

**RICOH**



# Device Manager NX

Operating Instructions

**Operation Guide**



# TABLE OF CONTENTS

---

How to Read This Manual.....	6
Symbols.....	6
Terminology.....	6
About Viewing This Manual.....	7
Important.....	8

## 1. What is Device Manager NX?

---

What You Can Do with Device Manager NX.....	9
Searching and Monitoring Devices on a Network.....	9
Managing Counter Information.....	10
Managing User Information.....	10
Managing Device Configuration Items.....	11
Managing SDK Applications and the SDK/J Platform.....	11
Using Energy Saver Mode.....	12
Starting Device Manager NX.....	13
Screen Configuration.....	14
Display Icons.....	15
Sorting/Classifying Lists.....	17

## 2. Monitoring the Devices

---

Configuring Access Accounts.....	19
Configuring a Web Service Account.....	19
Setting an SNMP Account.....	20
Setting an SDK Account.....	20
Overwriting an Access Account.....	20
Deleting an Access Account.....	21
Searching for Devices.....	22
Creating a Discovery Task.....	22
Adding a Device to Use.....	23
Deleting a Device.....	23
Hide View for a Device.....	24
Classifying Devices by Group Name.....	25
Creating a Manual Group.....	26
Creating a Filter Group.....	26
Deleting a Group.....	28

---

Importing/Exporting the Group Information.....	28
--	----

### **3. Checking the Device Statuses**

---

Retrieving the Device Status.....	31
Creating a Polling Task.....	31
Directly Performing Polling.....	32
Checking Device Properties.....	33
Displaying Device Properties.....	33
Main Properties.....	33
Status Details.....	35
Counters.....	39
Optional Properties.....	39
Access Account Settings.....	40
Checking Counters.....	41
Checking Counters on Each Device.....	41
Checking Per User Counters.....	42
Message Notification with Set Conditions.....	43
Setting Notification Conditions.....	43
Setting Devices as Monitoring Targets.....	44
Checking Notification Messages.....	45
Managing Device Logs.....	46
Configuring the Device Log Settings.....	46
Collecting Device Logs.....	47
Exporting the Device Log as a CSV File.....	48

### **4. Changing the Device Settings**

---

What is a Template?.....	49
Applying Same Settings to Multiple Devices.....	51
Creating a Template by Editing Device Settings (Basic Device Preferences).....	51
Creating a Template for Copying Device Settings (Advanced Device Preferences).....	52
Applying Energy Saver Mode to Multiple Devices at One Time.....	54
Managing the User Data.....	55
Creating a User Data Template.....	55
Registering a User or a Group to the Entry List.....	57
Resetting the User Counter Information.....	59

---

Managing SDK Applications and the SDK/J Platform.....	61
Template for Updating the SDK/J Platform.....	61
Creating a Template for SDK Application Settings.....	62
Registering Created Templates to Tasks.....	64
Configuration Task Type.....	64

## 5. Checking the System Operation Status

---

Managing Tasks.....	69
Managing a Task in the Schedule Standby Status.....	69
Checking Task Logs.....	70
Notifying/Confirming Overdue Tasks.....	72
Checking System Operation Logs.....	73
Checking the System Log.....	73
Checking the Notification Log.....	74
Error Code List.....	76
Server-related Errors.....	87

## 6. Maintenance

---

Activating Device Manager NX.....	91
Activating Online.....	91
Activating Offline.....	92
Deactivating the Product.....	94
Deactivating Device Manager NX Accounting in the Product.....	94
Performing a System Backup/Restore.....	96
Backing up the System.....	96
Restoring the System.....	97

## 7. Device Manager NX Setting Items

---

Configuration Item List.....	99
Device List.....	103
[Groups] Tab.....	103
[Filters] Tab.....	104
Device Access Settings.....	106
Discovery.....	106
Polling.....	110
Access Account Settings.....	111

---

Configuration.....	115
Device Preference.....	115
Software.....	118
Address Book.....	121
Power Mode.....	132
Tasks.....	134
Scheduled Tasks.....	134
Task Logs.....	134
System.....	135
System Settings.....	135
Authentication and Accounts.....	142
Notification Policy.....	143
Status Notification.....	143
Task Notification.....	145
Logs.....	147
System Log.....	147
Device Log Management.....	148
Device Log Collection.....	148
Device Log Management.....	151

## 8. Appendix

---

Setting a Password.....	153
Disabling SSLv3 and SSLv2Hello.....	154
The procedure to disable SSLv3 and SSLv2Hello Protocols.....	155
List of Device Preference Setting Items.....	157
General.....	157
Date and Time.....	158
Protocol.....	159
TCP/IP.....	159
SNMP.....	160
Administrator.....	161
Email.....	162
User Authentication.....	164
Paper Tray.....	167

---

Printer.....	167
LDAP Server.....	173
Kerberos Server Settings.....	174
Firmware Update Settings.....	174
User Lockout Policy.....	175
Interface Settings.....	175
Device Functions.....	175
Web Browser NX.....	176
Importing/Exporting the System Settings.....	177
Format of CSV Files.....	178
Format of a Device Information CSV File.....	178
Format of a Group Information CSV File.....	179
Format of an Address Book CSV File.....	180
Format of a Discovery Range CSV File.....	190
Format of a Device Preference CSV File.....	192
Format of a Device Log CSV File.....	216
Command Line Tools.....	228
Batch File for Registration as a Service.....	229
Batch File for Canceling Registration as a Service.....	229
Batch File for Starting the Service.....	229
Batch File for Stopping the Service.....	230
Troubleshooting.....	231
Trademarks.....	233

---

# How to Read This Manual

---

## Symbols

---

This manual uses the following symbols:

### **Important**

Indicates a situation that may result in property damage or malfunction if instructions are not followed. Be sure to read the instructions.

### **Note**

Indicates supplementary relevant information.

### [ ]

Indicates the names of keys that appear on the computer screen.

---

## Terminology

---

The terms used in this manual are described below.

### **Access Account**

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 access devices in Device Manager NX, configure the following access accounts:

- **SNMP Account**  
Use this account to search for a device or obtain information from a device.
- **Web Service Account**  
Use this account to modify the configuration of a device.
- **SDK Account**  
Use this account to manage the SDK/J platform or SDK applications on a device.

### **Administrator**

The person who manages device settings. There are various kinds of administrators depending on the device that is used. For example, a device administrator can configure device settings and a user administrator can manage user information. Both are referred to as "administrators" in this manual. Specify an administrator according to the device you are using or the device's configuration.



---

## **Device**

A printer or a multifunctional printer (MFP) on the network. The term "device" in this document refers to a printer or an MFP.

## **Discovery**

A function to search for devices on a network based on specified conditions. Also, it sends the device information to Device Manager NX.

## **Polling**

A function to retrieve information such as the remaining amount of consumables or the status of devices discovered by discovery.

## **RICOH Software Server**

A RICOH server that can be accessed via the Internet. You can download SDK applications and the SDK/J platform that are compatible with the device you use from the RICOH Software Server. You can install them on the device.

## **User**

A person who uses the device for printing, scanning, etc.

---

## **About Viewing This Manual**

---

If you want to view this manual on a computer, note the following:

- You can view the HTML documentation using a Web browser. We recommend the following browsers:
  - Internet Explorer 6 or later
  - Firefox 3.5 or later
  - Safari 4.0 or later
- If JavaScript is disabled or unavailable on your browser, you will not be able to search or use certain buttons in the HTML documentation.

---

# 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.

Some illustrations or explanations in this guide may differ from your product due to improvement or change in the product.

Contents of this document are subject to change without notice.

# 1. What is Device Manager NX?

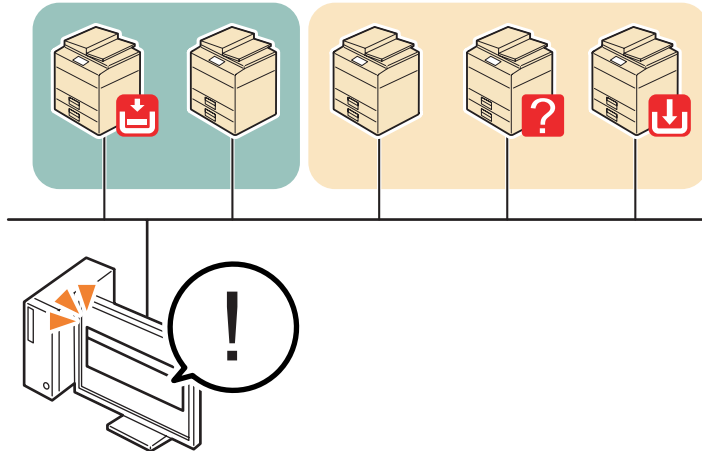
Device Manager NX is an application for integrated management of devices on the network. You can configure and monitor devices from a computer to simultaneously manage multiple devices as a group.

## What You Can Do with Device Manager NX

### Searching and Monitoring Devices on a Network

You can use Device Manager NX to search for devices within a specified IP address range and network and retrieve information such as errors and the remaining amount of consumables in the discovered device. The function used to search for devices is called Discovery and the function to retrieve the device information is called Polling. By combining these functions, Device Manager NX monitors the status of devices.

If the status of a device changes, such as due to a device error, a pop-up message will appear on the Device Manager NX display.



CQE003

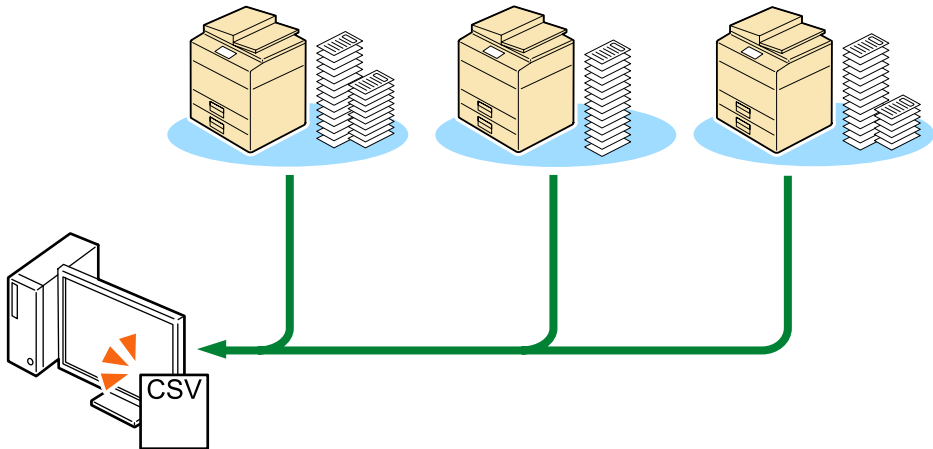
Any device discovered by the discovery function will be classified automatically by its IP address, hostname, or device manufacturer. Furthermore, it is also possible to manage devices by manually creating categories and groups such as "Installation floor" or "Applicable department".

#### ↓ Note

- For details about searching and monitoring devices and managing groups, see page 19 "Monitoring the Devices".
- For details about the notification settings, see page 43 "Message Notification with Set Conditions".

## Managing Counter Information

You can use Device Manager NX to retrieve any counter information from a device. The counter information includes the number of color/monochrome printed pages and transmitted fax pages. You can check the number of devices being used and the usage by the users registered to a device. This information can be exported as a CSV file.



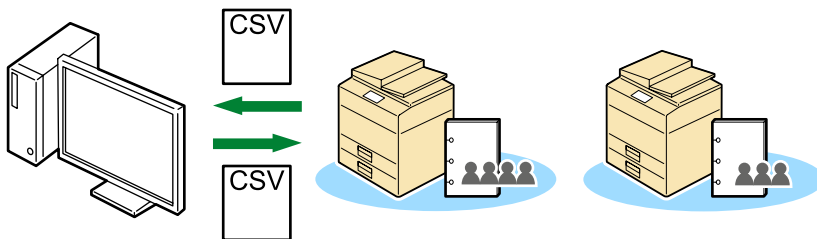
CQE004

### ↓ Note

- For details about the counters and how to check them, see page 41 "Checking Counters".

## Managing User Information

You can use Device Manager NX to manage the information about the users registered to a device. You can retrieve user information from a device, CSV or other types of files, add or delete users, limit available functions, set a usage limit, and apply these settings to the device. Also, you can directly edit settings configured using Device Manager NX after they are exported to CSV files, and you can back up settings after they are exported to encrypted files to ensure data security.



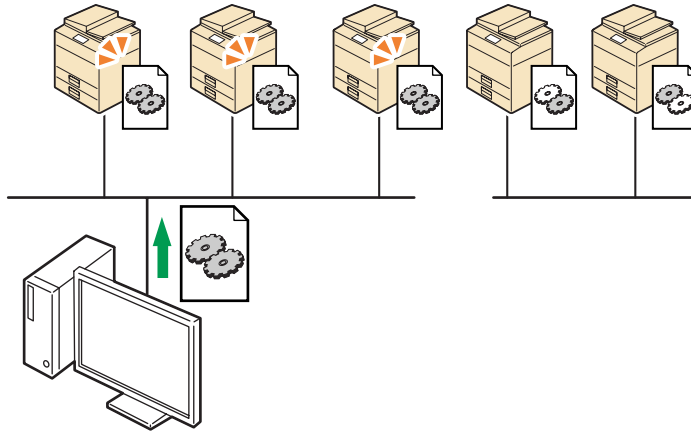
CQE005

### ↓ Note

- For details about managing user data, see page 55 "Managing the User Data".

## Managing Device Configuration Items

You can use Device Manager NX to change network, paper, and printer settings registered to a device. Settings of multiple devices can be changed simultaneously, so you do not have to make individual changes using the Web interface of the device. If a user is allowed to change the device settings, the status of devices can be maintained by performing this function periodically.



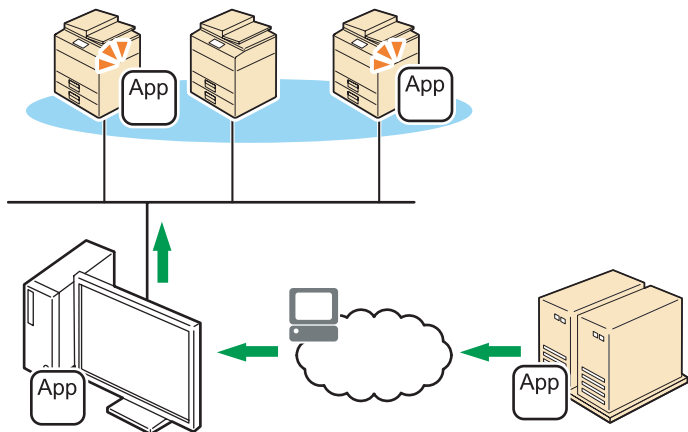
COE006

### ↓ Note

- For details about managing a device settings, see page 51 "Applying Same Settings to Multiple Devices".

## Managing SDK Applications and the SDK/J Platform

You can use Device Manager NX to update the SDK/J platform that is installed on a device. Also, you can install or uninstall SDK applications. Download the files for SDK applications and SDK/J platform from RICOH Software Server using the Internet, and update/install them on the target device.



CQE008

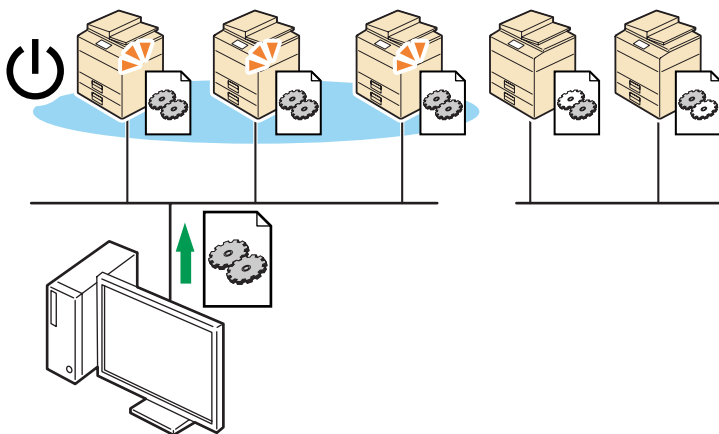
**Note**

- For details about managing SDK applications and the SDK/J platform, see page 61 "Managing SDK Applications and the SDK/J Platform".

## Using Energy Saver Mode

You can use Device Manager NX to change the power status of a device. By specifying a time period such as a device downtime, you can specify when the device enters or exits energy saver mode.

Energy consumption can be reduced by efficiently switching to the power saving mode.



CQE007

**Note**

- For details about the energy saver mode, see page 54 "Applying Energy Saver Mode to Multiple Devices at One Time".

# Starting Device Manager NX

Select Device Manager NX from the Start menu or by clicking the shortcut icon on the computer that Device Manager NX is installed on.

1. From the [Start] menu, select [All Programs], [Device Manager NX XXX], and then click [Start Device Manager NX XXX].

"XXX" varies depending on Device Manager NX to use.

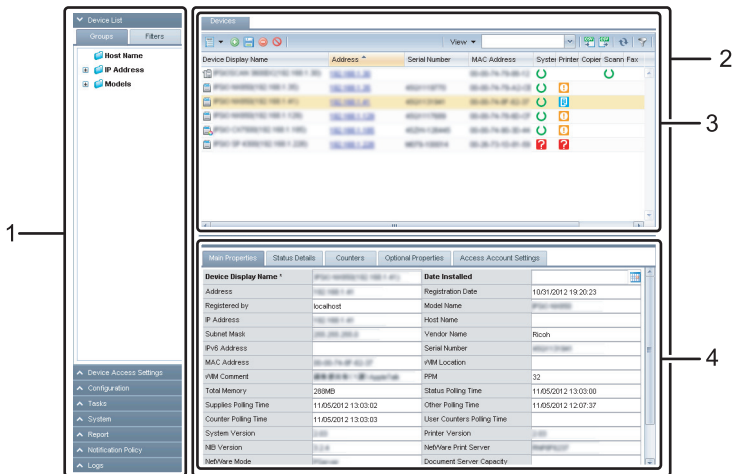
2. Enter the password if already set, and then click [Login].

## Note

- For the password setting method, see page 153 "Setting a Password".

# Screen Configuration

The standard screen configuration of Device Manager NX is explained below using the Device List section as examples.



CQE009

### 1. Section area

Items in each section are displayed in this area.

When a section is clicked, details of each item are displayed in a tree structure.

### 2. Tab area

The control screen that corresponds to the selected section tree item is displayed.

Use the tabs to switch between multiple control screens. To close multiple tabs at once, right-click on the tab and select [Close All but Current] or [Close All].

### 3. List area

A list of devices, tasks and other items are displayed above the tab area. Various icons are located on the tool bar in the list area and can be used for the following operations:

- Import and export information such as the list information
- Switch to an arbitrary view  
See page 15 "Display Icons".
- Sort and classify lists  
See page 17 "Sorting/Classifying Lists".
- Accumulate device counters  
See page 41 "Accumulating device counters in the list".
- You can access Web Image Monitor.

Click the IP address of the target device. The device management tool displayed may differ depending on the target device.



#### 4. Properties area












Detailed information about a device or task selected in the list area is displayed below the tab area and used for editing and configuring the information.












Click the name bar in the property area to open or close the selected area. Drag the name bar to change the size (height) of the area.

## Display Icons

All of the operation icons and device icons displayed by Device Manager NX are described below. There are some operation icons that are not displayed depending on the function.

### Operation icons




Icon	Description
	<p>The following menus used for the device list are displayed.</p> <ul style="list-style-type: none"> <li>•  Add Device: Add a device to the list. See page 23 "Adding a Device to Use".</li> <li>•  Delete: Delete a device from the list. See page 23 "Deleting a Device".</li> <li>•  Hide Device: Hide a device from the list. See page 24 "Hide View for a Device".</li> <li>•  User Counter: Show the user counter of the selected device.</li> <li>• Polling: Perform polling of the selected device and retrieve the device information. The retrieved information does not include user counters.</li> <li>•  Notification Options: Specify the selected device as a monitoring target. See page 43 "Message Notification with Set Conditions".</li> </ul>
	<p>Add or delete devices and tasks to/from the list. See page 23 "Adding a Device to Use", page 23 "Deleting a Device".</p>
	<p>Save the edited device information, configured task and templates.</p>
	<p>Hide a device from the list. See page 24 "Hide View for a Device".</p>
	<p>Copy a template, etc.</p>
	<p>Add or delete a target device or group.</p>






Icon	Description
	In the list of task logs, perform task suspension, stop, and restart. In the list of discovery, polling, or configuration task, click  to immediately perform the task.
	Save the list view and switch it to another. <ul style="list-style-type: none"> <li> Save: Save the view. The following statuses are maintained. Up to five views can be listed. <ul style="list-style-type: none"> <li>Row display items</li> <li>Sorting status of each row</li> </ul> </li> <li> Save as: Save a view as new.</li> <li> Delete: Delete a view in the list.</li> </ul> Selecting a view in the list box allows you to switch to the view.
	Export or import the list information in a CSV file.
	Update the list information.
	Filter the list information. Click to display an input/selection area over the item name in the list. Enter or select a search key and click  located to the right of the input area or press the Enter key. The relevant entry is displayed.
	Displays help for the setting items in the display area.

### Note

- Up to eight views can be saved.
- Specifying a blank column on the view list box allows you to switch to the default view. Basic device information and status and group information are displayed in a view by default. You cannot overwrite the default view.
- For details of the CSV file to be exported, see page 177 "Importing/Exporting the System Settings".
- For the format of CSV files, see page 178 "Format of CSV Files".

### Device icons

Icon	Description
	RICOH digital full color multifunctional machine *
	RICOH digital monochrome multifunctional machine *
	RICOH color laser printer *

Icon	Description
	RICOH monochrome laser printer *
	RICOH hybrid multifunctional machine
	RICOH gel jet printer
	RICOH OEM color/monochrome multifunctional machine or printer
	Non-RICOH brand color/monochrome multifunctional machine or printer

\* Device icons to be displayed differ depending on the machine being used.

## Sorting/Classifying Lists

This section describes how to sort and classify lists for ease of view.

Place the cursor on the item name of a row and right-click. The following menu items for sorting and classification are displayed. Some menu items are not displayed depending on the function.






