [Users]

2. **Click (Import Users from External LDAP).**
3. **Select users to be imported in the [Import External Users] dialog box.**
   - [Authentication Profile]

     Select the authentication profile for the LDAP server.
   - [User Name]

     Enter the user name to search for on the LDAP server. Users with matching criteria are displayed in the list.
4. **Select users to be imported into the Core Server, and then click [OK].**

Note

- To synchronize the user information on the Core Server and the LDAP server, select the users in the list who are displayed on the [Users] tab, and then click (Enable/disable LDAP Synch). A check mark appears on the "LDAP Synchronization" line for the users who are being synchronized to the LDAP server.

- The attributes of users synchronized with the LDAP server are synchronized according to the schedule specified in [Synchronization Tasks] in the navigation tree. Specify the attributes synchronized with the LDAP server as needed. For details, see page 626 "Synchronization Tasks".

Registering Local Users on the Management Console

Register a new user information to the Core Server. Create a local user to manage the user separately from the users on the LDAP server. You can synchronize the created local user to the LDAP server by clicking (LDAP sync.).

1. **Click the following items in the navigation tree to open the [Users] tab.**

   [User Management] ▶ [Users]

2. **Click (Add).**
3. **On the [User Setting] tab, configure the basic settings such as the user name and PIN code.**
4. **On the [Groups] tab, select the group to be associated with the user.**
5. **On the [Alias] tab, specify the alias name of the user.**
6. **On the [Delegation] tab, select a delegate user.**
7. **On the [Cards] tab, configure the information of the card to be assigned to the user.**
8. **On the [Permissions] tab, configure the functions and workflows that can be used by the user.**
9. **Click (Save).**

Importing local users from a CSV File

Use a CSV file to add a large number of local users at one time.

For the format of CSV files, see page 789 "Format of a Local User CSV File".

A sample CSV file can be downloaded from the import screen.

1. **Click the following items in the navigation tree to open the [Users] tab.**

   [User Management] ▶ [Users]

2. **Click (Import).**
3. **Click [Browse...] on the [Import CSV File] screen, and then select a CSV file.**

   If you have not yet created the CSV file, click [Download Sample File] to download a sample CSV file to be used as a template.

4. **Click [Upload], and then click [OK].**

   The information imported into the local users are displayed.

Note

- When importing a CSV file, make sure that the language of the Management Console is the same one as when the file has been exported. Otherwise, some setting values are not imported.

Managing User Roles and Privileges

Roles are used to specify access privileges required to access the functions in the Management Console.

To ensure good security of a large-scale system while maintaining security, assign each user an appropriate role and limit the operations the user can perform according to his or her job duties. By assigning the appropriate role for each user, you can prevent configuration changes or operation errors that were unintended by the system administrator and improve your operational security.

Note

- When using LDAP authentication, assign the role to an LDAP group name to apply the role to all users belonging to the group. Use the related LDAP profile to determine the role when using Kerberos authentication.
- A user can be a member of more than one group, and each user is granted security rights based on all matching profiles.

Typical Use-case for User Roles Assignment

A role that is pre-registered to the Management Console is referred to as a "system role". Each system role is granted appropriate permissions according to the responsibility of the role. For example, you can assign system roles according to the operation procedures of the system as shown below:

Case 1: Operation by users who can operate all functions

A few administrators manage all of the devices and RICOH Streamline NX system. In that case, "Full Admin" should be assigned all administrators.

This management style is suitable for:

- Less than several hundred devices
- The system manages one country

Case 2: Dividing users into those who manage the system and those who operate it

Typically, large enterprise will divide the management duties such as Administrator A manages RICOH Streamline NX servers, Administrator B manages US devices, and Administrator C manages UK devices. In that case, you can assign proper role to each administrator.

This management style is suitable for:

- Many hundreds (or thousands) of devices
- The system manages multiple countries

Examples

- Administrator who manages RICOH Streamline NX system

  Full Admin: Administrator.

- Operator who manages devices, user, workflow and report

Device Admin: Manages devices and configures settings when a device is added or removed.

Security Admin: Manages users and configures settings when a user is added or deleted.

Workflow Admin: Modifies and creates a workflow.

Report Admin: Creates a report template and generates reports.

- Helpdesk (Reference Only)

  Device Operator: Responds to inquiries regarding devices.

- Reception who provide temporary card to guest

  Temporary Card Admin: Registers a temporary card.

Note

- If you cannot find an appropriate system role to assign to a certain user, you can create a custom role by copying an existing system role as a template and modifying the permissions and other settings.
- You do not need to assign a role to a general user who uses only the device functions such as the printer or scanner function.

List of system roles

Types and permissions of the system roles that are registered to the system are shown in the list below:

Important

- **You cannot delete Full Admin and Customer Engineer.**

System roles with full management permissions

System role	Description	Default permission
Full Admin	• Access to almost all permissions including the management of driver packages	• All (except @RemoteCE, and Temporary Card Admin)

System roles for device management

System role	Description	Default permission
Device Admin	• Read/write information related to devices • Upload driver packages	• AddressBookRead • AddressBookWrite • DeviceBasicRead • DeviceAdvancedRead • DeviceBasicWrite • DeviceAdvancedWrite • SysConfigRead • EmbeddedOperationRead • WorkflowOperationRead
Address Book Admin	• Display all information related to devices • Create/update Address Book templates and tasks	• AddressBookRead • @RemoteCE • DeviceBasicRead • DeviceAdvancedRead • AddressBookWrite • EmbeddedOperationRead • WorkflowOperationRead
Customer Engineer	• Customer engineer with optional permissions of @Remote Connector	• @RemoteAdmin • @RemoteCE • DeviceBasicRead • DeviceBasicWrite • EmbeddedOperationRead • WorkflowOperationRead
Device Basic Admin	• Read all information related to devices • Update basic writing operations	• AddressBookRead • DeviceBasicRead • DeviceAdvancedRead • DeviceBasicWrite • SysConfigRead • EmbeddedOperationRead • WorkflowOperationRead

System role	Description	Default permission
Device Operator	• Display all information related to devices	• AddressBookRead • DeviceBasicRead • DeviceAdvancedRead • SysConfigRead • EmbeddedOperationRead • WorkflowOperationRead
Embedded Admin	• Read/write operations related to embedded settings	• EmbeddedOperationWrite • EmbeddedOperationRead • SysConfigRead • DeviceBasicRead • SecurityRead • DeviceAdvancedRead • SlnxUserOperationRead
Embedded Operator	• Read operations related to embedded settings	• EmbeddedOperationRead • SysConfigRead • DeviceBasicRead • SecurityRead • DeviceAdvancedRead • SlnxUserOperationRead
Driver Download	• Download the driver	• DriverDownload

System roles for reports

System role	Description	Default permission
Report Admin	• Execute, create, and store new reports, configure schedules	• ReportWrite • ReportRead
Report User	• Execute and display reports	• ReportRead

System roles for server management

System role	Description	Default permission
Security Admin	• Add user accounts and security profiles • Read/write the system audit log	• SecurityWrite • SysConfigRead • SecurityRead • AuditWrite • AuditRead • LogDelete
User Admin	• Add user accounts and security profiles	• SecurityWrite • SysConfigRead • SecurityRead
Temporary Card Admin	• Change the expiration period end date of a temporary card • The administrator creates a temporary card. Only the administrator can delete it.	• TemporaryCardChange • SlnxUserOperationRead
SLNX User Admin	• Read/write all information related to the user management for Streamline NX Embedded Applications	• SlnxUserOperationWrite • SlnxUserOperationRead • CardOperationWrite • CardOperationRead • AccountingOperationWrite • AccountingOperationRead • WorkflowOperationRead • SysConfigRead • SysConfigWrite • DeviceBasicRead • SecurityWrite • SecurityRead

System role	Description	Default permission
SLNX User Operator	• Read all information related to the user management for Streamline NX Embedded Applications	• SlnxUserOperationRead • CardOperationRead • AccountingOperationRead • WorkflowOperationRead • SysConfigRead • DeviceBasicRead • SecurityRead
Card Admin	• Read/write operations related to cards	• CardOperationWrite • CardOperationRead • SlnxUserOperationRead
Card Operator	• Read operations related to cards	• CardOperationRead • SlnxUserOperationRead

System roles for workflows

System role	Description	Default permission
Workflow Admin	• Read/write operations related to workflows • Display system configuration information	• WorkflowOperationWrite • WorkflowOperationRead • SysConfigRead • DeviceBasicRead
Workflow Operator	• Reading operations related to workflows • Display system configuration information	• WorkflowOperationRead • SysConfigRead • DeviceBasicRead

System roles for printing

System role	Description	Default permission
Print Admin	• Read/write operations related to printing • Display system configuration information	• PrintOperationWrite • PrintOperationRead • SysConfigRead • DeviceBasicRead • SlnxUserOperationRead

System role	Description	Default permission
Print Operator	• Read operations related to printing • Display system configuration information	• PrintOperationRead • SysConfigRead • DeviceBasicRead • SlnxUserOperationRead
Accounting Admin	• Read/write operations related to account management • Display system configuration information	• AccountingOperationWrite • AccountingOperationRead • SysConfigRead • DeviceBasicRead • WorkflowOperationRead • SlnxUserOperationRead
Accounting Operator	• Read operations related to account management • Display system configuration information	• AccountingOperationRead • SysConfigRead • DeviceBasicRead • WorkflowOperationRead • SlnxUserOperationRead

System roles for quota adjustment

System role	Description	Default permission
Quota Adjustment Admin	• Read/write operations related to page limits and balance • Display system configuration information	• QuotaOperationWrite • AccountingOperationRead • SysConfigRead • SlnxUserOperationRead • SecurityRead

Creating a Custom Role

Create a role to be assigned to a user. Duplicate an existing system role with the permissions that match the role you want to create, and then edit and register the duplicated role as the new role.

Important

- **Only a user who is assigned the system role of Full Admin or Security Admin can duplicate a role. Create a custom role that is assigned the permissions of SecurityRead and SecurityWrite to allow the user who is assigned the custom role to duplicate a role.**

1. **Click the following items in the navigation tree to open the [User Roles] tab.**

   [System] ▶ [Security] ▶ [User Roles]

2. **Select the system role to be used as the model of a new role, and then click (Copy).**
3. **On the [Role] tab, enter the custom role name.**
4. **Change [Login expiry time] as necessary.**
5. **Enter the LDAP group name in [LDAP group name].**

   The role is assigned to all members that belong to the LDAP group name entered here.

   The system does not check whether the LDAP group name is correct. Check that the entered LDAP group name is correct.

6. **On the [Restrictions] tab, specify [Security Context (Read)] or [Security Context (Write)].**

   You can display and edit the information of the devices that belong to the specified category. For details, see page 167 "Configuring Group Restrictions".

7. **Select the permission to be granted to the role on the [Permissions] tab.**
8. **On the [User] tab, select a local user account to be assigned to the role.**

   When LDAP/Kerberos authentication is used, you can assign a role to externally identified users by configuring the LDAP group name on the [Role] tab.

Note

- For details about the setting items on each tab, see page 557 "User Roles".
- Local User Account is the account to be used only for operating the Management Console. Create it using the following screen: For details about the configuration items, see page 561 "User Accounts".

Configuring Group Restrictions

Enable [Group Restrictions] to apply access restrictions on each device category or device group.

For example, when the "Tokyo" and "Osaka" groups exist in the first hierarchy of the "Location" category and you specify Security Context to the "Tokyo" group on the "Restrictions" tab for the roles, roles can perform allowed operations on devices that belong to the "Tokyo" and any subordinate groups. Operations cannot be performed on devices that belong to the "Osaka" group but do not belong to the "Tokyo" group.

The Group Restrictions setting applies only to a single device category and the subordinate device groups. To use the [Group Restrictions] function, organize device categories to which the devices belong and device groups in advance. For details, see page 71 "Organizing the Device List".

Use the group restrictions setting to restrict usage of the following functions in the system:

- User role

- Destination
- Configuration templates

All templates including standard device configuration, device specific preferences, SDK/J platform, Device Applications, address book, log collection templates.

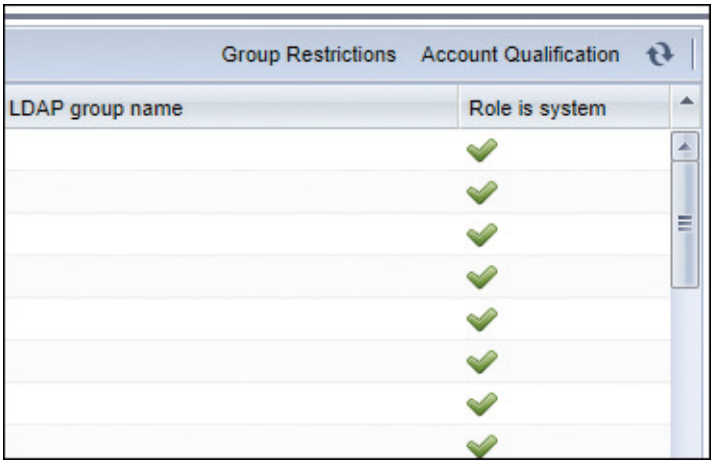
Note

- The group restrictions setting only applies to the items, devices, and groups displayed in the system. Therefore, a discovery task, polling profile, access profile, e-mail list, configuration template and report template are assigned to the security group that the creating user of those items belongs to. Group restriction only applies to the task itself. Note that it does not apply to the devices selected in the task. Also, group restriction only applies to report templates and not to the devices selected in the report.
  - Device Status Polling
  - Discovery
  - Notification Alerts

1. **Click the following items in the navigation tree to open the [User Roles] tab.**

   [System] ▶ [Security] ▶ [User Roles]

2. **Select the role to which to apply the group restrictions, and then click [Group Restrictions].**



3. **Select the [Enable restrictions] check box.**
4. **Select the device category to which to allow access.**

   The group restriction setting of each function applies to the group hierarchy selected by the administrator and specified by the subordinate hierarchy.

5. **Click [OK].**
6. **Click [Yes].**

7. **Select the roles for specifying Security Context from the list, and select [Security Context (Read)] and [Security Context (Write)] on the [Restrictions] tab.**
8. **Click (Save).**

Note

- For details about setting items, see page 557 "User Roles".

Configuring Account Qualification

Enable [Account Qualification] to qualify user accounts by the authentication profile. It is useful in cases where there are the same user names with different domains and they are RICOH Streamline NX administrators as well.

When [Account Qualification] is enabled, you can use the qualified user names when storing view settings of the device list, power filters, custom dashboards, reports, audit logs, and recording the last user who made a change to specific configurations.

View settings of the device list

When [Account Qualification] is enabled, the view is stored with the user name specified with the authentication profile used when the user logs in and the internal ID. Only the user who logged in using the specified authentication profile can access the stored view.

Power filters

When [Account Qualification] is enabled, the power filter is stored with the user name specified with the authentication profile used when the user logs in and the internal ID. Only the user who logged in using the specified authentication profile can access the stored power filter.

Dashboards

When [Account Qualification] is enabled, the custom dashboard is stored with the user name specified with the authentication profile used when the user logs in and the internal ID. Only the user who logged in using the specified authentication profile can access the stored dashboard.

Reports

When [Account Qualification] is enabled, the report template, schedule, and task are stored with the user name specified with the authentication profile used when the user logs in and the internal ID. Only the user who logged in using the specified authentication profile can access the report.

Audit logs

When [Account Qualification] is enabled, a user name is recorded in the audit log as follows:

- When the account is an internal account, only the user name is recorded
- When the account uses an authentication profile, the user name of the account qualified by the authentication profile is recorded together with the authentication profile used upon login and its internal ID. The audit log records the user name with the profile name at the time of the

audit, so if the profile name is changed, the user name with the old profile name may be recorded.

Last Updated Users

When [Account Qualification] is enabled, the name of the last user who changed the setting is recorded as follows:

- When the account is an internal account, only the user name is recorded
- When the account uses an authentication profile, the user name of the account qualified by the authentication profile is recorded together with the authentication profile used upon login and its internal ID. The user name with the profile name is recorded when changed, so if the profile name is changed, the user name with the old profile name may be recorded.

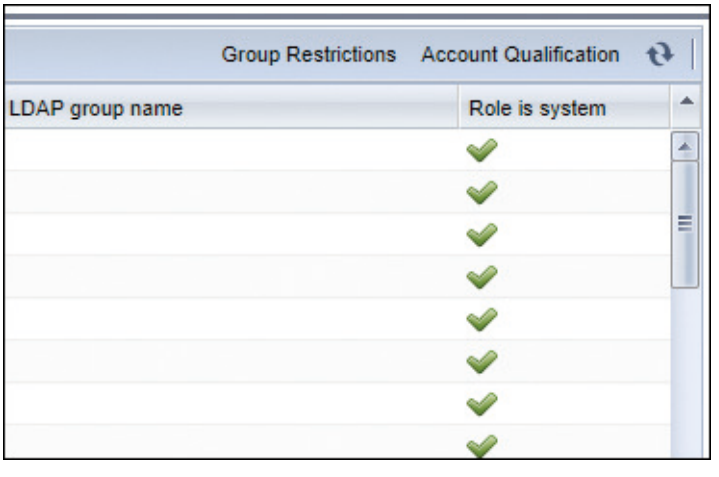
[Account Qualification] is disabled after RICOH Streamline NX is installed or updated from Device Manager NX, and the users with the same name are treated as the same account in the functions listed above.

Follow the procedure below to enable [Account Qualification].

1. **Click the following items in the navigation tree to open the [User Roles] tab.**

   [System] ▶ [Security] ▶ [User Roles]

2. **Click [Account Qualification].**



3. **Select the [Qualify accounts by Authentication Profile] check box.**
4. **Click [OK].**

Note

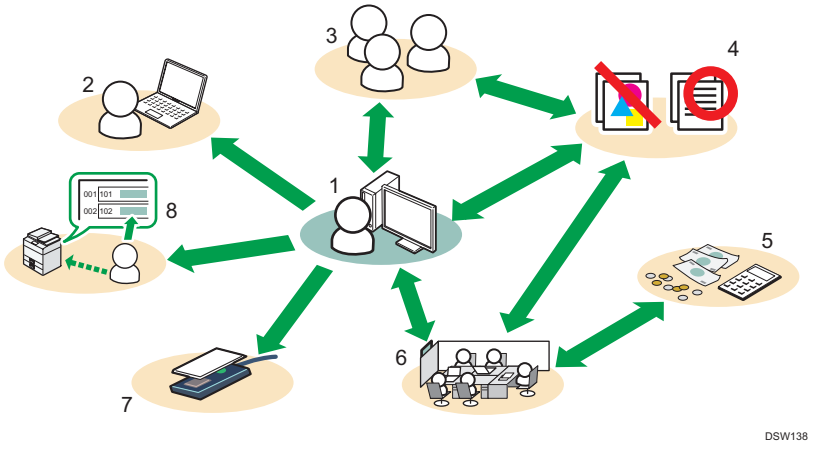
- If an authentication profile is deleted, any custom user data will be orphaned in the database. When the authentication profile is added again, it is assigned with a new internal ID so the custom user data will still be orphaned.

- When the [Account Qualification] setting is disabled, custom user data will be orphaned in the database. If the setting is enabled again, the data will be available.

Managing User Information

You can associate various information with a local user or externally identified user registered on the Core Server. For example, register card information to assign the card as part of the user information. In addition, you can combine multiple users to form a group and apply settings such as available device functions and workflows to users in a group at the same time.

The relationship of items that can be managed as user information is shown below. The direction of an arrow indicates that the setting item affects the destination item.



1. **User**

   A person that uses the system.

2. **Delegation User**

   A user that can execute a print job in place of another user.

3. **Group**

   Combine users that belong to a team or members of a project to form a group.

4. **Permissions**

   A set of definitions to specify usable device functions and workflows.

5. **Cost Center**

   The department that bears the cost incurred by the user.

6. **Department**

   The department to which the user belongs.

7. **Card**

   The card used to log in to a device.

8. **Alias**

   The name displayed on the print job list.

Managing Groups

You can combine multiple users to form a group.

Create a group to specify available device functions and workflows for multiple users at one time. You do not need to apply the settings to those users individually.

Important

- **You cannot create a group on the external authentication server.**
- **You can only add local users to the created group. You cannot add externally identified users to a group.**

1. **Click the following items in the navigation tree to open the [Groups] tab.**

   [User Management] ▶ [Groups]

2. **Click (Add).**
3. **On the [General] tab, enter the group name and description.**
4. **Click (Add) on the [Users] tab.**
5. **Select the user to be added to the group, and then click OK.**
6. **Click (Save).**

Note

- For details about the setting items, see page 612 "Groups".

Managing Departments

You can combine multiple users into a department.

Create a department to specify available device functions and workflows for a group of users at one time. Unlike a group, you can configure a Cost Center for a department. In addition, you can create departments in a hierarchical structure and organize them according to their actual hierarchical relationship.

Important

- **You cannot create a department on an external authentication server.**
- **You can only add local users to the created department. You cannot add externally identified users to a departments.**

1. **Click the following items in the navigation tree to open the [Departments] tab.**

   [User Management] ▶ [Department]

2. **Click (Add).**

3. **On the [General] tab, enter the department name and description.**
4. **To add a newly created department under an existing department, select the parent department from the [Parent Department] menu.**
5. **Click (Add) on the [Users] tab.**
6. **Select the user to be added to the department, and then click [OK].**
7. **Click (Edit) on the [Cost Centers] tab, and then select a Cost Center.**

   For example, when configuring a newly created sales department where costs of consumables are paid by the general affairs department, specify the Cost Center of the general affairs department.
8. **Configure the functions and workflows that can be used by the department on the [Permissions] tab.**
9. **Click (Save).**

Note

- For details about the setting items, see page 613 "Departments".

Managing Permissions

You can configure settings to use copier or other functions on a device or Device Applications workflow. You can specify use permissions for the following device functions:

Built-in Functions

Copier (Full Color Auto Selection, Full Color, Two-color, Single Color, Black and White)

Other Functions (Document Server, Facsimile, Scanner)

Workflows

(Workflow name)

Permissions can be assigned to departments, groups, and users.

When a permission is assigned to a user, the permissions assigned to the department or group that the user belongs to are ignored.

The permissions assigned to the department and group that the user belongs to are both applied to the user if no permission is assigned to the user. For example, if no permission for copying in color is given the group that the user belongs to, the user can copy in color if this permission is given the department.

1. **Click the following items in the navigation tree to open the [Permissions] tab.**

   [User Management] ▶ [Permissions]
2. **Click (Add).**
3. **On the [Permission Settings] tab, enter the permission name and description, and then select the check boxes of the native functions to be used.**

4. **Click (Add) on the [Departments] tab.**
5. **Select the department to which to apply the permissions you want to create, and then click [OK].**
6. **Click (Add) on the [Groups] tab.**
7. **Select the group to which to apply the permissions you want to create, and then click [OK].**
8. **Click (Add) on the [Users] tab.**
9. **Select the user to which to apply the permissions you want to create, and then click [OK].**
10. **Click (Save).**

Note

- For details about the setting items, see page 621 "Permissions".
- You can specify print rules and account balance in order to limit the use of the printer function. For details, see page 199 "Configuring Print Rules", or page 615 "Users".
- When importing a CSV file of the [Permission] settings, make sure that the language of the Management Console is the same one as when the file has been exported. Otherwise, some setting values are not imported.

Managing Cost Centers

Configure Cost Centers settings to transfer costs of consumables and other items among different departments. For example, when costs of consumables used by the sales department is paid by the general affairs department, specify the general affairs department as Cost Center.

1. **Click the following items in the navigation tree to open the [Cost Centers] tab.**

   [User Management] ▶ [Cost Centers]

2. **Click (Add).**
3. **On the [General] tab, enter the name and description of Cost Center.**
4. **To add a newly created Cost Center under an existing Cost Center, select the parent Cost Center from the [Parent Cost Center] menu.**
5. **Click (Add) on the [Users] tab.**
6. **Select the user to be added to the Cost Center, and then click [OK].**
7. **Click (Save).**

Managing Card Information

Register card information to log in to devices.

There are three methods for registering a card as follows:

The administrator registers card information from a CSV file

Import the information of numerous cards at one time from a CSV file.

Select [User Management] ▶ [Cards] to open the screen for downloading the CSV file. Enter additionally required information if any, and then save and import the file.

Note

- When importing a CSV file, make sure that the language of the Management Console is the same one as when the file has been exported. Otherwise, some setting values are not imported.

The administrator registers card information individually on the screen

To register some cards, select [User Management] ▶ [Cards] to open the screen for entering information manually.

The user registers card information on the device screen

The user registers the card information from the operation screen of the device.

The user can register the information if the [Enable Card Registration] check box is selected on [Authentication] tab under [System] ▶ [Server Settings] ▶ [Delegation Server Settings].

Registering card information individually

Important

- **Temporary Card and Limited Period Card are automatically deleted after the expiration date.**

1. **Click the following items in the navigation tree to open the [Cards] tab.**

   [User Management] ▶ [Cards]

2. **Click (Add).**
3. **Enter [Card Number] and [Card Name].**
4. **Click [Search User], select the user who uses the card, and then click [OK].**
5. **Select the card type, and specify the expiration date as necessary.**
   - Indefinite Period Card

     This card does not have an expiration date. Select this type to issue a card to a contract employee working without a fixed term.
   - Limited Period Card

     This card can only be used for a limited period. Select this type to issue a card to an employee or visitor who is working on site only for a limited period.
   - Temporary Card (only available for one day)

Specify the date of usage as the end date. Select this type to issue a card to an employee or visitor who is working on site as a guest for one day only.

6. **Click (Save).**

5. Managing Printing Functions

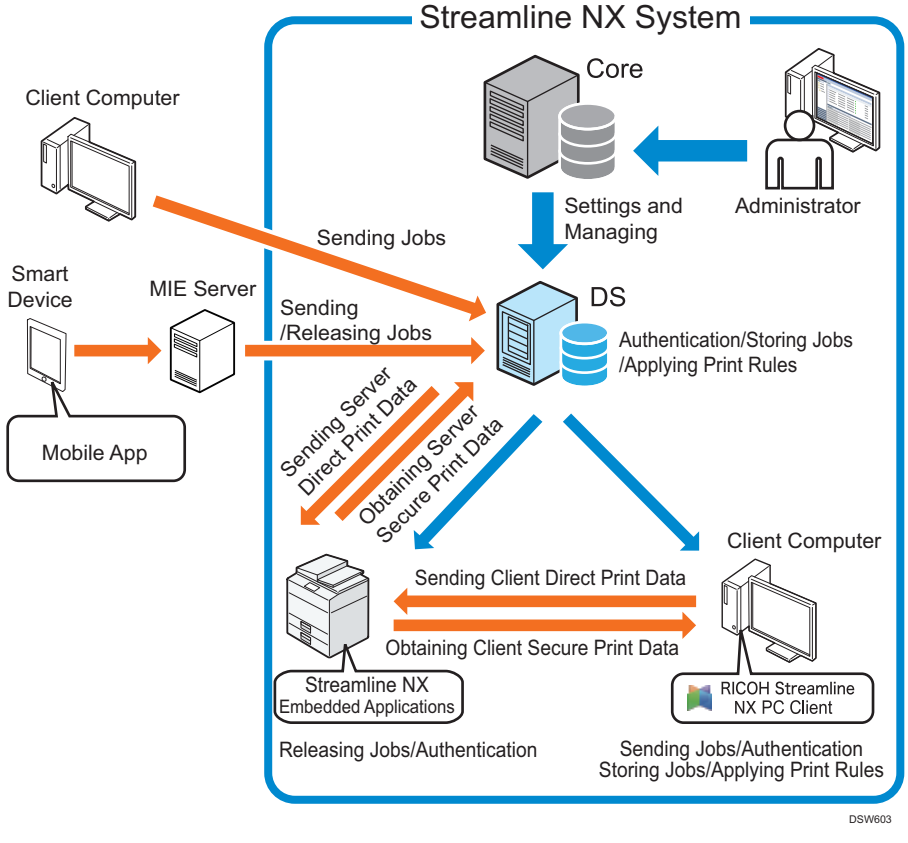
This chapter describes how to use secure printing, direct printing, print rules, and other printing functions of RICOH Streamline NX and the settings to be configured to use these functions.

This also describes printer driver distribution.

Overview of the Printing Functions

The RICOH Streamline NX system allows an administrator to configure and manage Delegation Servers and printing devices, all from a single Management Console. The Management Console can also be used to centrally manage information about print jobs sent from client computers.

In addition, when RICOH Streamline NX PC Client is installed to a client computer, the software works with RICOH Streamline NX to enhance printing functionality. In addition to processing print jobs based on print rules and storing secure print documents on a client computer, RICOH Streamline NX PC Client can also send metadata printed on a locally connected printer to the server. For details, see RICOH Streamline NX PC Client Operation Guide.



You can combine various printing features so you can achieve enhanced security, reduced cost, and greater printing efficiency at the same time.

The Secure Printing Function

The Secure Print Function allows only identified users to perform secure printing from devices that have Streamline NX Embedded Applications installed.

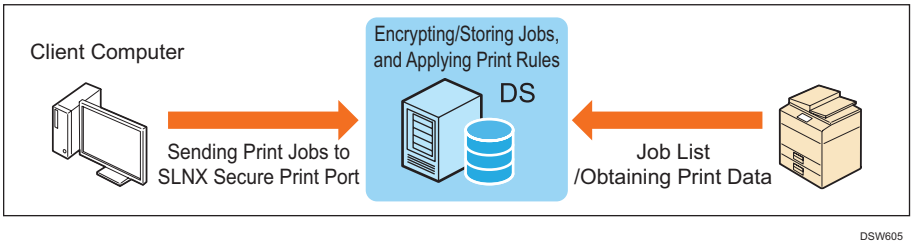
When the secure printing function is used, the print job sent by the user is not immediately output, but instead it is encrypted and stored in a folder on the Delegation Server, or on a client computer folder specified when installing RICOH Streamline NX PC Client. Users can view the list of documents held on the server or RICOH Streamline NX PC Client from any device with Streamline NX Embedded Applications embedded, access the required documents from a nearby device, and securely print them at any time. The same is possible using mobile devices with Streamline NX Mobile Application installed.

The secure printing function not only improves security, but it also reduces misprinting and non-essential printing to help reduce printing costs. For example, it can be used in the following cases:

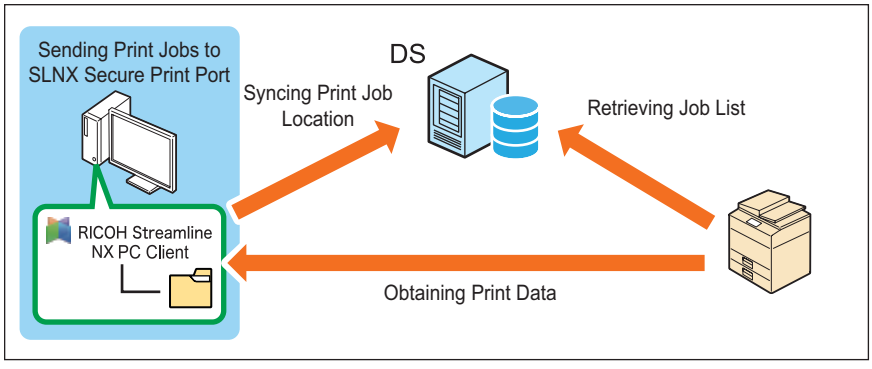
- When you want to print a document while you are standing by the device because it is confidential and should not be left on the output tray after printing
- When you store a document on the server for a meeting on another floor or separated office, so that you can print the required number of copies using the device located at the meeting site
- When you store a document to share it among project members by specifying them as delegate users

There are two types of secure printing: server secure printing, which uses the Delegation Server for authentication, storage, and processing of print jobs, and client secure printing, which uses RICOH Streamline NX PC Client for performing operations. The printing environment of the RICOH Streamline NX system can be set up to use the server or client secure printing according to the network environment such as transmission speed between the server and device.

Server Secure Printing



Client Secure Printing



Note

- For details about Secure Printing, see page 186 "Configuring Secure Printing".
- A user can print a secure print document by logging in to a Ricoh device with Embedded Client installed. A user can also use a mobile device with the RICOH Streamline NX mobile app installed to print from devices even without Embedded Client installed and from non-Ricoh devices.

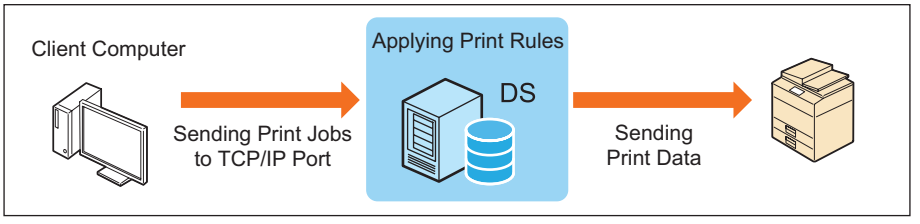
The Direct Printing Function

Using Direct Printing, you can print documents using the RICOH Streamline NX printing functions other than Secure Printing, including authentication, accounting, and print rules. In Direct Printing, authentication, application of print rules, and other job processing are performed on the Delegation Server or the RICOH Streamline NX PC Client, but print jobs are immediately printed from a device and not held on the Delegation Server or the RICOH Streamline NX PC Client.

Direct Printing is convenient in an environment in which you want to keep using the print settings already configured in your host system, for example. Also, the print jobs are output without having to release them from the control panel of the device and there is no need to wait next to the device for printing to end while printing a large document. Device Direct Print is also available if you want to print without involving the Delegation Server or the RICOH Streamline NX PC Client for environmental reasons such as using a low-spec server or low-speed communication (see page 182 "Device Direct Printing").

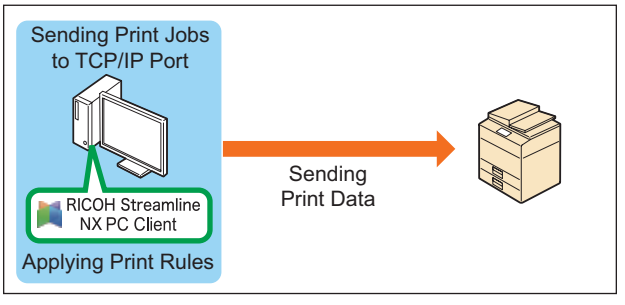
Users can also print jobs without user name or as user alias in a case such as printing from UNIX or a mainframe.

Server Direct Printing



DSW610

Client Direct Printing



DSW612

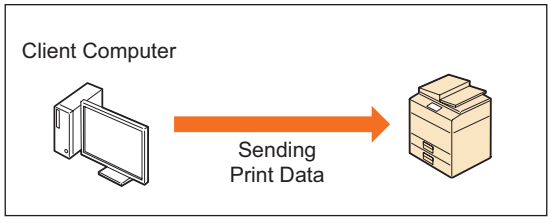
Note

- For details about Direct Printing, see page 195 "Configuring Direct Printing".
- Using Direct Printing, users can print document directly to a RICOH device with or without Streamline NX Embedded Applications installed and to non-RICOH devices or USB-connected devices.
- To print from a USB-connected device, it is necessary to install RICOH Streamline NX PC Client on the client computer.
- Print rules are not applied when printing from non-RICOH devices. For details, see page 213 "Supported Devices".

Device Direct Printing

Using Device Direct Printing, users can submit print jobs directly to a target device, without any Delegation Server or RICOH Streamline NX PC Client involvement.

When a user prints to a device using device direct print, information for user authentication is captured using the user ID entered by the user on the printer driver or the computer login user name from which the job is sent. You can also print jobs without a user name or using user alias.



DSW611

Important

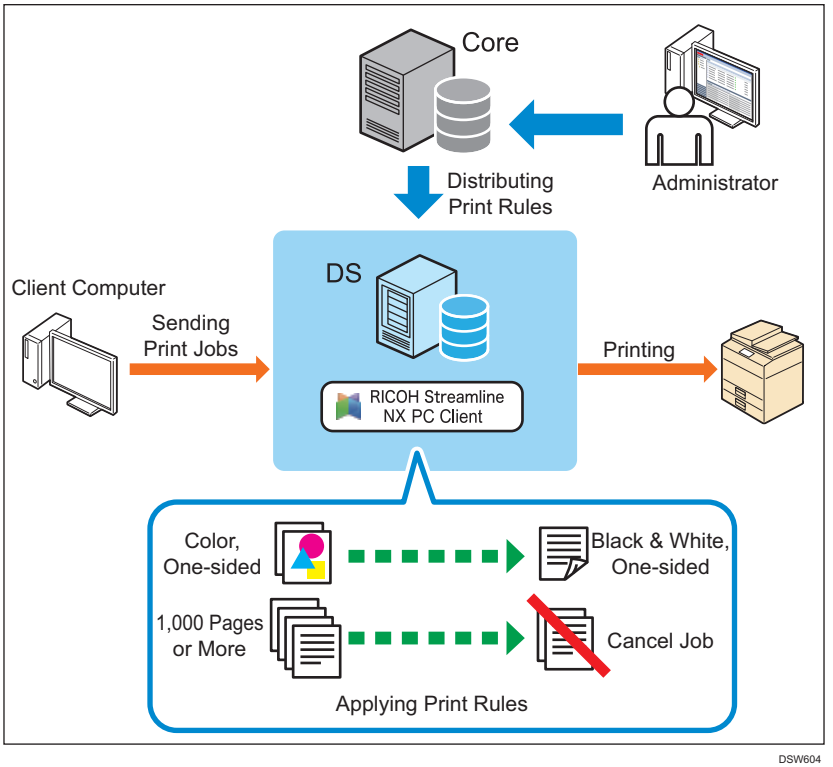
- **Install he printer driver of the device on your computer.**
- **The print rules function cannot be used.**

Note

- The Device Direct Printing does not require the optional Print Management license purchased and activated for the target device.

Print Rules

The print rules automatically modify print job settings sent by users to enforce printing policies defined by the administrator. The print rules are configured in advance by the administrator in the Management Console according to the operation purpose. The configured print rules are distributed to Delegation Servers and RICOH Streamline NX PC Client, and these are applied upon receiving a print job or releasing a secure print job.



Note

- For details about Print Rules, see page 199 "Configuring Print Rules".

Client Accounting

Configure Client Accounting to collect and store accounting data on a device that is connected only via USB and not on the network, or on a device that is not installed with the Streamline NX Embedded Applications. The user is identified using the user information registered to the system and can perform printing on the device.

The following accounting information is sent to the Delegation Server:

- User Name, Domain Name
- Job name
- Date
- Number of pages
- Black-and-white/color
- 1-sided/2-sided
- Job data size

- Device information (Serial number)
- Quantity
- Paper size
- Computer name
- Cost center name

Note

- If the Print Rules should satisfy the print job criteria that is specified on the Delegation Server, the rules will also be applied to print jobs that are performed using Client Accounting.

Configuring Secure Printing

This section describes the secure printing function of the RICOH Streamline NX system and the differences between server secure printing and client secure printing. It also explains how to manage secure print documents stored on the server.

Features of Secure Printing Functions

The secure printing function of RICOH Streamline NX has the following features:

Global secure printing

The Core Server centrally manages all job lists submitted by each user and enables the user to view all print lists and print jobs from the operation panel of a device, even if secure print documents are stored in folders across multiple Delegation Servers and RICOH Streamline NX PC Client.

The administrator can use the Management Console to check lists of print jobs stored on the Delegation Server and delete jobs as necessary. For details, see page 193 "Managing Job List".

Releasing by a Delegate User

A stored secure print document can be released by the user who sent the print job and also by a specified delegate if one is configured when the job was printed.

Even when a delegate user releases a secure print job, the print-rules are applied and the accounting information is registered based on the user who printed the job.

In addition, when secure printing is performed from RICOH Streamline NX PC Client, the user can use Client Delegation Print to specify up to five delegate users for each sent job from among 10 specified candidates.

All routing actions for print rules are disabled in Client Delegation Print.

Note

- For details about configuring delegate users using the Management Console, see page 158 "Registering Local Users on the Management Console".
- For details about configuring Client Delegation Print, see "Preferences", RICOH Streamline NX PC Client Operation Guide.

Changing Printing Preferences When Releasing a Job

The user can change the printing preferences when logging in and accessing a device used for printing a secure print document. Only the functions supported in the printer driver can be changed (the number of copies, print side (2 Sided or 1 Sided), color settings (Color or Black and White), and whether to delete after printing). When there are applicable print rules, these are applied according to the changed printing preferences. Job logs and accounting information are recorded with the details after the print settings are changed.

Note

- If a device does not support the specified printing preferences, the output result may not correctly reflect the specifications in the preferences.

Test Print

Before printing all copies, you can try to print one copy. Print rules are applied, and accounting and job log recording are performed even at test printing. However, the application result of the print rule may be different from normal printing depending on the quantity and other settings.

HotSpot Enterprise linkage

On a RICOH Streamline NX Delegation Server, the following print jobs are processed as follows when sent from a HotSpot Enterprise (HSE) system.

- If the user information of the print job can be obtained from the e-mail address when a normal print job is sent, the Delegation Server processes the job as a normal secure print job, and the user can log in and release the job as a RICOH Streamline NX user.
- When an HSE guest print job is sent to the SLNX Secure Print Port, the user can enter the HSE PIN and release a secure print job as a guest user. To print as a guest user, enable [Guest Login] of [Login Method] on the [Authentication and Accounting] tab of [Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Authentication]. For the configuration procedure, see page 508 "Embedded Authentication".

Note

- While print rules are applied to the HSE job, the routing action is ignored, and all HSE jobs are stored on the Delegation Server.
- The HSE job information is registered to the job list in the same manner as normal secure print jobs.
- For details about HSE, see RICOH Streamline NX v3 HotSpot Enterprise v3 Linkage Configuration Guide.

Linkage with external print systems

The users can access and release print jobs stored in external systems from devices with Streamline NX Embedded Applications or smart devices with RICOH Streamline NX mobile app installed. The print jobs can also be redirected to external systems by applying print rules.

The following print systems are supported:

- InfoPrint Manager
- LRS
- SEAL

Note

- For details about linkage with external print systems, see the manuals for external print systems.

- To use the linkage function with external print systems, it is necessary to register information about external systems such as their server addresses. For details, see page 574 "External Print Systems".
- [External] (for the Standard Operation Panel) or (for the Smart Operation Panel) is displayed in the data storage information in the Print Document List Screen for the documents stored in external systems. For details about the Print Document List Screen, see "Printing a Document from a Device", User's Guide.
- Contact your Seal Systems or LRS VPSX provider to obtain information on licensing requirements and supported versions of these applications.
- This function cannot be used with the HotSpot Enterprise System linkage function at the same time.

Differences between Server Secure Printing and Client Secure Printing

Secure Printing allows you to store a print job on the Delegation Server or in the specified folder on a client computer and release it later by selecting it from the job list on the operation screen of a device.

In either of Server Secure Printing or Client Secure Printing, the target printer is a shared printer configured with the SLNX Secure Print port.

However, there are differences between Server Secure Printing and Client Secure Printing as shown below. You can select the method most suitable for the environment where RICOH Streamline NX is operated.

	Server Secure Printing	Client Secure Printing
Job Processing location (job storage/print rules application/ encryption)	Delegation Server The job list can be managed directly using the Management Console.	Client Computer The administrator can only view the job list on the Management Console. This method consumes the least resources on the Delegation Server, so it is suitable for an environment where only few servers are available for printing or servers are running on low-spec hardware, etc. This method also reduces the traffic between client computers or devices and the Delegation Server.

	Server Secure Printing	Client Secure Printing
Installation of the printer driver of the target device on the client computer that performs printing	Not Required Jobs can be printed after registering the shared printer to the client computer by simply dragging and dropping the printer icon.	Required Installation of the printer driver of the target device and the SLNX Secure Print port configuration is required.
Installation of RICOH Streamline NX PC Client on the client computer that performs printing	Not Required No dedicated application is required.	Required In RICOH Streamline NX PC Client, you can receive a popup message when print rules are going to be applied.
Starting the client computer when printing	Not Required Print job data is held on the Delegation Server so print jobs can be released even if the client computer is off or not at hand.	Required The client computer must be turned on to accept access to the folder in which print job data is held.

Note

- When print rules are configured, storing and printing may not be performed depending on the print rule settings.
- You can delete the print jobs stored on the Delegation Server manually from the job list on the Management Console or the print document list screen of the device or mobile device. Stored jobs can also be automatically deleted by either specifying Job Storage Period on the Delegation Server, or by configuring how stored jobs are processed after being printed. For details about configuring automatic deletion of stored jobs, see page 395 "Managing the System Capacity".
- You can delete print jobs stored using RICOH Streamline NX PC Client manually from the print document list screen of the device or mobile device. Stored jobs can also be automatically deleted by either specifying Job Storage Period on the RICOH Streamline NX PC Client or by configuring how stored jobs are processed after being printed. For details about configuring automatic deletion of stored jobs, see "[Print] tab", page 539 "Delegation Server Settings".
- Specify the storage location of server secure print jobs when installing the Delegation Server. For details about installing a Delegation Server, see "Installing RICOH Streamline NX", Installation Guide. Use the following procedure to check the path specified at installation:
  1. From the navigation tree, click [Server Management].
  2. In [Server Group], select the group to which the Delegation Server belongs. In the displayed server list, select the Delegation Server whose path you want to check.

3. Click the [Print] tab.

- Specify the folder to store client secure print jobs when installing RICOH Streamline NX PC Client. For details, see "Installing RICOH Streamline NX PC Client", Installation Guide.

Settings to Use Secure Printing

Configure the following settings to use the secure printing functions:

Note

- To install a printer on the Delegation Server or client computer, it is convenient to use a driver package created in Printer Driver Packager NX/Ridoc Ez Installer NX for installation. Configure the following when creating a driver package:
  - To install a printer on the Delegation Server
    - Specify the port appropriate for the connection between the server and the device.
    - Configure the printer as a shared printer.
  - To install a printer on a client computer
    - Specify Secure Print Port as the port. For details about how to specify the port name, see the user's guide of Printer Driver Packager NX/Ridoc Ez Installer NX. In addition, install RICOH Streamline NX PC Client to create Secure Print Port.

Settings for Server Secure Printing

1. ▶ **Managing the Streamline NX Embedded Applications**

To use the secure printing functions on a device with the Streamline NX Embedded Applications installed, configure authentication and print-related settings in [Streamline NX Embedded Settings], and associate the device with a Delegation Server.

For details about [Streamline NX Embedded Settings], see page 122 "Managing the Streamline NX Embedded Settings".

For details about association with a Delegation Server, see page 539 "Delegation Server Settings".

2. ▶ **Configuring User Authentication**

To use the printing function of RICOH Streamline NX and to use the RICOH Streamline NX functions from a mobile device, register a user to the RICOH Streamline NX system, and grant printing privileges.

For details, see page 153 "Managing the Authentication Settings".

3. **▶ Defining a Shared Printer on a Delegation Server**

Install a shared printer driver to the Delegation Server, and configure an SLNX Secure Print Port. Configure the shared settings.

For details, see page 215 "Defining a Shared Printer on a Delegation Server".

4. **▶ Registering a Shared Printer to a Client Computer**

Copy and register the shared printer configured on the Delegation Server to the client computer.

For details, see "Printing", User's Guide.

Note

- The following options can be configured:
  1. ▶ Configuring the Fail Over Function

A device can be associated with multiple Delegation Servers. When a communication problem occurs between the device and the primary server and the server does not respond, operations can be temporarily switched to a secondary server. Specify the priority of the Delegation Servers in advance.

For details, see page 383 "Balancing the Workload among Servers".

  2. ▶ Specifying a Delegate User

Five delegate users can be specified for each user.

For details about manage user information, see page 157 "Creating and Importing Users".

  3. ▶ Configuring the Print Job Data Storage Period and Automatic Delete Setting

Configure the storage period for stored jobs and specify whether or not to delete stored jobs after printing.

For details, see "[Print] tab", page 539 "Delegation Server Settings".

Settings for Client Secure Printing

1. ▶ **Managing the Streamline NX Embedded Applications**

> To use the secure printing functions on a device with the Streamline NX Embedded Applications installed, configure authentication and print-related settings in [Streamline NX Embedded Settings], and associate the device with a Delegation Server.
>
> For details about [Streamline NX Embedded Settings], see page 122 "Managing the Streamline NX Embedded Settings".
>
> For details about association with a Delegation Server, see page 539 "Delegation Server Settings".

2. ▶ **Configuring User Authentication**

> To use the printing function of RICOH Streamline NX and to use the RICOH Streamline NX functions from a mobile device, register a user to the RICOH Streamline NX system, and grant printing privileges.
>
> For details, see page 153 "Managing the Authentication Settings".

3. ▶ **Installing RICOH Streamline NX PC Client on a Client Computer**

> Install RICOH Streamline NX PC Client on a client computer.
>
> For details, see "Installing RICOH Streamline NX PC Client", Installation Guide.

4. ▶ **Registering a Printer to a Client Computer**

> Install the printer driver of the device to be used on the computer with RICOH Streamline NX PC Client installed, and configure an SLNX Secure Print Port.
>
> For details, see "Printing", User's Guide.

5. ▶ **Configuring Authentication with RICOH Streamline NX PC Client**

> When not using Windows Authentication at installation of RICOH Streamline NX PC Client, register the user name and password to use for authentication to RICOH Streamline NX PC Client.
>
> For details, see "Authentication Settings", RICOH Streamline NX PC Client Operation Guide.

Note

- The following options can be configured:
  1. ▶ Configuring the Fail Over Function

A device can be associated with multiple Delegation Servers. When a communication problem occurs between the device and the primary server and the server does not respond, operations can be temporarily switched to a secondary server. Specify the priority of the Delegation Servers in advance.

For details, see page 383 "Balancing the Workload among Servers".

2. ▶ Specifying a Delegate User

Five delegate users can be specified for each user.

For details about manage user information, see page 157 "Creating and Importing Users".

3. ▶ Configuring the Print Job Data Storage Period and Automatic Delete Setting

Configure the storage period for stored jobs and specify whether or not to delete stored jobs after printing.

For details, see "Client Secure Print", RICOH Streamline NX PC Client Operation Guide.

Managing Job List

The job list is obtained via a Delegation Server and centrally managed by the Core Server. The administrator can check the job list on the Management Console. In addition, a user can check the job list on the operation screen of devices with Streamline NX Embedded Applications or on a mobile device with the RICOH Streamline NX mobile app installed.

This section describes how to check a job list in the Management Console.

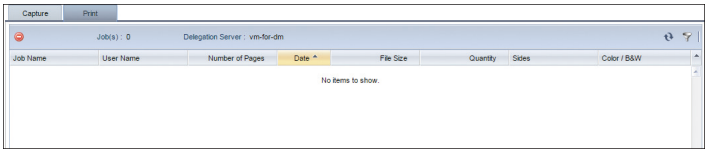
Note

- For details about checking a job list using the operation screen of a device or mobile device, see:
  - "Printing" or "Using the Streamline NX Mobile Application", User's Guide.
  - page 371 "Using RICOH Streamline NX on a Mobile Device"
- Only the Management Console can be used to manage the queue of secure print jobs stored on the Delegation Server.

1. **From the navigation tree, click [Server Management].**
2. **In [Server Group], select the group to which the Delegation Server belongs. In the displayed the server list, select the Delegation Server whose job list you want to check.**

   You can select multiple servers.
3. **Click the (Job Queue) button.**

4. **Click the [Print] tab.**



Item	Description
(Delete) button	Deletes the selected job.
Job(s)	Displays the number of jobs in the job list. When you are using the filter function, this displays the number of jobs matching the filter conditions.
(Filter) button	Filters the jobs displayed in the job list based on the conditions specified in each column. Enter the search terms you require in the Job Name and User Name columns. In the Date/Time column, specify the range of date and time. In the Sides and Color/B&W columns, select the value to use for the filter in the drop-down list.
(Refresh List) button	Refreshes the job list.
Job List	Displays the job list and their Job Name, User Name, Number of Pages, Date/Time, File Size, Quantity, Sides (2 Sided or 1 Sided), and Color / B&W settings.

Note

- Printable jobs are displayed in the job list.
- Deleted jobs and jobs that the rules have been applied rules and are waiting for user confirmation are not displayed in the job list.

Configuring Direct Printing

This section describes the differences between server direct printing and client direct printing and how to configure the settings to use direct printing.

Differences between Server Direct Printing, Client Direct Printing, and Device Direct Printing

Print jobs sent from a client computer are printed immediately from a target device via the Delegation Server during server direct printing and via RICOH Streamline NX PC Client during client direct printing.

The administrator can use the Management Console to view the log of direct print jobs.

There are differences among Server Direct Printing, Client Direct Printing, and Device Direct Printing as shown below. You can select the method most suitable for the environment where RICOH Streamline NX is operated.

	Server Direct Printing	Client Direct Printing	Device Direct Printing
Job Processing location (print rules application, etc.)	Delegation Server	Client Computer This method consumes the least resources on Delegation Servers, so it is suitable for an environment where only few servers are available for printing or servers are running on low-spec hardware, etc. This method also reduces the traffic between client computers or devices and the Delegation Server.	You cannot use rule-based printing.

	Server Direct Printing	Client Direct Printing	Device Direct Printing
Installation of the printer driver of the target device on the client computer that perform printing	Not Required Jobs can be printed after registering the shared printer to the client computer by simply dragging and dropping the printer icon.	Required Installation of the printer driver of the target device and the Standard TCP/IP port configuration is required.	Required Installation of the printer driver of the target device and the Standard TCP/IP port configuration is required.
Installation of RICOH Streamline NX PC Client on the client computer that performs printing	Not Required No dedicated application is required.	Required In RICOH Streamline NX PC Client, you can receive a popup message when print rules are going to be applied.	Not Required No dedicated application is required.

Note

- When print rules are configured, printing may not be performed depending on the print rule settings.
- If the target device is not registered in the device list of RICOH Streamline NX, print rules are not applied and the accounting information is not reported.

Configuring the Settings to Use Direct Printing

The following settings must be configured to use the direct printing functions:

Note

- To install a printer on the Delegation Server or client computer, it is convenient to use a driver package created in Printer Driver Packager NX/Ridoc Ez Installer NX for installation. Configure the followings when creating a driver package.
  - To install a printer on the Delegation Server
    - Specify the port appropriate for the connection between the server and device.
    - Configure the printer as a shared printer.
  - To install a printer on a client computer
    - Specify Secure Print Port as the port. For how to specify the port name, see the user's guide of Printer Driver Packager NX/Ridoc Ez Installer NX. In addition, RICOH Streamline NX PC Client must be installed to create Secure Print Port.

Configuring server direct printing

1. ▶ **Managing the Streamline NX Embedded Applications**

When using the direct printing functions on a device with Streamline NX Embedded Applications installed*, configure the authentication and print-related settings in [Streamline NX Embedded Settings] and associate the device with a Delegation Server.

For details about [Streamline NX Embedded Settings], see page 122 "Managing the Streamline NX Embedded Settings".

For details about association with a Delegation Server, see page 539 "Delegation Server Settings".

* This setting is not required when direct printing is used on a device without Device Applications installed or on a non-RICOH device.

2. ▶ **Defining a Shared Printer on a Delegation Server**

Install the printer driver of the shared printer to the Delegation Server, and configure the standard TCP/IP port. Also, configure the printer to be shared on the network.

For details, see page 215 "Defining a Shared Printer on a Delegation Server".

3. ▶ **Registering a Shared Printer to a Client Computer**

Copy and register the shared printer configured on the Delegation Server to the client computer.

For details, see "Printing", User's Guide.

Configuring client direct printing

1. ▶ **Managing the Streamline NX Embedded Applications**

When using the direct printing functions on a device with Streamline NX Embedded Applications installed*, configure the authentication and print-related settings in [Streamline NX Embedded Settings] and associate the device with a Delegation Server.

For details about [Streamline NX Embedded Settings], see page 122 "Managing the Streamline NX Embedded Settings".

For details about association with a Delegation Server, see page 539 "Delegation Server Settings".

* This setting is not required when direct printing is used on a device without Device Applications installed or on a non-RICOH device.

2. ▶ **Installing RICOH Streamline NX PC Client on a Client Computer**

Install RICOH Streamline NX PC Client on a client computer. For details, see “Installing RICOH Streamline NX PC Client”, Installation Guide.

3. ▶ **Registering a Printer to a Client Computer**

Install the printer driver of the device to be used on the computer with RICOH Streamline NX PC Client installed, and configure a standard TCP/IP port. For details about installing the printer driver, see the user's guide of the device being used.

Configuring device direct printing

1. ▶ **Managing the Streamline NX Embedded Settings**

When using device direct printing on a device with the Streamline NX Embedded Applications installed*, configure the authentication and print-related settings in [Streamline NX Embedded Settings] and associate the device with a Delegation Server.

For details about [Streamline NX Embedded Settings], see page 122 "Managing the Streamline NX Embedded Settings".

For details about association with a Delegation Server, see page 539 "Delegation Server Settings".

* This setting is not required when device direct printing is used on a device without the Streamline NX Embedded Applications installed or on a non-RICOH device.

Configuring Print Rules

This section describes how to specify print rules to be used for rule-based printing.

To use the Print rules, the administrator creates print rules in advance according to operation purposes, and when the user performs printing, the settings specified in the print rules are automatically applied.

Setting print rules as follows can reduce costs and improve productivity:

- Changing print settings to force black-and-white and/or two-sided printing
- Rejecting large print jobs
- Redirecting print jobs to appropriate devices in accordance with installation locations and/or operating costs

You can configure to display confirmation messages about the rules to be applied on print jobs on the operation panel of the device or RICOH Streamline NX PC Client. Once the rule is configured, users can check details of the rule to be applied on the confirmation screen and choose whether or not to continue printing.

Multiple print rules can be defined. Configure the following for each rule:

Condition

Specify conditions under which to perform an action set for a rule applicable to a sent job. When the print settings of a sent job match all or part of the set conditions, or when none of the print settings of a sent job match the set conditions, the set action is performed.

Action

Specify how to process jobs. There are four actions: Confirmation, Routing, Modify, and Notification.

- Confirmation

  Displays a pop-up notification of the details of the action before the action is executed.

- Routing

  Allows, denies, or holds a print job, or redirects a print job to TotalFlow or another printer.

- Modify

  Performs printing after changing the print settings forcibly.

- Notify

  Displays a pop-up notification on the screen of RICOH Streamline NX PC Client when a rule is applied, or sends a notification to users regarding the applied rule.

Target Users/Groups, Target Devices/Groups

Specifies the users or user groups, devices or device groups to apply print rules are applied. Only rules that match both users and devices are applied.

This setting is optional. If this setting is not configured, print rules are applied to all users and devices. It is recommended to configure this setting to search rules more efficiently.

The specified print rules are sent to the Delegation Server and RICOH Streamline NX PC Client.

When a user sends a print job from a computer or uses the operation panel of a device or mobile device to instruct the system to perform a secure print job, the Delegation Server or RICOH Streamline NX PC Client verifies whether or not there is an applicable rule and, if any, the server or computer applies all actions that meet the conditions.

Important

- **Print rules are disabled when the Device Direct Print Function is used.**

Creating Print Rules

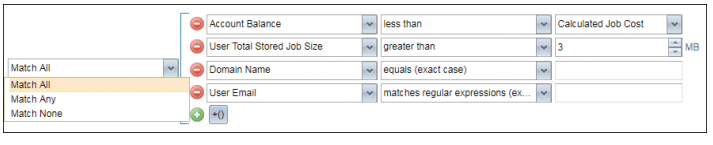
1. **Click the following item in the navigation tree to open the [Print Rules] tab.**

   [Workflow] ▶ [Print Rules]

2. **Click (Add).**

   To create a new rule based on an existing rule, click (Copy).

3. **On the [General] tab, enter the name and description of the print rule.**
4. **Select [On] to enable the print rule.**
5. **Click the [Criteria] tab.**
6. **Configure the conditions for performing actions.**



   Click (Add) to add a condition. Select a condition from the drop-down list.

   Click (Remove) to delete a condition.

   For details about the conditions that can be set, see page 201 "List of conditions".

7. **Specify how to apply conditions from [Match All], [Match Any], and [Match None].**
8. **Click the [Action] tab.**
9. **To display a confirmation message before performing an action, select [Show Pop Up Messages Before Applying Actions] under [Confirm].**

   To display the cost information on the confirmation window, select [Include Cost Information].

10. **Specify the action to be applied when a condition is met.**

    For the actions that can be specified, see page 204 "List of actions".

11. **To specify a user to be associated with the rule, click the [Target Users/Groups] tab.**

12. **Click (Add Group) or (Add User).**

    To delete all users, click (Delete All). To delete a specific user or user group, select the user or user group to and click (Delete Selected Entries).

    Select [Yes] on the confirmation window.

13. **On the [Target Groups] or [Select User] window, select the user or user group to be associated with the rule.**
14. **Click [OK].**
15. **To specify a device to be associated with the rule, click the [Target Device Groups] tab.**
16. **Click (Add (Target Group)) or (Add (Target Device)).**

    To delete all devices, click (Delete All). To delete a specific device or device group, select the device or device group and click (Delete Selected Entries).

    Select [Yes] on the confirmation window.

17. **On the [Target Groups] or [Select Device] window, select the device or device group to be associated with the rule.**
18. **Click [OK].**
19. **Click (Save).**

    The specified rules are distributed to the Delegation Server and RICOH Streamline NX PC Client.

    For details about checking whether the print rules have been applied, see page 209 "Testing the Print Rules".

List of conditions

The following is a list of conditions that can be specified. Multiple conditions can be combined together. When combining multiple conditions, specify how the conditions are applied from [Match All], [Match Any], and [Match None].

Variable	Comparison method	Description
Total Pages	less than/greater than	This is the number of copies multiplied by the total number of printed pages.
Data Size	less than/greater than	This is the data size of the print job.
Color Mode	equals (exact case)	This is the color setting of the print job. Select Color or B&W.
1 Sided/2 Sided	equals (exact case)	This is the print side setting of the print job. Select 1 Sided or 2 Sided.

Variable	Comparison method	Description
Job Name	equals/starts with/ends with/contains/equals (exact case)/starts with (exact case)/ends with (exact case)/contains (exact case)/matches regular expressions (exact case)	The job name of the submitted print job is compared with the job name or a part of job name entered here.
Day(s)	is one of	This is the day of the week the job was printed. Select from Monday to Sunday.
Time	between (inclusive)	This is the time of day the job was printed. Set the start and end times for printing.
PDL	is one of	This is the PDL of the print job. Select from PCL6, PCL5, PS, and RPCS.
User Type	equals (exact case)	This is the type of user who sent a print job. Select Registered or Guest. Guest is a user that performs guest printing using HotSpot Enterprise, etc.
User Department	equals/starts with/ends with/contains/equals (exact case)/starts with (exact case)/ends with (exact case)/contains (exact case)/matches regular expressions (exact case)	The name of the department to which the user directly belongs is compared with the name or a part of the name of department entered here.
User Email	equals/starts with/ends with/contains/equals (exact case)/starts with (exact case)/ends with (exact case)/contains (exact case)/matches regular expressions (exact case)	The user's e-mail address is compared with the e-mail address or a part of e-mail address entered here.
Job Cost	less than/greater than	This is an estimate of the job cost based on the job data. It may differ from the actual cost.

Variable	Comparison method	Description
Account Balance	less than/greater than	This is the user's current balance. It will be compared with the estimated Job Cost based on the job data.
User Total Stored Job Size	less than/greater than	This is the total size of other Server Secure Print jobs held by the same user in the Delegation Server.
Destination Printer Status	is one of	This is the status of the destination printer obtained when SNMP monitoring is enabled in the standard TCP/IP port setting of the printer driver. This condition is not taken into account when secure print jobs are printed. Select from [Ready], [Error], and [Unavailable]. **Note** • For print rules to operate properly, SNMP monitoring must be disabled in the standard TCP/IP port setting of the printer.
Domain Name	equals/starts with/ends with/contains/equals (exact case)/starts with (exact case)/ends with (exact case)/contains (exact case)/matches regular expressions (exact case)	The domain name or a part of domain name specified here will be compared with the name of the domain from which the print job is submitted.
Application Name	equals/starts with/ends with/contains/equals (exact case)/starts with (exact case)/ends with (exact case)/contains (exact case)/matches regular expressions (exact case)	The application name or a part of application name specified here will be compared with the name of the application from which the print job is submitted. Application Name totally depends on each application or driver regardless of whether it is input in PJL header or not. **Note** • This variable is effective only when the PCL6 or PS Driver for Universal Print 4.13 or later version is used.

List of actions

The following is a list of actions that can be specified. Multiple actions can be specified for individual rules.

Action category	Action	Description
Confirm	Show Pop Up Messages Before Applying Actions	This displays a pop-up notification of the action details before the action is taken. The user can choose to continue printing while applying the rule or cancel printing. Pop-up notifications appear on the screen in RICOH Streamline NX PC Client only when a print job is sent from the PC Client at the time the rule is applied. Pop-up notifications appear on the operations screen of the device when the rule is applied at the time the print job is released. Cost information appears in a pop-up notification when [Include Cost Information] is enabled.
Routing	Redirect to TotalFlow	This is the highest priority action during routing. This redirects print jobs to TotalFlow. Specify the workflow name when specifying this action. [Set Priority to] is not available when specifying this action. Be sure to enter the workflow name which exists in the TotalFlow system. If the specified name is not correct or the TotalFlow system is not available to accept the redirected print job and the job cannot be redirected to TotalFlow, the job will be processed as if the rule was not applied, and it will be recorded in the system log. The delegation server does not resend the job to TotalFlow at a later time. See the TotalFlow documentation for the configuration of a workflow compatible with RICOH Streamline NX. **Important** • **To integrate TotalFlow system, the TotalFlow URL must be specified in System ▶ External Print Systems. For details, see page 574 "External Print Systems".**

Action category	Action	Description
	Deny	This is the second highest priority action during routing. The print job is deleted without being held or printed.
	Hold	This is the third highest priority action during Routing. The print job should be printed later.
	Redirect to Printer	This is the fourth highest priority action during routing. This redirects print jobs to a specified print queue. The redirect results are specified using [Set Priority to] for the priority within the queue of the print jobs spooled in the printer of the redirect destination.
	Allow	This is the lowest priority action during routing. This allows the printing process in the current queue. Secure print jobs are held. All other print jobs are printed immediately.
Modify	Force B&W	Color print jobs are forcibly printed in black and white. This does not apply to print jobs from the RPCS driver.
	Force 2 Sided	Print jobs are forcibly printed on two sides.
	Do not Allow Release	[Do not Allow Release] is enabled only when a secure print job is printed. When the job is not allowed to be released, an error message will appear on the operation panel of the device, and the job is not released. The job is not deleted from the server until the job storage period configured by the administrator elapses, so it may be released if the print rule is changed.

Action category	Action	Description
Notify	Show Pop Up Message	A pop-up notification appears after a rule is applied. If print rules are triggered at the time of job submission from RICOH Streamline NX PC Client, the notification appears on the screen of RICOH Streamline NX PC Client. The notification does not appear on the operation panel of the device. You can add metadata to the notification details. For details, see page 206 "Including metadata in pop up message".
	Send Email	This sends an e-mail to the user after a rule is applied. If the user's e-mail address is not registered or the job is sent from RICOH Streamline NX PC Client, an e-mail is not sent. Enter the subject and main body of the e-mail. You can add metadata to the subject and main body of the e-mail. For details, see page 207 "Including metadata in e-mail messages".

Including metadata in pop up message

Metadata can be added to pop-up notifications that appear when a notification action is applied.

When the metadata tags to be added are described in the main body of the notification, those tags are replaced with metadata in the actual notification.

Specification example:

$[jobName]$ exceeds $[jobDataSize]$ and has been deleted.

Your balance is too low. This job will be printed with $[jobSides]$ and $[jobColorMode]$.

Use the following procedure to describe metadata tags in the notification main body.

1. **On the [Action] tab under [Notify], select the [Show Pop Up Message] check box.**
2. **Click (Add).**
3. **On the [Notify] screen, select the notification language from the drop-down list.**
4. **Enter the notification in [Body].**
5. **In [Body], right-click at the location to enter a metadata tag.**

6. **On the [Select Field Variable(s)] screen, select the metadata tag to be inserted.**

Display Name	Tag	Description
Copies	JobCopies	The number of print copies after the print rules are applied
Number of Pages	JobPages	The number of pages after the print rules are applied
Total Pages	JobTotalPages	The number of total pages (number of pages × copies) after the print rules are applied
Data Size	JobDataSize	The data size of the print job after the print rules are applied
Color Mode	JobColorMode	The color mode (Color or B&W) after the print rules are applied
1 Sided/2 Sided	JobSides	The print sides (2 Sided or 1 Sided) after the print rules are applied
Job Name	JobName	Name of the job
PDL	JobPDL	Job PDL (RPCS, PCL, PostScript, etc.)
User Name	UserName	Name of the user
Printer	QueueName	Name of the print queue before print rules are applied
Routing	Route	These are the redirect results after the print rules are applied. This is the name of the routing action (Allow, Deny, Hold) or the name of the print queue at the redirect destination.

7. **Click [OK] when the settings are complete.**

Including metadata in e-mail messages

Metadata can be added to the subject and body of the e-mail message that is sent when a notification action is applied.

When the metadata tags to be added are described in the subject or main body of the e-mail message, those tags are replaced with metadata in the actual notification.

Use the following procedure to describe metadata tags in the notification main body.

1. **On the [Action] tab under [Notify], select the [Send Email] check box.**
2. **Enter the subject in [Subject].**
3. **In [Subject], right-click at the location to enter a metadata tag.**
4. **On the [Select Field Variable(s)] screen, select the metadata tag to be inserted.**

Display Name	Tag	Description
Copies	JobCopies	The number of print copies after the print rules are applied
Number of Pages	JobPages	The number of pages after the print rules are applied
Total Pages	JobTotalPages	The number of total pages (number of pages × copies) after the print rules are applied
Data Size	JobDataSize	The data size of the print job after the print rules are applied
Color Mode	JobColorMode	The color mode (Color or B&W) after the print rules are applied
1 Sided/2 Sided	JobSides	The print sides (2 Sided or 1 Sided) after the print rules are applied
Job Name	JobName	Name of the job
PDL	JobPDL	Job PDL (RPCS, PCL, PostScript, etc.)
User Name	UserName	Name of the user
Printer	QueueName	Name of the print queue before print rules are applied
Routing	Route	These are the redirect results after the print rules are applied. This is the name of the routing action (Allow, Deny, or Hold) or the name of the print queue at the redirect destination.

5. **Enter the subject in [Body].**
6. **In [Body], right-click at the location to enter a metadata tag.**
7. **On the [Select Field Variable(s)] screen, select the metadata tag to be inserted.**

   For details about the metadata tags that can be inserted, see Step 4.

Note

- The main body of the pop-up notifications is displayed in the same language as the language displayed in RICOH Streamline NX PC Client. If the main body was not added with the same language settings, a notification in English is displayed. If a notification in English has not been added, the notification that is first discovered is displayed.
- The subject and main body of the e-mail notification will be displayed as they are entered on the Management Console and the language is not selectable.
- Any one routing action from among [Allow], [Deny], [Hold], and [Redirect to Printer] can be specified for each rule.
- Routing actions are not applied in the following cases:
  - When a secure print job has been instructed to be released from the operation panel of a device or mobile device
  - When a print job has already been redirected
  - When a print job specifying a delegation user is sent using RICOH Streamline NX PC Client
  - When a guest print job has been sent using HotSpot Enterprise, MyPrint, or some other third party web/email to print solution.
- When multiple rules including routing actions are applied, only the routing action with the highest priority in the above table is performed.
- When the routing action is [Redirect to Printer], specify part of the printer name as the redirect destination. The printer name is not case sensitive. Use the test function to check the redirect result and the printer to which the job was sent. For details about the test function, see page 209 "Testing the Print Rules".
- When multiple rules that include the [Redirect to Printer] action is applied, an action with the highest priority among those specified in [Set Priority to] is used.
- For notification actions, all pop-up notifications are displayed and all e-mails are sent only for the number of rules applied.
- Confirmation pop-up notifications do not appear on a client computer when a print job is sent from a computer that does not have RICOH Streamline NX PC Client installed.
- If the Delegation Server cannot connect to RICOH Streamline NX PC Client due to a network error even when a print job is sent from a computer that has RICOH Streamline NX PC Client installed, pop-up notifications are not displayed and the rules are applied without confirmation.
- A print job that was not redirected is deleted, and a pop-up error notification is displayed on the screen of RICOH Streamline NX PC Client.

Testing the Print Rules

Test the print rule that has been created.

Testing print rules can be performed for a single print rule or all print rules together.

1. **Click the following item in the navigation tree to open the [Print Rules] tab.**

   [Workflow] ▶ [Print Rules]

2. **Select the print rule you want to test.**

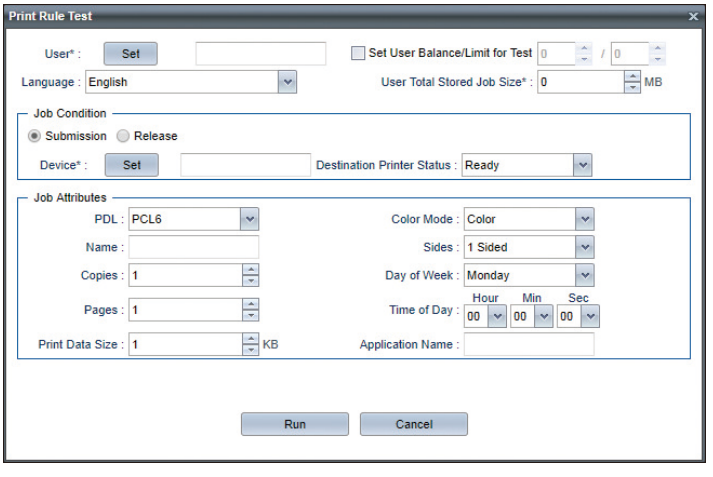
   Testing a specific print rule

   1. From the print rule list, select the print rule you want to test.
   2. Click [Test] on the [General] tab.

   Testing all print rules

   1. Click ▶ (Test) on the print rule list.

3. **On the [Print Rule Test] window, specify the conditions to be used in the test.**



Setting Item	Description
User	Click [Set], and select a user or guest user registered in User Management, and click [OK].
Set User Balance/Limit for Test	Specify whether or not to disable the user accounting data during testing. When this is disabled, the disabled balance and limit can be set. When this is not disabled, the current accounting data of the specified user is used.
User Total Stored Job Size	Specify the total size of user stored jobs.

Setting Item	Description
Language	Select the display language of pop-up notifications.
Job Condition	Specify whether to submit or release the print job. When [Submission] is selected, click [Set] and select the target device from the list or select [Secure Print Queue]. To run a test with the current device status disabled, select [Destination Printer Status], and select the device to be used during the test from the drop-down list. If the current device status is not disabled, the test runs with the current device status.
Job Attributes	Specify the job attributes. You can specify the following attributes: • PDL (PCL6, PCL5, PS, RPCS, Unknown) • Name (max. 255 characters) • Copies • Pages • Print Data Size • Color Mode (Color, B&W, Unknown) • Sides (1 Sided, 2 Sided, Unknown) • Day of Week (Monday to Sunday, Unknown) • Time of Day (hours, minutes, seconds)

4. **Click [Run].**

   A test of the print rules with the specified conditions is performed.

   When the test is completed, test results appear on the screen, and the applied rules and actions appear in the list.

Changing a Print Rule

Use the following procedure to change a created print rule:

1. **Click the following item in the navigation tree to open the [Print Rules] tab.**

   [Workflow] ▶ [Print Rules]

2. **In the print rule list, select the print rule you want to change.**

3. **Change the settings.**

   For the configuration procedure, see page 200 "Creating Print Rules".

4. **Click (Save).**

Deleting a Print Rule

1. **Click the following item in the navigation tree to open the [Print Rules] tab.**

   [Workflow] ▶ [Print Rules]

2. **In the print rule list, select the print rule you want to delete, and click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Adding a Printer

To use the secure printing and direct printing functions of RICOH Streamline NX, configure the printer on the Delegation Server and client computer.

Perform the following operations according to the printing function that you will use.

- Server Secure Printing

  Register a device with a configured SLNX Secure Print Port to a Delegation Server, and copy and register the shared printer to the client computer.

- Server Direct Printing

  Register a device with a configured Standard TCP/IP port to a Delegation Server, and copy and register the shared printer to the client computer.

- Client Secure Printing/Client Direct Printing

  Install RICOH Streamline NX PC Client on a client computer, and register a printer to the client computer.

- Device Direct Printing/Printing without using RICOH Streamline NX

  Use the Driver Distribution function to download the printer driver of a device, and install it to the client computer.

Note

- For details about registering a printer to a Delegation Server, see page 215 "Defining a Shared Printer on a Delegation Server".
- For details about registering a shared printer to a client computer, see “Printing“, User's Guide.
- For details about installing RICOH Streamline NX PC Client, see “Installing RICOH Streamline NX PC Client“, Installation Guide.
- For details about the Driver Distribution function, see page 133 "Distributing Printer Drivers".

Supported Devices

The printers shown below support the printing functions of Streamline NX as follows:

Device	Supported Functions
RICOH device (with Device Applications installed)	Secure printing, direct printing
RICOH device (without Device Applications installed)	Secure printing*1, direct printing
Non-RICOH device	Secure printing*1, direct printing

Device	Supported Functions
USB-connected device	Direct printing*2

*1 Requires a mobile device with the RICOH Streamline NX mobile app installed.

*2 Requires RICOH Streamline NX PC Client.

Note

- Add a name starting with "Other" to the printer name of non-Ricoh devices. (Example: Other non-Ricoh Printer)
- The print rules are not applied if the name of the printer that starts with "Other". When the printer driver name does not start with "Other", the device is treated as a Ricoh printer and print rules are applied even if it is a non-Ricoh device, but the print results cannot be guaranteed.

Device types and available functions

RICOH devices types and available functions are as follows: For details see “Printing“, User's Guide.

✓: Available

-: Not available

Function	MFP not equipped with 4.3-inch screen	MFP with 4.3-inch screen	Laser printer with 4.3-inch screen	Laser printer not equipped with 4.3-inch screen
Checking, printing, and deleting the print document on the print document list screen	✓	✓	✓	✓*
Directly printing from a device	✓	✓	✓	✓
Printing after changing the printing preferences	✓	-	-	-
Printing a document as delegate user	✓	✓	✓	-

* When a user logs in, all secure print documents of the login user are printed. You cannot check or delete a document without displaying the print document list screen.

Supported Printer Drivers

The following printer drivers are supported:

Delegation Server

While you can install a printer driver specific to each Ricoh model, the recommended print driver is the RICOH Universal Print Driver, which supports current devices. RICOH Universal Print Driver supports PCL and PS language, and these are provided as individual printer drivers. These drivers can be shared on models that support PCL or PS language.

Client Computer

- PCL 6 Driver for Universal Print
- PCL 6
- PCL 5
- PS Driver for Universal Print
- PS
- PS for Mac OS X*1
- LAN fax driver*2

*1 Mac OS X 10.9 or later

*2 Direct printing only. Print rules do not apply.

Defining a Shared Printer on a Delegation Server

Install the printer driver of the device to be used for printing on the Delegation Server, and configure the port and authentication.

This section describes how to install the RICOH Universal Print Driver and add a shared printer.

Important

- **To print from a client computer with 32-bit Windows installed, install the printer driver for a 32-bit operating system.**

Note

- This section describes how to use Internet Explorer to download and install the RICOH Universal Print Driver on Windows Server 2012. The procedure varies depending on web browsers, operating systems, and printer drivers used.
- Depending on the operating system you are using, you may have to log in with administrative privileges and execute the Add Printer Wizard.
- After installing the printer driver, select [Control Panel] ▶ [Devices and Printers], and then select the RICOH driver that you have installed to specify the installed printer as the default printer.
- For printing using the RICOH Universal Print Driver, see “Printing“, User's Guide.

Downloading the RICOH Universal Print Driver

Before installing the printer driver on a Delegation Server, download the printer driver to the Delegation Server. Use the following procedure to download the RICOH Universal Print Driver:

Important

- **Be sure to download the printer driver to the Delegation Server, not the client computer.**

1. **From the Delegation Server, go to http://support.ricoh.com/bb/html/dr_ut_e/rc3/model/p_i/p_i.htm.**
2. **Click [Download] under [PCL6 Driver for Universal Print] or [PS Driver for Universal Print].**
3. **Click [Run].**
4. **Open the download destination folder, and click [Unzip].**

   When a message is displayed indicating that extraction was successful, click [OK].

Adding a printer and configuring an SLNX Secure Print Port

To use the secure printing function, add a device with a configured SLNX Secure Print Port as a shared printer.

Note

- When installing the printer driver to a non-Ricoh device, enter "Other" in front of the printer name in Step 10.

1. **Open [Devices and Printers].**
2. **Click [Add a printer].**

   Note

   - To cancel searching for a device, click [Cancel].
3. **Click [The printer that I want isn't listed].**
4. **Select [Add a local printer or network printer with manual settings], and click [Next].**
5. **Select [SLNX Secure Print Port] in the [Use an existing port] drop-down list, and click [Next].**
6. **Select [RICOH] in the [Manufacturer] list, and click [Have Disk].**
7. **Click [Browse], navigate to the folder where the RICOH Universal Print Driver can be downloaded, and open the driver file.**
8. **Click [OK].**
9. **Select the printer driver to use, and click [Next].**
10. **Enter the printer name, and click [Next].**

11. **Select [Share this printer so that anyone on your network can find and use it], enter the [Share name], [Location], and [Comment], and click [Next].**
12. **Click [Finish].**

    The printer with the SLNX Secure Print Port configured is added to the list of printers.

Adding a printer and configuring a Standard TCP/IP Port

To use the direct printing functions, add a device with a configured Standard TCP/IP Port as a shared printer.

Note

- When installing the printer driver to a non-Ricoh device, enter "Other" in front of the printer name in Step 13.

1. **Open [Devices and Printers].**
2. **Click [Add a printer].**

   Note

   - To cancel searching for a device, click [Cancel].
3. **Click [The printer that I want isn't listed].**
4. **Select [Add a local printer or network printer with manual settings], and click [Next].**
5. **Select [Standard TCP/IP Port] in the [Create a new port] drop-down list, and click [Next].**
6. **Enter the printer name or IP address of the device, and click [Next].**
7. **Searching of a TCP/IP port starts.**
8. **Check that a correct port has been detected, and then click [Finish].**
9. **On the [Install the printer driver] screen, click [Have Disk].**
10. **Click [Browse], navigate to the folder where the RICOH Universal Print Driver can be downloaded, and open the driver file.**
11. **Click [OK].**
12. **Select the printer driver to use, and click [Next].**
13. **Enter the printer name, and click [Next].**
14. **Select [Share this printer so that anyone on your network can find and use it], enter the [Share name], [Location], and [Comment], and click [Next].**
15. **Click [Finish].**

    The printer with the Standard TCP/IP Port configured is added to the list of printers.

Shared printer authentication settings

The authentication information must be configured on the device registered to the client computer in the following cases:

- When the LDAP and Active Directory servers to be used for user authentication differ on the client computer and in RICOH Streamline NX.
- When the client computer has identified the user as a Windows local user.

To configure authentication information on a shared printer registered to the client computer, configure the following using the RICOH Universal Print Driver:

1. **Click [Start] and [Devices and Printers].**
2. **Right-click the printer icon of the shared printer, and select [Printer properties].**
3. **Select the [User authentication] check box on the [Preferences] tab.**
4. **Click [OK].**

6. Managing Document Delivery Functions

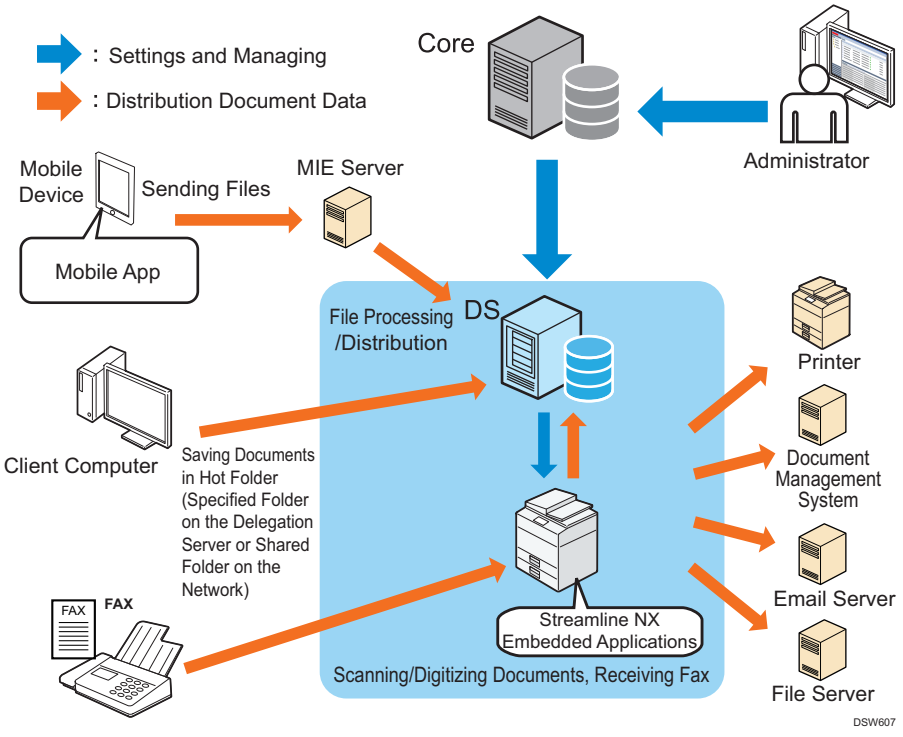
This section describes the settings for delivering a document scanned with a device using the delivery function of RICOH Streamline NX

Overview of the Delivery Function

The RICOH Streamline NX delivery function can process documents scanned using a device, incoming faxes, images sent from a mobile device, and images placed into a monitor folder, and distribute them to various destinations such as e-mails, network folders, printers, and file servers. Such documents can also be stored in a shared folder on the network or a folder on an FTP or WebDAV server.

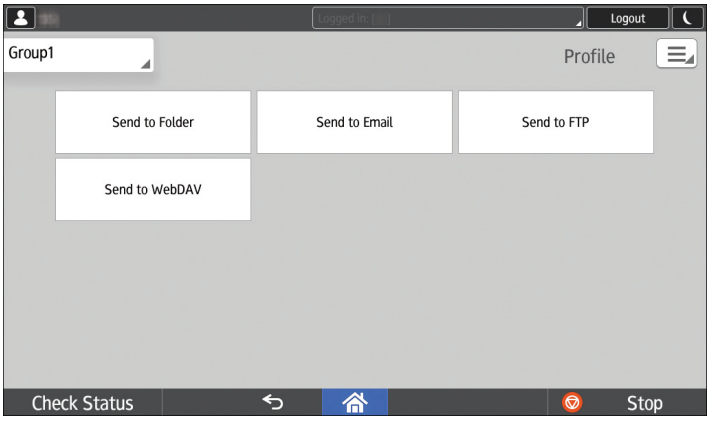
The administrator can use the Management Console to configure the job processing flow from scanning to delivery in advance according to business details and objectives. Users can then use the workflows to convert documents easily and correctly to electronic format and deliver them.

In the RICOH Streamline NX delivery function, documents are processed and delivered by a Delegation Server or a device.

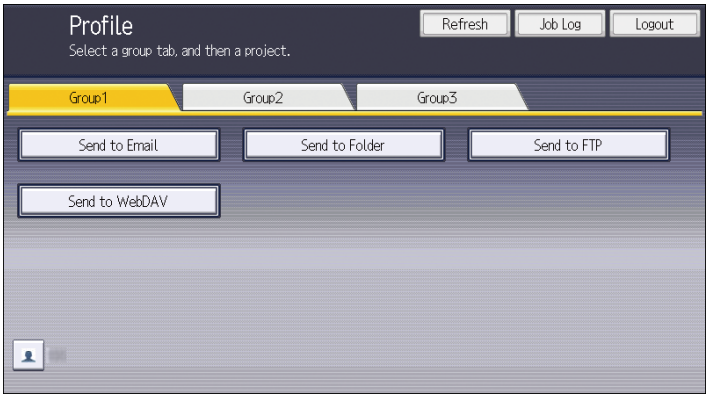


Workflows configured in the Management Console are displayed as buttons on the screen of the device connected to the Delegation Server. Simply press the desired workflow button to start the delivery process.

Workflow Menu (when using Smart Operation Panel)



Workflow Menu (when using the Standard Operation Panel)



Note

- To monitor a specified folder (Monitor Folder) on a Delegation Server or network and automatically import and deliver stored files, the license for Scan & Capture Input Connector must be purchased and activated. For details, see page 26 "List of Licenses and Functions".
- For details about delivering images from a mobile device, see page 371 "Using RICOH Streamline NX on a Mobile Device".
- Configure the days of the week and time periods that the delivery function is enabled for. For details, see "[Capture] tab" in page 629 "Server Group".

Overview of the Delivery Settings

To use the RICOH Streamline NX delivery function, perform the following in the Management Console:

1. **Create a workflow (page 227 "Creating a Workflow")**

   A workflow defines how a document is scanned, processed and delivered, and consists of one or more destination and process connectors.

   Delivery destinations can be specified by selecting and placing destination connectors. Process connectors enable users to convert data format, replace metadata information, decide subsequent delivery flow based on the specified rules, etc. For the types of destination connectors and process connectors available in RICOH Streamline NX, see page 222 "Available Destination Connectors" and page 224 "Available Process Connectors".

   The administrator combines destination connectors and process connectors and configures the properties of each connector to create the delivery flow.

   In workflows where the One-touch Scan function is configured and all parameters required for delivery are preset, the user can start the scan and delivery process simply by pressing [Start] (one-touch scan function) without entering anything on the device.

2. **Configure the workflow profile (page 321 "Configuring a Workflow Profile by Input Source")**

   The following three types of documents (files) can be processed in a workflow:

   - Documents scanned using a device with the Streamline NX Embedded Applications installed or received fax documents
   - Files sent from a mobile device with the Streamline NX Embedded Applications installed
   - Documents scanned from Monitor Folder (specified folder on a Delegation Server or a shared folder on a network)

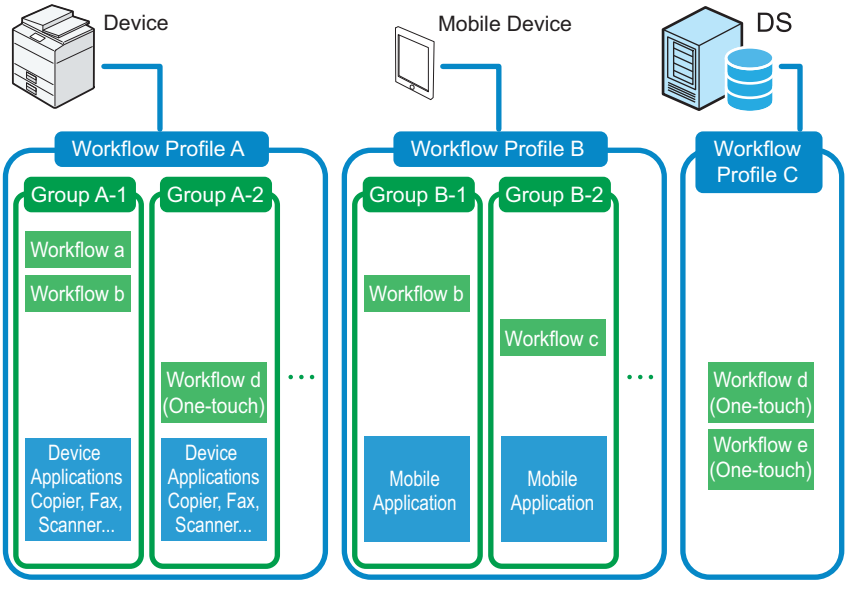
   For a preset workflow, use a workflow profile to configure the documents for processing.

   Create a group to add a workflow to a workflow profile associated with a device or mobile device. You cannot add a workflow that does not belong to a group.

   Groups are useful for organizing workflows within a profile by application. When workflows related to operations are divided by groups and configured in a profile, a user can quickly access the target workflow simply by selecting a group. Select a group from the group list on the Smart Operation Panel or from the Groups tab on the Standard Operation Panel.

3. **Synchronize the settings with devices and Delegation Servers (page 329 "Configuring a Profile Task")**

   Configure the schedule for syncing the workflow profile with a device or Delegation Server as a profile task. You can also perform syncing immediately.



Note

- In addition to a workflow, you can also add copy, scan, and other Device Applications to a workflow profile associated with a device.
- In addition to a workflow, you can also add print-related applications to a workflow profile associated with a mobile device.

Available Destination Connectors

The following destination connectors are available: The available connectors vary depending on whether the processing of delivery jobs within a workflow is performed by a server or device.