Menu item	Description
Sort Ascending	Sort the target row in the ascending order.
Sort Descending	Sort the target row in the descending order.
Configure Sort	Click this to display a sort dialog. For details, see page 18 "Setting Configure Sort".
Clear Sort	Clear the sorting status.
Auto Fit All Columns	Display all columns with widths automatically adjusted.
Auto Fit	Adjust the target column width.
Columns	Set the items to be displayed in or to be hidden from the list. In the item name list on the submenu, select check boxes for the items to be displayed and clear the check boxes for the items to be hidden.
Freeze Name "Item name"	The rows on the left including the target rows are fixed so that they are not hidden even when horizontal scrolling is performed. The item name is displayed as "Item name".
Unfreeze Name "Item name"	Unfreeze the target rows. The item name is displayed as "Item name".

Menu item	Description
Add Calculation Field	Add, edit, and/or delete the fields (rows) with accumulated device counters.
Edit Calculation Field	
Delete Calculation Field	
Right Align	The target row information is right-justified.
Left Align	The target row information is left-justified.

## Setting Configure Sort

1. In the list area, right-click an item name and select [Configure Sort].

The configure sort dialog is displayed.

2. Click  (Add).
3. Specify a sort target item from the drop-down list of the [Columns] row.
4. Select [Ascending] or [Descending] from the drop-down list of the [Sort Order] row.
5. To add another sorting condition, repeat Steps 2 to 4.
  - Click  (Copy) to copy the selected sorting condition.
  - Click  (Delete) to delete the selected sorting condition.
  - To change the sorting conditions, double-click the setting value.
6. When more than one sorting condition is set, click [] or [] to prioritize the sorting conditions.
7. Click [Apply] when the settings are configured.

## 2. Monitoring the Devices

This chapter explains how to search devices using the discovery function. It also explains the Device Grouping function.

This chapter explains about searching and grouping devices.

## Configuring Access Accounts

2

Specify user account information so that a user can access a device. Multiple accounts can be configured in Device Manager NX. If an account is created and its information is specified, the account can be used with the discovery function and associated with groups and devices.

Multiple accounts can be created for the Web service account, SNMP account, and SDK account. Each user can prioritize account access to devices. An account that is successfully accessed is registered to the device profile, and the registered device access account is used for future access to these devices.


By default, one access account is provided for the Web service account, SNMP account, and SDK account. These default access accounts can be edited but cannot be deleted.

### Configuring a Web Service Account

"Web service" in Device Manager NX is a service associated with RICOH MFPs, printers and Device Manager NX.

To access a device that requires user authentication or change the device's settings, configure a Web service account with a login user name and login password.

#### Important

- The Web service works in an HTTP/HTTPS environment.
  - The system's default values are applied to timeout and retry values that are specified in an HTTP/HTTPS environment.
  - The authentication information of the Web service account to be used for discovery must have all administrative privileges (Device Administrator, User Administrator, File Administrator, and Network Administrator) on the subject device.
1. In the section area, click [Device Access Settings].
  2. In the [Access Account Settings] category on the section tree, click [Web Service Account Setting].
  3. Click  (Add) in the list area.
  4. In the properties area, set [Profile Name], [Profile Description], [User Name], and [Password] for the account.



For details about values that can be specified, see page 111 "Access Account Settings".

5. Click  (Save) when the setting is configured.

---

## Setting an SNMP Account

---

1. In the section area, click [Device Access Settings].
2. In the [Access Account Settings] category on the section tree, click [SNMP Account Setting].
3. Click  (Add) in the list area.
4. In the properties area, set [Profile Name], [Profile Description], [Retry], and [Timeout (millisecs.)] for the account.
5. Select protocol [SNMP v1/v2] or [SNMP v3].
6. Specify values appropriate for the selected protocol.  
For details about values that can be specified, see page 111 "Access Account Settings".
7. Click  (Save) when the setting is configured.



---

## Setting an SDK Account

---

An SDK account is required to perform operations such as updating the SDK/J platform, and installing or uninstalling SDK applications.

 **Important**

- An SDK account does not need to be configured for normal operation.
1. In the section area, click [Device Access Settings].
  2. In the [Access Account Settings] category on the section tree, click [SDK Account Setting].
  3. Click  (Add) in the list area.
  4. In the properties area, set [Profile Name] and [Profile Description] of the account.  
For details about values that can be configured, see page 111 "Access Account Settings".
  5. Click  (Save) when the setting is configured.


---

## Overwriting an Access Account

---

How to change and overwrite an access account of a detected device is explained below.


1. Select the target device in the device list.
2. In the [Device Properties] area, click the [Access Account Settings] tab.

3. Click the target account tab, and then select the profile name of the account that you want to change in the [Profile Name] list.
4. Click  (Save) when the setting is complete.

---

## Deleting an Access Account

---

1. In the section area, click [Device Access Settings].
2. In the [Access Account Settings] category on the section tree, click the target account.
3. Select the profile name of the account that you want to delete from the list area.
4. Click  (Delete).
5. Click [Yes] when a confirmation message appears.

### Note

- The account may not be deleted depending on its state. For details, see page 231 "Troubleshooting".

# Searching for Devices

You can use Device Manager NX to search for devices on a network by using the discovery function and to detect monitoring and control target devices.

Before using the discovery function, set search conditions such as the IP address range, model name, and status, and then create a discovery task. Specifying a target search range based on the discovery task may result in improved discovery operations. Also, network traffic load can be reduced. To use discovery, identify appropriate methods and hours for your business operations.

The following two methods are available when using discovery on a network:

## Network Search

A specified IP address range is used for network search. Each of the IP addresses within the IP address range will be accessed using SNMP.


## Broadcast

SNMP broadcast is performed for all devices on a local or specified network so as to detect devices that are connected to the network.



### ★ Important

- The discovery function can detect devices that are compatible with Printer MIB v2 (RFC 3805), Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790).


## Creating a Discovery Task


1. In the section area, click [Device Access Settings].
2. In the [Discovery] category on the section tree, click [Network Search] or [Broadcast].
3. Click  (Add) in the list area.
4. On the [General] tab, enter a task name and description.
5. On the [Access Account Settings] tab, add to [Assigned Account] an account that you want to use for access to a device.

Up to ten accounts can be registered for Web service account, SNMP account, and SDK account.

6. On the [Discovery Range (Network Search)] or [Discovery Range (Broadcast)] tab, set a discovery search range by entering an address, subnet mask, etc.
  - If a search range is specified manually:
    1. Click  (Add).
    2. Set a search range.
    3. Click  (Save).
  - If a CSV file that specifies a search range is imported:



1. Click  (Import CSV File).
2. Click [Browse...].
3. Specify a CSV file to be imported, click [Open].
4. Click [Upload].
5. Click [OK].



The items that can be specified vary depending on whether [Network Search] or [Broadcast] is specified. Click  (Exports data to CSV files.) to export the set search range as a CSV file.

**7. On the [Schedule] tab, specify when to perform discovery.**

**8. Click  (Save) when the setting is configured.**


A discovery task is registered to the list. To immediately perform discovery, click  (Immediately).

**Note**

- Select the discovery task that is already registered to the list area and edit the settings in the property area. To save edited settings, click  (Save).
- To delete a discovery task, select the discovery task to be deleted, and click  (Delete).
- New devices may be added to the network. To find additional devices on the network after the initial network configuration, perform discovery again.
- For details on the configuration items of each tab, see page 106 "Discovery".
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.


## Adding a Device to Use

Manually add any device you want to use.

1. In the section area, click [Device List].
2. Click any category or a group.
3. Click  (Add Device) in the list area or right-click the device list, and select [Add Device].  
The Add Device dialog is displayed.
4. Enter the IP address or host name of the device.
5. Select the access account that you want to use for access to the device.
6. Click [OK].

## Deleting a Device

1. In the section area, click [Device List].

2. Click an arbitrary category or a group.
3. Select the device that you want to delete from the device list, and then click  (Delete), or right-click and select [Delete].


To select multiple devices, click a device while pressing the SHIFT key or CTRL key.

## 2

---


### Hide View for a Device

---

1. In the section area, click [Device List].
2. Click any category or a group.
3. Select the device that you want to delete from the device list, and then click  (Hide Device), or right-click and select [Hide Device].

### Display hidden devices

---

1. In the section area, click [Device List].
2. Right-click an arbitrary category or a group, and select [Display Hidden Devices].  
A list of hidden devices is displayed.
3. Select the device to be shown.
4. Click  (Show Device).

# Classifying Devices by Group Name

Monitoring and management of devices can be facilitated if devices are grouped by category such as installation site and user.

Three group types are available: automatic, manual, and filter.

## Automatic groups

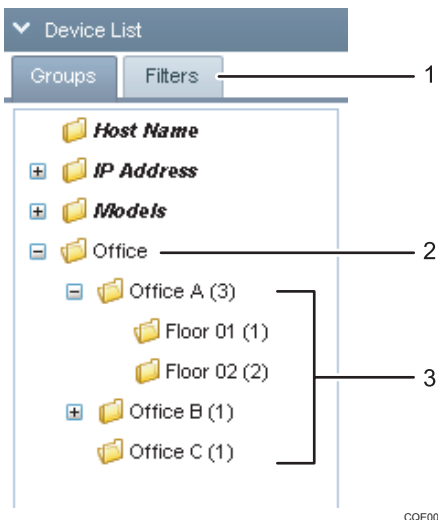
Device Manager NX classifies devices automatically. Groups [IP Address], [Host Name], and [Models] are provided.

## Manual groups

Any groups can be created. Any devices can be added to each of the groups you want to create.

## Filter groups

Groups of devices that meet specified search conditions can be created.



1. Auto and manual groups are displayed on the [Groups] tab. Filter groups are displayed on the [Filters] tab.

2. This is a category group that is created in the highest layer by [Add Category].

3. This is a group that is created in the lower layer of a category group by [Add Group].

The section tree structure is displayed with low-layer groups expanded/collapsed when the "+" / "-" icon next to the group (folder) icon is clicked.

### Note

- Up to 200 groups each can be created as manual groups and filter groups.
- Up to seven ranks can be created for manual groups.

---

## Creating a Manual Group

---

1. In the section area, click [Device List].
2. Click the [Groups] tab.
3. Right-click the section tree, and then select [Add Category].
4. Enter the name of the category, and then click [OK].

The maximum number of characters for a category name is 128.

The following characters cannot be used: "#\*./;<=>?[\|]

5. Right-click the created category, and then select [Add Group].
6. Enter the name of the group.

The maximum number of characters for a group name is 128.

The following characters cannot be used: "#\*./;<=>?[\|]

7. Add a device to the created group.

To narrow down the list of devices, specify the device search conditions, and then click [Select Device(s)]. The devices that are displayed in the list are added to the group.

For details about search conditions, see Step 5 in page 26 "Creating a Filter Group".

8. Click [OK].
9. In order add a device to a group individually, drag the device from the device list and drop it in the group to which the device is to be added.

To select multiple devices, click a device while pressing the SHIFT key or CTRL key.

### Note

- The specified search condition is valid while creating groups only. A device that is detected after a group has been created will not be automatically added to the group.

---

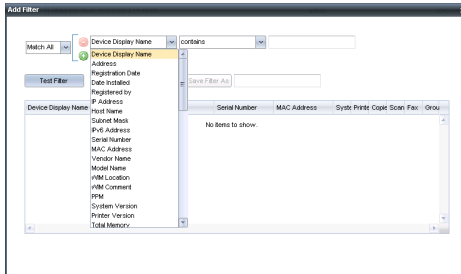
## Creating a Filter Group

---

This section explains how to specify device search conditions for a filters group.

1. In the section area, click [Device List].
2. Click the [Filters] tab.
3. Right-click the section area, and then select [Add Filter].
4. Specify a search target item.

Select a device properties item in the list.



**5. Specify a comparative operator to be applied to the specified item of the search target item.**

- If the search target item is a string:
  - contains: Includes the value as a partial string.
  - does not contain: The value is not included as a partial string.
  - equals: Includes the search value as a complete string.
  - starts with: The value matches the first part of the string.
  - ends with: The value matches the final part of the string.

Comparative operators are not case sensitive.
- If the search target item is a numerical value, date, or status:
  - equals: Matches the value.
  - not equal to: Does not match the value.
  - less than: Less than the value, and the display priority is low.
  - greater than: Greater than the value, and the display priority is high.
  - less than or equal to: Matches or is less than the value, and the display priority is low.
  - greater than or equal to: Matches or is greater than the value, and the display priority is high.

If the search target item is a status, only "equals" or "not equal" can be specified.

**6. Specify search values for search conditions.**

**7. To add a search condition, click  (Add).**

Set search conditions by repeating Steps 4 to 6.

**8. Specify a combination of search conditions from [Match All], [Match Any], and [Match None].**

[Match All]: All conditions are satisfied.

[Match Any]: Any condition is satisfied.

[Match None]: No condition is satisfied.

**9. Click [Test Filter] to check that a normal operation is performed.**

**10. Enter the name of the filter group, and then click [Save Filter As].**

**Note**

- To change the search conditions for the created filter group, right-click the filter group to be changed, and select [Edit Filter].

---

## Deleting a Group

---

2

1. In the section area, click [Device List].
2. On the section tree, right-click the group you want to delete, and then select [Delete].

**Note**

- Auto groups cannot be deleted.
- Devices that are registered in the deleted group will move to the unmanaged group.
- When a group to be deleted includes sub groups, these sub groups are also deleted.

---

## Importing/Exporting the Group Information

---

Group information can be imported or exported using a CSV file. Importing or exporting of automatic groups is not permitted.

**Important**

- Export and import of auto and filter groups are not permitted.

---

### Exporting group information

---

A group structure, group name, and internal ID can be exported.

1. In the section area, click [Device List].
2. Click the [Groups] tab.
3. Right-click the category group, and then click [Export].
4. Select the check boxes for the export target categories and groups. To export all groups, select the [Export All Groups] check box.
5. Click [OK].

---

### Importing group information

---

If there is a group that is identical to the group you want to import, the group information of the existing group is overwritten by that of the group to be imported. The internal ID is used to check whether groups are identical.

1. In the section area, click [Device List].

2. Click the [Groups] tab.
3. Right-click the category group, and then select [Import].
4. Click [Browse...].
5. Specify the CSV file that you want to import, and then click [Open].
6. Click [Upload].
7. Select the check boxes for the import target categories and groups. To import all groups, select the [Import All Groups] check box.
8. Click [OK].

 **Note**

- For details about the format of a CSV file, see page 178 "Format of CSV Files".





# 3. Checking the Device Statuses

This chapter explains how to monitor devices using the polling function.

## Retrieving the Device Status

The function of Device Manager NX to retrieve information about devices is called polling. Monitoring of a device by periodically performing polling enables users to check the device's current status, such as the remaining amount of toner and paper and errors.

The following types of polling are available:

### Status Polling

- Retrieved information: Status and system information about printer, copier, scanner and fax functions.
- Default execution schedule: Performed once every hour for all target devices.

### Supplies Polling

- Retrieved information: Statuses of toner, input trays, output trays, etc.
- Default execution schedule: Performed once every three hours for all target devices.

### Counter Polling

- Retrieved information: Counter information such as the number of pages printed or pages copied by the device.
- Default execution schedule: Performed once every six hours for all target devices.

### User Counter Polling

- Retrieved information: Counter information about every user registered in the device and counter information about unspecified users (unregistered users).
- Default execution schedule: Disable

### Other Polling

- Retrieved information: Device firmware, installed SDK application types, etc.
- Default execution schedule: Performed once every week for all target devices.

#### ↓ Note





- A pop-up notification will be displayed if a device error is detected or any supply is exhausted. For details about the notification settings, see page 43 "Message Notification with Set Conditions".

---

## Creating a Polling Task



---

Create a polling task and periodically monitor device statuses.

1. In the section area, click [Device Access Settings].
2. On the section tree, click [Polling].
3. Click  (Add) in the list area.
4. On the [General] tab, enter a task name and a description.
5. On the [Target Devices/Groups] tab, set the polling target devices/groups.
  1. Click  (Add Group) or  (Add Device).
  2. Select a target device/group.
  3. Click [OK].
6. Click the tab of the polling that you want to perform, and then set the schedule.
7. Click  (Save) when the setting is complete.

A polling task is registered to the list. To immediately execute polling, click  (Immediately).

#### Note

- Select the polling task that is already registered to the list area and edit the settings in the property area. To save the setting that has been edited, click  (Save).
- To delete a polling task, select the polling task to be deleted, and click  (Delete).
- A device in power mode recovers from the energy saving state when Other Polling of the device has been performed.
- When processing the polling task continues even after the specified prohibited time period has begun, the process will continue until the polling task is completed.
- For configuration items of each tab, see page 110 "Polling".
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.

## Directly Performing Polling

1. Select a target device in the device list.
 

To select multiple devices, click a device while pressing the SHIFT key or CTRL key.
2. Right-click the selected device, and then select [Polling].
3. Specify the types of polling to perform, and click [OK].

Polling results will be applied to the device.

#### Note

- A device in power mode recovers from the energy saving state when Other Polling of the device has been directly performed.

# Checking Device Properties

Device properties that are retrieved by Device Manager NX are explained below.

When a device is selected in the device list, the information about the device retrieved by discovery or polling is displayed in the properties area.

## ★ Important

- Some items are not displayed depending on the device.

3

## Displaying Device Properties

1. In the [Device List] section, click a target group to display the corresponding device list.
2. Select a target device in the list area.
3. The information about the selected device is displayed in the properties area.

Check the device information and statuses by switching the following tabs:

- Main Properties
- Status Details
- Counters
- Optional Properties
- Access Account Settings

## Main Properties

The device information retrieved by discovery or polling can be checked.

- Device Display Name

The name of the device is displayed. You can change the display name to the one you want. The device name that you have changed is used even after the device is detected again by discovery.

- Date Installed

The installation date of a device is displayed. Users can specify this value.

- Address

The address for Device Manager NX to access the device is displayed.

- Registration Date

The registration date is displayed. This date/time indicates when discovery or a device is manually added.

- Registered by

This is displayed as "localhost".

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

The installation site set in the device is displayed.

- WIM Comment

The comment set in the device is displayed.

- PPM
- Total Memory
- Status Polling Time
- Supplies Polling Time
- Other Polling Time
- Counter Polling Time
- User Counters Polling Time
- Last Communication Time
- System Version
- Printer Version
- NIB Version
- NetWare Print Server
- NetWare Mode
- Document Server Capacity
- Document Server Free Space
- DOSS Last Auto Delete Date
- DOSS Auto Delete
- DOSS Auto Deletion Method
- DOSS Number of Auto Deletions
- HDD Encryption

- Operation Panel
- Interface Settings
- Wi-Fi

#### ↓ Note

- On a RICOH MFP or printer, the settings configured in Web Image Monitor are displayed as "WIM Location" and "WIM Comment" information.

## Status Details













3

You can check the device status by switching the [Printer Status], [Paper Tray], [Toner/Ink], and [Output Tray] tabs.

### Printer Status

- System



You can check the system status.













- : No response
- : Service call
- : Replace/supply
- : Toner/ink exhausted
- : Paper jam
- : No paper
- : Paper jam in ADF
- : Performing maintenance
- : Fax transmission error
- : Open cover
- : Miscellaneous error
- : Access violation has been detected
- : Ready

- Printer

You can check the statuses of the printer functions. To display detailed information, place the mouse cursor on the status icon. If there are multiple statuses, the status of the higher priority is displayed.

Descriptions of the icons indicated below are displayed in the order of highest priority.















- : No response
- : Toner/ink exhausted

- : Paper jam
- : No paper
- : Open cover
- : Miscellaneous error
- : Offline
- : Warming up
- : Busy
- : Toner/ink cartridge almost empty
- : Paper almost empty
- : Caution
- : Energy saver mode
- : Ready

- Copier

You can check the statuses of the copier functions. To display detailed information, place the mouse cursor on the status icon. If there are multiple statuses, the status of the higher priority is displayed.

















Descriptions of the icons indicated below are displayed in the order of highest priority.

- : No response
- : Service call
- : Toner/ink exhausted
- : Paper jam
- : Paper jam in ADF
- : No paper
- : Open cover
- : Miscellaneous error
- : Warming up
- : Busy
- : Toner/ink cartridge almost empty
- : Caution
- : Energy saver mode
- : Ready

- Fax

You can check the statuses of the fax functions. To display detailed information, place the mouse cursor on the status icon. If there are multiple statuses, the status of the higher priority is displayed.










Descriptions of the icons indicated below are displayed in the order of highest priority.

- : No response
- : Service call
- : Performing maintenance
- : Fax transmission error
- : Paper jam in ADF
- : Open cover
- : Miscellaneous error
- : Busy
- : Toner/ink exhausted
- : Paper jam
- : No paper
- : Warming up
- : Toner/ink cartridge almost empty
- : Caution
- : Energy saver mode
- : Ready

- Scanner

You can check the statuses of the scanner functions. To display detailed information, place the mouse cursor on the status icon. If there are multiple statuses, the status of the higher priority is displayed.

Descriptions of the icons indicated below are displayed in the order of highest priority.

- : No response
- : Service call
- : Paper jam in ADF
- : Open cover
- : Miscellaneous error
- : Busy
- : Caution
- : Energy saver mode
- : Ready

### Paper Tray


You can check the paper tray type. Also, you can check the orientation, size, type and remaining quantity of paper loaded in each paper tray.

: Indicates two orientations of the loaded paper


On devices using rolled paper, the icon on the right-hand side that indicates the remaining paper amount is displayed.

: No paper

: 0-20%

: 20-40%

: 40-60%

: 60-80%

: 80-100%

### Toner/Ink

You can check the colors of toner/ink and the remaining quantity of each toner/ink. "Unknown" may be displayed for some devices or monochrome MFPs if the remaining quantity of toner or ink cannot be detected.

The level of remaining toner or ink is indicated as shown below. The color of the indicator is the same as that of the applicable toner. Black is used as an example below:

: Toner/ink is empty

: Toner/ink cartridge is almost empty

: 0-20%

: 20-40%

: 40-60%


: 60-80%

: 80-100%

### Output Tray

You can check the output tray type and the status of each tray.

The output tray status is indicated by the icons as shown below:

: Output tray is full

: Paper is located in output tray

: Miscellaneous error

(Nothing appears): Normal status



---

## Counters

---

You can check counter information such as the number of pages printed in color/monochrome or transmitted pages.

- Device Counter Total  
A total of the counters for the copier, printer, and fax functions
- Copier: B&W, Full Color, Single Color, and Two-color  
Counter for the copier function
- Printer: B&W, Full Color, Single Color, and Two-color  
Counter for the printer function
- Economy Color Counter
- Fax Prints: B&W, Single Color  
Counter for the fax function
- A3/DLT
- A2
- Duplex Print
- Send/TX Total: Color, B&W  
A total of the counters for the scanner transmission and fax transmission functions
- Fax Transmission
- Scanner Send: Color, B&W  
The counter for the scanner transmission function

---

## Optional Properties

---

You can check the individual information of optional properties by switching the [Custom Properties], [Installed Application], [SDK Information], and [Functions] tabs.

### Custom Properties

Users can configure custom properties. For details about configuring custom properties, see page 40 "Setting custom properties".

### Installed Application

You can check Extended Features Name, Version, Product ID, Activated, License Type, and Expiration Date.

### SDK Information

You can check Version, Heap Size, Stack Size, and Smart SDK version (models with Smart Operation Panel only)

## Functions

You can check the functions and printer language provided for the device.

- Functions

You can check the functions provided for the device, such as manual paper feed, duplex printing, and card printing functions.

- Printer Language


You can check the printer language provided for the device.

## 3

## Setting custom properties

---

Custom properties are used for adding unique information to devices. Information such as administration number and asset number can be set for each device.

1. In the section area, click [System].
2. In the [System Settings] category on the section tree, click [Custom Properties].
3. Enter the item name to be used for custom properties.  
Up to 255 characters can be entered for the item name.
4. Click [Save].
5. Select a device from the device list.
6. In the properties area, click the [Optional Properties] tab, and then click [Custom Properties] tab.
7. Double-click the [Value] row, and enter the unique information.
8. Click  (Save) when the setting is configured.

---

## Access Account Settings

---

You can check access account profiles used for access to devices. Also, you can change an access account profile for each device.

For the functional outlines or operations of access accounts, see page 19 "Configuring Access Accounts".

For items of access accounts, see page 111 "Access Account Settings".

# Checking Counters

Device Manager NX can retrieve and check the counter information of a device.

Device Manager NX classifies the counter information of a device as follows:

## Device counter

Counter information of a device that can be retrieved by Counter Polling.

## User counter

Counter per user information of a device that can be retrieved by User Counter Polling. You can check how frequently a user accesses the device.


3

## Checking Counters on Each Device

Check the counter information retrieved by Counter Polling.

1. Click a target group in the [Device List] section to display the device list.
2. Select a device to check the counter information.
3. Click the [Counters] tab in the properties area.

### Note

- For details about polling, see page 31 "Retrieving the Device Status".
- For details about device properties, see page 39 "Counters".
- To export the device counter information as a CSV file, select [Counters] in the [View] list, and then click  (Exports data to CSV files.).

## Accumulating device counters in the list

You can accumulate device counters and add rows of calculation fields.

1. Click a target group in the [Device List] section to display the device list.
2. Right-click the item name of a row, and then select [Add Calculation Field].
3. Enter the item name of the calculation field in the [Title] box.

Up to 125 characters can be entered for an item name.

4. Enter a calculation formula in the [Calculation Field] box.

The calculation formula permits use of operators (+, -, \*, /), numerical values, and source field keys.

Example: To calculate the total of counters indicated below, enter "A+B" as the calculation formula.

Key	Source Field
A	Copier: B&W
B	Printer: B&W

**5. Click [Save] when the setting is configured.**

A calculation field is added to the list.

**Note**

- The only source fields that can be used in a calculation formula are those related to counters. For the counters that can be retrieved from devices, see page 39 "Counters".
- To edit or delete the added calculation field, right-click the item name of the calculation field, and then select [Edit Calculation Field] or [Delete Calculation Field].

---

## Checking Per User Counters

---

Check the user counter information retrieved by User Counter Polling.

User counters may contain a large volume of information. To retrieve user counter information, make sure that the hard disk has sufficient free space.

- 1. Click a target group in the [Device List] section to display the device list.**
- 2. Right-click the device to check counter information, and then select [User Counter].**

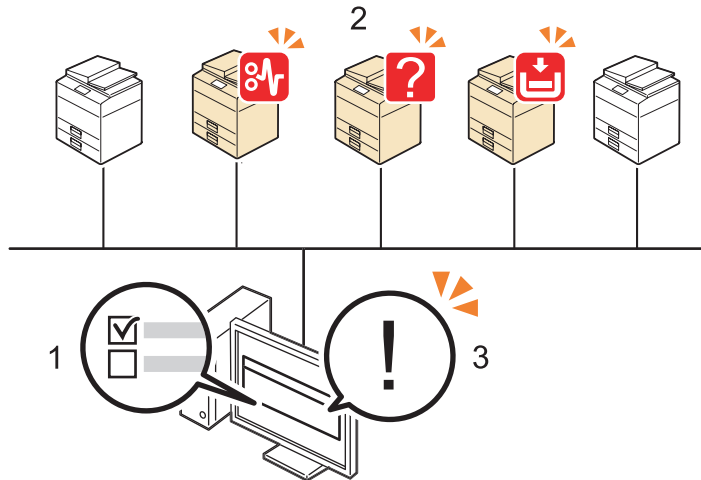
The user counter information tab opens. Click  (Exports data to CSV files.) if you want to export the user counter information as a CSV file.

**Note**

- You can export data as a CSV file in standard format that records data according to the column information that is currently displayed or in the format that is compatible with the old software (SmartDeviceMonitor for Admin).

# Message Notification with Set Conditions

When a toner cartridge in a device becomes nearly empty or when an error occurs, a pop-up message indicating the device status can be displayed on Device Manager NX.



QQE011

## 1. Notification occurrence criterion and notification conditions

Notification occurrence criterion means the following:

- A specific device status was detected by polling.

Notification condition is defined by the combination of the duration that a criterion is sustained, and the count of a criterion that occurs within the specified time interval.

Example: A notification is issued if the out-of-paper state continues for five minutes.

For details about setting the occurrence criterion and notification conditions, see page 43 "Setting Notification Conditions".

## 2. Monitoring target devices

The devices with which notification conditions are associated are monitoring target devices.

For details about setting monitoring target devices, see page 44 "Setting Devices as Monitoring Targets".


## 3. Confirmation of notification message

For details about the contents of the notification messages, see page 45 "Checking Notification Messages".

## Setting Notification Conditions


### ★ Important

- You can register up to 500 notification conditions.
- The notification messages will be displayed on the timer in Device Manager NX, and a delay of up to 5 minutes may occur.

1. In the section area, click [Notification Policy].
2. In the [Status Notification] category on the section tree, click [Notification Policy].
3. Click  (Add) in the list area.
4. Enter a definition name, and then click [Save].
5. Click the definition name that was registered in the list area.
6. Specify the notification occurrence criterion using the [Triggers] tab.

Select the check box for a device status to be used as the notification occurrence criterion. (More than one status may be selected.)

7. On the [Conditions] tab, set the notification conditions.
  - Notify only if criteria is repeated within specified time interval
  - Notify only if criteria is sustained for (time interval)
  - Specify a time interval that is longer than the status polling schedule.
  - For details about configuring a schedule for the status polling tasks, see page 110 "Polling".
8. On the [Monitored Devices] tab, check the devices and groups to be monitored.

To delete a device or group from the monitoring target, select a device or group and click  (Delete).

For details about setting monitoring target devices, see page 44 "Setting Devices as Monitoring Targets".

9. Click  (Save) when the setting is configured.

---




## Setting Devices as Monitoring Targets

---

Specify devices and groups to be associated with notification conditions.

More than one notification condition can be associated to a device.

1. Display the device list.
2. Right-click the device to be set as a monitoring target, and then select [Notification Options].

To associate notification conditions in group units, right-click a group, and then select [Notification Options].
3. Click  (Add) in the list area.
4. Select a notification condition to be associated in the [Notification Policy Name] list.
5. Click  (Save).
6. To associate another notification condition, click  (Add) and repeat Steps 4 and 5.

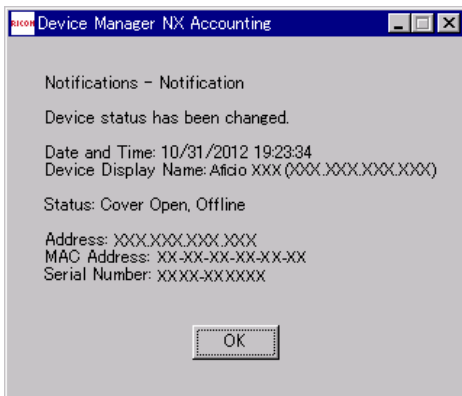
---

## Checking Notification Messages

---

Notification messages appear in pop-up windows.

Those messages indicate information such as the change in the status, the date and time it has been detected, the device name, IP address, and MAC address.



# Managing Device Logs

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

Using Device Manager NX, you can retrieve logs from registered devices and export them as CSV files.

There are three types of logs:

- Device Job Log

A log that records information such as copying, printing, sending faxes, and scanning of user documents.

- Device Access Log





A log that records authentication and user information such as the login or logout history and managing address books.

- Device Eco-friendly Log

A log that records the history of power status changes and usage of paper on a device.

Device Manager NX can retrieve Device Job Log.

### Note




- Use Device Manager NX Accounting to manage device logs. Device Manager NX Lite cannot be used for this purpose.
- Device logs can be recorded on devices represented by one of the following icons:     

- When a registered device is deleted, the device log will also be deleted.

---

## Configuring the Device Log Settings

---

You can configure the task to specify whether or not to store the device log internally in each device, and apply the setting to the device.

1. In the section area, click [Device Log Management].
2. Click [Device Log Settings] on the section tree.
3. In the list area, click  (Add).
4. On the [General] tab, enter the name and description of the device.
5. Select the task type from [Check], [Apply], and [Check & Apply].
6. On the [Device Log Settings] tab, configure the settings related to the device log.
7. On the [Target Devices/Groups] tab, specify the devices or groups that will be the target of the task.
  1. Click  (Add Group) or  (Add Device).



2. Select a target device or group, and click [OK].

**8. On the [Schedule] tab, specify the schedule to execute the task.**

**9. Click  (Save) when the setting is complete.**

#### Note

- For details about the settings on each tab, see page 148 "Device Log Management".
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.

## Collecting Device Logs

3

**1. In the section area, click [Log Management].**

**2. Click [Device Log Collection] on the section tree.**

**3. In the list area, click  (Add).**

**4. On the [General] tab, enter the name and description of the device.**

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

1. Click  (Add Group) or  (Add Device).

2. Select a target device or group, and click [OK].

**6. On the [Schedule] tab, specify the schedule to execute the task.**

**7. Click  (Save) when the setting is complete.**

#### Note

- Once a log has been retrieved, it will not be retrieved the next time the task is executed.
- Only one device log can be retrieved for each device even when Device Manager NX is used several times.
- You cannot use Device Manager NX and other device log collecting software at the same time for the same device.
- The log transfer setting specified in other log collecting software such as Remote Communication Gate S will be disabled when you configure Device Manager NX to retrieve device logs.
- When the number of logs exceeds the maximum number that can be stored in a device, the oldest log is deleted. Configure the schedule so that all logs are collected.
- The maximum number of logs that can be stored in a device may vary depending on the device. For details, consult your sales or service representative.
- The number of retrieved device logs is recorded in the task log. For details about task logs, see page 70 "Checking Task Logs".
- For details about the settings on each tab, see page 148 "Device Log Management".

- You cannot operate the device until the collection of the device log that is stored in the device is complete. Collect the log when the device is not used.
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.

---

## Exporting the Device Log as a CSV File

---

3

1. In the section area, click [Log Management].
2. Click [Device Log Export] on the section tree.
3. Specify the start and end dates of the device log you want to export.
4. Click [Export].

### Note

- For details about the settings, see page 148 "Device Log Management".
- For details about the items that will be exported to a CSV file, see page 216 "Format of a Device Log CSV File".

# 4. Changing the Device Settings

This chapter explains how to configure devices by using templates.

## What is a Template?

A template provides a set of configuration values to change device settings at one time. Use a template to share settings among devices so as to maintain device setting consistency. Applying a template regularly can provide shared settings among devices.

You can use Device Manager NX to create templates with the following categories:

### Device

Changes can be added to configuration items related to main unit settings such as system, paper, date/time, e-mail, and network.

For details, see page 51 "Applying Same Settings to Multiple Devices".

### User data

Per user restrictions on use of devices can be provided, or per user counter information can be reset.

For details, see page 55 "Managing the User Data".

### Software

Manages or installs software and applications on devices.

- SDK/J Platform Update  
Updates the SDK/J platform.
- SDK Application  
Performs installation, uninstallation, activation, and update of SDK applications.

For details, see page 61 "Managing SDK Applications and the SDK/J Platform".

### Power mode

Turns on energy saver mode. Also, this template can be used to return a device from energy saver mode to its previous mode.

For details, see page 54 "Applying Energy Saver Mode to Multiple Devices at One Time".

### Template Creation Process

Step	Description
1. Select a template type.	Select a template appropriate for the settings you want to change. In the [Configuration] section, click a template to change the settings.

Step	Description
<p><b>2. Create a template.</b></p>	<p>Edit the template that contains configuration items and setting values to be changed for target devices and groups.</p> <ul style="list-style-type: none"> <li>• Example 1: Change the paper type of the source tray 1 from [Plain Paper] to [Thick Paper].</li> <li>• Example 2: Update the SDK/J platform.</li> </ul>
<p><b>3. Register tasks and apply the template.</b></p>	<p>In the [Configuration] section, click [Tasks].</p> <p>Specify the target devices of the created template, and then configure "Task Type" for the template.</p> <ul style="list-style-type: none"> <li>• Example 1: When the task type of the template is [Apply], the paper type of the source tray 1 is set to [Thick Paper] automatically.</li> <li>• Example 2: When the task type of the template is [Check &amp; Apply], the version of the SDK/J platform available on RICOH Software Server is checked first. If a newer version is found on the server, it is updated.</li> </ul>



# Applying Same Settings to Multiple Devices

Create Device Preference to configure various device settings at one time.

## ★ Important

- The following access accounts are required to implement Device Preference.
  - Web Service account
  - SNMP account


The basic and advanced templates have different template target devices, settings of devices that can be retrieved when a template is created, and permission for editing settings.


Difference	Advanced Device Preferences	Basic Device Preferences
Template target device * <sup>1</sup>		
Retrieval of confidential information of device	Available	Not available
Editing of retrieved settings	Not available	Available
Retrieval of images on the [Home] screen	Available	Not available

\*<sup>1</sup> This can be checked by the device icons displayed in the device list.

## Creating a Template by Editing Device Settings (Basic Device Preferences)

Create a template by retrieving settings from a device or a file or by creating new settings.

1. In the section area, click [Configuration].
2. In the [Device Preference] > [Template] category on the section tree, click [Basic Device Preferences].
3. Click  (Add) in the list area.

Select a template that is registered to the list area and then click  (Copy) to create a new template based on the selected template. Proceed to Step 6.

4. Specify how to create a template.

- [Create Blank Template]  
Create a new template.

- [Get Data from Device]

Retrieve the present values of configuration items from a device, and then edit a template based on this data. Encrypted information, such as password and security settings, cannot be retrieved.

1. Click [Select Device].
2. Select a device to retrieve data, and then click [OK].

- [Import CSV File]

Import a CSV file.

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

5. Click [OK].

6. On the [General] tab, enter a template name and a description.

7. On the [Basic Device Preferences] tab, configure the necessary items.

8. Click  (Save) when the setting is configured.

 **Note**

- For details about the configuration items, see page 157 "List of Device Preference Setting Items".
- You must register a task to apply a template. For details, see page 64 "Registering Created Templates to Tasks".


---


## Creating a Template for Copying Device Settings (Advanced Device Preferences)

---

Create a template for applying settings of a device to another device as is.

 **Important**

- Settings of the advanced template are retrieved and the advanced template is applied to the following devices:
  - Devices of device icons: 
- A template cannot be applied to devices that are different from the model that has been acquired in the template.

1. In the section area, click [Configuration].
2. In the [Device Preference] > [Template] category on the section tree, click [Advanced Device Preferences].
3. Click  (Add) in the list area.
4. Enter a template name and a description.

## 5. Specify how to create the template.

- [Backup from Devices]

Retrieve settings of each item from a device and create a template. Confidential information, such as password and security settings, can also be retrieved. The retrieved settings cannot be changed.

1. Click [Select Device].
2. Select the device from which to retrieve the data, and then click [OK].
3. Enter a password to protect the data
4. To retrieve images, select the [Logo Image] check box.

- [Import Backup File]

Import a device backup file and create a template. The retrieved settings cannot be changed.

1. Enter the password that was specified when creating the backup file.
2. Click [Browse...].
3. Specify the file to be imported, and then click [Open].
4. To retrieve images, click [Browse...] under [Logo Image].
5. Specify the image file and click [Open].

## 6. Click [OK].

## 7. Click (Save) when the setting is configured.

### Note

- When applying an advanced template, all setting values from the device or backup file are retrieved.
- The images retrieved by a template are used for the [Home] screen on the device display panel. For images, see the instruction manual that comes with the device.
- You must register a task to apply a template. For details, see page 64 "Registering Created Templates to Tasks".





# Applying Energy Saver Mode to Multiple Devices at One Time

Create a template so that energy saver mode can be applied to multiple devices at one time. Also, create a template so that devices can be returned from energy saver mode to their previous modes.

## ★ Important

- The following access account is required to set the Power Mode Preference.
  - SNMP account
- Do not turn off the target device while configuring a device.

4

1. In the section area, click [Configuration].
2. In the [Power Mode] category on the section tree, click [Tasks].
3. Click  (Add) in the list area.
4. On the [General] tab, enter a template name and a description.
5. Select [Energy Saver Mode] or [Cancel Energy Saver Mode].
6. On the [Target Devices/Groups] tab, specify the target devices/groups.
  1. Click  (Add Group) or  (Add Device).
  2. Select a target device/group.
  3. Click [OK].
7. On the [Schedule] tab, specify when to perform a task.
8. Click  (Save) when the setting is complete.

## ↓ Note

- For Power Mode configuration items, see page 132 "Power Mode".
- Energy saver mode cannot be enabled if a device is operating a print job or its current mode cannot be changed to energy saver mode.
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.



# Managing the User Data

The method for managing user data is described below. Using User Data Preference, you can specify how to use devices per user and add or delete users.


## ★ Important


- The following access accounts are required to enable User Data Preference:
  - Web Service account
  - SNMP account

## Creating a User Data Template

### ★ Important

- When acquiring data from a device to create a template, the processing of the data may take longer, or a data-read error may occur if the address book of the device is encrypted. If you want to encrypt the address book data to protect it from being read by other users, use the data encryption function of the device.

1. In the section area, click [Configuration].
2. In the [Address Book] category on the section tree, click [Template].
3. Click  (Add) in the list area.

Select a template that is already registered in the list area and then click  (Copy) to create a new template based on the selected template. Proceed to Step 7.

4. Enter a template name and a description.
5. Specify how to create a template.

- [Get Data from Device]  
Retrieve user data from a specified device.
  1. Click [Select Device].
  2. Specify the device from which to retrieve data, and then click [OK].
- [Backup from Devices]  
Retrieve user data, including confidential information, from a specified device.
  1. Click [Select Device].
  2. Specify the device from which to retrieve data, and then click [OK].
  3. Enter a password.
- [Import CSV File]  
Import a template file.

1. Click [Browse...].
  2. Specify the file to import, and then click [Open].
- [Import CSV File (SmartDeviceMonitor for Admin)]  
Import SmartDeviceMonitor for Admin's address data and user data. Prepare two CSV files exported using the Address Management Tool and User Management Tool.
    1. Click [Browse...] under [File Path (Address Management Tool)].
    2. Specify the address information CSV file, and then click [Open].
    3. Click [Browse...] under [File Path (User Management Tool)].
    4. Specify the user data CSV file, and then click [Open].
  - [Import Backup File]  
Import user data from a device backup file.
    1. Click [Browse...].
    2. Specify the backup file, and then click [Open].
    3. Enter the password that was specified when creating the backup file.
  - [Create Blank Template]  
If a template is newly created, specify a user data authentication method using the following. Select the authentication method that was specified at the time of setting of the registered user or group.
    - User Code / None: With or without user code authentication
    - Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server

**6. Click [OK].**

**7. Click the [Preference Settings] tab.**

Configure the following settings here for all users registered to the device.

For details about the setting items, see page 121 "Address Book".

- Collection of per user counters
- Resetting of user counters (Reset Volume Use)
- Deletion of all entries at one time
- Configuration of complete entry matches

**Note**

- Collection of per user counters cannot be used in Device Manager NX Accounting.

**8. Click the [Entry List] tab, and select the user or group to be registered.**

For registration of a user or group, see page 57 "Registering a User or a Group to the Entry List".

For user or group setting items, see page 121 "Address Book".

**9. Click  (Save) when the setting is configured.**

### Note

- You must register a task to use a template. For details, see page 64 "Registering Created Templates to Tasks".
- If a template is created using [Backup from Devices], you cannot edit any existing user data. User restriction settings can be configured using [Preference Settings].
- If a template is created using [Import from File], only the existing user data can be retrieved. User restriction settings are part of the default settings.
- [Import from File] enables you to import a CSV file that was exported by SmartDeviceMonitor for Admin.

## Registering a User or a Group to the Entry List

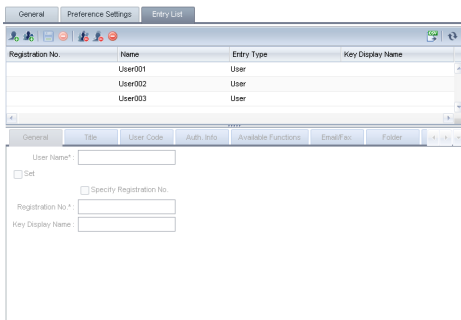
4

The following is the method for configuring settings for a user or a group to be registered to a device.

### Important

- **User authentication is implemented on some devices to protect user data.**

### How to read the entry list



: Add a new user.

: Add a new group.

: Save the edited user or group information.

(Delete): The selected user or group is deleted.

(Delete All Groups): All the groups are deleted.

(Delete All Users): All the users are deleted.

(Delete All): All the users/groups are deleted.

: The information of the entry list is exported to/imported from a CSV file.

Each tab: Specify the user or group selected in the entry list.

 **Note**

- For details about the setting items on each tab, see page 121 "Address Book".