Destination connector name	Description	Location
Send to Email	Delivers the scanned document to a specified e-mail address destination. For details, see page 240 "Send to Email".	Server or device
Send to Folder	Delivers the scanned document to a shared folder in the network or a local folder on a server. For details, see page 241 "Send to Folder".	Server or device

Destination connector name	Description	Location
Send to FTP	Delivers the scanned document to a folder on an FTP server. For details, see page 242 "Send to FTP".	Server or device
Send to Printer	Prints the scanned document from a printer with a Delegation Server configured. For details, see page 243 "Send to Printer".	Server
Send to WebDAV	Delivers the scanned document to a folder on a WebDAV server. For details, see page 243 "Send to WebDAV".	Server or device
Send to SharePoint	Delivers the scanned document to a folder on Microsoft Office SharePoint Server, Office 365, or SharePoint Online. For details, see page 245 "Send to SharePoint".	Server or device
Send to CMIS	Delivers the scanned document to CMIS repository. For details, see page 247 "Send to CMIS".	Server
Send to DocumentMall	Delivers the scanned document to Ricoh DocumentMall Content Management System. For details, see page 248 "Send to DocumentMall".	Server or device
Send to Exchange (EWS)	Delivers the scanned document by MS Exchange e-mail using Exchange Web Service. For details, see page 249 "Send to Exchange (EWS)".	Server
Send to RightFax	Sends the scanned document by fax or e-mail via a RightFax server. For details, see page 250 "Send to RightFax".	Server
Send to Gmail	Delivers the scanned document to a Gmail account. For details, see page 251 "Send to Gmail".	Server

Destination connector name	Description	Location
Send to Google Drive	Delivers the scanned document to Google Drive. For details, see page 253 "Send to Google Drive".	Server
Send to Dropbox	Delivers the scanned document to Dropbox. For details, see page 254 "Send to Dropbox".	Server

Available Process Connectors

The following process connectors are available: The available connectors vary depending on whether the processing of delivery jobs within a workflow is performed by a server or device.

Process connector name	Description	Location
PDF Converter	Converts the scanned document to PDF. For details, see page 261 "PDF Converter".	Server or device
Image Converter	Converts the scanned document data to a different file format depending on the administrator settings, and converts images to the image format specified on the operation screen on the device. For details, see page 264 "Image Converter".	Server or device
Archiver	Converts the scanned document into a .zip or .tgz format archive (compressed) file. For details, see page 270 "Archiver".	Server
OCR	Recognizes the characters in the scanned document and extracts them as text, and converts the data to docx, xml, or other file formats*1. It also identifies the top and bottom of the document and adds a file name based on the text extracted from the first page of the scanned document. For details, see page 271 "OCR".	Server

Process connector name	Description	Location
Section Specify *2	Extracts a section you need from the document and passes only that extracted section to the next destination connector in the delivery flow. The sections not extracted are deleted. For details, see page 272 "Section Specify".	Server
Section Division*2	Divides a job by separating document data that consists of multiple sections by the number of sections specified on the operation screen of the device. For details, see page 273 "Section Splitter".	Server or device
XML Stylesheet Converter	Extracts the scanned document metadata as XML data and converts it to another format (HTML, CSV, etc.) using a specified XSL file (XML stylesheet). For details, see page 276 "XML Transformer".	Server or device
Metadata Converter	Converts the specified metadata element values of the scanned document. This connector can also be used to change the values of metadata elements to different values of metadata elements based on the rules specified in the replacement table. For details, see page 276 "Metadata Converter".	Server or device
Metadata Replacement	Validates a specified value in the metadata elements of the scanned document and changes a specific part of the value using a regular expression. For details, see page 277 "Metadata Replacement".	Server
Image Correction	Corrects images of the scanned document to improve image quality. For details, see page 279 "Image Correction".	Server
Barcode Division/ Recognition*3	Analyzes a barcode included in the scanned document and saves it as metadata. For details, see page 281 "Barcode Separator/ Index".	Server

Process connector name	Description	Location
Zone OCR*3	Recognizes the characters in a specified area of the scanned document and extracts them as text. For details, see page 288 "Zone OCR".	Server
PDF Stamper	You can create a PDF with specific embedded text or image in the scanned document. For details, see page 289 "PDF Stamper".	Server
Decision Point	Changes the processing following the workflow according to preset rules. For details, see page 291 "Decision Point".	Server or device

*1 When the login language is Japanese, the output file format is the same as the input file format.

*2 A section is a file of a document scanned with a device, and it contains one or more pages. For example, when a five-page document is scanned in single-page TIFF file format, it is delivered in five one-page sections. Similarly, when a five-page document is scanned in multiple-page TIFF file format, it is delivered in one five-page section. In addition, when the process connector is used to convert multiple file formats, an individual section is created for each file format.

*3 Purchase of a license and activation are required to use this process connector. For details about activation, see “Activating RICOH Streamline NX”, Installation Guide.

Note

- For details about metadata, see page 348 "Metadata".

Confirming the Usable Connectors

Use the following procedure to view the list of usable connectors:

1. **Click the following items in the navigation tree to open the [Connectors] tab.**

   [Workflow] ▶ [Connectors]

2. **Click the [Destination] or [Process] tab.**

   A list of connectors that can be used on the system is displayed.

   To refresh the list, click (Refresh).

   Click a column title to sort in ascending or descending order.

3. **To view the details of a connector, select the connector in the connector list.**

   The connector name, description, job processing location, and version are displayed.

Creating a Workflow

Use the [Workflow Design] tab to create, edit, and delete workflows. This section describes how to configure the settings on the [Workflow Design] tab.

Creating a New Workflow

Use the following procedure to create a new workflow.

Note

- For details about creating a new workflow based on an existing workflow, see page 234 "Creating a New Workflow by Copying an Existing Workflow".

1. **Click the following items in the navigation tree to open the [Workflow Design] tab.**

   [Workflow] ▶ [Workflow Design]

2. **Click (Add).**

   The workflow creation screen is displayed.

3. **In Workflow Name, enter the name of the workflow.**
4. **In [Description], enter the description of the workflow.**
5. **In [Job Processing Location], select [On Server] or [On Device].**

   For details about the job processing location, see "Job Processing Location" below.

6. **Click [OK].**
7. **On the [General] tab, configure the workflow properties.**

   For details about the configuration items, see "[General] tab", page 589 "Workflow Design".

8. **On the [Delivery Flow] tab, position the destination and process connectors, and configure the properties.**

   Depending on the job processing location selected in Step 5, only the usable connectors are displayed.

   For details about adding a destination or process connector to the delivery flow, see page 230 "Understanding the [Delivery Flow] tab layout".

   For details about configuring the properties of a destination or process connector, see page 240 "Configuring the Properties of the Destination Connector" and page 260 "Configuring the Properties of a Process Connector".

9. **On the [Destination] tab, specify the default value of the destination connector and select the display method on the operation screen of the device.**

   For details about the settings, see page 294 "Customizing the Settings on the Operation Screen of the Device".

10. **On the [Process] tab, configure [Scan Settings] and [Scan Size], specify the default value of the process connector, and select the display method on the operation screen of the device.**

    For details about the settings, see page 294 "Customizing the Settings on the Operation Screen of the Device".

11. **On the [Metadata] tab, configure the metadata settings, default value, and layout of the operation screen of the device.**

    For details about the settings, see page 308 "Configuring Items in Metadata".

12. **On the [Notification] tab, specify whether or not to send notifications, and configure the notification conditions, destination, and metadata to be included in the notifications.**

    For details about the settings, see page 315 "Configuring the Notification Function".

13. **On the [Other Settings] tab, configure the default document name and the items displayed on the [Scan Settings] window, and specify whether or not to display the preview window.**

    For details about the settings, see page 316 "Configuring Other Settings".

14. **Click (Save) on the workflow list.**

    If the workflow is not properly configured, clicking (Save) displays an error message indicating the location of the error. Click [OK], and configure the workflow properly.

    If the following conditions are not met, an error occurs in the workflow.

    - At least one destination connector is positioned in the delivery flow.
    - A destination connector, not a process connector, is positioned at the end of the delivery flow. When a process connector is placed at the end of a delivery flow, is displayed.
    - All required setting items are configured. An asterisk (*) is displayed next to the setting name for required entry items.
    - All delivery parameters are configured in the one-touch scan workflow. (page 233 "Configuring one-touch scan")
    - All delivery parameters for connectors positioned after Decision Point are configured. (see page 240 "Configuring the Properties of the Destination Connector" and page 260 "Configuring the Properties of a Process Connector")

15. **Test the operation of the configured workflow.**

    See page 235 "Testing the Workflow".

Job Processing Location

When [Job Processing Location] is set to [On Device], delivery is performed by the device and not by the Delegation Server.

For example, specify how to process a job on a device when:

- When you want to reduce the load on the server
- Communication speed between the device and Delegation Server is slow
- Minimizing use of the network for delivery processing for the sake of security

In addition, workflows processing jobs on a device have the following restrictions:

- [Select Data to Attach] for Send to Email is fixed to [Attach All] and [Select Data to Attach] cannot be used.
- Send to Email does not support High Compression PDF or Searchable PDF.
- Even when a local folder on a Delegation Server is specified as the destination in Send to Folder, it does not function on a device.
- Even when [JIS] is selected as the character code of the file (folder) name in the StartPoint Path setting of Send to Folder, it does not function on a device.
- For [PDF Converter] and [Image Converter] of a process connector, there are fewer supported file formats than when jobs are processed on a server.
- You cannot use [Dropdown ListBox] that uses SQL Search on the Input Metadata screen.

Syncing the settings (changes)

- The created or updated workflow is applied to the device at the execution time according to the type of profile using that workflow.

Note

- For details about the setting items on each tab, see page 589 "Workflow Design".
- Depending on the granted user permission, only some workflows may be available for selection from the device. For details, see page 174 "Managing Permissions".

Using the [Delivery Flow] Tab

On the [Delivery Flow] tab, position the destination and process connectors, and configure the delivery flow and data processing of the scanned document. Add a destination connector to the delivery flow to configure the data delivery method and delivery location. Add a process connector to configure data conversion and change the metadata.

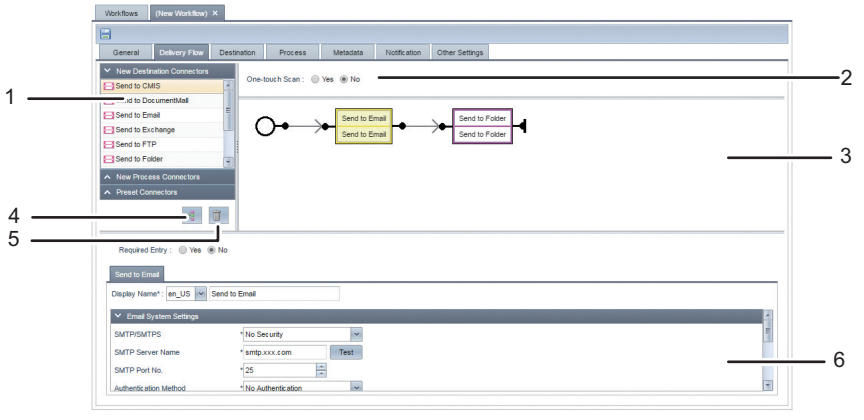
A new destination connector, a new process connector, and a shared connector can be added to the delivery flow.

When the new connector properties are configured on the [Delivery Flow] tab, the settings are applied only to the workflow being configured. The shared connector is a connector with preset properties, and

it enables you to apply the same settings to all workflows. For details about configuring the shared connectors, see page 317 "Creating a Shared Connector".

Understanding the [Delivery Flow] tab layout

The following shows the layout of the [Delivery Flow] tab and describes the functions.



DSW600

1. **Connector List**

   Select from [New Destination Connectors], [New Process Connectors], and [Shared Connectors] for the connector to use. The connectors that are displayed vary depending on the Job Processing Location Setting. For details, see page 222 "Available Destination Connectors" or page 224 "Available Process Connectors".

   Click the (Filters) button and enter filter conditions in the input field to filter the Shared Connectors list.

2. **One-touch Scan**

   To configure the workflow for one-touch scan, select [Yes]. For details about the one-touch scan settings, see page 233 "Configuring one-touch scan".

3. **Delivery flow edit pane**

   Create a delivery flow by dragging and dropping connectors from the [New Destination Connectors], [New Process Connectors], and [Shared Connectors] lists and positioning the connectors in the order of processing. For details, see page 231 "Creating a delivery flow".

4. **(Arrange)**

   This arranges the positioned destination and process connectors to make them easier to see. It also eliminates multiple destination and process connectors overlapping on each other.

5. **(Trash)**

   The connector can be removed from the delivery flow by dragging and dropping a connector from the delivery flow edit pane to the trash can button.

6. **Connector properties window**

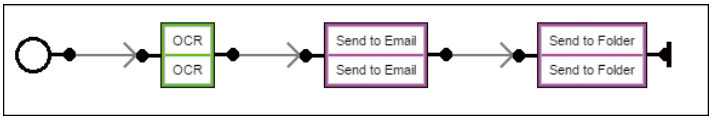
   The window for editing the properties of the selected connector is displayed in the delivery flow edit pane.

Creating a delivery flow

Create a delivery flow with or without redirects.

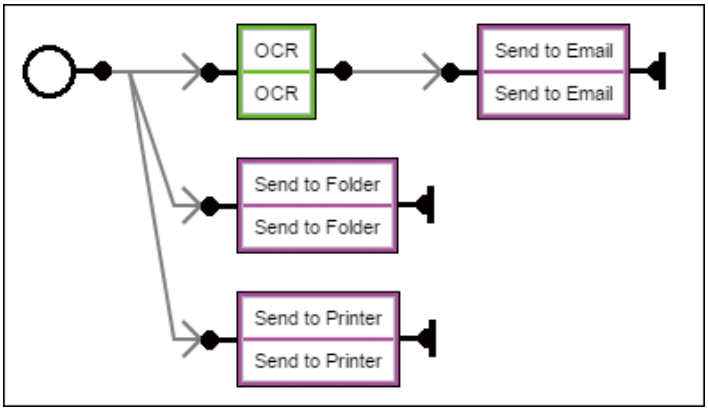
In a delivery flow without redirects, scanned documents are processed in order starting from the destination or process connector on the left side of the flow.

Example of a delivery flow without redirects



In a delivery flow with redirects, the document is processed using the different destination or process connector at each redirect.

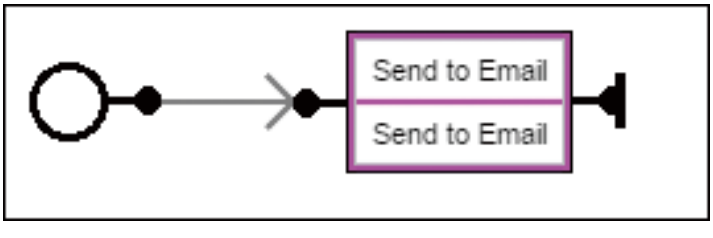
Example of a delivery flow with redirects



To add a destination or process connector to the delivery flow, use the following procedure:

1. **Drag the destination or process connector you want to add to the delivery flow from the connector list, and drop it in an open area in the delivery flow edit pane.**

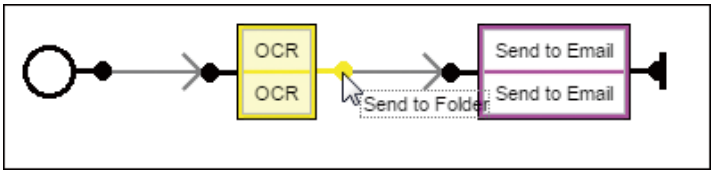
   A new redirect is added to the starting point ( ) of the delivery flow.



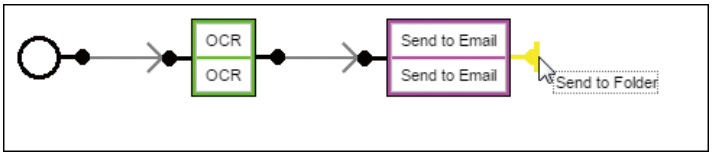
2. **To add another destination or process connector, drag the destination or process connector you want to add from the connector list and drop on the position you require.**

   To add a connector between connectors and at the end of the delivery flow, drop it on the position you require.

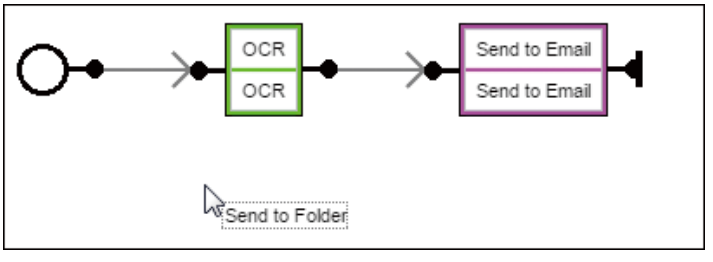
- Adding a connector between connectors



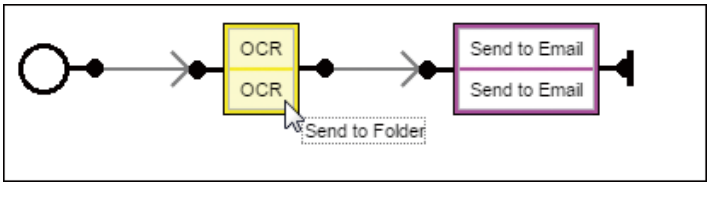
- Adding a connector at the end of the delivery flow



To add a new redirect at the starting point, drop the connector on an open area in the delivery flow edit pane.



To add a new redirect between connectors, drop the connector you want to add on top of the connector right before the start of the redirect.



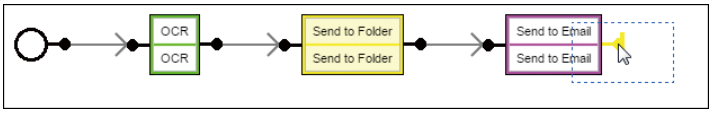
Precautions when positioning shared connectors

You can only add the same shared connector once to the same workflow.

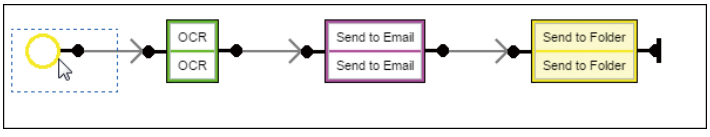
If you try to add it more than once, the message "You cannot use a shared connector multiple times in a workflow. Do you want to make it local to the workflow?" is displayed. When you select [Yes], the shared connector settings are copied, a new connector is created, and the settings can be changed. After you convert a connector to a new connector, the settings are not applied even when changing the original shared connector settings. When you select [No], the shared connector is not added.

Changing connector positions

To change the position of a connector, drag and drop the connector you want to move on top of the connection of the destination connector. To move a connector to the end of the delivery flow, drop it at the end of the delivery flow.



To change the position of a connector and create a new redirect, drag and drop the connector you want to move on top of the starting point or connector at the starting position of a redirect.



Deleting a connector from the delivery flow

1. **Drag and drop the connector to delete from the delivery flow edit pane to (Trash).**

   A connector can be deleted also by selecting it on the delivery flow edit pane and clicking (Trash).

2. **Click [OK] on the confirmation message that is displayed.**

   The connector is deleted.

   The connectors before and after the deleted connector are automatically connected.

Configuring one-touch scan

One-touch scan is a workflow with preset document delivery parameters.

A document can be scanned and delivered using the configured delivery parameters simply by placing the document in the ADF or on the exposure glass and pressing [Start]. The delivery parameter settings, such as the destination or [Scan Settings], cannot be changed on the operation screen of the device.

One-touch scan is useful when scanning and delivering documents with fixed delivery parameter settings. For example, when receipts scanned with the device are saved to the same folder, configure a one-touch scan workflow in which files are saved to a designated folder using a Send to Folder connector.

Use the following procedure to configure a one-touch scan workflow:

1. **At the top of the delivery flow edit pane, select [Yes] in [One-touch Scan].**

   The one-touch scan setting cannot be removed in the following workflows:

   - One-touch scan workflows that are configured for receiving faxes

- One-touch scan workflows that have Scan & Capture Input Connector specified

If you try to remove the one-touch scan settings of any of the above workflows, the message "One-touch Scan cannot be removed because this workflow is used for fax reception." is displayed.

2. **To display the metadata entry screen when scanning a one-touch scan job, select the [Display metadata entry screen] check box.**

   [Display metadata entry screen] is only displayed when [Yes] is selected for [One-touch Scan].

   When this check box is selected and the workflow has configured metadata, the metadata entry screen is displayed while scanning a one-touch scan job.

3. **Configure all required parameters.**

   An asterisk (*) is displayed next to the setting name for required entry items. Specify at least one destination.

   If a required parameter is not configured, a warning message is displayed next to the item or on the tab. When (Warning) is displayed, the setting is not saved.

Creating a New Workflow by Copying an Existing Workflow

Use the following procedure to create a new workflow based on an existing workflow:

1. **Click the following items in the navigation tree to open the [Workflow Design] tab:**

   [Workflow]s ▶ [Workflow Design]

2. **Select the workflow to copy, and then click (Copy).**
3. **Select the copied workflow in the workflow list, and click (Edit).**

   The workflow name is automatically added to the copied workflow with the format "<original-workflow-name>_<date-in-system-setting-format>". You can change the workflow name.

4. **Edit the workflow.**

   For details about the configuration procedure, see page 227 "Creating a New Workflow".

5. **Click (Save) in the workflow list.**

Note

- You cannot change [Job Processing Location] on the [General] tab.

Editing a Workflow

Use the following procedure to edit a created workflow:

1. **Click the following items in the navigation tree to open the [Workflow Design] tab.**

   [Workflow] ▶ [Workflow Design]

2. **Select the workflow to edit, and then click (Edit).**
3. **Edit the workflow.**

   For details about configuring a workflow, see page 227 "Creating a New Workflow".

4. **Click (Save) in the workflow list.**

Note

- You cannot change [Job Processing Location] on the [General] tab.

Deleting a Workflow

Use the following procedure to delete an existing workflow:

1. **Click the following items in the navigation tree to open the [Workflow Design] tab.**

   [Workflow] ▶ [Workflow Design]

2. **Select the workflow to delete, and then click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- A workflow being used in a workflow profile in a higher hierarchy cannot be deleted. In [Profile] displayed at the bottom of the window, remove the workflow from the corresponding profile, and then delete the workflow.

Testing the Workflow

The operation of the created workflow can be tested using a specific Delegation Server or all Delegation Servers.

Important

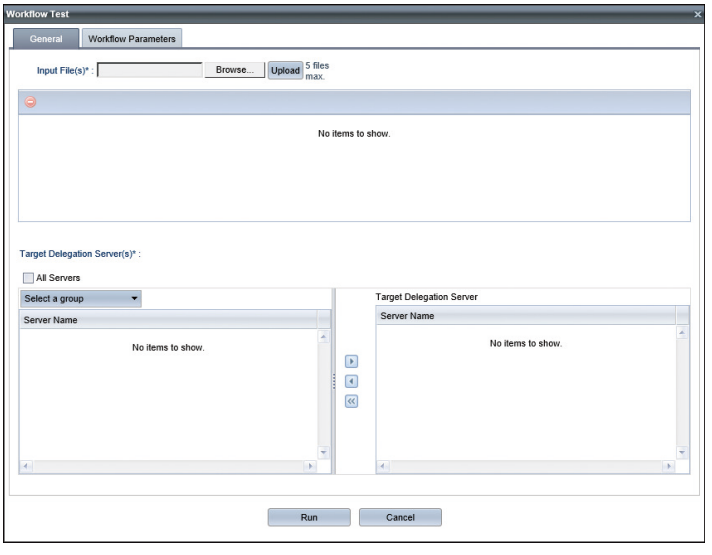
- **A workflow other than one-touch scan cannot be validated when the following conditions are satisfied:**
  - **The workflow contains a Send to CMIS connector that is "Required".**
  - **The workflow contains a destination connector that is only Send to CMIS.**
- **On the [Workflow Test] screen, you can only test a workflow whose [Job Processing Location] setting is set to [On Server].**

Use the following procedure to test the operation of the configured workflow:

1. **Click the following items in the navigation tree to open the [Workflow Design] tab.**

[Workflow] ▶ [Workflow Design]

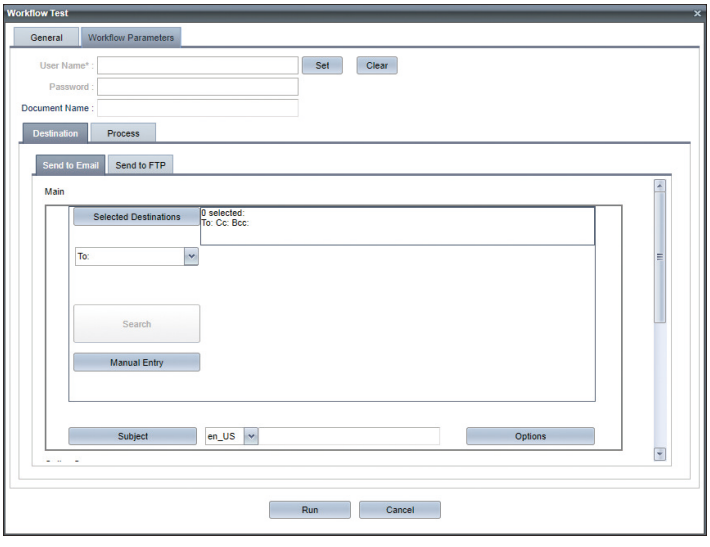
2. **Select the workflow to test in the workflow list, and click ▶ (Test).**
3. **On the [General] tab, upload the file to use in the test delivery, and configure the Delegation Server to be used.**



Setting item	Description
Input File(s)	Click [Browse], select the file to deliver, and then click [Upload]. **Note** • You can upload files with a BMP, GIF, JPEG, JPG, PDF, TIF, or TIFF extension. In addition, all files to be uploaded must have the same extension. • Each file to be uploaded must be less than 1 MB in size. • You can upload up to five files.
Target Delegation Server(s)	Specify the Delegation Server to use for test delivery. To test all Delegation Servers, select the [All Servers] check box. To test a specific Delegation Server, select the Delegation Server to use and click ▶ to add it to the [Target Delegation Server] list. Clicking ◀ removes the selected Delegation Server from the [Target Delegation Server] list, and clicking ◀◀ removes all Delegation Servers from the list.

4. On the [Workflow Parameters] tab, specify the user executing the workflow, destination connectors, process connectors, and metadata.

In the Management Console, configure the actual items to be configured by the user on the operation screen of the device.



Setting item	Description
User Name	Specify the user executing the workflow. Click [Set] to open the [Select User] window. Select a user registered in [User Management], and click [OK].
Document Name	Enter the document name to be used for test delivery. This item is not available when editing of the document name is disabled in the workflow settings. If the document name is not specified, the time stamp (local time of the Delegation Server) at the time of execution is set as the document name.

Setting item	Description
Destination/Process/Metadata	Configure the parameters for the destination connectors, process connectors, and metadata to be included in the selected workflow. These items are displayed only when there are items that can be configured on the operation screen of the device. **Note** • When a workflow is configured for one-touch scan, the [Destination] and [Process] tabs are not available. • When a workflow is configured for one-touch scan and editing of metadata is disabled, the [Metadata] tab is not available. • Even if you configure CSV Search or SQL Search on the [Metadata] tab, these functions are not available in the workflow test. Enter the metadata you want to use for the test manually. • For details about the settings, see page 691 "Setting Items in the Destination Connector Properties" and page 747 "Setting Items in the Process Connector Properties".

5. **Click the [General] tab, and then click [Run].**

   The workflow test starts.

6. **When a confirmation message is displayed indicating that the test was successful, click [Yes].**

   On the [Workflow Test Result] tab, check the test log and test result.

   When you select a Delegation Server to check a job log with the [Delegation Server] drop-down menu, the job log list is displayed.

   Click the column title of the log list to sort the list in ascending or descending order.

   When you select a job log to check for details from the log list, a detailed job log is displayed in [Detail Log] at the bottom of the screen.

   Click the column title of the Detail Log to sort the list in ascending or descending order.

   Note

   • If a required parameter is not configured in the workflow test, a warning message is displayed. When (Warning) is displayed, the test cannot be performed until the required settings are specified.

- When you perform a workflow test, the test job is processed using a thread that is different from a normal job, and the processing capacity of the Delegation Server can be affected during a workflow test that requires a workflow with a large load or synchronized processing.
- Retries and other job processing are performed as configured in the same manner as a normal job even for a workflow test.

Configuring the Properties of the Destination Connector

To use the destination connector located in the delivery flow, configure the properties of the connector.

Select the destination connector to configure on the [Delivery Flow] tab on the [Workflow Design] tab to display the destination connector properties window.

The settings are verified when the user moves to another tab after making changes to the properties. The settings with errors are indicated by and cannot be saved until the errors are resolved.

[Required] settings

When [Yes] is selected for [Required] on the properties window, at least one delivery destination (address, folder, printer, etc.) according to the destination connector type must be specified or the delivery flow cannot continue.

[Display Name] setting

The display name of a destination connector can be specified for each language allowed on the RICOH Streamline NX system, and can be switched automatically according to the log-in language to the device.

Select a language from the drop-down menu, and then enter the display name.

Send to Email

The Send to Email connector sends the scanned document by e-mail.

The Send to Email connector settings are divided into the following three screens. Use the accordion icons to display each tabs.

- [Email System Settings]

  Configure the SMTP server.

- [Send to Email Option Settings]

  Configure the sender e-mail address, file naming convention, and e-mail text.

- [Email Search Settings]

  Configure the LDAP server to enable the user to search the LDAP server address book.

  Use the following procedure to configure the properties of the Send to Email connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Email] connector icon.**
2. **On the [Send to Email]tab, enter the display name in [Display Name].**
3. **In [Email System Settings], configure the SMTP server.**

4. **In [Send to Email Option Settings], specify the sender e-mail address, file naming rules, e-mail body, etc.**
5. **In [Email Search Settings], configure the LDAP server.**

Note

- For the setting items on the [Send to Email] tab, see page 691 "Send to Email".

Send to Folder

The Send to Folder connector saves the scanned document in a selected folder on the network.

Send to Folder has the following two functions:

- [Send to Folder]
  Saves documents in a shared network folder.
- [Send to Home Folder]
  Saves documents in the [User Home Folder] using the home folder setting obtained from the Delegation Server.

Authentication

The Send to Folder connector supports both NTLMv2 and Kerberos as the authentication method. For details about selecting the authentication method, see page 539 "Delegation Server Settings".

The Send to Folder connector settings are divided into the following two tabs. Use the accordion icons to display each settings window.

- [Add/Delete StartPoint Path]

  Add, edit, or delete a start point path (root folder).

- [Send to Home Folder]

  Specify whether to enable or disable Send to Home Folder. When Send to Home Folder is enabled, also configure the related settings.

  This function is available only when LDAP/Kerberos authentication is used as the authentication method for the workflow. When the other authentication method is used, this function does not work even if it is selected.

Note

- The following shared folders can be configured as delivery destinations:
  - A shared folder on a computer running under Windows
  - Unix operating system running Samba that supports NTLMv2
  - Local folder on a server
- The attribute of the home folder must be "homeDirectory".

- When LDAP/Kerberos is used as the authentication method for the workflow, the proxy user information specified for the authentication profile, not the login information of the user, is used when accessing folders and delivering documents.
- When LDAP/Kerberos is used as the authentication method for the workflow, the leading element of the proxy user's DN is used when accessing folders.

Use the following procedure to configure the properties of the Send to Folder connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Folder] connector icon.**
2. **On the [Send to Folder] tab, enter the display name in [Display Name].**
3. **Under [Add/Delete StartPoint Path], click [Add].**

   To delete a start point path, select the path to delete in the list, and click [Delete].
4. **On the Add or Delete Start Point Path window, add or edit a start point path, and click [OK].**
5. **To use Send to Home Folder, select [Enable Send to Home Folder] in [Send to Home Folder]. When Send to Home Folder is enabled, also configure the related settings.**

   You can configure the same settings as for the start point path such as subfolder browsing and the file naming rule for the Home Folder.

Note

- For the setting items on the [Send to Folder] tab, see page 698 "Send to Folder".

Send to FTP

The Send to FTP connector uploads the scanned document to more than one specified FTP server.

Note

- SFTP (SSH2) is supported.
- FTPS (FTP over SSL/TLS) is not supported.
- The active mode is supported as the FTP connection method.
- A file name is added to the scanned document in accordance with the configured naming convention. See page 255 "File and Folder Naming Conventions".
- For details about establishing a secure connection with Send to FTP using a private key, see page 403 "Enabling SSL".

Use the following procedure to configure the properties of the Send to FTP connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to FTP] connector icon.**
2. **On the [Send to FTP] tab, enter the display name in [Display Name].**

3. **Under [Add/Delete StartPoint Path], click [Add].**

   To delete a start point path, select the path to delete in the list, and click [Delete].

4. **On the Add/Delete StartPoint Path window, add or edit a start point path, and click [OK].**

Note

- For the setting items on the [Send to FTP] tab, see page 703 "Send to FTP".

Send to Printer

The Send to Printer connector prints files to the printer configured on the Delegation Server.

Files in JPEG (jpeg, jpg, jpe extensions) or TIFF (tif and tiff extensions) format can be printed. The default settings of the selected printer driver are used for printing.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

The Send to Printer connector settings are divided into the following two tabs. Use the accordion icons to display each tab.

- [Header/Footer Print Settings]

  Specify the print position and embedded strings in the header and footer.

- [Page Setup]

  Specify the method to select paper size.

Use the following procedure to configure the properties of the Send to Printer connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Printer] connector icon.**
2. **On the [Send to Printer] tab, enter the display name in [Display Name].**
3. **On [Header/Footer Print Settings], specify the print position and embedded strings in the header and footer.**
4. **On [Page Setup], specify the method to select paper size.**

Note

- For the setting items on the [Send to Printer] tab, see page 706 "Send to Printer".

Send to WebDAV

The Send to WebDAV connector delivers scanned documents to more than one specified WebDAV server.

When a document management system from a different manufacturer that supports WebDAV is used, scanned documents can be stored directly in the repository.

Authentication

The Send to WebDAV connector supports both NTLMv2 and Kerberos as the authentication method. For details about selecting the authentication method, see page 539 "Delegation Server Settings".

The Send to WebDAV connector settings are divided into the following two tabs. Use the accordion icons to display each settings window.

- [Add/Delete StartPoint Path]

  Add, edit, or delete a start point path (root folder).

- [HTTP Proxy Server]

  Configure a proxy server when accessing a folder in the WebDAV server via a proxy server.

Note

- HTTP and HTTPS are supported.
- A file name is added to the scanned document in accordance with the configured naming convention. See page 255 "File and Folder Naming Conventions".

Use the following procedure to configure the properties of the WebDAV connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to WebDAV] connector icon.**
2. **On the [Send to WebDAV] tab, enter the display name in [Display Name].**
3. **When accessing a WebDAV folder outside the firewall via a proxy server, configure the proxy server in [HTTP Proxy Server].**

   Configure all setting items in [HTTP Proxy Server].

4. **Under [Add/Delete StartPoint Path], click [Add].**

   To delete a start point path, select the path you want to delete from the list, and click [Delete].

5. **On the [General Settings] tab of the Add/Delete StartPoint Path window, add or edit a start point path (root folder).**
6. **To associate a metadata element of a document with the WebDAV properties, click [Add] on the [Assign Metadata Elements] tab.**

   To delete an assigned metadata element, select the assigned metadata element you want to delete from the list, and click [Delete].

7. **In [Add Assigned Metadata Elements], enter the source metadata element to be assigned, the target WebDAV property, and the namespace of the WebDAV property.**

   Mapping Example (When the document name is "Document1.tif")

   - [Source]: Document Name (selected from the drop-down list)

- [Target]: doc_name
- [Namespace]: ns1

The document information will be set in the WebDAV server as follows:

<ns1:doc_name>Document1.tif</ns1:doc_name>

8. **Click [OK].**

Note

- For the setting items on the [Send to WebDAV] tab, see page 707 "Send to WebDAV".
- The Assign Metadata Elements setting may not be valid depending on the connected server specifications.
- When a scanned file is successfully delivered to a WebDAV server, it is treated as a successful delivery even if metadata element assignment fails, and it is not delivered again. However, metadata element assignment errors are recorded in the system log.

Send to SharePoint

The Send to SharePoint connector delivers scanned documents to Microsoft SharePoint Server or Office 365 SharePoint Online. It can also be used to automatically generate a delivery folder and associate the metadata elements with Microsoft SharePoint Server.

Sites and libraries can be configured not only using the Management Console, but also with the operation screen of the device.

Distribution destination libraries

The following libraries can be specified as the delivery destination:

- Document Library
- Image Library
- Form Library
- Media Library

Note

- The libraries provided vary depending on the version of the SharePoint Server.
- The following settings do not support delivery to a valid SharePoint Server:
  - Multi-tenant function
  - Form-based authentication
  - Content Approval/Content History function
- Delivery to libraries with View based on a setting other than the default is not supported.

Office 365 SharePoint Online Plans

The following SharePoint Online (OneDrive for Business) Plans are supported:

- Plan 1
- Plan 2
- E1 (E2)
- E3
- SharePoint Online

Authentication

You can use NTLMv2 or Kerberos authentication when accessing Microsoft SharePoint Server.

MS Account authentication or ADFS authentication can be used when accessing Office 365 SharePoint Online.

For details about selecting the authentication method, see page 539 "Delegation Server Settings".

Note

- To create a subfolder, access to the SharePoint server must be performed by a user with library write permissions.
- To browse a site, access to the SharePoint server must be performed by a user with post permissions or above. In addition, in the SharePoint Server, Office 365, and SharePoint Online settings, add directory browsing permissions to the read permissions.
- When configuring Field Settings, access to the SharePoint server must be performed by a user with post permissions or above.
- When using an IP address or FQDN in the SharePoint Server URL, add a public URL to the alternate access mapping on SharePoint Server. If the alternate access mapping is correctly configured, the document data may not be saved and the connection to a personal site may not be established even when a subfolder is generated at delivery. For details about the configuration, see SharePoint Server help.
- When Azure Active Directory (Azure AD) is used to identify Office 365 users, be sure to select [Use Microsoft Account] for [Authentication Method]. In this case, only the user accounts in root domain of Office 365 tenant are supported.

The Send to SharePoint connector settings are divided into the following two tabs. Use the accordion icons to display each tab.

- [Select Server Type]

  Specify the server type and configure the HTTP proxy server settings.

- [Add/Delete StartPoint Path]

  Add, edit, or delete a start point path (root folder).

Use the following procedure to configure the properties of the Send to SharePoint connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to SharePoint] connector icon.**
2. **On the [Send to SharePoint] tab, enter the display name in [Display Name].**

3. **Specify the server type and configure HTTP proxy server settings in [Select Server Type].**
4. **Under [Add/Delete StartPoint Path], click [Add].**

   To delete a start point path, select the path to delete in the list, and click [Delete].
5. **On the [General Settings] tab of the [Add StartPoint Path] window, specify [Display Name], [URL], [Authentication Method], [User Name], and [Password], and then click [Connect].**

   When a connection is successfully established, [Connect] changes to [Disconnect].
6. **In the list of read-only libraries displayed on the [Library] drop-down list, select the library to be specified as the delivery destination.**
7. **Configure other items as necessary.**
8. **To configure the property column in the library specified as the delivery destination, click [Add] on the [Field Settings] tab.**

   To delete the added document information association, select the association you want to delete from the list, and click [Delete].
9. **On the [Add Field Settings] window, configure the [MOSS Field] and [Setting Value], and then click [OK].**

   By adding and associating the names of metadata elements configured when the document is scanned as a property column on Microsoft SharePoint Server/Office 365 SharePoint Online, the metadata can be standardized and document management can be improved.
10. **Click [OK].**

Note

- For the setting items on the [Send to SharePoint] tab, see page 711 "Send to SharePoint".

Send to CMIS

The Send to CMIS connector delivers scanned documents to a CMIS repository, such as OpenText, EMC Documentum, and IBM FileNet.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported products and versions

- IBM File Content Manager
- OpenText Content Server
- EMC Documentum

The Send to SharePoint connector settings are divided into the following three screens. Use the accordion icons to display each tab.

- [General Settings]

  Configure the CMIS repository type, URL, authentication method, and other settings, and connect to the CMIS server.

- [Document Settings]

  Configure the default values of the document type filter and document properties.

- [Other Settings]

  Configure the settings related to subfolder and file naming conventions.

Use the following procedure to configure the properties of the Send to CMIS connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to CMIS] connector icon.**
2. **On the [Send to CMIS] tab, enter the display name in [Display Name].**
3. **In [General Settings], specify the CMIS repository type, CMIS server path, authentication method, and other settings, and then connect to the CMIS server.**
4. **Configure the delivery destination repository and folder settings.**
5. **Click [Test] to test the connection.**
6. **In [Document Settings], configure the default values of the document type filter and document properties.**
7. **In [Other Settings], configure the settings for using a subfolder as the delivery destination.**

Note

- For the setting items on the [Send to CMIS] tab, see page 719 "Send to CMIS".

Send to DocumentMall

The Send to DocumentMall connector delivers scanned documents to a Document Mall folder.

It can also be used to automatically generate a delivery folder and associate the metadata with Document Mall properties.

The Send to DocumentMall connector settings are divided into the following two screens. Use the accordion icons to display each tab.

- [Add/Delete StartPoint Path]

  Add, edit, or delete a start point path (root folder).

- [HTTP Proxy Server]

  Configure a proxy server when accessing a Document Mall folder via a proxy server.

Use the following procedure to configure the properties of the Send to DocumentMall connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to DocumentMall] connector icon.**

2. **On the [Send to DocumentMall] tab, enter the display name in [Display Name].**
3. **When accessing a Document Mall folder outside the firewall via a proxy server, use [HTTP Proxy Server] to configure the proxy server.**

   Configure all setting items in [HTTP Proxy Server].
4. **Under [Add/Delete StartPoint Path], click [Add].**

   To delete a start point path, select the path you want to delete from the list, and click [Delete].
5. **On the [General Settings] tab of the [Add StartPoint Path] window, specify [Display Name], [URL], [Authentication Method], [User Name], and [Password], and then click [Connect].**

   When a connection is successfully established, [Connect] changes to [Disconnect].
6. **Configure the settings to use a subfolder as the delivery destination as necessary.**
7. **To associate a metadata element of a document with the Document Mall properties, click [Add] on the [Assign Metadata Elements] tab.**

   To delete an association setting, select the association setting you want to delete from the list, and click [Delete].
8. **In [Add Assigned Metadata Elements], enter the source metadata element to be assigned and the target Document Mall property.**
9. **Click [OK].**

Note

- For the setting items on the [Send to DocumentMall] tab, see page 724 "Send to DocumentMall".

Send to Exchange (EWS)

The Send to Exchange connector delivers scanned documents to Microsoft Exchange Server or Office 365 Exchange Online.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

The Send to Exchange connector settings are divided into the following three screens. Use the accordion icons to display each tab.

- [Email System Settings]

  Configure the EWS server.
- [Send to Email Option Settings]

  Configure the sender e-mail address, file naming convention, and e-mail text.
- [Email Search Settings]

Configure the LDAP server to enable the user to search in the LDAP server address book.

Authentication

You can use NTLMv2 or Kerberos authentication when accessing Microsoft Exchange Server.

MS Account authentication or ADFS authentication can be used when accessing Office 365 Exchange Online.

Use the following procedure to configure the properties of the Send to Exchange connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Exchange] connector icon.**
2. **On the [Send to Exchange] tab, enter the display name in [Display Name].**
3. **In [Email System Settings], configure the EWS server.**
4. **In [Send to Email Option Settings], specify the method for attaching files, and specify the sender e-mail address, file naming convention, and e-mail text.**
5. **In [Email Search Settings], configure the LDAP server.**

Note

- For the setting items on the [Send to Exchange] tab, see page 727 "Send to Exchange".
- If RICOH Streamline NX has been installed with SSL/HTTPS, proxy server with basic authentication is not supported.

Send to RightFax

The Send to RightFax connector sends the scanned document by e-mail or fax via the RightFax server.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**
- **The Send to RightFax connector only supports the functions provided by your RightFax server. For details about RightFax functions, see the RightFax manuals.**
- **Create a RightFax Proxy User Accounts with administrator privileges. This account must not integrate with Windows NT.**
- **You can use the FaxUtil of the RightFax client software to check the status of a Send to RightFax job.**

Additional information of the RightFax Server

- When a fax number is specified as a destination, note the following:
  - An application that supports the format of the cover sheet file you are using must be installed on the RightFax server.

- Available process connectors vary depending on the version of RightFax you are using. Some process connectors such as PDF Converter may not be supported. For details, see the RightFax manuals.

- The fax may not be sent depending on the settings in [Sending Required Fields] under [Customize Cover Sheet Information]. Specify only [To Name] and [From Name].

The Send to RightFax connector settings are divided into the following four screens. Use the accordion icons to display each tab.

- [RightFax Server Settings]

  Specify the account details and configure the Authentication Profile. The information entered on this tab is required for both connectivity testing and operational connection with the RightFax server.

- [Phonebook Display and Search Settings]

  Specify the Phonebook search settings and configure the display on the MFP Destination Selection screen.

- [ODBC and Group Search Settings]

  Specify ODBC and group search settings. When ODBC is used, the search for RightFax user using [Search] on the MFP Service screen becomes faster.

- [Job Settings]

  Specify the job settings.

Use the following procedure to configure the properties of the Send to RightFax connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to RightFax] connector icon.**
2. **On the [Send to RightFax] tab, enter the display name in [Display Name].**
3. **In [RightFax Server Settings], configure the settings required for connecting to the RightFax server.**
4. **In [Phonebook Display and Search Settings] configure the settings required for searching in Phonebook.**
5. **In [ODBC and Group Search Settings], configure the settings to use ODBC for searching an SQL database.**
6. **In [Job Settings], configure the settings to determine how to process a job when an error occurs.**

Note

- For the setting items on the [Send to RightFax] tab, see page 733 "Send to RightFax".

Send to Gmail

The Send to Gmail connector sends the scanned document to a Gmail account.

Prerequisites for using the Send to Gmail connector

To use the Send to Gmail connector, create a service account and authorize it to access the user's Gmail data.

- Creating a service account
  - Login to "https://console.developers.google.com".
  - Enable Admin SDK, Gmail API and Google People API.
  - When creating a service account, be sure to enable G Suite domain-wide delegation.
  - After creating a service account, the new public/private key pair is generated and downloaded to the computer as a JSON file.
  - Be sure to write down the Client ID displayed when "View Client ID" next to the service account is clicked. You will need it when specifying the API scope.
- Managing API client access
  - Login to "https://admin.google.com".
  - In the "Manage API client access" screen, specify the API scope as follows:

    https://www.googleapis.com/auth/gmail.send

    https://www.googleapis.com/auth/gmail.readonly

    https://www.googleapis.com/auth/contact.readonly

    https://www.googleapis.com/auth/admin.directory.user.readonly

Send to Gmail connector settings are divided into the following three screens. Use the accordion icons to display each tab.

- [Email System Settings]

  Upload the private key file and configure the authentication method and proxy server.
- [Send to Gmail Option Settings]

  Configure the file attachment method, file naming convention, and e-mail text.
- [Email Search Settings]

  Enable or disable searching in Gmail personal contact or G Suite Directory when specifying destinations.

Use the following procedure to configure the properties of the Send to Gmail connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Gmail] connector icon.**
2. **On the [Send to Gmail] tab, enter the display name in [Display Name].**
3. **In [Email System Settings], upload the private key file, and configure the authentication method and proxy server.**
4. **In [Send to Gmail Option Settings], configure the file attachment method, file naming convention, and e-mail text.**

5. **In [Email Search Settings], enable or disable search methods.**

Note

- For the setting items on the [Send to Gmail], see page 737 "Send to Gmail".

Send to Google Drive

The Send to Google Drive connector saves the scanned document in Google Drive.

Prerequisites for using the Send to Google Drive connector

To use the Send to Google Drive connector, create a service account and authorize it to access the user's Google Drive data.

- Creating a service account
  - Login to "https://console.developers.google.com".
  - Enable Google Drive API.
  - When creating a service account, be sure to enable G Suite domain-wide delegation.
  - After creating a service account, the new public/private key pair is generated and downloaded to the computer as a JSON file.
  - Be sure to write down the Client ID displayed when "View Client ID" next to the service account is clicked. You will need it when specifying the API scope.
- Managing API client access
  - Login to "https://admin.google.com".
  - In the "Manage API client access" screen, specify the API scope as follows:

    https://www.googleapis.com/auth/drive

Send to Google Drive connector settings are divided into the following two screens. Use the accordion icons to display each tab.

- [Send to Google Drive Option Settings]

  Upload the private key file and configure the authentication method and proxy server.
- [Other Settings]

  Configure the settings related to subfolder and file naming conventions.

Use the following procedure to configure the properties of the Send to Google Drive connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Google Drive] connector icon.**
2. **On the [Send to Google Drive] tab, enter the display name in [Display Name].**
3. **In [Send to Google Drive Option Settings], upload the private key file, and configure the authentication method and proxy server.**
4. **In [Other Settings], configure the settings for using a subfolder as the delivery destination.**

Note

- For the setting items on the [Send to Google Drive], see page 741 "Send to Google Drive".

Send to Dropbox

The Send to Dropbox connector saves the scanned document in a business account of Dropbox.

Send to Dropbox connector settings are divided into the following two screens. Use the accordion icons to display each tab.

- [Send to Dropbox Option Settings]

  Configure the authentication and proxy settings to allow the Send to Dropbox connector to access to the repository.

- [Other Settings]

  Configure the settings related to subfolder and file naming conventions.

Use the following procedure to configure the properties of the Send to Dropbox connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Send to Dropbox] connector icon.**
2. **On the [Send to Dropbox] tab, enter the display name in [Display Name].**
3. **In [Send to Dropbox Option Settings], configure the authentication information and proxy server.**
4. **In [Other Settings], configure the settings for using a subfolder as the delivery destination.**

Note

- For the setting items on the [Send to Dropbox], see page 743 "Send to Dropbox".
- If RICOH Streamline NX has been installed with SSL/HTTPS, proxy server with basic authentication is not supported.

File and Folder Naming Conventions

Use the following conventions to automatically name a file or a folder using the metadata included in a scanned document.

Specifying Metadata in File and Folder Names

Metadata of the destination connector can be added to file and folder names.

Enter the metadata directly in the destination connector settings window, select basic metadata elements from the drop-down list, or use either of the following specification methods:

Enter a custom metadata element

Enter a metadata element by enclosing the element name (ID) in curly brackets ({ }). You can enter a metadata element that cannot be selected from the drop-down list.

Combine a string and metadata element

Enter a file name by combining a directly entered string and a metadata element enclosed in curly brackets ({ }).

For example, when "report ({userName})" is entered and the userName value is "Saito", the file name becomes "report (Saito)".

Note

- For details on metadata items, see page 348 "Metadata".
- For details about the characters that cannot be used in a string, see [Folder Naming Rules] and [File Naming Rules] of each connector in page 691 "Setting Items in the Destination Connector Properties".
- If the metadata specified as the file or folder name does not exist, "{tagName}" is used as the file or folder name.
  For example, when you select a port number that is metadata that applies only in a fax job as the file name or when you enter "{port}" directly, "{port}" is used as the file name of a scan job.

Numerical format of metadata

To include in the file name a numerical metadata element such as the page number or resolution, specify the numerical format.

Note

- You can only specify a numerical format when the value is an integer. When the value includes a decimal point, the value after the decimal point is omitted.

Specifying the numerical format

Input example	Description
{tagName: NXX}	XX is the number of digits in the value. When the number of digits in the value is less than XX, a space is added in front of the value. Example: When "file{page:N3}" is entered, and the "page" value is 12, the file name "file 12.tif" is generated.
{tagName: N0XX}	XX is the number of digits in the value. When the number of digits in the value is less than XX, one or more zeros are added in front of the value. Example: When "{page:N05}_file" is entered, and the "page" value is 12, the file name "00012_file.tif" is generated.

Example of output value of provisional tag "metatag"

"metatag" value	Input	Output
12	{metatag : N4}	_ _12
	{metatag : N04}	0012
123456	{metatag : N4}	123456
	{metatag : N04}	123456
-12	{metatag : N4}	_-12
	{metatag : N04}	-012
ABCDE	{metatag : N4}	_ _ _0
	{metatag : N04}	0000
123ABCDE	{metatag : N4}	_123
	{metatag : N04}	0123

"metatag" value	Input	Output
123.45	{metatag : N4}	_123
	{metatag : N04}	0123

Note

- The underscores in the Output column indicate spaces.
- Spaces before or after a metatag value are automatically deleted. For example, "_123" (where the underscore indicates a space) becomes "123".
- When a character other than "N" is included in the format, the format specification is ignored.
- When the numerical format is not correctly specified, the "N04" format applies.

Date and time format of metadata

Specify either the local time or UTC time for the date and time in the metadata such as the date created (generationEpoch) and date registered (registrationEpoch). The time is displayed down to milliseconds.

Specifying the date and time format

Input example	Description
{tagName: DX}	The format specified with X is displayed as the local time on the device.
{tagName: U0X}	The format specified with X is displayed as the UTC time (universal standard time).

"X" is the display format of the date. The table below shows the characters that can be used.

Character	Meaning
Y	Year
M	Month
d	Day
h	Hour in 12 hour format
H	Hour in 24 hour format
m	Minute
s	Second

Character	Meaning
S	Millisecond

For example, when the date and time are October 30, 2008, 2:37 PM Japan Standard Time, they are expressed as follows:

Format	Result
{metatag : DyyyyMMdd}	20081030
{metatag : DddMMyyyyHHmm}	301020081437
{metatag : UddMMyyyyHHmm}	301020080537
{metatag : DMMddyyhhmmss}	103008023700

Note

- Regardless of the value, it can be converted to a date and time by applying the format above.
- When a character other than "D" or "U" is included in the date and time format, the format specification is ignored.
- If the date and time format are not correctly specified, the format conversion may not be properly performed.

Other File Naming Conventions

The file name may change depending on the following conventions:

- When a process connector that allows specifying of the file name in front of the destination connector is positioned in the delivery flow, the priority is given to the conversion result of the process connector.
- If [File Naming Rules] is not configured in the destination connector properties, the document name specified on the device (or yyyyMMddHHmm when not specified) is used as the file name.
- When the document is configured with multiple sections, a four-digit suffix is added to the file name for each section. The format is "BaseName_XXXX", where "XXXX" is the section number.

Example

In the case of a document consisting of three sections with the base name "FileName", the following files are created:

FileName_0001.tif, FileName_0002.tif, FileName_0003.tif

Note

- When the section number exceeds four digits, the section number itself is added.

- When a file with the same name already exists in the delivery destination folder, a suffix enclosed in parentheses is added to the file name.

Example

FileName_0001(1).tif, FileName_0001(2).tif

A suffix is added to avoid a duplicate file name, and when 9999 is exceeded, an error occurs and the delivery fails. Because the number of suffixes increases and delivery takes longer to perform, accordingly try to avoid duplicate file names.

Configuring the Properties of a Process Connector

To use a process connector positioned in the delivery flow, configure the properties of the connector.

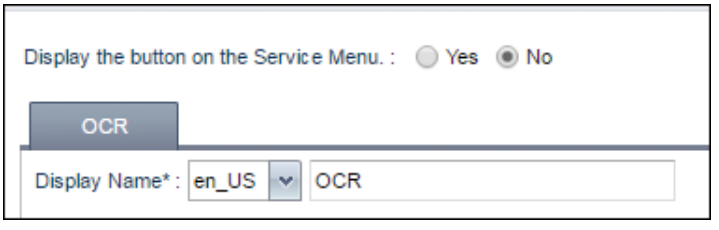
Select the process connector to configure on the [Delivery Flow] tab on the [Workflow Design] tab to display the process connector properties window.

The settings are verified when the user moves to another tab after making changes to the properties. The settings with errors are indicated by , and the user cannot move to another tab until the settings are corrected.

Displaying the process connector button on the Service Menu (Standard Operation Panel only)

You can configure whether or not to display the process connector buttons together with the workflow buttons on Service Menu.

Service Menu is a list of delivery services (types of destinations specified by destination connectors) displayed on the operation screen of the device.



To display the process connector buttons together with the workflow buttons on the operation screen of the device, select [Yes] in [Display the button on the Service Menu] at the top of the properties window. The user can press this button to access the process connector settings window.

When [No] is selected, the settings window can be accessed by pressing [Scan Settings], and then by selecting the tab of the process connector to be configured.

[Display Name] setting

The display name of a process connector can be specified for each language allowed on the RICOH Streamline NX system, and can be switched automatically according to the log-in language to the device.

Select a language from the drop-down menu, and then enter the display name.

Note

- The following process connectors do not handle the image orientation information (Exif Orientation tag) and may process the image in an orientation different from the original for images generated by some devices and applications.
  - PDF Converter
  - Image Converter

- Image Correction
- OCR (except Japanese)
- Zone OCR

PDF Converter

Use the PDF Converter to convert a document into a PDF file.

Supported formats (input data)

The following file formats are supported as input data for the PDF Converter connector.

- TIFF
- TIFF-F
- DCX
- BMP
- JPEG
- PNG
- GIF
- PDF

Note

- The following file formats are supported as input data in a workflow with [Job Processing Location] set to [On Device]:
  - TIFF (MMR, single page), JPEG
- You can only enter a PDF file via Monitor Folder.
- If a document with the following unsupported formats is entered, an error occurs and the data is not converted. However, documents with a format other than a password-protected PDF can be processed when an image converter is placed before a PDF converter and the document is converted to a format that can be input to the PDF converter.
  - TIFF (JBIG2)
  - TIFF (uncompressed, 32 bit)
  - TIFF (PackBits, 16/32 bit)
  - TIFF (ZIP compressed, 16/32 bit)
  - BMP (OS/2) V1, BMP (OS/2) V2
  - Password-protected PDF
- When a document with an unsupported format is entered and an error occurs, the queue is recorded in the error queue on the job list. For details about viewing error queues, see

page 366 "Managing Delivery Jobs". View detailed error information in the system log. For details about viewing this information, see page 416 "Viewing System Operation Logs".

- When a document with an unsupported format is entered and processing is canceled, the job is recorded as a success, and, it is not recorded in the error queue on the job list. View skipped jobs in the system log. For details about viewing this information, see page 416 "Viewing System Operation Logs".
- All document scanned using the device can be processed. However, if a document with an unsupported format is input via Monitor Folder or mobile devices, processing fails and the data is not converted.

Convertible formats (output data)

The following file formats are supported as output data for the PDF Converter connector:

File format	PDF version
Image PDF	1.3 (When [Location] is set to [On Server].)
	1.4 (When [Location] is set to [On Device].)
PDF/A	1.4
High Compression PDF	1.3
OCR Scanned PDF	1.3
Password-protected PDF	1.4

Note

- The following file formats are supported as out put data in a workflow with [Job Processing Location] set to [On Device].
  - Image PDF (version 1.4), password-protected PDF (version 1.4)
- When you select multiple output formats and convert them to one PDF file, it becomes a higher PDF version. For example, the version of a password-protected PDF with text becomes 1.4.
- The properties of a PDF file input via Monitor Folder are overwritten with the properties created by the PDF Converter connector.
- Images contained in the input file are compressed in the output file. Color and grayscale images are compressed to JPEG, and black-and-white images are compressed to JBIG2.
- When you select [PDF/A] for [PDF Type], you can only create an image PDF. You cannot create a PDF with text or a password-protected PDF.
- When you select [PDF/A] for [PDF Type], all setting items on the [PDF Converter] tab on the operation screen of the device are disabled.

- High compression PDF is the output format when [PDF] is selected for [PDF Type] and [On] for [Compression] in the PDF Converter connector properties.

PDF Converter processing conditions

- The PDF Converter connector and the Image Correction connector cannot be positioned in the same delivery flow.
- In a workflow with [Job Processing Location] set to [On Server], a PDF of up to 32,512 pixel × 32,512 pixel can be created.
- In a workflow with [Job Processing Location] set to [On Device], a multi-page PDF of up to 100 pages can be created. If the page number of the file exceeds 100, a separate file is created.
- The PDF Converter connector creates a PDF using ABBYY FineReader. The other applications that also use ABBYY FineReader cannot exist on the same Delegation Server.

Use the following procedure to configure the properties of the PDF Converter:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [PDF Converter] icon.**
2. **Specify the display name.**
3. **In [General Settings], configure PDF Type, PDF Format, and other settings.**

Note

- For the setting items on the [PDF Converter] tab, see page 747 "PDF Converter".
- The following file formats are supported as input data by the PDF Converter connector.

File Format
TIFF
TIFF-F
DCX
BMP
JPEG
PNG
GIF

Configuring the attributes of a password specified for a password-protected PDF

Double-click the password text box for either [Assign a User Password] or [Assign a Master Password] to configure the attributes of the password to be assigned to the password-protected PDF. After the configuration is completed, click [OK].

Item	Description
Min. Characters	Minimum number of characters required for a password. Specify a value between 0 and 32.
Regex for Validation	Regular expression to be used to check the password entered. **Note** • ^[!-~]*$ is set by default. This indicates that single-byte alphanumeric characters and symbols can be used for a password. If the password contains double-byte characters, the generated PDF may not be accessible. Do not change this setting unless required.
Retype	Specify whether or not to enable confirmation entry of password to prevent incorrect input. When Retype is selected, the user must enter his or her password twice when scanning a document.

Image Converter

The Image Converter connector converts a document to the file format the administrator specifies using the Management Console or to the one the user specifies on the operation screen of the device.

Supported formats (input data)

The following file formats are supported as input data for the Image Converter connector:

- TIFF (MH, single page/multiple pages)
- TIFF (MR, single page/multiple pages)
- TIFF (MMR, single page/multiple pages)
- TIFF (uncompressed, single page/multiple pages)
- TIFF-F (MH, single page/multiple pages)
- TIFF-F (MR, single page/multiple pages)
- TIFF-F (MMR, single page/multiple pages)
- DCX (single page/multiple pages)
- BMP (uncompressed)

- JPEG
- PNG
- GIF

Note

- Only the single-page TIFF format is supported in a workflow with [Job Processing Location] set to [On Device].

Convertible formats (output data)

The following file formats are supported as output data for the Image Converter connector:

- TIFF (MH, single page/multiple pages)
- TIFF (MR, single page/multiple pages)
- TIFF (MMR, single page/multiple pages)
- TIFF (uncompressed, single page/multiple pages)
- TIFF-F (MH, single page/multiple pages)
- TIFF-F (MR, single page/multiple pages)
- TIFF-F (MMR, single page/multiple pages)
- DCX (single page/multiple pages)
- BMP (uncompressed)
- JPEG
- PNG
- GIF
- File formats selected by the user on the operation screen of the device

Note

- Only the multi-page TIFF format and formats that the user selects on the operation panel of the device are supported in a workflow with [Job Processing Location] set to [On Device].
- For details about the input and output data restrictions, see page 268 "Input/output formats of the Image Converter Connector".

Image Converter Connector processing conditions

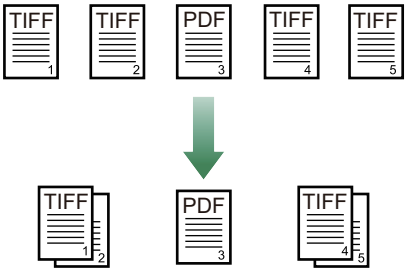
- When all input data cannot be processed

  Moves to the next step in the delivery flow without converting the data. An error does not occur.

- When the input data contains data that cannot be processed

  Data that cannot be processed is output without any conversion.

  For example, when four single page TIFF files and one PDF file are converted to one multiple page TIFF file, the result is as follows:



DSW615

- If an internal error occurs, the conversion process fails, and the remaining delivery flow is not executed.
- When image conversion is completed successfully, the original data is deleted.
- When converting to a multi-page PDF, the file can contain the following numbers of pages. If the file exceeds the maximum number of pages, a separate file is generated.
  - When [Job Processing Location] is set to [On Device]: 100 pages
  - When [Job Processing Location] is set to [On Server]: 500 pages
- The Image Correction connector and the PDF Converter connector cannot be positioned in the same delivery flow.
- In a workflow with Job Processing Location set to On Device, a different file will be created when the number of pages of a TIFF file exceeds 100.

Use the following procedure to configure the properties of the Image Converter connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Image Converter] connector icon.**
2. **Specify the display name.**
3. **In [General Settings], configure Output Format.**

Note

- For details about the [Image Converter] tab, see page 748 "Image Converter".
- When a format other than [File Format Selected on [Scan Settings] Tab] is selected as the output format in the [Image Format List], selecting the output format on the operation screen of the device has no effect. When the output format is preset, it is recommended to set [File Format] on the [Scan Settings] tab to Hide. For the configuration to hide the settings, see page 294 "Customizing the Settings on the Operation Screen of the Device".

Document format and Image Converter Connector

The default file format of documents scanned on the device is either TIFF or JPEG depending on the following [Scan Type] setting on the device:

- Black and white: TIFF (MMR, single page)
- Grayscale/full color: JPEG

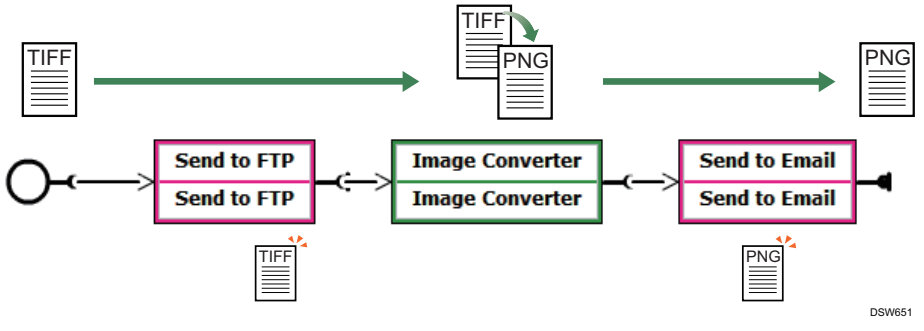
In all destination and process connectors prior to the Image Converter connector, documents are processed in the above-mentioned file format. When the Image Converter connector is not included in the delivery flow, data is output in the default file format (TIFF or JPEG) regardless of the file format selected by the user on the operation screen of the device.

In a delivery flow that does not use the Image Converter connector, selecting the output format on the operation screen of the device has no effect. When the Image Converter connector is not used, it is recommended to set [File Format] on the [Scan Settings] tab to Hide. For details about the Hide setting, see page 294 "Customizing the Settings on the Operation Screen of the Device".

The following figures show examples of the file formats output in various delivery flows:

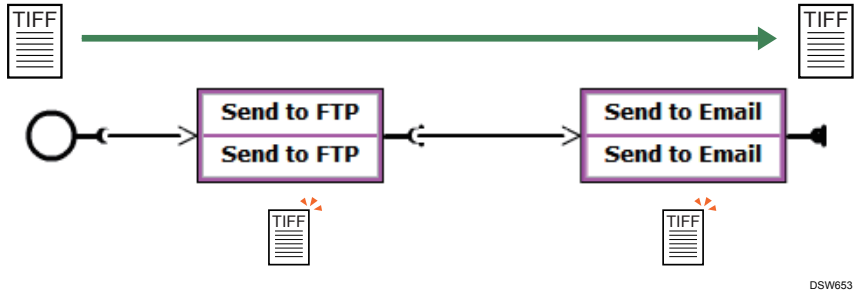
- The user selects PNG, and there is an Image Converter connector ([Document Type]: B&W)

  The Image Converter connector converts the TIFF file to the PNG format as specified by the user.



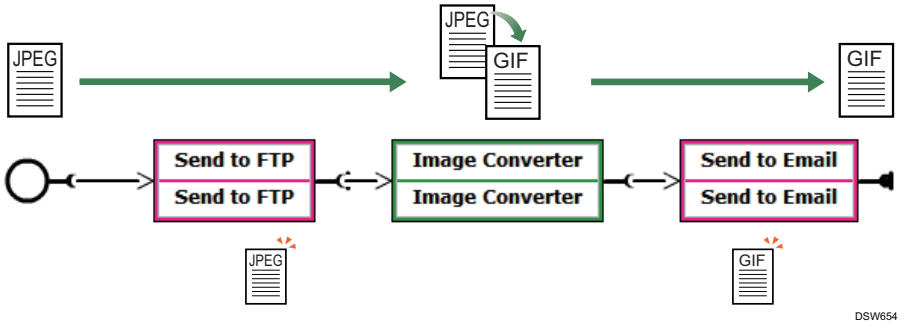
- The user selects PNG, and there is no Image Converter connector ([Document Type]: B&W)

  The file format the user specifies is ignored and the file is output in TIFF format because the Image Converter connector is not placed in the workflow.



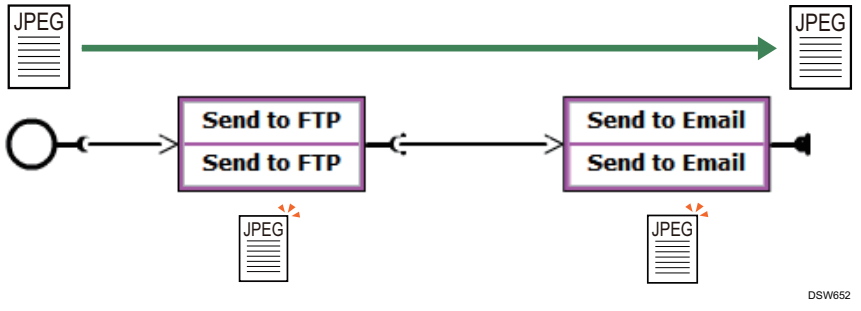
- The user selects GIF, and there is an Image Converter connector ([Document Type]: Grayscale/Full color)

  The Image Converter connector converts the TIFF file to the GIF format as specified by the user.



- The user selects GIF, and there is no Image Converter connector ([Document Type]: Grayscale/Full color)

  The file format the user specifies is ignored and the file is output in TIFF format because the Image Converter connector is not placed in the workflow.



Input/output formats of the Image Converter Connector

The Image Converter connector converts input data to a different format with the same color depth.

The input formats supported by RICOH Streamline NX and the convertible output formats are shown in the table below.

Black and White (1 bit)

The input data in each supported format can be converted into any convertible output data format.

Supported Formats (Input Data)	Convertible Formats (Output Data)
TIFF (MH, single page)	TIFF (MH, single page)
TIFF (MR, single page)	TIFF (MR, single page)
TIFF (MMR, single page)	TIFF (MMR, single page)
TIFF (uncompressed, single page)	TIFF (uncompressed, single page)
TIFF (MH, multi page)	TIFF (MH, multi page)
TIFF (MR, multi page)	TIFF (MR, multi page)
TIFF (MMR, multi page)	TIFF (MMR, multi page)
TIFF (uncompressed, multi page)	TIFF (uncompressed, multi page)
TIFF-F (MH, single page)	TIFF-F (MH, single page)
TIFF-F (MR, single page)	TIFF-F (MR, single page)
TIFF-F (MMR, single page)	TIFF-F (MMR, single page)
TIFF-F (MH, multi page)	TIFF-F (MH, multi page)
TIFF-F (MR, multi page)	TIFF-F (MR, multi page)
TIFF-F (MMR, multi page)	TIFF-F (MMR, multi page)
DCX (single page)	DCX (single page)
DCX (multi page)	DCX (multi page)
BMP (uncompressed)	BMP (uncompressed)
PNG	JPEG
GIF	PNG
	GIF

Grayscale/Full Color (4-bit, 8-bit, 24-bit)

Each supported format can be converted into any convertible format.

Supported Formats (Input Data)	Convertible Formats (Output Data)
TIFF (uncompressed, single page)	TIFF (uncompressed, single page)
TIFF (uncompressed, multi page)	TIFF (uncompressed, multi page)
BMP (uncompressed)	BMP (uncompressed)
JPEG	JPEG
PNG	PNG
GIF	GIF

Note

- When you select the JPEG format for the output data, the data is output in 24-bit color regardless of the color depth of the input data.
- When the input data has a color depth of 24-bit grayscale or full color and is converted to GIF format, the data is converted to 8-bit color.
- For details on the Image Converter connector settings, see page 747 "Setting Items in the Process Connector Properties".

Archiver

Use the Archiver connector to convert a scanned document into a .zip or .tgz format archive (compressed) file.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The Archiver connector supports all file formats compatible with RICOH Streamline NX.

Convertible formats (output data)

The following archive formats are supported as output data for the Archiver connector.

- zip
- tgz (tar compressed with gzip)

Note

- The maximum file size of the output data is 4 GB.
- One document is stored in one archive file regardless of the number of document sections.
- Encryption is not supported.

Archiver Connector processing conditions

- If an internal error occurs, the conversion process fails, and the remaining delivery flow is not executed.
- When archiving is completed successfully, the original data is deleted.

Use the following procedure to configure the properties of the Archiver connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Archiver] connector icon.**
2. **Specify the display name.**
3. **In [General Settings], configure Archive Format.**

Note

- For the setting items on the [Archiver] tab, see page 749 "Archiver".

OCR

The OCR connector recognizes the characters in a scanned document and extract them as text. When the OCR language is a language other than Japanese, the extracted text can be saved in the DOCX or XML format. The OCR connector also identifies the top and bottom of the document and adds a file name based on the text extracted from the first page of the scanned document.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The following file formats are supported as input data for the OCR connector:

- TIFF
- TIFF-F
- DCX
- BMP
- JPEG
- PNG
- GIF

Convertible formats (output data)

When the OCR language is Japanese, the file formats supported as output data for the OCR connector is the same as those supported for input data .

When the OCR language is not Japanese, the following file formats are supported as output data for the OCR connector when converting a document to text.

- RTF
- XLS
- XLSX
- DOCX

Note

- When the format conversion function is used, input files are connected to create one file.
- When [Top and Bottom Identification] is enabled and the input data is in TIFF-F format, the output data is converted to TIFF format. The compression format (MMR, MH, etc.), however, is the same as the original input data.

- When converted to the RTF or DOCX format, the extracted text is placed in text boxes to maintain document layout.
- If the document contain the languages other than that specified, parts that cannot be detected are output in blank space.

OCR Connector processing conditions

- When input data cannot be processed

  Moves to the next step in the delivery flow without performing OCR. An error does not occur.
- When the input data contains data that cannot be processed

  The file including data that cannot be processed is skipped, and only the processable data is processed by OCR.
- If an internal error occurs, OCR fails, and the remaining delivery flow is not executed.

Use the following procedure to configure the properties of the OCR connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [OCR] connector icon.**
2. **Specify the display name.**
3. **In General Settings, specify Document Name Extraction and Format Conversion.**

Note

- For the setting items on the [OCR] tab, see page 750 "OCR".

Section Specify

The Section Specify connector extracts a section from a document and pass only the extracted section to the next destination connector in the delivery flow. The sections not extracted are deleted.

Use this connector when delivering only the body of a document with a cover or cover letter.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The Section Specify connector supports all formats compatible with the RICOH Streamline NX delivery function.

Convertible formats (output data)

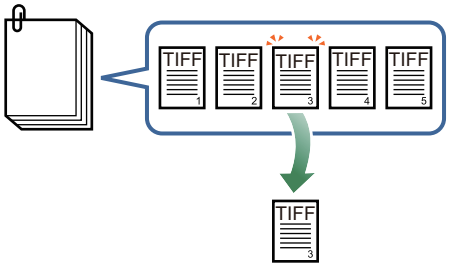
The output data format is the same as the input data.

Target of Section Specify Connector

Use the Section Specify connector for sections (in a file) not pages.

- Example 1 (multiple single page sections)

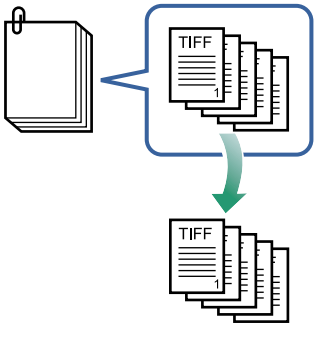
When a document (input data) consists of five single page TIFF files (five sections) and the third section in the document is specified, the third section is extracted to a file, and the other sections are deleted.



DSW620

- Example 2 (one multiple page section)

  When a document (input data) consists of one multiple page TIFF file (one section) and the first section of a document is specified, the section itself, not the first page, is extracted.



BMB289S

Use the following procedure to configure the properties of the Section Specify connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Section Specify] connector icon.**
2. **Specify Display Name.**

Section Splitter

Use the Section Splitter connector to divide a job by separating document data that consists of multiple sections by the number of sections specified on the operation screen of the device.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The Section Splitter connector supports all formats compatible with the RICOH Streamline NX delivery function.

Note

- The Section Splitter connector does not support multi-page files. When inputting a file with multiple pages, place the Image Converter connector before the Section Splitter connector to convert the file to a single-page one.

Convertible formats (output data)

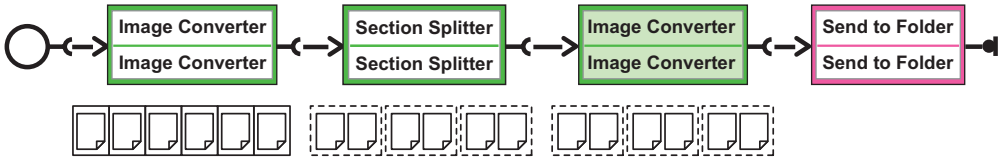
The output data format is the same as the input data.

Target of Section Splitter connector

Use the Section Splitter connector for sections (in a file) not pages.

Section Division Connector Usage Example

In the following workflow, a six-page document scanned in multi-page TIFF format is divided into three jobs comprising two pages each using the Image Converter and Section Division Connector, and distributed by Send to Folder.



DSW617

The document is converted into files in single-page TIFF or JPEG format for each page (each section) by the Image Converter.

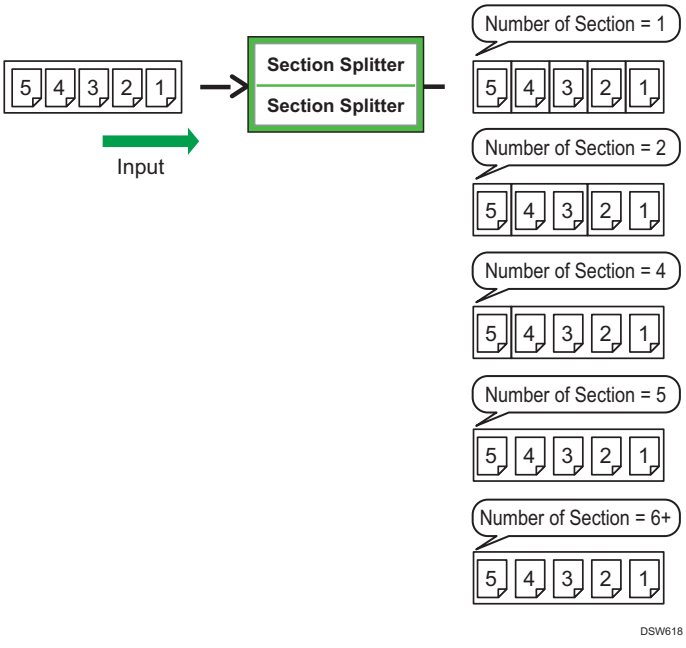
The job comprising six pages (six sections) is then divided for each two sections into three jobs by the Section Division Connector that is configured to divide a job for every two sections.

The jobs are then converted back into multi-page TIFF files by the Image Converter. Three multi-page TIFF files each comprising two pages are generated from three jobs.

Finally, three files that have been generated are distributed by Send to Folder.

No error will occur, and no special operation is required in the case shown in the figure shown below:

- The number of sections in the scanned document is fewer than the number of sections specified in the Section Division Connector
- The job cannot be divided into jobs comprising the same number of sections when divided by the specified number of sections



Five jobs consisting of one section each are generated when a job consisting of five sections is processed by the Section Division Connector in which the number of section is set to one.

Two jobs consisting of two sections each and one job comprising of one section are generated when a job consisting of five sections is processed by the Section Division Connector in which the number of section is set to two.

One job consisting of four sections and one job comprising of one section are generated when a job consisting of five sections is processed by the Section Division Connector in which the number of section is set to four.

One job consisting of five sections is generated when a job consisting of five sections is processed by the Section Division Connector in which the number of section is set to five or more.

Section Splitter connector processing conditions

If an error occurs during Section Splitter processing, the successfully processed sections are sent to the next process in the delivery flow, and the entire job is sent to the error queue. On the job that is sent to the error queue, the dividing process is applied for the pages after the processing has failed, and the job is sent to the next step in the delivery flow if processing is successful.

Use the following procedure to configure the properties of the Section Splitter connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Section Splitter] connector icon.**
2. **Specify Display Name.**

XML Transformer

The XML Transformer extracts metadata from a scanned document as XML data and converts it to another format (HTML, CSV, etc.) using a specified XSL file (XML stylesheet).

Supported formats (input data)

The XML Transformer supports all formats compatible with the RICOH Streamline NX delivery function.

Convertible formats (output data)

The output data of the XML Transformer is generated in the same format as the input data or the following formats:

- XML
- Format with XSL file as the target

Important

- **To use the XML Transformer, configure an XSL file (stylesheet for converting XML file) in advance according to your application.**
- **As samples, use the XSL files stored in the [samples] folder ▶ [StyleSheets] folder on the installation media.**
- **The XML Transformer converts only metadata and not the scanned document.**

Note

- For details about metadata format (XML format), see page 348 "Metadata".

Use the following procedure to configure the properties of the XML Transformer:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [XML Transformer] icon.**
2. **Specify Display Name.**
3. **In General Settings, configure the XSL file to use, the processing method of the conversion result file, and other settings.**

Note

- For the setting items on the [XML Transformer] tab, see page 750 "XML Transformer".

Metadata Converter

The Metadata Converter connector converts the values of the specified metadata item in a scanned document. This connector can also be used to change the values of metadata items to different values based on the rules specified in the replacement table.

For example, when the metadata contains corporate department numbers, those numbers can be replaced with the corresponding department names.

Important

- **To use the Metadata Converter connector, create a replacement table in advance. For details about creating replacement table, see page 334 "Configuring a Replacement Table".**

Note

- The Metadata Converter connector changes only the metadata. The details of the scanned document are not changed.
- For details about metadata, see page 348 "Metadata".

Supported formats (input data)

The Metadata Converter connector supports all formats compatible with the RICOH Streamline NX delivery function.

Convertible formats (output data)

The output data format is the same as the input data.

Metadata Converter Connector Processing Conditions

- When the target metadata value does not match the [Comparison Target String] configured in the replacement table, the data is processed using the method selected in [Select Action when Table Data does not Match].

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the Metadata Converter connector icon.**
2. **Specify the display name.**
3. **In General Settings, configure the replacement table to use and other settings.**

Note

- For the setting items on the [Metadata Converter] tab, see page 751 "Metadata Converter".

Metadata Replacement

The Metadata Replacement connector validates a specified value in the metadata items of the scanned document and changes a specific part of the value using a regular expression. For example, the hyphens in a phone number can be deleted, and all uppercase in the metadata can be changed to lowercase. Also, it can stop the workflow processing when the specified metadata item does not match the specified value.

Note

- A replacement table is not used for the Metadata Replacement connector.
- The Metadata Replacement connector changes only the metadata. The details of the scanned document are not changed.

- For details about metadata, see page 348 "Metadata".

Supported formats (input data)

The Metadata Replacement connector supports all formats compatible with the RICOH Streamline NX delivery function.

Convertible formats (output data)

The output data format is the same as the input data.

Metadata Replacement Connector processing conditions

When the specified metadata does not exist in the metadata of the document, the replacement process is skipped, and the delivery flow continues. The process is recorded as being successful in the job log, and the connector being skipped is recorded in the system log.

Use the following procedure to configure the properties of the Metadata Replacement connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Metadata Replacement] connector icon.**
2. **Specify the display name.**
3. **In General Settings, configure the regular expression, metadata items to validate, replacement string, and other settings.**

Note

- For the setting items on the [Metadata Replacement] tab, see page 752 "Metadata Replacement".

Usage examples of regular expressions

In addition to the regular expressions on page 358 "Regular Expressions", you can also use the following variables.

Variable	Content
$1, $2, ...	Part that matches a group in a regular expression
$&	Part that matches the entire regular expression

The following are setting examples of regular expressions used to confirm and replace the target values of metadata items.

Example 1: Confirming whether or not a phone number in a document is valid

When a valid phone number has a structure of "(2 to 4 digits)-(2 to 4 digits)-(4 digits)", specify as follows:

- [Regex]: \d{2,4}-\d{2,4}-\d{4}
- [Operations]: Select [Use Match Reference Function]

Example 2: Deleting hyphens from a phone number

To delete all hyphens (-) in a phone number with a structure of "(2 to 4 digits)-(2 to 4 digits)-(4 digits)", specify as follows:

- [Regex]: -
- [Operations]: Select [Use Match Reference Function]
- [Text to Replace]: (space)
- [Replace All]: Select the check box

The conversion result is as follows:

0123456789

Example 3: Changing a document name from the "yyyymmddhhmmss" format to the "yyyymmdd" format

To delete part of the file name and keep only the date when the date and time the file was created are used for the file name, specify as follows:

- [Regex]: (.{8{)(.*)
- [Operations]: Select [Use Text Replacement Function]
- [Text to Replace]: $1
- [Replace All]: Select the check box

The conversion result is as follows:

20081112

Example 4: Extracting a specified part of the document name

To extract "2008" from the document name "extracted_20081110135026", specify as follows:

- [Regex]: (.*)(.{4})(.{10})
- Select [Ignore Upper/Lower Case Characters] and [Disregard Blank Space(s) and Symbol(s)]
- [Operations]: Select [Use Text Replacement Function]
- [Text to Replace]: $2
- [Replace All]: Select the check box

The conversion result is as follows:

2008

Image Correction

The Image Correction connector corrects images in a scanned document.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The following file formats are supported as input data for the Image Correction connector.

- TIFF (MH, single page/multiple pages)
- TIFF (MR, single page/multiple pages)
- TIFF (MMR, single page/multiple pages)
- TIFF (uncompressed, single page/multiple pages)
- TIFF-F (MH, single page/multiple pages)
- TIFF-F (MR, single page/multiple pages)
- TIFF-F (MMR, single page/multiple pages)
- DCX (single page/multiple pages)
- BMP (uncompressed)
- JPEG
- PNG
- GIF

Convertible formats (output data)

The following file formats are supported as output data for the Image Correction connector.

- TIFF (MH, single page/multiple pages)
- TIFF (MR, single page/multiple pages)
- TIFF (MMR, single page/multiple pages)
- TIFF (uncompressed, single page/multiple pages)
- DCX (single page/multiple pages)
- BMP (uncompressed)
- JPEG
- PNG
- GIF

Note

- Output data in TIFF-F format is not supported. When a TIFF-F file is input, it is output in TIFF format.

Use the following procedure to configure the properties of the Image Correction connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Image Correction] connector icon.**
2. **Specify Display Name.**

Barcode Separator/Index

The Barcode Separator/Index connector analyzes a barcode contained in a scanned document and saves it as metadata. Also, it can divide the document into separate files starting with the page that contains the same barcode.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**

Supported formats (input data)

The following file formats are supported as input data for the Barcode Separator/Index connector:

- TIFF
- TIFF-F
- DCX
- BMP
- JPEG
- PNG
- GIF

Note

- A barcode contained in a PDF or other application data cannot be recognized. When data in an unrecognizable format is input, an error occurs and the job is terminated regardless of the [Error Handling] setting.
- When a file in an unsupported format is entered, error code 53260015 and the message "Failed to create list of barcode properties information included in images" are recorded in the system log.

Recognizable barcode types

The following barcode types are recognizable by the Barcode Separator/Index connector:

1D barcodes	2D barcodes
Code39 Standard ASCII Code39 Extended ASCII Code128 EAN 8 / JAN 8 EAN 13 / JAN 13 Interleaved 2 of 5 Codabar (NW7) GS1(EAN)-128 Code 2 of 5	PDF417 DataMatrix QR

Note

- JAN 8 and JAN 13 are supported only when the log-in language is Japanese.

Barcode Separator/Index connector function

- This function scans and recognizes only the barcode on the first page in the first section of a scanned document. Barcodes on the second page or later in the first section or on the pages in the second section or later are not scanned. However, when [Continue Recognition Even When 1st Page Has No Barcode] is enabled in [General Settings], barcodes on the second page or later in the first section or on the pages in the second section or later are scanned.
- Barcodes in skewed images and barcodes that are reversed, at an angle, or at a right angle can be detected and scanned.
- Obtained barcode data can be delimited based on a preset format.
- Data obtained by delimiting can be stored as custom metadata.
- The obtained metadata can be used for processing with another RICOH Streamline NX connector.
- The tag name can be specified when the information is stored as metadata.

Dividing a Job for Processing

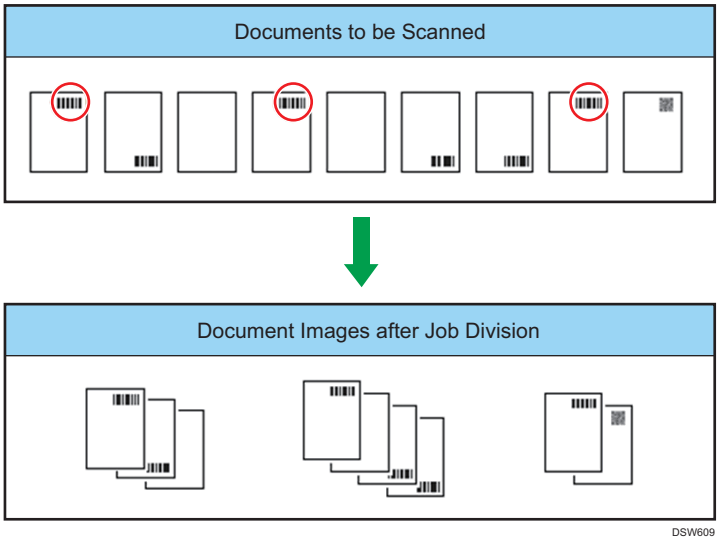
Normally, when you scan a multiple page document, all pages are handled as one job. The job division function of the Barcode Separator/Index connector can be used to divide a multiple page document and process it as multiple jobs.

When the job division function is used, each time the same barcode is scanned, the document is divided into a separate file starting with the page that contains the barcode.

- Job Dividing Example

  In this example, a nine-page document is scanned, and the job is divided by the same barcode that is located at the specified position at the top right. There are three barcodes of

the same value at the same specified location at the top right, and the nine-page document is divided into three jobs starting on the page containing the specified barcode.



Precautions on document orientation

The Barcode Separator/Index connector does not identify the top and bottom of the scanned document. Be sure to place the document in the correct orientation. For details about placing the document, see the user's guide of the device being used.

Depending on the orientation of the document, the position of the barcodes in the actual document may not match the position and coordinates of the barcode in the data scanned as an image.

To perform barcode recognition, register the barcode information for each barcode on the properties window of the Barcode Separator/Index connector. The registered settings are displayed in the list on the barcode information management window.

Use the following procedure to configure the properties of the Barcode Separator/Index connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Barcode Separator/Index] connector icon.**
2. **Specify Display Name.**
3. **In [Barcode Configuration], click [Add].**

   To edit the registered information, click [Edit].

   To delete registered information, select the information to delete, click [Delete], and select [Yes] on the confirmation window that appears.
4. **On the Properties window, register the barcode information.**

   When you use the job division function, the settings on the Properties window are used as the barcode information for job division.

5. Click [OK].

Note

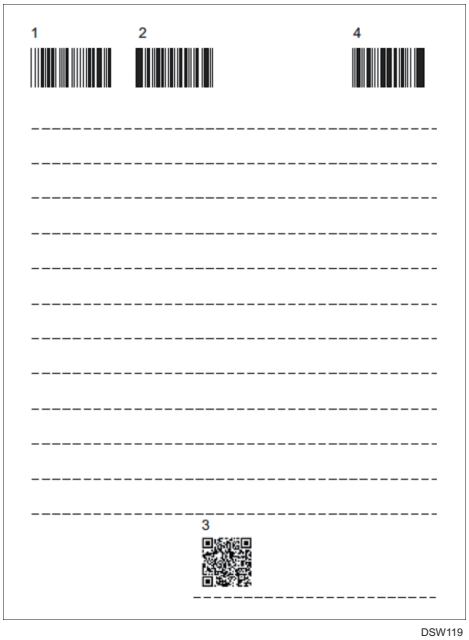
- For details about the setting items, see page 753 "Barcode Separator/Index".
- Depending on the setting of [Continue Recognition Even When 1st Page Has No Barcode], the value of LastResult_Barcode recorded in the metadata is as follows:

	Barcode on the first page	No barcode on the first page
When the check box is selected	Success	Success
When the check box is cleared	Success	Error

Specifying barcode numbers

This section describes how to specify barcode numbers when [Barcode Number] is selected in [Selection Method] on the Properties window.

- The top left corner of the scanned image is defined as coordinate (0,0).
- Determine the order by the coordinates of the upper left corner of each barcode.
- Compare the X coordinates, and order them starting with the smallest coordinate.
- When the X coordinate values are the same, order them starting with the smallest Y coordinate value.
- Assign numbers, as shown below, according to the number of specified barcode types.
  - When only one barcode type is specified
    Assign numbers only for barcodes of the specified type.
  - When multiple barcode types are specified
    Assign numbers for barcodes of all specified types.
  - When the barcode type is not specified
    Assign numbers to all barcodes.
- Example of barcode number specification
  The following figure shows an example of the number specification when four barcodes are located on one page.



DSW119

Measuring the barcode coordinates

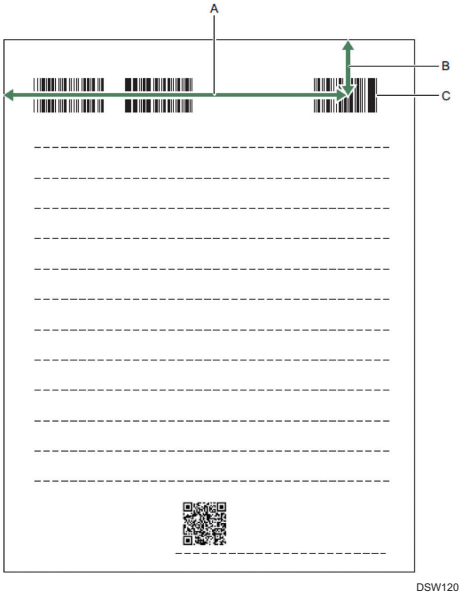
This describes how to measure the coordinates when [Rectangular Area] is selected in [Selection Method] on the Properties window.

- The top left corner of the scanned image is defined as coordinate (0,0).
- Measure the distance in the X and Y directions to the top left corner of the area for recognition.
- Measure the length of the area for recognition in the X and Y directions.
- Example of measuring the barcode coordinates
  The following is an example of measuring when the top right barcode is the target for recognition among the four barcodes on the document.

  A = Distance measured in the X direction

  B = Distance measured in the Y direction

  C= Barcode for recognition



Measuring the barcode area coordinates

This section describes how to measure the coordinates when [Rectangular Area] is selected in [Selection Method] on the Barcode Configuration window.

- The upper left corner of the scanned image is coordinate (0,0).
- Measure the distance in the X and Y directions to the upper left corner of the area for recognition.
- Measure the length of the area for recognition in the X and Y directions.
- Example of measuring the barcode coordinates
  The following is an example of measuring when the second from the left barcode is the target for recognition among the four barcodes on the document.

  A = Distance measured in the X direction

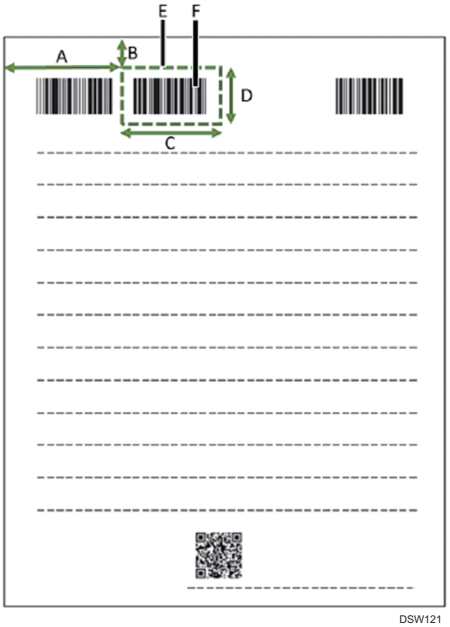
  B = Distance measured in the Y direction

  C = Length measured in the X direction

  D = Length measured in the Y direction

  E = Area for recognition

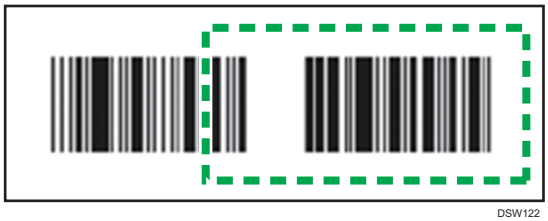
  F = Barcode for recognition



DSW121

Note

- When there is only one complete barcode in the area, the barcode can be recognized.
  - When the area is specified as shown below, only the complete barcode in the area on the right can be recognized.



DSW122

  - When the area is specified as shown below, because there is no complete barcode in the area, no barcode is recognized.

DSW123

  - When the area is specified as shown below, because more than one complete barcode is contained in the area, no barcode is recognized.

DSW124

Zone OCR

The Zone OCR connector recognizes the characters in a scanned document and extracts them as text.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**
- **To use the Zone OCR connector, create and register a Zone OCR form in advance. For details about creating a Zone OCR form, see page 338 "Configuring the Zone OCR Form".**

Note

- If there is a possibility that scanning cannot be performed properly, use the Image Correction connector to perform top and bottom identification as needed.

Supported formats (input data)

The following file formats are supported as input data of the Zone OCR connector.

- TIFF
- TIFF-F
- BMP
- JPEG
- PNG
- GIF

Use the following procedure to configure the properties of the Zone OCR connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the Zone OCR connector icon.**
2. **Specify the display name.**
3. **In [General Features], select the registration form.**

Note

- For the setting items on the [Zone OCR] tab, see page *757* "Zone OCR".

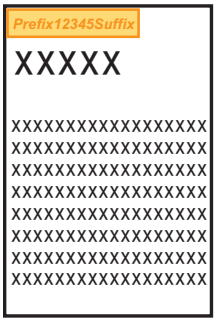
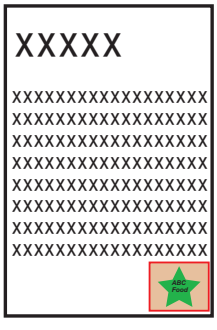
PDF Stamper

The PDF Stamper connector creates a PDF file with the specified text or image embedded. The stamp type can be selected from Bates Stamp, Image Stamp, Text Watermark, and Image Watermark.

Important

- **This connector can only be added to a workflow whose [Job Processing Location] is set to [On Server].**
- **To use the PDF Stamper connector, a PDF stamp must be registered in advance. For details about registering a PDF stamp, see page 345 "Registering a PDF Stamp".**

The following table shows output image samples using each stamp type:

Bates Stamp  A text stamp with counter	Image Stamp  An image stamp
Text Watermark  A text stamp as a watermark	Image Watermark  An image stamp as a watermark

Supported formats (input data)

The following file formats are supported as input data in the PDF Stamper connector:

- TIFF
- BMP

- PDF

However, the following data is not supported:

- BMP version 5
- Encrypted PDF document
- A TIFF image that matches any of the following conditions:
  - TIFF image with compression and multiple strips
  - TIFF image with tiles
  - TIFF image with more than 8 Bits per sample
  - TIFF 5.0-style LZW codes
  - TIFF image with extra samples
  - TIFF image with photometric 6

Note

- When an image that exceeds a vertical or horizontal size of 1250 mm is entered, an error occurs, and processing of the image is canceled.
- If an encrypted PDF file is passed to this connector, the conversion process fails and an error occurs.
- If a document in an unsupported format is passed to this connector, the process is skipped.
- If a PDF file is input via Monitor Folder connector, the version and additional functions of the PDF file such as tagged PDF are deleted.

Supported Formats (Output Data)

The following file formats are supported as output data in the PDF Stamper connector.

- PDF (version 1.4)

Limitations

- Only single-byte characters can be used for Bates stamp and watermark text.
- The PDF Stamper to embed the same type of Bates stamp can be placed only once in a tree-structured flow.
- To use the PDF Stamper for color documents, place the PDF Converter connector prior to the PDF Stamper in the delivery flow.
- To convert multiple jobs into a multiple page document and use the PDF Stamper for the document, place the Image Converter connector or PDF Converter connector prior to PDF Stamper in the delivery flow.
- When an error occurs in a workflow that includes a PDF Stamper specifying Bates Stamp, the counter number is as follows. The job is retried in any case:

- Even if the PDF Stamper fails to embed the counter number, the counter number increases when the counter can be updated on the Core Server. In this case the counter number for the failed embedding attempt has a missing number.
- In all other cases, such as when the counter cannot be updated on the Core Server, the counter number does not increase.

- The counter number to be added when Bates Stamp is selected is added in the order the jobs are processed and not in the order the documents are read. Therefore, when the PDF Stamper settings are shared with multiple workflows or devices, a serial number is added for jobs read on the same device and jobs thereafter. To add serial numbers in the order jobs are read by a device, configure the individual workflows with PDF Stamper configured for each device.

Use the following procedure to configure the properties of the PDF Stamper connector:

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [PDF Stamper] connector icon.**
2. **Specify the display name.**
3. **In [PDF Stamper Settings], configure the stamp to use.**

Note

- For the setting items on the [PDF Stamper] tab, see page 758 "PDF Stamper".

Decision Point

Use the Decision Point connector to determine the job process to be performed in the workflow based on preset rules.

Supported formats (input data)

The Decision Point connector supports all formats compatible with RICOH Streamline NX.

Convertible formats (Output data)

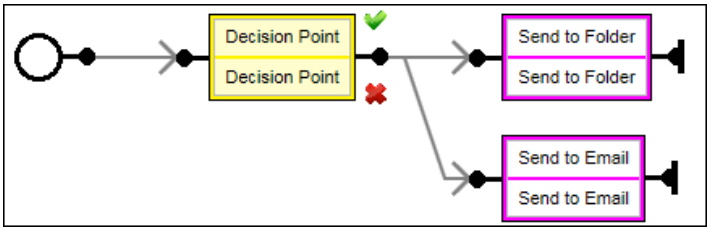
The output data format is the same as the input data.

Use the following procedure to configure the properties of the Decision Point connector.

1. **Navigate to the [Workflow Design] tab and [Delivery Flow] tab, and click the [Decision Point] connector icon.**
2. **In [Rule Definition], configure the conditions under which the flow redirect rules are applied.**

   For details about setting conditions, see page 201 "List of conditions".

3. **The workflow will proceed with the upper flow when the condition is evaluated as "true", and the lower flow when the condition is evaluated as "false".**



Note

- Up to two redirects can be configured for each Decision Point connector. If more than two redirects are required, position multiple Decision Point connectors.
- At least one destination connector must be positioned at each redirect and the parameters are specified for all destination connectors.

List of conditions

The following is a list of conditions that can be specified. Multiple conditions can be combined together. When multiple conditions are set, configure [Match All], [Match Any], or [Match None].

The Decision Point connector uses for comparison purposes the metadata specific to the destination connectors positioned prior to the Decision Point connector as well as the metadata specified for the workflow.

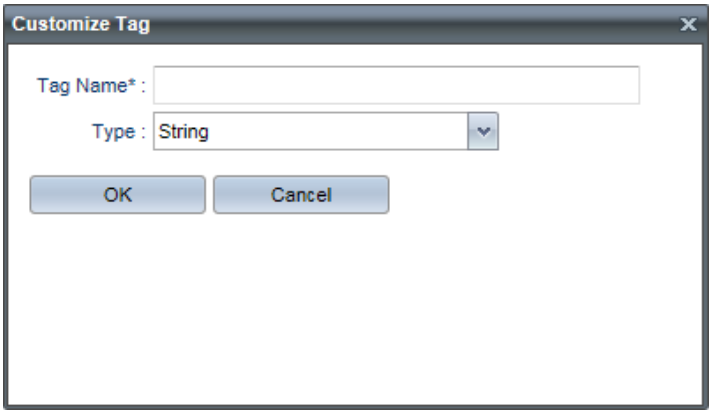
For details about the metadata specific to destination connectors, see page 360 "Exposed Metadata of Destination Connectors".

Metadata Type	Comparison method	Description
Number	equals/less than/greater than	Number type metadata is compared to the specified value.
String	equals/starts with/ends with/contains/Regex	String type metadata is compared to the specified string.
Date	less than/greater than/ between	Date type metadata is compared to the specified date.
Time	less than/greater than/ between	Time type metadata is compared to the specified time.
Boolean	equals	Boolean type metadata is compared using the check box status (checked or unchecked). Being checked is evaluated as "true", and being not checked is evaluated as "false".

Metadata Type	Comparison method	Description
Lit<String>	equals/starts with/ends with/contains/Regex	List<String> type metadata is compared to the specified string. If at least one string matches, it is evaluated as "true".

When using the custom metadata as the condition

1. Click [Customize Tag].
2. Specify the custom metadata, and then click [OK].



Item	Description
Tag Name	Enter the valid metadata tag manually For details about the valid metadata, see page 348 "Metadata".
Type	Select the type of the metadata from the drop-down list.

Customizing the Settings on the Operation Screen of the Device

The delivery flow configured in the Management Console is executed after the user configures several items other than one-touch scan on the operation screen of the device. Configure the setting items, including the values displayed as the default values, the display positions, and whether to show or hide the values, and customize the actual screen operated by the user at the time of delivery.

In addition to the destination connectors and process connectors positioned in the delivery flow, you can also configure the [Scan Settings], [Scan Size] and [OCR Scanned PDF] windows.

Destination connectors

- All destination connectors

Process connectors

- PDF Converter
- PDF Converter (Enhanced)
- OCR
- Section Specify
- Section Splitter
- Image Correction
- Barcode Separator/Index

On the [Workflow Design] tab, select and configure the [Destination] tab or [Process] tab to display on the connector tab that you want to use for customizing the operation screen.

Note

- You cannot customize the Shared Connectors screen.

Overview of the Settings Windows

This section describes an overview of the settings windows of the [Destination] and [Process] tabs and also provides examples of the Send to Email connector window.

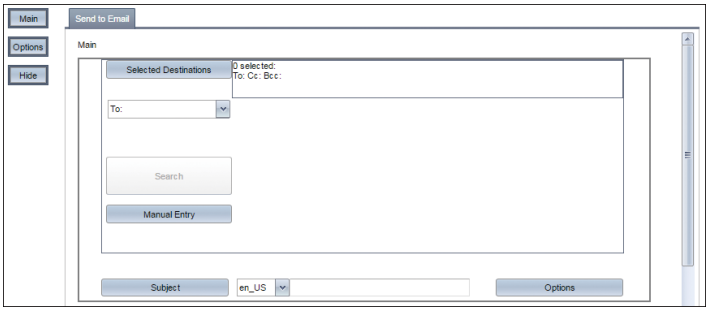
The settings windows of the [Destination] and [Process] tabs are divided into the following three panes. Move the scroll bar on the right side of the window up or down or click [Main], [Options], [Hide] on the left side to display the individual panes.

- General Features pane
- [Option Screen]
- [Hidden Items (Preset)] pane

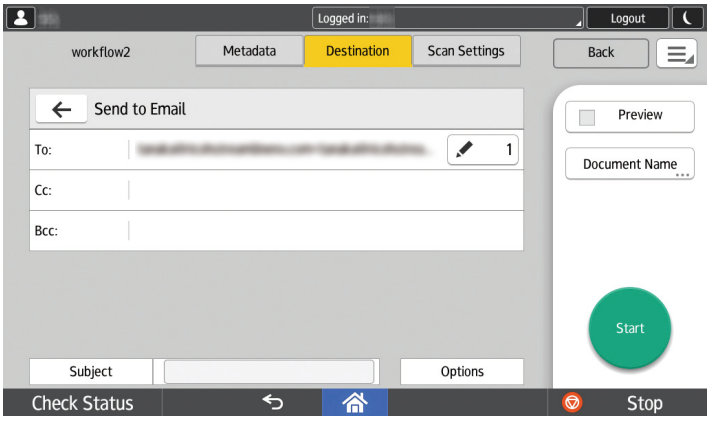
General Features pane

Configure the settings that are initially displayed when the Destination Connector or Process Connector button is pressed on the operation screen of the device. Those include the major setting items related to the connectors.

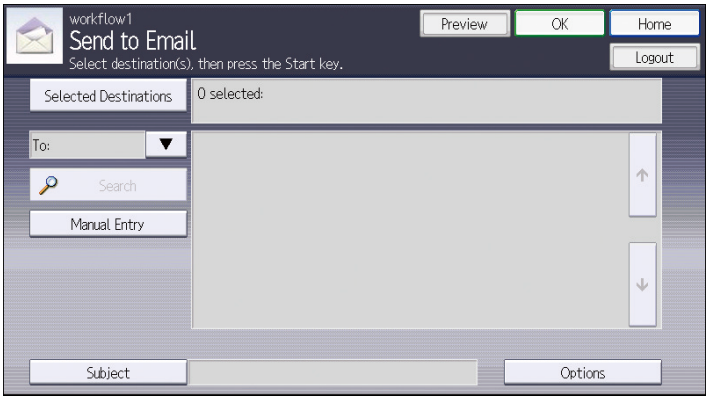
For example, you can configure the destination input and search settings on the General Features pane for Send to Email.



- Display on the operation screen of the device (Smart Operation Panel)

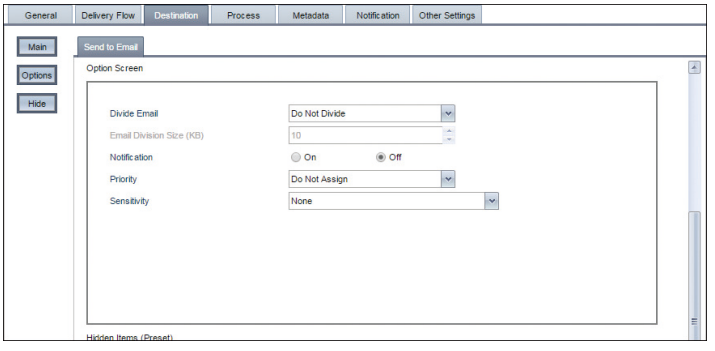


- Display on the operation screen of the device (Standard Operation Panel)

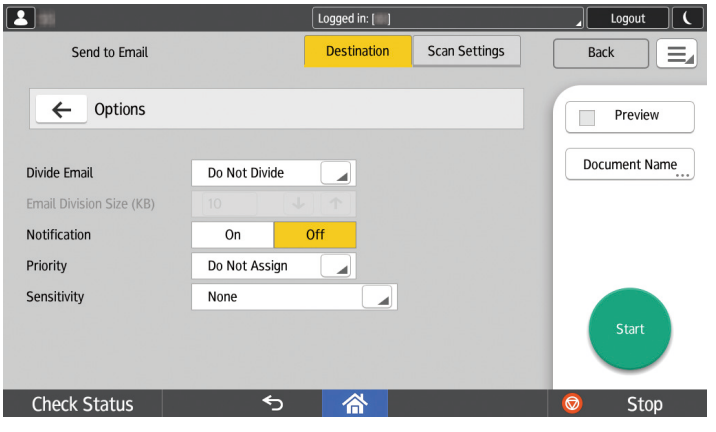


[Option Screen]

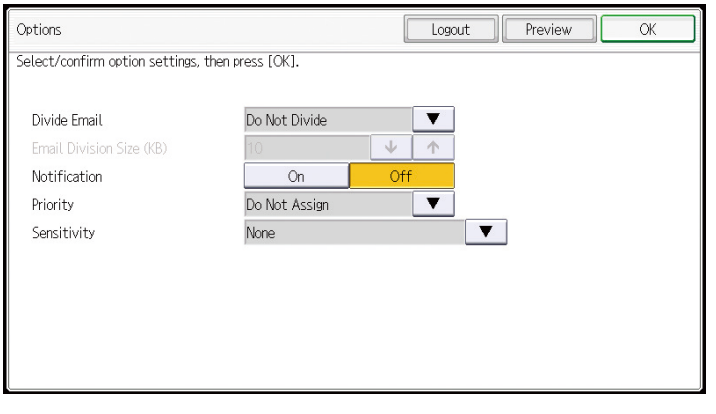
Configure the settings displayed when the [Options] button is pressed on the operation screen of the device. [Option Screen] is available only for the Send to Email and Send to Exchange connectors.



- Display on the operation screen of the device (Smart Operation Panel)

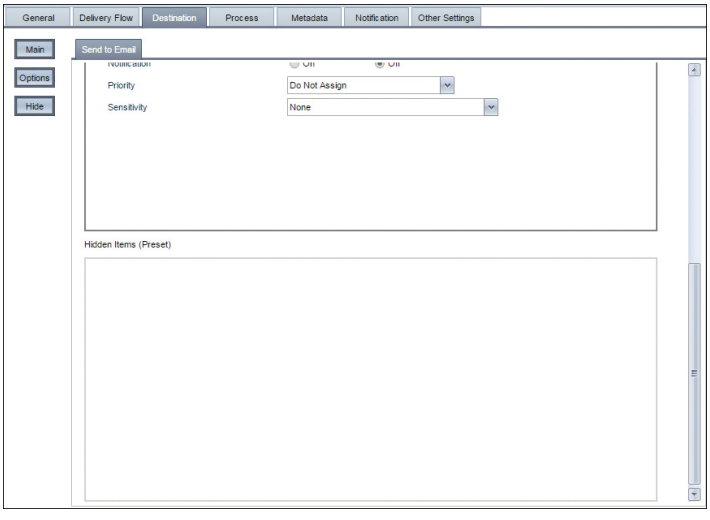


- Display on the operation screen of the device (Standard Operation Panel)



[Hidden Items (Preset)] pane

The setting items of [Hidden Items (Preset)] pane are not displayed on the operation screen of the device. Because the settings are used in the delivery flow, they must be set in advance.



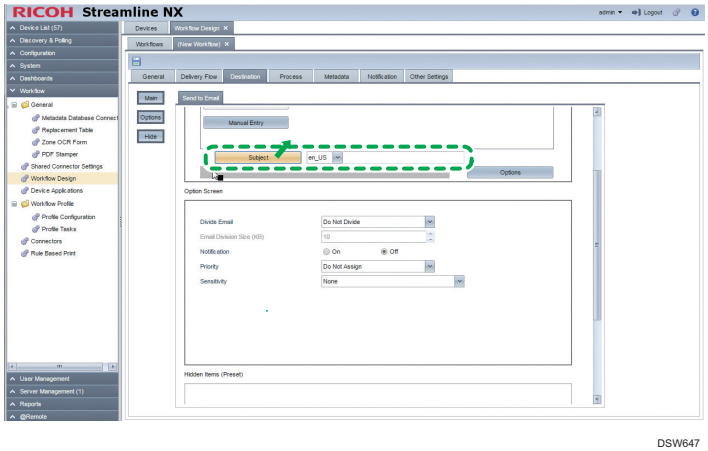
Operating in the Settings Windows

This section describes the operations that are common to the settings windows for all connectors.

Changing the display positions of the setting items

You can change the position of a setting item for easier access.

Select the item whose position you want to change, and drag and drop it to a new position.



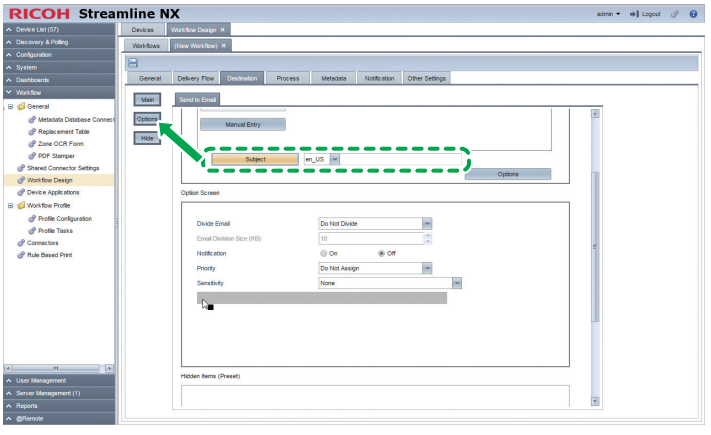
DSW647

Moving a setting item on the General Features pane to the [Option Screen]

You can move items whose settings are less frequently changed to the [Option Screen].

The moved setting items can be displayed by simply pressing [Options]. The changes to the setting can then be made.

To move an item, select the item, and drag and drop on [Options] in the top left section of the window.



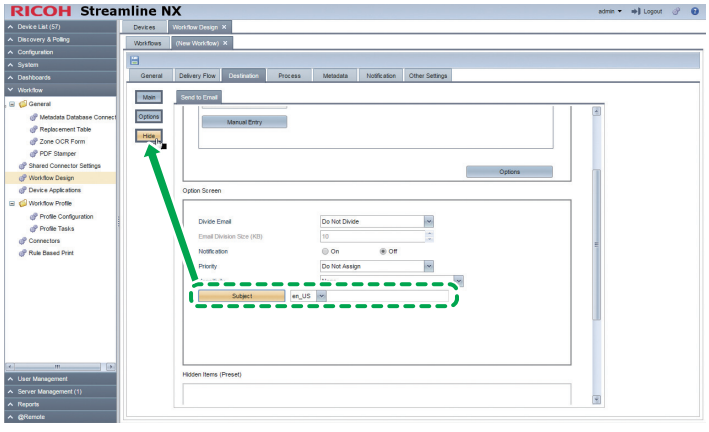
DSW648

The moved item is now displayed in the [Option Screen].

Hiding the setting items

To prevent changes from being made to the settings on the operation screen of the device, configure the setting items in advance, and then move the items to [Hidden Items (Preset)] pane. The items moved to the pane are not displayed on the configuration screen of the device, and the user can no longer change those settings.

Configure the items in advance, and drag and drop the items on [Hide] in the top left section of the window.



DSW649

To show a hidden item, select the item, and drag and drop it on [Main] or [Options] in the top left section of the window, and then use General Features pane or [Option Screen] to adjust the display position.

Note

- When hiding an item, be sure to first configure the value.
- If all items are hidden, the following are displayed on the operation screen of the device:
  - Destination connectors
    When the Smart Operation Panel is being used, the connector buttons are hidden.

    When the Standard Operation Panel is being used, the connector buttons (e.g., Send to Email on the Service Menu screen) are not available (grayed out).
  - Process connectors
    When the Smart Operation Panel is being used, the setting items of Scan Settings are grayed out.

    When the Standard Operation Panel is being used, [Scan Settings] is not available (grayed out).

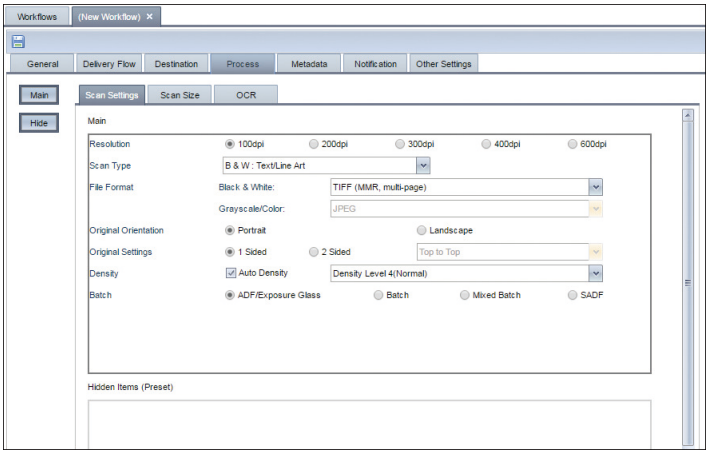
Configuring the default values

When the values of the setting items are specified on the General Features pane, [Option Screen], and [Hidden Items (Preset)] pane, the values are displayed as the default values on the operation screen of the device. The user can change the settings on the operation screen of the device.

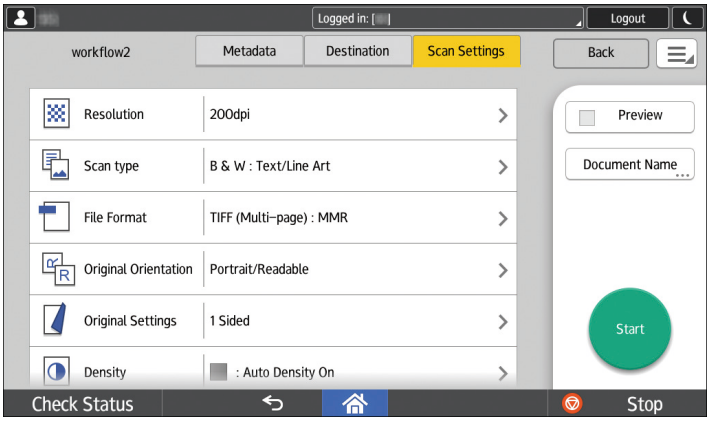
Customizing the [Scan Settings]

The scan settings include the resolution, file format, and document side, and these parameters are applied to a document when scanning. The [Scan Settings] tab is automatically added to all new workflows.

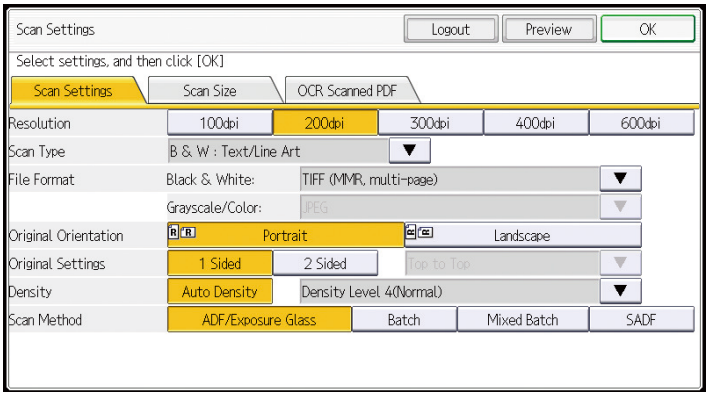
- [Scan Settings] tab of the Management Console



- Display on the operation screen of the device (Smart Operation Panel)



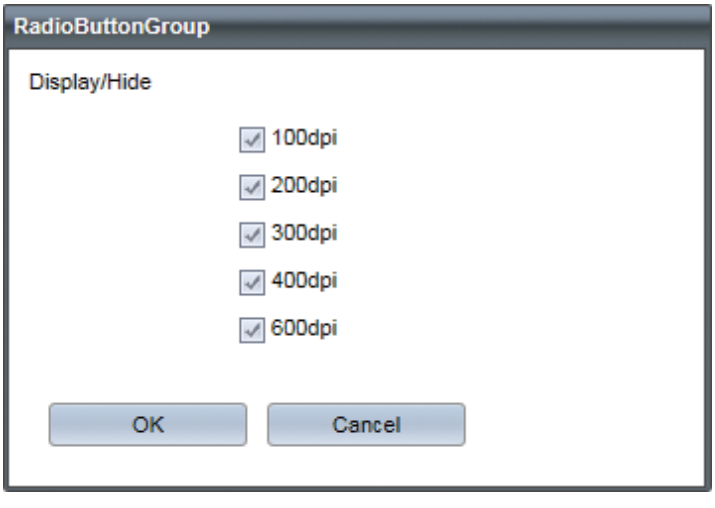
- Display on the operation screen of the device (Standard Operation Panel)



Restricting the settings

You can restrict the values that the user can select with [Scan Settings].

On the [Scan Settings] tab of the [Process] tab, right-click [Resolution], [File Format], or other setting items, and click [Edit Display/Hide Properties] to display the selection window for the settings.



Select only the settings to be displayed on the configuration screen of the device, and click [OK].

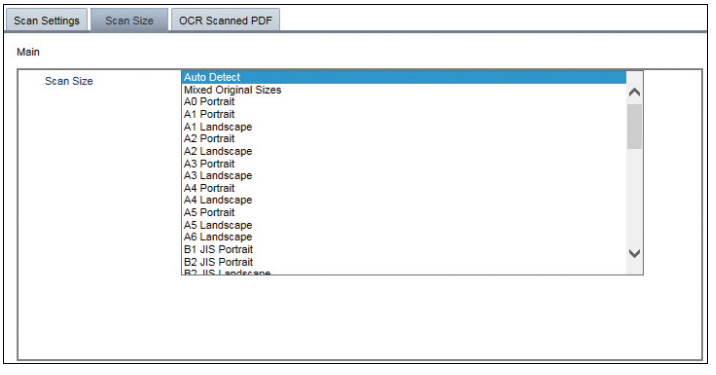
Note

- The setting items can be hidden on the screen. When the setting item is set to Hide, it is grayed out on the Smart Operation Panel, and it is not displayed on the Standard Operation Panel.
- The only scan settings that can be used are the functions the target device supports. If the device does not support the settings, the initial values of the device are applied.
- For details about the configuration items, see page 678 "Scan Settings".

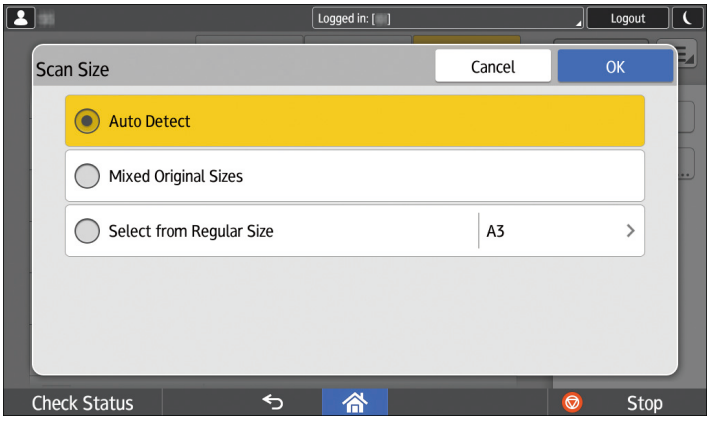
Customizing [Scan Size]

Use [Scan Size] to configure Auto Detect, Mixed Original Size, or any of the document sizes. The [Scan Size] tab is automatically added to all new workflows.

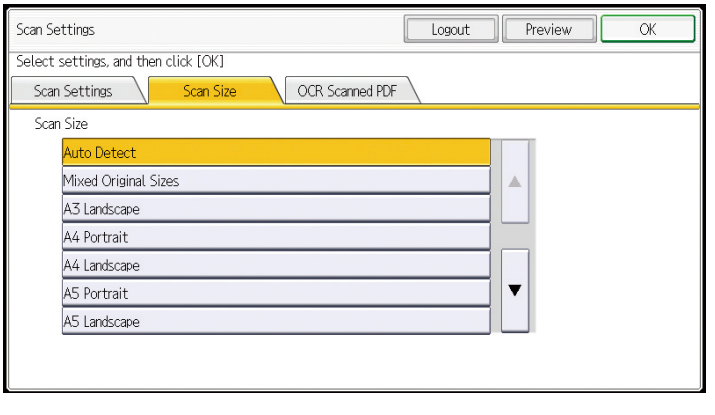
- [Scan Size] tab on the Management Console



- Display on the operation screen of the device (Smart Operation Panel)

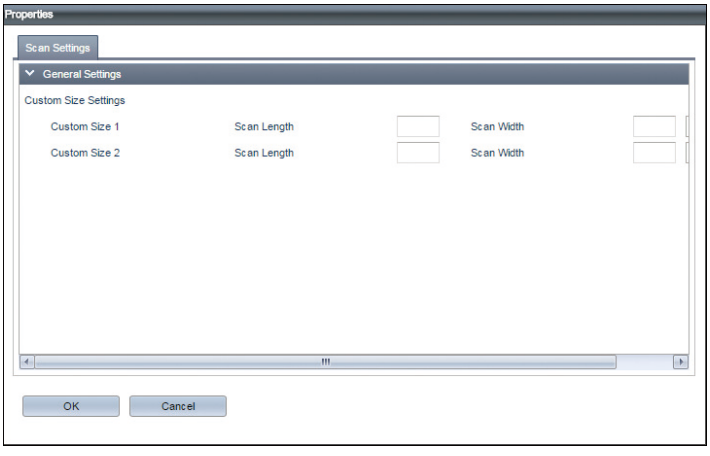


- Display on the operation screen of the device (Standard Operation Panel)



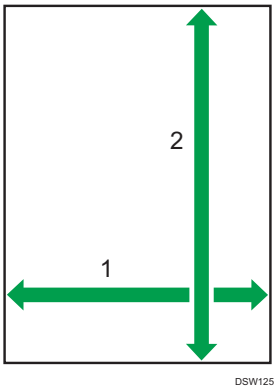
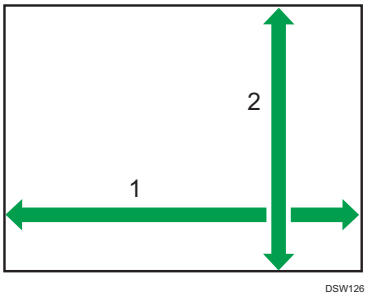
Configuring custom sizes

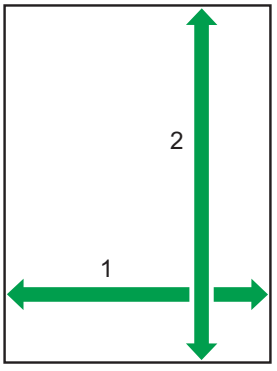
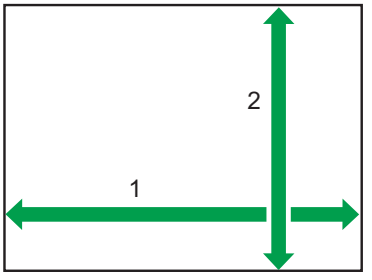
To configure a custom scan size, double-click the [Scan Size], [Scan Settings] or [OCR Scanned PDF] tab.



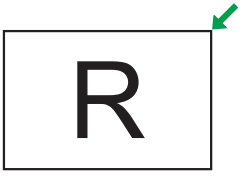
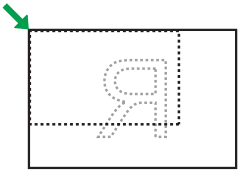
The value specified for [Custom Size] [1] or [Custom Size] [2] is displayed in Default Scan Size.

For [Scan Length] and [Scan Width], see the following table.

Scan direction of automatic document feeder (ADF)	When document direction is portrait	When document direction is landscape
←direction	 DSW125 1. Scan length 2. Scan width	 DSW126 1. Scan length 2. Scan width

Scan direction of automatic document feeder (ADF)	When document direction is portrait	When document direction is landscape
↑ direction	 1. Scan width 2. Scan length	 1. Scan width 2. Scan length

The starting point of the custom paper varies depending on the scanning method. See the following table for details:

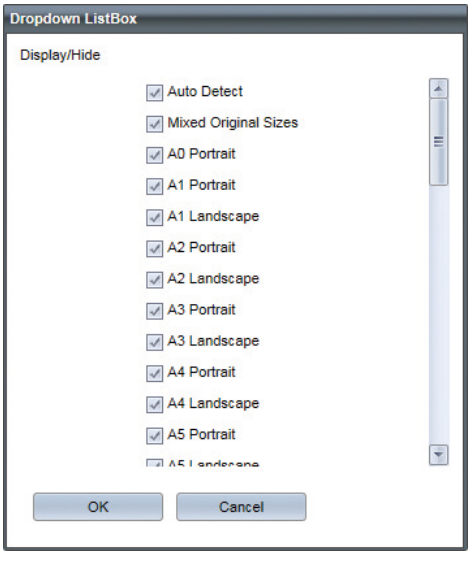
Scan type	Starting point
When using the exposure glass Top right of the document	 

Scan type	Starting point
When using the ADF to adjust both the scan length and width Center of the document landscape direction (The document landscape direction is perpendicular to the scan direction.)	
When using the ADF to adjust either the scan length or width Top left of the document	

Restricting the settings

The scan sizes that the user can select can be restricted according to the functions of the target device.

On the [Scan Size] tab of the [Process] tab, right-click a scan size setting and select [Edit Display/Hide Properties] to display the scan size properties window.



Select the check boxes for the scan size settings to be displayed on the configuration screen of the device, and click [OK].

Note

- [Scan Size] can be hidden on the screen. When this item is set to Hide, the [Scan Size] tab is not displayed on the Standard Operation Panel, and [Scan Size] on the [Scan Settings] window is grayed out on the Smart Operation Panel. The user cannot change the values of the scan settings that are configured in advance by the administrator in the Management Console.
- The only scan sizes that can be used are the sizes the target device supports. If the device does not support the setting, the Scan Size window is displayed with Auto Detect selected. If the device does not support Auto Detect, A4 Landscape is selected.
- For details about the setting items, see page 682 "Scan Size".

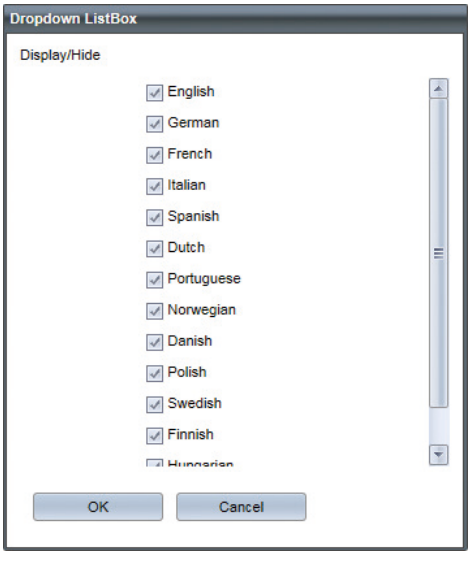
Customizing the [OCR Scanned PDF] Settings

Configure [OCR Language] and [Blank Page Sensitivity] under [OCR Scanned PDF]. The [OCR Scanned PDF] tab is automatically added to every new workflow.

Restricting the setting values

You can restrict the values that the user can select with [Scan Settings].

On the [OCR Scanned PDF] tab of the [Process] tab, right-click [Remove Blank Pages], [OCR Language], or other setting items, and then click [Edit Display/Hide Properties] to display the selection dialog box for the settings.



Select the check boxes for the values to be displayed on the configuration screen of the device, and click [OK].

Note

- You can hide [OCR Scanned PDF] on the screen. When this item is set to Hide, the [OCR Scanned PDF] tab is not displayed on the Standard Operation Panel, and [OCR Scanned PDF] on the [Scan Settings] window is grayed out on the Smart Operation Panel.
- The setting items on the [OCR Scanned PDF] become valid only when the device is installed with the OCR dictionary.
- For details about the configuration items, see page 683 "OCR Scanned PDF".

Configuring Items in Metadata

The metadata in a document to be delivered can contain the following metadata items: basic metadata items that are defined by the system automatically and custom metadata items that are configured by the administrator.

Configure the custom metadata items on the [Metadata] tab of [Workflow Design] tab.

Using the [Metadata] Tab

Use the Metadata tab screen to configure the custom metadata items that you want to add to the document to be sent using the currently configured workflow.

The following items can be specified for each metadata item:

- Display Position

  The items are displayed in the same order on the operation screen of the device and mobile device as the order displayed in the Management Console. You can change the display order by dragging and dropping items.

- Display/Hide

  You can specify whether or not to display a metadata item on the screen of the device or mobile app. To hide a metadata item, specify a setting value for the item. The specified setting value is used as the preset value, and the user cannot change the value of a hidden item from the device or mobile device.

- Default Value

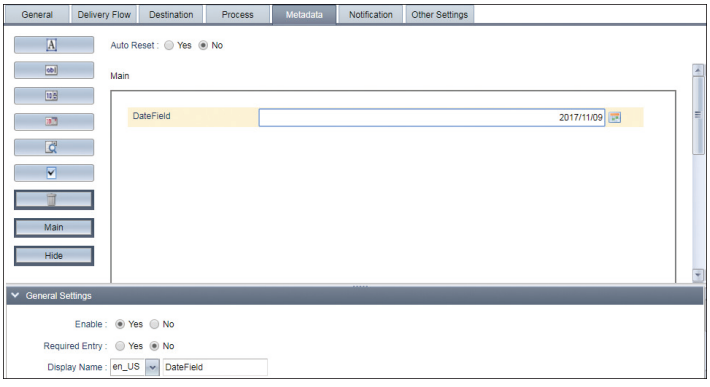
  Values specified on the [Metadata] tab appear as default values on the operation screen and mobile device. The user can change these values as necessary.

Note

- For details about metadata, see page 348 "Metadata".

Understanding the [Metadata] tab layout

The following shows the layout of the [Metadata] tab and describes the functions.



1. **Input element list edit screen**

   Select an input element such as a text box or drop-down menu from the list according to the specified method of the metadata item, and add the element to the layout screen. You can also delete and specify whether to display or hide the input element that has been added to the metadata entry screen.

2. **Metadata entry screen**

   Drag and drop the input element selected in the input element list on the metadata entry screen to edit the layout of the screen to be displayed on the operation screen of the device.

3. **General Settings**

   Configure the properties of the input element arranged on the metadata entry screen. Specify the display name, metadata to be configured, selection items to be displayed, and other settings.

Editing the metadata entry screen

Use the following procedure to edit the metadata entry screen:

1. **From the list, select an input element according to the method for specifying the metadata item to be added.**

   You can select from the following input elements:

   - (Label)
     You can add a preset text such as a message or description to the metadata screen.
   - (InputText)
     You can add a metadata item in string format.
   - (NumberStepper)
     You can add a metadata item in integral number format.
   - (DateField)
     You can add a metadata item in date format.
   - (Drop-down menu)
     You can add a drop-down menu that has values in a CSV or SQL file or values manually entered as selection items. For details about configuring a drop-down menu, see page 310 "Configuring a drop-down list".

- (Check box)
  You can add a metadata item in the form of a check box.

2. **To require entry of a metadata item specified in the positioned input element, select [Yes] in [Required Entry Item] on the [General Settings] screen.**
3. **In [General Settings] and [Dropdown ListBox], specify the other properties.**

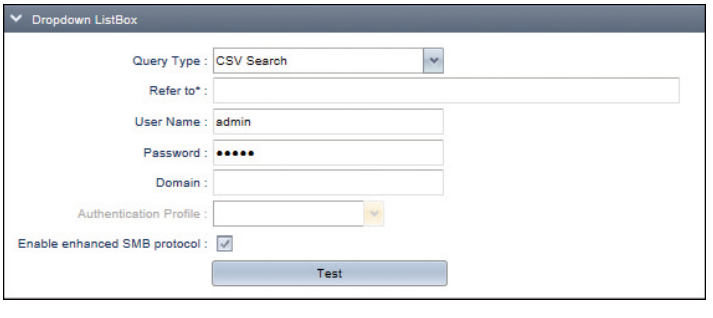
Note

- When [Yes] is selected for [Auto Reset], all metadata items resume their default values when scanning is complete. However, the metadata items are not reset when:
  - delivering from a smart device;
  - scanning has failed.
- For the setting items in the properties of the input elements, see "[Metadata] Tab", page 589 "Workflow Design".
- The number of characters that can be displayed on the device's operation panel may be fewer than what can be entered in the fields on the [Metadata] entry screen of the Management Console. In this case, the characters that cannot be displayed are omitted and "..." is displayed instead.
- When using the Standard Operation Panel, you can display up to seven input elements per screen on the operation screen of the device. A separator is automatically added as necessary in the Management Console.
- Up to 50 input elements can be displayed on the metadata screen of the device. Of these 50 input elements, only 21 can be placed on the General Features screen (seven input elements per screen on three screens).

Configuring a drop-down list

Use the following procedure to configure a drop-down list:

When [Query Type] is set to [CSV Search]



- Enter the UNC path in [File Name] to specify a CSV file. The system supports files with the ".csv" and ".CSV" extensions.
- You cannot use a local file path for a workflow when the [Job Processing Location] is set to [On Device].

- Entering a [User Name] and [Password] is optional. When you have not entered these items, the system uses the service account on the Delegation Server to access the CSV file.
- When you have not entered the domain, the system uses the domain of the profile selected in [Authentication Profile]. When you have not specified [Authentication Profile], the system does not use the domain.
- You can specify a domain name in [User Name] by using the following formats:

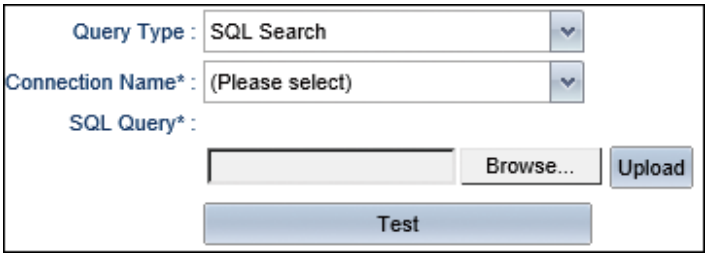
  - DomainName/UserName

  - UserName@DomainName

  If you specify a domain name in [User Name], the domain name specified in [Domain] is ignored.
- "\" and "@" cannot be used for a user name or a domain name.
- The system supports both NTLMv2 and Kerberos as the authentication method. To use Kerberos Authentication, specify the profile to be used in [Authentication Profile]. When the [Enable enhanced SMB protocol] check box is selected, [Authentication Profile] cannot be specified. In this case, Kerberos authentication is always used when Kerberos authentication is enabled. Otherwise, NTLM authentications used.
- When the [Enable enhanced SMB protocol] check box is selected, CSV search is executed using the SMB3.0 protocol. When it is cleared, the SMB1.0 protocol is used.

  [Enable enhanced SMB protocol] is not displayed for a workflow when [Job Processing Location] is set to [On Device]. The SMB1.0 protocol is used for CSV search executed on devices.
- When a workflow configured using RICOH Streamline NX v3.0.2 or older version is imported, the [Enable enhanced SMB protocol] check box is cleared.
- Click [Test] to check that the settings have been configured correctly. An error message is displayed if the specified CSV file cannot be accessed.

When [Query Type] is set to [SQL Search]



- You can select [SQL Search] only in a metadata item of a workflow when the [Location] setting is set to [Server].
- The database connector configured in advance in [Metadata Database Connection] is displayed in [Connection Name]. For details about the settings of [Metadata Database Connection], see page 333 "Configuring the Metadata Database Connection".

- Click [Browse] to select the SQL file to be used, and then upload the file. The system supports files with the ".sql" extension.
- Click [Test] to check that the settings have been configured correctly. An error message is displayed if the database cannot be accessed or the SQL statement is invalid.
- When setting a query string, specify input elements of the same data type for comparison. An error will occur due to a comparison failure if you specify input elements of data types that do not match.

  You can define the metadata items for the following input elements and data types:

Input element	Data type	Description
InputText	char, nchar, varchar, nvarchar	Enter manually
DateField	date	Select from a calendar or enter manually
NumberStepper	int, bigint	Enter manually or select from a list
Dropdown ListBox	char, nchar, varchar, nvarchar	Enter manually (when editable) or select from a list
Checkbox	boolean	Select or clear a check box

About Metadata Interdependence

You can use the metadata interdependence function to narrow down the selection items for custom metadata dynamically according to the value specified in another field. To use the interdependence function, use [ ] to enter the tag name of the metadata item to be referenced in the SQL statement that is assigned to the target drop-down list.

Example:

SELECT DISTINCT NAME FROM MEMBER WHERE MEMBER.DEPT = [DEPARTMENT]

When the SQL statement shown above is assigned to the field whose tag name is MEMBER, you must specify the value to be inserted to [DEPARTMENT] of the SQL statement in the field whose tag name is DEPARTMENT. An error occurs if the MEMBER field is specified without specifying a value in the DEPARTMENT field.

You can define the interdependence of metadata items for the following input elements and data types:

Input element	Data type	Description
InputText	String	Enter manually

Input element	Data type	Description
DateField	Date	Select from a calendar or enter manually
NumberStepper	LONG type	Enter manually or select from a list
Dropdown ListBox	String	Enter manually (when editable) or select from a list
Checkbox	Boolean	Select or clear a check box

Note

- Do not use a SQL identifier or reserved word, or the column name contained in a SQLDB instance as the metadata tag name entered in a SQL statement. Otherwise, a malfunction will occur in SQL search.
- Do not use [or] in a SQL statement except when describing a tag name of a metadata item.
- Do not reference a tag name of a metadata item that is not defined on the Metadata tab. Otherwise, an execution error will occur.
- The SQL statement specified in a .sql file only allows a SELECT statement.
- A value is not displayed on the drop-down menu if the query returns NULL.
- The value in the leading column is displayed on the drop-down menu if the query returns values in multiple columns.

When [Query Type] is set to [Manual Entry]

- Enter a value directly in [Option].
- Press the Enter key to start a new line, and then enter the next value.

Note

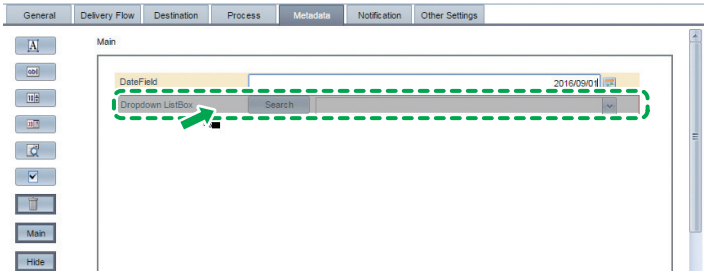
- You can add up to 50 values.

Changing the display order of input elements

Input elements will appear on the operation screen of the device in the order specified on the metadata entry screen.

Use the following procedure to change the display order:

1. **Select the input element to be moved, and then drag and drop the item to the desired position.**



DSW650

Hiding an input element

You can configure an input element to be hidden on the operation screen of the device. This functionality is useful when you want to add certain metadata in every document that does not need to be specified by the user. Configure the value for the input element to be hidden in advance.

1. **On the metadata entry screen, configure the preset values for the input element to be hidden.**
2. **Select the display name of the input element to be hidden, and then drag and drop the item to the hidden item (preset) field or** Hide.

Note

- To display a hidden entry element, select the display name of the input element, and then drag and drop the item to Main.

Deleting an input element

Use the following procedure to delete an input element:

1. **Select the display name of the input element to be deleted, and then drag and drop the item to (Trash).**

Configuring the Notification Function

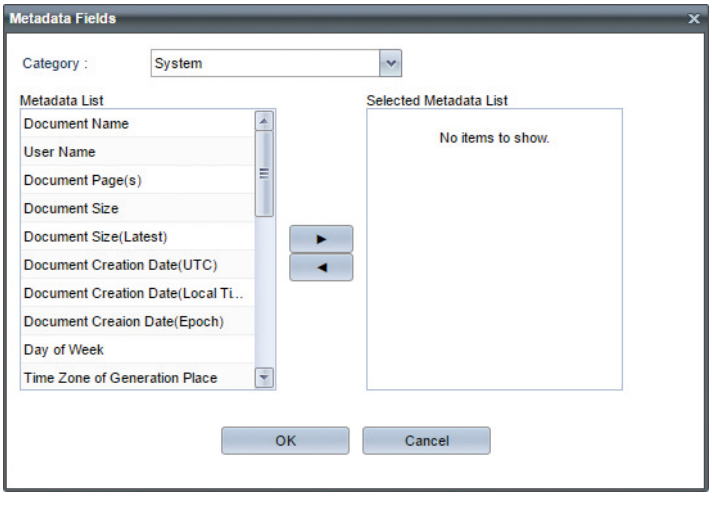
Specify when and where to send notifications and the metadata to be included in notifications.

1. **On the [Workflow Design] tab, click [Notification] tab.**
2. **Select the [Enable Notification] check box.**

   To disable the notification function, clear the check box.
3. **In [Notification Settings], specify the trigger for sending notification, destination, language to use in the notification e-mail, and e-mail server.**
4. **In [Add/Delete Metadata Field], select the check boxes of the metadata elements to be included in the notification.**

   If the metadata to be included is not on the list, use the following procedure to add the metadata element.

   1. In [Add/Delete Metadata Field], click [Add].
      The [Metadata Fields] window is displayed.



   2. Select the category of the metadata tag from the [Category] drop-down list.
   3. In [Metadata List], select the metadata element to add, and click ►. To remove an element, select the metadata element in [Selected Metadata List], and click ◄.
   4. Repeat Steps 1 and 3 to add more metadata elements as necessary.
   5. Click [OK].

Note

- For the setting items on the [Notifications] tab, see page 589 "Workflow Design".

Configuring Other Settings

Specify the default document name that appears when scanning a document, the items displayed on the [Scan Settings] window, and whether or not to display the preview window.

1. **Click the [Other Settings] tab on the [Workflow Design] tab.**
2. **Specify the default document name, the items displayed on the [Scan Settings] window, and the preview screen display setting.**

Note

- For the setting items on the [Other Settings] tab, see page 589 "Workflow Design".

Creating a Shared Connector

Although a destination connector or process connector can be configured each time it is added to the delivery workflow, those connectors can be configured as the shared connectors at the system level and used as the shared settings to simplify the configuration process of a workflow.

When a destination connector or process connector is added to the delivery workflow, the administrator can select and add either a local connector that is not preset or a shared connector.

Creating a New Shared Connector

Note

- To create a new shared connector based on an existing shared connector, see page 318 "Editing a Shared Connector".

1. **Click the following items in the navigation tree to open the [Shared Connector] tab.**

   [Workflow] ▶ [Shared Connector]

2. **Click (Add).**
3. **Enter the shared connector name in [Shared Connector Name].**
4. **Enter the shared connector description in [Description].**
5. **Select the category of the connector from the [Connector Category] drop-down list.**
6. **Select the job processing location from the [Location] drop-down list.**
7. **Select the type of the connector from the [Connector Type] drop-down list.**
8. **Click [OK].**
9. **On the [Settings] tab, configure the properties according to the type of the selected shared connector.**

   For details about configuring the properties of the destination connector, see page 240 "Configuring the Properties of the Destination Connector".

   For details about configuring the properties of the process connector, see page 260 "Configuring the Properties of a Process Connector".

10. **On the [Preset] tab, configure the setting items, layout, and display method according to the type of the selected connector.**

    For details about configuring the settings, see page 294 "Customizing the Settings on the Operation Screen of the Device".

11. **Click (Save).**

Note

- For details about the setting items on each tab, see page 588 "Shared Connector Settings".

Editing a Shared Connector

You can edit the properties of the existing shared connectors, or create a new one based on the existing one.

1. **Click the following items in the navigation tree to open the [Shared Connector] tab.**

   [Workflow] ▶ [Shared Connector]

2. **Select the shared connector to edit.**
3. **Change the settings.**

   For details about configuring the settings, see page 317 "Creating a New Shared Connector".

4. **Click (Save).**

Note

- You cannot change the category or type of the connector on the [General] tab.

Deleting a Shared Connector

1. **Click the following items in the navigation tree to open the [Shared Connector] tab.**

   [Workflow] ▶ [Shared Connector]

2. **Select the shared connector to delete, and click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- You cannot delete a shared connector being used in a workflow. Use the [Workflow] tab to view the workflows that are using the connector.

Configuring Device Applications

Device Applications can also be added to a workflow profile group. To add a Device Applications, the application must be configured in [Device Application] in advance.

Note

- When the Smart Operation Panel is being used, the Device Applications are always displayed on the home screen of the device.
- The available Device Applications vary depending on the model of the device.

Adding Device Applications

1. **Click the following items in the navigation tree to open the [Device Application] tab.**

   [Workflows] ▶ [Device Application]

2. **Click (Add).**

   To create a new Device Applications based on an existing Device Applications, select the application to be copied, click (Copy). Then select the copied application in the application list.

3. **On the [General] tab, configure the Device Applications properties.**
4. **Click (Save) on the application list.**

Note

- For details about the setting items on each tab, see page 597 "Device Applications".

Editing Device Applications

1. **Click the following items in the navigation tree to open the [Device Applications] tab.**

   [Workflows] ▶ [Device Applications]

2. **Select the Device Applications to edit.**
3. **On the [General] tab, change the settings.**

   For details about changing the settings, see page 319 "Adding Device Applications".

4. **Click (Save) in the application list.**

Note

- You cannot change [Application Type].

Deleting Device Applications

1. **Click the following items in the navigation tree to open the [Device Application] tab.**

   [Workflows] ▶ [Device Application]

2. **Select the application to delete, and click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- You cannot delete a Device Applications being used in a profile. You can use the [Profile] tab to view the profile using the application.

Configuring a Workflow Profile

To use the RICOH Streamline NX delivery function, configure a workflow profile that combines a workflow created in advance and Device Applications. By syncing the workflow profile settings with a device or Delegation Server at the date and time specified in the profile task, you can use the workflow profile with a device or mobile device. Syncing can also be immediately performed.

Configuring a Workflow Profile by Input Source

The procedure for configuring a workflow profile varies depending on the input source of the document to be delivered in the workflow.

- Creating a profile for a workflow that delivers documents scanned on a device with Device Application installed or received fax documents:
  See page 321 "Configuring a workflow profile associated with a device".
- Creating a profile for a workflow that delivers files sent from a mobile device with the RICOH Streamline NX mobile app installed:
  See page 381 "Configuring a Workflow Profile Associated with a Mobile Device".
- Creating a profile for a workflow that imports and delivers documents saved to a specified folder (Monitor Folder) on a Delegation Server or a shared folder on the network:
  See page 323 "Configuring a workflow profile associated with a monitor folder".

Note

- This section describes how to configure a new workflow profile. To configure a new profile based on a configured workflow profile, see page 328 "Changing a Workflow Profile".

Configuring a workflow profile associated with a device

1. **Click the following items in the navigation tree to open the [Profile Configuration] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Configuration]

2. **Click (Add).**

   The [Create Workflow Profile] window is displayed.

3. **In [Profile Name], enter the name of the workflow profile.**
4. **In [Description], enter the description of the workflow profile.**
5. **In [Input Source], select [MFP].**
6. **Click [OK].**

7. **On the [General] tab, configure the profile properties.**

   For setting items, see page 599 "Profile Configuration", "When [General] tab - Input Source is set to [MFP]".

8. **On the [Workflows] tab, click (Add Group) under [Capture Workflows].**

   To add a Device Applications or workflow to a created group, proceed to Step 12.

9. **On the [Group Properties] window, enter a group name.**

10. **In [Display], select [Yes] or [No].**

    When [No] is selected, the group is not displayed on the operation screen of the device. When using a workflow within a group for automatic transfer that does not require the user to configure the parameters (such as fax reception transfer), select [No].

11. **Click [OK].**

12. **From the group tree, select the group to which to add a workflow, and click (Add a workflow/application).**

13. **On the [Add a workflow/application] window, click the [Workflows] or [Device Applications] tab.**

14. **Select the workflow or Device Applications to add, and click [OK].**

    You can select from created workflows or Device Applications configured [Device Applications] under [Workflow].

    For details about creating workflows, see page 227 "Creating a Workflow".

    For details about configuring Device Applications, see page 319 "Configuring Device Applications".

    When adding a text box to a group, click , enter the text, and click [OK].

15. **From the group tree, select the Device Applications or workflow added to the group, and from the properties displayed on the right side, select [Small], [Medium], [Large], or [Extra Large] for the display size of the buttons of the Device Applications or workflow on the operation screen of the device.**

16. **To configure the fax reception document delivery function in the profile, click [Fax Workflow].**

    For details about delivering received fax documents, see page 331 "Delivering a Received Fax Document".

17. **Select the [Use Fax] check box.**

18. **From the [Fax Workflow] drop-down list, select the workflow to use for delivering the received fax.**

    You can only select the workflow for one-touch scanning.

19. **Select all fax spots to monitor.**

20. **On the [Preview] tab, you can preview the workflow buttons on the operation screen of a device.**
21. **Click (Save) on the workflow list.**
22. **Configure a profile task to associate the profile with a device or device group and to sync the settings.**

    Proceed to page 329 "Configuring a Profile Task".

Note

- For the setting items on the [Workflows] tab and the details of the [Preview] tab, see page 599 "Profile Configuration", "When [Workflow] tab - Input Source is set to [MFP]", and "Only when [Preview] tab - Input Source is set to [MFP]".

Group tree

- Newly added groups are added to the bottom of the group tree.
- Selecting a group on the tree displays the group properties on the right side. You can specify the group name and whether to show or hide the group.
- To delete a group or a workflow or Device Applications in a group, select the item to be deleted, and click (Delete). When a group is deleted, the workflows and Device Applications in that group are also deleted.
- The order of workflows or Device Applications in a group can be changed by dragging and dropping, and they can be moved to a different group. The buttons of the workflows and Device Applications are displayed on the operation screen of the device with the same order as in the group tree.

Configuring a workflow profile associated with a monitor folder

When Scan & Capture Input Connector is used, the folder specified on a Delegation Server or on a network is monitored, and when a file is stored in the folder, the file is automatically imported and delivered in accordance with the specified workflow. The workflow profile in which the monitor folder is specified as the input source can be configured only when Scan & Capture Input Connector is enabled.

1. **Perform Steps 1 to 4 of page 321 "Configuring a workflow profile associated with a device".**
2. **Select [Hot Folder] for [Input Source].**
3. **Click [OK].**
4. **On the [General] tab, configure the profile properties.**
5. **On the [Workflows] tab, click (Add).**

   The [Workflow Settings] window is displayed.
6. **In [General Settings], specify the folder to monitor, the workflow to use to deliver documents in the folder, and other settings.**

7. **In [Metadata Settings], configure the metadata mapping function.**
8. **Click [OK].**
9. **Click (Save) on the profile list.**
10. **Configure a profile task to associate the profile with a Delegation Server and to sync the settings.**

    Proceed to page 329 "Configuring a Profile Task".

Note

- For the setting items of each tab, see page 599 "Profile Configuration", "When [General] tab-Input Source is set to [Hot Folder]", and "When [Workflow] tab-Input Source is set to [Hot Folder]".
- When both of the Delegation Server and the computer or server on which the monitor folder exists are running on Windows 8 or later or Windows Server 2012 or later, SMB3.0 is used to connect to the folder.

Import file conditions

- The following files can be imported. Files that do not meet the conditions are stored in the error save folder without being imported.
  - Files with a bmp, gif, jpeg, jpg, pdf, png, tif, or tiff extension
  - Files with a name of 74 half-width characters or less
  - Files whose size is 200 MB or smaller
- Hidden files can also be imported.
- Read-only files cannot be imported.
- Depending on the communication status with the delivery destination, file distribution may result in an error.
- A file cannot be imported when the text encoding of the file name does not match the system language of the RICOH Streamline NX server.

Imported file metadata

You can configure the metadata in files imported with Scan & Capture Input Connector and distributed. The metadata for Scan & Capture Input Connector is as follows. For details about the other metadata, see page 348 "Metadata".

Element name (ID)	Description
sourceTimeZone	This element is always left blank in Scan & Capture Input Connector.
contentType	This element is always left blank in Scan & Capture Input Connector.

Element name (ID)	Description
application	Indicates the job queue type. In Scan & Capture Input Connector, the "hotfolder" is specified. The specified "hotfolder" is displayed in the job log type column.
userName	This element is always left blank in Scan & Capture Input Connector.
docType	This element displays the file extension.
devicename	The display name of the monitor folder is specified. This element is displayed in the format "devicename [machineID]" in the device name field of the job log. The device name is specified in this element when device input is specified.
machineId	This element is always left blank in Scan & Capture Input Connector.

Importing multiple files

- When Enable import of multiple files is selected, multiple files in the subfolder under the monitor folder are imported as one job.
- All files in the subfolder are deleted after being processed or saved.
- The control file that initiates the completion of file transfer must reside in the subfolder. Files in a subfolder without the control file cannot be imported. Be sure that the control file is the last file in the subfolder.

Monitor schedule

- When started, RICOH Streamline NX starts checking each monitor folder registered in monitor settings. When multiple monitor folders are configured, the folders are circulated in order, starting at the top of the list. After circulation is completed one time, the circulation pauses for one minute, and then starts again. When there is a file in the monitor folder or a subfolder of the monitor folder, the file is imported according to the monitor settings. The imported file is delivered according to the settings of the workflow selected with the delivery settings of the Monitor Folder Setting Tool.
- When there are multiple files directly under the monitor folder, the files are individually imported per job starting with the files updated last. When there are multiple files in a subfolder, all files are imported as one job.
- When a new file is added to the monitor folder after file importing has started, the file is imported in the next circulation.

- When the settings are changed with the Management Console, the changes are applied once importing of the file in the folder being monitored is completed.

Conditions for the Monitor Folder, Error Save Folder, and Store Folder that can be configured

You can specify a folder on a Delegation Server or a shared folder on the network as the monitor folder.

- Although there is no limit on the number of monitor folders that can be registered, it is recommended to keep the number to 50 or less for optimal performance.
- When specifying a folder on a Delegation Server as the monitor folder, the user who started the Windows Service "RICOH SLNX Delegation Server Service" should have all of the privileges required to read, write in, and delete the folder. When specifying a shared folder on the network as the monitor folder, the user specified in [General Settings] should have all of the privileges required to read, write in, and delete the folder.
- The maximum length of the path specifying the folder is 128 characters.
- A folder with a name ending in ".tmp" cannot be specified.
- A folder with a name ending in "." cannot be specified.
- A path containing the following characters cannot be specified: ~ " # % & * : < > ? { | }.
- A hidden folder can be specified.
- A folder with files saved directly under that folder cannot be specified as the monitor folder. A folder containing an empty folder can be specified as the monitor folder.
- A monitor folder that is specified in other monitor settings, an error save folder, or store folder that is specified in the same or other monitor settings cannot be specified as a new monitor folder.
- A monitor folder that is specified in the same or other monitor settings cannot be specified as the error save folder or store folder.

Precautions when using Scan & Capture Input Connector

- When a file is moved to an error save folder or store folder and a file with the same name exists in the destination folder, a suffix is added to the file name as shown below.
  Example: xxxxx(1).tif, xxxxx(2).tif
  The maximum value of the suffix is 9999. An error occurs when the maximum value is exceeded.
- When the file is imported, a folder with the name "HF.tmp" is created in the monitor folder, and that folder remains and is not deleted even after the import process is completed.
- The file moved to the error save folder or store folder is not automatically deleted. Delete the file manually as necessary.
- When the file is imported, it is not checked whether the file is a system file. Be careful not to specify a folder that may contain a system file.
- A file input via the Monitor Folder is recorded as a color file in the report, regardless of whether the file is actually in black and white or color.

Metadata mapping function

- The metadata mapping function allows you to hold the metadata of the documents scanned using a third party device and input via a monitor folder.
- In the [Metadata Settings] screen of the [Workflow] tab, you can map the index fields in the specified index file with the metadata generated in RICOH Streamline NX workflows.
- Specify the index files in XML or CSV format.
- Specify the index file name using regular expression. Make sure that no BOM is included in the index file.
- When an index file in XML format is to be used in metadata mapping, you need to import the XML schema of the index file. The file extension for the XML schema must be ".xsd". If an index file which does not follow the schema is received during job processing, the document will be processed without mapping the metadata.

  XML Schema example:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.w3schools.com"
xmlns="http://www.w3schools.com"
elementFormDefault="qualified">
<xs:element name="root" >
<xs:complexType >
<xs:sequence>
<xs:element name="Username" type="xs:string" />
<xs:element name="LoginID" type="xs:string" />
<xs:element name="DepartmentCode" type="xs:string" />
<xs:element name="OrderDate" type="xs:date" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

  Sample of an index file in XML format based on the above Schema:

```
<?xml version="1.0"?>
<root xmlns="http://www.w3schools.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.w3schools.com Control.xsd">
<Username>Test User</Username>
<LoginID>testUser</LoginID>
<DepartmentCode>1234</DepartmentCode>
<OrderDate>2013-12-11</OrderDate>
</root>
```

- When an index file in CSV format is to be used in metadata mapping, you need to import the schema file which defines all keys. Use a comma to separate the metadata key and value. All values are handled as string type.

  Schema file example:

  Username, LoginID, DepartmentCode, OrderDate

  Sample of an index file in CSV format based on the above Schema:

  Username, LoginID, DepartmentCode, OrderDate

  Test User, testUser, 1234, 2013-12-11

Changing a Workflow Profile

A configured workflow profile can be changed, and a new profile can be configured based on a configured workflow profile.

Each time a workflow profile is changed, the version of the profile displayed in the profile list increases by one. Only the latest version is displayed in the profile list.

Important

- **Only one workflow profile that is associated with a mobile device can be configured on any one system. Therefore, it not possible to copy an existing workflow profile that is associated with a mobile device.**

1. **Click the following items in the navigation tree to open the [Profile Configuration] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Configuration]

2. **Select the profile you want to change from the profile list.**

   To configure a new workflow profile based on an existing profile, select the profile to copy from the profile list, click (Copy), and select the profile to edit.

3. **Change the profile settings in the profile edit area.**

   You cannot change the [Input Source] setting on the [General] tab.

   When you copy a profile, it is created as a new profile, and therefore, the Associated [Devices/Groups] tab and [Associated Servers] tab are blank.

   For the procedure to modify profile properties, see Steps described in page 321 "Configuring a Workflow Profile by Input Source".

4. **Click (Save) on the profile list.**

Deleting a Workflow Profile

1. **Click the following items in the navigation tree to open the [Profile Configuration] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Configuration]

2. **Select the profile to delete from the profile list, and click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- The settings on a device with a synced profile are not changed even after the workflow profile is deleted.

Configuring a Profile Task

The schedule for syncing a configured workflow profile with a device or Delegation Server can be configured.

Creating a new profile task

Use the following procedure to configure a profile task:

1. **Click the following items in the navigation tree to open the [Profile Tasks] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Tasks]

2. **Select the profile with the task to be configured from the profile list.**
3. **For a profile associated with a device, click the [Target Devices/Groups] tab, and for a profile associated with a Monitor Folder, click the [Target Servers] tab.**
4. **When the input source is MFP or Hot Folder, add target devices or device groups, or target servers.**

   Adding a device

   1. On the [Target Devices/Groups] tab, click (Add Devices).
   2. Select the device to add, and click .
      To add all devices, select the [All Devices] check box.
   3. To add additional devices, repeat Step 2.
   4. Click [OK].

   Adding a device group

   1. On the [Target Devices/Groups] tab, click (Add Group).
   2. Select a device category and the group to add, and click .

Add to one profile only those groups that belong to the same device category.
To add all device groups under the same device category, select the [All Devices] check box.

3. To add additional groups, repeat Step 2.
4. Click [OK].

Adding a server

1. On the [Target Servers] tab, click (Add Delegation Server).
2. Select the server to add, and click .

   If the servers are divided into groups, select a server group, and then select the server to add. You cannot add a server group itself.

   When the monitor folder is a local folder on a Delegation Server, select the [All Servers] check box to enable adding of all servers.
   When the monitor folder contains a shared folder, only one server can be added.
3. Click [OK].

5. On the [Schedule] tab, clear the [Disable Schedule] check box.

6. Specify the date and time to sync the profile with the device and server in [Start Date] and [Start Time].

You can also click the calendar icon to select the date on a calendar for [Start Date].

The time of the local time zone of the Core Server is used.

When syncing with a device or server in a different time zone, consider the time difference for specifying the date and time.

7. To send an email notification of a task execution, select the [Enable Task Completion Notification] on the [Notification] tab.

8. Select [Input Email Address Manually] or [Select Destination].

9. When [Input Email Address Manually] is selected, enter the email address of the recipient. When [Select Destination] is selected, select the destination from the drop-down list.

10. When [Input Email Address Manually] is selected, select the language for the notification from the drop-down list.

11. Click (Save).

Immediately running a task

A profile can be immediately synced with a device or device group without having to wait for the profile task execution time.

1. **Click the following items in the navigation tree to open the [Profile Tasks] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Tasks]

2. **Select the profile to be immediately synced from the task list, and click ▶ (Run Immediately).**

   The profile syncs immediately with the device or device group.

Changing a profile task

1. **Click the following items in the navigation tree to open the [Profile Task] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Task]

2. **Select the profile to change from the task list, and change the settings.**

   For details about the procedure for changing the settings, see page 329 "Creating a new profile task".

3. **Click (Save) on the profile list.**

Delivering a Received Fax Document

To use the received fax document delivery function, configure a workflow profile that is configured with a workflow for delivering received fax in the Management Console. Also, set Reception Settings for fax documents on the device to [Store]. Received fax documents are stored in the document box on the device, and then forwarded to the Delegation Server for delivery. For details about the settings, see the User's Guide of the device.

Documents are automatically deleted from the document server after successful delivery.

Important

- **If an error occurs after a fax document is transferred to the server, the job is treated as an error job. When the fax document cannot be transferred to the server, it is stored in the document box and is not deleted. If error jobs are continually stored, the hard drive will become full, and received documents will be output on paper.**
- **When a received fax document cannot be delivered, check if it is stored in the document box. If there is no document in the document server, turn off and then on the main power of the device.**
- **Depending on the device settings, documents stored in the document box may be automatically deleted after a fixed period has elapsed. Be sure to check the document box for documents regularly. Some documents that have not been delivered may remain in the document server.**
- **You can perform printing on the device while storing documents even when Reception File Settings is set to [Store]. For details about the settings, see the User's Guide of the device.**

- Received fax documents can be held on the Delegation Server for a specified period after their delivery is complete. For details on the settings, see [Overwrite Backed Up Fax Jobs] under "[Capture] tab", page 629 "Server Group".

Configuring Necessary Settings for Using Certain Connectors

This section describes how to configure the metadata database connection, replacement table, and Zone OCR form. The procedure to add a PDF stamp is also described. The settings apply to all connectors being used in the workflows.

Configuring the Metadata Database Connection

The values of the metadata elements can be directly entered, imported as a CSV file, or obtained from a database table. To enable the user to select the values of the metadata elements obtained from a database table on the metadata tab when creating a workflow, configure the Metadata Database Connection.

Adding a database connection

1. **Click the following items in the navigation tree to open the [Metadata Database Connection] tab.**

   [Workflow] ▶ [General] ▶ [Metadata Database Connection]

2. **Click (Add) in the connector list.**

   To create a new connector based on an existing connector, select the connector to copy, click (Copy), and select the connector to edit.

3. **On the [General] tab, specify the connection name, the database server's address, etc., for the Metadata Database Connection.**
4. **Click [Test].**
5. **On the [Select Server] window, select the Delegation Server to use to test the connector.**
6. **Click [Run].**
7. **When a message is displayed indicating that the connector test was successful, click [OK].**

   If an error message is displayed, click [OK], check the settings, and test the connector again.

8. **Click (Save) on the connector list.**

Note

- For details about the setting items on each tab, see page 578 "Metadata Database Connection".

Changing a database connection

1. **Click the following items in the navigation tree to open the [Metadata Database Connection] tab.**

   [Workflow] ▶ [General] ▶ [Metadata Database Connection]

2. **From the connector list, select the connector to modify, and then change the settings.**

   For details about configuring the settings, see page 333 "Configuring the Metadata Database Connection".

3. **Click (Save) on the connector list.**

Deleting a database connection

1. **Click the following items in the navigation tree to open the [Metadata Database Connection] tab.**

   [Workflow] ▶ [General] ▶ [Metadata Database Connection]

2. **From the connector list, select the connector to delete, and then click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- A connector being used in a workflow cannot be deleted. Use the [Workflow] tab to view the workflows that are using the connector.

Configuring a Replacement Table

The Metadata Converter Connector replaces the values of the metadata elements according to the replacement table settings.

When a value of the metadata element matches a value in the table, the matching value of the metadata element is replaced with the output value.

You can configure multiple replacement tables and specify by replacement table name the replacement table to use for each workflow which uses Metadata Converter Connector.

The replacement table consists of a comparison string and an output value. When the input value matches the comparison string, the output value is output. The comparison string can be specified with a normal string, such as "Saito" or "555-5432" or a regular expression for a higher match rate. The input value is obtained from the metadata.

Note

- For details about regular expression, see page 358 "Regular Expressions".

- For details about metadata, see page 348 "Metadata".

Adding a replacement table

Use the following procedure to add a new replacement table:

1. **Click the following items in the navigation tree to open the [Replacement Table] tab.**

   [Workflow] ▶ [General] ▶ [Replacement Table]

2. **Click (Add) on the replacement table list.**

   To create a new replacement table based on an existing replacement table, select the connector to copy, click (Copy), and then select the replacement table to edit.

3. **On the [General] tab, specify the replacement table name, input/output information of metadata, etc.**

4. **On the [Comparison Entry] tab, click (Add) and then add entries to the replacement table.**

5. **On the [Comparison Entry] tab, click (Save).**

   To add more entries, repeat Steps 4 and 5.

6. **Click (Save) on the replacement table list.**

Note

- For details about the setting items on each tab, see page 579 "Replacement Table".
- You can up to 700 comparison entries can be added in one replacement table.
- You can up to 5,000 total comparison entries can be added in all replacement tables.
- To change a comparison entry, select the entry to change, change the setting, and then click (Save) on the [Comparison Entry] tab.
- To delete an entry, select the entry to delete, and then click (Delete).

Changing a replacement table

1. **Click the following items in the navigation tree to open the [Replacement Table] tab.**

   [Workflow] ▶ [General] ▶ [Replacement Table]

2. **In the replacement table list, select the replacement table to change, and then change the settings.**

   For the configuration procedure, see page 335 "Adding a replacement table".

3. **Click (Save) in the replacement table list.**

Deleting a replacement table

1. **Click the following items in the navigation tree to open the [Replacement Table] tab.**

   [Workflow] ▶ [General] ▶ [Replacement Table]

2. **F In the replacement table list, select the replacement table to delete, and then click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- You cannot delete a replacement table being used in a workflow.

Exporting and importing a replacement table

You can export or import the replacement table contents in CSV (comma separated value) format.

You can also edit the data in CSV format. To edit data, use an application that supports the character code selected at export. You can use the export/import function of the replacement table to store all replacement tables.

Important

- **Exported CSV files contain header information that begins with a number sign (#). Import the header information without editing it.**

Note

- For details about the CSV file format of the replacement table, see page 337 "Format of CSV file for a replacement table".

Exporting a Replacement Table

1. **Click the following items in the navigation tree to open the [Replacement Table] tab.**

   [Workflow] ▶ [General] ▶ [Replacement Table]

2. **On the [Comparison Entry] tab, click (Export).**

   The [Export Comparison Entries] window is displayed.

3. **Select the checkbox for the entries to export.**

   To add all entries, select the checkbox in the title row.

4. **Click [OK].**
5. **When a message appears prompting whether to open or save the download file, click [Save].**
6. **Click [Open Folder].**

   Save the exported file to the desired location.

Importing a Replacement Table

1. **Click the following items in the navigation tree to open the [Replacement Table] tab.**

   [Workflow] ▶ [General] ▶ [Replacement Table]

2. **On the [Comparison Entry] tab, click (Import).**
3. **Click [Browse...] for [File Path].**
4. **Select the file to import, and click [Open].**
5. **Clicking [Upload] to display the comparison entry list.**
6. **Click [OK].**

   The selected file is imported and added to the comparison entry.

7. **Click (Save) in the replacement table list.**

Note

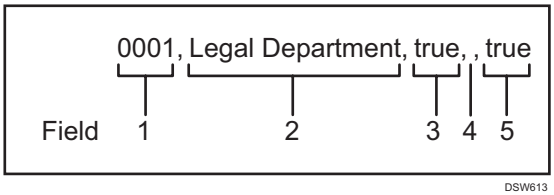
- The number of data items that can be imported in a replacement table is as follows:
  - Max. 700 per replacement table
  - Max. 5,000 for all replacement tables

Format of CSV file for a replacement table

The CSV file for a replacement table consists of text data. Each line in the CSV file corresponds to an item in the table, and the item values are separated by commas.

Important

- **The exported CSV files contain header information that begins with a number sign (#). Do not edit the header information.**
- **The diagram below shows an example of items indicated on one line of a replacement table.**



Field	Data	Applicable table item
1	This is the comparison string. The user can define the string.	[Comparison Target String]
2	This is the output string of the comparison result. The user can define the string.	[Comparison Target String]

Field	Data	Applicable table item
3	Specify "false" or "true". When you specify "false", a regular expression is not used in the comparison string. When you specify "true", a regular expression is used.	[Enable Regex]
4	A profile ID of the previous version of RICOH Streamline NX. It will be empty in the current version.	[Profile ID]
5	Specify "false" or "true". When you specify "false", this item is not compared. When you specify "true", this item is compared.	[Enable Comparison]

Import processing conditions of CSV file for a replacement table

- When no value is specified in the comparison string (field 1), the item is not used for comparison. ([Enable Comparison] is set to 0 in the replacement table.)
- When a value other than 0 or 1 is specified in [Enable Comparison] (field 4), the item is not imported.
- When the same item as the comparison string (field 1) is already in the table, the item value is overwritten with the value of the CSV file.
- When the same item as the comparison string (field 1) is not in the table, the value of the CSV file is added as a new item.
- When editing the CSV file with an application, be sure to save it in CSV format. Other file formats cannot be imported.

Configuring the Zone OCR Form

When a Zone OCR connector is used, a designated area in the scanned document is processed by OCR and extracted as text data.

To use a Zone OCR connector, you must register a Zone OCR form in advance.

Adding a Zone OCR Form

Use the following procedure to configure the Zone OCR Form:

1. **Prepare the image data of the document to perform Zone OCR.**

2. **Click the following items in the navigation tree to open the [Zone OCR Form] tab.**

   [Workflow] ▶ [General] ▶ [Zone OCR Form]

3. **Click (Add).**

   To create a new form based on an existing form, select the form to copy, click (Copy), and then select the form to edit.

   The copied form name is displayed with a suffix automatically added to the copy source name starting from (1). When the maximum number of characters (64) of the form name is exceeded as a suffix is used, the end of the form name is omitted, and a suffix is added.

4. **On the [General] tab, specify the form name, description, and the OCR language.**
5. **In [Zone OCR Form Template Image], click [Browse...].**
6. **Select the template image to use for configuring the anchor and designating the OCR area, and click [Open].**
7. **Click [Upload].**

   The file name, paper size, resolution, and number of pixels of the uploaded image are displayed.

8. **Click the [Form Design] tab.**
9. **Enlarge or reduce the image area, rotate the image, and configure other settings as necessary.**

   To enlarge or reduce the image area, configure the Magnification setting. Enlarge or reduce the size of the image area from 25% to 200% in increments of 25%.

   To rotate the image, click or . The image is rotated 90 degrees to the left or right, respectively.

10. **Drag the mouse over the image to specify the OCR area.**

    The [Area Properties] window is displayed. For details about configuring the settings, see "Configuring the Area Properties" described below.

11. **To configure a new anchor, click [Add Anchor].**

    The mouse cursor changes to a crosshair.

    When an anchor is already configured, [Add Anchor] is disabled and cannot be clicked.

12. **Drag the mouse over the image to specify the anchor area.**

    The [Area Properties] window is displayed. For details about configuring the settings, see "Configuring the Area Properties" described below.

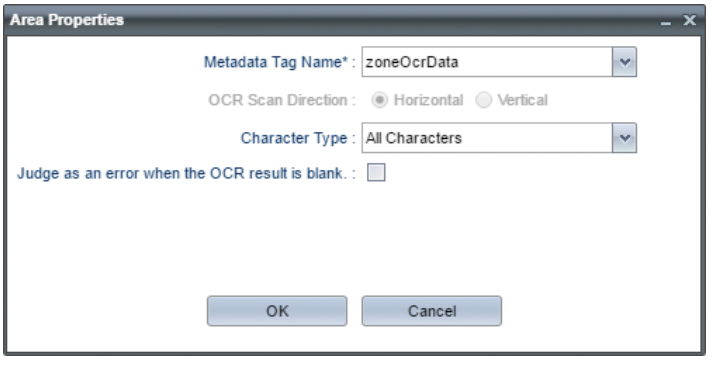
13. **Click (Save) in the form list.**

Configuring the Area Properties

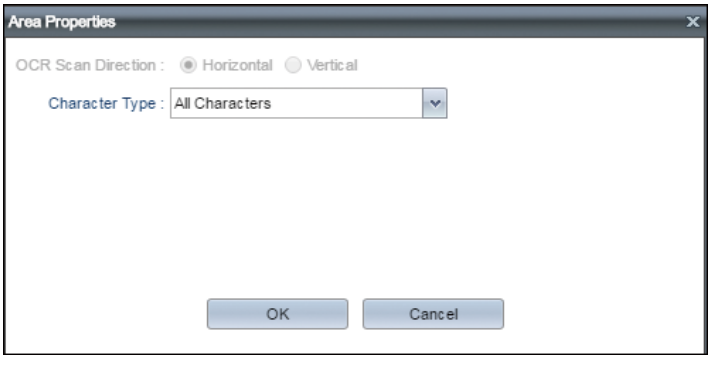
When the OCR area or anchor area is specified by dragging the mouse cursor over the [Form Design] tab, the [Area Properties] window is displayed. The [Area Properties] window is also displayed when the OCR area or anchor area border is double-clicked.

Configure the following items on the [Area Properties] window:

- OCR area properties



- Anchor area properties



Item	Description
Metadata Tag Name	You can specify the metadata tag name by using either of the following. • Customized Metadata Select this item to perform OCR on the selected area and treat the scanned strings as custom metadata elements. Enter the tag name of the custom metadata in [Tag Name]. • Basic Metadata Select this item to perform OCR on the selected area and treat the scanned strings as basic metadata elements. Select the element name from the drop-down list. **Note** • These settings can be configured only when an OCR area is specified. • For details about basic and custom metadata, see page 348 "Metadata".
OCR Scan Direction	Specify the direction of text when performing OCR. This is not available when a western language is selected for the OCR language. • Horizontal Perform OCR on horizontal text. • Vertical Perform OCR on vertical text.

Item	Description
OCR Character Type	Select the type of characters for which to perform OCR. • All Characters All characters that can be obtained as the OCR result are processed. • Numbers and Symbols The following characters are processed: • Numbers (0123456789) • Symbols (,.:;^/~'"()[]{}+-=) • Spaces (space, tab, line break) • Numbers only The following characters are processed: • Numbers (0123456789) • Spaces (space, tab, line break)
Judge as an error when the OCR result is blank.	Select this check box to output an error when no text is detected in the specified area while performing OCR. **Note** • These settings can be configured only when an OCR area is specified. • Select this check box to use the OCR result value of the area as a mandatory metadata element. • If an error occurs while a Zone OCR connector is being processed, the following metadata is added to the document regardless of the [Judge as an error when the OCR result is blank] setting. • Document information name: "LastResult_ZoneOCR" Value: "error" Use the above metadata to configure the error avoidance flow. **Example of flow to avoid errors** Set a Decision Point behind the Zone OCR connector, and configure the flow to be redirected when the metadata value is "error".

Note

- For details about the setting items on each tab, see page 757 "Zone OCR".
- You can configure up to five areas per form.
- You can configure one anchor area per form.
- The image data to be scanned in the form must meet the following conditions:
  - The image data has been created with the RICOH Streamline NX delivery function.
  - The file format is BMP, GIF, JPEG, TIFF, TIFF-F, or PNG.
  - The image data is stored in a local folder.
  - The number of pixels is between 200 × 350 and 7016 × 9921.
- The recommended minimum resolution of image data scanned to the form is 200 dpi. The recommended resolution when using the position correction function with anchor specification is 400 dpi.
- To delete the configured area, right-click the Zone OCR area or anchor, and select [Delete]. A deleted area cannot be restored.
- When you configure an anchor, the position is corrected, and the character recognition rate improves. The configured anchor must meet the following conditions.
  - A string that exists in both the form and scanned image data are selected as the anchor.
  - The anchor area has a string. If there is no text, the position is not corrected.
  - The string in the anchor area and the string in the same position on the scanned image data are the same.
  - The string configured at the anchor area and the string with the same content are within 20 mm from the top, bottom, left, and right of the area.
  - The page number and document name on the header are not specified as the anchor area. The page number, document name on the header, and other similar information cannot be used as an anchor.
- When the Zone OCR area or anchor is selected, the mouse cursor changes to a two-headed pointer in the four corners of the area and near the center mark on each side. Drag the mouse when this cursor is displayed to enlarge or reduce the area.
- When Japanese is selected for the OCR language, the following characters can be recognized:
  - Recognition target text: Roman letters, numbers, symbols, Greek letters, katakana, hiragana, JIS 1 standard kanji
- Half-width and full-width Roman letters, numbers, and symbols are not distinguished at the recognition stage. Text that can be converted to half-width text is output in half-width as the OCR result.
  - Supported fonts: Mincho, Gothic
  - Font size: 6 to 31 pt (approx. 2 to 10 mm)

- The following resolutions are supported depending on the document size of the images imported for the form.
- ✓: supported
- -: not supported

Document size	Resolution				
	100 dpi	200 dpi	300 dpi	400 dpi	600 dpi
B0 JIS	✓	-	-	-	-
A0	✓	✓	-	-	-
B1 JIS	✓	✓	-	-	-
A1	✓	✓	✓	-	-
B2 JIS	✓	✓	✓	-	-
A2	✓	✓	✓	✓	-
B3 JIS	✓	✓	✓	✓	-
A3	✓	✓	✓	✓	✓

Changing a Zone OCR form

1. **Click the following items in the navigation tree to open the [Zone OCR Form] tab.**

   [Workflow] ▶ [General] ▶ [Zone OCR Form]

2. **In the form list, select the form to change, and then change the settings.**

   For the configuration procedure, see page 338 "Adding a Zone OCR Form".