## Adding a user/group

---

**1. Display the entry list.**

Follow Steps 1 to 8 of page 55 "Creating a User Data Template".

**2. Click  (Add User) for adding a user. Click  (Add Group) for adding a group.**

**3. Click each tab and make necessary settings.**

For details about the setting items on each tab, see page 121 "Address Book".

**4. Click  (Save) when the setting is configured.**

4

## Adding a user to a group

---

**1. Display the entry list.**

Follow Steps 1 to 8 of page 55 "Creating a User Data Template".

**2. Select a user.**

To create a new group in another group, select a group in the list.

The group to which you want to add a user must be created beforehand.

**3. Click the [Group List] tab.**

**4. Select the [Set] check box.**

**5. After creating a destination group, add it to [Selected Groups].**

**6. Click  (Save) when the setting is configured.**

## Deleting a user/group

---

**1. Display the entry list.**

Follow Steps 1 to 8 of page 55 "Creating a User Data Template".

**2. Delete any or all users/groups.**

To select multiple users or groups, click a user or group while pressing the SHIFT or CTRL key.

**3. Click  (Delete).**

To delete all groups, click  (Delete All Groups).

To delete all users, click  (Delete All Users).

To delete all entries, click  (Delete All).

## Exporting user data

Save the user data displayed in the entry list as a CSV file.

### 1. Display the entry list.

Follow Steps 1 to 8 of page 55 "Creating a User Data Template".

### 2. Click (Exports data to CSV files.).

### 3. Specify the data format of the CSV file.

### 4. Specify a save destination and file name, and then click [Save].

#### Note

- For the CSV file format, see page 178 "Format of CSV Files".
- The following limitations apply when data is exported as a CSV file in SmartDeviceMonitor for Admin Compatible Format (Address Management Tool):
  - Only the items on the tab whose [Set] checkbox are selected are exported.
  - If a template contains an entry that does not have a registration number assigned, it cannot be exported. To export data as a CSV file, assign a registration number for each entry.
- The following limitations apply when data is exported as a CSV file in SmartDeviceMonitor for Admin Compatible Format (User Management Tool):
  - Only the items on a tab whose [Set] checkbox are selected are exported.
  - The entry information cannot be exported if a user code or login user name is not specified for the entry.

## Managing a special user

If no user code is registered for a user, all information about the user will be processed as described below.

- A print job is classified as "other".
- Any information about the user is included in the user counters, but it is not displayed in the entry list, etc., on the screen.
- No maximum value can be specified for print quantities. Also, the usage counter figures and user counter information cannot be cleared.

## Resetting the User Counter Information

The following is the method for resetting the counter per user data.

You can reset the following counter information:

- Printing (copier/fax printing/printer) counter

- Fax transmission counter
- Scanner counter
- Volume used (if the function to limit printing utilization quantity is enabled.)


**★ Important**

- Some devices are not compatible with this function.
- If user data is specified, user authentication can be used to protect user data. User authentication methods differ depending on which device is used. Only an administrator who can configure user authentication settings can implement user authentication.
- The counter for print quantities and user counter information cannot be specified for "Other" users.

4

1. Display the entry list.

Follow Steps 1 to 8 of page 55 "Creating a User Data Template".

2. Select a user.
3. Click the [Reset Counter per User] tab.
4. Select the [Set] check box.
5. To reset the counter, select the counter information check box.
6. Click  (Save) when the setting is configured.

# Managing SDK Applications and the SDK/J Platform

Create templates to check the version of the SDK/J platform or the versions of the SDK applications installed in the device. Also, create templates to update the SDK/J platform or SDK applications or to install SDK applications.

Device Manager NX can link to the RICOH Software Server using the Internet to acquire up-to-date information about the SDK/J platform and SDK applications.

## ★ Important

- Some SDK applications cannot be used in Device Manager NX. For the information about the applications that can be used in the product, see the manual for the SDK application, or contact your dealer or service representative.
- The following access accounts are required to perform the SDK/J Platform Update:
  - SNMP account
  - SDK account
- The following access accounts are required to configure the SDK Application:
  - Web Service account
  - SNMP account
  - SDK account
- Any operation applied to SDK applications for Smart Operation Panel will be canceled on a machine that is not equipped with Smart Operation Panel.

4

## Template for Updating the SDK/J Platform

Use the template indicated below, which is provided by default, to update the SDK/J platform.

- SDK/J Platform Update

You do not have to create and edit a template.

This template retrieves the latest version of the SDK/J platform from the RICOH Software Server and updates the SDK/J platform of the target device.

## ↓ Note

- You must register a task to use a template. For details, see page 64 "Registering Created Templates to Tasks".

---

## Creating a Template for SDK Application Settings


---

Create a template for installation, update, uninstallation, and activation of SDK applications.


### Create a template using the RICOH Software Server

---

#### ★ Important

- A connection to the RICOH Software Server is required to create a template.
1. In the section area, click [Configuration].
  2. In the [Software] > [Template] > [SDK Application] category on the section tree, click [RICOH Software Server].
  3. Click  (Add) in the list area.
  4. On the [General] tab, enter a template name and a description.
  5. Select a template action.
  6. Enter the product key of the target SDK application in the [Product Key] box.
  7. Click [Retrieve Application List].

The remaining license count and total license count of the entered product key are displayed.

8. On the [Application List] tab, set the SDK application to be registered to the template.
9. Click  (Save) when the setting is configured.

#### ↓ Note

- The following operations are performed automatically, as necessary:
  - Installation of an application file
  - File activation
  - Automatic change to the SDK/J platform heap size
  - Automatic update of the SDK/J platform
- You must register the country information. The country information specified for the system settings of Device Manager NX is registered automatically. For country information settings, see page 135 "Activation/Deactivation/Usage Report Notification".
- If an application is installed, there is a possibility where the RICOH Software Server may determine whether the application can be introduced.
- If an application is uninstalled, deactivation is performed automatically. If deactivation fails, the application is not uninstalled.
- A template created with the RICOH Software Server has a configuration wherein the SDK application that is specified by the template is delivered from the RICOH Software Server at the



time of task execution. If there is a time lag between the time of template creation and task execution, an error may occur in the version of the specified SDK application.


- For details about the configuration items of SDK Application Settings, see page 118 "Software".
- You must register a task to use a template. For details, see page 64 "Registering Created Templates to Tasks".
- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.

## Registering Created Templates to Tasks




To implement a template, register it to a task or create a task schedule so that the template can be implemented at a specified date/time.


### ★ Important

- Do not turn off the power for the target device while setting a device.

1. In the section area, click [Configuration].
2. In the each category on the section tree, click [Tasks].
3. Click  (Add) in the list area.
4. On the [General] tab, enter a task name and a description.
5. Select the template to be registered to the [Template] list.
6. Select [Check], [Apply], or [Check & Apply].

Some actions cannot be specified depending on the type of template. For details, see page 64 "Configuration Task Type".

7. On the [Target Devices/Groups] tab, set the execution target devices/groups.
  1. Click  (Add Group) or  (Add Device).
  2. Select a target device/group.
  3. Click [OK].
8. On the [Schedule] tab, specify when to perform the task.
9. Click  (Save) when the setting is complete.

A task is registered to the list. To immediately execute the task, click  (Run Immediately).

### ↓ Note

- When the schedule you set will be performed, Device Manager NX must be run on the PC. When Device Manager NX is not run, the schedule will not be performed.

## Configuration Task Type

### ★ Important

- Do not turn off the power for the target device while setting a device.
- The processing of the data may take longer time, or a data-read error may occur if the address book of the device is encrypted. If you want to encrypt the address book data to protect it from being read by other users, use the data encryption function of the device.

**Basic Device Preferences**

Task Type	Description
Check	Checks that the values configured by the template are applied.
Check & Apply	Checks that the values configured by the template are applied. If the applied values are different, the values configured by the template are applied. If all the setting values are identical with the values configured by the template, Apply is not implemented. Confidential information cannot be checked so that Apply is always implemented.
Apply	Applies the values configured by the specified template. If there are configuration items that require a device reboot after Apply is implemented, Device Manager NX restarts the device. Also, depending on how configuration items are combined, multiple reboots may be required.

**Advanced Device Preferences**

Task Type	Description
Check	-
Check & Apply	-
Apply	Applies the values configured by the specified template. If there are configuration items that require a device reboot after Apply is implemented, Device Manager NX restarts the device. Also, depending on how configuration items are combined, multiple reboots may be required.

**Address Book**

Task Type	Description
Check	Checks that the values configured by the template are applied. "Check" is implemented for all users registered to the device to check that the values configured by Preference Settings are applied.
Check & Apply	Checks that the values configured by the template are applied. If the applied values are different, the values configured by the template are applied. Confidential information cannot be checked so that Apply is always implemented. If a user logging on to a device is a target user to be deleted, the user cannot be deleted. Other target users are deleted, and the message "Failed to delete the Address Book for the device" is registered to the log file.

Task Type	Description
Apply	<p>Applies the values configured by the specified template.</p> <p>If the template is in backup format, "Apply" may fail for devices of different backup formats. Also, the address book data registered before "Apply" is implemented may be completely deleted and replaced by the backup address book data.</p>

**SDK/J Platform Update**

Task Type	Description
Check	Checks whether the version of the device's SDK/J platform is the latest.
Check & Apply	<p>Updates the SDK/J platform to the latest version.</p> <p>If the major version is different, updates fail.</p>
Apply	-

**SDK Application**

Task Type	Description
Check	<ul style="list-style-type: none"> <li>• Install/Update Checks that an application is installed and its version is as specified. Also, "Check" is implemented to check that the application is activated as required.</li> <li>• Uninstall Checks that the specified application is not installed.</li> <li>• Activate Checks that the specified application is activated.</li> </ul>

Task Type	Description
Check & Apply	<ul style="list-style-type: none"> <li>• Install/Update Updates the application if the required version is not installed. This process is skipped if the required version or later is installed. If a template is created using the connected RICOH Software Server, activation of the updated application, changes to SDK/J platform heap size, and updates of the SDK/J platform are performed automatically.</li> <li>• Uninstall If a specified application is installed, it is uninstalled from the device. If a template is created using the connected RICOH Software Server, deactivation is performed automatically.</li> <li>• Activate If a specified application is not activated, it is activated.</li> </ul>
Apply	-

**Note**

- If any setting item is not found in the setting target device, Apply is skipped.



# 5. Checking the System Operation Status

This chapter explains task management and the various logs.

## Managing Tasks

Device discovery, polling, application installation, and other functions are executed by tasks. The following describes how to check the working status of a task, task operations, or schedule settings to perform tasks at a specified time.

### Managing a Task in the Schedule Standby Status

1. In the section area, click [Tasks].
2. In the section tree, click [Scheduled Tasks].

A list of tasks in the schedule standby status is displayed.

#### Scheduled task list display items

Item	Description
Name	The task name entered during task registration.
Description	The task description specified during task registration.
Type	Displays the task status (Schedule Standby).
Enable	Indicates whether the task schedule is enabled or disabled.
Schedule Type	Displays the schedule settings. Example: Once Only, Interval, Daily, Weekly, Monthly
Interval	Displays the interval time when the schedule type is set to [Interval].
Start	Displays the task start date/time.
Update	Indicates the date/time at which the task was created or edited.
User	Indicates the name of the user who created or edited the task.

**Note**

- You cannot change the schedule or delete tasks in the scheduled task list. To delete a task or change its schedule, you must first select the destination to which the task is registered.

## Checking Task Logs

Task operations are recorded. You can check the operation results of a task for each device or setting item.



You can also use a task log to check tasks in progress and operations such as task suspension and restart.

- In the section area, click [Tasks].
- In the section tree, click [Task Logs].

A task log list appears.

- Select a task log to work on.

If you cannot find a task log, use filtering.

- Click  (Filters), and an input/select area is displayed.
- Select a keyword.
- Click  (Filters) located at the right end of the input/select area, or press the Enter key.

- Check the contents of the task log using the [Result Details] tab.

You can view the details of the task log. The displayed contents may differ depending on the task type.

For configuration tasks, the result of each device is displayed. When you select a device, the result of each item for the device appears.

### Items displayed in the task log list

Item	Description
Start Date	The task start date/time is displayed.
End Date	The task end date/time is displayed.
Task Name	The registered task name is displayed.
Category	The category of the function is displayed. Example: Discovery, Device Monitoring, Configuration, etc.
Event	Event details of the task are displayed.
Progress	The progress status of the task is displayed.



Item	Description
Result	Task implementation results are displayed.
Cause	If a task fails, reasons for the failure may be displayed.
Error Code	An error code is displayed. For details, see page 76 "Error Code List".
Owner	Task owner is displayed.


### ↓ Note

- If Device Manager NX is restarted or an unexpected shutdown occurs while a task is in process or is suspended, the task after restart is suspended. A log such as "Cancelled because of system suspension." is kept.
- If more than one device is added using Add Device, the result of the task log for Add Device will appear as "Failed" even when only one of the devices has failed to be added.

5

## Writing a task log to a file

Save the task log as a CSV file.

1. In the section area, click [Tasks].
2. In the section tree, click [Task Logs].  
A task log list appears.
3. Click  (Exports data to CSV files).
4. Specify the save destination and file name, and then click [Save].

## Retrying a failed task

If communication with a device has been interrupted or access to a device has been denied, and the task could not be performed normally, try registering the task again.

## Suspend (Short) / Resume a task


1. In the section area, click [Tasks].
2. In the section tree, click [Task Logs].
3. In the task logs, select the task that you want to set to Suspend (Short) or Resume.  
Suspend (Short) can be applied to a task being processed.  
Resume can be applied to a suspended task.

4. Click  (Suspend) or  (Resume).

---

### Canceling a task being processed

---

1. In the section area, click [Tasks].
2. In the section tree, click [Task Logs].
3. In the task logs, select the task you want to cancel.  
Task Cancel can be applied to a task being processed or suspended.
4. Click  (Stop).

---

### Notifying/Confirming Overdue Tasks

---

5

If Device Manager NX is not running at the time a task is scheduled to perform, The tasks that could not be executed are displayed in the list as "Non-executed Task List". You can execute those tasks immediately if necessary.

#### Note

- This item can be used in Device Manager NX Accounting.

---

### Specifying types of tasks for which to receive notification

---



Specify the types of task for which to receive notification as a "Non-executed Task List".

1. In the section area, click [Notification Policy].
2. In the [Task Notification] category of the section tree, click [Non-executed Task Notification Settings].
3. In the Tab area, select the check box of the task type for which to receive notification.
4. Click [Save].

---

### Performing a non-executed task immediately

---

1. Click [Yes] in the dialog box notifying you of non-executed tasks.
2. Select a non-executed task in the list area.
3. Click  (Search).
4. Select a non-executed task, click  (Immediately).

# Checking System Operation Logs

Use Device Manager NX to check the following logs that record system operations:

## Task Log

Task operations are recorded. You can check the operation results of a task for each device or setting item. For details, see page 70 "Checking Task Logs".

## System Log

System operations are recorded. System operations such as log storage period, limitation of hard disk space, task start/end, etc., can be checked in this log.

## Notification Log

Notification results are recorded.

---

## Checking the System Log

---

5

The following describes how to display the system log and items:

1. In the section area, click [Logs].
2. In the section tree, click [System Log].

A log list appears.


### Items displayed in the system log

Item	Description
Date	The date/time of log registration is displayed.

Item	Description
Category	The category of a function is displayed.
Function	The contents of execution by the system are displayed.
Function Details	The correlation among categories, functions, and function details is in a tree structure as shown below. Example: <ul style="list-style-type: none"> <li>• Device Monitoring (Category) <ul style="list-style-type: none"> <li>• Device Monitoring (Function) <ul style="list-style-type: none"> <li>• Status (Function Details)</li> <li>• Supplies (Function Details)</li> </ul> </li> </ul> </li> <li>• Device Configuration (Category) <ul style="list-style-type: none"> <li>• Device Preference (Function) <ul style="list-style-type: none"> <li>• Check (Function Details)</li> <li>• Apply (Function Details)</li> </ul> </li> </ul> </li> </ul>
Event	Event details are displayed.
Result	Implementation results of the system or operation are displayed.
Description	If a task fails, reasons for the failure may be displayed.
Error Code	An error code is displayed. For details, see page 76 "Error Code List".

## Exporting the system log as a file

Save the system log as a CSV file.

1. In the section area, click [Logs].
2. In the section tree, click [System Log].  
A log list appears.
3. Click  (Exports data to CSV files).
4. Specify a save destination and a file name, and then click [Save].

## Checking the Notification Log

The contents of notification settings and results of notification can be checked.

The following describes the method for displaying a log related to notification and display items.

1. In the section area, click [Notification Policy].
2. In the [Status Notification] category on the section tree, click [Logs].


A notification log list appears.

#### Items displayed in the notification log

Item	Description
Date	The date/time of delivery is displayed.
Notification Policy Type	The notification target function is displayed.
Notification Policy Name	The notification condition definition name is displayed.
Device Display Name	The device that sent notification is displayed.

#### Exporting the notification log as a file

Save the notification log as a CSV file.

1. In the section area, click [Notification Policy].
2. In the [Status Notification] category on the section tree, click [Logs].  
A notification log list appears.
3. Click  (Exports data to CSV files).
4. Specify a save destination and a file name, and then click [Save].

## Error Code List

The causes of errors and their solutions are described below:

Code	Cause	Solution
004	Unsupported device.	A function not supported by the target device is specified. Check the target device.
005	Unsupported item.	A setting item not supported by the target device is specified. Check the target device.
006	Unsupported value.	A configuration values not supported by the target device is specified. Check the target device.
018	The SDK/J platform has not been installed.	The machine is operating normally.
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.
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.
033	XX device logs have been collected.	The machine is operating normally.
051	A character(s) other than a numerical value is included in the version.	Check the configuration values.

Code	Cause	Solution
056	Unknown data has been retrieved.	Check the status of the retrieved 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.
060	The entry does not exist.	The Address Book entry for the device and the template are not the same.
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.
077	The device log settings are not enabled.	Enable the device log retrieval setting.
100	Device authentication has failed.	Check whether the following settings of the device access account are correct: <ul style="list-style-type: none"> <li>• User name and/or password of your Web service account</li> <li>• Community name if SNMPv1/v2 protocol is used</li> <li>• User name and password if SNMPv3 protocol is used</li> </ul> See page 19 "Configuring Access Accounts".

Code	Cause	Solution
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).
107	You do not have the privileges to perform this operation.	Check whether the following settings of the device access account are correct: <ul style="list-style-type: none"> <li>• User name and password of your Web service account</li> <li>• Community name if SNMPv1/v2 protocol is used</li> <li>• User name and password if SNMP v3 protocol is used</li> </ul> See page 19 "Configuring Access Accounts".
108	The setting target is different.	The target device does not support the set function. 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.



Code	Cause	Solution
150	Parameters for other devices are invalid.	<ul style="list-style-type: none"> <li>• Check the configuration values.</li> <li>• The target device does not support the set function. Check the target device.</li> <li>• A task that is not supported by the target device, was executed. Check the device.</li> <li>• 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.</li> </ul>
200	No response from the device.	<ul style="list-style-type: none"> <li>• Check the network environment.</li> <li>• Check the device status.</li> </ul>
201	Network is disconnected.	<ul style="list-style-type: none"> <li>• Check whether the network has any problems.</li> <li>• Contact the administrator.</li> </ul>
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.	<ul style="list-style-type: none"> <li>• Check the network environment.</li> <li>• Contact the administrator.</li> </ul>
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.	<ul style="list-style-type: none"> <li>• Retry the process later.</li> <li>• Do not use the device while a task in progress.</li> </ul>

Code	Cause	Solution
211	System busy has occurred on the device.	<ul style="list-style-type: none"> <li>• Retry the process later.</li> <li>• Do not use the device while a task in progress.</li> </ul>
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.
214	Failed to restart the device.	<p>Check whether the following settings of the device access account are correct.</p> <ul style="list-style-type: none"> <li>• User name and password of your Web service account</li> <li>• Community name if SNMP v1/v2 protocol is used</li> <li>• User name and password if SNMP v3 protocol is used</li> </ul> <p>See page 19 "Configuring Access Accounts".</p>
216	Unable to communicate with the SDK/J platform.	<ul style="list-style-type: none"> <li>• Check whether the SDK/J platform is installed.</li> <li>• Check whether the SDK/J platform is working.</li> </ul>
217	Failed to update the SDK/J platform.	Restart the device and perform the operation again.
218	The SDK/J platform file is invalid.	Perform the operation again.
220	Failed to install the SDK application.	Restart the device and perform the operation again.
221	Failed to update the SDK application.	Restart the device and perform the operation again.
222	Failed to uninstall the SDK application.	Restart the device and perform the operation again.
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.	<ul style="list-style-type: none"> <li>• Check whether the target device access account is correct.</li> <li>• The address book on the target device may be being edited. Check the device status.</li> </ul>
245	Failed to batch delete users.	<ul style="list-style-type: none"> <li>• Check whether the target device access account is correct.</li> <li>• The address book on the target device may be being edited. Check the device status.</li> </ul>
246	Failed to batch delete groups.	<ul style="list-style-type: none"> <li>• Check whether the target device access account is correct.</li> <li>• The address book on the target device may be being edited. Check the device status.</li> </ul>

Code	Cause	Solution
247	Failed to batch delete destinations.	<ul style="list-style-type: none"> <li>• Check whether the target device access account is correct.</li> <li>• The address book on the target device may be being edited. Check the device status.</li> </ul>
248	Device access control settings have failed.	<ul style="list-style-type: none"> <li>• Check whether the target device access account is correct.</li> <li>• The address book on the target device may be being edited. Check the device status.</li> </ul>
250	Failed to check.	A problem such as the device being turned off may have occurred while configuring the settings. Check the device status.
253	SDK/J platform is suspended	Retry the process after the device restarts.
260	Failed to change the entry information.	Restart the device and perform the operation again.
261	Failed to delete the entry.	Restart the device and perform the operation again.
263	Failed to delete the group.	Restart the device and perform the operation again.
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
280	Other device error occurred.	<p>Check the target device settings.</p> <p>Check the target device.</p> <p>Check that the specified password does not violate the password policy of the device.</p> <p>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.</p> <p>If none of the these conditions applies, restart the device and perform the operation again.</p>
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.	<ul style="list-style-type: none"> <li>• Check the network environment.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> </ul>
307	Unable to communicate with the RICOH Software Server.	Check whether RICOH Software Server 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.
310	Failed to transmit data.	<ul style="list-style-type: none"> <li>• Check that the server and network environment settings are correct.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> </ul>
311	Failed to receive data.	<ul style="list-style-type: none"> <li>• Check that the server and network environment settings are correct.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> </ul>

Code	Cause	Solution
313	SSL communication is unavailable.	<ul style="list-style-type: none"> <li>• Check that the certificate is correctly configured.</li> <li>• Check that the server and network environment settings are correct.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> <li>• If the error code is displayed while the product online is enabled, check whether the setting can be configured when activated offline.</li> </ul>
350	Other external system connection error.	<ul style="list-style-type: none"> <li>• Check that the server and network environment settings are correct.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> </ul>
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.
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.
450	Other system entry error.	Check that the specified setting values and parameters are correct.
503	Failed to read the data.	Check whether there is a problem with the data to be loaded.
504	Failed to save the data.	Check whether there is a problem with the data to be saved.
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.