3. **Click (Save) in the form list.**

Deleting a Zone OCR form

1. **Click the following items in the navigation tree to open the [Zone OCR Form] tab.**

   [Workflow] ▶ [General] ▶ [Zone OCR Form]

2. **In the form list, select the form to delete, and then click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- You cannot delete a zone OCR form being used in a workflow.

Registering a PDF Stamp

Register a PDF stamp to use in the PDF stamp connector.

PDF stamps include Bates Stamp, Image Stamp, Text Watermark, and Image Watermark.

Files with the following formats can be registered as a PDF stamp:

- BMP, JPEG, JPG, PNG, GIF

When you select a file in an unsupported format, an error message is displayed, and the file cannot be registered.

Note

- The images whose vertical or horizontal size exceeds 1,250 mm cannot be uploaded for the stamp.
- For details about the output image of Bates Stamp, Image Stamp, Text Watermark, or Image Watermark, see page 289 "PDF Stamper".

Adding a PDF stamp

Use the following procedure to register a PDF stamp:

1. **Click the following items in the navigation tree, and open the [PDF Stamper] tab.**

   [Workflow] ▶ [General] ▶ [PDF Stamper]

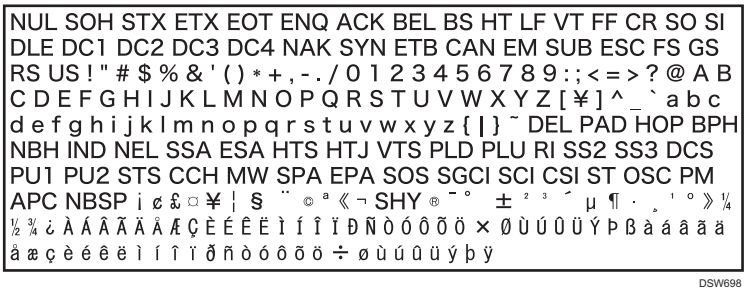
2. **Click (Add).**

   To create a new stamp based on an existing stamp, select the stamp to copy, click (Copy), and then select the stamp to edit.

3. **On the [General] tab, enter the stamp name and description, and select the stamp type from the drop-down list.**
4. **On the [Stamp] tab, specify the details of the stamp.**
5. **When Bates Stamp or Text Watermark is selected in Step 2, specify the font to use for the stamp on the [Font] tab.**
6. **On the [Position] tab, specify the position to insert the stamp.**
7. **Preview the stamp on the [Preview] tab.**
8. **Click (Save) on the stamp list.**

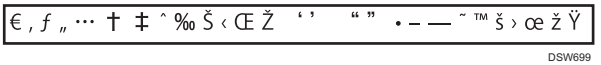
Note

- For details about the setting items, see page 581 "PDF Stamper".
- When uploading an image to use for [Image Stamp] or [Image Watermark], you cannot upload an image larger than the specified size.
- For details about the characters that can be used in [Prefix], [Suffix], and [Watermark Text] on the [Stamp] tab, see the following:
  - Unicode



DSW698

  - Windows 1252



DSW699

Editing a PDF stamp

1. **Click the following items in the navigation tree, and open the PDF Stamper tab.**

   [Workflow] ▶ [General] ▶ [PDF Stamper]

2. **From the stamp list, select the stamp to change, and change the settings.**

   For the configuration procedure, see page 345 "Adding a PDF stamp".

3. **Click (Save) on the stamp list.**

Deleting a PDF stamp

1. **Click the following items in the navigation tree, and open the PDF Stamper tab.**

   [Workflow] ▶ [General] ▶ [PDF Stamper]

2. **From the stamp list, select the stamp to delete, and then click (Delete).**
3. **When the confirmation message is displayed, click [Yes].**

Note

- You cannot delete a PDF stamp being used in a workflow.

Metadata

Metadata includes the document name, the user who created the document, and the date and time the file was created, and it is obtained automatically in XML format when a document is scanned. Metadata can be used to categorize documents intended for data searching as well as to process jobs with the Metadata Converter and Decision Point process connectors.

Metadata is categorized into basic and custom metadata elements.

- Basic metadata

  Basic metadata elements are defined by the system and are automatically added to a document when the document is scanned. This contains values and data that are not configurable.

- Custom metadata

  The administrator adds elements other than basic metadata for each workflow. Custom metadata can be configured to enable users to enter values and text on the operation screen of the device when a document is scanned, or users can enter the metadata in a text box or select from the drop-down list.

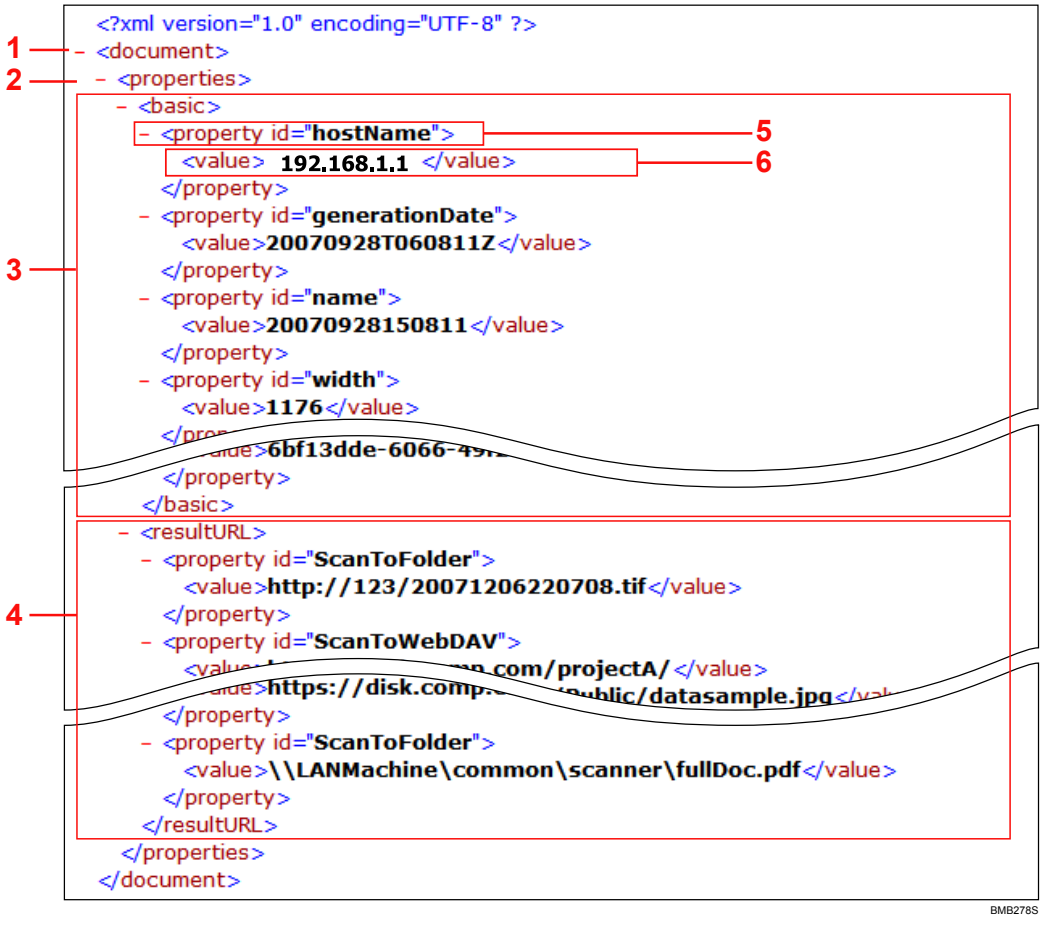
Metadata elements are managed by the element name (ID).

Some basic metadata item names can be selected from a drop-down list when a connector is configured. To specify a metadata element not displayed or a custom metadata element, enter the element name (ID) manually in the list box according to the rule.

Note

- To output metadata in XML format, use the XML Transformer without specifying an XSL file. For details, see page 276 "XML Transformer".
- For details about configuring the custom metadata for each workflow, see page 308 "Configuring Items in Metadata".

Metadata XML



1. **"document" element**

   The document element is a metadata root element.

2. **"properties" element**

   The properties element includes all property elements and the resultURL element.

3. **"basic" element**

   Basic and custom metadata items are described between the <basic> and </basic> tags.

4. **"resultURL" element**

   The destination URL to save the document is described between the <resultURL> and </resultURL> tags.

5. **Metadata properties**

   Element names are described in the "id" property in the <property id> tag of basic and custom metadata.

6. **Metadata element values**

   "192.168.1.1" between the <value> and </value> tags is the value associated with that metadata element.

Note

- The "resultURL" element is described in XML only when the following destination connector is configured before the XML Transformer in the delivery flow.
  - When a custom URL is specified in the Send to Folder connector. For details, see page 241 "Send to Folder".
  - When a Send to FTP or Send to WebDAV connector is being used. For details, see page 242 "Send to FTP" or page 243 "Send to WebDAV".
- The order of the metadata displayed in XML and the above order may differ.

Basic Metadata Elements and Corresponding Tag Names

Category - System

Item Name (ID)	Display Name	Type	Description
name	Document Name	String	Document Name
userName	User Name	String	User Name
pageCount	Number of Pages	Number	Number of pages of the document A 2-sided document is counted as two pages.
contentSize	Document Size	Number	Total size of the input data (byte) This is the initial value.
latestContentSize	Document Size (Latest)	Number	Total size of the input data (byte) This value is updated through workflow.
generationDate	Document Creation Date (UTC)	Date	Document creation date (in UTC (Coordinated Universal Time) format) • The format is "yyyymmddThhmmssTZD". (yyyy: year, mm: month, dd: day, hh: hours, mm: minutes, ss: seconds) • TZD is the time zone, and "Z" indicates UTC. • For example, when the document was created on September 9, 2014 at 12:34:00 AM (JST: UTC+9), the value is "20140909T123400Z".

Item Name (ID)	Display Name	Type	Description
generationDateLocal	Document Creation Date (Local Time)	Date	Document creation date in local date • The format is "yyyymmddThhmmss". (yyyy: year, mm: month, dd: day, hh: hours, mm: minutes, ss: seconds) • For example, when the document was created on September 9, 2014 at 12:34:00 AM (JST: UTC+9), the value is "20140909T123400". • The local time varies depending on the input source of the job. Scan/Fax: The device's local time HotFolder/Workflow test: The Delegation Server's local time Mobile device: The mobile device's local time
generationEpoch	Document Creation Date (Epoch)	Number	Document creation date Displays the date and time the file was registered with a value in milliseconds expressing the elapsed time since January 1, 1970 0:00 AM. This value is calculated based on the UTC (Coordinated Universal Time). Note • This metadata is not available for criteria configuration of the Decision Point connector.
dayOfWeek	Day of the week	String	Days of the week in English Example: Monday
sourceTimeZone	Time Zone of Place Document was Created	String	Time zone of the place the document was created (in GMT) • The format is "GMT[+|-]hh[:]mm". • Scan/Fax: The device's local time zone HotFolder/Workflow test: The Delegation Server's local time zone

Item Name (ID)	Display Name	Type	Description
application	Application	String	Input application type Example: Scan, fax, monitor folder, mobile device
contentType	MIME Type	String	MIME type of the first page The description conforms to RFC.
docType	Extension	String	Extension of the first page of the job This is the initial value.
latestDocType	Extension (Latest)	String	Extension of the first page of the job This value is updated through workflow.
jobId	Job ID	String	Job ID
profileId	Profile ID	String	Profile ID
groupId	Group ID	String	Group ID
projectId	Workflow ID	String	Workflow ID
registrationDate	Document Registration Date (UTC)	Date	Document Registration Date UTC (Coordinated Universal Time) is used.
registrationDateLocal	Document Registration Date (Local Time)	Date	Document Registration Date • The format is "yyyymmddThhmmss". (yyyy: year, mm: month, dd: day, hh: hours, mm: minutes, ss: seconds) • The local time varies depending on the input source of the job. Scan/Fax: The device's local time Other than scan and fax: The Delegation Server's local time

Item Name (ID)	Display Name	Type	Description
registrationEpoch	Document Registration Date (Epoch)	Number	Document Registration Date Displays the date and time the file was registered with a value in milliseconds expressing the elapsed time since January 1, 1970 0:00 AM. **Note** • This metadata is not available for criteria configuration of the Decision Point connector.
dsName	DS Server Name	String	Delegation Server's name This metadata is contained only in a job processed on the Delegation Server.
dsHostAddress	DS HostAddress	String	IP address of the Delegation Server This metadata is contained only in a job processed on the Delegation Server.
dsHostName	DS HostName	String	Host name of the Delegation Server This metadata is contained only in a job processed on the Delegation Server.
dsVersion	DS Version	String	Version of the Delegation Server This metadata is contained only in a job processed on the Delegation Server.

Category - Scan/Fax

Item Name (ID)	Display Name	Type	Description
hostAddress	Host Address	String	Device IP address
hostname	Host Name	String	Name of the domain to which the device belongs (in FQDN format)
hostDomain	Host Domain	String	Name of the domain of the device (same value as the device's "Domain Name") The DNS settings and the Domain Name must be correctly set on the device.

Item Name (ID)	Display Name	Type	Description
deviceName	Device Name	String	Device Name
macAddress	MAC Address	String	Device's MAC address
machineId	Machine ID	String	Device ID This value is empty when the document is input via Monitor Folder.
mfpApplicationVer	Application Version	String	The version of the Streamline NX application installed on the device.
transferKind	Purpose of Transfer	String	Purpose of transfer (delivery/capture)
pageSize	First Page's Size	String	Page size of the first page Example: A4 "Unknown" is displayed for size values not listed in page 357 "Page Size Values".
xResorution	Horizontal Resolution	Number	Horizontal resolution (dpi)
yResolution	Vertical Resolution	Number	Vertical resolution (dpi)

Category - Scan

Item Name (ID)	Display Name	Type	Description
outMode	2-Sided/1-Sided	String	2-sided/1-sided
length	Length	Number	Image width (pixels)
width	Width	Number	Image length (pixels)
rotation	Rotation Angle	Number	Rotation angle of the rotated image
rotationType	Rotation Type	String	Rotation type of the rotated image Example: TYPE_A, TYPE_B, TYPE_C, each

Item Name (ID)	Display Name	Type	Description
scanMethod	Scan Method	String	Document scanning method • ADF Scan using only the ADF • PLATEN Scan using only the exposure glass • MIX Scan using either the ADF or exposure glass
scanPageCount	Number of Scanned Pages	Number	Number of pages of the scanned document
colorPageCount	Number of Color Pages	Number	Number of pages in color of the scanned document
bwPageCount	Number of B&W Pages	Number	Number of pages in B&W of the scanned document
scanType	Document Type	String	Scan type selected in Scan Settings Example: OCR_TYPE, TEXT_TYPE, AUTO_SELECT

Category - Fax

Item Name (ID)	Display Name	Type	Description
port	Port Number	String	Fax Reception Port • G3-1 • G3-2 • G3-3 • G4 • InternetFAX • Ipfax
tsi	TSI	String	The TSI (Transmitting Subscriber Identification) or numbering display (transmitter phone number) This is set only for fax sending and receiving.

Item Name (ID)	Display Name	Type	Description
direction	Fax Scanning Direction	String	Fax scanning direction
faxJobId	Fax Job ID	String	ID of received fax document (SAF admin ID)
mailFaxSubject	Mail Fax Subject	String	Subject of received fax mail

Category - User

Item Name (ID)	Display Name	Type	Description
userDisplayName	Display Name	String	Display Name
userMailAddress	User Email Address	List	User's e-mail address
userHomeFolder	User Home Folder	List	User's home folder
userFaxNumber	User Fax Number	List	User's fax number
userGroup	User Group	List	User's group
userDepartment	Department	List	User's department
costCenter	Cost Center	String	Cost center associated with the job
userCustom1	Custom Property 1	String	User's Custom Property 1 **Note** • You can specify up to 10 custom properties. Specify the item names as userCustom1, userCustom2, ..., userCustom10.

Note

- For details about the numerical format of metadata elements output to the file and folder names, see page 255 "Numerical format of metadata".

- For details about the date and time format of metadata elements displayed in the file and folder names, see page 257 "Date and time format of metadata".

Page Size Values

Page Size Values of A-size Paper

A0 to A10

Page Size Values of B-size Paper

B0 to 10

Page Size Values of C-size Paper

C0 to C10

Page Size Values of JIS B-size Paper

JIS B0 to JIS B12

Page Size Values for other sizes

- Statement
- Quarto
- Foolscap Folio Foolscap Folio
- Executive Monarch
- Government-Letter
- Letter
- Legal
- Ledger Tabloid
- Post
- Crown
- Large Post
- Demy
- Medium
- Royal
- Elephant
- Double Demy
- Quad Demy
- Invoice
- Japanese Postcard
- Japanese Double Postcard

- 36 x 48 in
- 34 x 44 in
- 880 x 1,189 mm
- 765 x 1,085 mm
- 625 x 880 mm

Regular Expressions

For examples of regular expressions, see page 278 "Usage examples of regular expressions".

Metacharacters

The following characters are called metacharacters, and they have special meaning.

^ $ + ? . * ( ) [ ] { } | \

Other characters are called normal characters, and they do not have special meaning.

To use a metacharacter as normal character, place a backslash (\) in front of the metacharacter.

Character	Meaning
. (period)	Match any character (except Newline).
[...]	Match any single character within the brackets.
[^...]	Match any single character outside the brackets.
^	Match the beginning of the line.
$	Match the end of the line (or before Newline at the end).
\A	Match only at the beginning of string.
\Z	Match only at the end of string (or before Newline at the end).
\G	Match only at position () (for example at the end-of-match position of prior m//g).
\b	Match a word boundary.
\B	Match a non-word boundary.
\w	Match any "word" character (alphanumeric plus "_").
\W	Match any non-"word" character.
\s	Match any whitespace character.

Character	Meaning
\S	Match any non-whitespace character.
\d	Match any digit character (0-9).
\D	Match any non-digit character.
\1, \2, ...	Used to refer to previous group.
\x	Escape sequence. Match extended Unicode "combining character sequence". Equivalent to (?:\PM\pM*).
*	Match 0 or more times.
*?	Match 0 or more times (shortest match).
+	Match 1 or more times.
+?	Match 1 or more times (shortest match).
?	Match 1 or 0 times.
? ?	Match 0 or 1 time.
{n,m}	Match at least n but not more than m times.
{ n,m }?	Match at least n but not more than m times (shortest match).
(...)	Grouping.
|	Alternation.
(?:regexp)	A group that cannot be referred to by \1, \2, ...
(?=regexp)	Match following expression to "regexp".
(?!=regexp)	Match following expression to anything but "regexp".

Escape Sequences

You can use the following escape sequences.

Character	Meaning
\0	Null character.
\xhh	Hex character.

Character	Meaning
\n	Newline.
\t	Tab.
\b	Match a word boundary.
\ooo	Octal character.
\cC	Control character.
\r	Return.
\f	Form feed.
\a	Alarm (bell).

You can use the following escape sequences as alternative strings.

Character	Meaning
\u	Make the next character uppercase.
\l	Make the next character lowercase.
\U	Make all following characters uppercase until the next \E.
\L	Make all following characters lowercase until the next \E.
\E	End case modification, i.e., \U and \L.

Exposed Metadata of Destination Connectors

Mail Delivery

Item Name (ID)	Display Name	Type	Description
Sender_SendToEmail	Sender Email Address	String	Sender's email address
To_SendToEmail	To:	List	"To" address
Cc_SendToEmail	Cc:	List	"Cc" address
Bcc_SendToEmail	Bcc:	List	"Bcc" address

Item Name (ID)	Display Name	Type	Description
SendToMe_SendToEmail	My Address	List	Logged-in user's address
ReplyTo_SendToEmail	ReplyTo:	List	"ReplyTo" address
Sensitivity_SendToEmail	Sensitivity	String	E-mail sensitivity

Folder Delivery

Item Name (ID)	Display Name	Type	Description
DestinationFolderPaths_SendToFolder	Path	List	Path of the delivery destination
DestinationFolderURLs_SendToFolder	URL	List	URL created based on the folder path
SenderHomeFolderPath_SendToFolder	Home Folder Path	List	Delivery destination for Home Folder
SenderHomeFolderURL_SendToFolder	Home Folder URL	List	URL created based on the Home Folder path
DisplayName_SendToFolder	Display Name	List	Display name of each start point

Send to FTP

Item Name (ID)	Display Name	Type	Description
DestinationFolderURLs_SendToFTP	(S)FTP URL	List	URL of the Send to FTP delivery destination
DisplayName_SendToFTP	Display Name	List	Display name of each start point

WebDAV Delivery

Item Name (ID)	Display Name	Type	Description
DestinationFolderURLs_SendToWebDAV	Http(s) URL	List	URL of the Send to WebDAV delivery destination

Item Name (ID)	Display Name	Type	Description
DisplayName_SendToWebDAV	Display Name	List	Display name of each start point

Send to CMIS

Item Name (ID)	Display Name	Type	Description
DestinationRepositoryName_SendToCMIS	Repository	String	Repository name
DestinationFolderPaths_SendToCMIS	Destination Folder Path(s)	List	Send to CMIS
RepositoryURL_SendToCMIS	URL	String	URL of the CMIS server

Send to DocumentMall

Item Name (ID)	Display Name	Type	Description
DestinationFolderPaths_SendToDocMall	Path	List	URL of the Send to DocumentMall delivery destination
Attributes_SendToDocMall	Attributes	List	Attribute name and its value Format: DisplayName:Target value=Source value
DisplayName_SendToDocMall	Display Name	List	Display name of each start point

Send to Exchange

Item Name (ID)	Display Name	Type	Description
UserName_SendToExchange	User Account Name	String	User account name for Send to Exchange
To_SendToExchange	To:	List	"To" address for Send to Exchange

Item Name (ID)	Display Name	Type	Description
Cc_SendToExchange	Cc:	List	"Cc" address for Send to Exchange
Bcc_SendToExchange	Bcc:	List	"Bcc" address for Send to Exchange
SendToMe_SendToExchange	My Address	List	Logged-in user's address
ReplyTo_SendToExchange	ReplyTo:	List	"ReplyTo" address
Sensitivity_SendToExchange	Sensitivity	String	E-mail sensitivity

Send to RightFax

Item Name (ID)	Display Name	Type	Description
FaxDestinations_SendToRightFax	Selected Destinations	List	Destination's fax number
Account_SendToRightFax	Account	String	Cost Center of the logged-in user
Matter_SendToRightFax	Matter	String	Cost Center based on the value of Account
CoverSheetFile_SendToRightFax	Cover Sheet File	String	Cover sheet file to be attached to the outgoing fax Format: A value selected from the drop-down list except for None and SystemDefault
Priority_SendToRightFax	Priority	String	Fax priority Format: Normal: 0, Low: 1, High: 2
FineMode_SendToRightFax	Fine Mode	String	Fax resolution Format: Checked: 1, Not checked: 0

Item Name (ID)	Display Name	Type	Description
HoldForPreview_SendToRightFax	Hold for Preview	String	Hold for Preview Format: Checked: 1, Not checked: 0
FromName_SendToRightFax	From Name	String	Senders name to be printed on the cover sheet

Send to SharePoint

Item Name (ID)	Display Name	Type	Description
DestinationFolderURLs_SendToSPS	URL	List	URL of the Send to SharePoint delivery destination
DisplayName_SendToSPS	Display Name	List	Display name of each start point

Send to Gmail

Item Name (ID)	Display Name	Type	Description
To_SendToEmail	To:	List	"To" address
Cc_SendToEmail	Cc:	List	"Cc" address
Bcc_SendToEmail	Bcc:	List	"Bcc" address
SendToMe_SendToEmail	My Address	List	Logged-in user's address

Send to Google Drive

Item Name (ID)	Display Name	Type	Description
DestinationFolderPaths_SendToFolder	Path	List	Path of the delivery destination

Send to Dropbox

Item Name (ID)	Display Name	Type	Description
DestinationFolderPaths_SendToFolder	Path	List	Path of the delivery destination

Managing Delivery Jobs

Use the Management Console to manage the list of delivery jobs.

Only job logs can be displayed on the operation panel of the device.

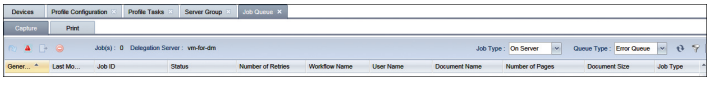
1. **From the navigation tree, click [Server Management].**
2. **From [Server Group], select the group to which the Delegation Server belongs to display the server list, and then select the Delegation Server with the job list to be checked.**

   You can select multiple servers.
3. **Click the (Job Queue) button.**
4. **Click the [Capture] tab.**
5. **Select [On Server] or [On Device] in [Job Type].**

   To display only the jobs of the workflows in which [On Server] is selected in [Job Processing Location], select [On Server]. Proceed to Step 7.

   To display only the jobs of the workflows in which [On Device] is selected in [Job Processing Location], select [On Device]. Proceed to Step 6.
6. **When [On Device] is selected in [Job Type], click (Select Device), select the device to display the job list, and then click [OK].**
7. **Confirm and delete the jobs as necessary.**

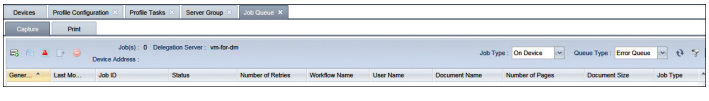
When [On Server] is selected



Item	Description
Job(s)	Displays the number of jobs in the job list. When the filter function is used, this displays the number of jobs matching the filter conditions.
Delegation Server	Displays the selected server. When [On Server] is selected in [Job Type], jobs that are being processed or have been processed on the server indicated here are displayed in the job list. To select a job on another server, repeat the procedure from Step 2.

Item	Description
Queue Type	Specify the queue type to narrow down the jobs in the job list. Select [Job Queue] to display the jobs being processed on the server, jobs in waiting, and jobs whose processing has been paused. Select [Error Queue] to display the jobs that were not delivered due to errors.
(Filter) button	Filters the jobs displayed in the job queue based on conditions specified in each column. • Specify the range of date and time in the [Generation Date] and [Last Modified Date] columns. • In the [Status] and [Job Type] columns, select the value to be used for the filter in each list. • Enter the search terms in the other columns.
(Refresh) button	Refreshes the job queue.
Job Queue	Displays the list of jobs in [Job Queue] or jobs that match the filter conditions in the order the jobs were added to the queue. The properties of each job are also displayed. Click the column title to sort the job queue in ascending or descending order. For the operations that can be performed on the job queue, see page 368 "Operating the Job Queue".

When [On Device] is selected



Item	Description
Job(s)	Displays the number of jobs in the job queue. When the filter function is used, this displays the number of jobs matching the filter conditions.
Device Address	Displays the host name of the selected server. To select a job on another device, repeat the procedure from Step 6.

Item	Description
Queue Type	Specify the queue type to narrow down the jobs in the job queue. Select [Job Queue] to display the jobs being processed on the device, jobs waiting in queue, and jobs whose processing has been paused. Select [Error Queue] to display the jobs that were not delivered due to errors.
(Filter) button	Filters the jobs displayed in the job queue based on conditions specified in each column. Specify the range of date and time in the [Generation Date] and [Last Modified Date] columns. In the [Status] and [Job Type] columns, select the value to use for the filter in each list. • Enter any search terms in columns other than shown above.
(Refresh) button	Refreshes the job queue.
Job Queue	Displays the list of jobs in [Job Queue], or jobs that match the filter conditions in the order the job was added to the queue. The properties of each job are also displayed. Click the column title to sort the job queue in ascending or descending order. For the operations that can be performed on the job queue, see page 368 "Operating the Job Queue".

Operating the Job Queue

Operations that can be performed on the job queue differ depending on the type of queue selected in [Queue Type].

When [Job Queue] is selected in [Queue Type]

- To cancel delivery of a job, select the job in the queue, and click (Cancel) on the toolbar. You can select more than one job to cancel delivery.
- Select a job and click (Move) to move the job to the top of the queue and process the job with the highest priority. You can select only one job at a time.

When [Error Queue] is selected in [Queue Type]

- To deliver a job again, select the job in the list, and click (Retry) on the toolbar. The job is moved from [Error Queue] to [Job Queue], and the status changes to [Waiting]. You can select more than one job for redelivery at a time.
- To display an image of the first page of a job that failed to be delivered, select the job and click (Error Image) on the toolbar. You can select only one job at a time.
- To generate images of a job that failed to be delivered and save the image to the location of the generated CSV file, select the job, and then click (Export) on the toolbar. You can select and export several job at a time.
- To delete the data of a job that failed to be delivered, select the job and click (Delete) on the toolbar. You can select and delete more than one job at a time.
- Select a job to display the detailed information of the job as [Detailed Log] below the job list. Information such as error messages and connection destinations is displayed in [Detailed Log].

Note

- Jobs in [Error Queue] are stored in the server or device. To prevent that too many serverless error jobs are accumulated in the hard drive of the device, it is recommended to enable [Job Storage Capacity Alert]. For details, see page 539 "Delegation Server Settings".

Checking Scan History

1. **From the navigation tree, click [Server Management].**
2. **From [Server Group], select the group to which the Delegation Server belongs to display the server list, and then select the Delegation Server with the job list to be checked.**

   You can select multiple servers.
3. **Click the (Scan History) button.**
4. **Check the scan history for the selected servers.**

Item	Description
Delegation Server	Displays the selected server.
(Filter) button	Filters the jobs displayed in the job queue based on conditions specified in each column. • Specify the range of date and time in the [Date/Time] column. • Enter the search strings in the other columns.
(Refresh) button	Refreshes the scan history.
Scan History	Display the list of scan history.

7. Using RICOH Streamline NX on a Mobile Device

This chapter describes the RICOH Streamline NX functions that can be used with a mobile device and how to manage a device from a mobile device. It also describes the settings for using the printing and delivery functions with a mobile device.

Functions Available on a Mobile Device

You can perform the following operations on a mobile device:

Printing secure print documents

The list of secure print jobs can be accessed, and released from a selected device. Print jobs are stored in advance on the Delegation Server or RICOH Streamline NX PC Client. In addition, documents can be printed to the Delegation Server from an app on a mobile device via the MIE.

To perform these operations, install the RICOH Streamline NX mobile app.

For details about the configuration necessary for using Secure Printing function, see page 381 "Configuring a Workflow Profile Associated with a Mobile Device".

For details about printing procedure, see User's Guide.

Delivering documents using workflows

A workflow configured in the Management Console can be used to deliver images captured with or stored on a mobile device.

To perform the operation above, install the RICOH Streamline NX mobile app.

For details about configuring the delivery function, see page 381 "Creating a Workflow". For details about delivering documents, see User's Guide.

Managing devices

Use your mobile device to check the status and information of devices registered to the RICOH Streamline NX system. For details, see page 376 "Screen Configuration of the RICOH Streamline NX Device Manager App".

To perform the operation above, install RICOH Streamline NX Device Manager app.

Sending print jobs

Print from an app on your mobile device to the RICOH Streamline NX system. For details, see User's Guide.

Mobile Intranet Extender

This software component identifies users on mobile devices, performs routing of the print jobs sent from mobile devices to the Delegation Server, and sends feedback on the print job status. You can install this software as an option when installing the Delegation Server. For details, see Installation Guide.

Note

- To print from a smart device, the PCL emulation must be supported on the printing device.
- Download the RICOH Streamline NX mobile app and RICOH Streamline NX Device Manager app from the mobile app store for each platform.
- Japanese version of Streamline NX Mobile Application is currently not provided.
- For details about storing secure print jobs, see page 186 "Configuring Secure Printing".
- For details about sending print jobs, see the User's Guide.
- For details about Mobile Intranet Extender, see Installation Guide.

Operating Environment

The RICOH Streamline NX mobile app and RICOH Streamline NX Device Manager app are supported under the following operating systems:

- Android 5.0 or later
- iOS 9.0 or later
- Windows Phone 10.0 or later

Note

- You can download the RICOH Streamline NX mobile app and RICOH Streamline NX Device Manager app from the mobile app store for each platform.
- To use the RICOH Streamline NX mobile app and RICOH Streamline NX Device Manager app on an iOS device, install the SSL certificate file for secure communication. For details, see "Installing the Certificate on a Mobile Device", User's Guide.

Configure the Initial Settings of the RICOH Streamline NX Device Manager App

When starting the RICOH Streamline NX Device Manager app for the first time after installation, use the following procedure to configure the initial settings:

Note

- The login screen is displayed the next time the application starts.
- Discovery, configuration, and report generation tasks cannot be created in the RICOH Streamline NX Device Manager app.
- [Use SSL] is always selected when you are using the iOS app. Also, the port to be used for HTTPS communication is selected as the default port number of the server.

1. **Start the RICOH Streamline NX Device Manager app.**
2. **Read [End User License Agreement], and press [Accept].**

   The [Settings] screen is displayed.
3. **Configure [Use SSL].**

   Select this check box if SSL is required to connect to the Core Server.

   When selecting this check box, use HTTPS to establish a connection to the Core Server.
4. **Enter the name or IP address of the Core Server in [Server Address].**
5. **Enter the port number in [Port Number].**

   When using http:

   "10100" is specified by default.

   When using https:

   "53443" is specified by default.

   Change the port number only if a different port was selected when the Core Server was installed.
6. **When IIS is used, enter the destination IIS alias in [IIS Alias].**

   Leave the field blank if IIS is not used.
7. **Press [Apply].**

   The login screen is displayed when the connection to the Core Server is successfully established.

   For the login procedure, see page 375 "Logging in to the RICOH Streamline NX Device Manager App".

Logging in to the RICOH Streamline NX Device Manager App

The login screen is displayed when you start the RICOH Streamline NX Device Manager app.

Note

- DeviceBasicRead privilege is required to use the RICOH Streamline NX Device Manager app. For details, see page 160 "Managing User Roles and Privileges".

Use the following procedure to log in to the RICOH Streamline NX Device Manager app:

1. **Select the profile to be used for [Profile]**

   Select the authentication profile that corresponds to the login user from the list.

2. **Enter the login user name and password for the RICOH Streamline NX Device Manager app.**

3. **To register the login information on your mobile device, select the [Remember me on this device] check box.**

   When this checkbox is selected, the user name will be automatically entered when you open the login screen. To log in, enter only the password.

4. **Tap [Login].**

   When login is successful, the home screen is displayed.

   For details about each screen of the RICOH Streamline NX Device Manager app, see page 376 "Screen Configuration of the RICOH Streamline NX Device Manager App".

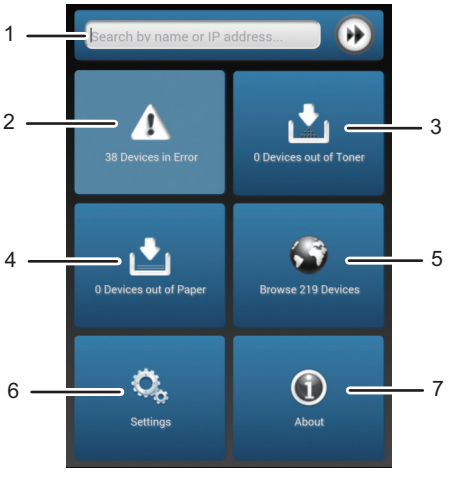
Screen Configuration of the RICOH Streamline NX Device Manager App

The following screens can be displayed in the RICOH Streamline NX Device Manager app.

- Home screen
- Select group/device list screen
- Device details screen (Description/Status History/Details/Photos)
- Settings screen
- About screen

Home Screen

The functions of the buttons displayed on the home screen are as follows:



DSW627

1. **Search**

   Performs a search based on the name or IP address of a device.

2. **Error**

   Displays the number of devices on which an error other than the out-of-toner/paper error occurs. Press to display the details.

3. **Out of Toner**

   Displays the number of devices that are out of toner. Tap to display the details.

4. **Out of Paper**

   Displays the number of devices that are out of paper. Tap to display the details.

5. **Browse Devices**

   Displays all the devices that are managed in RICOH Streamline NX. Tap to display the select group/device list screen. For details about the select group/device list screen, see page 377 "Select Group/Device List Screen".

6. **Settings**

   Press to display the configuration screen. For details about the configuration screen, see page 377 "Select Group/Device List Screen".

7. **About**

   Press to display the [About] screen. For details about the [About] screen, see page 379 "About Screen".

Note

- When the devices managed with [Group Restrictions] are restricted by role, the number of devices displayed on the home screen varies depending on the role of the logged-in user. For details about configuring [Group Restrictions], see page 167 "Configuring Group Restrictions".

Select Group/Device List Screen

The functions of the buttons displayed on the select group/device list screen are as follows:

DSW628

1. **Group/Category/Device List**

   Displays the device list for each group or category. Tap a group or category to display the list of devices in a group or category. When there are sub groups, the sub groups are displayed.

2. **Back**

   Returns you to the previous screen.

3. **Sort by**

   Tap this button to sort the list by the name, address, or status.

Device Details Screen (Description/Status History/Details/Photos)

The functions of the buttons displayed on the device details screen are as follows:

DSW629

7

1. **Overview**

   Displays the status icons of the functions (the system, printer, copier, fax, and scanner functions that are available on the device) on each device and a description.

2. **Status History**

   Displays the history of the device status changes (the date the status was recorded, status icon, description text, and other information).

3. **Details**

   Displays the properties information of the device in the following four categories: Main Properties, Status Details, Counters, and Toner Level. Scroll through the screen to view all the information.

4. **Photos**

   Displays the images that are registered as the photos of the selected device.

5. **Back**

   Returns you to the previous screen.

6. **Add Photo**

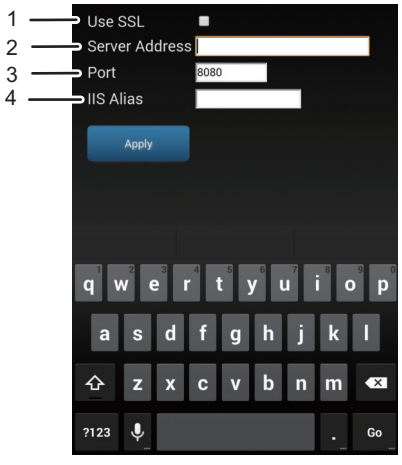
   Tap this button to select a photo that has been captured by the camera on your mobile device. Confirm the photo to add, and then enter a description. You can now configure the added photo to be displayed by default.

Note

- To upload a photo, log in using an ID with DeviceBasicWrite privilege.

Settings Screen

The functions of the buttons displayed on the settings screen are as follows:



DSW641

1. **Use SSL**

   When selecting this check box, use HTTPS to establish a connection to the RICOH Streamline NX server.

2. **Server Address**

   Enter the host name or IP address of the Core Server.

3. **Port Number**

   Enter the port number of the Core Server. “8080” is specified by default.

4. **IIS Alias**

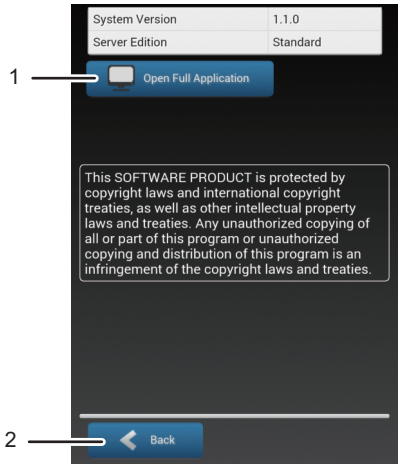
   Enter the destination IIS alias. Leave the field blank if IIS is not used.

Note

- [Use SSL] is always selected when you are using the iOS app. Also, the port to be used for HTTPS communication is selected as the default port number of the server.

About Screen

Use the about screen to confirm the system version information. The functions of the buttons displayed on the about screen are as follows:



DSW630

1. **Open Full Application**

   This opens the web Management Console in the default web browser on your mobile device.

2. **Back**

   Returns you to the previous screen.

Creating a Workflow

To use the delivery or printing function of secure print documents on a mobile device, create a workflow in the Management Console, and then configure a workflow profile to associate the workflow with a mobile device. This section describes how to configure a workflow profile to be associated with a mobile device.

page 329 "Configuring a Profile Task"

Note

- For details about configuring a workflow, see page 219 "Managing Document Delivery Functions".
- To apply the workflow profile on a mobile device, configure a profile task and synchronize it with the Delegation Server. After configuring the workflow profile, be sure to synchronize it with the server. For details about configuring a profile task, see page 329 "Configuring a Profile Task".

Configuring a Workflow Profile Associated with a Mobile Device

You can configure only one workflow profile that is associated with a mobile device on any one RICOH Streamline NX system.

1. **Click the following items in the navigation tree to open the [Profile Configuration] tab.**

   [Workflow] ▶ [Workflow Profile] ▶ [Profile Configuration]

2. **Click (Add).**

   The [Create Workflow Profile] window is displayed.

3. **In [Profile Name], enter the name of the workflow profile.**
4. **In [Description], enter the description of the workflow profile.**
5. **In [Input Source], select [Mobile].**
6. **Click [OK].**
7. **On the [General] tab, configure the profile properties.**
8. **On the [Workflows] tab, click (Add Group).**

   To add a mobile app or workflow to the created group, proceed to Step 12.

9. **On the [Group Properties] window, enter up to 128 characters for the group name.**
10. **In [Display], select [Yes] or [No].**

    When [No] is selected, the group is not displayed on the screen of the mobile device.

11. **Click [OK].**

12. **From the group tree, select the group to which to add a mobile app or workflow, and click (Add a workflow/application).**
13. **On the [Add a workflow/application] window, click the [Workflows] or [Mobile Applications] tab.**
14. **Select the workflow or mobile app to add, and click [OK].**

    Select the created workflow or a print-related mobile app ([Print using QR code], [Print Using NFC], or [Print using Device Search]).

    For details about creating a workflow, see page 227 "Creating a Workflow".
15. **From the group tree, select the mobile app or workflow added to the group, and from the properties displayed on the right side, select [Small], [Medium], [Large], or [Extra Large] for the display size of the buttons of the mobile app or workflow on the operation screen of the device.**
16. **Click (Save) on the workflow list.**
17. **Configure the profile task, associate the profile with a Delegation Server, and sync the profile settings.**

    For details, see page 329 "Configuring a Profile Task".

Note

- For details about the tabs, see "When [General] tab - Input Source is set to [Mobile]", page 599 "Workflow Profile".
- For how to operate the group tree, see "Group tree", page 321 "Configuring a workflow profile associated with a device".

8. Managing Servers

This chapter describes how to divide the Delegation Servers into groups, list of communication port numbers, and how to enable SSL on the Core Server.

Some of the procedures described in this chapter should only be performed by a server administrator.

Balancing the Workload among Servers

Configuring Load Balancing and Failover

Delegation Servers can perform various roles, such sending and receiving of print jobs, processing of the document scanning workflow, and managing of the devices, from a single computer. However, the hardware resources of a single server may not be sufficient to fulfill all the processing needs of a large-scale system, and this configuration may result in processing delays. To operate the system smoothly and prevent performance degradation, you may need to configure multiple Delegation Servers for load balancing the network traffic and processing load on the server hardware.

You can configure Delegation Servers to balance the workload of data processing among two or more Delegation Servers in [Delegation Server Failover/Load Balancing Groups] in the navigation tree.

Specify the priority Delegation Servers for authentication, capture, and print functions.

Also, if the primary Delegation Server fails to respond, job processing is automatically carried over by the secondary Delegation Servers.

1. **From the navigation tree, click [Server Management].**
2. **Click [Delegation Server Failover/Load Balancing Groups].**
3. **Click (Add).**
4. **On the [General] tab, configure Connection Timeout, Processing Timeout, and the other settings.**

   For details about the configuration items, see page 631 "Delegation Server Failover/Load Balancing Groups".
5. **Click [Authentication], [Capture], or [Print] tab, and then select the server to balance the workload.**

   1. Click (Add).
   2. Click [All Servers], or select a server group and then display a server.
   3. Select a server, and then click [▶] to add it as a target server to balance workload.
   4. Click [OK].

6. **Click [▲] or [▼] to specify the priority among servers.**

   The server on the top has the highest priority, and when the timeout period elapses, the processing is carried over to the other servers according to the order in the list.

7. **Click (Save) when the configuration is complete.**

Note

- When the fail over and load balancing groups for Delegation Servers are specified in [Configuration] ▶ [Streamline NX Embedded Settings] ▶ [Embedded Setting], be sure to specify more than one Delegation Server in this setting on each of the [Authentication], [Capture], and [Print] tabs. Those functions are processed via the Delegation Servers and cannot be used if the servers are not specified.

Dividing Servers into Groups for Management

When you are operating multiple Delegation Servers and assigning a different role for each, you can manage them more easily by creating a group for each role and dividing the servers into the created groups in the Management Console.

1. **From the navigation tree, click [Server Management].**
2. **Right-click [Server Group] and select [Add Group].**

   In [Server Management] in the navigation tree, you can add groups only and cannot create categories.

3. **Enter the name of the group you want to create, and click [OK].**

   For example, enter the category of the process the server is responsible for such as "Print Function" or "Scan Function" in the name of the group you want to create.

   Repeat the same procedure to create as many group names as required.

4. **Drag and drop the server name displayed in the list to the target group in the navigation tree.**

   You are recommended to assign all servers to the created groups and leave no servers in the [Unassigned] group.

Server management icons

Icon	Description
	Move the Delegation Server to another computer.
	Clears the cache on the Delegation Server.

Icon	Description
	Displays the job queue screen. Delivery jobs and print jobs can be managed. For details, see the followings: • Delivery jobs: page 366 "Managing Delivery Jobs" • Print jobs: page 193 "Managing Job List"

Note

- If you rename the Delegation Server on this screen, you must modify the configuration file on the Delegation Server side (dm.properties -> dm.serverName=xxxx).

Receiving Notifications from the Server

You can receive a notification, when a problem occurs on the server or the hard disk drive on the server is running out of free space. The configuration specified here is applied to all Delegation Servers.

The types of notification that can be received are as follows:

- System Error, Commercial Certificate Expiration, HDD Capacity

1. **Click the following items in the navigation tree to open the [Delegation Server Settings] tab.**

   [System] ▶ [Server Settings] ▶ [Delegation Server Settings]

2. **Click the [Server Notifications] tab.**
3. **Configure the type and language of the notification you want to receive from the server.**
   - System Error

     You can receive a notification when an internal error occurs on the Core Server or Delegation Server.
   - Commercial Certificate Expiration

     You can receive a notification when a commercial certificate expires or is renewed.
   - HDD Capacity

     You can receive a notification when the remaining amount of the hard disk drive on the Core Server reaches [Remaining Capacity When Nearly Full] specified in [System Data Management].
4. **Click (Save) when the settings are completes.**

Note

- When applying a specific configuration to each Delegation Server, select [Server Management] in the navigation tree and configure the Delegation Server one by one. For details about the configuration items, see page 629 "Server Group".

Changing the IP Address of a Server or Device

Use the procedure below to change the IP address of a server or device due to a move of the server or device, restructuring of the network configuration, or change to the organization.

Server

Use [Control Panel] in Windows to configure the settings. Use a user account with administrative privileges to log on to Windows, and configure the settings.

Device

Use the operation panel of the device to configure the settings. Use a user account with administrative privileges to log in to the device, and configure the settings.

Changing the IP Address of the Server

Windows Server 2012 R2 is used as an example.

1. **Use a user account with administrative privileges to log on to Windows.**
2. **Stop the RICOH Streamline NX service.**

   For details about stopping a service, see page 394 "Stopping or Restarting Services".
3. **Select [Control Panel] ▶ [Network and Sharing Center] to open the configuration screen.**
4. **Click the interface name of the connection displayed in the [View your active networks] area.**
5. **Click [Properties].**
6. **Select [Internet Protocol Version 4 (TCP/IPv4)], and then click [Properties].**
7. **Configure the IP address, subnet mask, default gateway, and other settings.**
8. **Click [OK].**
9. **Click [OK] to close the Properties screen.**
10. **Display the server manager, and check that the IP address of the local server is changed to the new IP address.**
11. **Start the RICOH Streamline NX service.**

    For details about starting a service, see page 394 "Stopping or Restarting Services".

Note

- After changing the IP address of the Core Server, change the IP address of the connecting Core Server on all Delegation Servers.
- To enable SNMP traps of the device after changing the IP address of the Delegation Server, apply to the device the device preferences template that enables [Enable SNMP Traps for SLNX]. The setting items in the template are displayed on the following screen:

[Configuration] ▶ [Standard Device Preference] ▶ [SNMP]

- To resume collecting logs of the target device after changing the IP address of the Delegation Server, use the Log Collection template.

Changing the IP Address of a Device

An MFP equipped with Smart Operation Panel is used as an example in the explanation.

1. **Log in to the device from the operation panel of the device as the network administrator, and then display the default settings screen.**

   The method to display the default settings screen differs depending on the device. For details, see the manual that is provided with the device.
2. **Press [Interface Settings] on the menu screen of [System Settings].**
3. **Press [Machine IPv4 Address].**
4. **Press [Change] under [Machine IPv4 Address].**
5. **Use the numeric keypad to enter the IPv4 address, and then press [#].**
6. **Press [Change] under [Subnet Mask].**
7. **Use the numeric keypad to enter the subnet mask, and then press [#].**
8. **Press [Settings].**
9. **Press [IPv4 Gateway Address].**
10. **Use the numeric keypad to enter the gateway address, and then press [#].**
11. **Press [Settings].**
12. **Press [Print List], and check that the settings are correct.**

Note

- After changing the IP address of the device, perform discovery again. For details about discovery, see page 77 "Searching for Devices".

Migrating the System to Different Hardware

This section describes how to replace the server hardware on which Core Server or Delegation Server is currently running with new hardware. To migrate the system to different hardware, create a backup of the data on the currently operating server hardware, and then restore the backed up data on the new server hardware.

Important

- **To use the @Remote function, perform a data migration on the @Remote center side. Before starting data migration, contact your RICOH service representative.**

1. **Deactivating the License**

   All licenses are associated with the network interface information of the server hardware. To use the same license on new server hardware to activate the product, deactivate the license that you are using on the current server hardware.

   To deactivate the license, select [System] ▶ [Server Settings] ▶ [Activation/Usage Report] in the navigation tree to open the tab for the procedure, and then deactivate all registered licenses.

2. **Backing Up the System**

   Create a backup of the data on the server hardware that you are currently using.

   Note

   - For details about creating a backup, see "Backing Up and Restoring RICOH Streamline NX", Installation Guide.

3. **Installing the System**

   Install RICOH Streamline NX on the new server hardware.

   Note

   - For details about the installation procedure, see "Installing RICOH Streamline NX", Installation Guide.

4. **Restoring the System**

   Restore the data on the new server hardware.

   Note

   - For details about the restoration procedure, see "Backing Up and Restoring RICOH Streamline NX", Installation Guide.

5. ▶ Activating the System

Log in to the Management Console on the new server hardware, and activate the license.

To activate the license, select [System] ▶ [Server Settings] ▶ [Activation/Usage Report] in the navigation tree to open the tab for the procedure, and activate all licenses.

Note

- For details about the activation procedure, see “Activating RICOH Streamline NX”, Installation Guide.

Manage Delegation Servers

If your deployment uses multiple Delegation Servers to manage the devices, you can use the tools in the [Server Group] tab to rename a Delegation Server or to move a Delegation Server from one computer to another.

Important

- **This option is only available to users with the SysConfigWrite access privilege. For details about privileges, see page 557 "User Roles".**

The [Server Group] tab reports communication details, device count, and current status per Delegation Server. This tab also allows you to:

- Rename a Delegation Server

  If you deploy multiple Delegation Servers, it is important to rename the servers to reflect your organization. By default, a single Delegation Server is identified as ‘localhost’.

- Move a Delegation Server

  Move a Delegation Server from one computer to another. Instructions are provided below.

Note

- The current status per Delegation Server only indicates how many days have passed since the Core Server communicated with each Delegation Server for the last time by the following colors. Note that it does not show if the Delegation Server currently exists or not.
  - Green: one day or less has passed since the last communication time
  - Orange: more than a day, but three days or less have passed since the last communication time
  - Red: more than three days have passed since the last communication time

Move a Delegation Server

1. **Before you can move the Delegation Server from one computer to another, shut down the original Delegation Server first.**
2. **On the navigation tree, click [Server Management], then locate the [Server Group] folder.**
3. **Select the Delegation Server you want to move, then click (Move).**

   Important

   - **If you failed to shutdown the Delegation Server before clicking (Move), you will receive a message indicating that you must shut it down before you can move it.**
4. **In the [Move] screen, identify the computer where you are moving the Delegation Server to, then click [OK].**
5. **Install and start the Delegation Server on the new computer.**

   For details, see Installation Guide.

   When the RICOH Streamline NX service is started, the service will register with the Core Server, and the configuration/devices that were previously assigned to the shutdown Delegation Server are downloaded to the new Delegation Server.

Note

- If you start the original Delegation Server again after you move it to another computer, the original Delegation Server will register as a new Delegation Server.
- The following are not moved to a new Delegation Server when moved to another computer:
  - Scan history
  - Scan jobs
  - Print jobs
  - Device Job Log and Device Access Log
- After moving the Delegation Server, it is necessary to uninstall and re-install Streamline NX Embedded Application on devices. if the old Delegation Server is eliminated and does not belong to any group in [Delegation Server Failover/Load Balancing Groups].

Changing the Domain Name of a Network

To change the domain name of a network due to a change in the company name or a restructuring of the organization, use DNS manager in Windows Server to create a new forward lookup zone and copy the information of the existing domain to the new domain.

Important

- **The workflow described below shows the overview of the procedures to change the domain name. Changes to the domain name must be made only by an engineer experienced in managing Windows Server.**

1. **Stopping the RICOH Streamline NX Service**

   Use a user account with administrative privileges to log on to Windows, and then stop the RICOH Streamline NX service.

   Note

   - For details about stopping a service, see page 394 "Stopping or Restarting Services".

2. **Backing Up the System**

   Back up the RICOH Streamline NX system in case a problem occurs.

   Note

   - For details about creating a backup, see "Backing Up and Restoring RICOH Streamline NX", Installation Guide.

3. **Creating a New Forward Lookup Zone**

   Start [Control Panel] ▶ [Administrative Tools] ▶ [DNS Manager], and create a new forward lookup zone.

   Note

   - For details, see the technical information from Microsoft.

4. **Migrating the Domain by Using Commands**

   - To migrate the domain, use the rendom command. Obtain Domainlist.xml, and rename the domain name.
   - To copy information from the existing domain, use the repadmin command.

   Note

   - For details, see the technical information from Microsoft.

5. **Integrating the New Domain into Active Directory**

- Start [Control Panel] ▶ [Administrative Tools] ▶ [DNS Manager], and change the type of the newly created forward lookup zone to [Active Directory-integrated].
- Delete the forward lookup zone of the old domain.

Note

- For details, see the technical information from Microsoft.

6. **Starting the RICOH Streamline NX Service**

After changing the domain, use a user account with administrative privileges to log on to Windows, and then start the RICOH Streamline NX service.

Note

- You do not have to perform this procedure if [Automatic] is selected as the startup type of the service.

Stopping or Restarting Services

To implement changes and adjustments to the system configuration such as backing up the system and enabling SSL communication, you may need to stop, start or restart the related services. Log on to the Windows server to operate the services. Windows Server 2012 R2 is used as an example in the procedure shown below.

1. **Use a user account with administrative privileges to log on to Windows.**
2. **Click [Control Panel] ▶ [System and Security] ▶ [Administrative Tools].**
3. **Click [Services].**
4. **Select the service you want to change in the list, and then click [Stop], [Start], or [Restart].**

   There are two types of RICOH Streamline NX services as follows:

   - RICOH SLNX Central Manager Service
   - RICOH SLNX Delegation Server Service
   - RICOH SLNX Mobile Intranet Extender Service

   Change the settings in both of those services. You can change either service first.
5. **After changing the settings, start that services so that they are [Running], and then close the [Services] screen.**

Managing the System Capacity

The server stores various types of data such as the system data base information and the files uploaded by the users. To prevent stops in user operations, constantly monitor the amount of free space on the hard disk drive.

In addition, consider how much space to allocate from the limited space on the hard disk drive for different purposes. If the amount of free space is insufficient, you may need to perform maintenance operations such deleting and archiving of old data more frequently.

Allocate the appropriate amount of storage for your operating environment, and manage the data capacity accordingly.

Data Types

There are two types of data as follows:

- Database information

  This includes all the information required to manage and monitor the connected devices such as the system settings, configuration settings, and security profiles.

- User and system generated data

  The device firmware and applications to be stored in the file repository, secure print jobs, template for reports and dashboards, and various types of logs fall under this category.

Data storage destination

Data type	Storage destination
Firmware	RICOH Streamline NX data folder*
Embedded Configuration	RICOH Streamline NX data folder*
Secure Print Jobs	Delegation Server data folder*
Delivery job	Delegation Server data folder*
Report/dashboard templates	Core Server data folder*
Logs	Database

* When the Core Server and Delegation Server are installed to separate hardware and a configuration task is executed, the same file is saved to the Core Server and Delegation Server.

Free Space Notifications

Configure the free space notification for the data storage capacity and database capacity. You can configure different settings for sending a notification for the amount of free space in the database and on the hard disk drive.

Configure the settings related to the free space notification of the Core Server, navigate to the [System Data Management] tab.

[System] ▶ [Server Settings] ▶ [System Data Management]

Configure the settings related to the free space notification of the Delegation Server, navigate to the [Delegation Server Settings] tab.

[System] ▶ [Server Settings] ▶ [Delegation Server Settings]

Note

- For details about the setting items, see page 527 "System Data Management" or page 539 "Delegation Server Settings".

Managing the System Data

Configure the data storage period, HDD/database capacity, and data deletion settings in System Data Management.

The data storage period specifies the default storage period of the following logs:

- Device Eco Log
- Device Access Log
- Device Job Log
- Status
- Device Counter
- User Counter
- System/Tasks/Auditing/Notifications Logs
- Report

The storage period of each data set is individually managed.

1. **Click the following items in the navigation tree to open the [System Data Management] tab.**

   [System] ▶ [Server Settings] ▶ [System Data Management]

2. **Specify the period to store the logs in [Data Storage Period].**

   All logs are stored for one year by default.

Note

- When there is sufficient hard disk drive space, select the [Unlimited] check box by all items to store all data unless the condition of the hard disk drive space setting is met. For details about the data storage specification, see Planning Guide.

3. **In [HDD Capacity], specify the capacity to send a notification about the amount of available space.**

   1. In the [Remaining Capacity When Nearly Full] field, enter the remaining capacity of the hard disk drive in gigabytes to trigger the nearly full status. By default, the "Nearly full" status is reported when the available space reaches 2 GB or less.
   2. In the [Remaining Capacity When Full] field, enter the remaining capacity of the hard disk drive in gigabytes to trigger the capacity full status. The [Deletion Settings When Capacity is Full] option is applied and the data is deleted according to this setting.

Note

- When you specify [System Alert Notification] ([System] ▶ [Server Settings] ▶ [Network] in the navigation tree) for the nearly full status, a notification about the available space is sent to the specified e-mail address.

4. **When using SQL Express, enter the following items in "DB Capacity":**

   1. In the [Remaining Capacity When Nearly Full] field, enter the remaining capacity of the database in gigabytes to trigger the nearly full status. By default, the "Nearly full" status is reported when the available space reaches 2 GB or less.
   2. In the [Remaining Capacity When Full] field, enter the remaining capacity of the database in gigabytes to trigger the capacity full status. The [Deletion Settings When Capacity is Full] option is applied, and the data is deleted according to this setting.

Note

- When [System Alert Notification] ([System] ▶ [Server Settings] ▶ [Network] in the navigation tree) for the database capacity full status is specified, a notification about the available space is sent to the specified e-mail address.

5. **In [Deletion Settings When Capacity is Full], configure the settings as shown below.**

   By default, the Device Status data for one day and data for Device Eco Log, Device Access Log, Device Job Log, Counter, User Counter, system/task/auditing/notification logs and reports for one month are retained, and any older data will be deleted.

   To prevent specific data from being deleted, select [Do not Delete].

6. **Click [Save].**

Note

- The data is deleted when RICOH SLNX Central Manager Service is restarted or every 24 hours after the service is started according to the settings configured in [Data Storage Period] or [Deletion Settings When Capacity is Full]. Even if the data is deleted, the blank space of the hard disk is not released until database is compressed manually.

Compressing the Database

Many of the data obtained by RICOH Streamline NX are stored on Microsoft SQL Server. However, data related to @Remote, device job log, device access log, and temporary data are also stored in the internal database (Derby Database).

Compress the database after deleting the data to reserve a free capacity on the hard disk.

For detailed procedure for compressing each database, see the following information:

- Microsoft SQL Server

  https://msdn.microsoft.com/library/ms189035(v=sql.110).aspx

Compressing the internal database

Use the database compression tool for tables associated with Derby Database. You can free up space on the hard drive by deleting device job logs and device access logs, using the database compression tool.

Important

- When you use the database compression tool, the RICOH Streamline NX service stops. Therefore, you cannot use RICOH Streamline NX while using the database compression tool.
- The conditions for using the database compression tool are as follows:
  - The server is installed with Java.
  - Polling, configuration, and other RICOH Streamline NX tasks must be stopped.
  - You must have Windows Administrator privileges.
  - Ensure that there is sufficient disk space for compression.
    If an error message is displayed indicating that the drive is full when the database compression tool is used, safeguard the other files temporarily.

1. Extract (install-path)\Tools\SLNX_ShrinkInternalDB.zip to a folder.
2. Move the extracted SLNX_ShrinkInternalDB folder to the install folder of RICOH Streamline NX.

   The default path of the install folder is C:\Program Files\Ricoh\Streamline NX.

3. **Run "shrink.bat" in the SLNX_ShrinkInternalDB folder.**

   When the process is completed, the following message is displayed on the command prompt screen.

Message	Description
compress derby database end. Starting service. Service has started successfully.	The process ended successfully.
Disk has insufficient space. compress derby database failed.	The process ended abnormally. Ensure that there is sufficient disk space, and then run the database compression tool again.
Database (path) not found. compress derby database failed.	The process ended abnormally. Move the SLNX_ShrinkInternalDB folder to the install folder of RICOH Streamline NX, and then run the database compression tool again.
Access denied. compress derby database failed.	The process ended abnormally. Log in with Administrator privileges, and then run the database compression tool again.

Formula for Calculating the Data Amount Stored in the Hard Disk Drive

The following describes the formula for calculating the estimated free space to be allocated for various data.

Secure Print Jobs

The following information is required to calculate the amount of storage required to store Secure Print Jobs:

- Total number of pages in Secure Print Jobs per month
- Average number of pages in a job
- Number of business days per month
- Number of business hours per day

$$\text{total print job storage per DS (MB)} = \frac{\left[\frac{\text{Number of monthly usage pages by DS}}{\text{Average number of pages in an individual print job}}\right] \times \text{Average file size of print job (KB)} \times \text{Job Storage period (hours)} \times \text{safety factor (1.5)}}{\left[\text{Number of working days per month} \times \text{Number of working hours per day}\right] \times 1024}$$

DSW660

Various Logs

Up to 4 GB of storage space is required to store the various log types. There are five types of logs as follows for a total required storage capacity of up to 20 GB:

- Task Log
- Notification Log
- Audit Log
- System Log
- Report Log

Formula for Calculating the Database Capacity

The following information is required for calculating the rough estimation of database capacity needed.

- Number of pages used per month
- Average number of pages in a job
- Number of users
- Number of devices
- Number of devices used per user
- Number of times the device information is obtained per hour
- Number of Standard Device Preferences templates
- Number of Standard Device Preferences profiles
- Number of RICOH Streamline NX server components
- Number of servers
- Number of business hours per day
- Unit of capacity (MB) (value: 1024)

The rough estimation of database capacity needed is the sum of the following values:

Templates and profiles

$$\text{Templates and Profiles data Total (MB)} = \frac{\left[\left[\text{Total number of templates} \times \text{Transaction data per template (63 KB)}\right] + \left[\text{Total number of profiles} \times \text{Transaction data per profile (8 KB)}\right]\right] \times \text{safety factor (1.5)}}{1024}$$

DSW661

Devices and servers

$$\text{Devices and Servers data Total (MB)} = \frac{\left[\left[\text{Total number of devices} \times \text{Transaction data per device (30 KB)}\right] + \left[\text{Total number of servers} \times \text{Transaction data per server (10 KB)}\right]\right] \times \text{safety factor (1.5)}}{1024}$$

DSW662

Device Information

$$\text{Polling data Total (MB)} = \frac{\left[\text{Total number of devices} \times \left[\text{Number of status polling transactions per hour} \times 24\ \text{(hours)} \times 31\ \text{(days)}\right] \times \text{Transaction data per server (0.4 KB)}\right] \times \text{safety factor (1.5)}}{1024}$$

DSW663

Accounting information

$$\text{Accounting Data (MB)} = \frac{\left[\frac{\text{Number of monthly usage pages by copy}}{\text{Average number of pages per copy job}} + \frac{\text{Number of monthly usage pages by scan}}{\text{Average number of pages per scan job}} + \frac{\text{Number of monthly usage pages by print}}{\text{Average number of pages per print job}}\right] \times \text{Transaction data per job (2.5 KB)} \times \text{Storage period for Usage Log (month)} \times \text{safety factor (1.5)}}{1024}$$

DSW664

Reports

$$\text{Reporting Data (MB)} = \frac{\left[\text{Number of users} \times \text{Number of devices used per user} \times \text{Transaction data per report (0.2 KB)}\right] \times \left[\text{Storage Period Daily report (month)} + 31\ \text{(days)} + \text{Storage Period for Monthly report (month)}\right] \times \text{safety factor (1.5)}}{1024}$$

DSW665

Users and groups

$$\text{User and Group Profile Data (MB)} = \frac{\left[\text{Number of users} \times \text{Transaction data per users (6.4 KB)}\right] \times \text{safety factor (1.5)}}{1024}$$

DSW666

Deleted jobs

$$\text{Deleted Job Data (MB)} = \frac{\left[\text{Number of monthly usage pages by print job deletion} \times \text{Transaction data per job (2.5 KB)} \times \text{Storage period for Usage Log (month)}\right] \times \text{safety factor (1.5)}}{1024}$$

DSW667

Job name

$$\text{Job Name Data (MB)} = \frac{\left[\frac{\text{Number of monthly usage pages by print}}{\text{Average number of pages per print job}} \times \text{Transaction data per job (2.7 KB)} \times \text{Storage period for Usage Log (month)}\right] \times \text{safety factor (1.5)}}{1024}$$

DSW668

Print job information

$$\text{Print job information data Total (MB)} = \frac{\left[\frac{\text{Number of monthly usage pages by DS}}{\text{Average number of pages per print job}} \times \text{Transaction data per job (2 KB)} \times \text{Job Storage period (hours)}\right] \times \text{safety factor (1.5)}}{\left[\text{Number of working days per month} \times \text{Number of jobs which a server component can process in a minute}\right] \times 1024}$$

DSW669

Report information

$$\text{Print information data Total (MB)} = \frac{\left[\frac{\text{Number of monthly usage pages by print}}{\text{Average number of pages per print job}} \times \text{Transaction data per job (7 KB)} \times \text{Retention period of reporting data (60 days)}\right] \times \text{safety factor (1.5)}}{\text{Number of working days per month} \times 1024}$$

DSW670

Enabling SSL

When installing the Core Server or Delegation Server with the setting to avoid using SSL, install the certificate from the Management Console and disable the HTTP connection.

Important

- **Restarting of the service is required to complete this setting. If the system is already running, configure the setting on the date when the service can be restarted without disrupting the tasks of users.**

Note

- When installing the Core Server or Delegation Server with the setting to avoid using SSL, install the certificate from the Management Console and disable the HTTP connection.

Install SSL Certificate

Install certificates on the Core Server and Delegation Server to use SSL.

RICOH Streamline NX supports certificates issued from Windows Local Certificate Authority, certificates issued from root certificate authorities (root CA) or intermediate certificate authorities (intermediate CA) such as Verisign, Thawte, and Entrust, in addition to self-signed certificates.

Use the following procedure to set the SSL certificate.

Note

- For the functional outlines and installation procedure of Windows Local Certificate Authority, see the Microsoft website.
  - https://technet.microsoft.com/library/cc755071(v=ws.11).aspx
  - https://technet.microsoft.com/library/jj717285(v=ws.11).aspx

1. **Click the following items in the navigation tree to open the [Networking] tab.**

   [System] ▶ [Server Settings] ▶ [Networking]

2. **Select [Commercial Certificate Authority] in [Use SSL], and then enter the port number to use for SSL communication.**

3. **If there is no SSL certificate, create a Certificate Signing Request (CSR).**

   1. Click [Create CSR].
   2. Enter the information required to create a CSR:

      Server Name, Organization, State/Province, Department Name, City/Locality, Country Code (two alphabetical letters)
   3. Click [Create CSR].
   4. Copy and paste the displayed information to the form to be submitted to the CA.
   5. Store the certificate issued from the Certificate Authority.

4. **Click [Install Certificate].**
5. **Select the type of certificate, click [Browse], and then select the certificate on the server or network.**
6. **Click [Upload].**
7. **Click [Save] at the bottom of the [Networking] tab.**

   You are automatically logged out from the Management Console, and a new login screen using the new URL via SSL communication is displayed after 30 seconds.

When the Core server, and Delegation or MIE server are installed on separate hardware

When the Core server, and Delegation or MIE server are installed on separate hardware, SSL is not enabled if only the certificate has been uploaded from the Management Console. You must also use SLNX Certificate Tool on the Delegation/MIE server to install the SSL certificate. Use the following procedure to make configuration:

1. **Start SLNX Certificate Tool.**

   (tool storage destination path)

   - Delegation Server

     \tools\SLNXCertificateTool\SLNXCertTool_DS.exe
   - MIE Server

     \tools\SLNXCertificateTool\SLNXCertTool_MIE.exe
2. **Select the interface language to use during installation.**

3. **Click [Create CSR] to create a Certificate Signing Request (CSR).**

   1. Enter the following information that is required to create a Certificate Signing Request (CSR):

      Server Name, Organizational Unit, City/Locality, State/Province, Country (two alphabetical letters)

   2. Click [Create].
   3. Copy and paste the displayed information to the form to be submitted to the Certificate Authority.
   4. Save the certificate issued from the Certificate Authority.

4. **Click [Install intermediate Certificate] in SLNX Certificate Tool.**
5. **Select the intermediate CA certificate issued from the Certificate Authority, and then click [Open].**
6. **Click [Install Certificate] in SLNX Certificate Tool.**
7. **Select the certificate issued from the Certificate Authority, and then click [Open].**
8. **Exit SLNX Certificate Tool.**

Note

- To trust all certificates while operating the system, select the [Trust All Certificates] check box.

Disabling HTTP Connection

To disable connection via HTTP after checking that you can establish a connection via HTTPS, configure the following settings:

1. **Click the following items in the navigation tree to open the [Networking] tab.**

   [System] ▶ [Server Settings] ▶ [Networking]

2. **Select the [Disable HTTP] check box.**
3. **Click [Save] at the bottom of the [Networking] tab.**

   When the Core server and the Delegation/MIE server are installed on the separate hardware, proceed to the next step to enable SSL for the Delegation Server and the MIE Server. Perform the following procedure for all Delegation servers and MIE servers.

   When the Core server and the Delegation/MIE server are installed on the same hardware, the configuration is complete.

4. **From [Control Panel] of Windows, open [Programs and Features], select RICOH Streamline NX, and then click [Change].**

5. **On the [Web Server] screen of the installation wizard, select the [Use SSL/TLS] check box, and then specify the port number.**

   When the [Use SSL/TLS] check box is selected, connection via HTTP is disabled for the Delegation Server and MIE Server.

6. **Follow the instructions on the screen to complete the installation wizard.**

Establishing SSL/TLS Connection between the Core Server and the External Database

The SSL encrypted communication between the Core Server and the external SQL database is disabled by default. Edit the core.properties file and restart the service of the Core Server to use SSL for connecting the Core Server and the external SQL database.

1. **Log on to the server and stop "RICOH SLNX Central Manager Service".**
2. **Open the following folder:**

   `(data_storage_path)\data\configuration\core`

3. **Open the core.properties file, and then edit the line with the description "core.database.connection.encrypt" as follows:**

   ```
   core.database.connection.encrypt=1
   ```

4. **To enable the validation of the server certificate, edit the line with the description "core.database.connection.encrypt.usetruststore" as follows:**

   ```
   core.database.connection.encrypt.usetruststore=1
   ```

   When the server certificate validation is executed, the root certificate of the certificate used by the database server must be trusted. To add a root certificate as the trustworthy certificate, follow the procedure below:

   1. Export the root certificate to a PKCS7 file.
   2. Extract the root certificate into the \data\repository\certs folder.

      The file name of the root certificate should be in the "cert_xxxx.p7b" format. xxxx can be any string.

   3. Delete the truststore file.

      The truststore file is stored in the following folder:

      `\data\repository\certs`

5. **Restart "RICOH SLNX Central Manager Service".**

Disabling SSLv3 and SSLv2Hello Protocols

The following SSL/TLS versions are enabled by default for RICOH Streamline NX:

- TLSv1.2
- TLSv1.1
- TLSv1.0
- SSLv3
- SSLv2Hello

In RICOH Streamline NX, you can disable the SSLv3 and SSLv2 protocols in order to avoid vulnerability in SSL/TLS communications.

Important

- **It is recommended to disable SSLv3 and SSLv2Hello unless it is required in your environment.**

1. **Log on to the server, and then stop the following services.**

   Core Server: RICOH SLNX Central Manager Service

   Delegation Server: RICOH SLNX Delegation Server Service

   You can stop either of the above first.

2. **Prepare the following property files provided in the installation media of RICOH Streamline NX.**

   - sslServer.properties
   - sslClient.properties
   - sslAtRemoteServer.properties

   The property file is stored in "\Documentation\Admin_Guide\Sample_Files".

3. **Copy three property files prepared in Step 2 to the "Configuration" folder in the destination to install the server. These files contains the protocols to be enabled or disabled, and the encryption settings to disable dangerous protocols.**

4. **Start the service stopped in Step 1.**

   Start "RICOH SLNX Central Manager Service" for the Core Server first, and then "RICOH SLNX Delegation Server Service" for the Delegation Server.

Note

- When the SSLv3 and SSLv2Hello protocols are disabled, communication with the external systems that only supports them are also disabled.
- The results of this setting is the following:
  - RICOH Streamline NX cannot receive device logs (job logs and access logs) from some devices with Smart Operation Panel.

- To restore the default settings, stop "RICOH SLNX Central Manager Service" and "RICOH SLNX Delegation Server Service", delete the property files added in Step 3 from the "Configuration" folder, and then start the stopped services again.

Available encryption algorithms and default settings

RICOH Streamline NX communicates with an external system using the strongest encryption algorithm or the algorithm with the required strength.

See the table below for the available encryption algorithms and the default settings of RICOH Streamline NX. "N/A" indicates that the protocol does not support the algorithm.

Algorithm	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	N	N	N	N
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	Y	Y	Y	Y
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
SSL_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	N	N	N	N
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	N	N	N	N
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y

Algorithm	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_RSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_RSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	N/A	N/A	N/A	Y

9. Managing System Operation and Logs

This chapter describes the management of tasks and logs performed by the system, error code list, and troubleshooting.

Managing Tasks

Perform tasks to search for devices, obtain device information, and install applications. This chapter describes how to check the status of a task, operate a task, and configure a schedule to execute a task at a specified time.

Checking Scheduled Tasks

1. **Click the following items in the navigation tree to open the [Scheduled Tasks] tab.**

   [System] ▶ [Scheduled Tasks]

   Displays the list of tasks to be executed.

Items displayed in the scheduled tasks list

Item	Description
Name	Displays the name entered when the task was registered.
Description	Displays the description entered when the task was registered.
Type	Displays the type of a task. Example: Discovery, Status Polling
Enable	Displays whether the schedule is enabled or disabled.
Schedule Type	Displays the schedule setting. Example: Once Only, Interval, Repeatedly, Immediately, Disabled
Interval	When the schedule type is [Interval Time], Interval displays the specified time interval.
Start	Displays the date and time to start the task.
Update	Displays the date and time you created or edited the task.
User	Displays the name of the user that created or edited the task.

Item	Description
Delegation server	Displays the Delegation Server name.

Note

- You cannot change a schedule or delete a task in the scheduled task list. Delete a task or change its schedule in the destination to which you registered the setting.

Viewing the Task Log

The task log records task execution results. For each task, you can confirm the operation result per device or setting item.

You can also check the progress of a currently executing task and suspend or resume a task in the task log.

Note

- A new log entry is added to the task log each time you start a new task. RICOH Streamline NX updates the log while a task is being executed. When the task is completed, the log is updated with the final result.
- Tasks are executed based on the time of a location where the Delegation Server is placed. Even if you created a task to be applied to all devices, the task is executed based on the time setting of each Delegation Server if multiple servers are located in different time zones.

1. **Click the following items in the navigation tree to open the [Task Log] tab.**

   [System] ▶ [Logs] ▶ [Task Log]

   The list of task logs is displayed.

   Items displayed in the task log list

Item	Description
Start Date	Displays the date and time when the task started.
End Date	Displays the date and time when the task ended.
Task Name	Displays the name of the registered task.
Category	Displays the function category. Example: Device Configuration, Device Management, Discovery
Event	Displays the task event details.

Item	Description
Progress	Displays the progress of the task.
Result	Displays the final result of the task.
Cause	Displays information such as the reason that a task failed.
Error Code	Displays an error code. For details about resolving errors, see page 423 "Error Code List".
Reg. by	Displays the user who registered the task.
Delegation Server	Displays the Delegation Server name.

2. **Select the task log you want to open.**

Use the filtering function if you cannot find in the list the task log you want to open.

1. Click (Filters). The input/select area is displayed.
2. Select a search key.
3. Click (Filter) on the right side of the input/select area, or press the Enter key.

Note

- To open the task list, click (Move to Task) on the option bar.

3. **Check the task log contents on the [Result Details] tab.**

Click a log entry to display the details about the particular device in the "Details" area. Displayed details may differ depending on the task type.

- Discovery: Details are displayed only for newly detected devices.
- Polling: Details are displayed only for devices for which polling has failed.
- Configuration: Details are displayed for all target devices.

The following information is available in the Result Details column: "Start Date", "End Date", "Model Name", "Address", "Serial Number", "Template Name", "Function" (such as "Network Device Discovery", "Device Monitoring", and "Device Preferences"), "Function Details" ("Status", "Polling", "Confirm", and "Apply", etc.), "Result", "Error Code", and "Last Communication Time".

When you click any device in "Result Details" only for configuration tasks, additional information is displayed on the new tab labeled with the device IP address (or host name).

Item Name, Template Value, Value Retrieved from Device, Result, Error Code, and other information in the columns are included in the details displayed for each device. For some templates, the following columns are also displayed:

- The Address Book template task includes the "Entry Type", "Login Name", "Entry Name", and "Mode" columns. The "Mode" column displays information about the operation such as "Add"/"Delete"/"Update" applied to the device.

- The Address Book template and Device Applications template tasks include the "Mode" column, which displays information related to the operations applied to the device. The Applications task displays the "Installation" and "Uninstallation" information, and the Address Book task displays the "Add", "Delete", and "Update" information.
- The SDK/J Platform template and Device Applications template tasks include columns for the template version (the software version defined in the template) and device version (the software version obtained from the device).

Note

- When an SDK/J platform update task is executed and the SDK/J platform of the target device does not support updating by RICOH Software Server, the task log displays an error indicating "Unsupported device".
- For a firmware update task, right-clicking the task log displays the Firmware information] tab and the detailed information about the firmware update can be confirmed.
- For details about filtering logs, see page 421 "Filtering Log Data".
- For details about exporting log data, see page 422 "Exporting Log Data".
- If you restart RICOH Streamline NX or an unexpected shutdown occurs while a task is running or suspended, the task will be in the "Suspended" state after the system restarts. An entry such as "Cancelled because of system suspension." is recorded in the log.
- In cases where a Device Application is installed/uninstalled as part of a task, the result “Does not match” or Match” may incorrectly appear in the Task log.

Re-executing a failed task

If you cannot execute the task normally due to interrupted communication with a device or denied access to a device, execute the task again by clicking (Repeat Failed Task).

Suspending or resuming a task

1. **Click the following items in the navigation tree to open the [Task Log] tab.**

   [System] ▶ [Logs] ▶ [Task Log]

2. **Select the task you want to suspend or resume in the task list.**

   You can only suspend a running task.

   You can only resume a suspended task.

3. **Click (Suspend) or (Resume).**

Canceling a task

1. **Click the following items in the navigation tree to open the [Task Log] tab.**

   [System] ▶ [Logs] ▶ [Task Log]

2. **Select the task you want to cancel in the task list.**

   You can only cancel a task that is currently running or suspended.

3. **Click ■ (Stop).**

Viewing System Operation Logs

You can display the logs that record the system operations in RICOH Streamline NX.

Task Log

The task log records task operations. You can check the results of operations such as the discovery and polling functions for individual tasks.

For details, see page 412 "Viewing the Task Log".

System Log

The system log records system operations. You can check the results of operations such as discovery and polling.

Notification Log

The notification log records notification results such as the notification time, method, and contents.

Audit Log

Use the log to check the operation details, time, and executing user to identify a particular operation started by the RICOH Streamline NX user.

Report Log

The report log records report task schedules and results.

Authentication Log

The authentication log records information such as logged-in time and user for each login.

Viewing the System Log

The system log records details of the internal system operation history. The log entry includes information about the event category, function, details, event type, result, description, and error code. To retrieve the latest log data, click [Update].

Note

- When an error occurs in the @Remote function or another malfunction associated with device information collection occurs, the Ricoh customer engineer may check the system log.

The following functions are recorded in the system log:

- Device Management/Monitoring: Adding/updating/deleting device/counter/user counter in the database*
- Software Management: Downloading the Device Application or SDK/J Platform
- Server Settings: Deleting data/performing activation or deactivation/executing Usage Report

  * These entries are recorded only when the process has failed.

- Successful synchronization with devices

Use the following procedure to display the system log and the items displayed in the log:

1. **Click the following items in the navigation tree to open the [System Log] tab.**

[System] ▶ [Logs] ▶ [System Log]

This displays a list of system logs.

Items displayed in the system log

Item	Description
Date	Displays the date and time when the log was recorded.
Category	The category of the device (Discovery/Polling/Software Management, etc.) is displayed.
Function	Displays the function name (Counter/Device Application/etc.).
Function Details	Displays the details of the function.
Event	Displays the event content (Start/End/Add).
Result	Displays the result (Failed/Does not Match/Succeeded) of the operation executed by the system.
Description	Displays information such as the reason that a task failed.
Error Code	Displays the error code of the failed task. For details about resolving the errors, see page 423 "Error Code List".
Server name	Displays the Delegation Server name.

Note

- The relationship among [Category], [Function], [Function Details] is configured as follows:
  Example:
  - Server Settings (Category)
    - System Data Management (Function)
      - Counter (Function Details)
      - HDD Capacity (Function Details)
      - Report Logs (Function Details)
      - Activation (Function)
        Deactivation (Function Details)
- For details about filtering logs, see page 421 "Filtering Log Data".

- For details about exporting log data, see page 422 "Exporting Log Data".
- For details about the Error Codes, see page 423 "Error Code List".

Viewing the Notifications Log

You can view the details and result of the notification setting. The notification log records the history of notifications regarding Polling, Discovery, Log Management, and the system.

This section describes how to view the log related to notifications and the items displayed in the log.

1. **Click the following items in the navigation tree to open the [Notification Log] tab.**

   [System] ▶ [Logs] ▶ [Notification Log]

   This displays a list of notification logs.

Items displayed in the notification log

Item	Description
Date	Displays the date and time when the notification was delivered.
Notification Settings Type Notification Policy Type	Displays the function (Polling, Configuration, Log Management, etc.) subject to notification.
Notification Name Notification Policy Name	Displays the Definition Name of Notification Conditions. Displays the notification policy that generated the log entry.
Device Display Name	Displays the device that initiated the notification.
Reason for Notification Block	Displays the reason of the failed notification.
Destination	Displays the destination name.

Note

- For details about filtering logs, see page 421 "Filtering Log Data".
- For details about exporting log data, see page 422 "Exporting Log Data".

Viewing the Audit Log

The Audit Log is read-only and contains the records of user operations applied to the system. It provides information for identifying the user who performed operations. This log is useful for tracking changes made by the user operations when multiple administrators are operating on the same system:

Items displayed in the audit log

Item	Description
User Name	Displays the login name of the user who made the change.
Date	Displays the date and time when the change was made.
Action	Displays the operation details (add/delete/edit/update).
Target	Displays the function used to perform the operation. • Groups • Filters • Views • Tasks/Templates • Access Account • Display Settings • Network Settings • Device Log Management • System Data Management • System Alert Notification • Authentication and Accounts • Notification Policy/Destinations
Audit Log Details	Displays information about the implemented measures.

Note

- For details about filtering logs, see page 421 "Filtering Log Data".
- For details about exporting log data, see page 422 "Exporting Log Data".

Viewing the Report Log

The report log records all operations related to the Report Tasks such as the task name, template, schedule, and storage period.

Items displayed in the report log

Item	Description
Start Time	Displays the time when the task started and the report data was collected.
End Time	Displays the time when the task ended and the report data was created.
Task Name	Displays the name of the task.
Schedule Type	Displays the schedule (daily/weekly/monthly/etc.) specified for the task.
Task Status	Displays the status of the task (in progress/failure/success).

Displays the description of the task (if entered by the user who created the task) and the report template name that was used to create the task in the "Task Log Details" area.

Viewing the Authentication Log

The authentication log records all operations related to login, such as the date and time, client type, and user information.

Items displayed in the authentication log

Item	Description
Date	The date/time of the login attempt.
Type	The login method. • User Name/Password • PIN • Card
User Name	The name of the user who performs the login attempt. When [Don't Record User Name in Accounting Transactions] is enabled in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings], the user name is not recorded.
Authentication Profile	The name of the Authentication Profile used for the login.

Item	Description
Client Type	The type of client from which the login occurred. • PC Client • Delegation Server • Embedded Application • Mobile
Client Identifier	An identifier for the client from which the login occurred, such as the serial number for an embedded device or the workstation name of the RICOH Streamline NX PC Client.
Authentication Time	The amount of time in milliseconds spent to perform the authentication.
Status	The result of login attempt, successful or failed.
Error Code	The error code indicating the type of failure.
Cause	A unique identifier generated during the login attempt to uniquely identify a login transaction. This will prevent duplicate-transaction posting.

Filtering Log Data

Use the Quick Filters options to filter the log entries by the values entered in one or more columns. Use this function to search for a specific log entry in the task log, notification log, audit log, or system log.

1. **Open the log to be filtered. In this example, a filter is applied to the Task Log.**
2. **Click (Filters) on the option bar.**

   The filter field is displayed above the log line.
3. **Enter the filtering condition in the text entry field, or select a condition from the menu in the fields (event, category, etc.) with configured conditions.**

   Press the [Enter] key to update the result after making an entry or selection. In the example, the list is filtered to display only the configuration notification entries.

   Enter a filter condition in an additional column to further narrow down the list entries. For example, if there are a large number of entries to be sorted, you can also filter the list based on the "Result" column.

Exporting Log Data

You can export a log to a CSV file. Logs are exported according to the currently specified view. Therefore, if a filter is applied to the log entries, only the filtered data and not the entire data in the log will be exported. The log includes the data, date created, log type (task, notification, audit, or system), and the line that corresponds to the log type.

1. **Open the log to be exported. In this example, export the task log.**
2. **Click (Export data as a CSV file) on the option bar.**
3. **Specify the location to save the file, or select an external application to open the file.**

Error Code List

The causes of errors and their solutions are described below:

Range Description

0-49 Notification Message.

50-99 Warning Message.

1xx: Error. Invalid parameters set on the device side.

2xx: Error. An error occurred on the device side.

3xx: Error. Failure to connect to an external system.

4xx: Error. Invalid parameters in internal system.

5xx: Error. Data I/O Error.

6xx: Error. System Error, particularly succeeded or warning.

7xx: Error. Error with unexpected or insufficient information.

8xx: Error. Error related to @Remote. Please contact your service representative.

Code	Cause	Solution
003	Matches with the template value.	The process has completed normally.
004	Unsupported device.	A function not supported by the target device is specified. Check the target device. When installing Streamline NX Embedded Applications, the target device must be equipped with a HDD.
005	Unsupported item.	A setting item not supported by the target device is specified. Check the target device. Check the item.
006	Unsupported value.	A configuration values not supported by the target device is specified. Check the target device. Check the parameter.
007	A Trap from an unmanaged device has been received.	The machine is operating normally.
008	A new device has been added because a Trap from an unmanaged device has been received.	The machine is operating normally.

Code	Cause	Solution
009	Suspended because of a prohibited time range.	The machine is operating normally.
010	Resumed because the prohibited time range has passed.	The machine is operating normally.
011	The status of the device log collection function is now normal.	The machine is operating normally.
012	The status of the available device log data capacity is now normal.	The machine is operating normally.
013	Secure items can only be set, not retrieved.	The machine is operating normally. This is a set-only item.
014	No item found for the check target	An item for Check does not exist. Change the setting as needed.
015	Settings have been made on HTTP because the device does not support SSL.	The configuration has completed normally in HTTP communication. When you want to communicate via HTTPS, Change the configuration.
016	The status of the HDD capacity has returned to normal.	The machine is operating normally.
017	The status of the DB capacity has returned to normal.	The machine is operating normally.
018	The SDK/J platform has not been installed.	The machine is operating normally. Please contact your RICOH service representative.
019	The target application is not installed.	The machine is operating normally.
020	The target application is not activated.	The machine is operating normally.
021	The SDK/J platform on the device is an earlier version.	The machine is operating normally.
022	The SDK application on the device is an earlier version.	The machine is operating normally.
023	An application is installed on the device.	The machine is operating normally.
024	The SDK/J platform on the device is a later version.	The machine is operating normally.

Code	Cause	Solution
025	The SDK application on the device is a later version.	The machine is operating normally.
026	Latest SDK/J Platform has been installed.	The machine is operating normally.
027	The latest application is already installed.	The machine is operating normally.
028	Already activated.	The machine is operating normally.
029	Already deactivated.	The machine is operating normally.
030	Skipped because of check action	The machine is operating normally.
031	The version of SDK application on the device is same	The machine is operating normally.
032	Unconnected device has been added because a Trap from an unmanaged device has been received but the connection was failure.	The machine is operating normally.
033	XX device logs have been collected.	The machine is operating normally.
034	Update Succeeded	The machine is operating normally.
035	Succeeded	The machine is operating normally.
050	Managed by MK-1 etc.	Because this device is controlled by other management tools, RICOH Streamline NX cannot manage it.
051	A character(s) other than a numerical value is included in the version.	Check the configuration values.
052	The status of the device log collection function is now on alert.	Confirm that the free area in the storage is allocated to device log data.
053	The status of the device log data capacity is now nearly full (alert).	Confirm that the free area in the storage is allocated to device log data.
054	Device log transfer has not been performed for a certain period of time for a particular device.	Confirm the configuration of the device transfer function.

Code	Cause	Solution
055	The DeviceEcologyLog that cannot be transferred within the device has been lost.: logs	The number of logs in a device has exceeded its limit value. Restart the log collection of RICOH Streamline NX.
056	Unknown data has been retrieved.	Check the status of the retrieved data or device.
057	An unknown device has been retrieved.	Check the status of the retrieved device.
058	Waiting to reboot	The device is restarting, so wait for it to be completed.
059	The entry does not exist.	The Address Book entry for the device and the template are not the same. The entry does not exist in <DEVICE> when processing a check task.
060	The entry does not exist.	The Address Book entry for the device and the template are not the same. The entry does not exist in <TEMPLATE> when processing a check task.
061	It is necessary to install the Type-C extended feature after this installation. Perform installation from Web Image Monitor. Restart the device after installation has completed.	Perform installation from Web Image Monitor. Restart the device after installation has completed.
062	It is necessary to uninstall the Type-C extended feature after this uninstallation. Perform uninstallation from Web Image Monitor. Restart the device after uninstallation has completed.	Perform uninstallation from Web Image Monitor. Restart the device after uninstallation has completed.
063	To install this application perform [SDK/J Platform Update].	Update SDK/J Platform.
064	The HDD capacity is nearly full.	Secure HDD capacity.
065	The HDD capacity is full.	Secure HDD capacity.
066	The DB capacity is nearly full.	Secure HDD capacity.
067	The DB capacity is full.	Secure HDD capacity.