Code	Cause	Solution
601	Cancelled because of system suspension.	Device Manager NX has exited or a computer shutdown occurred. Restart the computer and Device Manager NX.
602	The system has insufficient memory.	<ul style="list-style-type: none"> <li>The hard disk has insufficient free space. Delete unnecessary data.</li> <li>Restart the computer and Device Manager NX.</li> </ul>
604	The product key is invalid.	Enter a correct product key.
605	The template has been saved. Check there are enough licenses to execute the task.	<ul style="list-style-type: none"> <li>Purchase additional license(s).</li> <li>Deactivate software installed on other devices.</li> </ul>
606	Failed to read the data.	<ul style="list-style-type: none"> <li>Install on another device.</li> <li>Check the status of the retrieved device.</li> </ul>
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.
612	Failed to restart the device.	<ul style="list-style-type: none"> <li>Do not use the device when settings are configured.</li> <li>Check whether the access account is configured correctly.</li> </ul>
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
631	Failed to initialize the task because the task information is incorrect.	Check that the task setting is properly configured.
632	Failed to initialize the task because the target device does not exist.	Check the target device.
634	Failure has occurred on the previous setting item.	<ul style="list-style-type: none"> <li>• Check the target device.</li> <li>• Check that the task setting is properly configured.</li> </ul>
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.	For details, see page 87 "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.
642	There are no failed devices.	The machine is operating normally.
643	There are no configured devices.	The machine is operating normally.
648	Failed to transmit data.	<ul style="list-style-type: none"> <li>• Check that the server and network environment settings are correct.</li> <li>• Check that the proxy server has been correctly set in the [System] section.</li> </ul>
650	Other system error	Check that the system setting of Device Manager NX is properly configured.



Code	Cause	Solution
660	Failed to read the data.	Check that the following settings of the device access account are properly configured: <ul style="list-style-type: none"> <li>• User name and login password of Web Service Account</li> <li>• Community name if SNMP v1/v2 protocol is used</li> <li>• User name and login password if SNMP v3 protocol is used</li> </ul>
670	There are some non-executed tasks that cannot be performed because the system has been suspended.	The machine is operating normally.
708	System startup has not completed yet. The task will be run as soon as the system is ready.	Device Manager 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.

## 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.
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.

Code	Causes and solutions
E06	<p>This error occurs during product key entry.</p> <p>The license related to this product key has been canceled.</p> <p>Check the product key and enter it again.</p>
E07	<p>This error occurs during product key entry.</p> <p>The software corresponding to the entered product key was not found.</p> <p>Check the product key and enter it again.</p>
E09	<p>This error occurs during installation.</p> <p>Installation of the specified software onto the device is not permitted due to an insufficient number of licenses.</p> <p>Purchase the required number of licenses.</p>
E10	<p>This error occurs during installation.</p> <p>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.</p> <p>Enter the product key that was used last time.</p>
E13	<p>This error occurs during installation.</p> <p>The device number is incorrect.</p> <p>Check the device number, and perform the operation again.</p> <p>If the problem cannot be solved, contact your service representative.</p>
E18	<p>This error occurs during installation.</p> <p>A trial-use license cannot be used.</p> <p>Purchase the required license.</p>
E21	<p>This error occurs during installation.</p> <p>The license re-issue count exceeded the upper limit.</p> <p>If the problem cannot be solved, contact your service representative.</p>
E22	<p>This error occurs during product key entry.</p> <p>The requested parameter is invalid.</p> <p>Check the product key and enter it again.</p>

Code	Causes and solutions
E47	<p>This error occurs during installation.</p> <p>The software you are trying to install or update is not compatible with the software already installed on the device.</p> <p>Check the version of the software installed on the device.</p> <p>If the problem cannot be solved, contact your service representative.</p>
E53	<p>This error occurs during software installation/update.</p> <p>The version of the system installed on the device may be earlier than the required version.</p> <p>If the problem cannot be solved, contact your service representative.</p>
E54	<p>This error occurs during installation or update.</p> <p>The operation is not guaranteed with the selected device.</p> <p>Check the selected device or the product key.</p>
Exx xx: number	<p>Error code "Exx" is added to another error on the server side.</p> <p>For a detailed solution, contact your service representative.</p>
ER01	<p>This error occurs when publishing the installation license.</p> <p>An error occurred after the license has been published. The published license must be returned.</p> <p>For details about the solution to resolve the problem, consult your service representative.</p>



# 6. Maintenance

This chapter explains how to maintain Device Manager NX.

## Activating Device Manager NX

Device Manager NX must be activated in order to continue using the product after its trial-period has expired.

Activation can be executed after the device was registered in the device list in the [Device List] section.

### ★ Important

- **The trial-use period is 60 days. The functions of this product are disabled if the trial-use period expires without activation.**

There are two methods for activating the product: [Online] and [Offline].

### Online activation

Connect to the Internet directly from Device Manager NX and activate the product.

When a proxy server is required to access the Internet, configure the required settings in the [System Settings] category under the [System] section. For details, see page 135 "System Settings".

### Offline activation

If it is not possible to connect to the Internet in the environment where this product is used, retrieve the license code in advance from the license management Web site of RICOH, then activate the product.

### ↓ Note

- Device Manager NX cannot be activated if no device is registered in its device list. Search for and register a device using the discovery function before you activate the product.
- Activation may be performed after expiration of the trial-use period.
- If the network interface of the computer that is installed with Device Manager NX Accounting is replaced, the activation status enabled for the product is canceled (deactivation). In order to reactivate the product using the same product key, deactivate the product before replacing the network interface.
- If the product is not deactivated before the network interface is replaced, consult your sales or service representative.

---

## Activating Online

---

Connect to the Internet directly from Device Manager NX and activate the product.

1. **Start Device Manager NX.**
2. **Click the [System] section.**
3. **Click [Activation/Deactivation/Usage Report Notification] under [System Settings].**
4. **Select [Online] in [Activation Type].**
5. **Enter the product key.**
  - Using Device Manager NX Accounting  
Enter the product key that you purchased.
  - Using Device Manager NX Lite  
You do not need to enter the product key. Proceed to the next step.
6. **Click [Activate].**

A confirmation dialog box indicating the usage status appears.

- Using Device Manager NX Accounting  
Click [Yes] or [No] to finish activation process.
- Using Device Manager NX Lite  
Click [Yes] to finish activation process.

## Activating Offline

If it is not possible to connect to the Internet in the environment where Device manager NX is used, retrieve the license code in advance and activate the product.

### Flow of offline activation procedures

	Device Manager NX Accounting	Device Manager NX Lite
Step 1	-	Confirm the product key.
Step 2	Confirm the lock code.	
Step 3	Acquire the license code from the RICOH Web site for managing licenses.	
Step 4	Enter the license code in Device Manager NX to activate the product.	

### Step 1 - Confirming the product key

When using Device Manager NX Lite, check the product key that is displayed on the screen. When using Device Manager NX Accounting, start from Step 2.

1. **Start Device Manager NX.**
2. **Click the [System] section.**

3. Click [Activation/Deactivation/Usage Report Notification] under [System Settings].
4. Select [Offline] in [Activation Type].
5. Take a note of the text string that is displayed in [Product Key].

Then check the lock code. Proceed to Step 4 in "Step 2 - Confirming the lock code".

## Step 2 - Confirming the lock code

---

1. Start Device Manager NX.
2. Click the [System] section.
3. Click [Activation/Deactivation/Usage Report Notification] under [System Settings].
4. Write down the text string that is displayed in [Lock Code].

Select the lock code by dragging the mouse cursor over the string and press "Ctrl+C" key to copy the lock code to the clip board.

## Step 3 - Obtaining the license code

---

1. From a computer that can connect to the Internet, access the license management Web site of RICOH (<https://licensemanagement.ricoh.com/ai/>)
2. Click [Activation].
3. Enter the product key and lock code.
  - Using Device Manager NX Accounting  
Enter the purchased product key and the lock code that you wrote down in Step 2.
  - Using Device Manager NX Lite  
Enter the product key that you wrote down in Step 1 and the lock code in Step 2.
4. Follow the instruction displayed on the screen and enter the required information to acquire the license code.

## Step 4 - Activating the product

---

1. Start Device Manager NX.
2. Click the [System] section.
3. Click [Activation/Deactivation/Usage Report Notification] under [System Settings].
4. Select [Offline] in [Activation Type].
5. Enter the license code acquired in Step 3 in [License Code].
  - Using Device Manager NX Accounting

Click [Yes] or [No] to finish activation process.

- Using Device Manager NX Lite

Click [Yes] to finish activation process.

---

## Deactivating the Product

---

Make sure to deactivate Device Manager NX Accounting first, and then uninstall the product. This procedure is required to re-use the product key again.

### ↓ Note

- You cannot use the functions of Device Manager NX Accounting after the product has been deactivated.
- You do not need to perform any procedure to deactivate Device Manager NX Lite.

There are two methods for deactivating the product. Use any of the following procedure to deactivate the product:

### Deactivating Device Manager NX Accounting in the Product

Connect to the Internet directly from Device Manager NX and deactivate the product. If a proxy server is required to access the Internet, configure the required settings in the [System Settings] category under the [System] section. For details, see page 135 "System Settings".

### Deactivating the Product on the License Management Web Site.

Access the license management web site of RICOH from other computer, and deactivate Device Manager NX Accounting without using the product. To deactivate the product using this method, you must first uninstall Device Manager NX Accounting to acquire the license code.

---

## Deactivating Device Manager NX Accounting in the Product

---

1. Start Device Manager NX Accounting.
2. Click the [System] section.
3. Click [Activation/Deactivation/Usage Report Notification] under [System Settings].
4. Click [Deactivate].

### ↓ Note

- If the deactivation process fails, check that the computer on which Device Manager NX Accounting is installed can connect to the Internet.



## Deactivating the product on the license management web site

If you cannot access the Internet from the computer on which Device Manager NX Accounting is installed, use another computer that can access the Internet to access the license management web site of RICOH and perform the procedure to deactivate the product. To deactivate the product using this method, you must first uninstall Device Manager NX Accounting to acquire the license code.

**1. Quit Device Manager NX Accounting.**

**2. Start the uninstallation procedure of Device Manager NX Accounting.**

From the [Start] menu, select [All Programs], then select [Device Manager NX Accounting], and then click [Uninstall Device Manager NX Accounting].

You can also start the uninstallation process from [Programs and Features] in [Control Panel].

**3. Proceed as instructed on the screen.**

**4. When a message indicating that the uninstallation procedure is complete, read the message and check its contents.**

A message notifying that the deactivation process has failed appears. It also indicates the location where the file containing the license code is saved.

**5. Open the folder whose location is indicated in the completion message of the uninstallation process. Copy the file in which the license code is recorded to another computer.**

**6. Access the license management Web site of RICOH (<https://licensemanagement.ricoh.com/au/>).**

**7. Click [Deactivation].**

**8. Open the file that have been copied in Step 5, copy the license code in the file. On the web site, paste the license code in the text box, and click [Next].**

**9. Follow the instructions that are displayed on the screen and continue the deactivation process.**

# Performing a System Backup/Restore

System backup and restore are explained below.

**Note**

- Backup and restore are not recorded in the system log.

---

## Backing up the System

---

The backup file contains the following information:

- Device list and group settings
- Search/monitor conditions settings
- Device information retrieval timing settings
- Device access account information
- Device log information
- User data
- The password that is required to start Device Manager NX
- Proxy server settings
- Error notification settings
- Report data \*

\* This information is included in the backup only when using Device Manager NX Accounting.

**Important**

- **Quit Device Manager NX before execution of backup.**
  - **If Device Manager NX is used as a service, stop the service before executing the backup. For information on stopping services, see page 230 "Batch File for Stopping the Service".**
- 1. From the [Start] menu, select [All Programs], [Device Manager NX XXX], and then click [Backup].**  
"XXX" varies depending on Device Manager NX to use.
  - 2. Click [Browse].**
  - 3. Specify the destination folder and click [OK].**
  - 4. Click [OK].**

Backup is performed.

---

## Restoring the System

---

Restore the system using the backup file

 **Important**

- Quit Device Manager NX before restoring the system.
- If Device Manager NX is used as a service, stop the service before restoring the system. For information on stopping services, see page 230 "Batch File for Stopping the Service".
- "Restore" can be used when the system has a problem. Use this function only when required.
- When a restore sequence is applied, the current data is overwritten by the backup data. All data and settings that were added and changed after the system was backed up are deleted.

1. From the [Start] menu, select [All Programs], [Device Manager NX XXX], and then click [Restore].

"XXX" varies depending on Device Manager NX to use.

2. Click [Browse].
3. Specify the folder that contains the backup files you want to restore, and then click [OK].
4. Click [OK].

"Restore" is performed.

## System initialization

---

To initialize Device Manager NX, the backup file created immediately after its installation is required. When Device Manager NX is installed, back up the system immediately, so that system initialization can be performed.



# 7. Device Manager NX Setting Items

This chapter explains the detailed functions and operations of each configuration item of Device Manager NX.

## Configuration Item List

To change settings for device management or Device Manager NX operations, select an item in the section area on the left side of the screen and display the settings screen.

Refer to the table below, and check the items displayed in each section and the functional outlines and operations of each of the displayed items.

### [Device List] section

Tab name	Item name	Reference
Groups	Host Name	page 25 "Classifying Devices by Group Name"
	IP Address	
	Models	
Filters	-	

For explanations about each configuration item displayed on the screen, see page 103 "Device List".

### [Device Access Settings] section

Tree name	Item name	Reference
Discovery	Network Search	page 22 "Searching for Devices"
	Broadcast	
Polling	-	page 31 "Retrieving the Device Status"
Access Account Settings	Web Service Account Setting	page 19 "Configuring Access Accounts"
	SNMP Account Setting	
	SDK Account Setting	

For details about each setting item displayed on the screen, see page 106 "Device Access Settings".

**[Configuration] section**

Tree name	Item name	Reference
Device Preference	Template	page 51 "Applying Same Settings to Multiple Devices"
	Tasks	page 64 "Registering Created Templates to Tasks"
Software	Template	page 61 "Managing SDK Applications and the SDK/J Platform"
	Tasks	page 64 "Registering Created Templates to Tasks"
Address Book	Template	page 55 "Managing the User Data"
	Tasks	page 64 "Registering Created Templates to Tasks"
Power Mode	Tasks	page 54 "Applying Energy Saver Mode to Multiple Devices at One Time" page 64 "Registering Created Templates to Tasks"

For details about each configuration item displayed on the screen, see page 115 "Configuration".

**[Tasks] section**

Tree name	Reference
Scheduled Tasks	page 69 "Managing Tasks"
Task Logs	page 70 "Checking Task Logs"

For details about each configuration item displayed on the screen, see page 134 "Tasks".

**[System] section**

Tree name	Item name	Reference
System Settings	Activation/Deactivation/ Usage Report Notification	page 91 "Activating Device Manager NX"
	Custom Properties	page 40 "Setting custom properties"
	Display Settings	Date format can be specified.
	Proxy Server	The proxy server can be specified.
	System Data Settings	You can configure settings for data management and storage.
	System Information and Settings	You can check the system version of the product. You can also enable or disable SDK/J Platform.
Authentication and Accounts	Change Password	page 153 "Setting a Password"

For details about each configuration item displayed on the screen, see page 135 "System".

Device Manager NX, [Status Notification], [Task Notification] cannot be used.

**[Notification Policy] section**

Tree name		Reference
Status Notification	Notification Policy	page 43 "Message Notification with Set Conditions"
	Logs	
Task Notification *1	Non-executed Task Notification Settings	page 72 "Notifying/Confirming Overdue Tasks"
	Non-executed Task List	

For details about each setting item displayed on the screen, see page 143 "Notification Policy".

\*1 These are setting items that are displayed in Device Manager NX Accounting.

**[Logs] section**

Tree name	Reference
System Log	page 73 "Checking System Operation Logs"

For details about each configuration item displayed on the screen, see page 147 "Logs".

**[Device Log Management] section**

Tree name	Item name	Reference
Device Log Collection	Device Log Settings	page 46 "Managing Device Logs"
	Device Log Collection	
Device Log Management	Device Log Export	

For details about each configuration item displayed on the screen, see page 148 "Device Log Management".



# Device List

A list of the devices that can be managed by this product is displayed in the [Device List] section. Two tabs are used to classify the Device List.

For the functional outlines or operations of these configuration items, see page 25 "Classifying Devices by Group Name".

## [Groups] Tab

Groups that are automatically classified by the system and groups that are created manually are displayed on the [Groups] tab.

### Groups that are automatically classified by the system

The devices searched for by three types of groups indicated below are classified automatically.

#### Host Name

A tree view is used to display host names that are separated by domain hierarchies. Whether a domain hierarchy is an actual domain or not, domain hierarchies are separated by dots.

#### IP Address

A tree view is used to display IPv4 addresses that are separated every 8 bits.

#### Models

Names of device manufacturers or models are used for classification.

### Groups that are created manually

Group addition/deletion, name change and import/export can be performed from the right-click menu.

#### Right-click menu items

Menu item	Description
Refresh	Updates the displayed information.
Add Category/Add Group	To add a group to the root hierarchy, create a category group in [Add Category]. To add a group to a lower layer of a category group, create a group in [Add Group]. Enter the name of the group. Use 1 to 128 characters.
Rename	Changes the name of the selected group.
Delete	Deletes the selected group. Any devices that are registered in the deleted group will be transferred to the unmanaged group.

Menu item	Description
Display Hidden Devices	The devices that are hidden in the device list are displayed on the [Hidden Devices] tab.
Import	A group you want to import can be specified by uploading an import file to the system. If there is a group in the system and its internal ID is identical to the internal ID of the group you want to import, the group in the system will be overwritten. All groups are imported when the [Import All Groups] check box is selected.  To display the groups that have been imported, click [Refresh] to update the information.
Export	Exports the group structure, group name, and internal ID of the selected group. All groups are exported when the [Export All Groups] check box is selected.
Notification Options	"Notification Policy" is applied to the devices that belong to the selected group. This item cannot be specified for a category group.

**Note**

- For the functional outlines or operations of these configuration items, see page 25 "Classifying Devices by Group Name".

**[Filters] Tab**

Filter groups are displayed. The devices of the filter groups are narrowed using user-defined conditions. Use the right-click menu to add/delete groups, change names, and import/export groups.

**Right-click menu items**

Menu item	Description
Refresh	Updates the displayed information.
Add Filter	Adds a filter group with specified device filtering conditions.
Edit Filter	Changes the filtering conditions for the selected filter group.
Rename	Changes the name of the selected filter group.
Delete Filter	Deletes the selected filter group.

**Note**

- For the functional outlines or operations of these configuration items, see page 26 "Creating a Filter Group".

# Device Access Settings

Referring to the [Device Access Settings] section enables you to configure settings to access devices using the discovery and polling functions.

## Discovery

Discovery includes [Network Search] and [Broadcast].

### Network Search

Discovery tasks implemented by network search are displayed in a list.

A Network Search task is configured on the [General], [Access Account Settings], [Discovery Range (Network Search)], and [Schedule] tabs.

#### [General] tab

Set the task name.

Item name	Description
Name	Enter a name. Use 1 to 255 characters.
Description	Enter a description. Use 0 to 511 characters.

#### [Access Account Settings] tab

Set an account used for access to devices at the time of discovery. Change the account to be used from the Unassigned Account list to the Assigned Account list by clicking the [▲] button or by dragging and dropping.

Accounts are displayed by a tab for each type.

Tab name	Description
Web Service Account Setting	An access account used for the Web service protocol is displayed.
SNMP Account Setting	An access account used for SNMP is displayed.
SDK Account Setting	The access account for remote connection to SDK Platform is displayed.

#### [Discovery Range (Network Search)] tab

Set the target range of discovery by network search.

Item name	Description
Include/Exclude	Specify whether to include or exclude a specified range in the network search.
Range Type	Select [One Host Name], [One IP Address] or [Specify IP Range] as a type of the value to be specified.
Host Name	Enter a host name.
From	Specify the discovery target IP address or start IP address of the discovery target IP address range.
To	Enter the end IP address of the discovery target IP address range.
Subnet Mask	Enter the subnet mask in the IP address range specified by [From] and [To].

### [Schedule] tab

Configure a schedule to implement discovery tasks.

Item name	Description
Once Only	Executed only once at the specified date/time.
Interval	Network search begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify an interval from 1 minute to 7 days. Select whether the interval measurement is started at the start or end of the job.
Daily	Network search 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 select multiple days of the week from Monday to Sunday.
Monthly	Network search begins at the specified date/time, and it is executed monthly at the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

**Note**

- For the functional outlines or operations of these configuration items, see page 22 "Searching for Devices".

**Broadcast**

Tasks of discovery by broadcast appear in a list.

Broadcast tasks can be configured using the [General], [Access Account Settings], [Discovery Range (Broadcast)], and [Schedule] tabs.

**[General] tab**

Set a task name.

Item name	Description
Name	Enter a name. Use 1 to 255 characters.
Description	Enter a description. Use 0 to 511 characters.

**[Access Account Settings] tab**

Set an account used for access to devices at the time of discovery. Change the account to be used from the Unassigned Account list to the Assigned Account list by clicking the [▲] button or by dragging and dropping.

Accounts are displayed by a tab for each type.

Tab name	Description
Web Service Account Setting	An access account used for the Web service protocol is displayed.
SNMP Account Setting	An access account used for SNMP is displayed.
SDK Account Setting	The access account for remote connection to SDK Platform is displayed.

**[Discovery Range (Broadcast)] tab**

Set the target range of discovery by broadcast.

Item name	Description
Type	<ul style="list-style-type: none"> <li>Local Segment Only local segments are specified as the broadcast target.</li> <li>Subnet A subnet address for broadcast can be specified. If a subnet is selected, the discovery settings by broadcast will be displayed in the list.</li> </ul>
Subnet	Enter the subnet address of the broadcast. An IPv4 address can be specified.
Subnet Mask	Enter the subnet mask of the broadcast. An IPv4 address can be specified.

### [Schedule] tab

Configure a schedule for implementing discovery tasks.

Item name	Description
Once Only	Executed only once at the specified date/time.
Interval	Broadcast begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify an interval from 1 minute to 7 days. Select whether the interval measurement is started at the start or end of the print job.
Daily	Broadcast begins on the specified date, and it is executed daily at the specified time.
Weekly	Broadcast begins at the specified date/time, and it is executed weekly on the specified day of the week. You can select multiple days of the week from Monday to Sunday.
Monthly	Broadcast begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

**Note**

- For the functional outlines or operations of these configuration items, see page 22 "Searching for Devices".

**Polling**

Polling tasks are displayed in a list. A polling task is configured using the [General] and [Target Devices/Groups] tabs and also the polling type tabs.

**[General] tab**

Set a task name.

Item name	Description
Profile Name	Enter a name. Use 1 to 255 characters.
Profile Description	Enter a description. Use 0 to 511 characters.

**[Target Devices/Groups] tab**

Polling target devices are displayed in a list. The target devices can be added in device units or group units.

**[Status Polling] tab**

Specify a polling type and when to perform polling tasks. Tabs are used to classify polling types.

Item name	Description
Once Only	Executed only once at the specified date/time.
Interval	Polling begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify an interval from 1 minute to 7 days. Specify whether the interval measurement is started at the start or end of the job.
Daily	Polling begins on the specified date, and it is executed daily at the specified time.
Weekly	Polling begins at the specified date/time, and it is executed weekly on the specified day of the week. You can select multiple days of the week from Monday to Sunday.
Monthly	Polling begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.



Item name	Description
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

### [Supplies Polling] tab

Set the schedule for Supplies Polling. The setting items are the same as those of Status Polling.

### [Counter Polling] tab

Set the schedule for Counter Polling. The setting items are the same as those of Status Polling.

### [Other Polling] tab

Set the schedule for Other Polling. The setting items are the same as those of Status Polling.

### [User Counter Polling] tab

Set the schedule for User Counter Polling. The setting items are the same as those of Status Polling.

#### ↓ Note

- For the functional outlines or operations of these configuration items, see page 31 "Retrieving the Device Status".

## Access Account Settings

A list of the registered access accounts is displayed. An access account can be configured for [Web Service Account Setting], [SNMP Account Setting], and [SDK Account Setting].

#### ★ 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 specified on the device.**

### Web Service Account Setting

Configure an access account that can be used for the Web service protocol.

The registered access accounts are displayed in a list. Each account is configured with the following settings:

Item name	Description
Profile Name	Enter a profile name. Use 1 to 255 characters.

Item name	Description
Profile Description	Enter a profile description. Use 0 to 511 characters.
User Name	Enter a user name of up to 32 bytes. You cannot use ;, ", or a space.
Password	Enter a password of up to 32 bytes. You cannot use ;, ", or a space.
SSL Connection	<ul style="list-style-type: none"> <li>Off Communication with devices is in cleartext. However, when [Permit SSL/TSL Communication] is set to [Ciphertext/Cleartext] on the device and a certificate is installed on it, the communication method changes from cleartext to ciphertext.</li> <li>On Communication with devices is in ciphertext, regardless of whether [Permit SSL/TSL Communication] is set to [Ciphertext/Cleartext], [Ciphertext Priority] or [Ciphertext Only] on the device. Communication is not possible with devices that have no certificate installed.</li> </ul>

**Note**

- "default" is registered as a default account in the system.
- The authentication information of the Web service account must have all administrative privileges (Device Administrator, User Administrator, File Administrator, and Network Administrator).
- For the functional outlines or operations of these configuration items, see page 19 "Configuring Access Accounts".

**SNMP Account Setting**

Specify an access account that can be used for SNMP.

Registered access accounts are displayed in a list. Each account is configured with the following settings:

Item name	Description
Profile Name	Enter a profile name. Use 1 to 255 characters.
Profile Description	Enter a profile description. Use 0 to 511 characters.

Item name	Description
Retry	Specify how many retry attempts can be performed if a device does not respond during discovery. Select from 0 to 5 attempts. The default is 2 attempts.
Timeout (millisecs.)	Specify how long the waiting period can be if a device does not respond during discovery. Any value between 500 and 60000 milliseconds can be specified. The default is 2000 milliseconds.
Version	Select either [SNMP v1/v2] or [SNMP v3] as the protocol type. Configuration items vary depending on protocol types.
Read Community Name	Specify a read community name of up to 15 bytes. (SNMPv1/v2)
Write Community Name	Specify a write community name of up to 15 bytes. (SNMPv1/v2)
User Name	Enter a user name of up to 32 bytes. (SNMPv3)
Password	Enter a password of up to 32 bytes. (SNMPv3)
Authentication Algorithm	Select [MD5] or [SHA1] as the authentication algorithm. (SNMPv3)
Context Name	Enter a context name. Use 0 to 256 characters. (SNMPv3)
Encrypted Password	Enter an encryption password. Use 0 to 32 characters. (SNMPv3)
Encryption Algorithm	Select [DES] or [AES128] as the encryption algorithm. (SNMPv3)

#### Note

- "default" is registered as a default account in the system.
- For the functional outlines or operations of these configuration items, see page 19 "Configuring Access Accounts".

## SDK Account Setting

Configure an access account that can be used for the SDK/J Platform protocol.

The registered access accounts are displayed in a list. Each account is configured with the following settings:

Item name	Description
Profile Name	Enter a profile name. Use 1 to 255 characters.
Profile Description	Enter a profile description. Use 0 to 511 characters.
Password	This item cannot be specified.

**Note**

- "default" is registered as a default account in the system.
- For the functional outlines or operations of these configuration items, see page 19 "Configuring Access Accounts".

# Configuration

In the [Configuration] section, you can configure settings for changing device settings using this product.

## Device Preference

You can create a template to change the device settings and register the created template to a task.

### Template - Basic Device Preferences

The templates of the Basic Device Preferences are displayed in a list.

When creating a new template, specify the method for creating the template.

#### Configuration items when creating a template

Configuration items	Descriptions
Create Blank Template	Create a template without specifying any configuration values.
Get Data from Device	Retrieve configuration values from devices and create a template. You can edit the retrieved data. You cannot retrieve encrypted information such as passwords and security settings.
Import CSV File	Import setting values from an external file and create a template. You can edit the retrieved data.

The templates added to the list are configured using the [General] and [Basic Device Preferences] tabs.

#### [General] tab

Set a template name.

Item name	Description
Template Name	Enter a template name. Use 1 to 255 characters.
Description	Enter a template description. Use 0 to 511 characters.

#### [Basic Device Preferences] tab

The device configuration items that can be edited are displayed in a tree view.

For details about the configuration items, see page 157 "List of Device Preference Setting Items".

**Note**

- For the functional outlines or operations of these setting items, see page 51 "Applying Same Settings to Multiple Devices".

**Template - Advanced Device Preferences**

The templates of the Advanced Device Preferences are displayed in a list.

When creating a new template, specify the method for creating the template.

**Configuration items when creating a template**

Configuration item	Description
Template Name	Enter a template name. Use 1 to 255 characters.
Description	Enter a template description. Use 0 to 511 characters.
Backup from Devices	<p>Create a template with settings retrieved from a device.</p> <ul style="list-style-type: none"> <li>• [Select Device] Select the device to retrieve settings.</li> <li>• Password Enter a password at the time of retrieval of information such as passwords and security settings.</li> <li>• Logo Image Select this item for retrieval of a logo file.</li> </ul>
Import Backup File	<p>Create a template with settings imported from an external file.</p> <ul style="list-style-type: none"> <li>• Password Enter a password at the time of retrieval of information such as passwords and security settings.</li> <li>• File Specify the path of the file to be imported.</li> <li>• Logo Image Specify the path of the logo file to be imported.</li> </ul>

A template that was added to the list is configured with the settings shown below.

Item name	Descriptions
Template	Enter a template name. Use 1 to 255 characters.

Item name	Descriptions
Description	Enter a template description. Use 0 to 511 characters.

**Note**

- For the functional outlines or operations of these setting items, see page 51 "Applying Same Settings to Multiple Devices".

**Tasks**

The tasks of the Device Preferences are displayed in a list.

A Device Preferences task is configured using the [General], [Target Devices/Groups], and [Schedule] tabs.

**[General] tab**

Set the general information of a task.

Item name	Description
Name	Enter the task name. Use 1 to 255 characters.
Description	Enter the task description. Use 0 to 511 characters.
Template	Select a template to be registered to the task.
Type	Select [Check], [Apply], or [Check & Apply] for the task type. This setting can be specified in the template under Basic Device Preferences.

**[Target Devices/Groups] tab**

The target devices of the task are displayed in a list. The target devices can be added in device units or group units.

**[Schedule] tab**

Set the task execution 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 an interval from 1 minute to 7 days. Specify whether the interval measurement is started at the start or end of the print job.

Item name	Description
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 select multiple days of the week from Monday to Sunday.
Monthly	The task begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

**Note**

- For the functional outlines or operations of these configuration items, see page 64 "Registering Created Templates to Tasks".

**Software**

You can create a template to manage device software and register the created template to a task.

**Template (SDK/J Platform Update - RICOH Software Server)**

The templates for updating SDK/J Platform are displayed in a list.

You do not have to create and edit a template.

Use of this template retrieves the latest version of the SDK/J platform from the RICOH Software Server and updates the SDK/J platform of the target device.

**Note**

- For the functional outlines or operations of these setting items, see page 61 "Managing SDK Applications and the SDK/J Platform".

**Template (SDK Application - RICOH Software Server)**

The templates for setting SDK applications in conjunction with the RICOH Software Server are displayed in a list.

This Template is configured using the [General] and [Application List] tabs.



**[General] tab**

Set general information of Template.

Configuration item	Description
Template Name	Enter a template name. Use 1 to 255 characters.
Description	Enter a template description. Use 0 to 511 characters.
Action	<p>Set actions of the template.</p> <ul style="list-style-type: none"> <li>• [Install] Install an SDK application to the device.</li> <li>• [Update] Update the SDK application installed in the device.</li> <li>• [Uninstall] Uninstall the SDK application installed in the device.</li> <li>• [Activate] Activate the SDK application installed in the device.</li> </ul>
Product Key	Enter a product key to be sent to the RICOH Software Server.
Retrieve Application List	A list of SDK applications is retrieved from the RICOH Software Server and is displayed on the [Application List] tab.

**[Application List] tab**

The SDK applications to be set using a template are displayed in a list.

To specify the SDK application to be set, move the SDK application from the Selectable Application List to the Selected list.

**Note**

- For the functional outlines or operations of these setting items, see page 61 "Managing SDK Applications and the SDK/J Platform".

**Tasks**

The tasks of the Software are displayed in a list.

Software tasks are configured using the [General], [Target Devices/Groups], and [Schedule] tabs.

**[General] tab**

Set the general information of a task.

Item name	Description
Name	Enter the task name. Use 1 to 255 characters.
Description	Enter the task description. Use 0 to 511 characters.
Template	Select the template to be registered to the task.
Type	Select [Check] or [Check & Apply] for the task type.

**[Target Devices/Groups] tab**

The target devices of a task are displayed in a list. The target devices can be added in device units or group units.

You can check the number of remaining licenses when a template using the RICOH Software Server is selected.

**[Schedule] tab**

Set the task execution 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 an interval from 1 minute to 7 days. Specify whether the interval measurement is started 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 select multiple days of the week from Monday to Sunday.
Monthly	The task begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

**Note**

- For the functional outlines or operations of these setting items, see page 64 "Registering Created Templates to Tasks".

## Address Book

You can create a template to set the device address book and register the created template to a task.

### Template

The templates of the address book are displayed in a list.

When creating a new template, specify the method for creating the template.

#### Configuration items when creating a template

Configuration item	Description
Template Name	Enter a template name. Use 1 to 255 characters.
Description	Enter a template description. Use 0 to 511 characters.
Get Data from Device	Retrieve the settings from the device specified by [Select Device].
Backup from Devices	Retrieve the backup data from the device specified by [Select Device]. Enter a password to protect the data.
Import CSV File	Specify the file path, and import a CSV file.
Import CSV File (SmartDeviceMonitor for Admin)	Specify the file path, and import the CSV file to be used by SmartDeviceMonitor for Admin. The CSV of the Address Management Tool and User Management Tool can be imported.
Import Backup File	Specify the file path, and import the backup data. Enter the password that was specified when creating the backup file.

Configuration item	Description
Create Blank Template	<p>Create a template with blank settings. Select one of the following authentication methods:</p> <ul style="list-style-type: none"> <li>• User Code / None Select this when using user code authentication or not using user authentication.</li> <li>• Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server Select this item for Basic Authentication, Windows Authentication, LDAP Authentication, or Integration Server.</li> </ul>

The templates added to the list are configured using the [General], [Preference Settings], and [Entry List] tabs.

**[General] tab**

Set a template name.

Item name	Description
Template Name	Enter a template name. Use 1 to 255 characters.
Description	Enter a template description. Use 0 to 511 characters.

**[Preference Settings] tab**

Set the general information of the template.

Item name	Description
Counter Collection per User	<p>Before applying the template contents, such as batch entry delete, specify whether or not to collect user counters registered to the device.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Collection of per user counters cannot be used in Device Manager NX Accounting.</li> </ul>
Reset Counter per User	The volume use of all users registered to the device is reset.

Item name	Description
Delete Entry	<p>Specify whether or not to batch delete entries.</p> <ul style="list-style-type: none"> <li>All All entries of type are deleted.</li> <li>User Settings If the [Specify Batch Deletion of User Entries] check box is selected, all "User" entries whose login name or user code are 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 are not specified will be deleted. If the [Specify Batch Deletion of Group Entries] check box is selected, all "Groups" entries are deleted.</li> <li>Disable Batch deletion of entries is disabled.</li> </ul>
Check & Apply Entry List	<p>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 only addition or update of the entries that are present in the template is executed.</p>

#### ↓ Note

- In Device Manager NX Accounting, [Counter Collection per User] cannot be used.
- When you created the template files of an address book from the back up files, you can not set [Counter Collection per User], [Reset Counter per User], and [Delete Entry] option.
- The [CheckAction] Task will be run with [Counter Collection per User], [Reset Counter per User], and [Delete Entry] options, following message will be written in the Task Log. "Skipped because of check action."(30)"

#### [Entry List] tab

Edit settings for a user or a group. You can add or delete user or group entries. An entry is configured using the tabs shown below.

#### ↓ Note

- The displayed tabs are different when the entry is a user and when the entry is a group.
- The functions and items that are not supported by the device cannot be set.

**[General] tab**

This tab is displayed for user and group entries.

Select the [Set] check box to change the settings.

Item name	Description
User Name Group Name	Enter a name.
Specify Registration No.	Specify whether or not to specify a desired registration number manually or acquire the number from devices automatically. To specify a number, select this check box.
Registration No.	Enter this item to specify a desired registration number. You can specify a value between 1 and 50,000.
Key Display Name	Enter a name that is displayed on the display panel of the device. This name will not be displayed if the device does not support this function.
Display Priority	Specify the display priority on the control panel of the machine. You can specify a value between 1 and 10.

7

**[Title] tab**

This tab is displayed for user and group entries.

Select the [Set] check box to change the settings.

Item name	Description
Title 1-3	Select from Title 1 to 3 for the registered title. Title 1 to 3 may be required depending on target device.
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 [User Code / None] in [Authentication Method] was selected when the template was created.

Select the [Set] check box to change the settings.

Item name	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 settings.

Item name	Description
Authentication	<p>Enter a login user name and password. You cannot use ; , " , or a space in the login user name.</p> <p>This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</p>
SMTP Authentication	<ul style="list-style-type: none"> <li>• Do not Specify SMTP authentication is not specified.</li> <li>• Use Login Auth. Info SMTP authentication is performed using the login user name and password specified in [Authentication]. This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</li> <li>• Specify Other Auth. Info SMTP authentication is performed using the authentication information that is different from the login user name and password specified in [Authentication]. Enter a login user name and password to be used for SMTP authentication.</li> </ul>
Folder Authentication	<ul style="list-style-type: none"> <li>• Do not Specify Folder authentication is not specified.</li> <li>• Use Login Auth. Info Folder authentication is performed using the login user name and password specified in [Authentication]. This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</li> <li>• Specify Other Auth. Info Folder authentication is performed using the authentication information that is different from the login user name and password set in [Authentication]. Enter a login user name and password to be used for folder authentication.</li> </ul>

Item name	Description
LDAP Authentication	<ul style="list-style-type: none"> <li>• Do not Specify LDAP authentication is not specified.</li> <li>• Use Login Auth. Info LDAP authentication is performed using the login user name and password set in [Authentication].  This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</li> <li>• Specify Other Auth. Info LDAP authentication is performed using the authentication information that is different from the login user name and password specified in [Authentication]. Enter a login user name and password to be used for LDAP authentication.</li> </ul>

**[Available Functions] tab**

This tab is displayed for a user entry.

Select the [Set] check box to change the settings.

7

Item name	Description
Copier	<p>Set the classification of colors that are available for the copier function.</p> <ul style="list-style-type: none"> <li>• Disable All enabled items are disabled.</li> <li>• Black &amp; White Monochrome copying is enabled.</li> <li>• Single Color Monochrome copying and single color copying are enabled.</li> <li>• Two-color Monochrome copying, single color copying, and twin color copying are enabled.</li> <li>• Auto Color Auto color copying is enabled.</li> <li>• Full Color Full color copying is enabled.</li> </ul>



Item name	Description
Limit Value for Print Volume Use Limitation	Enter the limit of the printing volume. You can specify a value from 0 to 999999.
Printer	Specify colors that are available for the printer function. <ul style="list-style-type: none"> <li>• Disable All enabled items are disabled.</li> <li>• Black &amp; White Monochrome printing is enabled.</li> <li>• Color Monochrome printing and color printing are enabled.</li> </ul>
Other Functions	<ul style="list-style-type: none"> <li>• Scanner Select the check box of this setting item to enable the Scanner function.</li> <li>• Fax Select the check box of this setting item to enable the Fax function.</li> <li>• Document Server Select the check box of this setting item to enable the Document Server function.</li> </ul>

**[Email/Fax] tab**

This tab is displayed for a user entry.

Select the [Set] check box to change the settings.

Item name	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 feature. You cannot specify an advanced feature if the target device does not support it.
Select line type.	Set the line type to be used.
International Transmission Mode	Select the check box for this item to enable international transmission mode.

Item name	Description
Address	Enter the e-mail address of the user.
Use This Email Address for Email and Internet Fax	Select this item if you use this e-mail address for e-mail and internet fax.
Use This Email Address for Internet Fax	Select this item if you use this e-mail address for internet fax.
Internet Fax - via SMTP Server	Select the check box of this item to send an internet fax through the SMTP server.
Fax Header	Select an originator name.
Label Insertion	Select the check box of this item to use the setting label insertion function.
1st Line	The name used for label insertion is displayed.
Label Insertion 2nd Line (String)	Set the string of the second line fitted in label insertion. A custom message can be specified.
Label Insertion 3rd Line (Standard Message)	Specify the message of the third line used for label insertion. A fixed phrase can be specified.

**[Folder] tab**

This tab is displayed for a user entry.

Select the [Set] check box to change the settings.

Item name	Description
Protocol	Select the protocol to be used. <ul style="list-style-type: none"> <li>• SMB</li> <li>• FTP</li> <li>• NCP-NDS</li> <li>• NCP-Bindery</li> </ul>
Port Number	When the protocol is FTP, enter a port number.
Server Address	When the protocol is FTP, enter a server name.
Path	Enter a path.

**[Protection] tab**

This tab is displayed for a user entry and a group entry.

Select the [Set] check box to change the settings.

Item name	Description
Register as Destination	Select the check box of this item to use an entry as a destination.
Protect Dest.	Select the check box of this item to protect folder destinations. You cannot configure this setting unless the Register as Destination check box is selected.
Access Control List for Destination Protection Settings	<p>The names and authority statuses of the entries to which destination protection is specified are displayed in a list. To set destination protection, select the target entry from the pull-down menu, and select and add an access right from the following.</p> <ul style="list-style-type: none"><li>• read-only</li><li>• read-write</li><li>• Delete</li><li>• Full Control</li></ul> <p>This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</p>
Register as Sender	Select the check box of this item to use entries as destinations. This item will not be displayed if the target device does not support this function.
Protect Sender	Select the check box of this item to protect the sender. You cannot configure this item unless the Register as Sender check box is selected.
Protection Code	Enter a protection code. When you specify an entry, "*" appears 15 times regardless of how many characters are used for a protection code.

Item name	Description
Access Control List for Document Protection Settings	<p>The names and authority statuses of the entries to which destination protection is specified are displayed in a list. To set destination protection, select the target entry from the pull-down menu, and then select and add an access right from the following:</p> <ul style="list-style-type: none"> <li>• read-only</li> <li>• read-write</li> <li>• Delete</li> <li>• Full Control</li> </ul> <p>This setting item appears when the Authentication Method in the template is set to [Basic Authentication, Windows Authentication, LDAP Authentication, Integration Server].</p>

**[Group List] tab**

This tab is displayed for user and group entries.

Select the [Set] check box to change the settings.

Item name	Description
Selected Groups	The groups to which the entry is registered are displayed in a list. If you do not want to set the entry as the target of this template, move the entry to "Unselected Groups" by dragging and dropping or by using the up arrow button.
Unselected Groups	The group to which the entry is registered are displayed in a list. If you want to set the entry as the target of this template, move the entry to "Selected Groups" by dragging and dropping or by using the down arrow button.

**[Users and Groups] tab**

This tab is displayed for a group entry.

Item name	Description
User	Users registered to this entry are displayed in a list.
Group	Groups registered to this entry are displayed in a list.

**[Reset Counter per User] tab**

This tab is displayed for a user entry.