Code	Cause	Solution
068	Canceled the processing because of another task execution.	Try again after waiting a short interval. Stop other tasks.
069	The operation has been cancelled.	Review the configuration of permission.
070	Basil IP address was set.	An IP address of RICOH Streamline NX was set in the target device. Verify the configuration information on the target device.
071	Encryption strength was set.	A cipher strength was set in the target device. Verify the configuration information on the target device.
072	ID2 did not match.	The ID2 of the target device does not match the data saved in RICOH Streamline NX. Confirm the configuration information of the target device.
073	Connection type did not match.	The Connection type of the target device does not match the data saved in RICOH Streamline NX. Confirm the configuration information of the target device.
074	Core ID did not match.	The Core ID of the target device does not match the data saved in RICOH Streamline NX. Confirm the configuration information of the target device.
075	Serial Number did not match.	The Serial Number of the target device does not match the data saved in RICOH Streamline NX. Confirm the configuration information of the target device.
076	MAC address did not match.	The MAC Address of the target device does not match the data saved in RICOH Streamline NX. Confirm the configuration information of the target device.

Code	Cause	Solution
077	The device log settings are not enabled.	Enable the device log retrieval setting.
078	Changed : IP Address	The IP address of the target device is changed. Confirm the configuration information of the target device.
099	Other warning.	A generic code.
100	Device authentication has failed.	Confirm the administrator rights of the device. Check whether the following settings of the device access account are correct: • User name and/or password of your Web service account • Community name if SNMPv1/v2 protocol is used • User name and password if SNMPv3 protocol is used See page 76 "Configuring an Access Account".
101	Parameters for other devices are invalid.	Settings not supported by the target device are specified, or settings are incorrect. Check the settings. If the parameters indicate a backup file, check the specified password matches that of the backup file.
102	The device password policy has been violated.	Set a password that complies with the device password policy.
106	The support range (value) has been exceeded.	Set a value within the support range (value).

Code	Cause	Solution
107	You do not have the privileges to perform this operation.	Check whether the following settings of the device access account are correct: • User name and password of your Web service account • Community name if SNMPv1/v2 protocol is used • User name and password if SNMP v3 protocol is used See page 76 "Configuring an Access Account".
108	The setting target is different.	The target device does not support the set function and the setting is recognized as an error on the device side. Check the target device.
109	The authentication method for the device and the template is not the same.	Check the authentication methods for the device and the template.
111	Authentication failed because the authentication information was invalid or the device was in use.	Check the privileges of the device administrator. A task may fail when the device is in use. While a task is in progress, refrain from using the device.
150	Parameters for other devices are invalid.	• Check the configuration values. • The target device does not support the set function. Check the target device. • A task that is not supported by the target device, was executed. Check the device. • Check that the number of entries including the number that is currently registered to the device does not exceed the maximum number of entries that can be registered.
200	No response from the device.	• Check the network environment. • Check the device status.

Code	Cause	Solution
201	Network is disconnected.	• Check whether the network has any problems. • Contact the administrator.
202	Communication timeout has occurred.	Check the network environment.
203	SSL communication is unavailable.	Check whether the certificate is configured correctly.
204	Unable to connect to the Certificate Authority.	• Check the network environment. • Contact the administrator.
205	Device is in use.	The task was not executed because the target device is being used. Do not use the device while a task is being executed.
206	Device is in energy saver mode.	Disable energy saver mode on the target device.
208	System error has occurred on the device.	Retry the process after the device restarts.
210	The number of sessions on the device has reached the limit.	• Retry the process later. • Do not use the device while a task in progress.
211	System busy has occurred on the device.	• Retry the process later. • Do not use the device while a task in progress.
212	SC has occurred.	The target device has a problem. Resolve the device problem.
213	Failed to suspend the SDK application on the device.	Restart the device and perform the operation again.

Code	Cause	Solution
214	Failed to restart the device.	Check whether the following settings of the device access account are correct. • User name and password of your Web service account • Community name if SNMP v1/v2 protocol is used • User name and password if SNMP v3 protocol is used See page 76 "Configuring an Access Account".
215	The SDK/J platform file is invalid.	• Check the file version of SDK/J platform. • Check the SDK/J platform files.
216	Unable to communicate with the SDK/J platform.	• Check whether the SDK/J platform is installed. • Check whether the SDK/J platform is working.
217	Failed to update the SDK/J platform.	• Restart the device and perform the operation again. • Ensure the password of SDK/J platform is set normally.
218	The SDK/J platform file is invalid.	Perform the operation again.
219	The SDK application is not installed on the device.	• Confirm that SDK/J platform is installed. • When you install the Device Application, apply a dedicated template. • Confirm that the Device Application for the device is installed.

Code	Cause	Solution
220	Failed to install the SDK application.	• Restart the device and perform the operation again. • Ensure the password for the SDK/J Platform is set correctly. • Ensure the password for the Device Application is set correctly.
221	Failed to update the SDK application.	• Restart the device and perform the operation again. • Confirm that the password for the SDK/J Platform is set correctly. • Confirm that the password for the Device Application is set correctly.
222	Failed to uninstall the SDK application.	• Restart the device and perform the operation again. • Ensure the password for the SDK/J Platform is set correctly.
227	The firmware on the device is an earlier version.	When you update Firmware, apply a dedicated template.
228	The firmware on the device is a later version.	When you update firmware, apply latest Firmware.
229	RFU is prohibited by the device setting.	Permit working of RFU by changing the configuration of the device.
230	The firmware has been rejected.	Confirm whether right firmware is assigned.
231	The firmware data is defective.	Confirm whether the correct firmware is assigned.
232	The optional firmware has been skipped.	• It is not an error. • Confirm whether you selected the correct firmware file to set.
233	A process has been performed in rescue mode.	• Try again after taking a pause. • Try again after rebooting the device.
234	The number of user data preferences has exceeded the limit.	Delete entries from the entry list of the user data preference.

Code	Cause	Solution
235	The number of users has exceeded the limit.	Delete users from the entry list.
236	The number of groups has exceeded the limit.	Delete groups from the entry list.
237	The user data preference entry is duplicated.	Eliminate duplicate entries in the entry list.
238	The group does not exist.	Check the entries of the entry list.
239	The entry does not exist.	Check the entries of the entry list.
240	The user code/login name is prohibited.	Enter the correct user code/login name.
241	The user code/login name is duplicated.	Enter a user code/login name that is not already registered.
242	Failed to retrieve the counter per user.	Check the user data (address book) on the target device.
243	Failed to reset the counter per user.	Check the user data (address book) on the target device.
244	Failed to batch delete entries.	• Check whether the target device access account is correct. • The address book on the target device may be locked for editing by another user. Check the device status.
245	Failed to batch delete users.	• Check whether the target device access account is correct. • The address book on the target device may be locked for editing by another user. Check the device status.
246	Failed to batch delete groups.	• Check whether the target device access account is correct. • The address book on the target device may locked for editing by another user. Check the device status.

Code	Cause	Solution
247	Failed to batch delete destinations.	• Check whether the target device access account is correct. • The address book on the target device may be being edited. Check the device status.
248	Device access control settings have failed.	• Check whether the target device access account is correct. • The address book on the target device may be locked for editing by another user. Check the device status.
249	Failed to batch delete logs.	• Restart the device and try again. • Delete the device log from a device browser collectively.
250	Failed to check.	A problem such as the device being turned off may have occurred while configuring the settings. Check the device status.
251	Failed to change the heap size.	• Try again after the device boots. • Specify the available heap size in the device. • Change the heap size by the Device Browser.
252	Failed to change the stack size	• Try again after the device boots. • Specify the available stack size in the device. • Change the stack size by the Device Browser.
253	SDK/J platform is suspended	Retry the process after the device restarts.
254	The Address Book is not supported.	Use the device which supports the Address Book.

Code	Cause	Solution
256	Failed to retrieve the user information.	• Check if the user information exists in the address book. • Determine if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Check if the device supports the Address Book.
257	Failed to set the user information.	• Check if the configuration item exists in the address book. • Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Check if the device supports the Address Book.
258	Failed to create the entry.	• Check if the entry is duplicated in the address book. • Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Check if the device supports the Address Book.
259	Failed to retrieve the entry information.	• Check if the entry exists in the address book. • Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Determine if the device supports the Address Book.
260	Failed to change the entry information.	• Restart the device and perform the operation again. • Ensure the device can communicate. • Ensure the address book is written with the supported format.

Code	Cause	Solution
261	Failed to delete the entry.	• Restart the device and perform the operation again. • Ensure the device can communicate. • Ensure the address book is written with the supported format.
262	Failed to delete the user.	• Restart the device and perform the operation again. • Ensure the device can communicate. • Ensure the address book is written with the supported format.
263	Failed to delete the group.	• Restart the device and perform the operation again. • Ensure the device can communicate. • Ensure the address book is written with the supported format.
264	Failed to delete the destination.	• Check if the destination exists in the address book. • Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Check if the device supports the address book.
265	Failed to backup the Address Book.	• Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots. • Check if the device supports the address book.
266	Failed to restore the Address Book.	Restart the device and perform the operation again.
267	Failed to deactivate.	Retry the uninstallation after the device restarts.
268	Failed to activate the SDK application.	Retry the activation after the device restarts.

Code	Cause	Solution
269	Change encryption length	Wait for a brief interval and then try again after the device reboots.
270	Failed to collect the debug logs.	• Check if RICOH Streamline NX can communicate with the device. • Try again after the device boots.
271	Device setting items are not set for Streamline NX.	Configure the Device Application settings of the target device.
272	Failed to start the application.	Restart the device and perform the operation again.
273	The application is not started.	Restart the device and perform the operation again.
274	Failed to set the initial start-up settings of the application.	Restart the device and perform the operation again.
275	Configuration failed.	Restart the device and perform the operation again.
277	Insufficient disk space on the device.	• Delete SDK applications that are not necessary from the device, and allocate sufficient free space. • If allocating sufficient free space is not possible, contact a Ricoh service representative.
280	Other device error occurred.	• Check the target device settings. • Check the target device. • Check that the specified password does not violate the password policy of the device. • In the address book settings, check that the user whose account is to be deleted or the authentication information is updated is not being logged in on the control panel of the machine. • If none of these conditions applies, restart the device and perform the operation again.

Code	Cause	Solution
300	An authentication error for the external system has occurred.	Check the authentication information with the external system.
301	Unable to access the external system.	Access the system again after a brief interval.
302	Failed to send email. Verify email server settings and retry.	• Check the network. • Check the SMTP configuration of the mail server.
303	SMTP server authentication has failed.	• Check the network. • Check the configuration of the mail server.
304	Proxy authentication has failed.	If user authentication of the proxy server is enabled, check that it has been correctly configured.
305	Proxy connection has failed.	• Check the network environment. • Check that the proxy server has been correctly set in [Server Settings] under [System].
306	Failed to connect with the RICOH Software Server.	• Error is occurred when using Firmware Download functions. • Check the Proxy Server configurations. • Check the Firewall configurations.
307	Unable to communicate with the RICOH Software Server.	• Check whether RICOH Software Server communication can be established. • Error occurred when connecting to the RICOH Software Server. • Confirm communication can be established.
308	Communication with the RICOH Software Server has been interrupted.	Check whether RICOH Software Server communication can be established.
309	Failed to connect with the RICOH Backend Server.	Check that the server and network environment settings are correct.

Code	Cause	Solution
310	Failed to transmit data.	• Check that the server and network environment settings are correct. • Check that the proxy server has been correctly set in [Server Settings] under [System]. • Check if the Delegation Server can communicate with the device. • Check the server component.
311	Failed to receive data.	• Check that the server and network environment settings are correct. • Check that the proxy server has been correctly set in [Server Settings] under [System].
330	Unable to access Core server.	• Check the proxy server configuration. • Check the firewall configuration.
331	Connection with the Core Server has timed out.	Check if "RICOH SLNX Central Manager Service" in the Windows Services is running.
350	Other external system connection error.	• Restart the services. • Check the network settings of the system. • Check the access account profile.
400	Entered parameters are invalid.	Set the correct parameters.
401	The file format is invalid.	Check whether there is a problem with the file format.
402	The file version is invalid.	• Check whether there is a problem with the file version. • Check the file format.
403	The character code of the file is invalid.	Set a correct character code.
404	Interrupted by user operation.	The system operation is not completed. Perform the operation again.
421	Other system error.	Activation was finished normally.

Code	Cause	Solution
422	Other system error.	Deactivation was finished normally.
423	Entered parameters are invalid.	Confirm the sequence of activation.
424	Entered parameters are invalid.	Ensure the sequence of deactivation.
450	Other system entry error.	Check that the specified setting values and parameters are correct.
500	Database authentication has failed.	Confirm authentic method information of the Database.
501	Failed to access the database.	Reboot the server, then retry it. If the problem persists, contact Ricoh Service.
502	Failed to save data on the database.	• Determine if the Database is working normally. • Ensure the Database has sufficient free space. • Ensure that no other system or tool is connected to the database.
503	Failed to read the data.	• Check whether there is a problem with the data to be loaded. • Determine if there is a problem with the data to be loaded. • Ensure the Database is working normally. • Ensure that no other system or tool is connected to the database.
504	Failed to save the data.	• Check whether there is a problem with the data to be saved. • Determine if there is a problem with the data to be saved. • Ensure the Database is working normally. • Ensure that no other system or tool is connected to the database.

Code	Cause	Solution
505	The status of the device log data capacity is now log full (defective).	Verify that there is sufficient free space for Device Log data.
506	Failed to set the assigned volume for storing the device log information.	• Verify the Database startup status. • Reboot the Database
507	Failed to change the alert volume for device log information.	Verify the size of the Database storage area.
508	Failed to change the defective volume for the device log information.	Verify the size of the Database storage area.
509	Failed to receive device logs because of DB access problem.	• Verify the Database startup status. • Reboot the Database
514	Failed to save data on the database.	Verify that the database is functioning normally. Ensure there is no another system or tool which refers to the database.
550	Other data input/output error.	The hard disk may have insufficient free space.
600	Insufficient disk space.	The hard disk has insufficient free space. Delete unnecessary data.
601	Cancelled because of system suspension.	RICOH Streamline NX has exited or a computer shutdown occurred. Restart the computer and RICOH Streamline NX.
602	The system has insufficient memory.	• The hard disk has insufficient free space. Delete unnecessary data. • Restart the computer and RICOH Streamline NX.
603	The number of sessions has reached the limit.	• Confirm the RICOH Streamline NX access status. • Increase the number of allowable sessions on the server side.
604	The product key is invalid.	Enter a correct product key.

Code	Cause	Solution
605	The template has been saved. Check there are enough licenses to execute the task.	• Purchase additional license(s). • Deactivate software installed on other devices.
606	Failed to read the data.	• Install on another device. • Check the status of the retrieved device.
607	The application has not been released yet.	• Apply the installable application. • Ensure the application is installable.
608	Failed to retrieve the application file.	• An error has occurred in the system function. • Contact your service representative.
609	Failed to change the heap size.	The device has insufficient memory. Extend the device memory capacity or change the heap size settings.
611	Failed to lock the device.	• Do not use the device when settings are configured. • The device is currently in use. RICOH Streamline NX cannot configure the device setting while the device is in use.
612	Failed to restart the device.	• Do not use the device when settings are configured. • Check whether the access account is configured correctly.
618	There is no software available for update.	Check the application of the target device.
619	The Address Book backup file is invalid.	Check whether the file is correct.
620	The Device Preference backup file is invalid.	Check whether the file is correct.
621	The encryption key is invalid.	Check whether the encryption key is correct.
622	The item is unavailable for retrieval.	The specified item cannot be retrieved. Secure information such as passwords cannot be obtained.

Code	Cause	Solution
623	The status of the device log collection function is now defective.	Verify that there is sufficient free space for Device Log data.
624	Failed to change the device log collection function settings.	Verify the Database startup status.
625	Failed to set the device log information storage period.	Set the possible storage period.
626	Failed to change the device log update period.	Check the device log update period.
627	Failed to update the device logs.	• Check the free space of Database. • Check the free space of HDD.
628	Failed to batch delete the device eco logs.	• Reboot the device/devices and then try again. • Confirm the device/devices status.
629	Failed to receive device logs.	• Reboot the Delegation Server. • Reboot the device/devices. • If you have permission to delete the device log data, try to delete log data.
630	Reception has failed because incorrect data has been detected in the device logs.	• Reboot the device/devices. • If you have permission to delete the device log data, try to delete them.
631	Failed to initialize the task because the task information is incorrect.	• Check that the task setting is properly configured. • Check the policy.
632	Failed to initialize the task because the target device does not exist.	Check the target device.

Code	Cause	Solution
634	Failure has occurred on the previous setting item.	• Check the target device. • Check that the task setting is properly configured. • Confirm the device/devices status. • Check that the task settings and template settings are properly configured. • Try again.
635	The version contains nonnumeric characters	• Check the version file. • Use another file.
636	Value mismatch	Check is finished successfully and the value is not matched.
638	Unable to perform uninstallation because a SDK application that has been activated by the RICOH Software Server exists on the device.	Uninstall all applications that work in concordance with RICOH Software Server from the device first, and then proceed to uninstall the intended application.
639	An error has occurred. Refer to the error code list in the operation guide for details.	Within the Task Log, the error codes are listed by device. For details, see page 451 "Server-related Errors".
640	There is more than 1 newly discovered device.	The machine is operating normally.
641	There are no newly discovered devices.	• The machine is operating normally. • Check the policy.
642	There are no failed devices.	The machine is operating normally.
643	There are no configured devices.	The machine is operating normally. Set the target device/devices or group/groups properly if you needed.

Code	Cause	Solution
644	Communication timeout has occurred.	• Reboot the device/devices then try again. • Move the device/devices to other Delegation Server then try again. • Reboot the Delegation Server.
645	Cannot perform the operation because the data is used by some tasks.	Change the template settings from the tasks that uses the template.
646	Failed to delete the data. Assigned Account	Change the device settings as not using the account.
650	Other system error	Check that the system setting of RICOH Streamline NX is properly configured.
651	Delegation Server call has failed.	• Make sure the Delegation Server operates normally. • Reboot the Delegation Server.
655	Failed to read the data.	• Confirm Delegation Server status. • Confirm the network connection that can communicate between Core server and Delegation Server.
656	Failed to save data (The entry does not exist.:Template)	Create a new template.
657	Failed to read the data.	• Ensure the target device operates normally. • Make sure Delegation Server operate normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.

Code	Cause	Solution
660	Failed to read the data.	Check that the following settings of the device access account are properly configured: • User name and login password of Web Service Account • Community name if SNMP v1/v2 protocol is used • User name and login password if SNMP v3 protocol is used
661	Failed to read the data.: Logo Image	• Confirm that the target device operates normally. • Confirm that Delegation Server operate normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.
662	Failed to read the data.: Settings File	• Confirm that the target device operates normally. • Confirm that the Delegation Server operates normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.
663	Other system error.	• Confirm that the target device operates normally. • Confirm that Delegation Server operate normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.

Code	Cause	Solution
665	An unexpected error has occurred.	• Confirm that the target device operates normally. • Confirm that the Delegation Server operates normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.
666	Failed to confirm the SDK/J Platform existence.	• Confirm that the target device operates normally. • Confirm that the Delegation Server operates normally. • Retry the import after restarting the device. • Retry the import after restarting the Delegation Server.
670	There are some non-executed tasks that cannot be performed because the system has been suspended.	The machine is operating normally.
700	Failed to save data	• Ensure the database which the system requires operates normally. • Check capacity of the database which the system requires. • Ensure there is no other system or tool which refers to the database.
701	Failed to save data	• Ensure the database which the system requires operates normally. • Check capacity of the database which the system requires. • Ensure there is no other system or tool which refers to the database.

Code	Cause	Solution
702	An unexpected error has occurred.	• Ensure the database which the system requires operates normally. • Check capacity of the database which the system requires. • Ensure there is no other system or tool which refers to the database.
703	An unexpected error has occurred.	• Ensure the database which the system requires operates normally. • Check capacity of the database which the system requires. • Ensure there is no other system or tool which refers to the database.
704	An unexpected error has occurred.	• Ensure the database which the system requires operates normally. • Check capacity of the database which the system requires. • Ensure there is no other system or tool which refers to the database.
707	Running Tasks:Perform the process again later.	Try again after other task finished.
708	The Delegation Server cannot be reached. The task will execute when the service becomes available.	• RICOH Streamline NX was in the process of starting up, and the task could not be performed. The task will be automatically performed after the software starts up. • Check the Delegation Server status. • Check the network connection that can communicate between Core server and Delegation Server.
709	Map image exceeds maximum file size of 6MB.	Reduce the size of the map image file.

Code	Cause	Solution
710	The Delegation Server cannot be moved because it is still running. Stop the Delegation Server service before attempting to move it to another computer.	Try again after a brief interval.
801	Outside of regular office hours.	Try again during regular office hours.
802	Failed to obtain device information.	• Try again after a brief interval. • Check the network settings of the system. • Check the access account profile.
803	Failed to send message.	• Restart the services. • Check the network settings of the system. • Check a proxy server, router, and firewall settings.
804	A hardware related error has occurred.	Restart the services.
805	A database related error has occurred.	Restart the services.
806	An error on the Center server side that does not have an error code has occurred.	Contact your service representative.
807	An error on the appliance side that does not have an error code has occurred.	Contact your service representative.
808	Bad file.	Contact your service representative.
809	Cannot find the appliance in @Remote Center System.	Contact your service representative.
810	The managed device does not exist in @Remote Center System.	Contact your service representative.
811	There is no such data found in the database.	Contact your service representative.
813	In operation.	Try again after a brief interval.
814	The device has already been registered.	Contact your service representative.
815	Cannot register device.	Check the request number is correct.

Code	Cause	Solution
816	This is a device that is already registered.	Contact your service representative.
818	Parameter error.	Check the entered information is correct.
819	A property list item that does not exist has been specified.	Contact your service representative.
820	In the property list settings, an out of range or oversized value has been specified.	Restart the services.
821	A property list item that cannot be set has been specified.	Restart the services.
823	The size of the restore file is larger than the size of the free space in the system.	Check if the Delegation Server can communicate with the device.
824	The result has expired.	Contact your service representative.
826	The targeted schedule for cancelling does not exist.	Contact your service representative.
827	User cancellation.	-
828	Cannot access targeted device.	Check the network settings.
829	FTP login authentication failure	Check the device settings that the remote firmware update is allowed.
830	FTP disconnected.	• Check if the Delegation Server can communicate with the device. • Check the device is turned on.
831	A reply did not come back from the printing devices within a specified period of time.	Check if the Delegation Server can communicate with the device.
834	The operation has been canceled.	Contact your service representative.
835	There was an operation timeout.	Contact your service representative.
836	Timeout.	Contact your service representative.
841	The connector id is not correct.	Contact your service representative.

Code	Cause	Solution
842	The device id in this notification and in the installation plan information differs.	A request number different from the request number specified by the @Remote center is used. Contact your service representative.
843	The format of the connector id invalid.	Contact your service representative.
844	Received request number incorrect.	Check the request number is correct.
845	A device is already registered with the same IP address.	Contact your service representative.
847	An internal error has occurred with the restore operations.	Restart the services.
848	Communication test failed.	Restart the services.
849	Exchange is not supported by the service site.	Follow the appropriate steps.
851	Rescue error.	Contact your service representative.
852	Corresponding data does not exist.	Contact your service representative.
899	There was an unclassified error.	Contact your service representative.
951	Network connection error.	Check a proxy server, router, and firewall settings.
954	A function prohibited by the target device is specified.	Check the @Remote task permit setting.
955	XML parser error.	Contact your service representative.
1001	System error.	Restart the services.
9801	HTTP connection error.	Contact your service representative.

Server-related Errors

If a software installation or update performed in conjunction with the RICOH Software Server fails, an error code is displayed on the screen. The error codes and solutions are described below.

Code	Causes and solutions
M32	This error occurs during installation. To install the specified software, you must first update the software. Perform the installation again after updating all relevant software.
M42	This error occurs during installation. The software you are trying to install is already installed. Check the software installed on the device.
E01	Refer to our service person.
E03	Refer to our service person.
E04	Refer to our service person.
E05	This error occurs during product key entry. The entered product key is not found on the RICOH Software Server. Check the product key and enter it again.
E06	This error occurs during product key entry. The license related to this product key has been canceled. Check the product key and enter it again.
E07	This error occurs during product key entry. The software corresponding to the entered product key was not found. Check the product key and enter it again.
E09	This error occurs during installation. Installation of the specified software onto the device is not permitted due to an insufficient number of licenses. Purchase the required number of licenses.
E10	This error occurs during installation. Because the RICOH Software Server has a record that the target device used another product key in the past, the entered product key cannot be used. Enter the product key that was used last time.
E12	Refer to our service person.

Code	Causes and solutions
E13	This error occurs during installation. The device number is incorrect. Check the device number, and perform the operation again. If the problem cannot be solved, contact your service representative.
E18	This error occurs during installation. A trial-use license cannot be used. Purchase the required license.
E20	Refer to our service person.
E21	This error occurs during installation. The license re-issue count exceeded the upper limit. If the problem cannot be solved, contact your service representative.
E22	This error occurs during product key entry. The requested parameter is invalid. Check the product key and enter it again.
E25	Refer to our service person.
E45	Refer to our service person.
E46	Update the Firmware. Refer to our service person.
E47	This error occurs during installation. The software you are trying to install or update is not compatible with the software already installed on the device. Check the version of the software installed on the device. If the problem cannot be solved, contact your service representative.
E49	Refer to our service person.
E51	Refer to our service person.
E52	Refer to our service person.

Code	Causes and solutions
E53	This error occurs during software installation/update. The version of the system installed on the device may be earlier than the required version. If the problem cannot be solved, contact your service representative.
E54	This error occurs during installation or update. The operation is not guaranteed with the selected device. Check the selected device or the product key.
E61	• Update the firmware. • Confirm the installed version of the application on the device. • Confirm that JavaVM is installed on the device. • Refer to our service person.
E90	Refer to our service person.
E95	Refer to our service person.
Exx xx: number	Error code "Exx" is added to another error on the server side. For a detailed solution, contact your service representative.
ER01	This error occurs when publishing the installation license. An error occurred after the license has been published. The published license must be returned. For details about the solution to resolve the problem, consult your service representative.

Troubleshooting

Problem	Causes and solutions
A device on the network is not detected.	• Even when settings have been made to search for a device on another network, the target device may not be detected due to the network router settings. • Check the discovery range. For details, see page 77 "Searching for Devices".
Devices from a manufacturer other than RICOH are displayed on the device list, but some device information cannot be retrieved.	Discovery detects devices that support PrinterMIB. Devices from other manufacturers are also monitored, but the same information cannot be retrieved from such devices.
Device detection was disabled after setting up SNMPv3 as the SNMP access account monitoring protocol.	Set up SNMPv3 on the device side. If it is a RICOH device, setup can be performed from Web Image Monitor. For details, see the instruction manual that comes with the device.
Batch settings using a template cannot be performed.	• Check that the access account has been correctly set. • Correctly set the access account, and overwrite the access account of the target device. For details, see page 76 "Configuring an Access Account".
The number of remaining licenses does not increase even if applications are deactivated/ uninstalled.	Deactivation between the target device and the RICOH Software Server was not correctly processed. The message "Failed to deactivate because an internal error has occurred on the RICOH Software Server." is recorded in the task log. Check the device number of the target device and the product ID of the target application in this log, and contact a service representative.

Problem	Causes and solutions
An access account cannot be deleted.	An access account cannot be deleted if it's in any of the following conditions: • The account is assigned to a profile in [Administrator] or [SNMP] category in a [Basic Device Preferences] template. • The account is assigned to the access account of discovery task. • The account is assigned to the access account in any of the device that is displayed in the device list. In order to delete an access account, it must be released from those assignments.
The device screen displays a message indicating that Profile configuration information cannot be found.	No profile has been delivered to the device via the device settings, or no group has been created for the selected profile.
No group or workflow is displayed on the device screen.	All groups for the profile are set to hidden.
Cannot perform Inbound FAX Transfer.	Make sure that the device's reception setting function for facsimile is set to "Store". For details, refer to the device model's Operating Instructions.

10. List of Setting Items

This chapter describes the setting items displayed on the Management Console. This chapter also follows the items on the navigation tree of the Management Console.

Note

- When viewing this chapter as a PDF, you can use the index function of the PDF browsing application to display a list in the same format as the navigation tree of the Management Console.

Device List

This section describes the categories, groups, and power filters displayed in [Device List] in the navigation tree.

Groups

Groups include system categories, system groups, custom categories, and custom groups. For functional outlines and details about using the functions, see page 71 "Organizing the Device List".

Navigation Tree Right-click Menu

Item	Description
Refresh	Updates the categories/groups that are displayed.
Add Category	Adds a category in the root hierarchy.
Add Group	Adds a new group to a lower hierarchy of the selected category.
Rename	The following operations can be performed: • Rename / Edit Category Name • Adding a new device to a group • Rename / Edit Filter Criteria
Delete	Deletes the selected category or group. All devices that are registered in the deleted group will be transferred to the unmanaged group.
Display Hidden Devices	Displays the devices that are set to be hidden.
Import	Imports the information of the groups/categories. Specify the path of the CSV file to be imported. To import all groups in the file, select the [Import All Groups] check box.

Item	Description
Export	Exports the structure and name of the selected group and category. To export all groups, select the [Export All Groups] check box.
Add Map	Adds a device map to and associates it with the selected group.
Delete Map	Deletes the associated device map for the selected group.
Add Package	Adds a driver package to and associates it with the selected group.
Delete Package	Deletes the associated driver package for the selected group.

Power

From the drop-down menu displayed at the bottom of the navigation tree, filter the devices to be displayed in the [Devices] tab.

For outlines of the power filters and details about using power filters, see page 87 "Using Power Filter".

Drop-down Menu

Item	Description
Create Filter	Displays the [Create Filter] dialog box for creating a new filter. You can add a new filter in the dialog box. • [Filter Name] (The box located to the left of the (Save Filter) button): Enter the filter name. • (Save Filter) button: Saves the filter that has been created. • [Filter Blocks]: Select the filtering condition of the devices. You can select more than one condition for filtering devices. • [Models] • [IP Address] • [Device Status] • [System Status] • [Printer Status] • [Copier Status] • [Fax Status] • [Scanner Status] • [Delegation Server] • [Custom Criteria] The setting values of each condition are displayed when a filtering condition is selected. The number in parentheses () next to the name of the setting value name represents the actual number of corresponding devices.
Modify Filter	Changes the filtering conditions for the selected filtering group.
Delete Filter	Deletes the selected filtering group.

Note

- You can select and access the created filter from the [Select Filter] drop-down menu that is located to the right of .

Devices

The [Devices] tab consists of the device list and [Device Properties]. For details about the contents displayed on the tabs, see page 57 "Device Properties".

Discovery & Polling

This section describes the functions of items displayed in [Discovery & Polling] in the navigation tree.

Discovery

There are two ways to discover devices: [Broadcast] and [Network Search].

Broadcast

Click [Broadcast] in the navigation tree to display the discovery profile. When a profile name is selected from the list, you can configure the detailed information with the [General], [Access Accounts], [Discovery Range (Broadcast)], [Schedule], and [Auto Settings] tabs.

Note

- For an outline of broadcast and details about using broadcast, see page 77 "Searching for Devices".

[General] tab

Specify the task name.

Item	Description
Name	Enter the name of profile.
Description	Enter the description of profile.
DS Server	Select the Delegation Server to perform discovery.
Perform Reverse DNS Lookup	Specify whether or not to perform reverse DNS lookup in discovery. When this setting is enabled, reverse DNS lookup is performed to search for the name of the host that corresponds to the IP address.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Access Accounts] tab

Configure the account to be used to access the device when performing device discovery.
Move the account to be used from the [Not Assigned Accounts] list to the [Assigned Account] list by clicking the button or dragging and dropping.

There are three types of [Access Accounts] as shown in the following table. Each account type is displayed by a tab.

Tab name	Description
Device Administrator Access	Displays the access account that is used in Web service protocol.
SNMP Access	Displays the access account that is used for SNMP.
SDK/J Platform Access	Displays the access account that is used for remote connection to SDK Platform.

[Discovery Range (Broadcast)] tab

Specify the target range of discovery by broadcast.

Item	Description
Type	Specify the target range of broadcast. • [Local Segment] • [Subnet] The default is [Local Segment].
Subnet	When [Subnet] is selected in [Type], enter the subnet of the IPv4 address.
Subnet Mask	When [Subnet] is selected in [Type], enter the subnet mask of the IPv4 address. The default is 255.255.255.0.

[Schedule] tab

Configure the schedule for performing discovery tasks.

Item	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.

Item	Description
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify whether the interval measurement starts at the start or end of the job.
Daily	The task begins on the specified date, and it is executed daily at the specified time.
Weekly	The task begins at the specified date/time, and it is executed weekly on the specified day of the week. More than one day of the week can be specified.
Monthly	The task begins at the specified date/time, and it is executed monthly at the specified date. You can select multiple dates from the first to the last day of the month.
Advanced Settings	Select this check box to set a time period for preventing task execution.

[Auto Settings] tab

Configure the settings for SNMP Trap and Device Log Collection.

Item	Description
Enable SNMP Trap	Specify whether to enable or disable SNMP Trap. When SNMP Trap is enabled, notifications regarding the device status are sent.

Enable Device Log Collection	Specify whether or not to enable device log collection.
	• [Simple]
	Specify whether or not to collect device job logs, device access logs, and device eco logs.
	• [Advanced]
	  • Manual Input
	Specify whether to enable or disable the type of collection and encryption for each device log.
	  • Select Template
	Use the log collection template to apply the device log collection settings.

Item	Description
Delete Log data in Device	Specify whether or not to enable [Delete Log data in Device].
Encrypt Device Log Transfer	Specify whether or not to enable [Encrypt Device Log Transfer].
Enable Device Job Log	Specify whether or not to enable [Enable Device Job Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Copier] • [Printer] • [Scanner] • [Fax] • [Document Server] • [Saved Reports]
Enable Device Access Log	Specify whether or not to enable [Enable Device Access Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Authentication] • [Capture] • [Document Operation] • [Communication / Attack Verification] • [Invalid Scan] • [Validity Check] • [Administrator Operation] • [Address Book Operation] • [Log Transfer Settings] • [Device Configuration]
Enable Device Eco Log	Specify whether or not to enable [Device Eco Log].

Item	Description
Enable Device Eco Log	Specify whether or not to enable [Enable Device Eco Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Power ON] • [Power Status Transition Result] • [Power OFF] • [Paper Consumption]

Network Search

Click [Network Search] in the navigation tree to display the discovery profile. When selecting a profile name from the list, you can configure the detailed information with the [General], [Access Accounts], [Discovery Range (Network Search)], [Schedule], and [Auto Settings] tabs.

Note

- For an outline of network search and details about using network search, see page 77 "Searching for Devices".

[General] tab

Specify the task name.

Item	Description
Name	Enter the name of profile.
Description	Enter the description of profile.
DS Server	Select the Delegation Server to perform discovery.
Perform Reverse DNS Lookup	Specify whether or not to perform reverse DNS lookup in discovery. When this setting is enabled, reverse DNS lookup is performed to search for the name of the host that corresponds to the IP address.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Access Accounts] tab

Configure the account to be used to access the device when performing device discovery. 
Move the account to be used from the [Not Assigned Accounts] list to the [Assigned Account] list by clicking the button or dragging and dropping.

There are three types of [Access Accounts] as shown in the following table. Each account type is displayed by a tab.

Tab name	Description
Device Administrator Access	Displays the access account that is used in Web service protocol.
SNMP Access	Displays the access account that is used for SNMP.
SDK/J Platform Access	Displays the access account that is used for remote connection to SDK Platform.

[Discovery Range (Network Search)] tab

Configure the Discovery Range of the network search.

Item	Description
Include/Exclude	Specify whether to include or exclude a specified range in the network search.
Range Type	Select the value to search from the following: • [One Host Name] • [One IP Address] • [Specify IP Range] The default is [Specify IP Range].
Host Name	Enter the host name when selecting [One Host Name] in [Range Type].
From	Enter the IPv4 address used to perform device discovery or the starting IPv4 address for device discovery when selecting [One IP Address] or [Specify IP Range] in [Range Type].
To	Enter the ending IPv4 address for device discovery when selecting [Specify IP Range] in [Range Type].

Item	Description
Subnet Mask	Enter the subnet mask of the IPv4 address when selecting [Specify IP Range] in [Range Type]. The default is 255.255.255.0.

[Schedule] tab

Configure the schedule for performing discovery tasks.

Item	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify whether the interval measurement starts at the start or end of the job.
Daily	The task begins on the specified date, and it is executed daily at the specified time.
Weekly	The task begins at the specified date/time, and it is executed weekly on the specified day of the week. You can specify more than one day of the week.
Monthly	The task begins at the specified date/time, and it is executed monthly at the specified date. You can select multiple dates from the first to the last day of the month.
Extension setting	Select this check box to set a time period for preventing task execution.

[Auto Settings] tab

Configure the settings for SNMP Trap and Device Log Collection.

Item	Description
Enable SNMP Trap	Specify whether to enable or disable SNMP Trap. When SNMP Trap is enabled, notifications regarding the device status are sent.

Item	Description
Enable Device Log Collection	Specify whether or not to enable device log collection. • [Simple] Specify whether or not to collect device job logs, device access logs, and device eco logs. • [Advanced] • Manual Input Specify whether to enable or disable the type of collection and encryption for each device log. • Select Template Use the log collection template to apply the device log collection settings.
Delete Log data in Device	Specify whether or not to enable [Delete Log data in Device].
Encrypt Device Log Transfer	Specify whether or not to enable [Encrypt Device Log Transfer].
Enable Device Job Log	Specify whether or not to enable [Enable Device Job Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Copier] • [Printer] • [Scanner] • [Fax] • [Document Server] • [Saved Reports]

Item	Description
Enable Device Access Log	Specify whether or not to enable [Enable Device Access Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Authentication] • [Capture] • [Document Operation] • [Communication / Attack Verification] • [Invalid Scan] • [Validity Check] • [Administrator Operation] • [Address Book Operation] • [Log Transfer Settings] • [Device Configuration]
Enable Device Eco Log	Specify whether or not to enable [Device Eco Log].
Enable Device Eco Log	Specify whether or not to enable [Enable Device Eco Log], and select [Collection Type]. Select [Custom] to specify the types of logs to be collected. • [Power ON] • [Power Status Transition Result] • [Power OFF] • [Paper Consumption]

Polling

Click [Polling] in the navigation tree to display the profile list. When selecting a profile from the list, you can configure a device for periodic or immediate monitoring with the [General], [Target Devices/ Groups], [Status Polling], [Supplies Polling], [Counter Polling], [Other Polling], [User Counter Polling], and [Detailed Counter Polling] tabs.

Note

- The default profile "default" that enables periodical execution of status polling, supply polling, counter polling, and other polling is pre-registered to the system.
- For an outline of polling and details about using polling, see page 89 "Checking the Device Status".

[General] tab

Item	Description
Name	Enter the name of profile.
Description	Enter the description of profile.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Target Devices/Groups] tab

To select all the devices, select the [All Devices] check box at the top left of the dialog box that is displayed.

[Status Polling] tab

Configure the schedule for Status Polling.

Item	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify the interval from 1 minute to 7 days. Specify whether the interval measurement starts at the start or end of the job.
Daily	The task begins on the specified date, and it is executed daily at the specified time.
Weekly	The task begins at the specified date/time, and it is executed weekly on the specified day of the week. You can specify more than one day of the week.

Item	Description
Monthly	The task begins at the specified date/time, and it is executed monthly at the specified date. You can select multiple dates from the first to the last day of the month.
Extension setting	Select this check box to set a time period for preventing task execution.

[Supplies Polling] tab

Configure the schedule for Supplies Polling. The contents of the settings are the same as the settings of Status Polling.

[Counter Polling] tab

Configure the schedule for Counter Polling. The contents of the settings are the same as the settings of Status Polling.

[Other Polling] tab

Configure the schedule for Other Polling. The contents of the settings are the same as the settings of Status Polling.

[User Counter Polling] tab

Configure the schedule for User Counter Polling. The contents of the settings are the same as the settings of Status Polling.

[Detailed Counter Polling] tab

Configure the schedule for Detailed Counter Polling. The contents of the settings are the same as the settings of Status Polling.

Error Polling

Click [Error Polling] in the navigation tree to display the profile list. When selecting a profile from the list, you can configure the profile with the [General], [Target Devices/Groups], [Triggers], and [Schedule] tabs.

Note

- For an outline of error polling and details about using error polling, see page 92 "Creating an Error Polling Task".

[General] tab

Specify the name of the profile.

Item	Description
Name	Enter the name of profile.
Description	Enter the description of profile.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Target Devices/Groups] tab

To select all the devices, select the [All Devices] check box at the top left of the dialog box that is displayed.

[Triggers] tab

Select the device status that will become the criteria for starting error polling.

Type	Item
Errors	• [Select All] • [No Toner/Ink] • [Paper Misfeed] • [Call Service] • [Cover Open] • [Device Access Violation] • [No Paper] • [No Response] • [Original Misfeed: ADF] • [Fax Transmission Error] • [Error]

Type	Item
Warnings	• [Select All] • [Offline] • [Toner/Ink Almost Empty] • [Alert] • [Replace/Supply] • [Maintenance] • [Busy] • [Almost Out of Paper] • [Energy Saver Mode] • [Warming Up...]

[Schedule] tab

Configure the schedule for [Error Polling].

Item	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify whether the interval measurement starts at the start or end of the job.
Daily	The task begins on the specified date, and it is executed daily at the specified time.
Weekly	The task begins at the specified date/time, and it is executed weekly on the specified day of the week. You can specify more than one day of the week.
Monthly	The task begins at the specified date/time, and it is executed monthly at the specified date. You can select multiple dates from the first to the last day of the month.
Extension setting	Select this check box to set a time period for preventing task execution.

Access Profiles

The following types of [Access Profiles] are available: [SNMP] and [SDK/J Platform].

Device Administrator

Click [Device Administrator] in the navigation tree to display a list of access accounts used for the Web service protocol.

Note

- For an outline of the access account and details about using the access account, see page 76 "Configuring an Access Account".

Item	Description
Profile Name	Enter the profile name.
Description	Enter the task description.
User Name	Enter the user name. The user name can contain up to 32 characters.
Password	Enter the password. The password can contain up to 128 characters.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

SNMP

Click [SNMP] in the navigation tree to display a list of access accounts used for the SNMP protocol.

Note

- "default" is registered as a default account in the system.
- For an outline of the access account and details about using the access account, see page 76 "Configuring an Access Account".

Item	Description
Profile Name	Enter the profile name.
Description	Enter the task description.
Retry	Specify how many retry attempts can be performed if a device does not respond during discovery.
Timeout	Specify how long the waiting period is if a device does not respond during discovery. Specify a value between 500 and 60000 milliseconds. The default is 2000 milliseconds.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Protocol	Select the type of the protocol. • SNMP v1/v2 • SNMP v3 Configuration items vary depending on protocol types.
Read Community Name	Enter [Read Community Name]. Specify this item when [SNMP v1/v2] is selected in [Protocol]. The Read Community Name can contain up to 15 characters.
Write Community Name	Enter [Write Community Name]. Specify this item when selecting [SNMP v1/v2] in [Protocol]. The Write Community Name can contain up to 15 characters.
User Name	Enter the user name. Specify this item when selecting [SNMP v3] in [Protocol]. The user name can contain up to 32 characters.
Password	Enter the password. Specify this item when selecting [SNMP v3] in [Protocol]. The password can contain up to 128 characters.

Item	Description
Authentication Algorithm	Select the authentication algorithm. • [SHA1] • [MD5] Specify this item when selecting [SNMP v3] in [Protocol].
Context Name	Enter the context name. Specify this item when selecting [SNMP v3] in [Protocol]. The context name can contain up to 256 characters.
Encrypted Password	Enter the encryption password. Specify this item when selecting [SNMP v3] in [Protocol]. The encrypted password can contain up to 32 characters.
Encryption Algorithm	Select the encryption algorithm. • [DES] • [AES128] Specify this item when selecting [SNMP v3] in [Protocol].

SDK/J Platform

Click [SDK/J Platform] in the navigation tree to display a list of access accounts used for the SDK/J protocol.

Note

- "default" is registered as a default account in the system.
- For an outline of the access account and details about using the access account, see page 76 "Configuring an Access Account".

Item	Description
Profile Name	Enter the profile name.
Profile Description	Enter the task description.
Password	Enter the password. The password can contain up to 128 characters.

Item	Description
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

Configuration

This section describes the functions of items displayed in [Configuration] in the navigation tree.

Configuration Templates

Create a template to change the device settings.

Standard Device Preferences

Click [Device Settings] in the navigation tree to display the template list.

Note

- For an outline of the device settings and details about using the device settings, see page 102 "Managing the Device Settings".

Create New Standard Settings Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Create Blank Template	Create a template without specifying any configuration values.
Get Settings from Device	Retrieve the setting values from a device and create a template. You can edit the retrieved data. You cannot retrieve encrypted information such as passwords and security settings. • [Select Device] button: Click this button to display the dialog box for selecting the device.

Item	Description
Import Settings from File	Import setting values from an external file and create a template. You can edit the retrieved data. • [Browse...] button: Click this button to specify the path of the file to be imported.

You can edit the template from the [General] tab and [Standard Device Preferences] tab when selecting the template from the list.

[General] tab

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Standard Device Preferences] tab

The categories of the setting items that can be edited are displayed on the left side of the screen. Select a category to display the screen for editing the setting on the right side of the screen.

- General
- Date and Time
- Smart Operation Panel
- Network Protocols
- TCP/IP
- SNMP
- Administrator
- Email
- Authentication
- Service and Consumables
- Printer

- Security
- Interface
- Device Functions
- Web Browser NX

For details about the configuration items, see page 643 "List of Device Preference Setting Items".

Device-specific Preferences

Click [Device-specific Preferences] in the navigation tree to display the template list.

Note

- For an outline of the device-specific preferences and details about using the device-specific preferences, see page 102 "Managing the Device Settings".

Create New Device-Specific Settings Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Get Encrypted Settings from Device	Obtains the device-specific preferences from the device. • [Select Device] button: Click this button to display the dialog box for selecting the device. When a device is selected, [Device Name], [Vendor], and other device information are displayed. In addition, the following can be configured: • [Password]: Enter the password to encrypt and decrypt the obtained file. • [Logo Image]: Select this check box to obtain a logo file from the device for creating the template.

Item	Description
Import Encrypted Settings from File	Import the device-specific preferences from a file. Click an item to select and configure the following: • [Settings File]: Click the [Browse...] button to specify the path of the file to be imported. • [Logo File]: Click the [Browse...] button to specify the path of the logo file to be imported. • [Password]: Enter the password that was used when the encrypted data was created.
Get Smart Operation Panel Settings from Device	Obtains the Smart Operation Panel settings from devices equipped with Smart Operation Panel.

Firmware

Click [Firmware] in the navigation tree to display the template list.

Note

- For an outline of the firmware template and details about using the firmware template, see page 102 "Managing the Device Settings".

Create New Firmware Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Download from RICOH Software Server	Downloads the firmware file from RICOH server.

Item	Description
Use File in Repository	Displays the list of firmware files. The displayed files include both the files downloaded from the repository on RICOH server and the files uploaded from the local computer. Select a file from the following list: • [Firmware Package Information]: [Device Model Name], [Description], [Package Version], [Release Date], and [Registration Date] are displayed in the list. • [Firmware Module Information]: [No.], [Module Name], [Version], and [Part Number] are displayed in the list.
Upload New File to Repository	Updates the custom RICOH firmware. This is not normally selected. Uploads the firmware to the repository. • [File Path]: Click the [Browse...] button to select the firmware file. • [Description]: Enter the description of the firmware file. • [Firmware Package Information]: [Device Model Name], [Description], [Package Version], [Release Date], and [Registration Date] are displayed in the list. • [Firmware Module Information]: [No.], [Module Name], [Version], and [Part Number] are displayed in the list.
Retrieve Smart Operation Panel Settings from Device	Obtains the Smart Operation Panel settings from devices equipped with Smart Operation Panel.

When a firmware template is selected from the list, the [General] and [Firmware] tabs are displayed under the list.

[General] tab

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.

Item	Description
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Firmware] tab

From the [Firmware] tab, you can check the detailed information of the firmware template.

SDK/J Platform

Click [SDK/J Platform] in the navigation tree to display the template list.

Note

- For an outline of the SDK/J platform and details about using the SDK/J platform, see page 108 "Managing the SDK/J Platform".

Create New SDK/J Platform Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Download from RICOH Software Server	The latest version of the SDK/J platform that corresponds to the device can be obtained from the RICOH Software Server, and the file can then be distributed to the device. • [Country]: Select the country name.

Item	Description
Use File in Repository	Select a file from the list of SDK/J Platform file in the repository. • [Forced Installation]: When this check box is selected, the SDK/J platform is installed on the device regardless of the version of the SDK/J platform that has already been installed on the device. Clear the check box to not apply the update when the major version of the SDK/J platform is different.
Upload New File to Repository	Uploads the SDK/J Platform file to the repository. • [File Path]: Click the [Browse...] button to select the SDK/J platform file. • [Description]: Enter the description of the SDK/J platform file. • [Upload] button: Click to upload the selected firmware to the repository. • [Forced Installation]: When this check box is selected, the template is installed on the device regardless of the version of the SDK/J platform that is already installed on the device. Clear the check box to not apply the update when the major version is different.

When a template is selected from the list, the [General] and [SDK/J Platform] tabs are displayed under the list.

[General] tab

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.

[SDK/J Platform] tab

You can check the detailed information of the template from the [SDK/J Platform] tab.

Device Applications

Click [Device Applications] in the navigation tree to display the template list.

Note

- For an outline of the Device Applications and details about using Device Applications, see page 109 "Managing Device Applications".

Create Device application Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Application Source	Select the application source. • [RICOH Software Server] • [Local File]
Download from RICOH Software Server	This item can be selected when [RICOH Software Server] is selected in [Application Source]. Device Applications can be downloaded from [RICOH Software Server] after the following items are configured: • [Country]: Select the country name. • [Product Key]: Enter the product key.
Use File in Repository	This item can be selected when [Local File] is selected in [Application Source]. The application file on the repository can be selected. • [Heap Size]: Specify the heap size. Heap Size is the area in memory that can be used by both the Java Platform and all applications. • [Stack Size]: Specify the stack size. Stack Size is the data storage area where temporary files are stored when an application is executed.

Item	Description
Uninstall	**To uninstall the Device Application of RICOH Software Server:** Select [RICOH Software Server] in [Application Source]. • [Country]: Select the country name. • [Product Key]: Enter the product key. **To uninstall the Device Application installed on the device:** Select [Local File] in [Application Source]. • [Application Name]: Select the application. • [Version to uninstall]: Select the version.
Activate	Creates a template for activating the Device Application using [RICOH Software Server]. This item can be selected when [RICOH Software Server] is selected in [Application Source]. • [Country]: Select the country name. • [Product Key]: Enter the product key.
Upload New File to Repository	This item can be selected when [Local File] is selected in [Application Source]. Uploads the application file to the repository. • [File Path]: Specify the application. • [Description]: Enter the description of the application file. • [Heap Size]: Specify the heap size. Heap Size is the area in memory that can be used by both the Java Platform and all applications. • [Stack Size]: Specify the stack size. Stack Size is the data storage area where temporary files are stored when an application is executed. • [Upload] button: Click to upload the selected firmware to the Core Server.

When an application template is selected from the list, the [General] and [Application] tabs are displayed under the list.

[General] tab

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Product Key	Enter [Product ID] only for the Device Application template of [RICOH Software Server].

[Application] tab

From the [Application] tab, you can check the detailed information of the application template.

Address Book

Click [Address Book] in the navigation tree to display the template list.

Note

- For an outline of the address book and details about using the address book, see page 112 "Managing the Address Book".

Create New Address Book Template

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Create Blank Template	Creates a template without specifying any configuration values. Select one of the following authentication methods: • [User Code / None]: Select this when using user code authentication or when not using user authentication. • [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server]: Select this item for Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server.

Item	Description
Get Editable Settings from Device	Creates a template with the user information retrieved from a device. You can retrieve and modify user information such as e-mail addresses and authentication information. Highly sensitive information cannot be retrieved from devices. • [Select Device] button: Click this button to display the dialog box for selecting the device.
Get Encrypted Settings from Device	Creates a template with the encrypted information retrieved from a device. • [Select Device] button: Click this button to display the dialog box for selecting the device. • [Password]: Enter the password for the encrypted file.
Import Editable Data from File	Creates a template with the user information imported from a text or CSV file. • [File Path]: Click the [Browse...] button to select a file.
Import Encrypted Data from File	Creates a template from the information imported from a backup file. • [File Path]: Click the [Browse...] button to select a file. • [Password]: Enter the encryption key that was used when creating the backup file.
Import Data from SmartDevice Monitor for Admin/Ridoc IO Analyzer	Imports the data from SmartDeviceMonitor for Admin/ Ridoc IO Analyzer. • [File Path (Address Management Tool)]: Click the [Browse...] button to select the file of the address management tool. This item must be specified. • [File Path (User Management Tool)]: Select the file of the User Management Tool.

When a template is selected from the list, the [General], [Settings], and [Entry List] tabs are displayed under the list.

[General] tab

Set the general information of a task.

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Settings] tab

On this tab, configure the address book.

Item	Description
Counter Collection per User	Before applying the template contents, such as batch entry delete, specify whether or not to collect user counters registered to the device.
Reset Volume Use	Specify whether or not to reset the volume use of all users registered to the device.
Delete Entry	Specify whether or not to delete the address book before applying the template contents. • [All]: All entries in the address book are deleted at once. • [User Setting]: If the [Specify Batch Deletion of User Entries] check box is selected, all "User" entries whose login name or user code is not specified will be deleted. If the [Specify Batch Deletion of Destination Entries] check box is selected, all "User" entries whose login name or user code is not specified will be deleted. If the [Specify Batch Deletion of Group Entries] check box is selected, all “Groups" entries will be deleted. • [Disable]: Entries cannot be deleted at once.

Item	Description
Match All Settings	Specify whether or not to have device entries exactly match the template contents. If the [Match All Settings] check box is selected, the entries that are not present in the template are completely deleted from the device. If the [Match All Settings] check box is not selected, device data is not deleted, but entries that are present in the template are added or updated.

[Entry List] tab

Edit settings for a user or a group. You can add or delete user or group entries. You can configure an entry using the tabs shown below.

- [General] tab

  This tab is displayed for user and group entries.

  Select the [Set] check box to change the setting.

Item	Description
User Name	Enter a name.
Specify Registration No.	Specify whether to specify a registration number manually or to acquire the number automatically from the device. To specify a number, select this check box.
Registration No.	Enter this item to specify the registration number.
Key Display Name	Enter the name to be displayed on the display panel of the device.
Index	Enter the pronunciation characters for the key display name.
Display Priority	Specify the display priority on the control panel of the machine. Specify from the following range: • [Do not Specify] • [Priority]1–10 The default is [Priority]5.

- [Title] tab

  This tab is displayed for user and group entries.

  Select the [Set] check box to change the setting.

Item	Description
Title1-3	Select from Title 1 to 3 for the registered title.
Add to Freq.	Select the check box of this item to use it as a working title.

- [User Code] tab

  This tab is displayed for a user entry.

  This item appears only if you select [User Code / None] as the authentication method when creating the template.

  Select the [Set] check box to change the setting.

Item	Description
User Code	Enter the user code to be assigned to an account.

- [Auth. Info] tab

  This tab is displayed for a user entry.

  Select the [Set] check box to change the setting. The following setting items can be specified when the authentication method of the template is [Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Server]:

Item	Description
Authentication	Enter the login user name and password. Specify this setting when the authentication method of the template is [Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Server].
Folder Authentication	• [Do not Specify]: Folder authentication is not specified. • [Use Login Auth. Info]: Folder authentication is performed using the login user name and password specified in [Authentication]. • [Specify Other Auth. Info]: Folder authentication is performed using authentication information that is different from the login user name and password set in [Authentication]. Enter the login user name and password to be used for folder authentication.

Item	Description
SMTP Authentication	• [Do not Specify]: SMTP authentication is not specified. • [Use Login Auth. Info]: SMTP authentication is performed using the login user name and password specified in [Authentication]. • [Specify Other Auth. Info]: SMTP authentication is performed using authentication information that is different from the login user name and password set in [Authentication]. Enter the login user name and password to be used for SMTP authentication.
LDAP Authentication	• [Do not Specify]: LDAP authentication is not specified. • [Use Login Auth. Info]: LDAP authentication is performed using the login user name and password specified in [Authentication]. • [Specify Other Auth. Info]: LDAP authentication is performed using authentication information that is different from the login user name and password set in [Authentication]. Enter the login user name and password to be used for LDAP authentication.

Note

- [Login Password] and [Password] are secure information. The information cannot be obtained from devices, or checked whether the information in the device are the same as the information specified in the Management Console.

10

- [Available Functions] tab

  This tab is displayed for a user entry.

  Select the [Set] check box to change the setting.

Item	Description
Copier	Specify the color modes that are available for the copier function. • [Level]: Enable or disable the following items: When [Disable] is selected, all items are disabled. • [Black & White]: Monochrome copying is enabled. • [Single Color]: Monochrome copying and single color copying are enabled. • [Two-color]: Monochrome copying, single color copying, and two-color copying are enabled. • [Auto Color]: Auto color copying is enabled. • [Full Color]: Full color copying is enabled.
Printer	Specify the color modes that are available for the printer function. [Level]; All enabled items are disabled. Click the following items to enable or disable each function. All items are disabled when Disable is selected. • [Black & White]: Monochrome printing is enabled. • [Color]: Monochrome printing and color printing are enabled.
Other Functions	• [Scanner]: The scanner function is enabled when this check box is selected. • [Fax]: The facsimile function is enabled when this check box is selected. • [Document Server]: The document server function is enabled when this check box is selected.
Limit Value for Print Volume Use Limitation	Enter the limit of the printing volume.

- [Email/Fax] tab

  This tab is displayed for a user entry.

  Select the [Set] check box to change the setting.

Item	Description
Fax Destination	Enter a fax number or an IP-Fax destination. When a subaddress is combined with a UUI, enter the combined UUI-▶ subaddress in this order. Enter "^" between the IP-Fax destination and an advanced destination.
Select line type.	Set the line type to be used. • G3 • G3 PABX • G4 • G4 PABX • I-G3 • I-G3 PABX • G3 Auto • G3 Auto PABX • G3-1 • G3-1 PABX • G3-2 • G3-2 PABX • G3-3 • G3-3 PABX • H.323 • SIP The default is G3.
International Transmission Mode	Select the check box for this item to enable international transmission mode.
Address	Enter the e-mail address of the user.
Use This Email Address for Email and Internet Fax	The specified e-mail address is used for e-mail and Internet fax.
Use This Email Address for Internet Fax	The specified e-mail address is used for Internet fax.

Item	Description
Internet Fax – via SMTP Server	Select the check box to send an Internet fax via the SMTP server.
Fax Header	Select the sender's name.
Label Insertion	Select this check box to specify the label insertion.
1st Line	The name used for label insertion is displayed.
Label Insertion 2nd Line (String)	Set the string of the second line entered in label insertion. You can specify a custom message.
Label Insertion 3rd Line (Standard Message)	Specify the message of the third line used for label insertion. You can specify a fixed phrase.

- [Folder] tab

  This tab is displayed for a user entry.

  Select the [Set] check box to change the setting.

Item	Description
Protocol	Select the protocol to be used. • SMB • FTP • NCP-Bindery • NCP-NDS The default is SMB.
Port Number	When the protocol is FTP, enter a port number. Specify from the following range: • 1–65535 The default is 21.
Server Address	When the protocol is FTP, enter a server name.
Path	Enter the path.

Item	Description
Japanese Character Code Set	When the protocol is FTP, specify the character code of text in Japanese. • US-ASCII • SHIFT-JIS • EUC-JP The default is US-ASCII.

- [Protection] tab

  This tab is displayed for user and group entries.

  Select the [Set] check box to change the setting.

Item	Description
Register as Destination	Select the check box to use the address book as the destination. This tab is not displayed for a group entry.
Protect Dest.	Select the check box to protect folder destinations. This item is valid only when the folder destination is specified.
Register as Sender	Select the check box to use the address book as the sender. This item will not be displayed if the target device does not support this function.
Protect Sender	Select the check box to protect the sender. This setting is valid only when [Register as Sender] is selected.
Protection Code	Enter the protection code of the sender and folder This setting is valid only when [Protect Dest.] is selected.

Item	Description
Access Control List for Destination Protection Settings	The names and permissions of the entries to which destination protection is specified are displayed in a list. Select the address book, and specify the permissions from the following: • [read-only] • [read-write] • [Delete] • [Full Control] This item is not displayed when [User Code Authentication] or [No Authentication] is selected as the authentication method. This tab is not displayed for a group entry.
Access Control List for Document Protection Settings	The names and permissions of the entries to which document protection is specified are displayed in a list. Select the address book, and specify the permissions from the following: • [read-only] • [read-write] • [Delete] • [Full Control] This item is not displayed when [User Code Authentication] or [No Authentication] is selected as the authentication method. This tab is not displayed for a group entry.

Note

- [Protection Code] is secure information. The information cannot be obtained from devices, or checked whether the information in the device are the same as the information specified in the Management Console.

- [Group List] tab

  This tab is displayed for user and group entries.

  Select the [Set] check box to change the setting.

Item	Description
Selected Groups	The groups to which the entry is registered are displayed in a list. If you do not use the address book as the target of this template, move the address book to [Unselected Groups] by dragging and dropping or by using the button.
Unselected Groups	The groups to which the entry is registered are displayed in a list. To set the address book as the target of this template, move the address book to [Selected Groups] by dragging and dropping or by using the button.

- [Users and Groups] tab

  This tab is displayed for a group entry.

  The users and groups that are registered to the address book are displayed in the list.

- [Reset Counter per User] tab

  This tab is displayed for a user entry.

  Select the [Set] check box to change the setting.

Item	Description
Print (Copier, Fax Print, Printer)	The print counter using the copier, printer, and fax functions is reset.
Fax Transmission	The fax send counter is reset.
Scanner	The scanner counter is reset.
Volume Used	The user quota counter is reset.

Log Collection

Click [Log Collection] in the navigation tree to display the template list.

Note

- For an outline of the log collection and details about using the log collection, see page 114 "Managing Device Logs".

Log Collection

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

You can edit the template from the [General] tab and [Log Collection] tab when selecting the template from the list.

[General] tab

Item	Description
Template Name	Enter the template name.
Description	Enter the template description.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Log Collection] tab

Item	Description
Delete Log data in Device	Specify whether or not to delete all the log data on the device.
Configure log transfer settings	Specify whether or not to activate the log transfer setting.
Encrypt Device Log Transfer	Encrypts the data transfer of the device log. To encrypt transfer, enable the SSL settings of the system. For details, see page 403 "Enabling SSL".

Item	Description
Encrypt Logs in Device	To save a log to a device securely, configure the settings to encrypt and save the log on the device.
Enable Device Job Log	Collects the device job log. Select the configuration method of the Device Job Log. • [All]: All items in [Collection Type] are selected. • [Custom]: Select the items to check from [Collection Type]. When selecting [Custom], select [Collection Type] from the following: • [Copy] • [Scanner] • [Document Box] • [Printer] • [Fax] • [Report]
Enable Device Access Log	Specify whether or not to enable the Device Access Log. Select the configuration method of the Device Access Log. • [All]: All items in [Collection Type] are selected. • [Custom]: Select the items to check from [Collection Type]. When selecting [Custom], select [Collection Type] from the following: • [Authentication] • [Document Operation] • [Invalid Scan] • [Administrator Operation] • [Log Transfer Setting] • [Capture] • [Communication / Attack Verification] • [Validity Check] • [Address Book Operation] • [Device Configuration]

Item	Description
Enable Device Eco Log	Specify whether or not to enable the Device Eco Log. Select the configuration method of the Device Eco Log. • [All]: All items in [Collection Type] are selected. • [Custom]: Select the items to check from [Collection Type]. When selecting [Custom], select [Collection Type] from the following: • [Power ON] • [Power OFF] • [Power Status Transit] • [Per Hour Counter]

Configuration Tasks

Click [Configuration Tasks] in the navigation tree to display the task list.

Note

- For an outline of the configuration tasks and details about using the configuration tasks, see the following:
  - page 116 "Registering a Template to a Task"
  - page 118 "Rebooting a Device"
  - page 120 "Managing the Power Status of Devices"

[General] tab

Set the general information of a task.

Item name	Description
Name	Enter the task name.
Description	Enter the task description.

Item name	Description
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".
Type	Select the type of the task. • [Check] • [Apply] • [Reboot] • [Energy Saver Mode] • [Cancel Energy Saver Mode]

[Template] tab

Click the button on the toolbar to display the dialog box for selecting the template to be included in the task. Use the button to move the template to be used from the [Template] list to the [Target Template] list

Specify [Force Reboot after Template Execution] or [Switch into Energy Saver Mode after Execute Template] as necessary.

- When [Force Reboot after Template Execution] is specified, the device reboots after template execution regardless of the execution result.
- When [Switch into Energy Saver Mode after Execute Template] is specified, the device switches to energy saver mode after template execution.

Note

- The [Template] tab is not displayed when [Energy Saver Mode], [Cancel Energy Saver Mode], or [Reboot] is selected in [Type] on the [General] tab.

[Target Devices/Groups] tab

The target users/groups of the task are displayed in the list. Click the button on the toolbar to add the target devices in units of devices or groups.

[Schedule] tab

Specify the task execution schedule.

Item name	Description
Disable Schedule	Select the check box to disable the schedule.

Item name	Description
Once Only	Executed only once at the specified date/time.
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify the interval from 1 minute to 7 days. Specify whether the interval measurement starts at the start or end of the job.
Daily	The task begins on the specified date, and it is executed daily at the specified time.
Weekly	Network search begins at the specified date/time, and it is executed weekly on the specified day of the week. You can specify more than one day of the week.
Monthly	The task begins at the specified date/time, and it is executed monthly at the specified date. You can specify more than one date from the 1st to 31st day or the last day of the month.
Advanced Settings	Select this check box to set a time period for preventing task execution.

[Notifications] tab

Item	Description
Enable Task Completion Notification	Specify whether or not to send a notification e-mail when the task is completed.
Input Email Address Manually	Enter the e-mail address of the destination manually. • Email address: Enter the e-mail address of the destination. • [Language]: Select the language to use in the notification e-mail.
Select Destination	Select a destination from the destinations registered in [System] ▶ [Notification] ▶ [Destination].

Streamline NX Embedded Settings

Configure the operations related to the Device Applications of RICOH Streamline NX.

Embedded Login Screen

Click [Embedded Login Screen] in the navigation tree to display the list of screen names.

Note

- For an outline of the login screen and details about using the login screen, see page 122 "Managing the Streamline NX Embedded Settings".

[General] tab

Item	Description
Screen Name	Enter the name of the custom screen.
Description	Enter the description of the custom screen.

[WVGA] tab

Configure the login screen to be displayed on an MFP that is equipped with a WVGA screen.

The preview image is displayed on the right side of the screen, and the edit screen is displayed on the left side.

Item	Description
Screen Background Color	Specify the background color of the screen. Enter the color code in hexadecimal notation. You can also select the color from the color palette. The default is #FFFFFF (white).
Show Message	Select the check box to display a message on the login screen.

Item	Description
Message	Select the language of the message to be displayed on the login screen, and enter the message text. • [en_US] • [fr_FR] • [de_DE] • [it_IT] • [es_ES] • [nl_NL] • [zh_CN] • [zh_TW] • [ja_JP] • [pt_PT] • [pt_BR] • [ru_RU] • [da_DK] • [no_NO]
Message Background Color	Specify the background color of the message. Enter the color code in hexadecimal notation. You can also select the color from the color palette. To specify transparent background color, enter #ff00ff. The default is #FFFFFF (white).
Font Size	Select the size of the characters in the message. • [Large] • [Medium] • [Small] The default is [Large].
Font Color	Specify the color of the characters in the message. Enter the color code in hexadecimal notation. You can also select the color from the color palette. The default is #000000 (black).

Item	Description
Button Title	Configure the labels of the [Language], [Guest], [PIN Login], and [Login] buttons. You can specify this setting for each language. Select the language, and then enter the label name.
Button Style	Select the button style. • [Normal] • [String] • [Blue Edge] • [Red Edge] • [Green Edge] • [Gray] • [None] The default is [Green Edge].
Font Size	Select the size of the button text. • [Large] • [Medium] • [Small] The default is [Large].
Font Color	Specify the color of the button text. Enter the color code in hexadecimal notation. You can also select the color from the color palette. The default is #000000 (black).
Alignment	Select the alignment to be applied to the Guest Button. • [Center] • [Left]

Item	Description
New Image File	Import an image to be displayed as the new image of the card reader. An image of up to 128 kB can be imported. The specifications of the images that can be imported are as follows: • Length WVGA: 800 px, 4.3 inch: 480 px, Smart Operation Panel: 1024 px • Height WVGA: 444 px, 4.3 inch: 256 px, Smart Operation Panel: 520 px • File Size WVGA: 128 KB, 4.3 inch: 128 KB, Smart Operation Panel: 2 MB • Format JPEG, PNG
Show Screen icon	Displays an image on the login screen.

[4.3 inch] tab

Configure the login screen to be displayed on an MFP that is equipped with a 4.3-inch screen.

The preview image is displayed on the right side of the screen, and the edit screen is displayed on the left side.

Item	Description
Same as WVGA	Specify whether or not to apply the same settings as the WVGA login screen. To not apply the same settings as the WVGA login screen, clear the check box, and then configure the settings. The same setting items as the WVGA tab are available.

[Smart Operation Panel] tab

Configure the login screen to be displayed on an MFP that is equipped with the Smart Operation Panel.

The preview image is displayed on the right side of the screen, and the edit screen is displayed on the left side.

Item	Description
Same as WVGA	Specify whether or not to apply the same settings as the WVGA login screen. To not apply the same settings as the WVGA login screen, clear the check box, and then configure the settings. The same setting items as the WVGA tab are available.

Embedded Authentication

Click [Authentication] in the navigation tree to display the list of configuration names.

Note

- For an outline of authentication and details about using authentication, see page 122 "Managing the Streamline NX Embedded Settings".

[Authentication and Accounting] tab

Item	Description
Configuration Name	Enter the name of the setting.
Description	Enter the description of the setting.
Card Reader	Select the type of supported card reader. • [No Card Reader] • [Keyboard-emulation Reader] The default is [No Card Reader].
Auto Logout Timer	Specify whether or not to enable Auto Logout Time. If no operations are performed for the specified period of time, the user is automatically logged out, and the device returns to the login screen. Specify the period from the following range: • 1–60 second(s) The default is 30 seconds.
Login Screen	Specify whether to use the default login screen or the custom login screen.
Prioritized Application	Select the screen to be displayed after the login screen.

Item	Description
Login Method	Specify the Login Method. • [PIN Login]: Specify whether or not to enable login by entering a user PIN. • [Guest Login]: Specify whether or not to enable login by using a guest account. When [Guest Login] is enabled, configure [Guest User] and [Guest Prioritized Application].
Enable Local User Cache	Specify whether or not to enable the Local User Cache function. When this check box is selected, the user information is cached on the hard disk drive of the devices and used if the connection to the authentication server cannot be established. Configure the expiration time of the user information that is cached on the device. • [Expire]: Specify whether or not to set an expiration period. • [Expiration Time]: Specify the expiration time between 1 and 999 day(s). The default is 30 days.
Direct Print	Configure the Direct Print function. • [Allow device direct print]: Specify whether or not to allow the use of Direct Print. • [Accept anonymous user]: Specify whether or not to allow an anonymous user to perform printing. • [Accept alias user]: Specify whether or not to allow an alias user to perform printing. Note • Laser printers do not support printing using the [Accept anonymous user] option. To accept an anonymous user's print jobs when using a laser printer, configure print job authentication for the laser printer. For details, see page 639 "Servers".
Cost Center Label Level 1	Specify the label of Cost Center Level 1 to be displayed on the screen of the device.

Item	Description
Cost Center Label Level 2	Specify the label of Cost Center Level 2 to be displayed on the screen of the device.

Authentication Priority List

Click [Authentication Priority List] in the navigation tree to display the list of priority list names.

Note

- For an outline of the authentication priority list and details about using the authentication priority list, see page 122 "Managing the Streamline NX Embedded Settings".

[General] tab

Item	Description
Priority List Name	Enter the name of Priority List.
Description	Enter the description of Priority List.

[Authentication Order] tab

The authentication list is displayed. Use the buttons on the toolbar to add, delete, or sort the authentication profiles.

Embedded Print

Click [Embedded Print] in the navigation tree to display the list of configuration names.

Note

- For an outline of print and details about using print, see page 122 "Managing the Streamline NX Embedded Settings".

Item	Description
Configuration Name	Enter the name of the setting.
Description	Enter the description of the setting.
Sort Field	Specify how to sort the print jobs. • [Job Name] • [Date/Time]

Item	Description
Sort Order	Specify the sort order of the print jobs. • [Ascending] • [Descending]
Job Selection	Specify the type of print jobs to be selected in the job list. • [All Selected]: All jobs in the job list are selected by default. • [None Selected]: None of the jobs in the job list are selected by default. • [Print Not Selected] Only Unprinted Jobs Selected: Unprinted jobs in the job list are selected by default.

Cancel job on logout	Specify whether or not to cancel a print job when the user logs out while the job is being processed.
	• [Do not cancel]: A job is not canceled on logout.
	• [Always]: A job is always canceled on logout.
	• [On printer error]: A job is canceled on logout only when any of the following errors occurs:
	  • the device is running out of paper or toner
	  • a door of the device is open
	  • paper is jammed in the device
	  • the device is offline
	Note
	• The canceled job is also deleted from the Delegation Server and RICOH Streamline NX PC Client.
	• This function is not available for laser printers not equipped with Smart Operation Panel or 4.3-inch screen.
	• A user with read and write privilege on SNMPv2 should exist on the device.

Embedded Setting

Click [Embedded Setting] in the navigation tree to display the list of setting names.

Configure the settings to apply to the device by combining [Embedded Authentication], [Authentication Priority List], and [Embedded Print] of [Embedded Configuration].

Note

- For an outline of the login screen and details about using the login screen, see page 122 "Managing the Streamline NX Embedded Settings".

[General] tab

Item	Description
Setting Name	Enter the name of the setting.
Description	Enter the description of the setting.

Setting Configuration tab

Item	Description
Embedded Authentication	Specify the authentication settings to use with Streamline NX Embedded Applications.
Authentication Priority List	Select the order of the profile to apply in user authentication.
Embedded Print	Specify the print settings to use with Streamline NX Embedded Applications.
Delegation Server Failover/Load Balancing Groups	Select the Delegation Servers and specify the order of them that devices access when these devices request authentication, scanning, or printing. To select a Delegation Server, create a group in [Server Management] ▶ [Delegation Server Failover/Load Balancing Groups]. For details, see page 383 "Balancing the Workload among Servers".

Target Devices/Groups tab

The target users/groups of the setting are displayed in the list. Click the button on the toolbar to add the target devices in units of devices or groups.

Streamline NX PC Client Settings

Configure the RICOH Streamline NX PC Client settings.

PC Client Global Settings

Item	Description
Allow user to change location profile	Specify whether RICOH Streamline NX PC Client users are allowed to select the location profile on their RICOH Streamline NX PC Client.

PC Client Location Profiles

Click [PC Client Location Profiles] in the navigation tree to display the list of location profiles.

[General] tab

Item	Description
Name	Enter the name of the location profile.
Descriptions	Enter the description of the location profile.

Item	Description
Auto Update	Specify the update method for RICOH Streamline NX PC Client. You can update RICOH Streamline NX PC Client when the installer for the new version is stored on a Delegation Server. • Never Check RICOH Streamline NX PC Client does not check for updates. • Auto Check RICOH Streamline NX PC Client checks for updates automatically and the users can select whether to install them. • Auto Install RICOH Streamline NX PC Client checks for updates and installs them automatically. **Note** • To update the software, store the RICOH Streamline NX PC Client installer in .zip format on the Delegation Server. • Auto update is carried out when RICOH Streamline NX PC Client starts up.

Item	Description
Message Center	Specify the type of messages to be displayed on the desktop. • Error Displays a message only when a print process could not proceed. • Error/Warning Displays a message when a print process could not proceed or certain user operations are required. • Error/Warning/Information Displays all notification information as messages. **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.
Usage Report	Specify whether or not to send usage report data regularly to Ricoh. Usage report data is used to enhance the functions. Personal information is not included. • Disable • Enable
SLP Scope	Specify the SLP scope RICOH Streamline NX PC Client uses when searching Delegation Servers.
Use Windows Authentication	Specify whether or not to use the Windows logon user name and password as the authentication information of print jobs. • No • Yes

[Secure Print] tab

Item	Description
Delete after print is done	Specify whether or not to delete the print job after it has printed. **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.
Job Storage Period	Specify the period to retain the print job. • When [Days] is selected in [Storage Period Units]: 1–365 (Days) • When [Hours] is selected in [Storage Period Units]: 1–24 (Hours) **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.
Storage Period Units	Specify the unit for the period to retain the print job. • Days • Hours **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.
Exclude Saturdays and Sundays from Storage Period	Specify whether or not to exclude weekends from the specified job storage period. **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.

Item	Description
Auto Delete Interval (hours)	Specify the interval to delete the print jobs for which the job storage period has elapsed. **Allow Local Change** Specify whether RICOH Streamline NX PC Client users can change this setting from their computers.

[Delegation Servers] tab

This list defines the Delegation Servers with which the RICOH Streamline NX PC Clients may communicate. The order of the list defines the priority by which the RICOH Streamline NX PC Client accesses a different Delegation Server using the failover function. Click (Add) on the toolbar to add Delegation Servers. To select all Delegation Servers, select the [All Servers] check box at the top left of the dialog box.

System

This section describes the functions of items displayed in [System] in the navigation tree.

Server Settings

In the [Server Settings] category, you can configure the format of the date and device display name and the Delegation Server settings.

Activation/Usage Report Notification

Click [Activation/Usage Report] in the navigation tree to display the list of [Activated Licenses] and [Available Functions]. In the following dialog box, click [Add] to activate the license:

Item	Description
Activation Type	Select either [Online] or [Offline] as the activation type. If the Core Server cannot connect to the Internet, activate it offline. From a client computer connected to the Internet, navigate to the Ricoh license management website (https://licensemanagement.ricoh.com/aui/), and obtain the license code.
Product Key	Enter a product key for online activation.
License Code	When activating the software offline, enter the license code obtained from the Ricoh license management website.
Country	Select the country of the system. The country specified at the time of installation is registered as default.
Company	Enter the company name.

Usage Report Notification

Item	Description
Usage Report	Specify whether or not to send a notification for the usage of this product to the back-end server. **Note** • The usage information is anonymously sent to assist in the development of better products. Personal information is not included.

Note

- For details about activation, see “Activating RICOH Streamline NX”, Installation Guide.

Display

Click [Device Settings] in the navigation tree to display the setting screen for each item.

Note

- For functional outlines and details about using the functions, see page 50 "Changing the Display Settings".

Country Setting

Item	Description
Country	You can change the default country. The selected country is applied to Activation, Device Applications, and Power Usage.

Date Display Format

Item	Description
Date Display Format	Select the date display format from the following: • [YYYY/MM/DD] • [MM/DD/YYYY] • [DD/MM/YYYY]
First Day of Week	For the setting items displaying the day of the week, specify the day that the week starts.

Custom Properties

Item	Description
Custom Property 1–10	Set the item names of custom properties. Set the custom property labels for all devices.

Screen Lock

Item	Description
Screen Lock	Specify whether or not to switch the display to the login screen when the Management Console has not been used for a specific period of time. When you enter the password on the login screen, operation resumes with the previous displayed status.
Screen Lock Timer	Specify how long the device waits before turning on [Screen Lock]automatically. Specify from the following range: • 1–1440 minute(s) The default is 30 minutes.

Dashboards

Item	Description
Use current period as Most Recent	Specify whether or not to treat the current period as the most recent. For example, the current period is treated as the period to be displayed on the dashboard even if there are two weeks left until the current period ends.

Device Display Name Format

Item	Description
Device Display Name Format	Specify the format of the device display name. The default device display name is "model name (IP address of the device)". The items to be included in the display name can be entered manually or selected from the list of variables. To display the list of variables, right-click the text box. • [Model Name] • [Address] • [Serial Number] • [IP Address] • [MAC Address] • [Host Name] • [Vendor Name] • [WIM Location] • [WIM Comment] • [PPM] • [Custom Property] 1–10 **Note** • The configured format is applied only to devices newly registered after they are configured.

Mobile Device Access

Click [Mobile Device Access] in the navigation tree to display the setting screen for each item.

Note

- For an outline of the functions available on a mobile device, see page 371 "Functions Available on a Mobile Device".

Mobile Device Settings

Item	Description
Mobile Guest Print	Specify whether or not to enable Mobile Guest Print. The default is [Disable]. **Important** • **To use Mobile Guest Print, be sure to create a user named "guestuser" with any password. For details about creating a user, see page 157 "Creating and Importing Users".**
Mobile Device Access	Specify whether or not to access the device information from mobile devices. The default is [Disabled].
Maximum Session Length	Specify the duration before a timeout of the login session from mobile devices is detected. The default is 60 minutes.
Image Upload	Specify whether or not to upload images from mobile devices. The default is [Enable].
Maximum Image Width	Specify the horizontal size of the image to be uploaded from mobile devices. The default is 800 pixels.
Maximum Image Height	Specify the vertical size of the image to be uploaded from mobile devices. The default is 600 pixels.

Note

- The maximum acceptable values are 3200 Width and 3200 Height.

Networking

Click [Network Settings] in the navigation tree to display the setting screen for each item.

Proxy Server

Item	Description
Use Proxy Server	Specify whether or not to use a proxy server. The default is [Off].
Proxy Server Address	Enter the address of the proxy server.
Proxy Server Port Number	Enter the port number of the proxy server. The default is 8080.
Use Authentication	Specify whether or not to apply user authentication on the proxy server. The default is [Off].
User Name	Enter the user name to authenticate the proxy server.
Password	Enter the password to authenticate the proxy server.
Domain Name	Enter the domain name you want to use for authentication of the proxy server.
Check Connection button	Test the connection using the proxy server.

SSL

Item	Description
Use SSL	Specify whether or not to use the SSL port.
SSL Port	Configure the SSL port.

Item	Description
Certificate	• [Disable HTTP]: Select this check box to disable HTTP. • [Create CSR] button: Click to open the dialog box to enter [Server Name], [Organization], [State or Province], [Organizational Unit], [City or Locality], and [Country Code]. • [Install Certificate] button: Select the setting for [Certificate Type] from [Intermediate CA] or [SSL]. Click the [Browse...] button to select the certificate. **Note** • For details about the procedure for enabling an SSL connection, see page 403 "Enabling SSL".
SSL Client	To trust all certificates while operating the system, select the [Trust all Certificates] check box.

Email Server Setting

Item	Description
SMTP Server Address	Enter the address of the SMTP server.
SMTP Port Number	Enter the port number of the SMTP server. The default is 25.
Sender Email Address	Enter the sender's e-mail address.
Authentication Method	Select one of the following authentication methods: • [None] • [POP Before SMTP] • [SMTP] The default is [None].

Item	Description
SMTP/SMTPS	Specify whether or not to use secure connection. • No Security The connection is not encrypted. • SMTPS(SMTP over SSL) The connection is encrypted. • SMTPS(StartTLS) The connection is initially created over plain text. If the server supports the StartTLS command, the connection is updated to an encrypted channel.
POP3 Server Address	Enter the POP3 server address.
POP3 Port Number	Enter the port number of the POP3 server. The default is 110.
Account Name	Enter the account name you want to use for authentication.
Password	Enter the password to use for authentication.
Test Mail Address	Enter the e-mail address to send a test e-mail.

System Alert Notification

Item	Description
System Alert Notification	Specify whether or not to enable system notifications.

Item	Description
Trigger	Specify whether or not to enable system notifications. • [HDD Capacity is Full] • [DB Capacity is Full] • [System Errors] • [DS Communication Error Notification]: When selecting this trigger, specify the notification interval in minutes. **Note** • To receive a notification on licensing, specify an e-mail address in [Maintenance and Support Email] below.
Input Email Address Manually	Enter the e-mail address of the destination manually. • Notify Address: Enter the e-mail address. • Language: Select the language to use in the notification e-mail.
Select Destination	Select from the destinations registered to [System] ▶ [Notification] ▶ [Destination].

Maintenance and Support Email

Item	Description
Input Email Address Manually	Enter the e-mail address to which the notification about licensing is to be sent. • [Notify Address] Enter the e-mail address. • [Language] Select a language used in notification e-mail. **Note** • Notification e-mails are sent for the following remaining days: 0, 15, 30, 60 and 90.

Item	Description
Select Destination	Select a notification destination from e-mail addresses registered in [System] ▶ [Notifications] ▶ [Destinations].

FTP/SFTP

Item	Description
Protocol	Select the FTP/SFTP protocol to use for communicating with the device from the following: • [FTP] • [SFTP] • [SFTP Priority] **Note** • Before selecting [SFTP] or [SFTP Priority], enable SFTP on the device with Web Image Monitor.
SFTP Port	Enter the port number to use when selecting [SFTP] or [SFTP Priority]. The default is 22.

System Data Management

Click [System Data Management] in the navigation tree to display the setting screen for each item.

Note

- For an outline of system data management and details about using system data management, see page 395 "Managing the System Capacity".

Data Storage Period

Item	Description
Device Eco Log	Specify the storage period of the Eco log that is retrieved from devices. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
Device Access Log	Specify the storage period of the access log that is retrieved from devices. • 1 –31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
Device Job Log	Specify the storage period of the job log that is retrieved from devices. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
Status	Specify the storage period of the status history retrieved from devices. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited

Item	Description
Counter	Specify the storage period of the counter information retrieved from devices. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
User Counter	Specify the storage period of the user counter information retrieved from devices. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
System/Tasks/Audit/Notifications Logs	Specify the storage period of the system logs. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited
Report	Specify the storage period of the original data be used for generating reports. Specify one of the following: • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • Unlimited

Note

- The default for all the items listed above is 1 year.

HDD Capacity

Item	Description
Remaining Capacity When Nearly Full	Specify the value to check for insufficient hard disk space. You can specify any value between 1 and 100 GB. The default is 2 GB.
Remaining Capacity When Full	Specify the value to check that the hard disk is full. You can specify any value between 1 and 100 GB. The default is 1 GB.

DB Capacity

Item	Description
Remaining Capacity When Nearly Full	Specify the value to check for insufficient space of the database. You can specify any value between 1 and 7 GB. The default is 2 GB. Note • This setting is for SQL Server 2008 Express.
Remaining Capacity When Full	Specify the value at which to check for insufficient space for the database. You can specify any value between 1 and 70 GB. The default is 1 GB. Note • This setting is for SQL Server 2008 Express.

Deletion Settings When Capacity is Full

Item	Description
Device Eco Log	Specify how long the device Eco log is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
Device Access Log	Specify how long the device access log is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
Device Job Log	Specify how long the device job log is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
Status	Specify how long the status history is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]

Item	Description
Counter	Specify how long the counter data is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
User Counter	Specify how long the user counter data is stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
System/Tasks/Audit/Notifications Logs	Specify how long the system logs are stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]
Report	Specify how long created reports are stored when the value of Remaining Capacity When Full is reached. • 1–31 day(s) • 1–12 month(s) • 1–5 year(s) • [Unlimited]

Repository Management

Click [Repository Management] in the navigation tree to display the list of firmware, SDK/J platforms, Device Applications, and printer driver installer packages uploaded to the Core Server. You can display the list and delete the files in the list.

When [Firmware] is the type displayed in the list, double-click an item to display the firmware information.

Note

- A file cannot be deleted if the value of [Usage Count] is 1 or more.

Device Log Management

Click [Device Log Management] in the navigation tree to display the setting screen for each item.

Note

- For an outline of the device logs and details about using the device logs, see page 114 "Managing Device Logs".

Device Log Management

Item	Description
Device Log Reception	Displays the device log reception status. Use the [Start]/[Stop] button to start and stop reception of device logs.
Log Processing Interval	Specify the interval to obtain the log. The default is 1 hour.
Log Processing Start Time	Specify the time to start the log collection. The default is 00:00.
Upload device log from Delegation Server immediately	Updates the device log database. Note • Because the Job Logs and the Device Access Logs are stored and managed in an internal database rather than on the Oracle or SQL server, these logs are not included in a effective range of the Run button.

Monitor Transferring Log Setting

Item	Description
Monitor Device Log Transmission	Specify whether or not to send a notification when there is no device log for the specified period.

Item	Description
Monitor Interval	Select the interval to notify whether the device log is available or not. The default is 1 month.
Input Email Address Manually	Enter the e-mail address of the destination manually. • Notify Address: Enter the e-mail address. • Language: Select the language to use in the notification e-mail.
Select Destination	Select from the destinations registered to [System] ▶ [Notification] ▶ [Destination].

Device Log Export

A retrieved device log can be exported as a CSV file.

Item	Description
Select Device Log Type	Select the type of the device log to be exported. • [Device Job Log] • [Device Access Log] • [Device Eco Log]

Item	Description
Select Device Job Log Data by	Specify the start date/time and end date/time of the duration to export the device job log. • [Created Date Time in Device]: The date and time the data creation on the device started becomes [Start Date] and [Start Time], and the date and time the data creation on the device ended becomes [End Date] and [End Time]. • [Collected Date Time of System]: The date and time the data collection on the device started becomes [Start Date] and [Start Time], and the date and time the data collection on the device ended becomes [End Date] and [End Time]. **Note** • Specify the current time for Start Date/Time and End Date/Time. • Export the date and time of the device job log in GMT.
Delegation Server	When exporting a device job log or device access log, select the Delegation Server as the destination for exporting the log.

Note

- You can also use the job information output tool to export a device log. For details, see page 791 "Using Device Log Export Tool".

Email Address

Click [Email Address] in the navigation tree to display the list of setting names.

General tab

You can register multiple e-mail addresses to the address list. You can use an e-mail address registered to the address list as a destination.

Item	Description
Name	Enter the name of the address list.

Item	Description
Description	Enter the description.
Address List	Enter the destination address. Note • To enter more than one address, separate each address by a comma (,).
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. Note • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

System Information and Settings

Click [System Information and Settings] in the navigation tree to display the setting screen for each item.

System Information

The system version and the number of registered devices are displayed.

Server Settings

Specify whether or not to use the advanced function related to device settings.

Item	Description
Enable SDK/J Platform installed in the devices	Specify whether to enable or disable SDK/J Platform in the devices. When this setting item is enabled, SDK/J Platform is automatically enabled in devices when Other Polling tasks, Device Application and SDK/J Platform tasks are executed.
Enable SLNX Management Extension for Configuration Templates	When this setting item is enabled, you can configure items indicated with the dagger mark (†) on the device settings template. For details about the setting items, see page 643 "List of Device Preference Setting Items".

Item	Description
Enable SLNX Management Extension for DOSS checking	When this setting item is enabled, you can obtain DOSS-related properties by executing an Other Polling task.

Note

- To ensure normal operation of the SLNX Management Extension, one of the following versions of the SDK/J Platform must be met:
  - 4.05 or above
  - 5.02 or above
  - 6.00 or above
  - 7.00 or above
  - 10.00 or above
  - 11.00 or above
  - 12.00 or above

Debug Log Settings

Configure the debug log of the Delegation Server and the Core Server. You can add or delete the category of a log and change the level.

Debug Log Download

Item	Description
[Initiate Download] button	Specify the debug log search item. Select the download destination of the log from the following types: • [SLNX Device] • [Delegation Server] • [RICOH Streamline NX PC Client]
[View Downloads] button	View logs on the client computer displaying the Management Console.

@Remote Center RC gate ID Registration

You can register RC Gate ID of RICOH @Remote Connector NX when operating RICOH @Remote Connector NX and RICOH Streamline NX at the same time. After RC gate ID is registered, RICOH @Remote Connector NX can send the device information stored in RICOH Streamline NX to the @Remote center to reduce the network load at device discovery.

Driver Distribution

Click [Driver Distribution] in the navigation tree to display the setting screen for each item.

There are two driver package distribution functions: [Basic] and [Advanced].

Note

- For an outline of driver distribution and details about using driver distribution, see page 133 "Distributing Printer Drivers".

Basic

Item	Description
Format for Printer Name	Specify the printer name when a printer is installed. The items to be included in the printer name can be manually entered or selected from the list of variables. To display the list of variables, right-click the text box.
User Accounts	Specify whether or not to specify the account for installing the driver package. When specifying an account, configure the user name, domain name, and password.