Select the [Set] check box to change the settings.

Item name	Description
Print (Copier, Fax Print, Printer)	The print counter is reset.
Fax Transmission	The fax send counter is reset.
Scanner	The scanner counter is reset.
Volume Used	The user quota counter is reset.

**Note**

- For the functional outlines or operations of these setting items, see page 55 "Managing the User Data".

**Tasks**

The tasks of the Address Book are displayed in a list.

An Address Book task is configured using the [General], [Target Devices/Groups], and [Schedule] tabs.

**[General] tab**

Set the general information of a task.

Item name	Description
Name	Enter the task name. Use 1 to 255 characters.
Description	Enter the task description. Use 0 to 511 characters.
Template	Select a template to be registered to the task.
Type	Select [Check], [Apply], or [Check & Apply] for the task type.

**[Target Devices/Groups] tab**

The target devices of a task are displayed in a list. The target devices can be added in device units or group units.

**[Schedule] tab**

Set the task execution schedule.

Item name	Description
Once Only	Executed only once at the specified date/time.

Item name	Description
Interval	The task begins at the specified date/time, and it is repeatedly executed at a specified interval. Specify an interval from 1 minute to 7 days. Specify whether the interval measurement is started 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 select multiple days of the week from Monday to Sunday.
Monthly	The task begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st day to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

7

**Note**

- For the functional outlines or operations of these setting items, see page 55 "Managing the User Data".

## Power Mode

You can create tasks to change the power status of the device.

### Tasks

The tasks of the Power Mode are displayed in a list.

A Power Mode task is configured using the [General], [Target Devices/Groups], and [Schedule] tabs.

#### [General] tab

Set the general information of a task.

Item name	Description
Name	Enter the task name. Use 1 to 255 characters.

Item name	Description
Description	Enter the task description. Use 0 to 511 characters.
Task Type	<ul style="list-style-type: none"> <li>Energy Saver Mode The target device enters energy saver mode.</li> <li>Cancel Energy Saver Mode The target device exits energy saver mode.</li> </ul>

**[Target Devices/Groups] tab**

The target devices of a task are displayed in a list. The target devices can be added in device units or group units.

**[Schedule] tab**

Set the task execution 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 an interval from 1 minute to 7 days. Specify whether the interval measurement is started 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 select multiple days of the week from Monday to Sunday.
Monthly	The task begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

**Note**

- For the functional outlines or operations of these configuration items, see page 54 "Applying Energy Saver Mode to Multiple Devices at One Time".

## Tasks

In the [Tasks] section, the progress and results of all of registered tasks such as discovery and polling can be checked.

---

### Scheduled Tasks

---

The tasks in the scheduled status are displayed in a list.

The following task type items will be displayed:

- Discovery
- Polling
- Basic Device Preferences
- Advanced Device Preferences
- Software Management
- Address Book
- Power Mode

#### Note

- For the functional outlines or operations of these configuration items, see page 69 "Managing a Task in the Schedule Standby Status".

---

### Task Logs

---

Task logs are displayed in a list.

When a log is selected, details of the tasks can be checked on the [Result Details] tab.

#### Note

- For the functional outlines or operations of these configuration items, see page 70 "Checking Task Logs".



# System

In the [System] section, you can configure settings for the operation of this product and check task statuses and logs.

## System Settings

You can specify the date format for the date displayed on this product, proxy server, data storage period.

## Activation/Deactivation/Usage Report Notification

### Country Information

Item	Description
Country Information	Specify the country information of the system. The country information specified at the time of installation is registered as default.

### Activation

Item	Description
Activation Type	Select either [Online] or [Offline] as the activation type.
Product Key	Enter a product key for online activation.
License Code	Enter a license code for offline activation.
Activate	The product is activated. This item cannot be performed if no devices are registered to the device list in the [Device List] section.

### Note

- For the functional outlines or operations of these setting items, see page 91 "Activating Device Manager NX".

### Deactivation

Item	Description
Deactivate	The product is deactivated.

**Note**

- For the functional outlines or operations of these setting items, see page 91 "Activating Device Manager NX".

**Usage Report Notification**

Item	Description
Usage Report Notification	<p>Specify whether or not to send notification of the usage status of this product to RICOH.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The usage status is sent anonymously to make use of the information for development of better products. Personal information is not included.</li> </ul>

**Software Update Notification**

Item	Description
Software Update Notification	Specify whether or not to receive a notification of the update information about this product. Update information is received only once a week, and a notification will be displayed if an update is available. You can receive notifications only when this product is activated.
Run Immediately	Check the update information on this product.

**Custom Properties**

Item	Description
Custom Property 1 - 5	Set the item names of custom properties.

**Note**

- For the functional outlines or operations of these setting items, see page 40 "Setting custom properties".

## Display Settings

### Display Settings

Item	Description
Date Display Format	<p>Select from the following date display formats:</p> <ul style="list-style-type: none"> <li>• YYYY/MM/DD</li> <li>• MM/DD/YYYY</li> <li>• DD/MM/YYYY</li> </ul> <p>The default is MM/DD/YYYY.</p>
First Day of Week *	You can select the day to start a week in the calendar that is displayed in the date display settings.

\* This item can be used in Device Manager NX Accounting.

## Proxy Server

### Proxy Server

Item	Description
Use Proxy Server	Specify whether or not to use a proxy server.
Proxy Server Address	Enter the IP address of the proxy server.
Proxy Server Port Number	Enter the port number of the proxy server.
Use Authentication	Specify whether or not to apply user authentication to the proxy server.
User Name	Enter the user name to use for authentication of the proxy server. This item is enabled only when [Use Authentication] is [On].
Password	Enter the password to use for authentication of the proxy server. This item is enabled only when [Use Authentication] is [On].
Domain Name	Enter the domain name you want to use for NTLM authentication of the proxy server. This item is enabled only when [Use Authentication] is [On].
Check Connection	Perform a connection test using the proxy server.

## System Data Settings

### System Data Settings

Item	Description
Status	Specify the storage period of the status history retrieved from devices. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 1 day(s).
Counter	Specify the storage period of the counter information retrieved from devices. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 3 month(s).
User Counter	Specify the storage period of the user counter information retrieved from devices. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 3 month(s).
System/Tasks/Notifications Logs System/Tasks/Notifications/Report Logs *	Specify the storage period of the system logs. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 3 month(s).

Item	Description
Report *	Specify the storage period of the generated reports. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 1 year(s).
Device Job Log *	Specify the storage period of the job log that is retrieved from devices. Specify one of the following: <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Unlimited</li> </ul> The default is 3 month(s).

\* This item can be used in Device Manager NX Accounting.

#### ↓ Note

- The default value for each of the items other than "Status" and "Device Job Log" in Device Manager NX Accounting is "1 year(s)".

### HDD Capacity

Item	Description
Remaining Capacity When Nearly Full	Specify the value at which 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 at which to check that the hard disk is full. You can specify any value between 1 and 100 GB. The default is 1 GB.

#### ↓ Note

- A warning message appears in a dialog box when the amount of the free space on the HDD reaches the specified value.

**Deletion Settings When Capacity is Full**

Item	Description
Status	<p>Specify how long the status history is stored when the hard disk is full.</p> <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> <p>The default is Do not Delete.</p>
Counter	<p>Specify how long the counter data is stored when the hard disk is full.</p> <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> <p>The default is Do not Delete.</p>
User Counter	<p>Specify how long the user counter information is stored when the hard disk is full.</p> <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> <p>The default is Do not Delete.</p>
System/Tasks/Notifications Logs System/Tasks/Notifications/Report Logs *	<p>Specify how long the system logs is stored when the hard disk is full.</p> <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> <p>The default is Do not Delete.</p>

Item	Description
Report *	Specify how long reports are stored when the hard disk is full. <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> The default is Do not Delete.
Device Job Log *	Specify how long the device job log is stored when the hard disk is full. <ul style="list-style-type: none"> <li>• 1 to 31 day(s)</li> <li>• 1 to 12 month(s)</li> <li>• 1 to 5 year(s)</li> <li>• Do not Delete</li> </ul> The default is Do not Delete.

\* This item can be used in Device Manager NX Accounting.

## System Information and Settings

The system version of this product is displayed.

Select the [Enable SDK/J Platform] checkbox to allow the system to automatically enable SDK/J Platform on the machine that is equipped with Smart Operation Panel.

The platform is automatically enabled in the following cases:

- When [Other Polling] in any of the setting items under [Device Access Settings] in the section area is executed.
- When any of the following functions under [Configuration] in the section area is executed:
  - Installing, updating, uninstalling, or activating SDK application
  - Updating SDK/J Platform

When SDK/J Platform is disabled on the device side, the following functions of Device Manager NX can be applied partially.

- Obtaining the information of the applications that have been installed by [Other Polling]
- Installing, updating, uninstalling, or activating SDK Applications

---

## Authentication and Accounts

---

You can set a password to start this product.

### Change Password

---

#### Change Password

Item	Description
Login Password	Enter a new password.
Confirm Login Password	Reenter the new password to confirm it.



# Notification Policy

The [Notification Policy] section permits setting of conditions for pop-up notification of the device status.

## Status Notification

### Notification Policy

The notification policies are displayed in a list.

To create a new notification policy, specify when and how the policy is notified.

#### Configuration items to create a definition

Configuration item	Description
Policy Name	Enter a definition name.

The definitions added to the list are configured using the [Triggers], [Conditions], and [Monitored Devices] tabs.

#### [Triggers] tab

To specify when a notification is sent, select the device status from the available check boxes.

#### [Conditions] tab

Specify when a notification is sent. Depending on the situation, specify how many times a notification is repeated (repetition count) or how long a notification is sent continuously (continuance).

#### Setting the repetition count

Items	Description
second(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX seconds.
minute(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX minutes.
hour(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX hours.
day(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX days.

Items	Description
month(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX months.
year(s)	Specify when a notification is repeated. On the [Triggers] tab, specify "XX" in XX times in XX years.

Specify the count and period of "XX" using text boxes.

**Setting of continuance**

Item	Description
second(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX seconds.
minute(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX minutes.
hour(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX hours.
day(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX days.
month(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX months.
year(s)	Specify how long a notification is repeated continuously. On the [Triggers] tab, specify "XX" in XX years.

Specify the period of "XX" using text boxes.

**[Monitored Devices] tab**

A list of devices and groups that are monitored as notification targets is displayed.

**Note**

- For the functional outlines or operations of these setting items, see page 73 "Checking System Operation Logs".

**Logs**

Logs related to results of system actions are displayed in a list.

For the functional outlines or operations of these setting items, see page 73 "Checking System Operation Logs".

## Task Notification

### Non-executed Task Notification Settings

Specify the type of task for which a notification is to be sent when the task is not executed. A notification can be sent for the following task types:

- Discovery
- Polling
  - Status Polling
  - Supplies Polling
  - Other Polling
  - Counter Polling
  - User Counter Polling
- **Configuration**
  - Device Preference
  - SDK/J Platform Settings
  - SDK Application
  - Address Book
  - Power Mode
- Report \*
- Device Log Management \*
  - Device Log Settings
  - Device Log Collection

\* This item can be used in Device Manager NX Accounting.

#### Note

- For the functional outlines or operations of these setting items, see page 72 "Notifying/Confirming Overdue Tasks".

### Non-executed Task List

The tasks that are yet to be executed are displayed in the list. The following information can be notified:

Item	Description
Start Date	The date the non-executed tasks was scheduled to be performed

Item	Description
Task Name *1	Names of the unexecuted tasks
Category	Categories of the unexecuted tasks

\*1 The task is the same as the task name in the logs.

Items that are displayed in Device Manager NX Accounting.

**Note**

- For the functional outlines or operations of these setting items, see page 72 "Notifying/Confirming Overdue Tasks".

---

# Logs

You can check logs of the executed system operations and operation results.

---

## System Log

---

Logs related to results of system actions are displayed in a list.

For explanations about the displayed information, see page 73 "Checking System Operation Logs".

# Device Log Management

To retrieve device logs and export collected logs, see the [Device Log Management] section.

## Device Log Collection

You can create a task to specify the device settings related to device logs and configure the settings for retrieving devices logs.

## Device Log Settings

Tasks that are related to the device log settings are displayed in a list. A task that retrieves the device logs is configured using the [General], [Device Log Settings], [Target Devices/Groups], and [Schedule] tabs.

### [General] tab

Set the general information of a task.

Item name	Description
Name	Enter the name of the task. Use 1 to 255 characters.
Description	Enter the description of the task. Use 0 to 511 characters.
Task Type	<p>Select [Check], [Apply], or [Check &amp; Apply] for the task type.</p> <ul style="list-style-type: none"> <li>• [Check] Checks that the settings of the target device match exactly the settings configured on the [Device Log Settings] tab.</li> <li>• [Apply] Applies the settings configured on the [Device Log Settings] tab regardless of the device settings.</li> <li>• [Check &amp; Apply] Checks that the settings of the target device match those configured on the [Device Log Settings] tab. If they do not match, the settings configured on the [Device Log Settings] tab are applied. If all settings match exactly, no changes will be applied.</li> </ul>

### [Device Log Settings] tab

You can configure the settings related to retrieving device logs.

Item name	Description
Job Log Collection	Specify whether or not to enable the retrieval of job logs stored in devices. When this settings is enabled, access logs and ecology logs of devices are not retrieved.
Encrypt Device Logs in Device	Specify whether or not to internally encrypt the device logs stored in devices.

### [Target Devices/Groups] tab

The target devices of a task are displayed in a list. The target devices can be added in device units or group units.

### [Schedule] tab

Specify the schedule to perform tasks.

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 an interval from 1 minute to 7 days. Specify whether the interval measurement is started at the start or end of the print job.
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 it is executed weekly on the specified day of the week. You can select multiple days of the week from Monday to Sunday.
Monthly	The task begins at the specified date/time, and it is executed monthly on the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.

### ↓ Note

- For the functional outlines or operations of these configuration items, see page 46 "Managing Device Logs".

## Device Log Collection

Tasks that are related to collecting device logs are displayed in a list. A task that retrieves the device logs is configured using the [General], [Target Devices/Groups], and [Schedule] tabs.

### [General] tab

Set the general information of a task.

Item name	Description
Name	Enter the name of the task. Use 1 to 255 characters.
Description	Enter the description of the task. Use 0 to 511 characters.

### [Target Devices/Groups] tab

The target devices of a task are displayed in a list. The target devices can be added in device units or group units.

### [Schedule] tab

Specify the schedule to perform tasks.

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 an interval from 1 minute to 7 days. Specify whether the interval measurement is started at the start or end of the print job.
Daily	The task begins at the specified time every day starting the specified day.
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 time every month starting the specified date. You can select multiple dates from the 1st to the last day of the month.
Disable Schedule	The schedule is disabled if this check box is selected.
Advanced Settings	You can set a time period for preventing task execution when this check box is selected.



**Note**

- For the functional outlines or operations of these configuration items, see page 46 "Managing Device Logs".

---

## Device Log Management

---

You can export retrieved device logs.

### Device Log Export

---

Retrieved device logs can be exported as a CSV file.

#### Device Log Export

Item name	Description
Start Date	Specify the start date of the duration to export the device log.
End Date	Specify the end date of the duration to export the device log.

**Note**

- The local time of the computer on which Device Manager NX is installed is used as a reference when you export logs.
- For the functional outlines or operations of these configuration items, see page 46 "Managing Device Logs".



# 8. Appendix

---

## Setting a Password

Specify the password to use when logging on to Device Manager NX. Unauthorized access can be prevented by setting a password.

1. In the section area, click [System].
2. In the [Authentication and Accounts] category on the section tree, click [Change Password].
3. Enter a new password or a password to be changed in the [Login Password] box.
4. Re-enter the password in the [Confirm Login Password] box.
5. Click [Save].

## Disabling SSLv3 and SSLv2Hello

To avoid vulnerability in certain protocols or encryption algorithms, configure Device Manager NX to enable or disable each protocol individually. When Device Manager NX communicates with external systems, it uses the most secure encryption algorithm possible or the algorithm of the required encryption strength. The following protocols are enabled by default in Device Manager NX:

- TLSv1.2
- TLSv1.1
- TLSv1.0
- SSLv3
- SSLv2Hello

### ★ Important

- **It is recommended that you disable SSLv3 and SSLv2Hello protocols unless these protocols are required in your environment. Disabling these protocols disrupts your normal operation.**

For the available encryption algorithms and the default setting in Device Manager NX, see the following table. "N/A" indicates that the protocol does not support the corresponding algorithm.

Algorithms	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_RC4_128_SHA	N	N	N	N
TLS_ECDHE_RSA_WITH_RC4_128_SHA	N	N	N	N
SSL_RSA_WITH_RC4_128_SHA	N	N	N	N
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	N	N	N	N
TLS_ECDH_RSA_WITH_RC4_128_SHA	N	N	N	N
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	Y	Y	Y	Y

Algorithms	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
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
SSL_RSA_WITH_RC4_128_MD5	N	N	N	N
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_RSA_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y
TLS_RSA_WITH_AES_128_CBC_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_RSA_WITH_AES_128_CBC_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_DSS_WITH_AES_128_CBC_SHA256	N/A	N/A	N/A	Y

#### ↓ Note

- When the protocols specified above are disabled, the communication with external systems these protocols support cannot be performed.
- In particular, the following restriction applies when you operate the software:
  - Device Manager NX can no longer receive device logs (job log and access log) from some devices that are equipped with Smart Operation Panel.

## The procedure to disable SSLv3 and SSLv2Hello Protocols

Disable SSLv3 and SSLv2Hello Protocols as follows:

### 1. Exit Device Manager NX.

2. Find the properties file (`sslClient.properties`) that is provided with the installer file of Device Manager NX. This properties file can be found under the following directory:  
`\Manual\Sample_Files`
3. Copy the properties file to the "Configuration" folder in the installation path of Device Manager NX. This file contains the information of the protocols to be enabled or disabled and the encryption setting that disables unsafe protocols.

The high-risk protocols are now disabled.

 **Note**

- To revert the setting to its default, exit Device Manager NX, and then delete the properties file that has been added in Step 3 from the "Configuration" folder, and restart Device Manager NX.

# List of Device Preference Setting Items

The following describes the configuration items on devices that can be specified in the Device Preference templates.

## General

### <General>

Setting	Description
Display IP Address on Device Display Panel	Set whether the IP address is displayed for a device.

### <Password Policy>

Setting	Description
Password	Select [None], [Type 1], or [Type 2] for the password policy of the device.

### <Web Page>

Setting	Description
URL Name	Enter the URL name of the device.
URL	Enter the URL of the device.

## Date and Time

### <Date/Time Settings>

Setting	Description	
SNTP Server Settings	Set the SNTP server.	
	SNTP Server Address	Enter the SNTP server host name or IP address.
	Polling Interval	<ul style="list-style-type: none"> <li>[When Printer On] Select this to perform polling only when the device is activated.</li> <li>[Every Time] Select this to perform polling at a given interval. Enter the polling interval in units of minutes.</li> </ul>

### <Time Zone/Daylight Saving Time Settings>

Setting	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.



## Protocol

### <NetWare>

Setting	Description
NetWare	Specify whether to enable the NetWare protocol.

### <AppleTalk>

Setting	Description
AppleTalk	Specify whether to enable the AppleTalk protocol.
Zone Name	Specify the AppleTalk zone. Enter the zone name.

### <SMB>

Setting	Description
SMB	Specify whether to enable SMB.
Workgroup Name	Enter the Workgroup name.
Notify Print Completion	Specify whether to enable Print Completion Notification.

## TCP/IP

### <TCP/IP>

Setting	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.
LPR	Specify whether to enable LPR.
RSH/RCP	Specify whether to enable RSH/RCP.
DIPRINT	Specify whether to enable Direct Print.
FTP	Specify whether to enable printing using FTP.

Setting	Description
IPP	Specify whether to enable printing using IPP.
Telnet	Specify whether to enable printing using Telnet.
SSH	Specify whether to enable printing using SSH.
SFTP	Specify whether to enable printing using SFTP.

## SNMP

### <SNMP Profile>

Setting	Description
Profile Name	Select the Profile when specifying the SNMP account configured in the Access Account Settings to Community 1 to 10.  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].
<SNMP v1/v2>	The community name specified in the SNMP account is displayed. Select the Community number to which you want to assign the settings.
<SNMP v3>	The Authentication Algorithm specified in the SNMP account setting is displayed.

**<Community 1> to <Community 10>**

Setting	Description
Community 1	<ul style="list-style-type: none"> <li>Community Name Enter the community name.</li> <li>Access Type Select [Not Accessible], [read-only], [read-write], or [trap] for the access type.</li> <li>Protocol Type Select [TCP/IP+IPX], [IPX], [TCP/IP], or [Off] for the protocol type.</li> <li>IP Address When enabling SNMP Trap and selecting TCP/IP, enter the IP address of the host receiving the information.</li> <li>Manager IPX Address When enabling SNMP Trap and selecting IPX, enter the IPX address of the host receiving the information.</li> </ul>
Community 2	
Community 3	
Community 4	
Community 5	
Community 6	
Community 7	
Community 8	
Community 9	
Community 10	

**<SNMP v3 Setting>**

Setting	Description
SNMP v3 Setting	<ul style="list-style-type: none"> <li>SNMP v3 Select whether to enable SNMPv3.</li> <li>Authentication Algorithm Select [MD5] or [SHA1].</li> </ul>

**Administrator****<Administrator Account Settings>**

Setting	Description
Profile Name	<p>Select the Web service account that was created in the Access Account Settings.</p> <p>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].</p>

Setting	Description
User Name	The user name of the user's Web service account is displayed.
Password	The masked password of the user's Web Service Account is displayed.

### <Administrator Authentication Management>

Setting	Description
Network Administrator Authentication	Specify whether to authenticate network administrators. Check applicable items. If you select [On] for an item, that item will be authenticated. You can select multiple items. File Transfer, Interface Settings, Administrator Tools
Machine Administrator Authentication	Specify whether to authenticate device administrators. Check applicable items. 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
User Administrator Authentication	Specify whether to authenticate user administrators. Select [On] for the user administrator, and then [Administrator Tools] to authenticate a user administrator.
File Administrator Authentication	Specify whether to authenticate document administrators. Select [On] for the user administrator, and then [Administrator Tools] to authenticate a file administrator.