Advanced

Item	Description
Authorized Groups - [Enabled]	Specify an LDAP or Active Directory user group to allow downloading of the driver.
Supported OS	Select one of the following operating systems for the driver package: • [Windows Vista 32-bit] • [Windows Vista 64-bit] • [Windows 7 32-bit] • [Windows 7 64-bit] • [Windows 8 32-bit] • [Windows 8 64-bit] • [Windows XP] • [Windows 10 32-bit] • [Windows 10 64-bit]

Item	Description
Non-driver Packages	Specify whether or not to allow downloading of other files or files from an external link.
Format for Printer Name	Specify the printer name when a printer is installed. The items to be included in the printer name can be manually entered or selected from the list of variables. To display the list of variables, right-click the text box.
Browsing	On the driver package search screen, specify whether or not to allow viewing using a device category or group. When selecting [Enabled], specify the categories that can be viewed in [Categories to Browse].
Searching	On the driver package search screen, specify whether or not to allow device discovery.
Quick Filters	On the driver package search screen, specify whether or not to allow filtering with Quick Filters.
Maps	On the driver package search screen, specify whether or not to allow maps.
User Accounts	Specify whether or not to specify the account for installing the driver package. When specifying an account, configure the user name, domain name, and password.

Delegation Server Settings

Click [Delegation Server Settings] in the navigation tree to display the setting screen for each item.

Note

- The settings on the [Delegation Server Settings] tab are applied to all Delegation Servers. To apply individual settings to specific Delegation Servers, configure [Server Management] ▶ [Server Group] in the navigation tree.

[General] tab

Item	Description
Remaining Capacity When Nearly Full	Configure this setting to notify the administrator when the remaining space on the hard disk of the server becomes insufficient. Specify the capacity to send the notification. The default is 2 GB. The notification is not sent when [0] is specified.
Device Association	Select the category of the devices with the configuration of Device Applications, [Profile Tasks] of workflow, and [Pricing Table] enabled. • [IP Address] • [Location] The default is [IP Address].

[Authentication] tab

Item	Description
Enable Card Registration	Specify whether or not to register cards.
Registration Limit per User	Specify the maximum number of cards that can be registered to each user. The default is three.

Item	Description
Card Login Method	Specify the card login method. • [Enter Password from Operation Panel] User login is performed with a user name and password. You cannot use a secondary PIN at the same time. • [Do not Enter Password (Proxy User)] Use a card ID or user ID to search for an external authentication server and log in. • [Do not Enter Password (User Saved Password)] Use a password or user ID saved in the system to perform authentication on an external authentication server and log in. If a password is not registered, using a secondary PIN results in an error. • [Enter PIN from Operation Panel] The user logs in with a PIN. The default is [Enter Password from Operation Panel].
Access to Authentication Server	When this check box is not checked, the system identifies the user with card details against Authentication servers. If you check this check box, the system identifies user based on related information stored in the Core server database.

Item	Description
PIN	Specify the PIN code setting to use when logging in. • [Disable User PIN] • [User PIN Only] The default is [Disable User PIN]. • [User PIN Pattern]: Specify the pattern of the PIN code. The character type of the generated PIN varies depending on the entered text. Enter one of the following character types for the number of digits of the PIN: a: Lowercase letters (a-z) A: Lowercase and uppercase letters (a-z, A-Z) N: Numbers (0-9) m: Numbers and lowercase letters (0-9, a-z) M: Numbers and lowercase and uppercase letters (0-9, a-z, A-Z) • [Email Options]: Specify whether or not to send a notification e-mail when a new user PIN is generated. • [Language]: Select the language to use in the notification e-mail. • [Subject]: Enter the subject of the notification e-mail. • [Body]: Enter the body text of the notification email.
Secondary PIN	Specify the [Minimum Digits] and [Maximum Digits] settings for [Secondary PIN].
Threshold	The account can be locked after the specified number of login attempts has failed. The default is 3 times. When [0] is specified, the account is not locked if the user fails to login.

Item	Description
Lockout Duration	Specify the period to wait before resetting the login failure counter when a login attempt has failed. The default is 60 minutes.

[Capture] tab

Item	Description
Number of Retries	Specify the number of retries to attempt when a job has failed. The default is 3 times.
Retry Interval	Specify the interval between retries when a job has failed. The default is 180 seconds.
Configuration Validation Server	Specify the server to use for testing the workflow. The default is [Core Server].
Start service automatically when server starts	Specify whether or not to start the workflow transmission service immediately after starting Delegation Server.
Delivery Schedule	Configure the transmission schedule of the workflow job.

Item	Description
Save Fax job(s)	• Specify whether or not to back up the original job data that is obtained from the source, such as the fax, monitor folder, or mobile device. • [Job Storage Period]: Configure the storage period. The default is 0 days. • [Auto Delete Time]: Specify the time to perform auto delete. The default is 1 hour. • The backed-up fax jobs are stored in the following folder: (Data folder on the Delegation Server)\data\scan\ds\fax-jobs
OCR Mode	Select the operational mode of the OCR engine. • [Balance]: In this mode, the character recognition process is performed while a balance between the recognition rate and speed is maintained. • [Recognize Rate Priority]: In this mode, priority is given to the recognition rate. • [Speed Priority]: In this mode, priority is given to speed. The default is [Balance].
Kerberos Option	Specify the authentication method for each connector type from the drop-down menu. • [Use Kerberos authentication as a priority] • [Use only the ticket received on Kerberos authentication] • [Use only NTLM] The default is [Use Kerberos authentication as a priority].

Item	Description
Auto Delete Error Jobs	Specify whether or not to delete the error jobs automatically. The defaults are OFF for both [Fax] and [Scan] jobs.
Error Job Storage Period	Specify the storage period of the error jobs. The default is 1 hour, 0 minutes.
Job Storage Capacity Alert	Specify the remaining amount of available space on the hard disk drive to send a warning to the administrator. The default is 100 MB.

[Print] tab

Item	Description
Job Storage Period	Specify the storage period of the jobs in print queue. When the specified period elapses, the jobs are automatically deleted.
Scheduled Processing Settings	Specify whether the jobs for which the period specified in Job Storage Period has elapsed are deleted at a specific time or interval. • Time: Specify the time to delete the jobs in HH:MM format. • Interval: Specify the interval to delete the jobs.
Include selected day(s)	Specify the day of the week to include in Job Storage Period. For example, if you want to store a job for seven days but weekends excluded, select Monday to Friday.
Delete Printed Jobs	Specify whether or not to delete jobs after printing.

[Server Notifications] tab

Item	Description
System Error	Specify the language and destination to be used for notification when a system error occurs.

Item	Description
Commercial Certificate Expiration	Specify the language and destination to be used for notification when an expiration or renewal of the certificate occurs.
HDD Capacity	Specify the language and destination to be used for notification when the available hard disk space falls below the capacity set in [HDD Capacity] ▶ [Remaining Capacity When Nearly Full].

[Security] tab

Item	Description
Ethernet Card Reader Release Code	Enter the release code for the Ethernet card reader. The entered release code is masked with asterisks. Click [Display Release Code] to display the release code.

User Management and Accounting Settings

Click [User Management and Accounting Settings] in the navigation tree to display the setting screen for each item.

Item	Description
Enable Local Authentication	Specify whether or not to enable local user authentication.
Enable New User Auto-creation at Login	Specify whether or not to register a user automatically to the system when the user logs in and has not registered to the system yet.
Enable User Information Auto-update at Login	Specify whether or not to update the user automatically when the user attributes on the LDAP server and the database do not match.

Item	Description
Attributes to be Updated	You can synchronize the user attributes. Select the items to synchronize from the following: • [Display Name] • [Email] • [Fax] • [Home Folder] • [User Group] • [Department] • [Cost Center]
Enable Language Registration per User	Specify whether or not a general user can register a display language to the operation screen of the device.
Hide PIN in UI and Encrypt in Database	Specify whether or not to encrypt the user PINs in database. When it is enabled, the options in the [User Setting] tab in [Users] in [User Management] cannot be changed either.
Hide Card Number in UI and Encrypt in Database	Specify whether or not to encrypt the card numbers in database. When it is enabled, [Card Number] in [Card] in [User Management] is masked with asterisks.
Hide Job Name Column from Job Queue	Specify whether or not to hide the document name and job name columns in the delivery job and print job lists. When it is enabled, the document names and job owners' names on the print spooler of Delegation Server are also masked with asterisks.
Encrypt Job Name in DS-Print database	Specify whether or not to encrypt the job name of the secure print jobs with AES128. When it is enabled, only the job owners and administrators can display the job name. **Note** • When [Encrypt Job Name in DS-Print database] is enabled, no Job Name filter is available in job queue.

Item	Description
Don't Record Job Name in Accounting Transactions	Specify whether or not to record the job name in accounting transaction. When it is enabled, the job name does not appear in reports.
Hide User Name Column from Job Queue	Specify whether or not to hide the user name column in the delivery job and print job lists.
Don't Record User Name in Accounting Transactions	Specify whether or not to record user names in accounting transactions. The slnxuser_id field in slnx_job table is left blank (Null) when a user name is not recorded. **Note** • [Target Users/Groups/Departments] Specify the users, groups, or departments whose user names are not recorded in accounting transactions.
Enforce Color Page Limit	Specify whether or not to allow the user to continue printing in color when the maximum number of color prints has been exceeded. • [Alert Threshold]: To send a notification, specify the remaining number of pages that can be printed in color. The default is 5.
Enforce Account Limit	Specify whether or not to allow the user to continue printing when the maximum numbers of both monochrome and color prints have been exceeded. • [Alert Threshold]: To send a notification, specify the remaining number of pages that can be printed either in black-and-white or color. The default is 10.
Enable Cost Center	Specify whether or not to use the Cost Center function.

Item	Description
Enable Cost Center Association	Specify whether or not to apply the cost center associated with a logged-in user. When this item is disabled, the user can select the cost center after logging in to a device. **Note** • Even when a login user selects a cost center, the default cost center of the guest user is applied to guest user jobs, host printing, and reception fax printing. In addition, no cost center is specified in direct printing.
Zero Count Stop	When Zero Count Stop is enabled, the Streamline NX Embedded Applications stop a copy or print job at the page the user's point runs out. When Zero Count Stop is disabled, a print job is canceled if the user's remaining balance calculated by the Streamline NX Embedded Applications is not enough to complete printing. A copy job is not interrupted once it is started even if the user's point runs out. When Zero Count Stop is disabled, a copy job is not interrupted once it is started even if the user's point runs out. **Note** • Zero Count Stop is a setting effective for a device not equipped with a finisher. To use Zero Count Stop when using a device with a finisher, enable [Zero Count Stop With Finisher]. • A copy job is not interrupted even if the color page point runs out. • The user with no color page point remaining can log in to a device but can only use black and white copying and fax functions. • The user with no point remaining can log in to a device but cannot use the copy and fax functions.

Item	Description
Zero Count Stop With Finisher	This setting is available when the [Zero Count Stop] check box is selected. Specify whether or not to enable Zero Count Stop when printing is performed on a device with a finisher.
Apply Pricing By	Specify whether the pricing tables are configured by Devices and Device Groups or Users and Departments. • Devices and Device Groups Pricing tables are configured by devices and device groups. • Users and Departments Pricing tables are configured by users and departments. Note • For details about pricing tables, see page 572 "Pricing Table".

Limitations for Zero Count Stop

- If a copy job is interrupted by Zero Count Stop while copying is performed on a device with a finisher, a piece of paper of the job may remain in the finisher.
- Zero Count Stop is disabled on devices for which SNMPv2 is disabled.
- Direct print jobs are not restricted, but expend the user's point.
- Print jobs without user name is not restricted.
- When a user logs in to multiple devices at the same time, Zero Count Stop is disabled.
- Even if a print job fails because of an error (e.g. a paper jam), the printed part of the job expends the user's point.
- When using Zero Count Stop, a print job may be interrupted even if the user's remaining point is sufficient for the job, or it may not stop even if the user's point runs out during printing.
- If the user logs out from the device while printing or copying, the job is interrupted. In this case, the printed part of the job expends user's point.
- When Zero Count Stop is disabled, the user's balance may be negative after all print jobs are complete. It is because the print jobs are allowed based on the estimated balance of the user's point.

- If enough attributes cannot be obtained from a print job, it is treated as a job with the following attributes:
  - Black and white
  - One-sided
  - Number of faces/2 pieces of paper
- All copied pages are counted as one-sided when the cost is calculated because enough attributes cannot be obtained regarding the sides for each page. So, always select [1 Sided] in [1 Sided/2 Sided] for copy jobs on the [Cost Per Page] tab in [Pricing Table].

Security

Configure the security-related settings such as user roles or creation of authentication profiles.

Custom Properties

Click [Custom Properties] in the navigation tree to display the list of custom properties.

In [Custom Property Name], enter an item name to be used as a custom property.

Authentication Profiles

Click [Authentication Profile] in the navigation tree to display the profile list.

Note

- For an outline of authentication profiles and details about using authentication profiles, see page 153 "Managing the Authentication Settings".

[General] tab

Item	Description
Type	Select from [LDAP] or [Kerberos] for the type of profile to create.
Name	Enter the profile name.

[LDAP] tab

Configure the information of the LDAP server.

Item	Description
Server Name	Enter the server name.

Item	Description
Port	Enter the port number. The default is 389. **Note** • The port number is automatically changed from 389 to 636 when the SSL setting is enabled.
SSL	Specify whether to enable or disable SSL.
Active Directory	Specify whether or not to enable Active Directory. When Active Directory is enabled, enter the following items: • [Domain] • [Alt UPN Suffix]
Base DN	Enter the start point for searching for an account name. Starting from the base DN, the search is performed toward the end of the branches. Example: ou=member,dc=mycompany,dc=com
Search Scope	Specify the range of the search from the base DN. • [Single level]: The search is performed in the hierarchy that is a level below the base DN. • [Subtree]: The search is performed in the base DN and all levels in the hierarchy under the Base DN.
Search Condition	Enter the search condition. The following string is set as the default value: (&(objectClass=organizationalPerson)(sAMAccountName=^))
Prefix	Enter the prefix of the LDAP search filter.
Suffix	Enter the suffix of the LDAP search filter.
Proxy User Name	Enter the name of the proxy user.

Item	Description
Proxy User Password	Click the [Change Password] button, and then enter the password of the proxy user.
Enable DNS Round Robin	Specify whether or not to enable the DNS round robin function. **Note** • The DNS round robin function assigns multiple IP addresses to a single domain name and disperses the connection workload among multiple servers.
Timeout	Specify the LDAP operation timeout. The default is 5 seconds.
[Test Connection] button	Check whether or not a connection can be established to the LDAP server.
Login User Name	Enter the attribute to identify the login user name. Enter the following string as the default value: sAMAccountName
Display Name	Enter the display name. Enter the following string as the default value: displayName
Email Address	Enter the attribute of the e-mail address of the user. Enter the following string as the default value: mail
Fax Destination	Enter the attribute of the fax destination. Enter the following string as the default value: facsimileTelephoneNumber
Group	Enter the attribute of the group name. Enter the following string as the default value: memberOf
Home Folder	Enter the attribute of the user home folder. Enter the following string as the default value: homeDirectory

Item	Description
Card ID	Enter the attribute of the card ID.
Department	Enter the attribute of the department.
Cost Center	Enter the attribute of the cost center.
Group Look Up Mode	Select the method to identify the group member. • [Simple Search]: Search is performed based on the identifier (DN). • [Full Search]: Search is performed based on the user login group attribute. The default is [Full Search].
Group Name Attribute	Enter the attribute to obtain the group name. Specify this setting when [Full Search] is selected in [Group Look Up Mode].
Group Search Condition	Enter the attribute to search for a group. Specify this setting when [Full Search] is selected in [Group Look Up Mode].

[Kerberos] tab

Configure the information of the Kerberos server.

Item	Description
KDC	Enter the Kerberos Key Distribution Center (KDC) server. Example: mycompany.com
Realm	Enter the name of the Kerberos realm. Example: MYCOMPANY.COM
Trust Relationship Domain button	Specify the domain server address and domain name used to establish a trust relationship.
Server Name	Enter the server name.

Item	Description
Port	Enter the port number. The default is 389. **Note** • The port number is automatically changed from 389 to 636 when the SSL setting is enabled.
SSL	Specify whether to enable or disable SSL.
Domain	Enter the domain name of the Kerberos server.
Alt UPN Suffix	Enter the alternate UPN suffix. Input example: mycompany.com
Base DN	Enter the start point for searching for an account name. Starting from the base DN, the search is performed toward the end of the branches. Example: ou=member,dc=mycompany,dc=com
Search Scope	Specify the range of the search from the base DN. • [Subtree]: The search is performed in the base DN and all levels in the hierarchy under the Base DN. • [Single level]: The search is performed in the hierarchy that is a level below the base DN.

Item	Description
Search Condition	Enter the search condition. Enter the following string as the default value: (&(objectClass=organizationalPerson)(|(userPrincipalName=^)(userPrincipalName=^alt))) In the following example, the search targets are entries with an objectClass attribute that includes "organizationalPerson" and an sAMAccountName attribute that includes an account name entered when login to RICOH Streamline NX is performed. Example: (&(objectClass=organizationalPerson)(sAMAccountName=^))
Proxy User Name	Enter the name of the proxy user.
Proxy User Password	Click the [Change Password] button, and then enter the password of the proxy user.
Enable DNS Round Robin	Specify whether or not to enable the DNS round robin function. **Note** • The DNS round robin function assigns multiple IP addresses to a single domain name and disperses the connection workload among multiple servers.
Timeout	Specify the operation timeout of Kerberos. The default is 5 seconds.
[Test Connection] button	Check whether or not a connection can be established to the Kerberos server.
Login User Name	Enter the attribute to identify the login user name. Enter the following string as the default value: sAMAccountName
Display Name	Enter the display name. Enter the following string as the default value: displayName

Item	Description
Email Address	Enter the attribute of the e-mail address of the user. Enter the following string as the default value: mail
Fax Destination	Enter the attribute of the fax destination. Enter the following string as the default value: facsimileTelephoneNumber
Group	Enter the attribute of the group name. Enter the following string as the default value: memberOf
Home Folder	Enter the attribute of the user home folder. Enter the following string as the default value: homeDirectory
Card ID	Enter the attribute of the card ID.
Department	Enter the attribute of the department.
Cost Center	Enter the attribute of the cost center.
Group Look Up Mode	Select the method to identify the group member. • [Simple Search]: Search is performed based on the identifier (DN). • [Full Search]: Search is performed based on the user login group attribute. The default is [Full Search].
Group Name Attribute	Enter the attribute to obtain the group name. Specify this setting when selecting [Full Search] in [Group Look Up Mode].
Group Search Condition	Enter the attribute to search for a group. Specify this setting when selecting [Full Search] in [Group Look Up Mode].

User Roles

Click [User Roles] in the navigation tree to display the list of roles.

Important

- **To configure the User Role settings, your user access role must have SecurityWrite access permissions such as System Roles of Security Admin or Full Admin.**

Note

- For an outline of the roles and details about using the roles, see page 160 "Managing User Roles and Privileges".

[Role] tab

Item	Description
Name	Enter the name of the role.
Description	Enter the description of the role.
Login expiry time	Specify the duration before a timeout of the login session is detected.
LDAP group name	Enter the LDAP group name.
Role is system	This displays whether or not the role is a default system role.

[Restrictions] tab

Specify whether or not to grant read/write permissions to a device group for device categories with configured group restrictions.

Item	Description
Security Context (Read)	Specify the device groups that allow viewing of roles.
Security Context (Write)	Specify the device groups that allow updating of roles from among the groups that allow viewing of roles.

Note

- For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Privileges] tab

Select the privileges to be granted to the user.

Item	Description
AddressBookRead	• Display Address Book contents
AuditRead	• Display software settings audit logs
SysConfigRead	• Display the system settings information
DeviceBasicRead	• Display all information related to devices other than tasks, templates and notifications • Accessing devices from the mobile app
DeviceAdvancedRead	• Display all information related to devices such as tasks, templates and notifications • Display structure change notification policies
SecurityRead	• View the role, user, LDAP/Kerberos profile of a user
AddressBookWrite	• Create/update/delete Address Book contents
AuditWrite	• Delete software settings audit logs
SysConfigWrite	• Update system settings (other than the role, user, LDAP/Kerberos profile of a user)
DeviceBasicWrite	• Create/update/delete discovery profiles, polling tasks and related tasks • Create/update/delete device groups • Change device access accounts and custom properties • Update e-mail address lists
DeviceAdvancedWrite	• Create/update/delete device settings, SDK/J Platform and Device Applications • Add/update/delete structure change notification policies • Update device drivers
SecurityWrite	• Create/update/delete the role, use, LDAP/Kerberos profile of a user
LogDelete	• Delete logs

Item	Description
ReportRead	• Display reports
ReportWrite	• Create/update/delete/configure schedules for reports
@RemoteAdmin	• Read all @Remote setting items and update partial @Remote setting items
@RemoteCE	• Read and update all @Remote setting items
DriverDownload	• Download device drivers and driver packages
TemporaryCardChange	• Change the use day of a temporary card
WorkflowOperationRead	• Display General Settings of Workflows, Shared Connector Settings, Design of Workflows, Device Applications, Workflow Profile, and Connectors
PrintOperationRead	• Display Print Rules
AccountingOperationRead	• Display Pricing Table • Display Accounting Tasks
SlnxUserOperationRead	• Display Groups, Departments, Cost Centers, Users, Permissions, and Synchronization Tasks of User Management • Display User Management and Accounting Settings of System Settings
CardOperationRead	• Display Card Information
EmbeddedOperationRead	• Display Streamline NX Embedded Applications Information (related to authentication function)
WorkflowOperationWrite	• Create/update/delete General Settings of Workflows, Shared Connector Settings, Design of Workflows, Device Applications, Workflow Profile, and Connectors
PrintOperationWrite	• Create/update/delete Print Rules

Item	Description
AccountingOperationWrite	• Create/update/delete Pricing Table • Create/update/delete Accounting Tasks
SlnxUserOperationWrite	• Create/update/delete Groups, Departments, Cost Centers, Users, Permissions, and Synchronization Tasks of User Management • Update User Management and Accounting Settings of System Settings
CardOperationWrite	• Create/update/delete Card Information
EmbeddedOperationWrite	• Create/update/delete Streamline NX Embedded Applications Information (related to authentication function)
DisplayMessageRead	• Obtain device display messages
DisplayMessageWrite	• Update device display messages
QuotaOperationWrite	• Enable/disable Enforce Color Page Limit, Enforce Account Limit, Adjust Color Page Limit, Adjust Accounting Limit, Adjust Color Page Balance, and Adjust Account Balance

Note

- DeviceAdvancedRead and DeviceAdvancedWrite are required to upload drivers. DeviceAdvancedWrite is required to manage assignments of driver packages.
- The DriverDownload permissions that enable downloading of drivers and packages are automatically allocated to users who can access the download URL.

[Users] tab

You can assign a specific role to a user who does not belong to an LDAP group.

User Accounts

Click [User Accounts] in the navigation tree to display the Local User Account setting screen. Local User Account is the account to be used only for operating the Management Console.

Note

- For an outline of user accounts and details about using user accounts, see page 160 "Managing User Roles and Privileges".

Item	Description
User name	Enter the user name. The user name cannot be edited after the account is saved. Ensure you type the correct user name.
Password	Click the [Change] button, and then enter a new password.
Full name	Enter the full name of the user.
Role	Select the user role. You can select more than one role.
Disabled	Specify whether or not to invalidate the user account. You can display the date on which the account expired.

Local Password Policy

Click [Local Password Policy] in the navigation tree to display the setting screen for each item.

Configure the rules and a valid period of time related to the local user password.

Note

- For an outline of the local password policy and details about using the local password policy, see page 155 "Specifying the Extended Security Functions".

Item	Description
Maximum Password Age	Configure the maximum password age. When the password expires, a dialog box for configuring a new password is displayed.
Account Lockout Threshold	Specify whether or not to lock the account when an incorrect password is entered several times.
Minimum Password Length	Configure the minimum password length.
Requires Uppercase	Creates a rule that the password must contain at least one uppercase character.
Requires Numeric	Creates a rule that the password must contain at least one number.
Requires Special Case	Creates a rule that the password must contain at least one special character (@, #, $, %, ^, &, +, =).

Notifications

Configure the notification policies and the recipients of the notification. For details, see page 94 "Notifying the Device Status by E-mail".

Policies

Click [Policy] in the navigation tree to display the list of policies.

Note

- For an outline of notifications and details about sending notifications, see page 94 "Notifying the Device Status by E-mail".

Create Notification Policy

Item	Description
Policy Name	Enter the policy name.
Type	Select the policy type. • [Polling] Configure discovery notification settings for when to send notifications and how they are sent. • [Discovery] Configure polling notification settings for when to send notifications and how they are sent.
Destination	Specify the notification destinations.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

The [Policies] section consists of the following five tabs: [General], [Triggers], [Conditions], [Message], and [Monitored Devices].

[General] tab

Item	Description
Policy Name	Enter the policy name.
Type	The type of the policy that is selected in the [Notification Policy] dialog box is displayed. • [Polling] • [Discovery]
Destination	Specify the notification destinations.
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

[Triggers] tab

Specify the criteria for sending [Notification].

Item	Description
Advanced Criteria	When the [Advanced Criteria] check box is selected, the simple criteria screen changes to the advanced criteria screen. By using variables on the Advanced Criteria screen, you can configure more detailed notification criteria. You can only configure either Advanced Criteria or Simple Criteria.

Simple Criteria

Item	Description
Errors	Select from the following the type of errors you want to specify as Simple Criteria: • [Select All] • [No Toner/Ink] • [Paper Misfeed] • [Call Service] • [Cover Open] • [Device Access Violation] • [No Paper] • [No Response] • [Original Misfeed: ADF] • [Fax Transmission Error] • [Error]
Warnings	Select from the following the type of warnings you want to specify as Simple Criteria: • [Select All] • [Offline] • [Toner/Ink Almost Empty] • [Alert] • [Replace/Supply] • [Maintenance] • [Busy] • [Almost Out of Paper] • [Energy Saver Mode] • [Warming Up...]

Advanced Criteria

Variable	Conditions	Value
Device Status	not equal to, equal to	Select the items that can be specified in [Error] or [Warning] of Simple Criteria as values.
Combined device status (previous)	not equal to, equal to	
Copier Status	not equal to, equal to	
Copier Status (previous)	not equal to, equal to	
Printer Status	not equal to, equal to	
Printer Status (previous)	not equal to, equal to	
Fax Status	not equal to, equal to	
Fax Status (previous)	not equal to, equal to	
Scanner Status	not equal to, equal to	
Scanner Status (previous)	not equal to, equal to	
System Status	not equal to, equal to	
System Status (previous)	not equal to, equal to	
Device Counters Total	not equal to, equal to, greater than, less than	Integer
Device Counters Total (previous)	not equal to, equal to, greater than, less than	Integer
Input Tray Status	not equal to, equal to, greater than, less than	0-100
Output Tray Status	not equal to, equal to	Ready, Output Bin is Almost Full, Output Bin is Full, Other errors
Printer Version	not equal to, equal to, greater than, less than	Version (example: 1.0.6)
System Version	not equal to, equal to, greater than, less than	Version (example: 1.0.6)

Variable	Conditions	Value
Toner Level	not equal to, equal to, greater than, less than	0-100
Toner Level (Black)	not equal to, equal to, greater than, less than	0-100
Toner Level (Cyan)	not equal to, equal to, greater than, less than	0-100
Toner Level (Magenta)	not equal to, equal to, greater than, less than	0-100
Toner Level (Red)	not equal to, equal to, greater than, less than	0-100
Toner Level (Yellow)	not equal to, equal to, greater than, less than	0-100
Discovered Devices Count	not equal to, equal to, greater than, less than	Integer

[Conditions] tab

Specify additional criteria for sending [Notification].

Item	Description
Block if not Settled	Disables repeated notifications in the specified period. Specify the interval using the following units: [Time Interval]: [day(s)], [hour(s)], [minute(s)], [month(s)], [second(s)], [year(s)]
Notify only if criteria is repeated within specified time interval	A notification is sent only when the specified status occurs for the specified number of times during the specified period. [Repeat Count]: Specify the number of repetitions. [Time Interval]: [day(s)], [hour(s)], [minute(s)], [month(s)], [second(s)], [year(s)]

Item	Description
Notify only if criteria is sustained for	A notification is sent only when the specified status continues for the specified duration. [Time Interval]: [day(s)], [hour(s)], [minute(s)], [month(s)], [second(s)], [year(s)]
Resend Notification	A notification is sent again after the specified time has passed. [Time Interval]: [day(s)], [hour(s)], [minute(s)], [month(s)], [second(s)], [year(s)]
Notify on cleared conditions	A notification is sent again when the notified status is resolved.

[Message] tab

Configure the notification message.

Item	Description
Language	Select the language to use in the notification e-mail.
Subject	Enter the subject of the notification e-mail. Enter the variable using the right-click menu.
Body	Enter the body of the notification e-mail. Enter the variable using the right-click menu.

[Monitored Devices] tab

Specify the device groups for applying [Notification Policy].

Destinations

Click [Destination] in the navigation tree to display the list of destinations.

Note

- For an outline of notifications and details about sending notifications, see page 94 "Notifying the Device Status by E-mail".

Item	Description
Destination Name	Enter the destination name.

Item	Description
Notification Type	Select the transmission method. • [Email] • [Execute an application] The default is [Email].
Email Address	Enter the destination e-mail address. Click the [Address List] button to select a destination registered to [System] ▶ [Server Settings] ▶ [Email Address]. **Note** • To enter more than one address, separate each address by a comma (,).
Language	Select the language of the destination.
Application file	Enter the path to the application when selecting [Execute an application] in [Notification Type].
Security Group Context	[Security Group Context] is displayed when Group Restrictions is enabled. Select the device group to which to allow access. **Note** • For details about Group Restrictions, see page 167 "Configuring Group Restrictions".

Configuration Alerts

Click [Configuration Alert] in the navigation tree to display the list of policies.

Note

- For an outline of notifications and details about sending notifications, see page 94 "Notifying the Device Status by E-mail".

[General] tab

Specify the basic settings such as the destination e-mail address and the language to be used in the notification.

Item	Description
Policy Name	Enter the destination name.

Item	Description
Notify Address	Select the method to specify the notification destination, and enter the destination e-mail address. • [Input Email Address Manually]: Enter the e-mail address manually. • [Select Destination]: Select the destination from the drop-down list. Select a destination registered to [System] ▶ [Notification] ▶ [Destination].
Language	When selecting [Input Email Address Manually], select the language of the destination.

[Attributes] tab

This tab displays the list of attributes for the tasks that are subject of notification.

Select the check box in the [Enabled] column for the function for sending notifications.

[Monitored Devices] tab

Specify the device or device group subject to [Configuration Alert].

Logs

You can check the logs of the executed system operations and operation results.

Task Log

Click [Task Log] in the navigation tree to display the log list.

Note

- For an outline of the task log and details about using the task log, see page 411 "Managing Tasks".

Notification Log

Click [Notification Log] in the navigation tree to display the log list.

Note

- For an outline of the notification log and details about using the notification log, see page 416 "Viewing System Operation Logs".

Audit Log

Click [Audit Log] in the navigation tree to display the log list.

Note

- For an outline of the notification log and details about using the notification log, see page 416 "Viewing System Operation Logs".

System Log

Click [System Log] in the navigation tree to display the log list.

Note

- For an outline of the system log and details about using the system log, see page 416 "Viewing System Operation Logs".

Report Logs

Click [Report Logs] in the navigation tree to display the log list.

Note

- For an outline of the report log and details about using the report log, see page 416 "Viewing System Operation Logs".

Authentication Log

Click [Authentication Log] in the navigation tree to display the log list.

Note

- For an outline of the authentication log and details about using the authentication log, see page 416 "Viewing System Operation Logs".

Scheduled Tasks

Click [Scheduled Tasks] in the navigation tree to display the list of tasks registered to the system.

Note

- For an outline of scheduled tasks and details about using scheduled tasks, see page 411 "Managing Tasks".

Pricing Table

[Pricing Table] contains [Built-in Functions] and [Workflows].

Built-in Functions

Click [Built-in Functions] in the navigation tree to display the list of pricing tables.

Note

- For an outline of pricing tables and details about using pricing tables, see page 131 "Managing the Pricing Tables".

[General] tab

Item	Description
Pricing Table Name	Enter the name of Pricing Table.
Description	Enter the description.

[Target Devices/Groups]/[Target Users/Departments] tab

When [Apply Pricing By] is set to [Devices and Device Groups] in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings], the [Target Devices/Groups] tab is displayed. When it is set to [Users and Departments], the [Target Users/Departments] tab is displayed.

Display or select [Target Devices/Groups]/[Target Users/Departments]. You can add or delete [Target Devices/Groups]/[Target Users/Departments]. To select all devices or users, select the [All Devices] or [All Users] check box at the top right of the displayed dialog box.

[Cost Per Page] tab

You can specify the rate for each page based on criteria such as job type, paper size, color mode, or duplex.

Item	Description
Job Type	Select the job type. • Copy • Print • Scan • Fax Send • Fax Reception

Item	Description
Paper Size	Select the paper size. • A2, A3, A4, A5, A6, B3, B4, B5, B6, HLT, Ledger, Legal, Letter, Other
Color Mode	Select the job color mode. • Black and White • Single Color • Two-color • Full Color
1 Sided/2 Sided	Specify whether the job is for one-sided or two-sided printing. • 1 Sided • 2 Sided
Rate	Specify the cost per page. You can specify it in units of 0.00001.

Workflow

Click [Workflows] in the navigation tree to display the list of pricing tables.

Note

- For an outline of pricing tables and details about using pricing tables, see page 131 "Managing the Pricing Tables".

[General] tab

Item	Description
Pricing Table Name	Enter the name of the Pricing Table.
Description	Enter the description.

[Target Workflows] tab

Select the target workflow from the workflow list.

[Cost Per Page] tab

Item	Description
Base Rate	You can specify it in units of 0.00001. Counted once each time the workflow is executed.
Page Rate	You can specify it in units of 0.00001. Counted according to the number of pages processed in the workflow.

External Print Systems

In the [External Print Systems] category, you can configure information about external print systems so that the users can view and release print jobs stored in external systems from devices with Streamline NX Embedded Applications embedded or smart deices with RICOH Streamline NX mobile app installed.

[LRS] tab

Item	Description
URL	Enter the server address of LRS beginning with http or https.
Input Queue Type	Specify the print queue on the external print system pulled by RICOH Streamline NX. • Output Queue: Queue for the jobs which are not retained. • Retained: Queue for the retained jobs. • Both: Queue for jobs which are retained and not retained.
Output Queue Mapping	Specify the information passed to the external print system to identify devices. • IP: IP Address of the device • Host Name: Host name of the device • FQDN: FQDN of the device

[SEAL] tab

Item	Description
URL	Enter the server address of SEAL beginning with http or https.

Item	Description
Input Queue Type	Specify the print queue on the external print system pulled by RICOH Streamline NX. • Output Queue: Queue for the jobs which are not retained. • Retained: Queue for the retained jobs. • Both: Queue for jobs which are retained and not retained.
Output Queue Mapping	Specify the information passed to the external print system to identify devices. • IP: IP Address of the device • Host Name: Host name of the device • FQDN: FQDN of the device

[InfoPrint Manager] tab

Item	Description
URL	Enter the server address of InfoPrint Manager beginning with http or https.
Input Queue Type	Specify the print queue on the external print system pulled by RICOH Streamline NX. • Output Queue: Queue for the jobs which are not retained. • Retained: Queue for the retained jobs. • Both: Queue for jobs which are retained and not retained.
Output Queue Mapping	Specify the information passed to the external print system to identify devices. • IP: IP Address of the device • Host Name: Host name of the device • FQDN: FQDN of the device

[TotalFlow] tab

Item	Description
URL	Enter the server address of TotalFlow to redirect print jobs to external systems using print rules. If not specified, the print rule to redirect to external systems is not applied.

Note

- For details about linkage with external print systems, see the manuals for external print systems.

Dashboards

Click [Dashboards] in the navigation tree to display the dashboards list.

About dashboard functions, see Reporting and Dashboards Guide for details.

Workflow

This section describes the functions of items displayed in [Workflows] in the navigation tree.

General

Configure the metadata database connection, replacement table, and zone OCR form, and also register PDF stamps. The settings apply to all Metadata Replacement, Metadata Converter, Zone OCR, and PDF Stamper connectors that are used in the workflows.

Metadata Database Connection

Click [Metadata Database Connection] in the navigation tree to display the connection list.

Note

- For an outline of the metadata database connection and details about using the metadata database connection, see page 333 "Configuring the Metadata Database Connection".

[General] tab

Item	Description
Connection Name	Enter the connection name.
Description	Enter the description of the replacement table.
Database Server Address	Enter the host name or IP address of the server with the connected database.
Database Instance Name	The instance with the connected database can contain up to 127 characters.
Database Port Number	Specify the port number used when connecting to the database.
Database Name	Enter the connected database name.
User Name	Enter the user name with access privileges to the database.
Password	Enter the password of the user with access privileges to the database.
[Test] button	Test the connection to the database.

[Workflows] tab

Displays the workflows that configure the database connection.

Replacement Table

Click [Replacement Table] in the navigation tree to display the list of replacement tables.

Note

- For an outline of the replacement table and how to use a replacement table, see page 334 "Configuring a Replacement Table".

[General] tab

Item	Description
Replacement Table Name	Enter the name of the replacement table.
Description	Enter the description of the replacement table.
Input Metadata	Select the input metadata from the drop-down list or enter the item name (ID). The target metadata element in the document is compared with the value of [Comparison Target String] in the replacement table. **Note** • An error occurs if the specified metadata element is not included in the delivery document.
Output Metadata	Select the output metadata from the drop-down list or enter the item name (ID). The input metadata element is replaced with the output metadata value according to the Comparison Target String rules of the replacement table. The output metadata target can be input manually. **Note** • An error occurs if the specified metadata element is not included in the delivery document.

Item	Description
Enable Auto Entry	If the input value does not match a value in the replacement table, specify whether to add that input value to the replacement table. When [Enable Auto Entry] is selected and a value that is not in the table is entered, that value is added to the table. This input value becomes the comparison string of that item, and the output value becomes blank. **Note** • Auto entry is valid only when the [Job Processing Location] setting for a workflow is set to [On Server]. When [Location] is set to [On Device], auto entry processing is canceled.
Default Output	Enter the default output value. When the input value does not exist in the replacement table, this output value is used. You can enter up to 1000 characters.
Export File Character Encoding	Select the encode type to be used when exporting the replacement table from the following: • UTF-8 • Windows Shift-JIS • JIS • Latin-1

[Comparison Entry] tab

Item	Description
Comparison Target String	Enter the string used for comparison of the input value. You cannot enter the same comparison string. You can enter up to 1000 characters.
Comparison Result String	Enter the string to be used as the output value when the input value matches the value of Comparison Target String.
Using Regex	Select this to use a regular expression in the comparison string. You can enter up to 1000 characters.
Enable Comparison	Select this to use the item to compare with the input value.

Zone OCR Form

Click [Zone OCR Form] in the navigation tree to display the list of forms.

Note

- For an outline of the zone OCR form and how to use a zone OCR form, see page 338 "Configuring the Zone OCR Form".

[General] tab

Item	Description
Form Name	Enter the form name. Do not use the following characters: / : ? * " < > | The name is not case-sensitive.
Description	Enter the description for the form.
OCR Language	Select the language for performing OCR from the drop-down list. • English, German, French, Italian, Spanish, Dutch, Danish, Portuguese, Norwegian, Russian, Simplified Chinese, Traditional Chinese, Japanese
Zone OCR Form Template Image	Select the template image to be used to configure the anchor and OCR zone. Click [Browse...] to select the image file, and then click [Upload].

[Form Design] tab

Use the uploaded image file to configure the anchor and OCR zone.

PDF Stamper

Click [PDF Stamper] in the navigation tree to display the list of PDF stamps.

Note

- For an outline of PDF stamps and how to use PDF stamps, see page 345 "Registering a PDF Stamp".

[General] tab

Item	Description
Stamp Name	Enter a stamp name.

Item	Description
Stamp Type	Select from the following types of stamps to embed in the PDF. • Bates Stamp • Image Stamp • Text Watermark • Image Watermark
Description	Enter a description of the stamp.

[Stamp] tab

The setting items vary depending on the type of stamp selected in the [General] tab.

When [Bates Stamp] is selected

Item	Description
Prefix	Enter the string to be added before the counter numerals. Example input: Prefix Display example: Prefix0001
Leading Spaces	Specify the number of spaces to be entered between the prefix and the numerals. Note • The width of the space may vary depending on the specified [Font Size].
Suffix	Enter the string to be added after the counter numerals. Example input: Suffix Display example: 0001Suffix
Trailing Spaces	Specify the number of spaces to be entered between the suffix and the numerals. Note • The width of the space may vary depending on the specified [Font Size].

Item	Description
Current Counter	The current value of the counter is displayed. Select the [Update Counter] check box to update the counter. **Note** • This item is displayed only when editing a registered stamp that is selected from the stamp list. • Specify a value within the range between [Counter Start] and [Counter End] in [Current Counter].
Counter Start	Specify the starting value of the counter.
Counter End	Specify the ending value of the counter.
Update Counter	Select the [Update Counter] check box to update the counter. **Note** • This item is displayed only when editing a registered stamp that is selected from the stamp list.
Pad Zero	When the [Pad Zero] check box is selected, "0" is added to fill in the digits for the counter numerals that do not reach the maximum digits specified in [Counter End]. Example: When 4 is specified in [Counter End] and the counter value is 5, the value is displayed as "0005".

When [Image Stamp] or [Image Watermark] is selected

Item	Description
Stamp Image	Specify the image to be embedded as a watermark in a PDF. Click [Browse...] to select the image file, and then click [Upload].

Item	Description
Image Scale Percentage	Specify the scaling factor of the image to be embedded as a watermark in a PDF.

When [Text Watermark] is selected

Item	Description
Watermark Text	Select a string from the drop-down list, or enter the string to be embedded as the PDF watermark. • Copy • Confidential • Confidential Copy • Sample

[Font] tab

This item is displayed when Bates Stamp or Text Watermark is selected on the [General] tab.

Item	Description
Font Family	Select the font family from the drop-down list. • Courier • Helvetica • Times Roman
Font Style	Select the font style from the drop-down list. • Standard • Bold • Italic • Bold Italic
Font Size	Specify the font size.

Item	Description
Font Color	Select the color of the font from the drop-down list. • Black • White • Red • Green • Blue • Cyan • Magenta • Yellow • Orange • Pink • Gray • Light Gray • Dark Gray
Background Color (Bates Stamp only)	Select the color of the background from the drop-down list. • Black • White • Red • Green • Blue • Cyan • Magenta • Yellow • Orange • Pink • Gray • Light Gray • Dark Gray

Item	Description
Border Color (Bates Stamp only)	Select the color of the border line from the drop-down list. • Black • White • Red • Green • Blue • Cyan • Magenta • Yellow • Orange • Pink • Gray • Light Gray • Dark Gray
Border Width (Bates Stamp only)	Specify the border width.

[Position] tab

Item	Description
Vertical (Bates Stamp and Image Stamp only)	Specify the vertical position of the image to be embedded. • Top • Middle • Bottom **Note** • When [Middle] is selected, [Top/Bottom Margin] cannot be specified.

Item	Description
Horizontal (Bates Stamp and Image Stamp only)	Specify the horizontal position of the image to be embedded. • Left • Center • Right **Note** • When [Center] is selected, [Left/Right Margin] cannot be specified.
Top/Bottom Margin (Bates Stamp and Image Stamp only)	Specify the top and bottom margins. Select [mm] or [inch] for the margin unit.
Left/Right Margin (Bates Stamp and Image Stamp only)	Specify the left and right margins. Select [mm] or [inch] for the margin unit.
Rotation (Degree)	Specify the angle of rotation width.
Page Range (multi-page)	Select the range of pages to embed the stamp from the drop-down list. • All Pages • First Page • Last Page • Even Pages • Odd Pages • Specified Pages
Page Numbers (multi-page)	When [Specified Pages] is selected in [Page Range], specify the pages to embed the stamp. **Example** • When specifying separate pages: 1,5,8 • When specifying ranges of the pages: 1-3,5-9 • When specifying separate pages and ranges of pages at the same time: 2-5,9,13-20 • When specifying from the first page to a specific page: -7 • When specifying from a specific page to the last page: 2-

Item	Description
Single-page Settings	Specify whether or not to embed the stamp in a single-page document. • Do not Stamp • Stamp All
Allow User Modifications	Specify whether or not to allow modifying of the specified numbers in [Page Range] and [Page Numbers] on the operation screen of the device.

[Preview] tab

Item	Description
Page Size	Select the preview page size from the drop-down list.
Page Orientation	Select the page orientation from [Portrait] or [Landscape].
[Show Preview] button	Downloads the preview PDF using a five-page sample document. The document is only a sample and not the actual document on which the stamp can be embedded. Note • The preview is displayed on a white background. When white is specified as the color of the watermark text, the text will be invisible in the preview.

Shared Connector Settings

Click [Shared Connector Settings] in the navigation tree to display the list of preset connectors.

Note

- For an outline of preset connectors and details about using preset connectors, see page 317 "Creating a Shared Connector".

[General] tab

Item	Description
Connector Name	Enter a name for the shared connector.
Description	Enter a description for the shared connector.

Item	Description
Connector Category	Displays the category of the shared connector. • Process Select this item when creating a shared connector of a process connector. • Destination Select this item when creating a shared connector of a destination connector.
Connector Type	Displays the type of the connector to be configured as a shared connector.
Job Processing Location	Displays whether the job is processed on a server or device.

[Settings] tab

Configure the properties of the connector that is selected in [Connector Type].

For details about the setting items, see page 691 "Setting Items in the Destination Connector Properties" or page 747 "Setting Items in the Process Connector Properties".

[Preset] tab

Configure the settings, layout, and display method according to the type of shared connector that is selected in [Connector Type].

For details about configuring the settings, see page 294 "Customizing the Settings on the Operation Screen of the Device".

[Workflow] tab

Displays the workflow that uses the selected shared connector.

Workflow Design

Click [Workflow Design] in the navigation tree to display the list of workflows.

When you select an item registered to the list and click (Edit), the setting tabs are displayed.

Note

- For an outline of workflows and details about using workflows, see the following:
  - page 219 "Overview of the Delivery Function"
  - page 227 "Creating a Workflow"

[General] tab

Item	Description
Workflow Name	Enter a workflow name.
Description	Enter a description for the shared connector.
Job Processing Location	Specify whether the document delivery process is performed on the server or device. This cannot be changed.
Configuration Validation Server	Specify the server to be used to test the connection to the external server. If this setting is not specified, a connection test cannot be performed while the workflow is configured.
Display Name	Select a language, and enter the title text to be displayed on the operation screen of the device.
Screen Icon	Click [Browse], select an icon from the icon library, and click [OK]. To upload an image in PNG format, click [Upload] on the icon library screen. You can upload an image with a size of 192 × 192 pixels, 128 × 128 pixels, 64 × 64 pixels, or 32 × 32 pixels. The size of an icon to be used depends on the size of the operation screen of the device. To ensure user-friendly operations, upload an image whose size is the same as the size of the operation screen of the device. The preview image is displayed when the screen icon is specified.

[Delivery Flow] tab

Place a destination connector and process connector to configure the flow of the processing and delivery of the scanned document. For details about each item on the Delivery Workflow tab and how to use the Delivery Workflow tab, see page 230 "Understanding the [Delivery Flow] tab layout".

For details about configuring the connector properties, see page 691 "Setting Items in the Destination Connector Properties" or page 747 "Setting Items in the Process Connector Properties".

[Destination] tab

Customize the scan settings, scan sizes, setting values, and configuration items displayed on the operation screen of the devices of the destination connectors. You can also specify the default values, whether to show or hide items, and how they are displayed on the operation screen.

For the setting items, see page 667 "[Destination] Tab".

[Process] tab

Customize the scan settings, scan sizes, and setting values of the destination connectors. You can also specify the default values, whether to show or hide items, and how they are displayed on the operation screen.

For the setting items, see page 678 "[Process] Tab".

[Metadata] tab

Specify the items to be displayed on the [Metadata] screen on the operation screen of the device. For details about each item in the [Metadata] tab screen, see page 308 "Using the [Metadata] Tab".

The properties of each input element on the [Metadata] tab screen are as follows:

Item	Description

 (Label)	Adds a preset text such as a message or description to the metadata screen.
	• Display Name
	  • Language
	  • Name

Item	Description
(InputText)	Adds a metadata element in string format. The following attributes can be specified: • Enable ([Yes] or [No]) • Required Entry Item ([Yes] or [No]) • Display Name • Metadata Tag Name • Max. Characters • Min. Characters • Password ([Yes] or [No]) • Regex for Validation **Note** • To make the entry of an item mandatory, select [Yes] in [Required Entry Item]. • When [Yes] is selected in [Required Entry Item], 0 cannot be specified in Max. Characters and Min. Characters. • An error occurs if a string that does not match [Regex for Validation] is entered. For details about regular expressions, see page 358 "Regular Expressions".
(NumberStepper)	Adds a metadata element in integral number format. The following attributes can be specified: • Enable ([Yes] or [No]) • Display Name • Metadata Tag Name • Max. Value • Min. Value **Note** • When 0 is in between the [Max. Value] and [Min. Value] and this field is left blank, the value of this field becomes 0. • When the [Max. Value] and [Min. Value] are either positive or negative and 0 is not in between those values, the value of the maximum or minimum that is closer to 0 is specified as the value of this field.

Item	Description
 (DateField)	Adds a metadata element in date format. The following attributes can be specified: • Enable ([Yes] or [No]) • Required Entry Item ([Yes] or [No]) • Display Name • Metadata Tag Name • Start Date • End Date • Use date of operation as default value ([Yes] or [No]) **Note** • The entered date is used as the default date on the operation screen of the device. • To specify the date of operation on the device as the default value, select [Yes] in [Use date of operation as default value].
 (Dropdown ListBox)	Adds a drop-down list that has the values in various sources or the values manually entered as the selection items. The following attributes can be specified: • Enable ([Yes] or [No]) • Required Entry Item ([Yes] or [No]) • Editable ([Yes] or [No]) • Display Name (max. 128 characters) • Metadata Tag Name (max. 128 characters) • Query Type ([Manual Entry], [CSV Search], [SQL Search])

Item	Description

(Dropdown ListBox)	**Note**
	• When [Yes] is selected in [Editable], the user can enter the value manually in addition to selecting the value from the drop-down list.
	• When [CSV Search] or [SQL Search] is selected in [Query Type], the values obtained from a CSV or SQL file are displayed from the drop-down list. When [Manual Entry] is selected, enter the value manually. For details about configuring the list, see page 310 "Configuring a drop-down list".
	• When selecting [CSV Search] or [SQL Search] in [Query Type], you cannot specify the default value on the Management Console because the value is obtained by the device.
	• The values are not displayed from the drop-down list on the operation screen of the device in the following cases:
	  • When the number of the items in the result exceeds 100 when CSV or SQL search is executed. To display the selection items, press [Search] and narrow down the result.
	  • When more than 50 values are entered manually (Manual Entry)
	  • When the SQL query that refers to other metadata is specified, but the metadata of the reference target is empty.
	• The result of the [Search] function cannot be confirmed in the Management Console.

(Checkbox)	Adds a metadata element in form of a check box. The following attributes can be specified: • Enable ([Yes] or [No]) • Display Name • Metadata Tag Name

Note

- For an outline of metadata and description of operations, see page 308 "Configuring Items in Metadata".

[Notifications] tab

Item	Description
Enable Notification	Specify whether or not to notify the deliver result.
Triggers	Specify when a notification is sent. • Failed jobs only • Successful jobs only • Both failed and successful jobs
Destination	Enter the destination e-mail address of the notification. To enter more than one e-mail address, separate each address by a comma (,). Up to 512 characters can be entered. To select an e-mail address that is registered in RICOH Streamline NX system, click [Copy from System Address Book]. Select the e-mail address, and then click [OK].
Language	Select the language to be used for notifications from the drop-down list.
Email Server Setting	Configure the e-mail server for the destination e-mail address of the notification. This can only be configured for workflows where [On Device] is selected in [Location]. In workflows where [On Server] is selected in [Location], the network settings in RICOH Streamline NX are used. Specify the following items: • SMTP Server Address • SMTP Port Number • Authentication Algorithm ([None], [POP before SMTP], [SMTP]) When [POP before SMTP] is selected in [Authentication Algorithm], specify the following items: • POP3 Server Address • POP3 Port Number • Account Name • Password

Item	Description
Add/Delete Metadata Field	Select the check box of the metadata to be included in the notification. If the metadata that you want to include is not in the list, click [Add] to add the desired metadata.

Note

- For an outline of notifications and description of operations, see page 315 "Configuring the Notification Function".

[Other Settings] tab

Item	Description
Default Document Name	Select a language, and specify the default document name. The metadata element "Document Name" is specified, and this is used for the name of the file delivered by Send to Email and Send to Folder. This is also displayed in the document name field on the operation screen of the device. The document name is specified as a metadata element as shown below. **Note** • When [Add Scanned Time to Document Name] is specified on the workflow profile, the scan date and time are added to the document name. For details, see page 321 "Configuring a workflow profile associated with a device". • You can also add a document name using a connector-specific function. For details, see the description of the each connectors. • See page 255 "File and Folder Naming Conventions".
Enable Editing	Specify whether or not to enable the user to edit the document name. • Yes The user can specify the document name on the operation screen of the device when scanning. • No The default document name is used, and the user cannot edit the document name even when scanning.

Item	Description
Select Items to be Displayed on the Device's Configurations Screen (Standard Operation Panel only)	Specify the items to be displayed in [Scan Settings] on the operation screen of the device. To add an item, select the item in [Item Settings List] and click ▶. To remove an item, select the item in [Selected Item(s) List] and click ◀.
Scan Preview	Specify whether or not to display a preview of the scanned document before delivery. This function is not available on devices with a screen size of 4.3 inches. • Preview always Displays a preview of the scanned document before delivery. You cannot change the preview setting on the operation screen of the device. • Preview on by default Displays a preview of the scanned document before delivery unless [Preview] is set to [Off]. • Preview off by default Does not display a preview of the scanned document before delivery unless [Preview] is set to [On].

Note

- For a description of operations of the [Other Settings], see page 316 "Configuring Other Settings".

10

Device Applications

Click [Device Applications] in the navigation tree to display the list of Device Applications.

Note

- For an outline of the Device Applications and details about using Device Applications, see page 319 "Configuring Device Applications".

[General] tab

Item	Description
Application Name	Enter the Device Applications name.
Description	Enter a description of the Device Applications.
Application Type	Select the type of the application from the drop-down list. • [Copier] • [Scanner] • [Printer] • [Fax] • [Document Server] • [Secure Print] **Note** • The applications that can be selected vary depending on the model of the device being used.
Display Name	Enter the title text to be displayed on the operation screen of the device. The name of the application is displayed when [Display Name] is not specified.
Screen Icon	Click [Browse], select an icon from the icon library, and click [OK]. To upload an image in PNG format, click [Upload] on the icon library screen. You can upload an image with a size of 192 × 192 pixels, 128 × 128 pixels, 64 × 64 pixels, or 32 × 32 pixels. The size of an icon to be used depends on the size of the operation screen of the device. To ensure user-friendly operations, upload an image whose size is the same as the size of the operation screen of the device. The preview image is displayed when the screen icon is specified.

[Profile] tab

Displays the workflow profile that uses the Device Applications being configured.

Workflow Profile

Profile Configuration

Click [Profile Configuration] in the navigation tree to display the profile list.

The displayed tab and setting items differ depending on the input source that is selected while a new workflow profile is being created.

Note

- For an outline of the profile configuration and details about using the profile configuration, see page 321 "Configuring a Workflow Profile".
- You can configure only one workflow profile that is associated with a mobile device on any one system. Therefore, if a workflow profile that is associated with a mobile device is created, [Mobile] is not displayed in [Input Source] when a new workflow profile is created.

When [General] tab - Input Source is set to [MFP]

Item	Description
Profile Name	Enter a profile name.
Description	Enter a description of the profile.
Input Source	Displays the selected input source. This cannot be changed.
Add Scanned Time to Document Name	Specify whether or not to add the scan date and time to the document name. • Yes The scan date and time are added to the document name. Example: “Expense Report_yyyymmddhhmmss” (yyyy: year, mm: month, dd: day, hh: hours, mm: minutes, ss: seconds) • No The scan date and time are not added to the document name.

Item	Description
Capture Pause Timeout	Specify how long to wait for the next original when batch scanning or scanning using the exposure glass is performed. Specify whether to start sending automatically after the wait time elapses or to cancel scanning. When the preview function is enabled, the preview is displayed for the specified timeout time. If [Send] is not pressed while the preview is displayed, scanning is canceled or the scanned data is automatically sent according to the setting. **Note** • [Capture Pause Timeout] is enabled only on devices with the Smart Operation Panel.
Display Job Log on Device Display Panel	Specify the job log to display on the operation screen of the device. • Display Job Log(s) for All Workflows • Display Job Log(s) by Workflow
Job Log Security Mode	Specify whether or not to mask the sensitive information in the job log. • On The document name and user name are masked by asterisks (*). • Off All the information in the properties of the job log is displayed.
Max. No. of Groups (Standard Operation Panel only)	Specify the maximum number of groups (1 to 11, default is 5) to be displayed in a single screen on the device operation screen. **Note** • The horizontal scroll buttons are displayed when there are too many group tabs to be displayed on the screen. • When more than one group tab is displayed on a single screen, the names of the groups that cannot fit in the screen are shortened and shown only in part.

Item	Description
Date Format Settings	Specify the format of the date to be displayed on the operation panel of the device. (YYYY: year, MM: month, DD: day) • YYYY/MM/DD • MM/DD/YYYY • DD/MM/YYYY
Display Name	Select a language, and specify the title text to be displayed on the application bar of the operation panel of the device.
Number of columns on screen	Specify the number of icons displayed in a row on the workflow selection screen.
Screen Icon	Click [Browse], select an icon from the icon library, and click [OK]. To upload an image in PNG format, click [Upload] on the icon library screen. You can upload an image with a size of 64 × 64 pixels, 48 × 48 pixels, or 32 × 32 pixels. The size of an icon to be used depends on the size of the operation screen of the device. To ensure user-friendly operations, upload an image whose size is the same as the size of the operation screen of the device. The preview image is displayed when the screen icon is specified.

When [General] tab - Input Source is set to [Mobile]

Item	Description
Profile Name	Enter a profile name.
Description	Enter a description of the profile.
Input Source	Displays the selected input source. This cannot be changed.
Display Name	Select a language, and enter the display name to be displayed on the screen of the mobile device.

When [General] tab - Input Source is set to [Hot Folder]

Item	Description
Profile Name	Enter a profile name.
Description	Enter a description of the profile.
Input Source	Displays the selected input source. This cannot be changed.
Configuration Validation Server	Select from the drop-down list the server to perform monitoring, store errors, and verify the folder for storing files.

When [Workflow] tab - Input Source is set to [MFP]

Item	Description
Capture Workflows	Create a new group, and then add the workflow and the Device Applications. You can check and configure the following properties of the added groups, workflows and Device Applications: **Group** • Group Name • Show ([Yes] or [No]) **Workflow** • Workflow Name (for display only) • Description (for display only) • Button Height ([Single], [Double], [Triple], [Quadruple]) **Note** • For the workflows used on devices with 4.3-inch screen, set [Button Height] to [Double], [Triple], or [Quadruple]. If it is set to [Single], the workflow button will not be displayed on the device's operation panel. **Device Applications** • Device Applications Name (for display only) • Description (for display only) • Button Height ([Single], [Double], [Triple], [Quadruple])

Item	Description
Fax Workflow	Configure the delivery function of the received fax. • Use Fax Specify whether or not to use the delivery function on the received fax. • Fax Workflow Select the workflow to be used for delivering the received fax from the drop-down list. Also, select the check boxes of all fax reception ports to be monitored. • G3-1 Port • G3-2 Port • G3-3 Port • Internal Port • IP Port

When [Workflow] tab - Input Source is set to [Mobile]

Create a new group, and then add the workflow and mobile apps.

You can check and configure the following properties of the added groups, workflows and mobile apps:

Group

- Group Name
- Show ([Yes] or [No])

Workflow

- Workflow Name (for display only)
- Description (for display only)
- Button Height ([Single], [Double], [Triple], [Quadruple])

Mobile Applications

- Application Name (for display only)
- Description (for display only)
- Button Height ([Single], [Double], [Triple], [Quadruple])

When [Workflow] tab - Input Source is set to [Hot Folder]

When you select an item registered to the list and click (Edit), the setting screen is displayed.

Item	Description
General Features	
Monitor Folder	Specify the path of the Monitor Folder to be monitored. Use "\" and "/" to delimit folder names. Use a UNC path (\\ComputerName\SharedFolder) to specify a shared folder. Also enter the [User Name] and [Password] when a shared folder is selected. Press [Test] to test the connection from Configuration Validation Server to the Monitor Folder. Performs authentication tests using the entered user name and password. **Note** • For the conditions that can be specified for Monitor Folder, see page 323 "Configuring a workflow profile associated with a monitor folder".
Workflow Name	Select the workflow to be used for delivering the scanned file from the drop-down list. **Note** • You can only select a one-touch workflow for Monitor Folder. • You cannot select a workflow that requires authentication.

Item	Description
Error Save Folder	Enter that path of the folder to save the file that caused the error when an import error occurred. Use "\" and "/" to delimit folder names. Use a UNC path (\\ComputerName\SharedFolder) to specify a shared folder. Also enter the [User Name] and [Password] when a shared folder is selected. Select the [Same as Monitor Folder] check box when the same [User Name] and [Password] as the monitored folder are used to access Error Save Folder. Press [Test] to test the connection from Configuration Validation Server to Error Save Folder. **Note** • For the conditions that can be specified for Error Save Folder, see page 323 "Configuring a workflow profile associated with a monitor folder".

Item	Description
Store Import File	Specify whether or not to save the imported file on the local hard disk drive after its delivery is completed. To save the file, select the [Store Import File] check box and enter the path to [Store Folder]. Use "\" and "/" to delimit folder names. Use a UNC path (\\ComputerName\SharedFolder) to specify a shared folder. Also enter the [User Name] and [Password] when a shared folder is selected. Select the [Same as Monitor Folder] check box when the same [User name] and [Password] as the monitored folder are used to access Store Folder. Press [Test] to test the connection from Configuration Validation Server to Store Folder. The imported files are deleted and not stored when the [Store Import File] check box is cleared. **Note** • For the conditions that can be specified for Store Folder, see page 323 "Configuring a workflow profile associated with a monitor folder".
Enable import of multiple files	Select this check box to import and process more than one file at one time as a single job. Specify the file name in [Control File Name]. **Note** • For details about the function for importing multiple files, see page 323 "Configuring a workflow profile associated with a monitor folder".
Metadata Settings	
Map Metadata	Select this check box to use the metadata mapping function. When the metadata mapping function is used, the index fields in the index file and the metadata fields that are used in the workflow of RICOH Streamline NX are associated with each other.

Item	Description
Index File Type	Select the file format of the index file from the following: • XML • CSV
Index File Name	Use regular expressions to specify the file name of the index file that contains the index field to be used for metadata mapping.
Default Document Name	• Enter a document name manually for the file to be created, or select a name from the metadata elements that already exist. • Select from Existing Metadata Select the metadata element from the drop-down list. • Manual Entry Enter the tag name of the metadata element. • When the metadata mapping function is disabled, the time stamp (local time of the Delegation Server) at the time of execution is set as the Default Document Name.
Schema File Path	Specify the XML Schema path to the index file to be used for mapping the metadata elements. Click [Browse...] to select the XML Schema file, and then click [Upload].
Assign Metadata Elements Table	Displays the list of the association of document information settings that are registered. Use the following procedure to add an association setting: 1. Click (Add). 2. On the [Metadata Assignment] screen, select the [Source] index field. 3. Select the Basic Metadata from the drop-down list, or enter Customized Metadata Tag. 4. Click [OK].

Only when [Preview] tab - Input Source is set to [MFP]

The display on the device operation screen can be confirmed. The appearances on the Standard Operation Panel and on Smart Operation Panel are separately displayed.

Only when [Associated Devices/Groups] tab - Input Source is set to [MFP]

The devices or device groups that are associated with the currently selected workflow profile are displayed.

Only When [Associated Servers] tab-Input Source is [Hot Folder]

The servers that are associated with the currently selected workflow profile are displayed.

Profile Tasks

Click [Profile Tasks] in the navigation tree to display the task list.

Note

- For an outline of profile tasks and details about using profile tasks, see page 329 "Configuring a Profile Task".

[General] tab

Item	Description
Profile Name	Displays the name of the selected profile.
Input Source	Displays the input source of the selected profile.

When [Target Devices/Groups] tab - Input Source is set to [MFP]

The devices or device groups that are to be synchronized with the currently selected task are displayed. Also the devices or groups to synchronize can be added or deleted.

When [Target Server(s)] tab - Input Source is set to [Hot Folder]

The servers that are to be synchronized with the selected task are displayed. Also the servers to synchronize can be added or deleted.

[Schedule] tab

Item	Description
Enable Schedule	Specify whether or not to enable the schedule to execute the task.
Start Date	Specify the date to start the synchronization. Click the calendar icon to select the date on a calendar.
Start Time	Specify the time to start the synchronization.

[Notifications] tab

Item	Description
Enable Notification	Specify whether or not to notify by e-mail when a task is executed.
Input Recipient Manually	Select this item when you want to enter the destination e-mail address manually. Enter the destination e-mail address of the notification.
Select Destination	Select this item when you want to select the destination from the list of e-mail addresses that are registered in RICOH Streamline NX. From the drop-down list, select the destination e-mail address of the notification.

Connector

Click [Connectors] in the navigation tree to display the list of shared connectors.

Note

- For details about operating this function, see page 226 "Confirming the Usable Connectors".

[Process] tab

Item	Description
Connector Type	Displays the type of the connector.
Description	Displays the description of the connector.
Location	Displays the location (server or device) where the workflow job including the connector is processed.
Version	Displays the version of the connector.

[Destination] tab

Item	Description
Connector Type	Displays the type of the connector.
Description	Displays the description of the connector.
Location	Displays the location (server or device) where the workflow job including the connector is processed.

Item	Description
Version	Displays the version of the connector.

Print Rules

Click [Print Rules] in the navigation tree to display the list of print rules.

Note

- For an outline of print rules and details about using print rules, see page 199 "Configuring Print Rules".

[General] tab

Item	Description
Name	Enter the name of the print rule.
Description	Enter the description of the print rule.
Enable	Specify whether to enable or disable the print rule that is currently configured.
[Test] button	Tests the print rule that is currently configured.

[Conditions] tab

Specify whether or not to perform an action set for a rule applied to a sent job.

For the conditions, see page 201 "List of conditions".

[Action] tab

Specify the type of action that is applied when a condition is met.

For the actions, see page 204 "List of actions".

[Target Devices/Groups] tab

Specify the device(s) or device group(s) to which to apply the print rules.

[Target Users/Groups] tab

Specify the user(s) or user group(s) to which to apply the print rules.

User Management

This section describes the functions of items displayed in [User Management] in the navigation tree.

Groups

Click [Groups] in the navigation tree to display the list of groups.

There are two types of groups as follows:

- Local Group: This includes the local group that is available by default and the groups that are locally created.
- External Group: This includes the groups that are imported together with the external user information.

Note

- For the functional outlines or operations of groups, see page 172 "Managing User Information".
- The groups pre-registered in the system cannot be deleted, or the names of the groups cannot be changed.
- [Default Local Group] cannot be deleted or renamed.

[General] tab

- For the local group

Item	Description
Group Name	Enter the local group name.
Description	Enter the description of the local group.

- For the external group

Item	Description
Authentication Profile	Displays the authentication profile that was used when the selected external group was imported.
Group Name	Displays the name of the external group.
Description	Enter the description of the external group.

[Users] tab

Add a local or external user to a local group.

[Permissions] tab

Item	Description
Permission Name	Displays the list of permissions specified in [User Management] ▶ [Permissions] in the drop-down list. Select the permission to be granted to the group.
Built-in Functions	Displays the functions that can be used with the selected permission.
Workflows	Displays the workflows that can be used with the selected permission.

Departments

Click [Departments] in the navigation tree to display the list of departments.

Departments can be associated with [Users], [Cost Centers], or [Permissions].

There are two types of departments as follows:

- Local Department: This includes the local department that can be created or edited in the Management Console.
- Department on External Authentication Server: This includes departments that can be imported from an external authentication server. This type of groups cannot be edited in the Management Console.

Note

- For the functional outlines or operations of departments, see page 172 "Managing User Information".
- Departments can be added or deleted in the local database. Departments cannot be added or deleted in a location other than the local database.

[General] tab

Item	Description
Department Name	Enter the department name.
Description	Enter the description of the department.
Parent Department	Select the department in the upper hierarchy.

[Users] tab

Add or delete the user to be associated with the department.

[Cost Centers] tab

Edit the list of [Cost Center] to be associated with the department.

[Permissions] tab

Item	Description
Permission Name	Displays the list of permissions specified in [User Management] ▶ [Permissions] in the drop-down list. Select the permission to be granted to the group.
Built-in Functions	Displays the functions that can be used with the selected permission.
Workflows	Displays the workflows that can be used with the selected permission.

Cost Centers

Click [Cost Centers] in the navigation tree to display the list of cost centers.

Cost centers can be associated with [Users].

There are two types of Cost Centers as follows:

- Local Cost Center: This includes the local cost center that can be created or edited in the Management Console.
- Cost Center on External Authentication Server: This includes cost centers that can be imported from an external authentication server. This type of groups cannot be edited in the Management Console.

Note

- For the functional outlines or operations of cost centers, see page 172 "Managing User Information".

[General] tab

Item	Description
Cost Center Name	Enter the name of the Cost Center.
Description	Enter the description of the Cost Center.

Item	Description
Parent Cost Center	Select the cost center in the upper hierarchy.

[Users] tab

Add or delete a user to be associated with [Cost Center].

Users

Click the [Users] tab in the navigation tree to display the list of users.

There are two types of users as follows:

- Local User: This user is created in the local database by the administrator. Click (Add) on the toolbar to add a new local user.
- External User: This user is registered to the LDAP server. To add a new external user, click on the toolbar, and then specify an authentication profile to search for the user name.

When adding a new user, you can configure the [User Setting], [Groups], [Alias], [Delegation], [Cards], and [Permission] tabs under the user list.

Note

- For the functional outlines or operations of users, see page 172 "Managing User Information".

[User Setting] tab

- For local users

Item	Description
User Name	Enter the user name.
Password	Click the [Change Password] button, and then enter the password of local users.
Display Name	Enter the display name.
Email	Enter the e-mail address of the user.
Fax	Enter the fax number.
User Home Folder	Enter the home folder of the user.

Item	Description
User PIN	Configure the PIN code of the user. • [Change User PIN] button: Creates a new PIN code. The character type and number of digits of the generated User PIN follows the rules specified in [System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [PIN Pattern]. • [Display User PIN] button: Displays the PIN code. • [Locked]: This check box is selected and the PIN code is locked when login fails after an incorrect or invalid PIN code is entered for a certain number of times. Clear the check box to unlock the PIN code. **Note** • [User PIN] appears when [User PIN] is set to [PIN Only] on the [System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [Authentication] tab in the navigation tree.
Secondary PIN	Enter [Secondary PIN]. • [Change PIN] button: Creates a new PIN code. **Note** • [Secondary PIN] appears when [Card Login Method] is set to [Enter PIN from Operation Panel] on the [System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [Authentication] tab in the navigation tree.
Department	Enter the department name.
Default Cost Center	Displays the Cost Center to be assigned to the user when the user logs in to the device.

Item	Description
Custom Property 1-10	Enter the custom property. Note • [Custom Property 1–10] appears when a custom property is created from [System] ▶ [Server Settings] ▶ [Display] in the navigation tree.
Enforce Color Page Limit	Specify whether or not to allow the user to continue printing or making copies in color when the maximum number of color prints or color copies has been exceeded. The default is specified in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings] when a user is newly created.
Enforce Account Limit	Specify whether or not to allow the user to continue using the device function when the specified limit has been exceeded. The default is specified in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings] when a new user is created.
Default Color Page Limit	Specify the default to limit the number of color prints and color copies that can be made.
Color Page Balance	Displays the balance of color prints and color copies.
Default Accounting Limit	Specify the default to limit the number of monochrome and color prints that can be made.
Account Balance	Displays the balance required to use the device function.

Item	Description
[Set/Add] button	Specify the balance of Color Print and Color Copy and the balance for using device functions. You can also specify the limit value of each balance. Click the button on the toolbar to set/add the balance of prints. • : Adds/sets the balance of color prints and color copies. • : Adds/sets the balance required to use the device function.

- For external users

Important

- **The grayed-out items cannot be configured.**

Item	Description
User Name	Displays the user name.
Display Name	Displays the display name.
User Email Address	Displays the e-mail address of the user.
User Home Folder	Displays the home folder of the user.
Fax Number	Displays the fax number.

Item	Description
User PIN	Enter the PIN code of the user. • [Change User PIN] button: Creates a new PIN code. • [Display User PIN] button: Displays the PIN code. • [Locked]: This check box is selected and the PIN code is locked when login fails after an incorrect or invalid PIN code is entered for a certain number of times. Clear the check box to unlock the PIN code. **Note** • A PIN code is issued to an existing LDAP user for which the Core Server does not have the PIN code when the LDAP user is imported after the PIN code is enabled on [System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [Authentication] tab.
Secondary PIN	Enter [Secondary PIN]. • [Change PIN] button: Creates a new PIN code. **Note** • [Secondary PIN] appears when [Card Login Method] is set to [Enter PIN from Operation Panel] on the [System] ▶ [Server Settings] ▶ [Delegation Server Settings] ▶ [Authentication] tab in the navigation tree.
Department	Displays the department name.
Default Cost Center	Displays Cost Center.
Custom Property 1-10	Enter the custom property. **Note** • [Custom Property 1–10] appears when a custom property is created from [System] ▶ [Server Settings] ▶ [Display] in the navigation tree.

Item	Description
LDAP Synchronization	Specify whether or not to synchronize the external LDAP users with the local database.
Enforce Color Page Limit	Specify whether or not to allow the user to continue printing in color when the maximum number of color prints has been exceeded. The default is the value specified in [System] ▶ [Server Settings] ▶ [User Management] ▶ [Accounting Settings].
Enforce Account Limit	Specify whether or not to allow the user to continue printing when the maximum numbers of both monochrome and color prints have been exceeded. The default is specified in [System] ▶ [Server Settings] ▶ [User Management and Accounting Settings] when the user is newly created.
Default Color Page Limit	Specify the default to limit the number of color prints and color copies that can be made.
Color Page Balance	Displays the balance of color prints and color copies.
Default Accounting Limit	Specify the default to limit the usage of the MFP or printer.
Account Balance	Displays the balance to use the MFP or printer.
[Set/Add] button	Specify the balance of Color Print and Color Copy and the balance for using device functions. You can also specify the limit value of each balance. Perform the same operation by clicking the button on the toolbar. Click the button on the toolbar to set/add the balance of prints. • : Adds/sets the balance of color prints and color copies. • : Adds/sets the balance required to use the device function.

[Groups] tab

Use this tab to add a local user to a local group.

[Alias] tab

Register the alias name to be used when printing.

You can perform authentication using an alias name instead of the user name when the alias name is registered.

[Delegation] tab

Register the candidates for the delegate users who can be selected when performing Dynamic Delegation Print.

For details about Dynamic Delegation Print, see page 186 "Features of Secure Printing Functions".

[Cards] tab

An existing card can be assigned to a user, or a new card can be issued to a user.

For details about the purposes of cards, see page 155 "Authentication Methods".

[Permissions] tab

Item	Description
Name	Displays the list of permissions specified in [User Management] ▶ [Permissions] in the drop-down list. Select the permission to be granted to the group. **Note** • To grant both permissions assigned to the user's department and group, select [Inherited Permission]. For example, if permissions for copying in color are given the user's department, the user can make color copies while copying in color is not allowed for the user's group.
Built-in Functions	Displays the functions that can be used with the selected permission.
Workflows	Displays the workflows that can be used with the selected permission.

Permissions

Click [Permissions] in the navigation tree to display the list of permissions.

Permissions can be associated with [Departments], [Groups], or [Users].

Note

- For the functional outlines or operations of permissions, see page 172 "Managing User Information".

[Permission Settings] tab

Item	Description
Permission Name	Enter the permission name.
Permission Description	Enter the description of the permission.

Built-in Functions	Select the device functions to allow usage.
	• Copier:
	  • Full Color Auto Selection
	  • Full Color
	  • Two-color
	  • Single Color
	  • Black & White
	• Other Functions:
	  • Document Server
	  • Fax
	  • Scanner

Workflows	Select the workflow to allow usage. • Allow all workflows Allow usage of all workflows. • Workflows The workflow to allow usage can be selected from the drop-down list.

[Departments] tab

Add or delete a department to be associated with the permission.

[Groups] tab

Add or delete the group to be associated with the permission.

[Users] tab

This tab displays the list of users who are associated with the permission.

Cards

Click [Cards] in the navigation tree to display the list of cards.

Note

- For the functional outlines or operations of cards, see page 172 "Managing User Information".

Item	Description
Card Number	Enter the card ID.
Card Name	Enter the card name.
User Name	To assign a card to a user, click [Search User], and then select the user to whom the card is assigned.
Enabled	Specify whether or not to validate the card.
Indefinite Period	No expiration date is specified on the card.
Limited Period	A validation period is specified on the card.
Temporary Period	The card is valid for only one day.
Effective Date	Specify the date when the validation period of the card starts.
Expiry Date	Specify the date when the validation period of the card ends.

Note

- For the functional outlines or operations of these setting items, see page 175 "Managing Card Information".

Accounting Tasks

Click [Accounting Tasks] in the navigation tree to display the accounting tasks.

[General] tab

Item	Description
Task Name	Enter the name of the task.
Description	Enter the description of the task.

Item	Description
Default Color Page Limit	Select [Settings], and then specify the default to limit the number of color prints and color copies that can be made.
Default Accounting Limit	Select [Settings] to specify the default to limit the usage of the MFP or printer.
Color Page Balance	For the balance on color prints and color copies, specify the following: • [Reset]: Resets the balance to the default value specified in [Default Color Page Limit]. • [Set]: Specifies the balance. • [Add]: Adds to the balance.
Account Balance	For the usage balance on the MFP or printer, specify the following. • [Reset]: Resets the balance to the default value specified in [Default Accounting Limit]. • [Set]: Specifies the balance. • [Add]: Adds to the balance.

[Message] tab

Configure the contents of a notification e-mail to be sent to the specified user.

Item	Description
Language	Select the language to use in the notification e-mail. The default is same as the language selected when login. You can change the language for each task if necessary.
Subject	Enter the subject of the notification e-mail.
Body	Enter the body of the notification e-mail.

You can specify the following variables in the messages for the accounting task. A variable entered in the message is replaced as shown in the table below:

Variable	Description
$[accounting_task_result]$	Replaced by the accounting task result ("Success" or "Failure").
$[accounting_task_name]$	Replaced by the accounting task name.
$[accounting_task_start_end_time]$	Replaced by the start and end date/time of the accounting task.

[Target Users/Groups/Departments] tab

The target users/groups/departments of the task are displayed in the list.

From [Select Target], select the target to display in the list.

[Schedule] tab

Configure a schedule for performing the task.

Item name	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.
Daily	The task begins on the specified date and is executed daily at the specified time.
Weekly	The task begins at the specified date/time and is executed weekly on the specified day of the week. You can specify more than one day of the week.
Monthly	The task begins at the specified date/time and is executed monthly at the specified date. You can specify more than one date from the 1st to 31st day or the last day of the month.
Start Date	Specify the date to start the schedule.
Start Time	Specify the time to start the schedule.

[Notifications] tab

Item	Description
Enable Task Completion Notification	Specify whether or not to send a notification e-mail when the task is completed.

Item	Description
Input Email Address Manually	Enter the e-mail address of the destination manually. • Email address: Enter the e-mail address of the destination. • [Language]: Select the language to use in the notification e-mail.
Select Destination	Select a destination from the destinations registered in [System] ▶ [Notification] ▶ [Destination].

Synchronization Tasks

Open the [Synchronization Tasks] to display the registered synchronization tasks. To modify an existing task, select the task from the list.

[General] tab

Item	Description
Task Name	Enter the task name.
Description	Enter the description of the task.
User Synchronization	Select the type of the user to synchronize from the LDAP server. • [Update Users Only] • [Update Users and Add New Users] • [Add New Users Only] The default is [Update Users Only].
Groups to Synchronize	Enter the group to synchronize. To enter more than one group, separate each group by a comma (,). To synchronize all groups, leave the box blank.

[Authentication Profile] tab

Item	Description
Authentication Profile	Select the authentication profile.

Item	Description
Attributes to be Synchronized	Select items to synchronize. Items are displayed in the drop-down list if they are with values that are specified for the user attribute in the authentication profile.
[Test Connection] button	Specify whether or not a connection can be established to the LDAP server.

[Schedule] tab

Configure a schedule for performing the task.

Item name	Description
Disable Schedule	Select the check box to disable the schedule.
Once Only	The task is executed only once at the specified date/time.
Daily	The task begins on the specified date and is executed daily at the specified time.
Weekly	The task begins at the specified date/time and is executed weekly on the specified day of the week. You can specify more than one day of the week.
Monthly	The task begins at the specified date/time and is executed monthly at the specified date. You can specify more than one date from the 1st to 31st day or the last day of the month.
Start Date	Specify the date to start the schedule.
Start Time	Specify the time to start the schedule.

[Notifications] tab

Item	Description
Enable Task Completion Notification	Specify whether or not to send a notification e-mail when the task is completed.

Item	Description
Input Email Address Manually	Enter the e-mail address of the destination manually. • Email address: Enter the e-mail address of the destination. • [Language]: Select the language to use in the notification e-mail.
Select Destination	Select a destination from the destinations registered in [System] ▶ [Notification] ▶ [Destination].

Server Management

This section describes the functions of items displayed in [Server Management] in the navigation tree.

Server Group

In [Server Group] to display the list of servers, select the server's group. Select a server in the list to display the detailed information of the selected server. The tabs that are displayed on this screen differ depending on the components that are enabled on the selected server.

Important

- **For the settings to be applied to all Delegation Servers, use [System] ▶ [Delegation Server Settings] in the navigation tree. Select and configure a target server in [Server Group] only when configuring the settings specific to each Delegation Server.**
- **Priority is given to the values specified in [Server Group] for the common settings that can be configured in [Delegation Server Settings] and [Server Group].**

Note

- For the functional outlines or operations of server group, see page 386 "Receiving Notifications from the Server".

[General] tab

This tab shows the server host name, IP address, and other general server information.

[Capture] tab

Item	Description
Overwrite Delivery Schedule	Configure the schedule to overwrite the workflow process at the system level over the Delegation Server. When a day of the week is not specified, overwriting of the item occurs every day.
Delivery Schedule	Specify the day of the week to start a workflow job, the start time, and end time.
Auto Delete Error Jobs	Specify the period and maximum capacity to store error jobs.
Overwrite Backed Up Fax Jobs	Specify whether or not to overwrite the fax job save settings of the system level to the Delegation Server.

Item	Description
Save Fax job(s)	Specify whether or not to back up fax jobs. When specifying a backup, also specify the storage period and the time to automatically delete unnecessary backups. The backed up fax jobs are stored in the following folder: (Data folder on the Delegation Server)\data\scan\ds\fax-jobs
Overwrite OCR Mode	Select the operation mode of the OCR engine. • [Balance]: In this mode, the character recognition process is performed while maintaining a balance between the recognition rate and speed. • [Recognize Rate Priority]: In this mode, priority is given to the recognition rate. • [Speed Priority]: In this mode, priority is given to speed. The default is [Balance].
Overwrite Kerberos Option	An authentication method can be specified for each connector type from the drop-down list. • [Use the ticket received on Kerberos authentication as the priority] • [Use only the ticket received on Kerberos authentication] • [Use only NTLM] The default is [Use Kerberos authentication as a priority].
Hot Folder Profile	Displays the Hot Folder Profile that is monitored by the target server.

[Device Management] tab

This tab shows the total number of devices and other device management information.

[Server Notifications] tab

When the [Overwrite Server Notifications] check box is selected, priority is given to the notification setting on the [Server Notifications] tab over the one specified in [System] ▶ [Server Settings] ▶ [Delegation Server Settings]. The types of notifications that can be configured are as follows:

- [System Error]
- [Commercial Certificate Expiration]

- [HDD Capacity]

For details about each setting item, see "[Server Notifications] tab", page 539 "Delegation Server Settings".

Delegation Server Failover/Load Balancing Groups

Click [Delegation Server Failover/Load Balancing Groups] in the navigation tree to display the list of setting names.

Those settings are used to distribute the data processing load on the server over multiple Delegation Servers.

The priority order of Delegation Servers to perform data processing can be specified for each functions such as authentication, scanning, or printing.

Also, processing load is automatically carried over to the secondary Delegation Server to avoid the process being interrupted if a problem occurs on the primary Delegation Server.

The list of server groups is displayed at the top right of the screen. Select a server group from the list to display the detailed information of the selected group. Alternatively, click (Add) on the toolbar to add a new server group.

Note

- For the functional outlines or operations of load balance and fail over, see page 386 "Receiving Notifications from the Server".

[General] tab

Configure the connection settings that are common to all server groups.

Item	Description
Name	Enter the setting name.
Description	Enter the description.
Connection Timeout	Specify the time limit until the connection from the device to the server times out. The default is 4 seconds.
Processing Timeout	Specify the time limit until the request sent from the device to the server times out. The default is 30 seconds.

Item	Description
Recovery Check Interval	Removes the job request from the list until a retry request is received from the device when the server fails to process the job request. Specify the time limit until the job request is removed. The default is 1 minute.

[Authentication] tab, [Capture] tab

Add a combination of servers to distribute processing load to the list, and change the priority order.

Reports

Click [Reports] in the navigation tree to display [Report Templates], [Saved Reports], and [Report Tasks].

About reporting functions, see Reporting and Dashboards Guide for details.

@Remote

This section describes the functions of items displayed in [@Remote] in the navigation tree.

Note

- @RemoteAdmin or @RemoteCE permission is required for operations on some of the following items: To modify them, assign @RemoteAdmin or @RemoteCE permission to the user role. For details about the permissions, see page 160 "Managing User Roles and Privileges".

@Remote Settings

Click [@Remote Settings] in the navigation tree to display the list of servers. Eight tabs are displayed under the list when [Status] of the server changes to [Registered].

[Proxy Server] tab

This tab displays the settings of [Server Settings] ▶ [Networking] ▶ [Proxy Server]. Configure the following items:

Item	Description
Use Proxy Server	Specify whether or not to use a proxy server. The default is Off.
Refer to System Settings	Select this check box when [Use Proxy Server] is set to On to reference the settings of [Server Settings] ▶ [Networking] ▶ [Proxy Server].
Proxy Server Address	Enter the server address when not referencing the [Proxy Server] settings.
Proxy Server Port Number	Enter the port number when not referencing the [Proxy Server] settings.
Use Authentication	Specify [On] or [Off] for user authentication.
User Name	Enter the user name when user authentication is set to [On].
Password	Enter the password when user authentication is set to [On].
Domain Name	Enter the domain name when user authentication is turned [On].
[Check Connection] button	Test the connection using the proxy server.

[Connector Settings] tab

Item	Description
Send IP addresses	Specify whether or not to send the IP address to Ricoh.
Send non-RICOH devices information	Specify whether or not to send the information of non-Ricoh devices.
Request number	Enter the request number for connecting to @Remote Center.
RC gate ID	Automatically displays the RC gate ID.
Status	Displays the registration status of the server to @Remote Center.
Test Call button	Attempts to obtain a command from @Remote Center.
[Confirm Communication] button	Attempts to connect to @Remote Center. If the connection attempt fails, detailed information is displayed.
Change encryption length	Select the length of the encryption key. • [512 bit] • [2048 bit] The default is [512 bit].
@Remote center address	Displays the address of @Remote Center. Click the [Change] button to change the address.

[Communication Settings] tab

This tab displays the communication setting of @Remote Connector. Configure the following items:

Item	Description
Use onsite data for device status information notification	Specify whether or not to use information other than the onsite counter.
Use onsite data for device counter information notification	Specify whether or not to use the information of the onsite counter.

[Permission Settings] tab

Configure the task permission settings of @Remote. The following settings can be configured for each displayed task. The setting items may change depending on the task.

Item	Description
Permit	Allows the execution of the task.
Do not permit	Prohibits the execution of the task.
Confirm before running	Displays a confirmation message before executing the task.
Select email address...	This button is enabled only when [Confirm before running] is selected. Click the button to select the e-mail address.

[Device Access Information] tab

Displays the device access settings that have been configured by @Remote Center.

[Serial Number Acquisition] tab

Enter OID to obtain the serial number of a non-Ricoh device. Up to 10 OIDs can be entered.

Item	Description
Test...	Click to confirm that the entered OID is valid. The [Test MIB OID] dialog box is displayed when this item is clicked. Enter the following: • [Device (Hostname or IP Address)]: Enter the host name or IP address of the target device. Use only ASCII code characters. • [SNMP Community Name]: Enter the SNMP community name. Use only ASCII code characters. • [MIB Value]: Click the [Get MIB Value] button to get the MIB value.
Comment	Enter a comment regarding the device such as the name of the manufacturer.

[Device List Update] tab

Select the method for updating the device list and device status, and specify the update schedule when sending the data to the @Remote Center system.

Item	Description
Device List Update Method	Select the method for updating the device list and device status. • [Send information after discovery] • [Send information after polling] • [Send information after device list import] • [Send information only] The default is [Send information after polling].
Discovery Profile Name	Click the [Select Profile] button to select the name of [Discovery Profile]. This item is valid only when [Device List Update Method] is set to [Send information after discovery].
Server Address	Enter the server address. This item is valid only when [Device List Update Method] is set to [Send information after device list import].
Port Number	Enter the port number of the server. Specify from the following range: • 0–65535 This item is valid only when [Device List Update Method] is set to [Send information after device list import].
DM Name	Click [Get DM List] to select the Delegation Server. This item is valid only when [Select Server Type] is set to [Device Manager NX Enterprise].
Test Connection	Tests the connection.
Daily	The task begins at the specified time every day starting on the day that the update task on the device list is specified.
Weekly	The task begins at the date/time that the update task on the device list is specified, and it is executed weekly on the specified day of the week. Specify from the following range: • From [Sunday] to [Saturday]

Item	Description
Monthly	The task begins at the date/time that the update task on the device list is specified, and it is executed monthly on the specified day of the month. Specify from the following range: • 1–31 day(s) The default is 1 day(s).
Start Time	Specify the time to start the update task on the device list.

[Migration] tab

Item	Description
Request number	Enter the request number for connecting to @Remote Center.
Connect	Obtains the migration data from @Remote Center.
OK	When a confirmation phone call is received from the @Remote operator, click this button to complete the migration process of @Remote Center.

Note

- For the functional outlines or operations of these setting items, see page 128 "Monitoring Devices Using the @Remote Function".

10

Task Permit

Click [Task Permit] in the navigation tree to display the task list. The following operations can be performed on each displayed task. The setting items may change depending on the task.

Operation	Description
Download	Downloads the data sent to @Remote Center System. This item is available for a [To center] task.
Run	Allows executing of the task.

11. Appendix

Limitations

This section describes limitations regarding the print function.

Servers

- When the PostScript driver is used on the server, information on the print document list may not be correctly retrieved. For example, RICOH Streamline NX may not be able to retrieve the color mode and layout information from print jobs created by some Mac OS X applications.
- Print document data whose storage period has elapsed can be displayed in the print document list and printed until the automatic deletion period is reached.
- When the print job is sent without enabling sorting on the PCL driver, the driver behaves as follows:
  - You cannot use the Check Print function (prints one copy to enable checking of the print settings).
  - You cannot change the number of copies to one copy (the originally specified quantity is printed without sorting).
  - The document is printed with sorting specifications applied when the number of copies is changed to two or more.
- When the same user name is used across multiple domains, specify a domain when logging in. (e.g. foo@child 1.foo.com, foo@child 2.foo.com)
- Kerberos authentication is not possible if the user name contains "@" and an Alternative UPN is used.
- Depending on print settings, print job data, and a combination of optional functions on the device, you may not be able to print using the current print driver settings. In such case, not the user settings but the print settings of the print driver are displayed on the print document queue.
- If the device used for printing is a non-Ricoh printer or USB-connected device and data is accounted based on the job data before printing and not the actual print results, you may not be able to retrieve accurate accounting information.
- When using Japanese, Chinese, or non-ASCII Latin-1 characters in the print document name, user name, or display name displayed on the operation screen, configure the local settings for the character code to use on the Delegation Server, device, client computer with RICOH Streamline NX PC Client installed, or web client. If local settings are not properly configured, a print document name will not be correctly displayed.
- Two-color print jobs are displayed on the print document list as black-and-white print jobs.
- Two-color print jobs cannot be printed with a normal printer driver.

- Depending on the environment in which the print job is sent, the user name may be displayed as "SYSTEM".
- When a computer fax driver is used to send a "Send & Print" job or "Print" job, "000000" is recorded as the user performing printing in the accounting information.
- Even if you delete or change a SLNX Secure Print Port, a job associated with the original port is not deleted immediately and it remains in the database and file system for several days after the port is deleted or changed.
- If the operating system does not support the language information of a print data string when it is printed with the specified SLNX Secure Print Port, the printed string may include garbled text.
- You cannot delete the default SLNX Secure Print Port.
- Depending on the device, you may not be able to print using the current print driver settings.
- Depending on the settings of the print job or driver, you may not be able to retrieve an accurate accounting log. For example, when a job is printed with multiple sizes, all pages are counted as the same size as the first page.
- Direct printing only supports Normal Print.
- There is a limit to the number of user accounts that can be added to the address book of each RICOH device. If authentication of a new user is attempted after the limit is reached, an authentication error will occur. However, when existing users are configured for automatic deletion, authentication will be successful. See the user's guide of the device. Also, use the configuration task to delete entries in the address book at a regular interval if necessary.
- Paper sizes are retrieved from the Printer Job Language (PJL) and the spooler. If this information cannot be retrieved, the cost estimate may not be accurate.
- SNMPv3 cannot be used when you access a device with the SNMP protocol for accounting jobs or using print rules.
- Names of device direct print jobs are not displayed in reports.
- Accounting information for multiple device direct print jobs may be displayed in the report as the data for one job.
- The accounting information for one secure print job or direct print job may be displayed in the report as data for multiple jobs. In this case, job names are not displayed for multiple jobs.
- When printing is performed with device direct printing running on an operating system other than Windows, the print job may not have user name information. If the device is an MFP and has the Streamline NX Embedded Applications installed, you can print by enabling [Accept anonymous user] for [Authentication] on [Streamline NX Embedded Settings]. Print jobs without user name information are classified in a report as "Host print". For details, contact Ricoh service representative.
- Laser printers do not support printing using the [Accept anonymous user] option. When printing a job without user name information using a laser printer, configure print job authentication as follows:

1. On the Management Console, click the following items in the navigation tree to open the [Standard Device Preferences] tab.

   [Configuration] ▶ [Configuration Templates] ▶ [Standard Device Preferences]
2. Select the preference to be edited.
3. On the [Standard Device Preferences] tab, click [Authentication] ▶ [Print].
4. Select the [Print Job Authentication] check box, and then select [Simple (Limitation)] from the drop-down list.
5. Specify the range of IP addresses of devices (computers, smart devices, etc.) subject to authentication.
6. Apply the setting to the laser printer.

- When device direct printing is used to print on a device without the Streamline NX Embedded Applications installed, print rules and reports cannot be used.
- If an IP address is changed, restart the computer with the Delegation Server installed.
- When authentication settings are configured in a non-PCL driver, such as a PostScript printer driver, the user may be recognized as a different user. Depending on the device, the print document properties may not be retrieved, and you may not be able to print using the current print driver settings.
- You cannot use double-byte characters for the user name in the PostScript printer driver. To use double-byte characters in a user name, use the PCL printer driver.
- Color printing is available when PDF data is sent to a Delegation Server using a black-and-white PostScript printer driver and printing from a color printer.
- Install a printer driver that is compatible with the device you are using. If the printer driver is not compatible with the device, you may not be able to print using the current print driver settings. To print on multiple devices, install the RICOH Universal Print Driver supports PCL and PS language, and these are provided as individual printer drivers. These drivers can be shared on models that support PCL or PS language.
- When a color print job is sent by Direct Print to a non-Ricoh black-and-white printer or a black-and-white printer without the Streamline NX Embedded Applications installed, it is accounted as a color job.
- When a print job from the PCL 5 driver or non-RICOH driver is redirected, the color setting specified in the driver is not applied. Instead, the default setting of the machine that executes printing is applied as the color setting. Therefore, the job lists displayed on the control panel of the machine and in the Management Console, and the contents displayed in the confirmation dialog box will show the default settings of the machine. Also, the values specified in the report function will reflect the default settings of the machine if no Streamline NX Embedded Application is installed on the machine.
- When an error occurs such as Paper Jam, Toner End, etc. in printing process, the print job is reported in separated records in SLNX Report before and after the error. Also in this case, when

Print Rule is applied and the print cost is changed after the rule application, the Original Cost field in the report could be different from the originally intended one.

- It takes up to 5 minutes before the job name mask setting is applied to jobs in print queue of the Delegation Server.

Devices

- The MFP does not enter energy saver mode in the following cases:
  - A document is being printed
  - The device is paused due to a printing error
  - A document is being deleted
- The hard keys on the device may be slow to respond when a document is being printed.
- When the administrator or service engineer operates Secure Print, the device recovers from energy saver mode.
- Printing of a document may be canceled by a user who can log in to the device.
- When Secure Print is activated, specify the auto off timer on the device to five minutes or more. If the device enters sleep mode before Secure Print can finish startup, the device may not correctly operate.
- The owner must have the privileges to perform printing by print rules or based on the account balance. Otherwise, delegate users cannot print documents.

Regular Backups

- Regularly back up all settings of the device. Ricoh is not responsible for any loss or damage to data on devices.

Document Delivery

- When the OCR language is Japanese, you cannot use the format conversion function. If you use the format conversion function in such case, the job will result in an error.
- The following connectors do not support TIFF format that uses Old-style JPEG compression (Compression=6):
  - ImageConverter
  - ImageCorrection
  - Zone OCR
  - OCR (when the OCR language is Japanese)

List of Device Preference Setting Items

The following describes the configuration items on devices that can be specified in the Device Preference templates.

Important

- **If you configure the setting items with indicated the dagger (†), the Extended Item Setting license is must be activated. For details about extended item settings, see Important Information about Device Configuration.**

Note

- Even when SLNX Management Extension is installed, you can disable configuration changes to the setting items indicated with a dagger (†) in configuring the system settings.
- Categories that have settings that differ from the defaults are shown in italic, bold text.

General

<Information>

Setting Item	Description
Comment	Enter the comment of the device.
Location	Enter the location of the device.
URL Name	Enter the URL name of the device.
URL	Enter the URL of the device.

<General>

Setting Item	Description
Display IP Address on Device Display Panel	Set whether the IP address is displayed for a device.

Date and Time

<Date/Time Settings>

Setting Item	Description	
SNTP Server Settings	Set the SNTP server.	
	SNTP Server Address	Enter the SNTP server host name or IP address.
	Polling Interval	• [When Printer On] Select this to perform polling only when the device is activated. • [Every Time] Select this to perform polling at a given interval. Enter the polling interval in units of minutes.

<Time Zone/Daylight Saving Time Settings>

Setting Item	Description	
Time Zone/Daylight Saving Time Settings	To use daylight saving time, select the check box.	
	Time Zone (GMT)	This sets the time zone used by the device.
	DST	Specify whether or not to adjust for daylight savings time.
	Offset Time	Select the offset time for the daylight savings adjustment from the pull-down menu.
	Start Date/Time	Select the daylight savings start date and time from the pull-down menu.
	End Date/Time	Select the daylight savings end date and time from the pull-down menu.

Smart Operation Panel

<Application Assignment to Home Key>

Setting Item	Description	
Assign Application to Home Key	Specify whether or not to assign an application to the [Home] key.	
	Application assigned to the Home key	Select the application to assign to the [Home] key.
	Allow Unauthenticated User to Transit to RICOH Home	Specify whether or not to allow a guest user to operate the default home screen when specifying user authentication on a device.

<table>
<tr><th>Setting Item</th><th colspan="2">Description</th></tr>
<tr><td rowspan="3">Assign Application to Function Key</td><td colspan="2">Specify whether or not to assign applications to the function keys.</td></tr>
<tr><td>Function Key Settings</td><td>Specify whether or not to assign applications to the function keys. When selecting [Enable], assign an application to each function key (#1 to #3).
Note
• The [Function Key Settings] check box is cleared and function keys cannot be set when the items on the [Standard Device Preferences] tab are populated using [Get Settings from Device] and any of the assigned functions are for an application that does not exist in the SDK application table. It can occur when [Other Polling] was not performed to populate the SDK/J applications.</td></tr>
<tr><td>Function Key 1 to Function Key 3</td><td>Select an application installed on the device from the drop-down list to assign it to a function key. The following applications are always displayed:
• SLNX User Info
• SLNX Scan
• SLNX Secure Print
When the [Display Name] check box is selected, a display name for the application can be assigned to the function key. When it is cleared, the default name of the application is assigned to the function key.
Note
• Function Key #1 is not available when SLNX Scan is assigned to the Home key.</td></tr>
</table>

Network Protocols

<IPv4 protocols>

Setting Item	Description
SMB	Specify whether to enable SMB.
Workgroup Name	Enter the Workgroup name.
Notify Print Completion	Specify whether to enable Print Completion Notification.
Enable Telnet	Specify whether to enable printing using Telnet.
Enable Bonjour	Specify whether to enable Bonjour.
Enable SSL	Specify whether to enable SSL.
Enable SSDP	Specify whether to enable SSDP.
Enable BMLinkS	Specify whether to enable BMLinkS.
Enable SSH	Specify whether to enable SSH.
Enable SFTP	Specify whether to enable SFTP.
Enable FTP	Specify whether to enable FTP.
Enable IPDS	Specify whether to enable IPDS.
Enable RHPP	Specify whether to enable RHPP.
Enable WS-Device	Specify whether to enable WS-Device.
Enable WS-Printer	Specify whether to enable WS-Printer.
Enable WS-Scanner	Specify whether to enable WS-Scanner.
Enable LPR	Specify whether to enable LPR.
Enable RSH	Specify whether to enable RSH.
Enable DIPRINT	Specify whether to enable DIPRINT.
Enable IPP	Specify whether to enable IPP.

<IPv6 protocols>

Setting Item	Description
Enable Telnet	Specify whether to enable printing using Telnet.
Enable Bonjour	Specify whether to enable Bonjour.
Enable SSL	Specify whether to enable SSL.
Enable SFTP	Specify whether to enable SFTP.
Enable RHPP	Specify whether to enable RHPP.
Enable WS-Device	Specify whether to enable WS-Device.

<SSL Options>

Setting Item	Description
SSL/TLS Version	Specify whether to enable SSL/TLS by version.
Encryption Strength Setting	Specify encryption strength.

Important

- **The following conditions should be met so that the configuration is evaluated as "valid" to prevent vulnerability in security:**
  - **One or more items of [SSL/TLS Version] are enabled.**
  - **One or more items of [Encryption Strength Setting] other than "RC4 128 bit" are selected.**
  - **One or more items of [SSL/TLS Version] other than [SSL 3.0] should be enabled when "AES 128 bit" or "AES 256 bit" is selected.**

<Other Protocols>

Setting Item	Description
AppleTalk	Specify whether to enable the AppleTalk protocol.
Zone Name	Specify the AppleTalk zone. Enter the zone name.
NetWare	Specify whether to enable the NetWare protocol.

TCP/IP

<Addressing>

Setting Item	Description
DHCP	Specify whether to obtain IP addresses from DHCP servers.
WINS	Specify whether to enable name resolution using WINS servers.
Primary WINS Server	Enter the IP address for the primary WINS server.
Secondary WINS Server	Enter the IP address for the secondary WINS server.
Display IP Address on Device Display Panel	Specify whether the IP address is displayed for a device.

SNMP

<Quick Configuration>

Setting Item	Description	
Enable Quick Configuration	Enables Quick Configuration for SNMP Profile.	
	Profile Name	Select the SNMP profile created in [Access Accounts].
	Restrict access to SLNX	Allows only the system to be the destination of communication via SNMP from devices.
	Enable SNMP Traps for SLNX	Enables the system to receive SNMP Traps from devices.
	Clear other settings	Initializes SNMP and other settings specified on the device.

<Advanced Configuration>

Setting Item	Description	
SNMP Profile	Enables the Advanced Settings for SNMP Profile.	
	Profile Name	Select the SNMP profile created in [Access Accounts].
	<SNMP v1/V2>	The Community Name specified in the SNMP account setting is displayed. Select the Community number to assign the settings
	<SNMP v3>	The Authentication Algorithm specified in the SNMP account is displayed.
	SNMP Trap	Specify whether or not to enable SNMP trap.
SNMP V3	Enables the SNMP v3 setting.	
	SNMP v3	Specify whether or not to enable SNMP v3 on the device.
	Authentication Algorithm	Select the authentication algorithm from [MD5] or [SHA1].
Community 1–10	• Community Name Enter the community name. • Access Type Select an Access Type from [Not Accessible], [read-only], [read-write], or [trap]. • Protocol Type Select a Protocol Type from [TCP/IP+IPX], [IPX], [TCP/IP], or [Off]. • IP Address Enter the IP address to allow connection in the TCP/IP protocol. An SNMP Trap is sent to the entered IP address when [trap] is selected for Access Type. • Manager IPX Address Enter the IP address to allow connection in the IPX protocol. An SNMP Trap is sent to the entered IP address when [trap] is selected for Access Type.	

Administrator

<Administrator Account >

Setting Item	Description	
Administrator Account	Select the primary administrator account.	
	Profile Name	If you configure a device using the Profile selected in this item, the selected Profile will be also applied to the Access Account Settings selected for the device in [Device List].
	User Name	The user name of the administrator account is displayed.
	Password	The masked password of the administrator account is displayed.
Administrator 2–4	Name	Select the user name of the administrator account.
	Password	Specify the administrator's password.
	Access	Specify the management category of a device functions.
Supervisor	Password	Specify the supervisor's password.

<Administrator Authentication>

Setting Item	Description	
En/disable Network Administrator	Specify whether to authenticate network administrators.	
	Network Administrator Authentication	If you select [On] for an item, that item will be authenticated. You can select multiple items. • File Transfer • Interface Settings • Administrator Tools

Setting Item	Description	
En/disable Machine Administrator	Specify whether to authenticate machine administrators.	
	Machine Administrator Authentication	If you select [On] for an item, that item will be authenticated. You can select multiple items. • General Features • Tray Paper Settings • Timer Settings • File Transfer • Interface Settings • Administrator Tools
En/disable User Administrator	Specify whether to authenticate user administrators.	
	User Administrator Authentication	Select [On] for the user administrator, and then [Administrator Tools] to authenticate a user administrator.
En/disable File Administrator	Specify whether to authenticate file administrators.	
	File Administrator Authentication	Select [On] for the user administrator, and then [Administrator Tools] to authenticate a user administrator.

Email

<Email>

Setting Item	Description
Email	• Administrator Email Address Enter the administrator's e-mail address.

<Reception>

Setting Item	Description
Reception Protocol	Select the receiving protocol: [POP3], [IMAP4], [SMTP]

Setting Item	Description
Email Reception Interval	Specify whether to set receiving intervals. Enter the interval length in minutes.
Max. Reception Email Size	Enter a size limit value for receiving e-mails in MB.
Email Storage in Server	Specify whether to retain e-mails on mail servers.

<Email Address>

Setting Item	Description
Fax Email Address	Enter e-mail addresses for fax mail.
Fax Email User Name	Enter user names for fax mail.
Fax Email Password	Enter passwords for fax mail.
Email Notification Address	Enter e-mail addresses to receive notification by the e-mail notification function.
Email Notification User Name	Enter user names for the e-mail notification function.
Email Notification Password	Enter passwords for the e-mail notification function.

<POP3/IMAP4>

Setting Item	Description
POP3/IMAP4 Server Name	Enter the POP3/IMAP4 server name.
POP3/IMAP4 Encryption	Select an encryption option from the following: [Auto Select], [Enable], [Disable]
POP3 Reception Port No.	Enter the number of the port used by the POP3 server for data reception.
IMAP4 Reception Port No.	Enter the number of the port used by the IMAP4 server for data reception.

<SMTP>

Setting Item	Description
SMTP Server Address	Enter the SMTP server address or host name.
SMTP Port Number	Enter the port number used by an SMTP server.

Setting Item	Description
SMTP Authentication	Specify whether to perform SMTP authentication.
SMTP Authentication Email Address	Enter the e-mail address used for SMTP authentication.
SMTP Authentication User Name	Enter the user name used for SMTP authentication.
SMTP Authentication Password	When performing SMTP authentication, enter the password used for authentication.
SMTP Authentication Encryption	Specify whether to encrypt SMTP authentication from the following: [Auto Select], [Enable], [Disable]

<POP before SMTP>

Setting Item	Description
POP before SMTP	Specify whether to perform POP before SMTP.
Timeout Setting after POP Auth.	Enter a time (in msecs) that the machine waits before going into standby mode following authentication by the POP server.

Authentication

Important

- **To apply the settings in this category to a device, Administrator Authentication Management must be enabled in the device settings. When Administrator Authentication Management is disabled, apply the template that enables Administrator Authentication Management in the [Administrator] category of the device before configuring this category.**

<Authentication Type>

Setting Item	Description
User Authentication Settings	Select the user authentication type: [Off], [User Code Authentication], [Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Server Authentication]

<Access Control>

Setting Item	Description
Copier	Specify whether to enable access control for the copier function for each user. Select the color settings that can be used when making copies from the following: [Black & White], [Single Color], [Two-color], [Full Color], or [Off].
Printer	Specify whether to enable access control for the printer function for each user. Select the color settings that can be used when making prints from the following: [Black & White], [Color], or [Disable]. • Auto Register User Codes Specify whether to automatically register the user code contained in a print job.
Fax	Specify whether to enable the access control for the fax function for each user.
Scanner	Specify whether to enable the access control for the scanner function for each user.
Document Server	Specify whether to enable the access control for Document Server for each user.

<LDAP>

Setting Item	Description	
LDAP Authentication	Specify whether to enable the LDAP Authentication.	
	LDAP Server 1–5	If you select [LDAP Authentication] in [User Authentication Settings], select an LDAP authentication server. **Note** • If your machine does not support configuration of multiple LDAP servers, be sure to select only one LDAP server at a time. Selecting multiple LDAP servers at the same time will result in a batch settings failure.
	LDAP Login Attribute	Enter an LDAP login attribute.
	Global Identifier	Enter a global identifier.
LDAP Server	Specify whether to use the LDAP search.	

Setting Item	Description	
LDAP Server 1–5	Perform batch settings for LDAP servers 1 to 5. To use the selected LDAP server, select LDAP servers 1 to 5. Select [Program] to configure the selected LDAP server. Select [Delete] to clear the settings of a LDAP server.	
	Identification Name	Enter the name.
	Server Name	Enter the server name.
	Search Base	Enter the search start point.
	Port Number	Enter the port number. If SSL is not used, the initial port number is 389. If SSL is used, the initial port number is 636.
	SSL	Specify whether to use SSL.
	Authentication	For authentication, select either of the following: [Off], [On], [High Security], [Kerberos Authentication]
	Authentication Realm	If you specify [Kerberos Authentication], you must then specify the realm that you want to protect with Kerberos authentication.
	User Name	Enter the user name.
	Password	Enter the password.
LDAP Server 1–5 (Search Conditions)	Identification Name	Enter the name as a search condition.
	Email Address	Enter the e-mail address as a search condition.
	Fax Number	Enter the fax number as a search condition.
	Company Name	Enter the company name as a search condition.
	Department Name	Enter the department name as a search condition.
	Attribute	Enter the attribute as an optional search condition.
	Key Display	Enter the key display name as an optional search condition.

<Integration Server>

Setting Item	Description	
Integration Server Authentication	Specify whether to enable the Integration Server Authentication.	
	Server Name	If you select [Integration Server Authentication] in [User Authentication Settings], enter the Integration server name.
	Domain Name	Enter the name of the domain where integration server authentication will be performed.
	Authentication Type	Select the type of integration server authentication from the following: [Windows Authentication (Native)], [Windows Authentication (NT Compatible)], [Basic Authentication (Integration Server)], [Notes Authentication], [Default]
	SSL	You can specify whether or not to perform SSL.

<Windows>

Setting Item	Description	
Windows Authentication	Specify whether to enable the Windows Authentication.	
	Domain Name	If you select [Windows Authentication] in [User Authentication Settings], enter the domain name to be used for authentication.
	SSL	Specify whether or not to perform SSL.
	Use Kerberos	Specify whether to use Kerberos authentication. If you select [On] under [Kerberos Authentication], you must specify the realm to protect with Kerberos authentication.
	Authentication Realm	Specify the realm to protect with Kerberos authentication.

<Kerberos>

Setting Item	Description	
Realm 1–5	Enter the information about the realm you want to protect with Kerberos authentication. Up to five realms can be set. Select [Program] to configure the selected authentication realm. Select [Delete] to clear the settings of a selected realm.	
	Realm Name	Enter the name.
	KDC Server Name	Enter the key distribution center (KDC) server address.
	Corresponding Domain Name	Enter the name of the domain that corresponds to the realm.

<Print>

Setting Item	Description	
Printer Job Authentication	Specify whether to enable the Printer Job Authentication.	
	Printer Job Authentication	Select the printer job authentication method: [Entire], [Simple (All)], [Simple (Limitation)]
	Limitation Range 1–5	Enter the range of IP addresses subject to authentication.
	Parallel Interface (Simple)	Specify whether to allow parallel interface.
	USB (Simple)	Specify whether to allow USB interface.

Note

- [Access Control] can be specified only when [User Authentication Settings] is set to [User Code Authentication].

Service and Consumables

<Paper Tray>

Setting Item	Description
Paper Tray 1 to 10	Select the paper type loaded in each paper trays.

Printer

<Maintenance>

Setting Item	Description
Protect Printer Display Panel	[Off], [Level 1], [Level 2]
List/Test Print Lock	List/test print lock: Select whether to prohibit test prints.

<System>

Setting Item	Description
Misfeed Recovery	Specify whether to use the Misfeed Recovery function.
Print Error Report	Specify whether to print a report when an error occurs.
Auto Continue	Select the time period the machine waits before continuing printing when there is no paper matching the size and type specified by the printer driver in the paper trays: [Off], [Immediate], [1 min.], [5 min.], [10 min.], [15 min.]
Memory Overflow	Select the action to perform in the event of a memory overflow. [Do not Print], [Error Information]
Job Separation	Specify whether to separate jobs.
Auto Delete Temporary Print Jobs	Specify whether or not to automatically delete temporarily stored documents. Enter the period (1 to 200 hours) after which temporarily stored documents are deleted.
Auto Delete Stored Print Jobs	Specify whether to delete saved documents automatically. Enter the period (1 to 180 days) after which saved documents are deleted.

Setting Item	Description
Initial Print Job List	Select [Complete List] or [List per User ID] by User ID for Initial Print Job List.
Rotate by 180 Degrees	Specify whether to perform 180-Degree Rotation printing.
Print Compressed Data	Specify whether to print incoming compressed job data after decompressing it on the printer. The only supported compression format is GZIP.
Memory Usage	Select [Font Priority] or [Frame Priority] for memory usage.
Duplex Print	Select [Off] to disable duplex printing. To enable duplex printing, select either [Long Edge Feed] or [Short Edge Feed] as the binding orientation.
Copies	Enter the default number of copies using single-byte numbers. Enter a number from 1 to 999.
Blank Page Print	Specify whether to print blank pages.
B&W Page Detect	Specify whether to use the Black and White Image Recognition function. Off, On, Per page, Per job
Edge Smoothing	Specify whether to enable Edge smoothing. If you select [On], rough edges of letters or figures will be smoothed before printing.
Toner Saving	Specify whether to enable Toner saving. If you select [On], toner is saved by reducing the number of dots in solid black areas of print.
Spool Image	Specify whether to perform Spool Image printing.
Reserved Job Waiting Time	Select a wait time: [Long Wait], [Medium Wait], [Short Wait], [In Reserved Job Order]
Printer Language	Enter the printer language to be used.
Sub Paper Size	[Off], [Auto]
Default Paper Size	Select the default paper size.

Setting Item	Description
Letterhead Setting	Specify whether to perform letterhead paper printing: [Off], [Auto Detect], [On (Always)]
Edge to Edge Print	Specify whether to use the Edge to Edge Print function.
Bypass Tray Setting Priority	If the bypass tray is used, specify whether to follow the printer driver or the command setting or device setting.
Default Printer Language	Enter the default printer language.
Tray Switching	Specify whether to search for another paper tray if the paper size or type specified for the job does not match the paper in the tray specified for printing.
Collate Type	Specify whether to use the sort function. To use the sort function, select a sort method: [Collate], [Rotating Collate], [Shift Collate]
Staple Type	Specify whether to use the staple function. To use the staple function, select a staple position: [Off], [Top Left Slant], [Top Right Slant], [Left 2], [Top 2], [Right 2], [Top Left], [Top Right], [Center]
Punch Type	Specify whether to use the punch function. To use the punch function, select the punching method and position: [Off], [Left 2], [Top 2], [Right 2], [Left 3], [Top 3], [Right 3], [Left 4], [Top 4], [Right 4]
Extended Auto Tray Switching	If paper runs out during printing, the tray will be switched automatically if there is another tray that is loaded with paper of the required size, orientation, and type.
Virtual Printer	Specify whether to enable or disable the Virtual Printer function.

<Host Interface>

Setting Item	Description
I/O Buffer	Select a receive buffer size: [16 KB], [32 KB], [64 KB], [128 KB], [256 KB], [512 KB], [1 MB]

Setting Item	Description
I/O Timeout	Select the interface switching time: [10 sec.], [15 sec.], [20 sec.], [25 sec.], [60 sec.]

<Language Settings>

Setting Item	Description
PCL	
Orientation	Select either [Portrait] or [Landscape].
Form Lines	Enter the number of lines per page (5 to 128).
Font Source	Select a font source: [Resident], [RAM], [HDD], [Slot DIMM], [SD], [SD Font Download]
Font Number	Enter the default font ID.
Point Size	Enter the default font size in points.
Font Pitch	Enter the default font pitch in points.
Symbol Set	Select the character set to be used for the default font.
Courier Font	Select either [Regular] or [Dark] for the Courier font type.
Extend A4 Width	Specify whether to use the Extend A4 Width function.
Append CR to LF	Specify whether to use the Append CR to LF function.
Resolution	Select a resolution: [300 dpi], [600 dpi Fast], [600 dpi Standard], [1200 dpi]
Tray Parameters	You can use parameter settings to control tray switching. If settings are not needed, leave the space blank. [Auto Select], [Tray 1], [Tray 2], [Tray 3], [Tray 4], [Tray 5], [Tray 6], [Tray 7], [Large Capacity Tray], [Bypass Tray]
PostScript	
Job Timeout	Specify the time the machine waits for a currently printing job that has stalled before canceling the job. Enter a value of up to 999 seconds.

Setting Item	Description
Wait Timeout	Specify the time that the machine waits for a job before canceling the job. Enter a value of up to 999 seconds.
Data Format	Select either [Binary Data] or [TBCP] for the data format.
Resolution	Select a resolution from the following: [300 dpi], [600 dpi Fast], [600 dpi Standard], [1200 dpi]
Color Settings	Select an RGB color quality: [None], [Fine], [Super Fine]
Color Profile	Select a color profile: [Auto], [Presentation], [Solid Color], [Photographic], [User Setting]
Process Color Model	Select [Color] or [Black & White].
Orientation Auto Detect	Specify whether or not the machine automatically detects the image orientation (Portrait/Landscape) of the job data it receives. To enable auto detection of orientation, select [On].
Tray Parameters	Trays can be made to switch under parameters settings. Up to three parameters can be set for each tray. If settings are not needed, leave the space blank. [Auto Select], [Tray 1], [Tray 2], [Tray 3], [Tray 4], [Tray 5], [Tray 6], [Tray 7], [Large Capacity Tray], [Bypass Tray]
PDF	
Resolution	Select a resolution from the following: [300 dpi], [600 dpi Fast], [600 dpi Standard], [1200 dpi]
Color Settings	Select an RGB color quality from the following: [None], [Fine], [Super Fine]
Color Profile	Select a color profile from the following: [Auto], [Presentation], [Solid Color], [Photographic], [User Setting]
Process Color Model	Select [Color] or [Black & White].

Setting Item	Description
Orientation Auto Detect	Specify whether or not the machine automatically detects the image orientation (Portrait/Landscape) of the job data it receives. To enable auto detection of orientation, select [On].
New PDF Fixed Password	Enter a new PDF password.
New PDF Group Password	Enter a new PDF group password.

Security

<Password>

Setting Item	Description
Password	Select [None], [Type 1], or [Type 2] for the password policy of the device.
Lockout/Release	Specify whether to enable or disable the user lockout function.
Number of Attempts before Lockout	If you enable the lockout function, you must specify a number from 1 to 10 to indicate the number of attempts at password entry the user can make before being locked out.
Lockout Release Timer	If you enable the lockout function, you must specify whether to enable or disable lockout release.
Lock Out User for	If you enable the lockout release, you must specify how many minutes must elapse before the lockout is released.

<Remote Firmware Update>

Setting Item	Description
Permit Firmware Update	Specify whether to permit firmware updates.
Permit Firmware Structure Change	Specify whether to permit changes to the firmware structure.

Interfaces

<Interface Settings>

Setting Item	Description
Ethernet Speed	Ethernet communication speed. For normal use, select [Auto Select]. This allows the device to select the optimum speed. If communication with the device fails, select [100Mbps Full Duplex], [100Mbps Half Duplex], [10Mbps Full Duplex], or [10Mbps Half Duplex].

Device Functions

<Enable SDK/J Platform>

Setting Item	Description
Enable SDK/J Platform	Specify whether to enable or disable SDK/J Platform.

Web Browser NX

<General>

Setting Item	Description
Action	Select the action you want to perform on the shortcut icon of a Web page. You can add, edit, or delete the icon on the Home screen that is displayed on the operation panel.
Title	Enter the name for the shortcut icon.
URL	Enter the URL to associate it to the shortcut icon.
Images	Select the image to be applied to the shortcut icon. You can select an image in png, jpg, or bmp format. The icon of Web Browser NX is used when no image is selected.

Note

- If adding new icons will exceed the device's maximum capacity, the new icon will not be created on the device's operation panel. However, it will be recorded as successful in the Task Log.

Setting Items on the Operation Screen of Devices

Customize the setting items to be displayed on the operation screen of devices and the setting values for those items. You can also configure how each item appears on the operation screen, and specify whether to show or hide each item and its default value.

[Destination] Tab

Specify the setting items of the destination connector on the operation panel of the device.

Send to Email

Basic screen

Selected Destinations

This displays the number of selected e-mail addresses and the actual e-mail addresses.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of the destination e-mail addresses on the Selected Destinations screen. Click [Reset All] to remove all selected e-mail addresses.

To, Cc, Bcc, ReplyTo

From the drop-down list, select the destination type of the destination e-mail address.

To specify a different e-mail address than the sender's address as the return address, enter the address you want to use in [ReplyTo].

Search

This searches for a destination e-mail address from the address book of the LDAP server and displays the search results in the Search Results list. It searches for all e-mail addresses that contain the search keyword

When you only enter a space or leave the field blank, it searches for all e-mail addresses.

Note

- To use this function, select [Enable Address Search] under [Email Search Settings] on the properties screen of the Send to Email connector. For details about the setting, see page 691 "Send to Email".

Manual Entry

Enter an e-mail address manually.

Note

- To use this function, select [Enable Manual Address Entry] under [Send to Email Option Settings] on the properties screen of the Send to Email connector. For details about the setting, see page 691 "Send to Email".
- In [Default Domain for Manual Input] under [Send to Email Option Settings] on the properties screen of the Send to Email connector, enter a domain name to be added to the e-mail address entered without a domain name. This is useful when the recipient is using the same domain.

Subject

You can specify a different subject for each language selected from the drop-down list

You can use the metadata in the scanned file as the subject, except "resultURL".

Note

- For details about metadata items, see page 348 "Metadata".

Options

Press this on the operation screen of the device to display the Send to Email Options screen.

To allow the device user to open the Options screen, set [Options] on the basic settings screen.

Send to Email Options screen

Divide Email

Specify how to divide an e-mail.

- Do Not Divide

  All scanned documents are sent in one e-mail.

- Page Divide

  Each page of a scanned document is attached as a file and separately sent.

- Size Divide

  Scanned documents are divided by the size specified in [Email Division Size (KB)] and separately sent. If the e-mail software of the recipient has a data restore function, the received divided data can be restored to one file.

Email Division Size (KB)

When [Size Divide] is selected in [Divide Email], enter the file size for dividing the document.

Notification

Specify whether or not to send a notification e-mail when the recipient opens the e-mail. Select [On] to send a notification e-mail to the logged-in user. This setting is valid only when the destination e-mail server supports the notification e-mail function.

If the e-mail address of the logged-in user cannot receive the notification e-mail, it is sent to the e-mail address specified by the administrator.

Priority

Select the priority assigned to the e-mail.

- None
- 1 (High)
- 2
- 3 (Standard)
- 4
- 5 (Low)

Sensitivity

Select the sensitivity assigned to the e-mail. The sensitivity is added in the e-mail header when you select a setting other than [None].

- None
- Personal
- Private
- Company-Confidential

Send to Folder, Send to FTP, and Send to WebDAV

Selected Destinations

This displays the entered or selected folder.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of a destination folder on the Selected Destinations screen. Click [Reset All] to remove all selected folders.

Search

This searches folders. It searches all folders that contain the search keyword.

When you only enter a space or leave the field blank, it searches for all folders.

Folder View

This closes the search screen and returns you to the folder list.

Root

This displays the root folder. This item is valid only when a subfolder is displayed.

Folder browser icons

Select a folder to be added to the Selected Destinations list.

The functions of the browser icons are as follows:

- 

Displays the subfolder(s) of the selected root folder.

- 

  Displays the folder one layer up. This item is valid only when a subfolder is displayed.

Send to Printer

Printer Name

Select a printer to be used for printing from the list of printers installed on the server.

Quantity

Use [↓] [↑] to specify the number of copies.

Send to SharePoint

Selected Destinations

This displays the entered or selected folder.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of a destination folder on the Selected Destinations screen. Click [Reset All] to remove all selected folders.

Search

This item is not used in Send to SharePoint.

Folder View

This item is not used in Send to SharePoint.

Root

This displays the root folder. This item is valid only when a subfolder is displayed.

Folder browser icons

Select a folder to be added to the Selected Destinations list.

The function of each browser icons is as follows:

- 

  Displays the subfolder(s) of the selected root folder.

- 

  Displays the folder one layer up. This item is valid only when a subfolder is displayed.

Send to DocumentMall

Selected Destinations

This displays the entered or selected folder.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of a destination folder on the Selected Destinations screen. Click [Reset All] to remove all selected folders.

Search

This item is not used in Send to DocumentMall.

Folder View

This item is not used in Send to DocumentMall.

Root

This displays the root folder. This item is valid only when a subfolder is displayed.

Folder browser icons

Select a folder to be added to the Selected Destinations list.

The function of each browser icon is as follows:

- 

  Displays the subfolder(s) of the selected root folder.

- 

  Displays the folder one layer up. This item is valid only when a subfolder is displayed.

Send to Exchange

Basic screen

Selected Destinations

This displays the number of selected e-mail addresses and the actual e-mail addresses.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of the destination e-mail addresses on the Selected Destinations screen. Click [Reset All] to remove all selected e-mail addresses.

To, Cc, Bcc, ReplyTo

From the drop-down list, select the destination type of the destination e-mail address.

To specify a different e-mail address than the sender's address as the return address, enter in [ReplyTo] the address you want to use.

Search

This searches for a destination e-mail address from the address book of the LDAP server and displays the search results in the Search Results list. It searches for all e-mail addresses that contain the search keyword.

When you only enter a space or leave the field blank, it searches for all e-mail addresses.

Note

- To use this function, select [Enable Address Search] under [Email Search Settings] on the properties screen of the Send to Exchange connector. For details about the setting, see page 727 "Send to Exchange".

Manual Entry

Enter an e-mail address manually.

Note

- To use this function, select [Enable Manual Address Entry] under [Send to Email Option Settings] on the properties screen of the Send to Exchange connector. For details about the setting, see page 727 "Send to Exchange".
- In [Default Domain for Manual Input] under [Send to Email Option Settings] on the properties screen of the Send to Exchange connector, enter a domain name to be added to the e-mail address entered without a domain name. This is useful when the recipient is using the same domain.

Subject

You can specify a different subject for each language selected from the drop-down list

You can use the metadata in the scanned file as the subject, except "resultURL".

Note

- For details about metadata items, see page 348 "Metadata".

Options

Press this on the operation screen of the device to display the Send to Email Options screen.

To allow the device user to open the Options screen, set [Options] on the basic settings screen.

Send to Email Options screen

Divide Email

Specify how to divide an e-mail.

- Do Not Divide

  All scanned documents are sent in one e-mail.

- Page Divide

  Each page of a scanned document is attached as a file and separately sent.

Notification

Specify whether or not to send a notification e-mail when the recipient opens the e-mail. Select [On] to send a notification e-mail to the logged-in user. This setting is valid only when the destination e-mail server supports the notification e-mail function.

If the e-mail address of the logged-in user cannot receive the notification e-mail, it is sent to the e-mail address specified by the administrator.

Priority

Select the priority assigned to the e-mail.

- None
- 1 (High)
- 2
- 3 (Standard)
- 4
- 5 (Low)

Sensitivity

Select the sensitivity assigned to the e-mail. The sensitivity is added in the e-mail header when you select a setting other than [Normal].

- Normal
- Personal
- Private
- Company-Confidential

Send to RightFax

Selected Destinations

This displays the number of selected fax numbers and e-mail addresses and the actual fax numbers and e-mail addresses.

Press [Selected Destinations] to display the selected destinations list screen.

Private, Public

This switches the phonebook to be searched between [Private] and [Public].

Search

This searches for destination fax numbers and e-mail addresses from the phonebook, and displays the search results in a list. It searches for all fax numbers and e-mail addresses that contain the search keyword.

The procedure for adding destinations is the same as that for Send to Email.

Manual Entry

This displays the text input screen for entering a fax number or e-mail address.

The procedure for adding destinations is the same as that for Send to Email.

You can omit the hyphens and parentheses in the fax number.

Recent Destinations

This displays the 10 most recent fax numbers or e-mail addresses from the sent history for the same user in the Search Results list. Press the fax numbers or e-mail addresses to specify the destinations.

Search results list

This displays the fax number or e-mail address search results.

Account, Matter

Specify the Cost Center.

Note

- The setting names of Account and Matter vary according to the RightFax server settings.

Cover Sheet File

Select the file of a cover sheet to be attached to faxes. When you select [System Default], the file "FCS.pcl." is used as the cover sheet.

Fine Mode

Select this check box to send the fax in fine mode. The resolution of fine mode is 200 x 200 dpi.

Clear this check box to send the fax in standard mode. The resolution of standard mode is 100 x 100 dpi.

From Name

Enter up to 59 characters for the sender's name to be printed on the fax coversheet.

Priority

Specify the priority to be assigned to the fax.

Hold for Preview

Specify whether or not to hold the fax for previewing before sending.

Phonebook Entry

Select this to add a destination in the phonebook on the RightFax server.

Adding a Destination in the Phonebook

ID

Enter the ID of the destination to be added. If you do not enter an ID, the string entered in Name is automatically entered here.

Name

Enter the name of the destination to be added.

Company

Enter the company name.

Address

Enter the mailing address.

City/State

Enter the state and city names.

Destination

Select [Fax] or [Email] for the destination type.

Fax Number 1, Fax Number 2

Enter the main and secondary fax numbers. When Destination is set to [Fax], enter a main fax number.

Email Address

Enter the e-mail address. When Destination is set to [Email], enter an e-mail address.

Voice Number 1, Voice Number 2

Enter the main and secondary voice numbers.

Result

Press [Add] to display the entered destinations.

Clear

Press this to clear the entered destinations and input results and return the items to their default values.

Published

Specify whether or not to publish this destination.

Read Only

Specify whether or not to make this destination read-only.

Add

Press this to add the entered destinations to the phonebook.

Send to Gmail

Selected Destinations

This displays the number of selected e-mail addresses and the actual e-mail addresses. Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of the destination e-mail addresses on the Selected Destinations screen. Click [Reset All] to remove all selected e-mail addresses.

To, Cc, Bcc

From the drop-down list, select the destination type of the destination e-mail address.

Search

For the Personal Contact List, it searches for all e-mail addresses that contain the search keyword. Search is performed on contact names, contact e-mail addresses and personal group names of proxy or logged-in user e-mail addresses. Search by regular expression is not supported.

For the G Suite Directory, it searches on individual contact entries in the directory but not group entries. Search is performed against G Suite Directory individual contact names and e-mail addresses.

Manual Entry

Enter an e-mail address manually.

Note

- To use this function, select [Enable Manual Address Entry] under [Send to Gmail Option Settings] on the properties screen of the Send to Gmail connector. For details about the setting, see page 691 "Send to Email".
- In [Default Domain for Manual Input] under [Send to Gmail Option Settings] on the properties screen of the Send to Gmail connector, enter a domain name to be added to the e-mail address entered without a domain name. This is useful when the recipient is using the same domain.

Subject

You can specify a different subject for each language selected from the drop-down list

You can use the metadata in the scanned file as the subject, except "resultURL".

Note

- For details about metadata items, see page 348 "Metadata".

Send to Google Drive

Selected Destinations

This displays the entered or selected folder.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of a destination folder on the Selected Destinations screen. Click [Reset All] to remove all selected folders.

Search

This searches folders. It searches all folders that contain the search keyword.

When you only enter a space or leave the field blank, it searches for all folders.

Folder View

This closes the search screen and returns you to the folder list.

Root

This displays the root folder. This item is valid only when a subfolder is displayed.

Folder browser icons

Select a folder to be added to the Selected Destinations list.

The functions of the browser icons are as follows

- 

  Displays the subfolder(s) of the selected root folder.
- 

  Displays the folder one layer up. This item is valid only when a subfolder is displayed.

Send to Dropbox

Selected Destinations

This displays the entered or selected folder.

Click [Selected Destinations] to display the Selected Destinations screen. You can select or cancel selection of a destination folder on the Selected Destinations screen. Click [Reset All] to remove all selected folders.

Search

This searches folders. It searches all folders that contain the search keyword.

When you only enter a space or leave the field blank, it searches for all folders.

Folder View

This closes the search screen and returns you to the folder list.

Root

This displays the root folder. This item is valid only when a subfolder is displayed.

Folder browser icons

Select a folder to be added to the Selected Destinations list.

The functions of the browser icons are as follows

- 

  Displays the subfolder(s) of the selected root folder.
- 

  Displays the folder one layer up. This item is valid only when a subfolder is displayed.

[Process] Tab

Specify the setting items of the [Scan Settings] screen, [Scan Size] screen, and process connector on the operation panel of the device.

Scan Settings

Resolution

Specify the resolution to be displayed as the default on the operation panel of the device from the followings: [100 dpi], [200 dpi], [300 dpi], [400 dpi] or [600 dpi].

Note

- The standard resolution setting is 200 dpi. If the resolution is higher, images are clearer and the file size is larger.

Scan Type

Select the scan types to be displayed on the operation panel of the device from the followings:

- Auto Color
- Black & White: Text
- Black & White: Text/Photo
- B & W : Text/Line Art
- Black & White: Photo
- Gray Scale
- Full Color: Text/Photo
- Full Color: Glossy Photo

Note

- Select only one of these scan types (black-and-white, gray scale, or full color) per scan.
- Depending on the device, [Auto Color Select] may not be available.
- Select [Auto Color Select] to determine the color (black-and-white or color) of the original automatically during scanning. When color is specified for the document, a JPEG file is generated. When black-and-white is specified for the document, a TIFF file is generated.
- [File Format] (Black & White, Grayscale/Color) may not appear correctly on the operation screen of the device if you select only one check box in [Scan Type]. To display the setting correctly, select more than one check box on the properties screen of [Scan Type], and then select [Scan Type] on the scan settings screen of the device again. [File Format] is then correctly switched. To specify only one selection item available for [Scan Type], clear the check boxes of unnecessary properties while the correct file format is displayed on the operation screen of the device.

File Format

RICOH Streamline NX supports various file formats.

The file formats are divided into the display and hidden groups to simplify the [Black & White] and [Gray Scale/Color] drop-down lists. To add a hidden format to the display list, right-click the [Black & White] or [Gray Scale/Color] drop-down list. The available settings appear on the screen.

Select or clear the check box of the file format if you want to use or do not want to use it respectively. The selected file formats appear automatically in the drop-down list on the settings screens of both the Management Console and the operation screen of the device.

Note

- For details about selectable file formats, see page 680 "Supported File Formats".

Original Orientation

When scanning an original using the ADF, specify [Portrait] or [Landscape] for the orientation of the original placed in the ADF.

Note

- When you are using Smart Operation Panel, the setting appears as [Portrait/Readable] or [Landscape/Unreadable] on the operation screen of the device.

Original Settings

Specify [1 Sided] or [2 Sided] for the number of scanning sides on the original.

When the original is scanned using the ADF, specifying the number of sides of the original and how the original opens can enable scanning with the correct orientation.

When [2 Sided] is selected, specify [2-Sided (Top to Top)] or [2-Sided (Top to Bottom)]. When the page closing position is on the side, specify [2-Sided (Top to Top)]. When the page closing position is at the top, specify [2-Sided (Top to Bottom)].

Density

Specify the scan density.

When [Auto Density] is selected, the color of the paper is automatically detected, and the scan density is corrected for originals that are off-white or have show-through, such as a newspaper, to improve the scanned image quality.

To adjust the image density, select the density level from the drop-down list next to [Auto Density].

Scan Method

Specify the scan method.

- ADF/Exposure Glass

  Scans the original from the ADF or exposure glass.

- Scan Method

When using the Smart Operation Panel

You can scan a large volume original from the ADF or exposure glass and send them all at once.

Set the additional originals, and then press [Continue] to start the scan.

The device waits until additional originals are placed. After all originals are scanned, press [Finish].

When using the Standard Operation Panel

You can scan a large volume original in multiple jobs and send them all at once.

Set the additional originals, and then press [Start] to start the scan. The device waits until the additional originals are placed. After all originals are scanned, press #.

- Mixed Batch

  Scans multiple originals from the ADF or exposure glass and sends the originals all at once. To scan additional originals, press the [Start] key, and after all originals are scanned, press #.

  This item only appears on the Standard Operation Panel.

- SADF (Semi-Automatic Document Feeder)

  Scans a large volume original in multiple jobs and sends them all at once. When additional originals are placed in the ADF, scanning starts automatically. After all originals are scanned, press #.

Note

- When the maximum document size exceeds the internal memory of the device, the document is not sent.
- When [Mixed Batch] is selected and the original is placed both in the ADF and on the exposure glass, the ADF has priority.
- Wide format devices do not support [Mixed Batch].
- A confirmation screen appears for each sheet of the scanned original when the preview function is used.

Reset

Resets the values on the [Scan Settings], [Scan Size], and [OCR Scanned PDF] tabs on the Standard Operation Panel, or [Scan Settings] and [Scan Size] screens on the Smart Operation Panel to their defaults.

Supported File Formats

File formats shown below are supported.

When a black and white option is selected for [Scan Type]

- BMP (uncompressed)

- PNG
- GIF
- PDF (multi-page/single page)
- PDF/A (multi-page/single page)
- OCR Scanned PDF (multi-page)
- TIFF (MMR, multi-page/single page)
- TIFF (MR, multi-page/single page)
- TIFF (MH, multi-page/single page)
- TIFF (uncompressed, multi-page/single page)
- TIFF-F (MMR, multi-page/single page)
- TIFF-F (MR, multi-page/single page)
- TIFF-F (MH, multi-page/single page)
- DCX (multi-page/single page)

Note

- Workflows that process jobs on the device support the following file formats:
  - TIFF (MMR, multi-page/single page)
  - PDF (multi-page/single page)
  - PDF/A (multi-page/single page)
  - OCR Scanned PDF/A (multi-page)

When a gray scale or full-color option is selected for [Scan Type]

- JPEG
- BMP (uncompressed)
- PNG
- GIF
- PDF (multi-page/single page)
- PDF/A (multi-page/single page)
- OCR Scanned PDF (multi-page)
- High Compression PDF (multi-page/single page)
- High Compression Searchable PDF (multi-page)
- TIFF (uncompressed, multi-page/single page)

Note

- Workflows that process jobs on the device support the following file formats:
  - JPEG

- PDF (multi-page/single page)
- PDF/A (multi-page/single page)
- OCR Scanned PDF/A (multi-page)
- High Compression Searchable PDF (multi-page)

Scan Size

Scan Size

From the drop-down list, select the scan sizes and methods for size detection to be displayed on the operation panel of the device.

- Auto Detect

  Detects the size of the original automatically. Also, this detects the size of the first page of the original and applies the same size to all remaining pages.

- Mixed Sizes

  Detects the size of each page of the original that contains mixed page sizes.

- Custom Size 1/Custom Size 2

  Displays defined custom sizes. For details about how to define a custom size, see page 302 "Customizing [Scan Size]".

- Other scan sizes

  Select the size of the original from the size list.

  A3 Landscape, A4 Portrait, A4 Landscape, A5 Portrait, A5 Landscape, A6 Portrait, A6 Landscape, B4 JIS Landscape, B5 JIS Portrait, B5 JIS Landscape, 11 x17 Landscape, 11 x 17 Portrait, 8 1/2 x 14 Landscape, 8 1/2 x 14 Portrait, 8 1/2 x 13 Landscape, 8 1/2 x 11 Portrait, 8 1/2 x 11 Landscape, 5 1/2 x 8 1/2 Portrait, 5 1/2 x 8 1/2 Landscape, A0 Portrait, A0 Landscape, A1 Portrait, A1 Landscape, A2 Portrait, A2 Landscape, A3 Portrait, B1 JIS Landscape, B1 JIS Portrait, B2 JIS Portrait, B2 JIS Landscape, B3 JIS Portrait, B3 JIS Landscape, B4 JIS Portrait, 625 x 880 mm Landscape, 625 x 880 mm Portrait, 880 x 1189 mm Portrait, 880 x 1189 mm Landscape, 36 x 48 Portrait, 36 x 48 Landscape, 34 x 44 Portrait, 34 x 44 Landscape, 24 x 36 Portrait, 24 x 36 Landscape, 22 x 34 Portrait, 22 x 34 Landscape, 18 x 24 Portrait, 18 x 24 Landscape, 17 x 22 Landscape, 12 x 18 Portrait, 12 x 18 Landscape, 9 x 12 Portrait, 9 x 12 Landscape, 30 x 42 Portrait, 30 x 42 Landscape

Note

- Depending on the device, [Auto Detect] and [Mixed Sizes] may not be available.

OCR Scanned PDF

OCR Language

Select the language to be used for OCR.

- English
- German
- French
- Italian
- Spanish
- Dutch
- Portuguese
- Norwegian
- Danish
- Polish
- Swedish
- Finnish
- Hungarian
- Japanese

Remove Blank Pages

This removes unnecessary blank pages from the scanned original that comprises multiple pages.

This function is useful for scanning a document with mixed one-sided and two-sided originals.

- Yes
- No

Blank Page Sensitivity

Specify the threshold value for the original to be detected as blank.

- Level 1 (only pure white is blank)
- Level 2
- Level 3
- Level 4
- Level 5 (dirty paper is blank)
- Link to Device Settings

PDF Converter

Create Searchable PDF

You can create a searchable PDF with embedded text.

Select [Yes] to extract text data from the document and converts it to a searchable PDF file.

Select the language to be used during text extraction from the drop-down list.

- English
- German
- French
- Italian
- Spanish
- Dutch
- Danish
- Portuguese
- Norwegian
- Russian
- Simplified Chinese
- Traditional Chinese
- Brazilian Portuguese
- Japanese
- Swedish*1
- Polish*1
- Hungarian*1
- Czech*1
- Finnish*1
- Thai*1
- Greek*1
- Korean (Hangul) *1
- Catalan*1
- Turkish*1
- Arabic*1
- Hebrew*1
- Vietnamese*1

*1 This language is not displayed by default. To display, right-click the drop-down list and select the check box of the language to be displayed on the screen for specifying the language to be shown or hidden.

Select [No] to convert the scanned document to a PDF file that does not include the text data.

Assign a User Password

You can create a PDF file that prompts the user to enter a password when opening the file.

When you select [Yes], enter a password.

You can enter a password up to 32 characters.

Usable characters include alphanumeric characters and the following symbols:

^,[,!,-,~,],*,$

Assign a Master Password

By assigning a password to a PDF file, you can restrict printing and editing of the file and copying of text and images.

You can enter a password up to 32 characters.

Usable characters include alphanumeric characters and the following symbols:

^,[,!,-,~,],*,$

When you select [Yes], enter a master password. You can restrict usage of the functions selected from the following [Prohibit] items:

- Print
- Modify
- Copy/Extract

Important

- **Specify a different password for the user password and master password. An error occurs if you specify the same password.**

Configuring the attributes of the password specified for a password-protected PDF

Double-click the password text box for either [Assign a User Password] or [Assign a Master Password] to configure the attributes of the password to be assigned to the password-protected PDF. Click [OK] after the configuration is completed.

Item	Description
Min. Characters	This is the minimum number of characters required for a password. Specify a value from 0 to 32.

Item	Description
Regex for Validation	This regex is used to check the string configured as a password. **Note** • [^[!-~]*$] is specified by default. This indicates that half-width alphanumeric characters and symbols can be entered for a password. Use this setting unless otherwise required. An unreadable PDF file may be generated if the password contains a double-byte character.
Retype	Specify whether or not to enable the confirmation entry of a password (repeat entry) to prevent input errors. When this check box is selected, enter the password twice when performing a scan.

OCR

OCR Language

Select the language to be used for OCR.

- English
- German
- French
- Italian
- Spanish
- Dutch
- Danish
- Portuguese
- Norwegian
- Russian
- Simplified Chinese
- Traditional Chinese
- Brazilian Portuguese
- Japanese

Auto Orientation

Select this check box to detect and adjust the orientation of the scanned original automatically according to the OCR result.

Section Specify

Section Range

Specify the section to be extracted from the scanned document.

Examples

To specify a section to be extracted, enter a number in the field beside the item.

The following table shows examples of the specification range of a document comprising five sequential sections and the extraction results.

Input example	Result
No input	All sections are extracted.
3	Section 3 is extracted.
-3	Sections 1 to 3 are extracted.
3-	Sections 3 and thereafter are extracted.
1-4	Sections 1 to 4 are extracted.
1,2	Sections 1 and 2 are extracted.
1-2, 5	Sections 1, 2, and 5 are extracted.
(1,2)	Every other section starting from section 1 is extracted (sections 1, 3, and 5).
(2,3)	Every third section starting from section 2 is extracted (sections 2 and 5).
(2,2), 4	Every other section starting from section 2 is extracted (sections 2 and 4). **Note** • Here, section 4 is specified two times, but it is only extracted one time.
8-10	An error occurs, and the document is not delivered.
1-5, 10-	Sections 1 to 5 are extracted. "10-" is ignored, as there are no corresponding sections.
3-8	Sections 3 to 5 are extracted. "6-8" is ignored, as there are no corresponding sections.
5-1	Sections 1 to 5 are extracted.
0-5	Sections 1 to 5 are extracted.

Input example	Result
(0,2)	Every other section is extracted starting at zero (sections 2 and 4).

Section Splitter

Number of Sections

Specify the number of sections to be created by dividing the scanned original.

Image Correction

Noise Reduction (Black & White image only)

This removes noise on the scanned original.

Note

- When using the Smart Operation Panel:
  When [Scan Type] is specified on the Scan Settings tab is Gray Scale or Full Color, this function is disabled.
- When using the Standard Operation Panel:
  When [File Type] is specified on the Scan Settings tab is [Grayscale/Color], this function is disabled.

Remove Punch Holes (Black & White image only)

This removes punch hole marks from the scanned original.

Note

- When using the Smart Operation Panel:
  When [Scan Type] is specified on the Scan Settings tab is Gray Scale or Full Color, this function is disabled.
- When using the Standard Operation Panel:
  When [File Type] is specified on the Scan Settings tab is [Grayscale/Color], this function is disabled.
- Nothing is removed if a punch hole mark is missing or only an outline is present.
- The supported combinations of the number of holes, distance between holes, and the paper size are as follows:

Number of holes	Distance (mm) between holes	Paper Size
2	80	A3, A4, A5, B4, B5, B6

Number of holes	Distance (mm) between holes	Paper Size
3	10	8 1/2 x 1 inches, A4
	89	7 x 9 inches
	70	6 1/3 x 8 1/2 inches
4	57	B5
	80	A4
	20, 70	A4

Remove Blank Pages

This removes unnecessary blank pages from the scanned original that comprises multiple pages.

This function is useful for scanning a document with mixed one-sided and two-sided originals.

Note

- This function is also effective when sheets of single-color paper are included in the original.

Deskew

This corrects image skew in the scanned original.

Note

- White margins may be added around the deskewed image.
- Skew angles between -7° and 7° can be corrected.

Auto Orientation

This identifies the top and bottom of the scanned original and adjusts the orientation of the image.

Note

- It can correct originals rotated by 90°, 180°, or 270°.

Change Resolution

This changes the resolution of the scanned image to the specified value.

You can change the resolution only when either the vertical or horizontal resolution of the image data is higher than the specified resolution.

However, resolution change occurs when the following conditions are fulfilled:

- The horizontal and vertical resolutions of the image data differ.
- [Yes] is selected for one or more of the image correction functions (noise reduction, punch hole removal, blank page removal, deskew, and auto orientation) other than resolution change.

Note

- You can specify a resolution from 100, 200, 300, 400, or 600 dpi.
- The resolution of the scanned original does not change if it is lower than the specified resolution.
- The vertical and horizontal resolutions of the output image data become equal when the resolution changes.

Setting Items in the Destination Connector Properties

Configure the properties for each destination connector.

Display Name

Specify the display name for each destination connector on the operation screen of the device.

Select a language from the drop-down list, and specify the display name for each language.

Send to Email

Email System Settings

SMTP/SMTPS

Select the security method to be used when connecting to the SMTP server.

- No Security

  The communication data is not encrypted.

- SMTPS (SMTP over SSL)

  SSL is used to encrypt the communication data and protect security of the connection to the SMTP server.

  You must register the certificate to be used on the system in advance. Otherwise, an error occurs when an e-mail is sent. For details about registering a certificate, see page 403 "Enabling SSL".

- SMTPS (StartTLS)

  TLS is used to encrypt the communication data and protect security of the connection to the SMTP server.

  The SMTP server to be used must support StartTLS. Otherwise, an error occurs when an e-mail is sent.

SMTP Server Name

Enter the IP address or hostname of the SMTP server.

Click [Test] to check the connection to the SMTP server that has been entered. Does not perform authentication tests using the user name and password.

SMTP Port No.

Enter the port number to be used.

Note

- SMTP and SMTPS port numbers are 25 and 465 by default respectively.

Authentication Method

Specify the authentication method to be used.

- No Authentication

  No authentication is performed.

- SMTP Authentication

  The SMTP server is used to perform authentication. Enter the account information in [User Name] and [Password] to perform authentication.

- POP Before SMTP

  The POP server is used to perform authentication. Enter the POP server information in [POP Server Name] (IP address or host name) and [POP Port No.] (default is 110), and the account information in [User Name] and [Password] to perform authentication.

  Click [Test] to check the connection to the POP server that has been entered. Does not test authentication using the user name and password.

  Note

  - The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Login Information

When you are using [SMTP-AUTH] or [POP before SMTP] for the authentication method, select the type of account to be used for logging in to the SMTP server.

- Proxy User

  The login information entered for the user name and password is used for authentication.

- Login User

  The login information of the workflow is used for authentication.

Send to Email Option Settings

Default Sender Address

Enter the e-mail address of the default sender.

If the e-mail address of the logged-in user cannot be obtained, this e-mail address is set as the sender.

When Kerberos or LDAP authentication is used, the e-mail address obtained from the login information of the workflow is set as the sender. In [User Management] on the Management Console, register the e-mail address of the login user in advance.

When you select the [Always Use Default Sender Address] check box, the system uses the sender's e-mail address specified in the default sender address setting even when the user's e-mail address is obtained from the authentication server.

Select Data to Attach

Specify how to attach the data to e-mails.

- Attach All
- Attach First Page Only
- Do Not Attach

Note

- In the workflows that process jobs on the device, the setting is fixed at [Attach All].

File Naming Rules

Specify the name to be given to the attached file.

Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata to use for the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Attach Document Link(s) and Deliver

Specify whether or not to include the URL that indicates the save location of the distributed document in the e-mail.

- On

  The URL is added to the body of the e-mail.

- Off

  The URL is not included in the e-mail.

Note

- To use this setting, add at least one of the following connectors before the Send to Email connector in the delivery flow: Send to Folder connector, Send to FTP connector, Send to WebDAV connector, Send to SharePoint connector, and Send to Document Mall connector.
- For details about how to create the URL that points to the document save location when the Save to Folder connector is used, see the StartPoint Path setting of the Send to Folder service.

Body

Enter the body of the e-mail to be sent.

You can specify a different body text for each language selected from the drop-down list

You can also use the metadata elements in the scanned file except "resultURL" can as the body text. For details about metadata items, see page 348 "Metadata".

Send to Me

Specify whether or not to add the logged-in user automatically to the Selected Destinations list.

- On

  When the e-mail address of the logged-in user can be retrieved from the login information of the workflow, the string "Send to Me" is automatically added to the "To" field in the Selected Destinations list.

  The system can retrieve the e-mail address of the logged-in user when LDAP/Kerberos authentication is used as the workflow authentication method.

  When the Core Server cannot obtain the e-mail address or the user's e-mail address is not registered, the [Send to Me] button is displayed on the operation screen of the device, while a copy of the e-mail is not sent to the login user.

- Off

  The e-mail address of the logged-in user is not added to the Selected Destinations list.

Default Domain for Manual Input

Enter the default domain name to be automatically added to the e-mail address that is entered manually.

Example

Default domain: ABCCorp.com

User input: john

Generated e-mail address: john@ABCCorp.com

Note

- "@" is automatically entered.
- The default domain is not added if the logged-in user entered an e-mail address including a domain name.

Option Settings

Select the items that are optional.

- Show Cc

  The user can enter an e-mail address in the CC field.

- Show Bcc

  The user can enter an e-mail address in the Bcc field.

- Show ReplyTo

  The user can enter the ReplyTo e-mail address.

- Enable Manual Address Entry

The user can enter an e-mail address manually.

- When using the Smart Operation Panel:

  When [Enable Manual Address Entry] is disabled, [Manual Entry] is not displayed on the Send to Email destination adding screen.

- When using the Standard Operation Panel:

  When [Enable Manual Address Entry] is disabled, [Manual Entry] on the Send to Email screen is grayed out.

- Enable Address Validation

  When entering an e-mail address manually on the operation screen of the device or sending scan data, use the following rules to verify the format of the e-mail address:

  - Do not use spaces, colons, or other prohibited characters
  - Use only one @ symbol
  - Do not use a period (.) at the end of the e-mail address
  - Include the top level domain
  - Do not use non-alphanumeric characters in the top level domain
  - Do not use a period (.) in the top level domain

Note

- While the format of the e-mail address is verified, the domain and e-mail address are not verified.
- An error message is displayed if the format of the e-mail address is invalid.

Email Search Settings

Enable Address Search

Select this to allow the logged-in user to search for e-mail addresses in the address book of the LDAP server.

LDAP/LDAPS

Select the security method to be used when connecting to the LDAP server.

- No Security

  The communication data is not encrypted.

- LDAPS (LDAP over SSL)

  SSL is used to encrypt the communication data and protect security of the connection to the LDAP server. You must register the certificate to be used on the system in advance. Otherwise, an error occurs when the address book is retrieved.

- LDAPS (StartTLS)

TLS is used to encrypt the communication data and protect security of the connection to the LDAP server. The LDAP server to be used must support StartTLS. Otherwise, an error occurs when the address book is retrieved.

LDAP(S) Server

Enter the IP address or hostname of the LDAP server. Click [Test] to check the connection to the LDAP server that has been entered. Performs authentication tests using the entered user name and password.

LDAP(S) Port No.

Enter the port number to be used.

Authentication Method

Select the type of account to be used for logging in to the LDAP server.

- Proxy User

  The system uses the login information entered in [User Name] and [Password] is used for authentication.

- Login User

  The login information of the workflow is used for authentication.

  To browse the address book using the Management Console when selecting [Login User], enter [User Name] and [Password].

- No Authentication

  No authentication is performed.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

LDAP Base DN

Specify the identifier (DN) of the node in the directory tree to be searched.

Setting example

cn=users, dc=ricoh, dc=co, dc=jp

Address Search Settings

Specify the search condition in the address book.

LDAP Search Condition

Specify the LDAP Search Condition when you only enter a space or enter no character at all, the system searches the entire address book.

The default setting is as follows:

(&(objectclass=organizationalPerson)(cn=*^s*)(mail=*))

Replace "^s" with the search keyword.

The maximum number and range of characters, and input condition that can be specified in LDAP Search Condition are as follows:

Search condition	Maximum number of characters or input range	Input condition
LDAP(S) Server	1,000 characters	None
LDAP(S) Port No.	1–65535	Integer only
User Name	1,000 characters	None
Password	1,000 characters	None
LDAP Base DN	1,000 characters	None
LDAP Search Condition	1,000 characters	None
Display Name	1,000 characters	None
Address Format	1,000 characters	None

Example

- When using the wildcard character "*" to modify the search condition
  1. The following examples match the search condition when you specify cn=*les*.
     - charles smith
     - lester frank
     - Lorraine Lester
     - Steven Morales

     The system searches for all names that contain the search keyword ("les").
  2. The following examples match the search condition when you specify cn=les*.
     - lester frank
     - Lester, lorraine

     The system searches for all names that contain a string starting with the search keyword("les").
  3. The following examples match the search condition when you specify cn=*les.
     - Smith, charles
     - steven morales

     The system searches for all names that contain a string ending with the search keyword ("les").

Note

- Up to 50 LDAP search results are displayed in the Management Console, and up to 1,000 LDAP search results are displayed on the operation screen of the device.

Display Name

Specify the LDAP attribute for the display name of each item to be displayed when searching for an e-mail address. To specify more than one LDAP attribute, separate each attribute by a comma (,).

The default is "cn" (common name).

Example

sn, givenName, mailaddress

Address Format

Specify the LDAP attribute to be used for displaying the e-mail addresses in the search results.

The default is "mail".

Send to Folder

Adding and Deleting StartPoint Path

Add, Edit, Delete

Use these to add a new root folder, edit an existing root folder, and delete a root folder.

- Add

  Adds a new root folder. The StartPoint Path screen appears.

- Edit

  Changes the setting of the selected root folder. The StartPoint Path screen appears.

- Delete

  Deletes all selected root folders.

Root Folder List

Displays the list of root folders that are registered.

Select the check box of the root folder to be edited or deleted.

To select all root folders, select the check box in the first line or row.

StartPoint Path - General Settings

Display Name

Specify the display name of the folder.

Path

Enter the path name of the destination folder in the UNC format. You can specify any folder included in the entered path name as the destination.

Example

\\192.168.1.1\shared-folder-name

Note

- You can specify a local folder as the destination folder. Use an absolute path of each platform to enter a local folder.
  Example: Windows
  C:\local-folder-name

Click [Test] to check the connection to the folder that has been entered.

In the connection test, authentication is performed using the entered user name, password, and domain, and the authentication method selected in [Authentication Method] is ignored.

Enable enhanced SMB protocol

Select this check box to switch to Send to Folder, which uses the JCIFS library and Windows API. The function will then support the SMB 3.0 protocol.

This check box is displayed only when the connector is processed on the server.

Note

- For SMB 3.0 + protocol support, .NET Framework 4 or later needs to be installed on server PC where the Send to Folder connector is installed and executed.

Authentication Method

Specify the authentication method to be used.

The system uses the information specified here when accessing the destination folder and saving the scanned document.

- Proxy User

  The system uses the login information specified in [User Name], [Password], and [Domain] for authentication.

- Login User

  The login information of the workflow is used for authentication.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.
- To browse the address book using the Management Console when selecting [Login User], enter [User Name] and [Password].

- In the Send to Home Folder function, the system uses the login information of the workflow to distribute the scanned documents to the folder of the logged-in user even if [Proxy User] is selected.

Authentication Profile

Select an authentication profile. When an authentication profile is selected, the user must enter the password to use Send to Folder on the operation screen of the device.

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Naming Rules

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Enter the folder name manually.
- From the drop-down list, select the metadata element to be used as the folder name.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved in the destination folder.

Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata element to be used as the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".
- If a file with the same name already exists, a suffix is added to the file name. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

Create URL

Select the [Create URL Using Base URL] check box to create an URL that indicates the location to store the scanned file.

The metadata of the URL is added to the "resultURL" metadata element.

Example

StartPoint Path: \\192.168.1.1\targetPath

Destination folder: \\192.168.1.1\targetPath\myfolder

File name: doc.tif

Base URL: http://samplemyurl.com/path1

Resulting URL: http://samplemyurl.com/path1/myfolder/doc.tif

Note

- If you select the [Enable Subfolder Delivery] check box, the URL of the created subfolder is added to the "resultURL" metadata element. If you select the [Enable Subfolder Delivery] check box, all sections (files) in the scanned document are added to the "resultURL" metadata element.
- When this check box is cleared, a URL that indicates the location where the scanned document is stored using the StartPoint Path.

Example

StartPoint Path: \\192.168.1.1\targetPath

Destination folder: \\192.168.1.1\targetPath

\myfolder

File name: doc.tif

Resulting URL: \\192.168.1.1\targetPath\myfolder\doc.tif

Character Encoding for File (Folder) Name

Select a character code from the drop-down list.

The following character codes are supported:

- UTF-8
- Windows Shift-JIS (Only in Japan)
- JIS (Only in Japan)

- Latin -1

Note

- [JIS] is only displayed for workflows processing jobs on a server.
- If the file server at the delivery destination does not support the specified character code, either delivery fails or a file (folder) is created with corrupt characters.

Check Writable Access Rights

Select the [Enable when selecting destinations on the device panel] check box to check whether the user has the permission to access the destination on the operation screen of the device when distributing a document.

Send to Home Folder

Send to Home Folder

Select the [Enable Send to Home Folder] check box to allow a user to distribute a scanned document to the user's home folder using the user's login information.

The string “Send to Home Folder" is automatically added to the default destination list if the system has succeeded in obtaining the user's home folder information from the authentication server.

After a home folder is configured for each authentication method, all home folders are added to Selected Destinations on the device.

Also, select Proxy User in the authentication method to send the document as a different user.

A distribution error occurs when the user does not have the write access permission to the home folder.

Access to Subfolder

See page 698 "StartPoint Path - General Settings".

Create a Subfolder

See page 698 "StartPoint Path - General Settings".

File Naming Rules

See page 698 "StartPoint Path - General Settings".

Create URL

See page 698 "StartPoint Path - General Settings".

Character Encoding for File (Folder) Name

See page 698 "StartPoint Path - General Settings".

SMB 3.0 Support

See page 698 "StartPoint Path - General Settings".

Authentication Method

See page 698 "StartPoint Path - General Settings".

Send to FTP

Adding and Deleting StartPoint Path

Add, Edit, Delete

Use these to add a new root folder, edit an existing root folder, and delete a root folder.

- Add

  Adds a new root folder. The StartPoint Path screen appears.

- Edit

  Changes the setting of the selected root folder. The StartPoint Path screen appears.

- Delete

  Deletes all selected root folders.

Root Folder List

Displays the list of root folders that are registered.

Select the check box of the root folder to be edited or deleted.

To select all root folders, select the check box in the first line or row.

StartPoint Path - General Settings

Display Name

Enter the display name of the root folder.

URL

Enter the URL of Send to FTP

Example

- ftp://ftp.rgscorp.net/
- ftp://192.168.1.1:21/home/user/
- sftp://ftp.rgscorp.org/data/ (when using SFTP)

Click [Test] to check the connection to the URL that has been entered.

In the connection test, authentication is performed using the entered user name, password, and domain, and the authentication method selected in [Authentication Method] is ignored.

Authentication Method

Specify the authentication method to be used.

- Proxy User

  The system uses the login information specified in [User Name] and [Password] for authentication. When you are using IIS, enter the user name in the form of "<domain>\<user-name>" in [User Name].

- Login User

  The login information of the workflow is used for authentication.

- Use Certificate

  A certificate is automatically selected from the registered certificates. For details about registering a certificate, see page 403 "Enabling SSL". Specify the following:

  - User Name
  - Password

    Enter the password of the private key file.

  - Private Key File

- Anonymous

  You may be prompted to enter the password depending on the settings of the FTP server. Enter the password in the input field if the FTP server is configured to require a password for anonymous authentication. If the password is not required, leave the input field blank.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.
- The system supports the private key in SSH DSS and SSH RSA.
- OpenSSH is supported.
- Key generation using PuTTYgen is not supported.
- When the firewall of the server is active, set the FTP server of the delivery destination to passive mode. Otherwise no connection can be established.

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Naming Rules

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Enter the folder name manually.
- From the drop-down list, select the metadata element to be used as the folder name.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved on the FTP server.

Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata element to be used as the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".
- If a file with the same name already exists, a suffix is added to the file name. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

Character Encoding for File (Folder) Name

Select a character code from the drop-down list.

The following character codes are supported:

- UTF-8
- Windows Shift-JIS (Only in Japan)
- JIS (Only in Japan)
- Latin -1

Note

- [JIS] is only displayed for workflows processing jobs on a server.

Send to Printer

Header/Footer Print Settings

Header/Footer Settings 1, Header/Footer Settings 2

Configure the header and hooter.

Select the check box of the setting to be used, and then specify the following:

Position

Select the position of the header and footer from [Top Left], [Top Center], [Top Right], [Bottom Left], [Bottom Center], and [Bottom Right].

Embedded String

Specify the method to specify the string in the header and footer.

- Select [Edit Embedded String] to enter the string in the header and footer manually.
- From the drop-down list, select the metadata element to be used when the document is printed.

Note

- You cannot select the same position for [Header/Footer Settings 1] and [Header/Footer Settings 2].

Range

Specify the range of pages to embed the header and footer.

- All

  Select this to embed the header and footer in all pages.
- Specify Page

  Specify the [Start] and [End] pages of the page range to embed the header and footer.

Page Setup

Paper Size

Specify the method for selecting the paper size.

- Comply with printer driver settings

  The paper size specified in the printer driver is selected.
- Auto select paper to fit image size

An appropriate paper size is automatically selected according to the image size.

You can select the size system from ISO/JIS and inches.

Send to WebDAV

Adding and Deleting StartPoint Path

Add, Edit, Delete

Use these to add a new root folder, edit an existing root folder, and delete a root folder.

- Add

  Adds a new root folder. The StartPoint Path screen appears.

- Edit

  Changes the setting of the selected root folder. The StartPoint Path screen appears.

- Delete

  Deletes all selected root folders.

Root Folder List

Displays the list of root folders that are registered.

Select the check box of the root folder to be edited or deleted.

To select all root folders, select the check box in the first line or row.

StartPoint Path - General Settings

Display Name

Enter the display name of the root folder.

URL

Enter the path name of the destination folder of Send to WebDAV.

Example

- http://webdav.rgscorp.com/
- http://192.168.1.1:8080/Smith/docs/
- https://webdav.rgscorp.biz/users/Jones (when using SSL)

Click [Test] to check the connection to the URL that has been entered.

In the connection test, authentication is performed using the entered user name, password, and domain, and the authentication method selected in [Authentication Method] is ignored.

When [HTTP Proxy Server] is configured, a connection test is performed using the setting.

Authentication Method

Specify the authentication method to be used.

- Proxy User

  The system uses the login information specified in [User Name] and [Password] for authentication. When using IIS, enter the user name in the form of "<domain>\<user-name>" in [User Name]. Enter up to 14 characters in [Password]. If you enter 15 or more characters, distribution will fail.

- Login User

  The login information of the workflow is used for authentication.

- No Authentication

  No authentication is performed.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Authentication Profile

Select an authentication profile. When an authentication profile is selected, the user must enter the password to use Send to WebDAV on the operation screen of the device.

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Naming Rules

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Enter the folder name manually.
- From the drop-down list, select the metadata element to be used as the folder name.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved on the WebDAV server.

Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata element to be used as the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".
- If a file with the same name already exists, a suffix is added to the file name. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 9999, an error occurs and delivery fails.

Character Encoding for File (Folder) Name

Select a character code from the drop-down list.

The following character codes are supported:

- UTF-8
- Windows Shift-JIS (Only in Japan)
- JIS (Only in Japan)
- Latin -1

Note

- [JIS] is only displayed for workflows processing jobs on a server.

Add StartPoint Path - Assign Metadata Elements

Add, Edit, Delete

You can add a new metadata assignment setting, edit an existing metadata assignment setting, or delete a metadata assignment setting.

- Add

  Creates a new property bind setting. The Add Assigned Metadata Elements screen appears.

- Edit

  Changes the setting of the selected property bind setting. The Add Assigned Metadata Elements screen appears.

- Delete

  Deletes all property bind settings.

Metadata elements assignment list

Displays the list of assigned metadata.

Select the check box of the assignment setting to be edited or deleted. Select the check box on the title column to select all assignment settings.

Add Assigned Metadata Elements - General Settings

Source

Select the metadata element from the drop-down list, or enter the metadata element manually.

Target

Enter the name of the corresponding WebDAV property.

Namespace

Enter the name space of the WebDAV property.

HTTP Proxy Server

IP Address

Enter the IP address or hostname of the proxy server.

Click [Test] to check the connection to the proxy server that has been entered. Does not perform authentication tests using the entered user name and password.

Port Number

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Password

Enter the account password.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Exclusion Setting

Enter the IP address and domain name to be accessed without using the proxy server. Use a semicolon (;) to separate each address.

You can use an asterisk (*) to specify the IP address and domain name classes.

Example

- *.abccorp.com (an address such as www.abccorp.com or ftp.abccorp.com)
- 192.168.*.*
- *.abcsample.* (an address such as ftp.abcsample.net or www.abcsample.biz)

Send to SharePoint

Select Server Type

Connect to SharePoint Server with On-premises Environment

The system recognizes any StartPoint Path as an On-Premises URL. Select this in an environment that uses the SharePoint server only.

Connect to Office365

The system recognizes any StartPoint Path as an Office365 URL. Select this in an environment that uses SharePoint Online (OneDrive for Business) only.

Authentication Method

Specify the authentication method to be used when connecting to Office365.

- Use Alternate Credentials of AD FS 2.0

  The system performs ADF authentication on the logged-in user.

  When the federation domain is not the same as the domain setting of the authentication profile used for logging in to devices, specify the domain name to be mapped in [Domain Name Mapping]. When specifying multiple entries, use semi-colon (;) as a delimiter.

Example

srcDomainName1.com=tgtDomainName1.com;srcDomainName2.com=tgtDomainName2.com

When the domain name of the authentication profile of the user logging in to the device is "domainName1.com", it is replaced with "domainName2.com" which is used for ADFS authentication.

Note

- The format of the user credential for Office365 must be "username@domainname". The local users cannot use [Use Alternate Credentials of AD FS 2.0] because they do not have any associated domains.

- Use Microsoft Account

  The login screen is displayed on the operation screen of the device, and the user must enter the Microsoft Account ID when one or more StartPoint Path that requires the user logging in is configured.

  From the operation screen of the device, specify a domain name in [Selectable Domains on Login Screen] when [Use Microsoft Account] is selected. Use a semicolon (;) to separate domain names.

HTTP Proxy Server

IP Address

Enter the IP address or FQDN of the proxy server.

Click [Test] to check the connection to the proxy server that has been entered. Does not perform authentication tests using the entered user name and password.

Port Number

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Password

Enter the account password.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Exclusion Setting

Enter the IP address and domain name to be accessed without using the proxy server. Use a semicolon (;) to separate each address.

Adding and Deleting StartPoint Path

Add, Edit, Delete

Use these to add a new root folder, edit an existing root folder, and delete a root folder.

- Add

  Adds a new root folder. The StartPoint Path screen appears.

- Edit

  Changes the setting of the selected root folder. The StartPoint Path screen appears.

- Delete

  Deletes all selected root folders.

Root Folder List

Displays the list of root folders that are registered.

Select the check box of the root folder to be edited or deleted.

To select all root folders, select the check box in the first line or row.

StartPoint Path - General Settings

Display Name

Enter the display name of the root folder.

URL

Enter a valid HTTP/HTTP(s) URL of the destination SharePoint site or subsite.

Website Address

Enter the URL of the SharePoint Server or Office 365 SharePoint Online site to be connected.

When publishing a server certificate and specifying SSL (encrypted communication), enter the URL in the format of "https://'(IP address or FQDN name):(port number)/(site name)".

Library and Folder Path

Enter the URL of the SharePoint site library and the subordinate folder to be connected.

Example:

library

library/folder1

Enable SPS Site Selection

The user is prompted to select a site and library when the user selects this check box. If selected, the library and folder path cannot be entered. Also, [Pre-selected Destination] cannot be selected.

Deliver to Login User's My Site

Select this check box to deliver documents to My Site of the logged-in user.

When this check box is selected, you can only select [Login User] in [Authentication Method]. Also, you cannot select [Enable SPS Site Selection]. Specify a library or folder in [Library and Folder Path].

Enter only the server name in [Website Address].

Example:

http://servername

https://servername

Note

- Only the root site of My Site can becomes the StartPoint folder when you select [Deliver to Login User's My Site].
- To distribute documents to My Site of the proxy user, clear this check box and enter the URL of the proxy user's My Site in [Website Address].
- If the [Deliver to Login User's My Site] is selected and the StartPoint folder does not exist for the logged-in user, an error message is displayed on the device's operation panel and the user cannot access the folder. However, when the folder is set as the delivery destination and the specified library exists, the Send to SharePoint connector creates a destination folder using logged-in user credential.

Pre-selected Destination

Select this check box and specify the library and folder to distribute documents to the pre-selected destination. When configuring workflows including this connector for one-touch scan, you must enable the pre-selected destination setting.

When the [Pre-selected Destination] check box is selected, you must specify a library or folder in [Library and Folder Path].

The system uses the selected content type if more than one field is registered, and it uses the default content type and value if no field is registered.

Authentication Method

Select the account type to be used for logging in to the destination Microsoft SharePoint Server or Office 365 SharePoint Online. You cannot select this when [Deliver to Login User's My Site] is specified.

- Proxy User

  The system uses the login information specified in [User Name] and [Password] for authentication.

- Login User

  The login information of the workflow is used for authentication.

User Name

Specify the user name to be used for logging in to the destination Microsoft SharePoint Server or Office 365 SharePoint Online.

- If the server requires the domain information, enter the user name in the format of "domain \username".
- When using MS cloud authentication, specify the user name in the format of "user@domain".

Only when [Connect to Office365] is selected for the server type and [Use Alternate Credentials of AD FS 2.0] is selected for [Authentication], you can specify [User Name] by selecting one of the following attributes:

- Login User Name
- User Email Address
- Custom Property 1 to 10

You can also specify the user name manually in the "user@domain" format.

Password

Enter the password of the user who is logging in to the destination Microsoft SharePoint Server or Office 365 SharePoint Online.

Authentication Profile

Select an authentication profile. The user must enter the password to use Send to SharePoint on the operation screen of the device when an authentication profile is specified.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.
- Also when [Authentication Method] is set to [Login User], the user enters [User Name] and [Password] to browse the folder, library information, and SPS field information using the Management Console.

Test

Click [Test] to perform connection test to the Microsoft SharePoint Server or Office 365 SharePoint Online using the entered URL, user name and password. When [HTTP Proxy Server] is configured for Microsoft SharePoint Server and Test Connection, a connection test is performed using the setting.

- When the [Enable SPS Site Selection] check box is selected

  The system checks for read permission using the Web site address and authentication information.

- When the [Enable SPS Site Selection] check box is not selected

  The system checks for read permission using the Web site address, library and folder path, and authentication information.

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a library or folder and select it as the destination. When this check box is selected, be sure to specify a library or folder in the start point.

Note

- For subfolders, only "Document" type libraries are supported.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Prefix (Name)

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the folder name.

- Manual Entry

  Enter the folder name manually.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 99 that increases by 1. When the suffix exceeds 99, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

File Naming Rules

Specify the name of the file to be saved in the destination folder.

Use either of the following methods to specify the file name:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the file name.

- Manual Entry

  Enter the file name manually.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".
- The following characters cannot be used in a file name. When used, the character is replaced with "_".
- Prohibited characters: ~"#%&*:<>?/\{|}
- If the file name starts or ends with ".", it is replaced with "_".
- If there is another file with the same name, a suffix is added to the file name. The suffix is a number from 1 to 99, and it is incremental to avoid duplicating file names. When the suffix exceeds 99, an error occurs and delivery fails.

StartPoint Path - Field Settings

Note

- Field Settings are necessary only when [Connect to SharePoint Server with On-premises Environment] is selected for the server type.

Add, Edit, Delete

Use these to add a new metadata assignment, edit an existing metadata assignment, or delete a metadata assignment.

- Add

  Adds a new metadata assignment. The [Add Field Settings] screen appears.

You can add only one content type to the table when [Pre-selected Destination] is selected in [URL] on the [General Settings] tab.

- Edit

  Changes the setting of the selected metadata assignment. The [Add Field Settings] screen appears.

- Delete

  Deletes all assigned metadata settings.

Field Settings List Table

Displays the list of field settings that are registered.

Allow User Modification

Select this check box to allow users to modify the document property presets on the operation screen of the device.

[Add Field Settings] Screen

Content Type

Select the content type. If the library is not configured, an error message is displayed.

MOSS Field

This displays the field items list of the Microsoft SharePoint Server/Office 365 SharePoint Online library configured in "Library" on the General Settings tab in the format "Field Display Name [Field Type]".

Note

- Only the library field items that can be modified appear in the list.
- The document creation date, date element specified in the metadata of the workflow, and the check boxes selected in the metadata of the workflow will be automatically converted to the library fields of Microsoft SharePoint Server/Office 365 SharePoint Online when a document is scanned.
- You can specify the following Field Types:
  - Single line text, browse

    Specify a text string.

  - Numerical Value

    Specify a text string that indicates a numeric value.

  - Yes/No (check box)

    Specify either of "TRUE" and "False" or "1" and "0".

  - Currency

    Specify a text string that indicates a numeric value such as a currency.

- Multi-line text

  Specify a text string of multiple lines.
- Selection item (radio button/drop-down menu)

  Specify a text string for an item such as an option button or drop-down list.
- Date and time

  Specify a text string in the format "MM/DD/YYYY hh:mm am/pm" such as date and time.

  "hh:mm" and "am/pm" can be omitted.
- Hyperlink, image

  Specify a text string in the URL format.

Setting Value

Configure the metadata element of RICOH Streamline NX to be added or assigned to the library field.

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, select a metadata element to be added or assigned to the library field.
- Manual Entry

  Enter a metadata element manually. You can specify a tag defined in the metadata settings or enter a text string as you require. You can also combine more than one metadata or enter any text string.

Send to CMIS

General Features

Repository Type

Select the repository type from the following:

- Documentum
- FileNet
- Opentext

URL

Specify the path to the CMIS destination folder.

Authentication Method

Specify the authentication method to be used.

The information specified here is used to access the CMIS server for saving the scanned document.

- Proxy User

  The system uses the information specified in [User Name] and [Password] for authentication.

- Login User

  The login information of the workflow is used for authentication.

- No Authentication

  No authentication is performed.

User Name

Enter the user name to be used when logging in to the destination CMIS server.

The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Password

Enter the password to be used when logging in to the destination CMIS server.

The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Load Repositories

Select this to obtain the repository information from the CMIS server, and update the repository list.

Specify [URL], [User Name], and [Password] before loading the repository.

Repository

Preset Repository

Select this check box to send the scanned documents to the fixed repository. Specify the destination repository when selecting the check box.

Repository

Specify the destination repository.

Initial Folder

Specify the path to the initial folder. The path specified here becomes the root folder to be displayed on the operation screen of the device when the user is browsing for a destination.

Specification example: test or test/subfolder_test

Destination Folder Path(s)

Specify the path to the destination folder. The path specified here becomes the default folder to be displayed on the operation screen of the device when the user is browsing for a destination.

To specify more than one path, separate each path by a comma (,).

Test

Click [Test] to check whether or not the entered initial folder and destination folder path are correct. If the path is invalid, the message "Object not found." is displayed.

Document Settings

Document Type Filter

Click [Load] to import the document types to be displayed in the metadata entry screen on the operation screen of the device. Up to 14 properties can be displayed on the operation screen of the device. Distribution fails if there are 15 or more properties.

Default Document Type

Select the default document type to be displayed on the operation screen of the device.

Document Property Presets

This displays the list of document property presets.

Add, Edit, Delete

Use these to add a new Document Property, edit an existing Document Property, and delete a Document Property.

- Add

  Adds a new metadata assignment. The [Add Property Settings] screen appears.

- Edit

  Changes the setting of the selected metadata assignment. The [Edit Property Settings] screen appears.

- Delete

  Deletes all assigned metadata settings.

Allow User Modification

Select this check box to allow users to modify the document property presets on the operation screen of the device.

Add Property Settings (Edit)

Document Type

Select the document type to be used for the property from the document types obtained from the CMIS server.

Property Name

Select the metadata property according to the selected document type.

Property Value

Use one of the following methods to specify the property value:

- Select from Existing Metadata

  From the basic metadata elements in RICOH Streamline NX, specify a metadata element to be used for the property value.

- Manual Entry

  Enter a metadata element manually so that it is used as a property value. To specify more than one metadata element, separate each element by a comma (,).

Note

- Select the property and metadata element from the list that is displayed when selecting a property that allows multiple choices in [Property Name].

Other Settings

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Naming Rules

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Select from Existing Metadata

  From the basic metadata elements in RICOH Streamline NX, specify a metadata element to be used as the subfolder name.

- Manual Entry

  Enter the subfolder name manually.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 99 that increases by 1. When the suffix exceeds 99, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".
- "cmis:folder" is the only supported subfolder type.
- Use "/" as the path delimiter. Do not use "\".
- The following characters cannot be used for a folder name. When used, the character is replaced with "_". However, "/" is recognized as a path delimiter and is not replaced with "_".
- Prohibited characters: ~"#%&*:<>?/\|
- If the folder name starts or ends with "." or a space, it is replaced with "_".
- If periods (...) are used in succession, such as in "...", they are replaced with one period.

File Naming Rules

Specify the name of the file to be saved in the CMIS repository.

Use either of the following methods to specify the file name:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the file name.

- Manual Entry

  Enter the file name manually.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".
- The following characters cannot be used in a file name. When used, the character is replaced with "_".
- Prohibited characters: ~"#%&*:<>?/\|
- If the file name starts or ends with ".", this is replaced with "_".

Send to DocumentMall

Adding and Deleting StartPoint Path

Add, Edit, Delete

Use these to add a new root folder, edit an existing root folder, and delete a root folder.

- Add

  Adds a new root folder. The StartPoint Path screen appears.

- Edit

  Changes the setting of the selected root folder. The StartPoint Path screen appears.

- Delete

  Deletes all selected root folders.

Root Folder List

Displays the list of root folders that are registered.

Select the check box of the root folder to be edited or deleted.

To select all root folders, select the check box in the first line or row.

StartPoint Path - General Settings

Display Name

Enter the display name of the root folder.

Path

Enter the destination cabinet path of Send to DocumentMall. You can select either the cabinet or a folder within the cabinet.

Example

- /Cabinet name/Folder name
- /Cabinet name

Account

Select the account to be used for logging in to DocumentMall.

Authentication Method

Specify the authentication method to be used.

- Proxy User

  The system uses the login information specified in [User Name], [Password], and [Account] for authentication.

- Login User

The system uses the login information specified in [Account] for authentication.

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When selecting the [Enable Subfolder Delivery] check box, specify the following:

Folder Naming Rules

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Select from Existing Metadata

  From the basic metadata elements in RICOH Streamline NX, specify a metadata element to be used as the subfolder name.

- Manual Entry

  Enter the subfolder name manually.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved in the DocumentMall cabinet.

Use either of the following methods to specify the file name:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the file name.

- Manual Entry

  Enter the file name manually.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Document Type

Select the [Specify document type on delivery] check box to specify the document type to be distributed to DocumentMall.

Add StartPoint Path - Assign Metadata Elements

Add, Edit, Delete

You can add a new metadata assignment setting, edit an existing metadata assignment setting, or delete a metadata assignment setting.

- Add

  Creates a new property bind setting. The Add Assigned Metadata Elements screen appears.

- Edit

  Changes the setting of the selected property bind setting. The Add Assigned Metadata Elements screen appears.

- Delete

  Deletes all property bind settings.

Metadata elements assignment list

Displays the list of assigned metadata.

Select the check box of the assignment setting to be edited or deleted. Select the check box on the title column to specify all assignment settings.

Add Assigned Metadata Elements - General Settings

Target

Enter the name of the corresponding DocumentMall property.

Source

Select the metadata element from the drop-down list, or enter the metadata element manually.

HTTP Proxy Server

IP Address

Enter the IP address or hostname of the proxy server.

Port Number

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Password

Enter the account password.

Note

- The number of characters and character types that can be entered for [User Name] and [Password] varies depending on the specifications of the delivery destination server.

Send to Exchange

Email System Settings

Select Server

Select [Connect to on-premises Exchange] when using the system in an environment where Exchange Server performs independently or Exchange Server performs with Office 365 Exchange Online. Select [Connect to Office 365] when you are using the system in an environment where Office 365 Exchange Online performs independently.

Enable Autodiscover

Select this checkbox to use [Autodiscover Email].

When this check box is not selected, specify the EWS Server endpoint.

HTTP/HTTPS

Specify the security method to be used when connecting to the EWS server.

Specify this setting only when [Select Server] is set to [Connect to on-premises Exchange].

- No Security

  The communication data is not encrypted.

- HTTPS (HTTP over SSL)

  SSL is used to encrypt the communication data and protect security of the connection to the EWS server.

  You must register the certificate to be used on the system in advance. Otherwise, an error occurs when an e-mail is sent. For details about registering a certificate, see page 403 "Enabling SSL".

EWS Server Name

Enter the IP address or hostname of the EWS server.

Specify this setting only when [Select Server] is set to [Connect to on-premises Exchange].

Use FQDN to specify the setting when using Kerberos authentication.

HTTP Port No.

Enter the port number to be used.

Specify this setting only when [Select Server] is set to [Connect to on-premises Exchange].

Autodiscover Email

You can use this setting when using Exchange 2010 or later.

Specify this setting only when [Select Server] is set to [Connect to on-premises Exchange].

Client ID

To use Office 365 Exchange Online, register the application to Azure Active Directory first. Then, copy and paste the registered "Application ID" in [Client ID].

Specify this setting only when [Select Server] is set to [Connect to Office 365].

Note

- For details about registering the application to Azure Active Directory, see the manual provided with Azure Active Directory.
- Enable the following permissions for Office 365 Exchange Online when registering it to Azure Active Directory:
  - Send e-mail as a user
  - Read and write user e-mail
  - Access mailboxes as the signed-in user via Exchange Web Services

Authentication Method

Specify the authentication method to be used.

Proxy User

The information specified in [Proxy User Name], [Proxy Password] is used for authentication.

Login User

The login information of the workflow is used for authentication.

Note

- If RICOH Streamline NX has been installed with SSL/HTTPS, proxy server with basic authentication is not supported.
- The number of characters and character types that can be entered for [Proxy User Name] and [Proxy Password] varies depending on the specifications of the delivery destination server.

Authentication Profile

Select an authentication profile, and then enter the password on the operation screen of the device to use Send to Exchange.

Test

Click this to check connections with the Exchange Server or Exchange Online using the specified settings. Does not perform authentication tests using the entered user name and password.

Send to Email Option Settings

Select Data to Attach

Specify how to attach the data to e-mails.

- Attach All
- Attach First Page Only
- Do Not Attach

File Naming Rules

Specify the name to be given to the attached file.

You can Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata element to be used as the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Attach Document Link(s) and Deliver

Specify whether or not to include the URL that indicates the save location of the distributed document in the e-mail.

- On

  The URL is added to the body of the e-mail.

- Off

  The URL is not included in the e-mail.

Note

- To use this setting, you must add at least one of the following connectors in front of the Send to Exchange connector: Send to Folder connector, Send to FTP connector, Send connector.

Body

Enter the body of the e-mail to be sent.

You can specify a different body text for each language selected from the drop-down list

You can also use the metadata elements in the scanned file except "resultURL" as the body text. For details about metadata items, see page 348 "Metadata".

Send to Me

Specify whether or not to add the logged-in user automatically to the Selected Destinations list.

- On

  When the e-mail address of the logged-in user can be retrieved from the login information of the workflow, the string "Send to Me" is automatically added to the "To" field in the Selected Destinations list.

  The system can retrieve the e-mail address of the logged-in user when LDAP/Kerberos authentication is used as the workflow authentication method.

- Off

  The e-mail address of the logged-in user is not added to the Selected Destinations list.

Default Domain for Manual Input

Enter the default domain name to be added to the e-mail address that is manually entered.

Example

Default domain: ABCCorp.com

User input: john

Generated e-mail address: john@ABCCorp.com

The default domain is not added if the logged-in user entered an e-mail address including a domain name.

Note

- "@" is automatically entered.

Option Settings

Select the items that are optional.

- Show Cc

  The user can enter an e-mail address in the CC field.

- Show Bcc

  The user can enter an e-mail address in the Bcc field.

- Show ReplyTo

  The user can enter the ReplyTo e-mail address.

- Enable Manual Address Entry

  - When using the Smart Operation Panel:

    When [Enable Manual Address Entry] is disabled, [Manual Entry] is not displayed on the Send to Email destination adding screen.

- When using the Standard Operation Panel:

  When [Enable Manual Address Entry] is disabled, [Manual Entry] on the Send to Email screen is grayed out.

- Enable Address Validation

  Checks for the validity of the e-mail address when a scan data is sent or an e-mail address is manually entered on the operation screen of the device.

Email Search Settings

Enable Address Search

Select this to allow the logged-in user to search for e-mail addresses in the address book of the LDAP server.

LDAP/LDAPS

Select the security method to be used when connecting to the LDAP server.

- No Security

  The communication data is not encrypted.

- LDAPS (LDAP over SSL)

  SSL is used to encrypt the communication data and protect security of the connection to the LDAP server. You must register the certificate to be used on the system in advance. Otherwise, an error occurs when the address book is retrieved.

- LDAPS (StartTLS)

  TLS is used to encrypt the communication data and protect security of the connection to the LDAP server. The LDAP server to be used must support StartTLS. Otherwise, an error occurs when the address book is retrieved.

LDAP(S) Server

Enter the IP address or hostname of the LDAP server.

Click [Test] to check the connection to the LDAP server that has been entered. Performs authentication tests using the entered user name and password.

LDAP(S) Port No.

Enter the port number to be used.

Authentication Method

Select the type of account to be used for logging in to the LDAP server.

- Proxy User

  The system uses the login information entered in [User Name] and [Password] is used for authentication.

- Login User

The login information of the workflow is used for authentication.

To browse the address book using the Management Console when selecting [Login User], enter [User Name] and [Password].

- No Authentication

  No authentication is performed.

LDAP Base DN

Specify the identifier (DN) of the node in the directory tree to be searched.

Setting example

cn=users, dc=ricoh, dc=co, dc=jp

Address Search Settings

Specify the search condition in the address book.

LDAP Search Condition

Specify the LDAP Search Condition when you only enter a space or enter no character at all, the system searches the entire address book.

The default setting is as follows:

(&(objectclass=organizationalPerson)(cn=*^s*))

Replace "^s" with the search keyword.

The maximum number and range of characters, and input condition that can be specified in LDAP Search Condition are as follows:

Search condition	Maximum number of characters or input range	Input condition
LDAP(S) Server	1,000 characters	None
LDAP(S) Port No.	1–65535	Integer only
User Name	1,000 characters	None
Password	1,000 characters	None
LDAP Base DN	1,000 characters	None
LDAP Search Condition	1,000 characters	None
Display Name	1,000 characters	None
Address Format	1,000 characters	None

Example

- When using the wildcard character "*" to modify the search condition

1. The following example matches the search condition when you specify cn=*les*.
   - charles smith
   - lester frank
   - Lorraine Lester
   - Steven Morales

   The system searches for all names that contain the search keyword ("les").
2. The following examples match the search condition when you specify cn=les*.
   - lester frank
   - Lester, lorraine

   The system searches for all names that contain a string starting with the search keyword ("les").
3. The following examples match the search condition when you specify cn=*les.
   - Smith, charles
   - steven morales

   The system searches for all names that contain a string ending with the search keyword ("les").

Display Name

Specify the LDAP attribute for the display name of each item to be displayed when searching for an e-mail address. To specify more than one LDAP attribute, separate each attribute by a comma (,).

The default is "cn" (common name).

Example

sn, givenName, mailaddress

Address Format

Specify the LDAP attribute to be used for displaying the e-mail addresses in the search results.

The default is "mail".

Send to RightFax

RightFax Server Settings

RightFax Server

Enter the IP address or hostname of the RightFax server.

Click [Ping] to check connections with the specified RightFax server.

User ID

Specify the user ID of the RightFax server account that has the administrator privilege.

Note

- The number of characters and character types that can be entered for [User ID] varies depending on the specifications of the delivery destination server.

Password

Enter the password of the RightFax server account as necessary.

Note

- The number of characters and character types that can be entered for [Password] varies depending on the specifications of the delivery destination server.

Authentication Method

Select the type of account to be used for logging in to the RightFax server.

- Proxy User

  The system uses the account entered in [User ID] to send fax or e-mail.

- Login User

  The login information of the workflow is used for authentication.

Note

- Add LDAP/Kerberos authentication or NT authentication to the authentication profile when selecting [Login User].

Enforce Strict Security

You must integrate the login user to NT when this check box is selected. This cannot be configured when [Proxy User] is selected in [Authentication Method].

Test Fax Number

Enter a valid fax number, and then click [Test]. You can view the authentication using the account with the specified user name and password, and you can check whether or not the RightFax server settings are correctly configured.

Phonebook Display and Search Settings

Search Fields

Enter the field to be searched. Use a comma (,) to specify more than one field.

Select a syntax from the drop-down list, and then insert the selected syntax into [Search Fields].

When you select [All Items], all items are inserted into [Search Fields].

If an invalid syntax is included, it will be replaced by a valid syntax when it is moved to another item.

Display Format

Enter the tokens in the order to be displayed on the operation screen of the device. The cardinality such as 0 and 1 must match the order of the fields entered in [Display Fields].

Display Fields

Enter a valid RightFax phonebook field to be used for the display format of search results.

Select a syntax from the drop-down list, and then insert the selected syntax into [Display Fields].

If an invalid syntax is included, it will be replaced by a valid syntax when it is moved to another item.

Preferential Order

Specify the priority of the fields to be used from fax1, fax2, email, voice1, and voice2.

An entry for which all the fields specified here are empty is omitted when a search is performed. If even one field has a value, the entry is displayed in the search results.

When you are sending a scanned document, this priority is used as the priority order of the destinations. The leading value of the field that is not empty is selected as the destination.

Disallow Phonebook Search

If you select this check box, [Search] becomes disabled and the user can no longer use the search function.

Disallow Manual Entry

If you select this check box, [Manual Entry] becomes disabled and the user can no longer enter the destination manually.

The user cannot use the phonebook entry function when [Manual Entry] is disabled.

Disallow Recent Destinations Selection

If you select this check box, [Recent Destinations] becomes disabled and the user can no longer select a destination from the destination history.

[Recent Destinations] cannot be used while the load balance and fail over functions are enabled. In such a case, select the [Disallow Recent Destinations Selection] check box. For details about the load balance and fail over functions, see page 383 "Balancing the Workload among Servers".

Auto Load Private Phonebook

In the list of search results on the destination selection screen, select this check box to display the private phonebook of the logged-in user.

Auto Load Public Phonebook

In the list of search results on the destination selection screen, select this check box to display the public phonebook.

Require Manual Entry Confirmation

Select this check box to make sure to enter the destination when the user specifies the destination by entering it manually. The destination is confirmed only when the destination entered for the second time matches the one entered first.

Note

- An error message is displayed because no method for specifying the destination is available when all of the following conditions are fulfilled:
  - All check boxes for [Disallow Phonebook Search], [Disallow Manual Entry], and [Disallow Recent Destinations Selection] are selected
  - Both check boxes of [Auto Load Private Phonebook] and [Auto Load Public Phonebook] are not selected
  - No destination is specified for the default setting on the Send to RightFax screen
- When the total number of destination to be automatically loaded exceeds the following values, no entry is displayed in the list of search results:
  - Management Console: 50 items
  - Device Operation Screen: 100 items

ODBC and Group Search Settings

Use ODBC?

The system uses the ODBC information when this check box is selected.

RightFax Database Server

Specify the server name or IP address of the RightFax database.

RightFax Database User

Specify the SQL user ID that can access the SQL database. Configure this in advance to use ODBC search.

RightFax Database Password

Specify the password of the SQL user who can access the SQL database. Configure this in advance to use ODBC search.

RightFax Database Name

Enter the database name to save the RightFax phonebook.

Record Limit

Specify the upper limit of records to be returned from the SQL server to the device.

The device can obtain up to 1000 records.

Group Display

Specify how to display the groups in the search result from the following: You must enable [Use ODBC?] to use the group search function.

- Items Only
- Items First, then Groups
- Groups First, then Items
- Items and Groups Sorted Together

Prefix

Specify the prefix to be added to the group.

Suffix

Specify the suffix to be added to the group

Job Settings

Error Processing

Login User Does not Exist in RightFax

Specify how the system behaves when the logged-in user cannot be found in the RightFax database.

- Use Proxy User Authentication

  The system uses the information of the proxy user for authentication. This item is available when [Enforce Strict Security] is enabled in [RightFax Server Settings].

- Enforce Delivery (see error on RightFax server)

  The system sends the job forcibly that is created by the logged-in user, causing an error. The administrator can check the error log information, and add the user to the database.

- Prohibit Scan

  The user cannot create a Send to RightFax job.

Send to Gmail

Email System Settings

Private Key File

Specify the private key file for accessing Google API.

Click [Browse] to select the private key file, and then click [Upload].

Note

- Only JSON type key can be uploaded. Select JSON for the key type when creating the private key. For details about creating and downloading the private key file, see G Suite Administrator Help Center.

Authentication Method

Specify the authentication method to be used when accessing the mailbox.

- Proxy User

  The system uses the e-mail address specified in [Email Address]. Click [Test] to check the connection to the specified e-mail address.

- Login User

  The e-mail address of the logged-in user is used for authentication.

HTTP Proxy Server

IP Address

Enter the IP address or hostname of the proxy server.

Click [Test] to check the connection to the proxy server that has been entered. Does not perform authentication tests using the entered user name and password.

Port No.

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Password

Enter the account password.

Send to Gmail Option Settings

Select Data to Attach

Specify how to attach the data to e-mails.

- Attach All
- Attach First Page Only
- Do Not Attach

File Naming Rules

Specify the name to be given to the attached file.

Use either of the following methods to specify the file name:

- Enter the file name manually.
- From the drop-down list, select the metadata to use for the file name.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Attach Document Link(s) and Deliver

Specify whether or not to include the URL that indicates the save location of the distributed document in the e-mail.

- On

  The URL is added to the body of the e-mail.

- Off

  The URL is not included in the e-mail.

Note

- To use this setting, add at least one of the following connectors before the Send to Gmail connector in the delivery flow: Send to Folder connector, Send to FTP connector, Send to WebDAV connector, Send to SharePoint connector, and Send to Document Mall connector.
- For details about how to create the URL that points to the document save location when the Save to Folder connector is used, see the StartPoint Path setting of the Send to Folder service.

Body

Enter the body of the e-mail to be sent.

You can specify a different body text for each language selected from the drop-down list.

You can also use the metadata elements in the scanned file except "resultURL" can as the body text. For details about metadata items, see page 348 "Metadata".

Send to Me

Specify whether or not to add the logged-in user automatically to the Selected Destinations list.

- On

  When the e-mail address of the logged-in user can be retrieved from the login information of the workflow, the string "Send to Me" is automatically added to the "To" field in the Selected Destinations list.

  The system can retrieve the e-mail address of the logged-in user when:

  - Active Directory authentication is used as the workflow authentication method;
  - LDAP authentication is used as the workflow authentication method, and [Active Directory] is selected as the LDAP server type in [Server Type];
  - The email address of the user is registered with the User Profile in the RICOH Streamline NX server.

- Off

  The e-mail address of the logged-in user is not added to the Selected Destinations list.

Default Domain for Manual Input

Enter the default domain name to be automatically added to the e-mail address that is entered manually.

Example

Default domain: ABCCorp.com

User input: john

Generated e-mail address: john@ABCCorp.com

Note

- "@" is automatically entered.
- The default domain is not added if the logged-in user entered an e-mail address including a domain name.

Option Settings

Select the items that are optional.

- Show Cc

  The user can enter an e-mail address in the CC field.

- Show Bcc

  The user can enter an e-mail address in the Bcc field.

- Enable Manual Address Entry

  The user can enter an e-mail address manually.

  - When using the Smart Operation Panel:

    When [Enable Manual Address Entry] is disabled, [Manual Entry] is not displayed on the Send to Email destination adding screen.

  - When using the Standard Operation Panel:

    When [Enable Manual Address Entry] is disabled, [Manual Entry] on the Send to Email screen is grayed out.

- Enable Address Validation

  When entering an e-mail address manually on the operation screen of the device or sending scan data, use the following rules to verify the format of the e-mail address:

  - Do not use spaces, colons, or other prohibited characters
  - Use only one @ symbol
  - Do not use a period (.) at the end of the e-mail address
  - Include the top level domain

- Do not use non-alphanumeric characters in the top level domain
- Do not use a period (.) in the top level domain

Note

- While the format of the e-mail address is verified, the domain and e-mail address are not verified.
- An error message is displayed if the format of the e-mail address is invalid.

Email Search Settings

Enable Gmail Personal Contact Search

Specify whether or not to enable searching in the Gmail personal contact list when specifying destinations on a device.

Enable G Suite Directory Search

Specify whether or not to enable searching in the G Suite Directory when specifying destinations on a device.

G Suite Administrator Email Address

Register the G Suite administrator's e-mail address when selecting the [Enable G Suite Directory Search] check box is selected.

Send to Google Drive

Send to Google Drive Option Settings

Private Key File

Specify the private key file for accessing Google API.

Click [Browse] to select the private key file, and then click [Upload].

Note

- Only JSON type keys can be uploaded. Select JSON for the key type when creating the private key. For details about creating and downloading the private key file, see G Suite Administrator Help Center.

Authentication Method

Specify the authentication method to be used when accessing the repository.

- Proxy User

  The system uses the e-mail address specified in [Email Address]. Click [Test] to check the connection to the specified e-mail address.

- Login User

The e-mail address of the logged-in user is used for authentication.

HTTP Proxy Server

IP Address

Enter the IP address or hostname of the proxy server.

Click [Test] to check the connection to the proxy server that has been entered. Does not perform authentication tests using the entered user name and password.

Port No.

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Password

Enter the account password.

Other Settings

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Prefix (Name)

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the folder name.

- Manual Entry

Enter the folder name manually.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 99, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved in the repository.

Use either of the following methods to specify the file name:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the file name.

- Manual Entry

  Enter the file name manually.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Send to Dropbox

Send to Dropbox Option Settings

Authorization URL

The administrator accesses the URL displayed in [Authorization URL] using a web browser, log in with a credential, and grant the connector access to a team whose users will use the connector.

Authorization Code

Enter the authorization code acquired by accessing the URL displayed in [Authorization URL]. Click [Authorize] to validate the authorization code and generate a token. When authorization is successful, [Authorization Code] and [Authorize] are disabled to prevent accidental change of an authorization code. To change the code, click [Modify].

Note

- Each authorization code can be used only once. It the Send to Dropbox connector is expected to be used in multiple workflows, it is recommended that you configure it as a shared connector.

Authentication Method

Specify the authentication method to be used when accessing the repository.

- Proxy User

  The system uses the e-mail address specified in [Email Address]. Click [Test] to check the connection to the specified e-mail address.

- Login User

  The e-mail address of the logged-in user is used for authentication.

Note

- If RICOH Streamline NX has been installed with SSL/HTTPS, proxy server with basic authentication is not supported.

HTTP Proxy Server

IP Address

Enter the IP address or hostname of the proxy server.

Click [Test] to check the connection to the proxy server that has been entered. Does not perform authentication tests using the entered user name and password.

Port No.

Enter the port number to be used.

Note

- The default port number is 8080.

Account

Enter the login account to be used for logging in to the proxy server.

Password

Enter the account password.

Note

- If RICOH Streamline NX is installed with SSL/HTTPS, no proxy server with basic authentication is supported.

Other Settings

Access to Subfolder

Select the [Enable Subfolder Browsing] check box to allow the user to browse for a folder and select the folder as the destination.

Create a Subfolder

Select the [Enable Subfolder Delivery] check box to create a subfolder under the destination folder automatically.

When the check box is cleared, the scanned documents are directly distributed under the specified destination folder.

When you select the [Enable Subfolder Delivery] check box, specify the following:

Folder Prefix (Name)

Specify the subfolder name. A folder is created under the subfolder when you include a separator in the name. For example, enter "abc\xyz" to create the folder "abc" under the root folder, and folder "xyz" under that folder. The scanned documents are saved in "xyz".

Use one of the following methods to specify the name of the subfolder to be created:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the folder name.

- Manual Entry

  Enter the folder name manually.

Add Suffix to Folder Name

A suffix is added to the subfolder name when another subfolder with the same name already exists. A suffix is a number between 1 and 9999 that increases by 1. When the suffix exceeds 99, an error occurs and delivery fails.

If a folder with the same name already exists while [Add Suffix to Folder Name] is not selected, the scanned document is saved in the existing folder.

Note

- For details about the procedure to specify the folder name, see page 255 "File and Folder Naming Conventions".

File Naming Rules

Specify the name of the file to be saved in the repository.

Use either of the following methods to specify the file name:

- Select from Existing Metadata

  From the basic metadata elements of RICOH Streamline NX, specify a metadata element to be used as the file name.

- Manual Entry

  Enter the file name manually.

Note

- For details about the procedure to specify the file name, see page 255 "File and Folder Naming Conventions".

Setting Items in the Process Connector Properties

Configure the properties for each process connector.

Display Name

Specify the name to be displayed on the operation screen of the device for each process connector.

Select a language from the drop-down list, and specify the display name for each language.

PDF Converter

General Features

PDF Type

Specify the PDF type.

- PDF
- PDF/A-1a
- PDF/A-1b

Note

- When you select [PDF/A-1a] or [PDF/A-1b] for PDF type, the logged-in user can only create an image PDF. The user cannot create a password-protected PDF.
- When you select [PDF/A-1a] or [PDF/A-1b] for the output format, all setting items on the [PDF Converter] tab becomes unavailable (grayed out) on the operation screen of the device.

PDF Format

- Single page PDF

  A PDF file is generated for each page.
- Multi-page PDF

  A PDF file that comprises multiple pages is generated.

Compression

Specify whether or not to perform compression on the generated PDF.

When you select [On], specify the degree of compression in [Compression Rate].

When you select [Auto-judge], the system determines whether or not to perform compression according to the file contents.

Compression Rate

Specify the degree of compression.

- High
- Middle
- Low

Note

- You can specify the compression rate only when selecting [On] or [Auto-judge] in [Compression].

PDF Conversion Mode

Specify the compression mode to apply on the PDF file.

- Accuracy Priority
- Balance
- Speed Priority

Note

- This setting may not have any effect depending on the scanned document.

Deskew

Specify whether or not to apply the deskew function.

Select [On] to generate a PDF file on which the deskew function is applied.

The output image size may become larger than the original when white margins are added around the deskewed image.

Image Converter

Image Converter List

Select the output format.

For a Workflow that Processes Jobs on the Server

- The file format specified on the [Scan Settings] tab
- TIFF (MH, single-page)
- TIFF (MR, single-page)
- TIFF (MMR, single-page)
- TIFF (uncompressed, single-page)
- TIFF (MH, multi-page)
- TIFF (MR, multi-page)
- TIFF (MMR, multi-page)

- TIFF (uncompressed, multi-page)
- TIFF-F (MH, single-page)
- TIFF-F (MR, single-page)
- TIFF-F (MMR, single-page)
- TIFF-F (MH, multi-page)
- TIFF-F (MR, multi-page)
- TIFF-F (MMR, multi-page)
- DCX (single-page)
- DCX (multi-page)
- BMP (uncompressed)
- JPEG
- PNG
- GIF

For a Workflow that Processes Jobs on the Device

- The file format specified on the [Scan Settings] tab
- TIFF (multi-page)

Note

- In a workflow that processes jobs on the device, a file is automatically generated for every 100 pages when you create TIFF or PDF files from a document containing 100 pages or more.
- When the output format is set to a setting other than [File Format Selected on [Scan Settings] Tab], selecting the output format on the operation screen of the device has no effect. When the output format is preset, it is recommended to specify the Hide settings for the [File Format] on the [Scan Settings] tab. For details about the Hide setting, see page 294 "Customizing the Settings on the Operation Screen of the Device".

Archiver

Archive Format

Specify the archive format.

- zip
- tgz

OCR

Document Name Extraction

The file name is generated using the keyword on the first page of the scanned document.

Format Conversion

The system converts the file into the specified format.

- Rich Text Format (RTF)
- Excel (XLS)
- Excel (XLSX)
- Word (DOCX)

Note

- Input files are combined into a single file when you are using the format conversion function.
- Files in the format that cannot be processed among the input files are skipped.

XML Transformer

XSL File Path

Click [Browse] to select the XSL file to be used for the XML transformer connector.

To apply the setting, click [Upload]. To download the XSL file, click [Download].

When you do not specify a XSL file, the original metadata (XML) is added to the document.

Important

- **Check that there is enough space available on the hard disk drive before downloading the file. You may not be able to open the downloaded file if the space is insufficient.**

Note

- You must save the XSL file to be used using UTF-8 for the character code.
- The XSL file must conform to the following specifications. Otherwise, the delivery flow will fail.
  - XSL Transformations (XSLT) version 1.0
  - XML Path Language (XPath) version 1.0
- Upload a new XSL file to replace the existing XSL file.
- You cannot delete the XSL file from the process connector. To delete the file, delete the process connector from the delivery flow, and then add a new XML Transformer.
- When you click [Upload], the fixed file name of <desk.xls> always appears in the XSL file path display area instead of the name of the uploaded file.

Conversion Result Save-in Location

Specify the location to add the information of the converted document.

Select [First Page] to append add the conversion result to the first section in the document.

Select [Last Page] to append add the conversion result to the last section in the document.

Conversion Result File Name

Enter the file name of the conversion result. Be sure to enter an extension at the end.

- If you leave this field blank, the current document name is used.
- When a document name is not specified, the time stamp (local time) is used as the document name.

  Timestamp format: "yyyymmddhhmmss"

  (yyyy: year, mm: month, dd: day, hh: hours, mm: minutes, ss: seconds)
- If you enter a period (.) for the first character in the file name, the extension of the input data is added behind the timestamp.
- When the last character of the file name is a period (.), it is automatically replaced by an underscore (_).
- Do not use the following characters in the file name:\ : / * ? | " < > If you enter any of those characters, it is automatically replaced by an underscore (_).

Note

- A file extension is not appended when an extension is not entered with the file name. Also, an extension is not appended when the user does not enter a file name.

Select Character Encoding

Select a character code from the drop-down list.

The supported character codes are as follows:

- UTF-8
- Latin -1
- Windows Shift-JIS (Only in Japan)
- JIS (Only in Japan)

Note

- In the workflows that process jobs on the device, the setting becomes invalid even when JIS is selected.

Metadata Converter

Replacement Table Name

Specify the replacement table to be used in the metadata converter.

The table determines the changes to be made to the metadata.

Select Action when Table Data does not Match

Specify how to process the delivery flow when the value of the target metadata does not match the [Comparison Target String] setting in the replacement table.

- Continue flow using default values

  The target metadata is replaced using the value of [Default Output] in the replacement table. The delivery flow proceeds without pausing. The output value becomes blank when [Default Output] is not specified. The process is recorded as being successful in the job log.

- Continue flow without performing replacement

  The flow continues without replacing the metadata element that does not match the replacement table.

- Skip subsequent flow, status Succeeded

  All proceeding processes behind the delivery flow is skipped, and no error is recorded in the system log. The process is recorded as being successful in the job log.

  When a redirect exists in front of the table replacement connector in the delivery flow, the process is normally performed in other flows behind the redirect.

- Stop subsequent flow, status Failed

  The delivery flow fails.

  The job is moved to the error queue and recorded as an error in the job log and system log.

Metadata Replacement

Regex

Enter a regular expression (regex) to be used to confirm and replace the metadata elements.

- Ignore upper/lower case characters

  Select this option to ignore the difference in upper and lower case letters (such as "a" and "A").

- Disregard Blank Space(s) and Symbol(s)

  Select this option to disregard unnecessary blank spaces and symbols in a regex.

Metadata

Select the target metadata element from the drop-down list, or enter the item name (ID) manually. Use this item to compare the target metadata element (such as the document name) with the value of [Regex] and replace the value of the target metadata element.

To use a custom metadata element, enter the item name (ID) of the metadata element manually.

Action

Select the action to be performed in this process connector from the following:

- Use match reference function

  The value of the specified metadata element is compared with the regular expression specified in [Regex].

- Use text replacement function

  The value of the specified metadata element is compared with the regular expression specified in [Regex], and replace it by the value specified in [Text to Replace].

Output to

Select the [Specify Where to Output] option to specify the output location of the replacement result. The functionality of the item is the same as Use Text Replacement Function, except for the target metadata element being selectable from the drop-down list.

When specifying a custom metadata element for the target, enter the item name (ID) of the metadata element manually.

Text to Replace

Enter the characters to replace the value of the target metadata.

Note

- Select [Use text replacement function] in [Operation] to use this function.

Replacement Options

Select the [Replace all] option to replace all text strings that match the regex.

Clear the check box to replace only the first matching text string.

Note

- Select [Use string replacement function] in [Operation] to use this function.

Barcode Separator/Index

Add, Edit/Delete

You can add a barcode information for recognition (add as new), or edit or delete the registered barcode information.

- Add

  Adds new barcode information. The barcode information settings screen is displayed.

- Edit

  Modifies the selected barcode information. The barcode information settings screen is displayed.

- Delete

  Deletes all selected barcode information.

Barcode Information Management Table

The list of registered barcode information is displayed.

To edit or delete the barcode information, select the check box of the barcode information in the list that you want edit or delete.

Barcode Information Settings Screen

Use barcode to perform batch separation

Select this option to use the barcode as the symbol for job division.

- Perform batch separation when the barcode data match

  Select this option to compare the barcode data with an arbitrary string, and if they match, use the barcode as the symbol for job division. In [Barcode data], enter the string to compare with the scanned barcode data.

- Do not include the barcode sheet in the separated document

  Select this option to delete the sheet containing the barcode when using the barcode as the symbol for job division.

Continue Recognition Even When 1st Page Has No Barcode

Select this option to specify barcodes on the second page or thereafter or in the second section or thereafter as the target for recognition if there is no barcode on the first page or it cannot be recognized.

Clear the check box to not recognize the barcodes on the second page or thereafter or in the second section or thereafter if there is no barcode on the first page or it cannot be recognized.

Selection Method

Select the method for identifying the barcode uniquely for recognition.

- Do not Specify

  The barcode for recognition is not uniquely identified.

- Barcode Number

  Adds a number to all barcodes on the page according to the number designation rule. You can use that number to identify the barcode for recognition. In [Position], enter a barcode number from 1 to 99.

- Coordinates

  Recognizes the barcode at the specified coordinates. Specify the coordinates in [Position]. With the upper left corner of the image at 0,0, specify the coordinates for the approximate center of the barcode for recognition in positive numbers as X,Y. You can specify the coordinates up to two decimal places. You can switch units between "mm" and "inch".

- Rectangular Area

Recognizes the barcode within a specified area. With the upper left corner of the image at 0,0, specify the coordinates for the upper left corner of the area for recognition in positive numbers as X,Y in [Position]. Next, specify the width and height of the area for recognition in [Width] and [Height]. You can specify the coordinates up to two decimal places. You can switch units between "mm" and "inch".

Note

- For details about the rules for specifying the barcode number, see page 284 "Specifying barcode numbers".
- For details about the measurement method of the barcode coordinates, see page 285 "Measuring the barcode coordinates".
- For details about the measurement method of the barcode area coordinates, see page 286 "Measuring the barcode area coordinates".

Barcode Type

Specify the type of barcode.

- Do not specify
- Code39 Standard ASCII
- Code39 Extended ASCII
- Code 128 / GS1(EAN)-128
- EAN 8
- EAN 13
- Interleaved 2 of 5
- Codabar(NW7)
- Code 2 of 5
- Codabar(NW7)
- PDF417
- DataMatrix
- QR

Data Format

Specify the format of data stored in the barcode.

- Non-delimiter Type

  Select this option when the data stored in the barcode is separated over multiple pages or when not dividing the data stored in the barcode over multiple pages.

- Delimiter Type

Select this option when the format of data stored in the barcode is divided by an arbitrary delimiter character. The data obtained from the barcode is divided by the delimiter character entered in [Delimiter Rule] and separated into multiple pages.

The characters that can be specified as delimiter characters are as follows:

[a-z] [A-Z] [0-9]

!"#$%&'()*+,-./:;<=>?@[]^_` { | }

- Digit Type

  Select this option when the format of data stored in the barcode is divided by the number of characters. The data obtained from the barcode is divided by the number of characters entered in [Delimiter Rule] and separated into multiple pages.

  Enter the number of digits separated by commas in the format "1,2,3,4". For example, when the barcode data is "123xx789yyy" and you want to divide the data into individual pages using the units "123", "xx", "789", and "yyy", specify "3,2,3,3". You can use an asterisk (*) when entering the number of digits. The asterisk means "all strings thereafter".

Character Code

Specify the character code of the data stored in the barcode.

- ASCII
- Latin 1
- JIS
- Windows Shift_JIS
- UTF-8

Note

- Be sure to select the character code used in the barcode.

Error Handling

Specify the method for handling errors that occur during processing with the barcode recognition connector.

- Stop the job when barcode filter fails

  Ends the job when a barcode cannot be detected or reading of the detected barcode data or division of the data fails.

- Ignore error and continue the job

  Continues the job without ending when a barcode cannot be detected or reading of the detected barcode data or division of the data fails. Data read from a barcode, however, cannot be added as metadata. A warning log is recorded in the log.

Tag Name

Specify a tag name when analyzing data read from a barcode and storing it as metadata. For the tag name of custom metadata, the string specified in [Tag Name] is given the prefix "P0001" and the suffix "_" (underscore) followed by a serial number between 1 and 99.

Example of metadata tag name

Metadata name added to the document when the string "DOC" is specified in [Tag Name]

- P0001_DOC_01
- P0001_DOC_02
- P0001_DOC_03...

Note

- When a tag name is not specified, the string "bcData" (default value) is used.
- Do not use curly brackets ({ }) in the tag name.
- Do not use an existing tag name.

Zone OCR

Form

Select one of the registered forms.

Section (1–500)

Specify the section to perform OCR.

You can only specify one section. If the job contains more than one section, the system performs OCR only on the first page.

Note

- Use the Section Splitter plugin to divide a job containing multiple sections into multiple files per section.

Error Processing

Specify how to process when an error occurs from [Stop Processing] or [Skip Errored Process].

- [Stop Processing]

  The system stops processing when an error occurs.

- [Skip Errored Process]

  The system ignores the error and continues processing.

  If you select [Skip Errored Process] while selecting the [Judge as an error when the OCR result is blank.] option on the Area Properties screen, the job is processed and an error log is added to both the job log and system log.

PDF Stamper

Stamp Name

Select a stamp from the registered stamps.

Stamp Type

The type of the stamp selected in [Stamp Name] is displayed. This cannot be changed.

Details

The details of the stamp selected in [Stamp Name] are displayed. This cannot be changed.

Format of CSV Files

CSV files are used for import/export of RICOH Streamline NX.

Devices, groups, address book, etc., can be exported to a CSV file, and the data from the CSV file can be loaded after editing it.

Note

- UTF-8 is used as the character code for CSV files. However, GB18030 is used as the character code when the language is Chinese.
- When data includes commas (,) or double quotations ("), enclose the entire data with double quotations.

Format of a Device Information CSV File

A device information CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: **X.X.X.X**
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Device List
4	**# (Item name of the column)**
5	**"(Column name of the database)"**
6	**"(Value of the device that corresponds to the item name of the column)"**

As "Item name of the column" in line four, the item name of the column displayed in the header of the device list is written out row-by-row sequentially from the left-hand side.

In line six and subsequent lines, the values of all devices displayed in the device list at the time of export are written out line-by-line.

Note

- Do not change the information in lines one through four. This information is used for identification.
- You can import the following item name of the columns (Column name of the database) from CSV file:
    - Address (dev_address)

- Serial Number (dev_serialnumber)
- Network: MAC Address (dev_mac_address)
- Vendor Name (dev_manufacturer)
- Delegation Server (dev_dmserver_id)
- Display Name (dev_displayname)
- Custom Properties 1–10 (dev_cust_prop 1–10)
- Date Installed (installation_date)
- Group (dev_real_group_name)

Format of a Device Group Information CSV File

A device group information CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: **X.X.X.X**
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Device Groups
4	"**(Row name)**"
5	"**(Value that corresponds to row name)**"

The "Row name" and row number in line four, and their corresponding values of line five and subsequent lines, are as follows:

Row names and their corresponding values

Row number	Row name	Value of line 5 and subsequent lines
1	category	Category name
2	dev_group_name_lv_1	Child group name of category
3	dev_group_name_lv_2	Child group name of dev_group_name_lv_1
4	dev_group_name_lv_3	Child group name of dev_group_name_lv_2
5	dev_group_name_lv_4	Child group name of dev_group_name_lv_3

Row number	Row name	Value of line 5 and subsequent lines
6	dev_group_name_lv_5	Child group name of dev_group_name_lv_4
7	dev_group_name_lv_6	Child group name of dev_group_name_lv_5

Note

- Do not change the information in lines one through three, as this information is used for identification.

Typical description of a group information CSV file

```
# Format Version: X.X.X.X,,,,,,,
# Generated at: XXXX/XX/XX XX:XX:XX,,,,,,,
# Function Name: Device Groups,,,,,,,
"category","dev_group_name_lv_1","dev_group_name_lv_2","dev_group_name_lv_3","dev_group_name_lv_4","dev_group_name_lv_5","dev_group_name_lv_6"
"(Category name)","(Group name Lv 1)","(Group name Lv 2)","(Group name Lv 3)","(Group name Lv 4)","(Group name Lv 5)","(Group name Lv 6)",
```

Format of a Discovery Range CSV File

CSV files are divided into two types depending on the search method of discovery.

Network Search

A discovery range CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: X.X.X.X
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Network Search Discovery Range
4	**"(Row name)"**
5	**"(Value that corresponds to row name)"**

The "Row name" and row number in line four, and their corresponding values of line five and subsequent lines are as follows:

Row names and their corresponding values

Row number	Row name	Value of line five and subsequent lines
1	0=Import/1=NOT Import	Specify whether or not to import line data. The line to which "1" is entered is not imported.
2	IP Address (From)/Host Name	Enter the discovery target hostname, IP address, or start IP address of the discovery target IP address range.
3	IP Address To	Enter the end IP address of the discovery target IP address range.
4	Subnet Mask	Enter the subnet mask.
5	0=Include/1=Exclude	Specify whether to include or exclude a specified range in the network search.

Note

- Do not change the information in lines one through three, as this information is used for identification.

Broadcast

A discovery range CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: X.X.X.X
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Broadcast Discovery Range
4	"**(Row name)**"
5	"**(Value that corresponds to row name)**"

The "Row name" and row number in line four, and their corresponding values of line five and subsequent lines are as follows:

Row number	Row name	Value of line five and subsequent lines
1	0=Import/1=NOT Import	Specify whether or not to import line data. The line to which "1" is entered is not imported.
2	Subnet	Enter the subnet address. An IPv4 address can be used.
3	Subnet Mask	Enter the subnet mask.

Note

- Do not change the information in lines one through three, as this information is used for identification.

Format of an Address Book CSV File

An Address Book CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: 4.1.2.**X**
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: User Data Preference
4	# Template Name: **(Template name of Address book)**
5	# Description: **(Contents set in [Description] of the template)**
6	# Authentication Method (0=none or user code/1=others): **(0 or 1)**
7	"**(Row name)**"
8	"**(Value that corresponds to row name)**"

In line six, specify "0" for user code authentication or no authentication, or specify "1" for another authentication method.

The "Row name" in line seven, and their corresponding values of line eight and subsequent lines, are as follows:

Note

- The item in the parenthesis () under each item of the column names is the item name displayed on the setting screen of a template.

Row names and their corresponding values

Row name	Value of line 8 and subsequent lines
Index in ACLs and Groups	Enter a number to use as the entry number in CSV files. The item specified by this number will be used in "Access Privilege to User", "Access Privilege to Protected Files" or "Groups". Each entry number in a CSV file must be unique.
Name (User Name)	Enter the name of the entry. This entry is required. Enter up to 20 characters.
Set General Settings (Set)	Specify whether or not to configure the device. 0: Do not configure the device 1: Configure the device
Set Registration No. (Specify Registration No.)	Specify whether or not to set the registration number. 0: Do not set the registration number 1: Set the registration number
Registration No. (Registration No.)	Enter the registration number. Enter a unique number that does not match other registration numbers. Enter a value between 1 and 50,000. If the value is empty, a registration number is assigned automatically on the device side.
Entry Type	Select the type of entry from User (Account) or Group. U: Account G: Group
Display Name (Key Display Name)	Enter the user display name. Up to 16 characters can be entered. If a display name is not specified, it will be specified automatically using up to 16 characters.
Phonetic Name (Index)	This item cannot be specified.

Row name	Value of line 8 and subsequent lines
Display Priority (Display Priority)	Specify the display priority. The priority does not apply if no value is specified. Enter a value between 1 and 10.
Set Title Settings (Set)	Specify whether or not to specify an index. 0: Do not configure the settings 1: Configure the settings
Title 1 (Title 1)	Specify the index registered in Index Set 1. 0: Do not register 1 to 10: "AB"-"XYZ"
Title 2 (Title 2)	Specify the index registered in Index Set 2. 0: Do not register 1 to 10: "1"-"10"
Title 3 (Title 3)	Specify the index registered in Index Set 3. 0: Do not register 1 to 10: "1"-"5"
Title Freq. (Add to Freq.)	Specify whether or not to register the entry in the commonly used index. 0: Do not register 1: Register
Set User Code Settings (Set)	Specify whether or not to specify the user code. 0: Do not configure the settings 1: Configure the settings
User Code (User Code)	Specify the user code assigned to a user. The code must be unique. Up to 8 characters can be entered.
Set Auth. Info Settings (Set)	Specify whether or not to configure the login authentication settings. 0: Do not configure the settings 1: Configure the settings

Row name	Value of line 8 and subsequent lines
Device Login User Name (Login User Name)	Enter the user name to log in to a device. Up to 32 characters can be entered. The following characters cannot be used: colons, double quotation marks, and spaces.
Device Login Password (Login Password)	This item cannot be specified.
Device Login Password Encoding	This item cannot be specified.
SMTP Authentication (SMTP Authentication)	Specify whether or not to configure the SMTP authentication settings. 0: Do not specify 1: Use the login authentication information 2: Use other authentication information
SMTP Authentication Login User Name (User Name)	Enter the user name for SMTP authentication. Up to 191 characters can be entered. The following character cannot be used: space.
SMTP Authentication Login Password (Password)	This item cannot be specified.
SMTP Authentication Password Encoding	This item cannot be specified.
Folder Authentication (Folder Authentication)	Specify whether or not to configure the folder authentication settings. 0: Do not specify 1: Use the login authentication information 2: Use other authentication information
Folder Authentication Login User Name (User Name)	Enter the user name for folder authentication. Up to 128 characters can be entered.
Folder Authentication Login Password (Password)	This item cannot be specified.

Row name	Value of line 8 and subsequent lines
Folder Authentication Password Encoding	This item cannot be specified.
LDAP Authentication (LDAP Authentication)	Specify whether or not to configure the LDAP authentication settings. 0: Do not specify 1: Use the login authentication information 2: Use other authentication information
LDAP Authentication Login User Name (User Name)	Enter the user name for LDAP authentication. Up to 128 characters can be entered.
LDAP Authentication Login Password (Password)	This item cannot be specified.
LDAP Authentication Password Encoding	This item cannot be specified.
Set Access Control Settings (Set)	Specify whether or not to configure the usage restriction settings. 0: Do not configure the settings 1: Configure the settings
Can Use B/W Copy (Copier)	Specify the type of colors used in the Copy function. 0: Do not enable Black & White copy 1: Enable Black & White copy The selection becomes valid only when it is specified in certain combinations with other items. For details, see Note.
Can Use Single Color Copy (Copier)	Specify the type of colors used in the Copy function. 0: Do not enable Black & White and Single Color copy 1: Enable Black & White and Single Color copy The selection becomes valid only when it is specified in certain combinations with other items. For details, see Note.

Row name	Value of line 8 and subsequent lines
Can Use Two Color Copy (Copier)	Specify the type of colors used in the Copy function. 0: Do not enable Black & White, Single Color, and Two Color copy 1: Enable Black & White, Single Color, and Two Color copy The selection becomes valid only when it is specified in certain combinations with other items. For details, see Note.
Can Use Full Color Copy (Copier)	Specify the type of colors used in the Copy function. 0: Do not enable Full Color copy 1: Enable Full Color copy The selection becomes valid only when it is specified in certain combinations with other items. For details, see Note.
Can Use Auto Color Copy (Copier)	Specify the type of colors used in the Copy function. 0: Do not enable Auto Color copy 1: Enable Auto Color copy The selection becomes valid only when it is specified in certain combinations with other items. For details, see Note.
Can Use B/W Print (Printer)	Specify the type of colors used in the Print function. 0: Do not enable Black & White printing 1: Enable Black & White printing
Can Use Color Print (Printer)	Specify the type of colors used in the Print function. 0: Do not enable Black & White and Color printing 1: Enable Black & White and Color printing "Can Use Color Print" can be set to "1" only when "Can Use B/W Print" is also set to "1".
Can Use Scanner (Scanner)	Specify the scanner usage restrictions. 0: Restrict scanner usage 1: Do not restrict scanner usage
Can Use Fax (Fax)	Specify the fax usage restrictions. 0: Restrict fax usage 1: Do not restrict fax usage

Row name	Value of line 8 and subsequent lines
Can Use Document Server (Document Server)	Specify the Document Server usage restrictions. 0: Restrict Document Box usage 1: Do not restrict Document Box usage
Maximum of Print Usage Limit (Limit Value for Print Volume Use Limitation)	Enter the maximum value of print usage. Enter a value between 0 and 999,999. If you do not need to set the print usage limit, leave the item blank.
Set Email/Fax Settings (Set)	Specify whether or not to configure the fax and e-mail settings. 0: Do not configure the settings 1: Configure the settings
Fax Destination (Fax Destination)	Enter the fax number or IP fax address. Up to 128 characters can be entered. To combine the sub address with UUI, enter the address in the order of UUI-sub address. Enter "^" between the IP fax address and address extension.
Fax Line Type (Select line type.)	Select the type of phone line to use from the following: g3, ext (G3 internal line), g4, g4 (G4 internal line), ig3, ig3_ext (I-G3 internal line), g3_auto (G3 unused line), ext_auto (G3 unused line, internal line), g3_1, g3_1_ext (G3-1 internal line), g3_2, g3_2_ext (G3-2 internal line), g3_3, g3_3ext (G3-3 internal line, h323, sip)
International Fax Transmission Mode (International Transmission Mode)	Specify whether or not to enable the international transmission mode. 0: Disable 1: Enable
E-mail Address (Address)	Enter the e-mail address. Up to 128 characters can be entered. Usable characters include alphanumeric characters and the following symbols: !, #, $, %, &, ', *, +, -, /, =, ?, ^, _, `, {, |, }, ~, ., @

Row name	Value of line 8 and subsequent lines
Ifax Address (Address)	Enter the destination e-mail address for Internet fax. Up to 128 characters can be entered. Usable characters include alphanumeric characters and the following symbols: !, #, $, %, &, ', *, +, -, /, =, ?, ^, _, `, {, |, }, ~, ., @
Ifax Enable (Use This Email Address for Email and Internet Fax)	Specify whether to use the e-mail address as the Internet fax destination only, or as both the e-mail and Internet fax destinations. 0: E-mail and Internet fax 1: Internet fax only
Direct SMTP (Use This Email Address for Internet Fax)	Specify whether or not to send e-mail via an SMTP server (not using the SMTP Direct function). 0: Send via SMTP server 1: Do not send via SMTP server
Ifax Direct SMTP (Internet Fax - via SMTP Server)	Specify whether or not to send Internet faxes via an SMTP server (not using the SMTP Direct function). 0: Send via SMTP server 1: Do not send via SMTP server
Fax Header (Fax Header)	Enter the sender name to be printed. 0: Do not Set 1: 1 Name 2: 2 Name 3: 3 Name 4: 4 Name 5: 5 Name 6: 6 Name 7: 7 Name 8: 8 Name 9 : 9 Name 10 : 10Name

Row name	Value of line 8 and subsequent lines
Label Insertion 1st Line (Selection) (Label Insertion)	Specify whether or not to use merge print. 0: Do not use merge print 1: Use merge print
Label Insertion 2nd Line (String) (Label Insertion 2nd Line (String))	Specify the string to print on the second line when using merge print. Up to 28 characters can be entered.
Label Insertion 3rd Line (Standard Message) (Label Insertion 3rd Line (Standard Message))	Specify the string to print on the third line when using merge print. 0: Do not print 1 to 4: Print the corresponding pre-registered text
Set Folder Settings (Set)	Specify whether or not to configure folders. 0: Do not configure the settings 1: Configure the settings
Folder Protocol (Protocol)	Select the Protocol to use. 0: SMB 1: FTP 2: NCP-Bindery 3: NCP-NDS
Folder Port No. (Port Number)	Enter the port number to use in FTP. Enter a value between 1 and 65,535.
Folder Server Name (Server Address)	Enter the server name to use in FTP. Up to 128 characters can be entered.
Folder Path (Path)	Enter the path name. Up to 256 characters can be entered.
Folder Japanese Character Encoding (Japanese Character Code Set)	This item cannot be specified.
Set Protection Settings	Specify whether or not to configure the authentication protection settings. 0: Do not configure the settings 1: Configure the settings

Row name	Value of line 8 and subsequent lines
Is Setting Destination Protection (Register as Destination)	Specify whether or not to use the entry as a destination. 0: Do not use the entry as a destination 1: Use the entry as a destination
Is Protecting Destination Folder (Protect Dest.)	Specify whether or not to protect the folder destination. 0: Do not protect 1: Protect
Is Setting Sender Protection (Register as Sender)	Specify whether or not to use the entry as the sender. 0: Do not use the entry as the sender 1: Use the entry as the sender
Is Protecting Sender (Protect Sender)	Specify whether or not to protect the sender. 0: Do not protect 1: Protect
Sender Protection Password (Protection Code)	This item cannot be specified.
Sender Protection Password Encoding	This item cannot be specified.
Access Privilege to User (Access Control List for Destination Protection Settings)	Specify the access privilege of the folder destinations. Specify the privilege by entering the "Index in ACLs and Groups" number and one of the following letters: R: Viewing allowed W: Editing allowed D: Editing/deleting allowed X: Full control To specify multiple groups, separate each group using a comma. For example, to set the access privilege of entries whose "Index in ACLs and Groups" is "10" to "viewing only", and entries whose index number is "20" to "full control", enter "10R,20X". When "0" is specified, all entries are subject to change.
Access Privilege to Protected File (Access Control List for Document Protection Settings)	Specify the protection privilege of documents stored in the Document Server. The same setting as Access Privilege to User applies.

Row name	Value of line 8 and subsequent lines
Set Group List Settings (Set)	Specify whether or not to specify the groups to which users will be assigned. 0: Do not configure the settings 1: Configure the settings
Groups	Enter the "Index in ACLs and Groups" number to specify the group to which the user is assigned. To specify multiple groups, separate each group using a comma.
Set Counter Reset Settings (Set)	Specify whether or not to configure the counter reset settings. 0: Do not configure the settings 1: Configure the settings
Enable Plot Counter Reset (Print (Copier, Fax Print, Printer))	Specify whether or not to reset the print counter in the copier, printer, and fax functions. 0: Do not reset the counter 1: Reset the counter
Enable Fax Counter Reset (Fax Transmission)	Specify whether or not to reset the fax usage counter. 0: Do not reset the counter 1: Reset the counter
Enable Scanner Counter Reset (Scanner)	Specify whether or not to reset the scanner usage counter. 0: Do not reset the counter 1: Reset the counter
Enable User Volume Counter Reset (Volume Used)	Specify whether or not to reset the print usage counter. 0: Do not reset the counter 1: Reset the counter

Note

- Do not change the information in lines one through three, as this information is used for identification.
- The values of "Can Use B/W Copy", "Can Use Single Color Copy", "Can Use Two Color Copy", "Can Use Full Color Copy", and "Can Use Auto Color Copy" must be specified in one of the following combinations:
  - [0,0,0,0,0], [1,0,0,0,0], [1,1,0,0,0], [1,1,1,0,0], [1,1,1,1,0], [1,1,1,1,1]

- For the CSV format of the Address Management Tool and User Management Tool, which are used by SmartDeviceMonitor for Admin/Ridoc IO Analyzer, see the instruction manual for SmartDeviceMonitor for Admin/Ridoc IO Analyzer.

Format of a Device Log CSV File

The following field names and their corresponding values are exported to the device log CSV file. A description of each field name is as follows:

Job Log

A job log CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	#Job Log
2	#Format Version **X.X.X.X**
3	GMT"**(time zone)**"

In the fourth line and thereafter, a value that is specific to the device is exported for each line.

general

Field name	Explanation
general#logVersion	log version number
general#logSourceId	device serial number
general#logSourceId_sId	device alias ID
general#logId	log ID
general#logLinkId	job ID
general#sourcePropNum	total number of source properties
general#destinationPropNum	total number of destination properties
general#accessPropNum	total number of access properties
general#finishState	status/results

Field name	Explanation
general#occurrenceDate	time of occurrence
general#entryDate	start time (log information registered without being processed)
general#entryDate_c	start time (corrected by service)
general#entryValidTimeFlag	reliability of corresponding start time information
general#finishDate	end time (log information registered without being processed)
general#finishDate_c	end time (corrected by service)
general#finishValidTimeFlag	reliability of corresponding end time information
general#originalType	detailed job type
general#clientName	user code/user name (type + value)
general#clientNameType	user code/user name type
general#clientNameBody	value of user code/user name
general#clientName_sId	alias ID of the value of user code/user name
general#displayName	user display name
general#operation	performed from
general#hostAddress	address of request issuer
general#hostAddressType	address type of request issuer
general#hostAddressBody	address value of request issuer
general#reportId	log ID of the status notification issuer
general#entryId	entry ID
general#joblogNumber	job log number
general#bindId	bind ID
general#jobRsvId	reservation number
general#specialMention	completion status

Field name	Explanation
general#sdkApliInfo	Device Application information
general#billingCode	Classification Code (code for billing according to usage)
general#machineCooperationLogId	remote information: machine ID information
general#machineCooperationNum	remote information: log ID
general#registDate	registered time in RICOH Streamline NX log

source_scan

Field name	Explanation
source_scan#parentLogId	parent log ID
source_scan#parentLinkId	parent link ID
source_scan#subLogId	sublog ID
source_scan#subJobType	subjob type
source_scan#scanSubState	status/results
source_scan#scanStartTime	start time (log information registered without being processed)
source_scan#scanStartTime_c	start time (corrected by service)
source_scan#scanStartValidTimeFlag	reliability of corresponding start time information
source_scan#scanEndTime	end time (log information registered without being processed)
source_scan#scanEndTime_c	end time (corrected by service)
source_scan#scanEndValidTimeFlag	reliability of corresponding end time information
source_scan#scanOriginalSidePages	original pages
source_scan#scanColorMode	color mode
source_scan#scanOriginalKind	type of original
source_scan#scanResolutionV	scan resolution(main scan)
source_scan#scanResolutionH	scan resolution (secondary scan)

Field name	Explanation
source_scan#scanOriginalSizeName	original size name
source_scan#scanOriginalSizeV	original size (main scan)
source_scan#scanOriginalSizeH	original size (secondary scan)
source_scan#scanSubStatusDetail	reason of abnormal termination

source_memory

Field name	Explanation
source_memory#parentLogId	parent log ID
source_memory#parentLinkId	parent link ID
source_memory#subLogId	sublog ID
source_memory#subJobType	subjob type
source_memory#srcMemSubState	status/results
source_memory#srcMemStorePages	stored pages
source_memory#srcMemDocumentName	stored file name
source_memory#srcMemDocumentId	stored file ID
source_memory#srcMemDevice	stored device
source_memory#srcMemPdlName	PDL name
source_memory#srcMemCreatePages	created pages
source_memory#srcMemIntensive	layout
source_memory#srcMemBindBook	book/poster
source_memory#srcMemMagnification	enlarge/reduce
source_memory#srcMemPoster	poster
source_memory#srcMemStamp	stamp
source_memory#srcMemUserId	user ID
source_memory#srcMemCreateDate	create date

Field name	Explanation
source_memory#srcMemCreateTime	create time
source_memory#srcMemTrackId	track ID
source_memory#srcMemPdlDocumentName	print document name
source_memory#srcMemPcLoginName	login name
source_memory#srcMemPcLoginName_sId	alias ID of the login name
source_memory#srcMemPcName	computer name
source_memory#srcMemPcName_sId	alias ID of the computer name
source_memory#srcMemPcLoginComp_sId	alias ID of the login name and computer name
source_memory#srcMemPcPortName	port name
source_memory#srcMemPcPrinterName	printer name
source_memory#srcMemClientUserName	client user name
source_memory#srcMemJobDocumentName	document name
source_memory#srcMemJobPassword	password presence
source_memory#srcMemColorMode	color mode
source_memory#srcMemTonerSaveMode	toner saving
source_memory#srcMemFolderName	source folder name
source_memory#srcMemFolderNo	folder number of stored files
source_memory#srcMemSubStatusDetail	reason of abnormal termination

source_network

Field name	Explanation
source_network#parentLogId	parent log ID
source_network#parentLinkId	parent link ID
source_network#subLogId	sublog ID
source_network#subJobType	subjob type

Field name	Explanation
source_network#srcNetSubState	status/results
source_network#srcNetStartTime	start time (log information registered without being processed)
source_network#srcNetStartTime_c	start time (corrected by service)
source_network#srcNetStartValidTimeFlag	reliability of corresponding start time information
source_network#srcNetEndTime	end time (log information registered without being processed)
source_network#srcNetEndTime_c	end time (corrected by service)
source_network#srcNetEndValidTimeFlag	reliability of the corresponding end time information
source_network#srcNetReceiveName	sender name
source_network#srcNetReceiveKind	type of line (reception)
source_network#srcNetReceiveMode	reception mode
source_network#srcNetReceivePages	received pages
source_network#srcNetFileNo	file number of fax
source_network#srcNetSourceAddress	destination (IP address/fax number)
source_network#srcNetSubStatusDetail	reason of abnormal termination

source_pdl

Field name	Explanation
source_pdl#parentLogId	parent log ID
source_pdl#parentLinkId	parent link ID
source_pdl#subLogId	sublog ID
source_pdl#subJobType	subjob type
source_pdl#pdlSubState	status/results
source_pdl#pdlStartTime	start time (log information registered without being processed)

Field name	Explanation
source_pdl#pdlStartTime_c	start time (corrected by service)
source_pdl#pdlStartValidTimeFlag	reliability of corresponding start time information
source_pdl#pdlEndTime	end time (log information registered without being processed)
source_pdl#pdlEndTime_c	end time (corrected by service)
source_pdl#pdlEndValidTimeFlag	reliability of corresponding end time information
source_pdl#pdlName	PDL name
source_pdl#pdlCreatePages	created pages
source_pdl#pdlIntensive	combine
source_pdl#pdlBindBook	book/poster
source_pdl#pdlMagnification	enlarge/reduce
source_pdl#pdlPoster	poster
source_pdl#pdlStamp	stamp
source_pdl#pdlUserId	user ID
source_pdl#pdlCreateDate	create date
source_pdl#pdlCreateTime	create time
source_pdl#pdlTrackId	track ID
source_pdl#pdlDocumentName	print document name
source_pdl#pdlPcLoginName	login name
source_pdl#pdlPcLoginName_sId	alias ID of the login name
source_pdl#pdlPcName	computer name
source_pdl#pdlPcName_sId	alias ID of the computer name
source_pdl#pdlPcLoginComp_sId	alias ID of the login name and computer name
source_pdl#pdlPcPortName	port name
source_pdl#pdlPcPrinterName	printer icon name

Field name	Explanation
source_pdl#pdlClientUserName	client user name
source_pdl#pdlJobDocumentName	document name
source_pdl#pdlJobPassword	password presence
source_pdl#pdlColorMode	color mode
source_pdl#pdlTonerSaveMode	toner saving
source_pdl#pdlSubStatusDetail	reason of abnormal termination

source_inner

Field name	Explanation
source_inner#parentLogId	parent log ID
source_inner#parentLinkId	parent link ID
source_inner#subLogId	sublog ID
source_inner#subJobType	subjob type
source_inner#innSubState	status/results
source_inner#innReportIndicate	report type: originated from
source_inner#innReportAuto	auto output
source_inner#innSubStatusDetail	reason of abnormal termination

destination_memory

Field name	Explanation
destination_memory#parentLogId	parent log ID
destination_memory#parentLinkId	parent link ID
destination_memory#subLogId	sublog ID
destination_memory#subJobType	subjob type
destination_memory#desMemSubState	status/results
destination_memory#desMemStartTime	start time (log information registered without being processed)

Field name	Explanation
destination_memory#desMemStartTime_c	start time (corrected by service)
destination_memory#desMemStartValidTimeFlag	reliability of corresponding start time information
destination_memory#desMemEndTime	end time (log information registered without being processed)
destination_memory#desMemEndTime_c	end time (corrected by service)
destination_memory#desMemEndValidTimeFlag	reliability of corresponding end time information
destination_memory#desMemStorePages	stored pages
destination_memory#desMemDocumentName	file name
destination_memory#desMemDocumentId	file ID
destination_memory#desMemDevice	stored device
destination_memory#desMemFolderName	source folder name
destination_memory#desMemFolderNo	folder number of stored files
destination_memory#desMemSubStatusDetail	reason of abnormal termination

destination_network

Field name	Explanation
destination_network#parentLogId	parent log ID
destination_network#parentLinkId	parent link ID
destination_network#subLogId	sublog ID
destination_network#subJobType	subjob type
destination_network#desNetSubState	status/results
destination_network#desNetStartTime	start time (log information registered without being processed)
destination_network#desNetStartTime_c	start time (corrected by service)

Field name	Explanation
destination_network#desNetStartValidTimeFlag	reliability of corresponding start time information
destination_network#desNetEndTime	end time (log information registered without being processed)
destination_network#desNetEndTime_c	end time (corrected by service)
destination_network#desNetEndValidTimeFlag	reliability of corresponding end time information
destination_network#desNetAddressName	destination name
destination_network#desNetAddress	destination (number/address)
destination_network#desNetSendKind	transmission (line) type
destination_network#desNetSendOwner	sender
destination_network#desNetSendMode	transmission mode
destination_network#desNetSendPages	transmitted sheets
destination_network#desNetFileNo	file number of fax
destination_network#desNetSubStatusDetail	reason of abnormal termination

destination_plot

Field name	Explanation
destination_plot#parentLogId	parent log ID
destination_plot#parentLinkId	parent link ID
destination_plot#subLogId	sublog ID
destination_plot#subJobType	subjob type
destination_plot#plotSubState	status/results
destination_plot#plotStartTime	start time (log information registered without being processed)
destination_plot#plotStartTime_c	start time (corrected by service)
destination_plot#plotStartValidTimeFlag	reliability of corresponding start time information

Field name	Explanation
destination_plot#plotEndTime	end time (log information registered without being processed)
destination_plot#plotEndTime_c	end time (corrected by service)
destination_plot#plotEndValidTimeFlag	reliability of corresponding end time information
destination_plot#plotPrintPages	print pages
destination_plot#plotCopies	copies
destination_plot#plotStaple	stapling position
destination_plot#plotPunch	punching position
destination_plot#plotOutMode	designation of print side
destination_plot#plotColorMode	color mode
destination_plot#plotPaperKind	paper type
destination_plot#plotPaperSize	paper size
destination_plot#plotConnect	connect
destination_plot#plotPrintCountPlotKind	plotter type
destination_plot#plotPrintCountBKa	print count info-B&W large sizes
destination_plot#plotPrintCountBKb	print count info-B&W small sizes
destination_plot#plotPrintCount1Ca	print count info-single color large sizes
destination_plot#plotPrintCount1Cb	print count info-single color small sizes
destination_plot#plotPrintCount2Ca	print count infotwo-color large sizes
destination_plot#plotPrintCount2Cb	print count infotwo-color small sizes
destination_plot#plotPrintCountFCa	print count infofull color large sizes
destination_plot#plotPrintCountFCb	print count infofullcolor small sizes
destination_plot#plotPrint-CountYMC	print count infocolor (YMC) development
destination_plot#plotPrintCountBK	print count infoblack development
destination_plot#plotBindbook	booklet

Field name	Explanation
destination_plot#plotCoverSheet	cover/slip sheet
destination_plot#plotIntensive	layout
destination_plot#plotMagnification	enlarge/reduce
destination_plot#plotPoster	poster
destination_plot#plotStamp	stamp
destination_plot#plotSubStatusDetail	reason of abnormal termination

Eco Log

An eco log CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	#Eco Log
2	#Format Version X.X.X.X

In line four and subsequent lines, the values that are specific to the device are written out line-by-line.

Field name	Explanation
general#deviceAddress	IP address of the device
general#serialNumber	serial number of the device
general#dateTime	device time/date log
ecology_ecology#logType	log type such as the power status change, paper consumption, power usage, and job type
ecology_ecology#powerMode	energy saver mode of the device
ecology_ecology#jobType	job type
ecology_ecology#jobInterval	job interval
ecology_ecology#jobProcessingTime	job processing time

Field name	Explanation
ecology_ecology#paperConsumptionLarge	number of pages larger than A4/Letter
ecology_ecology#paperConsumptionSmall	number of pages smaller than A4/Letter
ecology_ecology#paperConsumptionDuplexLarge	number of duplex printed pages larger than A4/Letter
ecology_ecology#paperConsumptionDuplexSmall	number of duplex printed pages smaller than A4/Letter
ecology_ecology#powerConsumptionStandy	controller standby status
ecology_ecology#powerConsumptionSTR	standby status
ecology_ecology#powerConsumptionMachineOff	power off status
ecology_ecology#powerConsumptionScanPrint	scanner or printer function

Access Log

An access log CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	#Access Log
2	#Format Version **X.X.X.X**

In line four and subsequent lines, the values that are specific to the device are written out line-by-line.

Field name	Explanation
Device Serial No.	serial number of the device
Start Date/Time	start time
End Date/Time	end time
Log Type	job type
Result	result
Operation Method	operation

Field name	Explanation
Status	status
User Entry ID	entry ID
User Code/User Name	user code/user name (type+value)
Log ID	log ID
Access Log Type	type of the subordinate job
Authentication Server Name	name of the authentication server
No. of Authentication Server Switches	switch number of the authentication server
Logout Mode	logout status
Login Method	authentication method
Login User Type	login type
Target User Entry ID	entry ID of the lock target user
Target User Code/User Name	user name of the lock target user
Registration No.	registration number of the target user
Address Book Operation Mode	operation mode of the address book
Address Book Change Item	modified item the address book
Client Address	requesting source of the authentication information
Lockout/Release	operation mode
Lockout/Release Method	operation mode (automatic or manual)
Lockout Administrators	administrator who lifted the lockout
Clear Counters	cleared counter
Export Range	target to be exported
File to Import	name of the imported file
Stored File ID	document ID
Stored File Name	document name
File Location	location of the deleted file

Field name	Explanation
Collect Job Logs	log related setting: job log function
Collect Access Logs	log related setting: access log function
Collect Eco-friendly Logs	log related setting: ecology log
Transfer Logs	log related setting: log transfer
Encrypt Logs	log related setting: device log encryption
Log Type	log type setting: log type
Log Collect Level	log type setting: log collection level
Encryption/Cleartext	whether the communication log was encrypted or not
Machine Port No.	port number of the device
Protocol	protocol (TCP or UDP)
IP Address	IP address of the communication destination
Port No.	port number of the communication destination
MAC Address	MAC address of the communication destination
Primary Communication Protocol	primary protocol name
Secondary Communication Protocol	secondary protocol name
Encryption Protocol	encryption protocol name
Communication Direction	communication destination
Communication Start Log ID	log ID
Communication Start/End	communication start/end time identifier
Network Attack Status	network attack status
Network Attack Type	network attack type
Network Attack Type Details	network attack type (details)
Network Attack Route	network attack route
Login User Name used for Network Attack	name of the user who was used in the network attack

Field name	Explanation
Add/Update/Delete Firmware	firmware update mode
Module Name	module name
Parts Number	parts number
Version	updated version
Machine Data Encryption Key Operation	type of machine data encryption operation
Machine Data Encryption Key Type	type of machine data encryption key
Validity Error File Name	name of the file in which an error has been detected
Configuration Category	configuration information (setting category)
Configuration name	configuration information (setting)
Configuration value	configuration information (setting value)
Destination Sever Name	server name
Hdd Init Partition No.	HDD partition number
Access Result	access result

Format of a Local User CSV File

A local user information CSV file is written out in the format indicated below:

The variables are indicated in **bold letters**.

Line number	Contents
1	# Format Version: **X.X.X.X**
2	# Generated at: **(Date/time of write-out)**
3	# Function Name: Users
4	# **(Item name of the column)**
5	"**(Column name of the database)**"

Line number	Contents
6	"(Value of the device that corresponds to the item name of the column)"

The "Item name of the column", "Column name of the database ", and their row number, are as follows.

Item name of the column and Column name of the database

Row number	Item name of the column	Column name of the database
1	User Name	slnxuser_name
2	Authentication Profile	auth_name
3	Display Name	slnxuser_displayname
4	Email	slnxuser_email
5	User Home Folder	slnxuser_homefolder
6	Department	slnxdep_name
7	Default Cost Center	slnxuser_defaultcc
8	Permission	slnxperm_name
9	LDAP Synchronization	slnxuser_synflag
10	Enforce Color Page Limit	slnxuser_enforce_colorbalance
11	Enforce Account Limit	slnxuser_enforce_balance
12	Default Color Page Limit	slnxuser_colorquota
13	Color Page Balance	slnxuser_colorbalance
14	Default Account Limit	slnxuser_quota
15	Account Balance	slnxuser_balance

Note

- Do not change the information in lines one through three, as this information is used for identification.

Using Device Log Export Tool

The Device Log Export tool allows an Administrator to export a job log to a CSV format file in a specified folder. The command line tool must be run on the Delegation Server that manages the device from which you want to export the log. In cases where you have more than one Delegation Server, you can install the Device Log Export tool on each Delegation Server.

These instructions explain how to export a job log from the Command prompt.

1. **Open a command prompt and navigate to the installation path of RICOH Streamline NX (by default the path where the tool is located is c:\Program Files\Ricoh\ RICOH Streamline NX \tools\DeviceLogExportingTool, but the full path may be different in your installation).**
2. **Optionally, configure the following parameters in the file '\DeviceLogExportingTool \config.properties' prior to running the .bat file in the step below.**

   These options allow you to specify the output settings that will be applied when a job log is exported.

Parameter	Default Value	Description
output.folder	" "	• Folder path for output of the job log. • Specify the folder path for outputting the job log. • If this parameter is empty, it outputs to the directory that stored the .bat file.
output.filename	" "	• File name for output of the job log. • Specify the file name for output the job log. If you do not set this parameter, it saves as the following name: deviceJobLog-[start date] [end date].csv • If the specified file already exists, the new file will overwrite the existing file.

output.encode	UTF-8	File encoding for the output job log.
		• Options are either UTF-8 or Shiftjis:
		  • UTF-8: Output the encoding of the csv file is UTF-8.
		  • Shiftjis: Output the encoding of the csv file encode is Shift-JIS.

Parameter	Default Value	Description
devicelog.timetype	GMT	Specify the time zone as either GMT or LocalTime: • GMT: Output the date as GMT (Greenwich mean time). The date format is YYYY-MM-DDThh:mm:ssZ when "GMT" is selected. • LocalTime: Output the date as Local time of the server. The date format is YYYY-MM-DDThh:mm:ss as local time of the server when "LocalTime" is selected. • Time conversion information (i.e. GMT+540) is recorded in the third line of the exported .csv file.
devicelog.isRegistDate	true	Target the registDate of the output job log: • false: To determine the scope of output in the occurrence date (occurrenceDate) of Device Log. • true: To determine the scope of output in the registration date (registDate) of Device Log.

3. Optionally, configure the following parameters in the file '\DeviceLogExportingTool \result.properties' prior to running the .bat file in the step below.

When the application runs for the first time, it records the date of execution to 'result.properties'. The next time you run the application, it will use the last recorded date of execution to output the job log for the period between the last recorded executed date and the date prior to the current date (yesterday).

If the devicelog.lastExecutedDate parameter is empty (as it will be the first time you run the application), the job log will contain data from the oldest possible information available to the date prior to the current date (yesterday).

Parameter	Default Value	Description
devicelog.lastExecuted Date	" "	• Last executed date is updated each time you run the application. • You can edit this parameter manually as needed.

4. Run the command 'DeviceLogExportingTool.bat'.

Note

- To schedule this task using Windows Scheduler, refer to the technical information provided by Microsoft at https://technet.microsoft.com/library/Cc748993.aspx.
- The job log will be export as per the settings in the config. Properties file. The devicelog.timetype and devicelog.isRegistDate parameters determine the output in the following columns:

general#registDate	source_pdl#pdlStartTime_c
general#occurrenceDate	source_pdl#pdlEndTime
general#entryDate	source_pdl#pdlEndTime_c
general#entryDate_c	destination_memory#desMemStartTime
general#finishDate	destination_memory#desMemStartTime_c
general#finishDate_c	destination_memory#desMemEndTime
source_scan#scanStartTime	destination_memory#desMemEndTime_c
source_scan#scanStartTime_c	destination_network#desNetStartTime
source_scan#scanEndTime	destination_network#desNetStartTime_c
source_scan#scanEndTime_c	destination_network#desNetEndTime
source_network#srcNetStartTime	destination_plot#plotStartTime
source_network#srcNetStartTime_c	destination_plot#plotStartTime_c
source_network#srcNetEndTime	destination_plot#plotEndTime
source_network#srcNetEndTime_c	destination_plot#plotEndTime_c
source_pdl#pdlStartTime	

Filtering the Log

To specify which items are included in the exported CSV file, edit the 'filterJobLog.text file' located in <Install path>\tools\DeviceLogExportingTool.

For any items you do not want to include in the CSV file, add a '#' symbol at the beginning of the item, or remove the item from the file completely.

For example:

```
[general]
finishState
entryDate
#entryValidTimeFlag…Not output item
finishDate
finishValidTimeFlag
```

List of Communication Port Numbers (1)

This is a list of communication port numbers used in the RICOH Streamline NX system.

Overview

Communication with Device

Operation	Sender → Destination	Protocol	Port Number
Collecting and Configuring device information	Delegation Server → Device	SNMP	UDP/161
		HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443
		HTTP or HTTPS	TCP/80 or TCP/443
		HTTPS/SOAP	TCP/7443
		HTTPS	TCP/51443
		FTP or SFTP	TCP/21, TCP22 or TCP/10021
Notify device information	Device → Delegation Server	SNMP	UDP/162
		HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090) or TCP/52443
		HTTPS	TCP/443

Note

- You can change the port number of the SFTP protocol using the Management Console. For details, see page 522 "Networking".

Communication with external systems

Operation	Sender → Destination	Protocol	Port Number
DNS resolution	Delegation Server → DNS Server	DNS	UDP/53 or TCP/53
Authentication	Core Server → LDAP Server	LDAP or LDAPS	TCP/ Port Number of LDAP Server (default: 389)
Activation/Deactivation	Core Server → Ricoh Software Server	HTTPS	TCP/443
Usage reports	Core Server → Ricoh Backend Server	HTTPS	TCP/443
Notification	Core Server → Email Server	SMTP/SMTPS or POP	TCP/25, TCP/587 or 110
Dispatch files	Core Server → Network drive	SMB/CIFS	TCP/445

Note

- You can change the port number of the SMTP protocol using the Management Console. For details, see page 522 "Networking".

Common

Operation	Sender → Destination	Protocol	Port Number
Operate UI	Management Console → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)

Operation	Sender → Destination	Protocol	Port Number
with IIS	Management Console → IIS	HTTP or HTTPS	TCP/ Port Number of IIS (default: 80)
	IIS → Core Server (Redirect)	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)
external Database	Core Server → Database (SQL Server)	JDBC	TCP/ Port No of the Database (default: SQL: 1433)
Synchronize data	Delegation Server → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)

Tools

Operation	Sender → Destination	Protocol	Port Number
Certificate Management Tool	Certificate Management Tool → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)
	Certificate Management Tool → Device	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443
	Certificate Management Tool → SCEP server	HTTP or HTTPS	TCP/80 or TCP/443

Other Ricoh products

Operation	Sender → Destination	Protocol	Port Number
Printer Driver Packager NX	Printer Driver Packager NX → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)
@Remote Connector NX	@Remote Connector NX → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server (default: 8080)

Discovery

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
DNS resolution (Delegation Server → DNS Server)	DNS	UDP/53 or TCP/53	-
Collecting device information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting detail device information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Confirming the Device Administrator account. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Configuring device log collection setting. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Configuring SNMP Trap setting. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Write Community or SNMP V3 access account
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Network Device with FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
DNS resolution (Delegation Server → DNS Server)	DNS	UDP/53 or TCP/53	-
Collecting device information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

USB Device

Operation (Sender → Destination)	Protocol	Port Number	Access Account
DNS resolution (Streamline NX → DNS Server)	DNS	UDP/53 or TCP/53	-
Collecting device information. (Delegation Server → PC)	SNMP	UDP/161	SNMP V1/V2: The value of Read Community Name is fixed to "Public".

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling

Polling (Status)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device status information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting detail device information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Network Device with FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device status information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

USB Device

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device status information. (Delegation Server → PC)	SNMP	UDP/161	SNMP V1/V2: The value of Read Community Name is fixed to "Public".
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling (Tray, Toner/Ink)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Tray/Toner Ink information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting device Toner detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Network Device with FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Tray/Toner Ink information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

USB Device

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Tray/Toner Ink information. (Delegation Server → PC)	SNMP	UDP/161	SNMP V1/V2: The value of Read Community Name is fixed to "Public".
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling (Counter)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Counter information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting detail device information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Network Device with FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Counter information. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

USB Device

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Counter information. (Delegation Server → PC)	SNMP	UDP/161	SNMP V1/V2: The value of Read Community Name is fixed to "Public".
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling (Other)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Other information, such as MAC address, etc. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community <or> SNMP V3 access account
Collecting detail device information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Configure the device's SDK/J Platform to install the SLNX Device Management Extension (Delegation Server → Device)	HTTPS	TCP/51443	SDK account
Collecting DOSS / HDD Encryption information (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Collecting DOSS / HDD Encryption information (Delegation Server with SLNX Management Extension → Device)	HTTPS	TCP/51443	-
Collecting SDK information and Firmware information (Delegation Server → Device)	FTP/SFTP and HTTPS	TCP/21 or TCP/22 TCP/51443	Device Administrator account and SDK account
Collecting SmartSDK information (Delegation Server → Device)	HTTP or HTTPS	TCP/80 Or TCP/443	Device Administrator account
Collecting SOP information (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Network Device with FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Other information, such as MAC address, etc. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

USB Device

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting device Other information, such as MAC address, etc. (Delegation Server → PC)	SNMP	UDP/161	SNMP V1/V2: The value of Read Community Name is fixed to "Public".
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling (User Counter)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting User Counter information. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Polling (Detailed Counter)

Network Device without FMAudit Engine

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting Detail Counter information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Notify device information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Device-specific Preferences

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting preference information. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Configuring device preferences. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Standard Device Preferences

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Configure the device's SDK/J Platform to install the SLNX Device Management Extension (Delegation Server → Device)	HTTPS	TCP/51443	SDK account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Collecting preference information. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Collecting preference information. (Service Program items) (Delegation Server with SLNX Management Extension → Device)	HTTPS	TCP/51443	-
Configuring device preferences. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
	HTTP or HTTPS	TCP/80 or TCP/443	Device Administrator account
	SNMP	UDP/161	SNMP V1/V2: Write Community or SNMP V3 access account
Configuring device preferences. (SP items) (Delegation Server with SLNX Management Extension → Device)	HTTPS	TCP/51443	-
Restarting the device. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Address Book

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Collecting Address Book information. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Configuring the Address Book. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Power Mode

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Configuring the power mode. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Write Community or SNMP V3 access account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Reboot Task

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Restarting the device. (Delegation Server → Device)	SNMP or HTTP/SOAP or HTTPS/SOAP	UDP/161 or TCP/80 or TCP/443	SNMP V1/V2: Write Community or SNMP V3 access account or Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

SDK/J Platform

SDK/J Platform Update (Ricoh Software Server)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Download SDK/J Platform. (Delegation Server → Core Server)	HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Download SDK/J Platform. (Core Server → Ricoh Software Server)	HTTPS	TCP/443	Retained in Streamline NX
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's SDK/J Platform (Delegation Server → Device)	FTP and HTTPS	TCP/21 TCP/51443	Device Administrator account and SDK account
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Updating the device's SDK/J Platform (Delegation Server → Device)	HTTPS	TCP/51443	Device Administrator account and SDK account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

SDK/J Platform Update (Local file)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Confirming the device's SDK/J Platform (Delegation Server → Device)	FTP and HTTPS	TCP/21 TCP/51443	Device Administrator account and SDK account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Updating the device's SDK/J Platform (Delegation Server → Device)	HTTPS	TCP/51443	Device Administrator account and SDK account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

List of Communication Port Numbers (2)

Device Applications

Device Applications (Ricoh Software Server)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Download SDK/J Application (Delegation Server → Core Server)	HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Download SDK/J Application (Core Server → Ricoh Software Server)	HTTPS	TCP/443	Retained in Streamline NX
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Confirming the device's SDK/J Platform (Delegation Server → Device)	FTP/SFTP and HTTPS	TCP/21 and the other ports assigned by the device for FTP or TCP port number for SFTP on the device (default: 22) TCP/51443	Device Administrator account and SDK account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Installing/Updating/ Uninstalling/Activating the device's SDK App (Delegation Server → Device)	HTTPS	TCP/51443	Device Administrator account and SDK account
Restarting the device. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Device Applications (Local file)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's SDK/J Platform (Delegation Server → Device)	FTP/SFTP and HTTPS	TCP/21 and the other ports assigned by the device for FTP or TCP port number for SFTP on the device (default: 22) TCP/51443	Device Administrator account and SDK account
Configuring the device's SDK/J Platform to enable (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Installing/Updating/ Uninstalling/Activating the device's SDK App (Delegation Server → Device)	HTTPS	TCP/51443	Device Administrator account and SDK account
Restarting the device. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Firmware Update

Firmware update (Ricoh Software Server)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Download Firmware. (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Download Firmware. (Core Server → Ricoh Software Server)	HTTPS	TCP/443	Retained in Streamline NX
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Confirming the device's Firmware Information (Delegation Server → Device)	FTP or SFTP	TCP/21 or TCP/22	Device Administrator account
Collecting SmartSDK information (Delegation Server -> Device)	HTTP or HTTPS	TCP/80 Or TCP/443	Device Administrator account
Updating the device's Firmware (Delegation Server → Device)	FTP or SFTP	TCP/21 or TCP/22	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Firmware update (Local file)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Confirming the device's Firmware Information (Delegation Server → Device)	FTP or SFTP	TCP/21 or TCP/22	Device Administrator account
Collecting SmartSDK information (Delegation Server → Device)	HTTP or HTTPS	TCP/80 Or TCP/443	Device Administrator account
Updating the device's Firmware (Delegation Server → Device)	FTP or SFTP	TCP/21 or TCP/22	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

11

Log Collection

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device's response. (Delegation Server → Device)	SNMP	UDP/161	SNMP V1/V2: Read Community or SNMP V3 access account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirming the device detail information. (Delegation Server → Device)	HTTPS/SOAP	TCP/7443	-
Collecting log preference information. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Configuring device log preferences. (Delegation Server → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Notify task result (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

SNMP Trap

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify SNMP Trap. (Device → Delegation Server)	SNMP	UDP/162	SNMP V1/V2:Trap Community or SNMP V3 access account

Device Log (Jog Log, Access Log, Eco Log)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify Device Log. (Device → Delegation Server)	HTTP Or HTTPS	TCP/ Port Number of the Delegation Server	-

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Notify Device Log data. (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Report

"Save on Disk" is activated as "Delivery Methods".

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Report task	-	-	-
Save on Disk	SMB/CIFS	TCP/445	Account who starts up RICOH SLNX Central Manager Service

"Send by Email" is activated as "Delivery Methods".

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Report task	-	-	-
Send by Email	SMTP/SMTPS or POP	TCP/25, TCP/587 or 110	SMTP Authentication or Pop Authentication

Notifications

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Complete tasks Refer to the following functions. Addition, Update, Removal • Configuration Alerts • DM Communication Error	-	-	-
Notification (Core Server → Email Server)	SMTP/SMTPS or POP	TCP/25, TCP/587 or 110	SMTP Authentication or Pop Authentication

Activation/Deactivation

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Confirm the request for Activation/Deactivation. (Core Server → Ricoh Software Server)	HTTPS	TCP/443	Retained in Streamline NX

Usage Report Notification

Usage Reports is internet-based, so this communication must pass through the proxy server, if one is in use.

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Transmit usage reports (Core Server → Ricoh Backend Server)	HTTPS	TCP/443	Retained in Streamline NX

Common

Operate UI (including Mobile Access) with Internal Authentication

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (Management Console → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Internal User Account
Operate UI (Management Console → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Internal User Account

Operate UI (including Mobile Access) with external Authentication

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (Management Console → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	LDAP User Account
Authentication (Core Server → LDAP Server)	LDAP or LDAPS	TCP/ Port Number of LDAP Server	LDAP User Account
Operate UI (Management Console → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	LDAP User Account

Operate UI (including Mobile Access) with IIS

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (Management Console →IIS)	HTTP or HTTPS	TCP/ Port Number of IIS	Internal User Account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Redirect (IIS → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Internal User Account
Operate UI (Management Console → IIS)	HTTP or HTTPS	TCP/ Port Number of IIS	Internal User Account
Redirect (IIS → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Internal User Account

Get/Set Data

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Get/Set Data (Core Server → Database (SQL Server))	JDBC	TCP/ Port No of the Database.	SQL Server Authentication or Windows Authentication
Get/Set Data (Delegation Server → Internal database (Derby))	JDBC	TCP/1527 (default)	User Authentication by the internal account.

Synchronize Core Server

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Synchronize Data (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

If the Delegation Server loses the connection to the Core Server, the Delegation Server will reconnect to the Core Server at a different time.

Certificate Management Tool

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Import Device List (Certificate Management Tool → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	User Account
Import Certification (Certificate Management Tool → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Export Certification (Certificate Management Tool → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Get Status of Certification (Certificate Management Tool → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Delete Certification (Certificate Management Tool → Device)	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Generate and Install Certificate (Certificate Management Tool -> Device)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Generate and retrieve CSR from the device	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account
Enroll with SCEP to generate and download certificate on Certificate Authority server	HTTP or HTTPS	TCP/80 or TCP/443	N/A
Import Certificate to device	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Get Status of Certificate from device	HTTP/SOAP or HTTPS/SOAP	TCP/80 or TCP/443	Device Administrator account

Printer Driver Packager NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
@Remote Connector NX → Core Server	HTTP or HTTPS	TCP/ Port Number of the Core Server	User Account

SLNX Application Common

Login

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Makes Login request to DS Server. (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Retrieve latest user information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Authenticate against external server and get user attributes (Delegation Server → LDAP Server)	LDAP or LDAPS	TCP/ Port Number of LDAP Server	LDAP User Account

Accounting Transactions

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Send Accounting Transactions to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Populate Accounting Transactions to Core Database (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Scan

On Server workflow

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Project details retrieved from DS. (Delegation Server → SLNX Application)	HTTPS	TCP/51443	Retained in Streamline NX
Scan data sent to DS. (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Processed scan document sent to destination. (Delegation Server → Other System)	Depends on connection method	Depends on connection method	Depends on connection method

On Server workflow with load balance

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Project details retrieved from DS. (Delegation Server → SLNX Application)	HTTPS	TCP/51443	Retained in Streamline NX
Send the DS information that listed in load balance group. (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Request for load information to each DS. (Delegation Server → Delegation Server (Other))	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Scan data sent to DS. (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Processed scan document sent to destination. (Delegation Server → Other System)	Depends on connection method	Depends on connection method	Depends on connection method

On Device workflow

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Processed scan document sent to destination. (Delegation Server → Other System)	Depends on connection method	Depends on connection method	Depends on connection method

Print

Direct print

Operation (Sender → Destination)	Protocol	Port Number	Access Account
User prints job (payload) to Streamline NX queue on Print Server. (PC Client → Delegation Server)	SMB	-	Windows account
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Get Transaction ID, Temporary User Code from device (Delegation Server → Device)	HTTPS	TCP/51443	SDK account
Send Accounting Transactions to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Populate Accounting Transactions to Core Database (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Secure Print (Submission)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
User prints job (payload) to Streamline NX queue on Print Server. (PC Client → Delegation Server)	SMB	-	Windows account
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Register Print Location information in Core (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Secure Print (Job list)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Job list acquisition request to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX

Secure Print (Release)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Print request to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Send Accounting Transactions to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Populate Accounting Transactions to Core Database (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Print request to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX

Client Secure Print (Submission)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Register Print Location information in Core (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Client Secure Print (Job list)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Login (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Login (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Job list acquisition request to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Get Print Location information from Core (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Get list from PC Client (Delegation Server → PC Client)	HTTP or HTTPS	TCP/ Port Number of the PC Client	Retained in Streamline NX

Client Secure Print (Release)

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Print request to DS (SLNX Application → PC Client)	HTTP or HTTPS	TCP/ Port Number of the PC Client	Retained in Streamline NX
Retrieves user information (PC Client → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Retrieves user information (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX

Operation (Sender → Destination)	Protocol	Port Number	Access Account
Send Accounting Transactions to DS (SLNX Application → Delegation Server)	HTTP or HTTPS	TCP/ Port Number of the Delegation Server (default: 9090)	Retained in Streamline NX
Populate Accounting Transactions to Core Database (Delegation Server → Core Server)	HTTP or HTTPS	TCP/ Port Number of the Core Server	Retained in Streamline NX
Print completion notification to Client (SLNX Application → PC Client)	HTTP or HTTPS	TCP/ Port Number of the PC Client	Retained in Streamline NX

@Remote

Operation (Sender → Destination)	Protocol	Port Number	Access Account
@Remote Connector is connecting to Device by FTP (@Remote Connector → Device)	FTP	TCP/21	Device Administrator account
Device is sending required data (Device → @Remote Connector)	FTP	TCP/21	-
@Remote Connector is sending firmware information (@Remote Connector → Device)	FTP	TCP/ Specified by Device	Device Administrator account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
@Remote Connector is capturing MIB information of device (@Remote Connector → Device)	SNMP	UDP/161	SNMP V3 access account
@Remote Connector is sending notification to Communication Server via HTTPS (@Remote Connector → Communication Server)	HTTPS	TCP/443	@Remote access account
Device is sending notification such as Emergency Call (Device → @Remote Connector)	HTTPS	TCP/443 (This port is always open regardless of the activation status of @Remote Connector)	-
@Remote Connector is requesting firmware information (@Remote Connector → Communication Server)	HTTPS	TCP/443	@Remote access account
@Remote Connector is capturing device information (@Remote Connector → Device)	HTTPS	TCP/7443	@Remote access account
@Remote Connector tries to communicate with device at the first time (@Remote Connector → Device)	HTTPS	TCP/7444	@Remote access account

Operation (Sender → Destination)	Protocol	Port Number	Access Account
CE/Service Technician is operating @Remote Connector via laptop (CE's Laptop → @Remote Connector)	HTTP	TCP/ Port number of the @Remote Connector (default:8080)	Internal User Account

MEMO