## Email

### <Email>

Setting	Description
Email	<ul style="list-style-type: none"> <li>Administrator Email Address Enter the administrator's e-mail address.</li> </ul>

**<Reception Settings>**

Setting	Description
Reception Protocol	Select the receiving protocol: [POP3], [IMAP4], [SMTP]
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.
SMTP Server Address	Enter the SMTP server address or host name.
SMTP Port Number	Enter the port number used by an SMTP server.
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	Description
POP before SMTP	Specify whether to perform POP before SMTP.
Timeout Setting after POP Auth.	Enter a time (in msec) that the machine waits before going into standby mode following authentication by the POP server.

**<POP3/IMAP4>**

Setting	Description
POP3/IMAP4 Server Name	Enter the POP3/IMAP4 server name.

Setting	Description
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.

**<Email Address>**

Setting	Description
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.

**User 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	Description
User Authentication Settings	Select the user authentication type: [Off], [User Code Authentication], [Basic Authentication], [Windows Authentication], [LDAP Authentication], [Integration Server Authentication]

**<Printer Job Authentication>**

Setting	Description
Printer Job Authentication	<ul style="list-style-type: none"> <li>• Printer Job Authentication Select the printer job authentication method: [Entire], [Simple (All)], [Simple (Limitation)]</li> <li>• Limitation Range 1 - 5 Enter the range of IP addresses subject to authentication.</li> <li>• Parallel Interface (Simple) Specify whether to allow parallel interface.</li> <li>• USB (Simple) Specify whether to allow USB interface.</li> </ul>

**<Windows Authentication>**

Setting	Description
Windows Authentication	<ul style="list-style-type: none"> <li>• Domain Name If you select [Windows Authentication] in User Authentication Settings, enter the domain name to be used for authentication.</li> <li>• SSL Specify whether or not to perform SSL.</li> <li>• Kerberos Authentication Specify whether to use Kerberos authentication. If you select [On] under [Kerberos Authentication], you must specify the realm to protect with Kerberos authentication.</li> <li>• Authentication Realm Specify the realm to protect with Kerberos authentication.</li> </ul>

<LDAP Authentication>

Setting	Description
LDAP Authentication	<ul style="list-style-type: none"> <li>• LDAP Server 1 - 5 If you select [LDAP Authentication] in User Authentication Settings, select an LDAP authentication server.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• LDAP Login Attribute Enter an LDAP login attribute.</li> <li>• Global Identifier Enter a global identifier.</li> </ul>

<Integration Server Authentication>

Setting	Description
Integration Server Authentication	<ul style="list-style-type: none"> <li>• Server Name If you select [Integration Server Authentication] in User Authentication Settings, enter the Integration server name.</li> <li>• Domain Name Enter the name of the domain where integration server authentication will be performed.</li> <li>• 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]</li> <li>• SSL You can specify whether or not to perform SSL.</li> </ul>



**<Access Control>**

Setting	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]. <ul style="list-style-type: none"> <li>Auto Register User Codes Specify whether to automatically register the user code contained in a print job.</li> </ul>
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 Box for each user.

**Note**

- [Access Control] can be specified only when [User Authentication Settings] is set to [User Code Authentication].

**Paper Tray**

Setting	Description
Paper Tray 1 to 10	Select the paper type loaded in each paper trays.

**Printer****<Maintenance>**

Setting	Description
Protect Printer Display Panel	[Off], [Level 1], [Level 2]

Setting	Description
List/Test Print Lock	List/test print lock: Select whether to prohibit test prints.

**<Printer System>**

Setting	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.
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.

Setting	Description
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]
Paper Size	Select the default paper size.
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.

Setting	Description
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.

**<Interface Settings>**

Setting	Description
I/O Buffer	Select a receive buffer size: [16 KB], [32 KB], [64 KB], [128 KB], [256 KB], [512 KB], [1 MB]
I/O Timeout	Select the interface switching time: [10 sec.], [15 sec.], [20 sec.], [25 sec.], [60 sec.]

**<PCL settings>**

Setting	Description
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]

Setting	Description
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]

**<PS Settings>**

Setting	Description
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.
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]

Setting	Description
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 Settings>**

Setting	Description
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].
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.

## LDAP Server

### <LDAP Server Settings>

Setting	Description
LDAP Server	Specify whether to use the LDAP search.

### <LDAP Server 1> to <LDAP Server 5>

Setting	Description
LDAP Server 1 to 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.
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.

Setting	Description
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.

## Kerberos Server Settings

### <Authentication Realm Settings 1> to <Authentication Realm Settings 5>

Setting	Description
Realm 1 to 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.
Domain Name	Enter the name of the domain that corresponds to the realm.

## Firmware Update Settings

### <Firmware Update Settings>

Setting	Description
Permit Firmware Update	Specify whether to permit firmware updates.
Permit Firmware Structure Change	Specify whether to permit changes to the firmware structure.



## User Lockout Policy

### <User Lockout Policy>

Setting	Description
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.

## Interface Settings

### <Interface Settings>

Setting	Description
Ethernet Speed	<p>Ethernet communication speed. For normal use, select [Auto Select]. This allows the device to select the optimum speed.</p> <p>If communication with the device fails, select [100Mbps Full Duplex], [100Mbps Half Duplex], [10Mbps Full Duplex], or [10Mbps Half Duplex].</p>

## Device Functions

### <Enable SDK/J Platform>

Setting	Description
SDK/J Platform	Specify whether to enable or disable SDK/J Platform.

---

## Web Browser NX

---


### <General>

Setting	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.

# Importing/Exporting the System Settings

Importing CSV files to Device Manager NX enables you to integrate register volume information such as devices, groups, and user data.

## Information that can be imported/exported as a CSV file

Information type	Import	Export	Reference
Device display information	Available	Available	page 15 "Display Icons"
Group information	Available	Available	page 28 "Importing/Exporting the Group Information"
Device counter	Not available	Available	page 41 "Checking Counters"
Per user counter	Not available	Available	page 41 "Checking Counters"
User data	Available	Available	page 57 "Registering a User or a Group to the Entry List"
Discovery range	Available	Available	page 22 "Searching for Devices"
Device preference template	Available	Available	To export a Device Preference template, click  in the list area. Select [Import File] during the template creation procedure to import a template. For details, see page 51 "Applying Same Settings to Multiple Devices".
Device log	Not available	Available	page 46 "Managing Device Logs"

### Note

- The creation date, the exported function name, and its category will be automatically appended to the exported CSV file name. The date and time format of the creation date depends on the format specified in [Date Display Format]. For details about the date and time format, see "Display Settings".
- When editing the CSV file to be imported, follow the formatting rule, and edit the file accordingly. For details about the format of CSV files, see page 178 "Format of CSV Files".
- You can download a CSV file to use as a sample in the file selection dialog box for selecting the CSV file to be imported. Use this template for editing CSV files.

## Format of CSV Files

CSV files are used for import/export of Device Manager 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.
- A sample format of an imported CSV file can be downloaded from Device Manager NX. For the downloading method, see page 177 "Importing/Exporting the System Settings".

### 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: 4.1.1.X
2	# Generated at: <b>(Date/time of write-out)</b>
3	# Function Name: Device List
4	# Custom Property 1= <b>(Value of Custom Property 1)</b> , Custom Property 2= <b>(Value of Custom Property 2)</b> , Custom Property 3= <b>(Value of Custom Property 3)</b> , Custom Property 4= <b>(Value of Custom Property 4)</b> , Custom Property 5= <b>(Value of Custom Property 5)</b>
5	<b>"(Item name of the column)"</b>
6	<b>"(Value of the device that corresponds to the item name of the column)"</b>

As "Item name of the column" in line five, 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.

## Format of a Group 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: 4.1.1.X
2	# Generated at: <b>(Date/time of write-out)</b>
3	# Function Name: Device Groups
4	<b>"(Row name)"</b>
5	<b>"(Value that corresponds to row name)"</b>

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	Device Group ID	Group ID
2	Device Group Name Lv 1	Group name of a category group
3	Device Group Name Lv 2	Child group name of Device Group Name Lv 1
4	Device Group Name Lv 3	Child group name of Device Group Name Lv 2
5	Device Group Name Lv 4	Child group name of Device Group Name Lv 3
6	Device Group Name Lv 5	Child group name of Device Group Name Lv 4
7	Device Group Name Lv 6	Child group name of Device Group Name Lv 5
8	Device Group Name Lv 7	Child group name of Device Group Name Lv 6

"Device Group ID" in row one is the ID for identification of a group by Device Manager NX. Negative integers are given for category groups, and integers are given for groups in child layers.

At the time of import, groups of the same ID are overwritten. If this row is blank, a group is added without overwriting.

#### ↓ 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: 4.1.1.0
# Generated at: XX/XX/XXXX XX:XX:XX
# Function Name: Device Groups
"Device Group ID","Device Group Name Lv 1","Device Group Name Lv 2","Device Group
Name Lv 3","Device Group Name Lv 4","Device Group Name Lv 5","Device Group Name Lv
6","Device Group Name Lv 7"
"-15","Category Group",,,,,,
"110",,,,,,"Sub-Group-1",,,,,,
"111",,,,,,"Sub-Group-1-2",,,,,,
"112",,,,,,"Sub-Group-1-3",,,,,,
"113",,,,,,"Sub-Group-2",,,,,,
"114",,,,,,"Sub-Group-2-1",,,,,,
```

### 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: <b>(Date/time of write-out)</b>
3	# Function Name: User Data Preference
4	# Template Name: <b>(Template name of Address book)</b>
5	# Description: <b>(Contents set in [Description] of the template)</b>

Line number	Contents
6	# Authentication Method (0=none or user code/1=others): <b>(0 or 1)</b>
7	<b>"(Row name)"</b>
8	<b>"(Value that corresponds to row name)"</b>

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:

#### 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	Enter the name of the entry. This entry is required. Enter up to 20 characters.
Set General Settings	Specify whether or not to configure the device. 0: Do not configure the device 1: Configure the device
Set 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.	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

Row name	Value of line 8 and subsequent lines
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.
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	Specify whether or not to specify an index. 0: Do not configure the settings 1: Configure the settings
Title 1	Specify the index registered in Index Set 1. 0: Do not register 1 to 10: "1"-"10"
Title 2	Specify the index registered in Index Set 2. 0: Do not register 1 to 10: "AB"-"XYZ"
Title 3	Specify the index registered in Index Set 3. 0: Do not register 1 to 10: "1"-"5"
Title Freq.	Specify whether or not to register the entry in the commonly used index. 0: Do not register 1: Register
Set User Code Settings	Specify whether or not to specify the user code. 0: Do not configure the settings 1: Configure the settings
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	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	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	This item cannot be specified.
Device Login Password Encoding	This item cannot be specified.
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	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	This item cannot be specified.
SMTP Authentication Password Encoding	This item cannot be specified.
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	Enter the user name for folder authentication. Up to 128 characters can be entered.
Folder Authentication Login Password	This item cannot be specified.
Folder Authentication Password Encoding	This item cannot be specified.

Row name	Value of line 8 and subsequent lines
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	Enter the user name for LDAP authentication. Up to 128 characters can be entered.
LDAP Authentication Login Password	This item cannot be specified.
LDAP Authentication Password Encoding	This item cannot be specified.
Set Access Control Settings	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	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	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.
Can Use Two Color Copy	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.

Row name	Value of line 8 and subsequent lines
Can Use Full Color Copy	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	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	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	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	Specify the scanner usage restrictions. 0: Restrict scanner usage 1: Do not restrict scanner usage
Can Use Fax	Specify the fax usage restrictions. 0: Restrict fax usage 1: Do not restrict fax usage
Can Use 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	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.

Row name	Value of line 8 and subsequent lines
Set Email/Fax Settings	Specify whether or not to configure the fax and e-mail settings. 0: Do not configure the settings 1: Configure the settings
Fax Destination	Enter the fax number or IP fax address. Up to 512 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 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) , cloud (Cloud Fax)
International Fax Transmission Mode	Specify whether or not to enable the international transmission mode. 0: Disable 1: Enable
E-mail Address	Enter the e-mail address. Up to 128 characters can be entered.  Usable characters include alphanumeric characters and the following symbols: !, #, \$, %, &, ', *, +, -, /, =, ?, ^, _ , ` , { ,   , } , ~ , . , @
Ifax 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	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

Row name	Value of line 8 and subsequent lines
Direct SMTP	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	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	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
Label Insertion 1st Line (Selection)	Specify whether or not to use merge print. 0: Do not use merge print 1: Use merge print
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)	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

Row name	Value of line 8 and subsequent lines
Set Folder Settings	Specify whether or not to configure folders. 0: Do not configure the settings 1: Configure the settings
Folder Protocol	Select the Protocol to use. 0: SMB 1: FTP 2: NCP-Bindery 3: NCP-NDS
Folder Port No.	Enter the port number to use in FTP. Enter a value between 1 and 65,535.
Folder Server Name	Enter the server name to use in FTP. Up to 128 characters can be entered.
Folder Path	Enter the path name. Up to 256 characters can be entered.
Folder Japanese Character Encoding	Specify the Japanese character code used for FTP. <ul style="list-style-type: none"> <li>• us-ascii</li> <li>• shift_jis</li> <li>• euc-jp</li> </ul>
Set Protection Settings	Specify whether or not to configure the authentication protection settings. 0: Do not configure the settings 1: Configure the settings
Is Setting Destination Protection	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	Specify whether or not to protect the folder destination. 0: Do not protect 1: Protect
Is Setting Sender Protection	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

Row name	Value of line 8 and subsequent lines
Is Protecting Sender	<p>Specify whether or not to protect the sender.</p> <p>0: Do not protect</p> <p>1: Protect</p>
Sender Protection Password	This item cannot be specified.
Sender Protection Password Encoding	This item cannot be specified.
Access Privilege to User	<p>Specify the access privilege of the folder destinations.</p> <p>Specify the privilege by entering the "Index in ACLs and Groups" number and one of the following letters:</p> <p>R: Viewing allowed</p> <p>W: Editing allowed</p> <p>D: Editing/deleting allowed</p> <p>X: Full control</p> <p>To specify multiple groups, separate each group using a comma.</p> <p>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.</p>
Access Privilege to Protected File	Specify the protection privilege of documents stored in the Document Server. The same setting as Access Privilege to User applies.
Set Group List Settings	<p>Specify whether or not to specify the groups to which users will be assigned.</p> <p>0: Do not configure the settings</p> <p>1: Configure the settings</p>
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	<p>Specify whether or not to configure the counter reset settings.</p> <p>0: Do not configure the settings</p> <p>1: Configure the settings</p>

Row name	Value of line 8 and subsequent lines
Enable Plot Counter Reset	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	Specify whether or not to reset the fax usage counter. 0: Do not reset the counter 1: Reset the counter
Enable Scanner Counter Reset	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	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, see the instruction manual for SmartDeviceMonitor for Admin.

## 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: 4.1.1.X
2	# Generated at: <b>(Date/time of write-out)</b>
3	# Function Name: Network Search Discovery Range
4	<b>"(Row name)"</b>
5	<b>"(Value that corresponds to row name)"</b>

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: 4.1.1.X
2	# Generated at: <b>(Date/time of write-out)</b>
3	# Function Name: Broadcast Discovery Range
4	<b>"(Row name)"</b>
5	<b>"(Value that corresponds to row name)"</b>

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 a Device Preference CSV File

A Basic Device Preferences template CSV file is written out in the format indicated below:

The variable portions are indicated in **bold letters**.

Line number	Contents
1	# Format Version: 4.1.1.X
2	# Generated at: <b>(Date/time of write-out)</b>
3	# Function Name: Device Preference Template

Line number	Contents
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 line five and subsequent lines
1	Attribute	Enter the attribute name included in the device preference template.
2	Value	Enter the settings.

The value or string between parentheses ([Value]) represents the setting that corresponds to the item in each template. When the specified value is a text string, it is represented as characters enclosed in double quotations (""). When the specified value is a number, its acceptable range is represented as XX-XX.

#### Attribute names and values for each items

Configuration item	Attribute	Value
<General Features>		
Display IP Address on Device Display Panel	system.commonBase: 01.ipAddrDisp	TRUE [Enable] FALSE [Disable]
<Password Policy>		
Password	common.PasswordPolicy: 01.passwordComplexity	COMPLEXITY0 [None] COMPLEXITY1 [Type 1] COMPLEXITY2 [Type 2]
<Web Page>		
URL Name	networkGeneral:01.UrlName	URL name of a Device
URL	networkGeneral:01.UrlLink	URL of a Device
<Date/Time Settings>		

Configuration item	Attribute	Value
SNTP Server Address	system.snmp:01.snmpServerAddress	IP address or hostname of SNTP server
Polling Interval	system.snmp:01.snmpPollingEnabled	TRUE [Every Time] FALSE [When Printer On]
milli-second (15-10080)	system.snmp:01.interval	15 to 10080
<Time Zone/Daylight Saving Time Settings>		
Time Zone (GMT)	system.timezone:01.standardOffset	-720 to + 839
DST	system.timezone: 01.summerTimeEnabled	TRUE [On] FALSE [Off]
Offset Time	system.timezone:01.daylightOffset	0 to 590
Start Date/Time (Month)	system.timezone:01.daylightMonth	0 [January] to 11 [December]
Start Date/Time (Week)	system.timezone:01.daylightDay	0 [The First] to 4 [The Fifth]
Start Date/Time (Day of the week)	system.timezone: 01.daylightDayOfWeek	0 [Sunday] to 6 [Saturday]
Start Date/Time (Time of day)	system.timezone: 01.daylightStartTimeOfDay	0 to 23
End Date/Time (Month)	system.timezone: 01.standardMonth	0 [January] to 11 [December]
End Date/Time (Week)	system.timezone:01.standardDay	0 [The First] to 4 [The Fifth]
End Date/Time (Day of the week)	system.timezone: 01.standardDayOfWeek	0 [Sunday] to 6 [Saturday]
End Date/Time (Time of day)	system.timezone: 01.standardStartTimeOfDay	0 to 23
<NetWare>		
NetWare	networkGeneral: 01.NwAdminStatus	TRUE [Enable] FALSE [Disable]
<AppleTalk>		

Configuration item	Attribute	Value
AppleTalk	networkGeneral: 01.AtkAdminStatus	TRUE [Enable] FALSE [Disable]
Zone Name	networkAppleTalk: 01.AtkZoneName	AppleTalk zone name
<SMB>		
SMB	networkGeneral: 01.MsnAdminStatus	TRUE [Enable] FALSE [Disable]
Workgroup Name	networkNetBEUI: 01.MsnWorkGroupName	Workgroup name
Notify Print Completion	networkNetBEUI: 01.MsnSwitchPrintCompletion	TRUE [Disable] FALSE [Enable]
<TCP/IP>		
DHCP	networkTCPIP:01.NetBootDHCP	TRUE [Enable] FALSE [Disable]
WINS	networkTCPIP:01.IpModeWINS	TRUE [Disable] FALSE [Enable]
Primary WINS Server	networkTCPIP: 01.WINSIpAddressPrimary	IP address of primary WINS server
Secondary WINS Server	networkTCPIP: 01.WINSIpAddressSecondary	IP address of secondary WINS server
LPR	networkTCPIP:01.IpModeLPR	TRUE [Disable] FALSE [Enable]
RSH/RCP	networkTCPIP:01.IpModeRSH	TRUE [Disable] FALSE [Enable]
DIPRINT	networkTCPIP:01.IpModeDiprint	TRUE [Disable] FALSE [Enable]
FTP	networkTCPIP:01.IpModeFTP	TRUE [Disable] FALSE [Enable]

Configuration item	Attribute	Value
IPP	networkTCPIP:01.IpModeIPP	TRUE [Disable] FALSE [Enable]
Telnet	networkTCPIP:01.IpModeTelnet	TRUE [Disable] FALSE [Enable]
SSH	networkTCPIP:01.IpModeSSH	TRUE [Disable] FALSE [Enable]
SFTP	networkTCPIP:01.IpModeSFTP	TRUE [Disable] FALSE [Enable]
<Community 1> to <Community 10>		
Community Name	networkSNMP:<xx>.CommunityName (<xx> represents a number between 01 and 10.)	"Community name"
Access Type	networkSNMP:<xx>.CommunityType (<xx> represents a number between 01 and 10.)	0 [Not Accessible] 1 [read-only] 2 [read-write] 4 [trap]
Protocol Type	networkSNMP:<xx>.CommunityProtocol (<xx> represents a number between 01 and 10.)	0 [TCP/IP+IPX] 1 [IPX] 2 [TCP/IP] 3 [Off]
IP Address	networkSNMP:<xx>.CommunityAddress (<xx> represents a number between 01 and 10.)	IP address
Manager IPX Address	networkSNMP:<xx>.CommunityIPXAddress (<xx> represents a number between 01 and 10.)	IP address
<SNMP v3 Setting>		

Configuration item	Attribute	Value
SNMP v3	network.snmpv3Common: 01.snmpv3Enabled	TRUE [Enable] FALSE [Disable]
Authentication Algorithm	network.snmpv3Common: 01.authenticationAlgorithm	MD5 [MD5] SHA1 [SHA1]
<Administrator Authentication Management>		
Network Administrator Authentication	system.adminauthCommon: 01.networkAdminAuth	TRUE [On] FALSE [Off]
Network Administrator Authentication (Privilege)	system.adminauthCommon: 01.networkAdminAuthPrivilege	File Transfer [File Transfer] Interface Settings [Interface Settings] Administrator Tools [Administrator Tools] Multiple values can be specified by separating each value using a comma.
Machine Administrator Authentication	system.adminauthCommon: 01.machineAdminAuth	TRUE [On] FALSE [Off]
Machine Administrator Authentication (Privilege)	system.adminauthCommon: 01.machineAdminAuthPrivilege	General Features [General Features] Tray Paper Settings [Tray Paper Settings] Timer Settings [Timer Settings] File Transfer [File Transfer] Interface Settings [Interface Settings] Administrator Tools [Administrator Tools] Multiple values can be specified by separating each value using a comma.
User Administrator Authentication	system.adminauthCommon: 01.userAdminAuth	TRUE [On] FALSE [Off]

Configuration item	Attribute	Value
User Administrator Authentication (Privilege)	system.adminauthCommon: 01.userAdminAuthPrivilege	Administrator Tools [Administrator Tools]
File Administrator Authentication	system.adminauthCommon: 01.documentAdminAuth	TRUE [On] FALSE [Off]
File Administrator Authentication (Privilege)	system.adminauthCommon: 01.documentAdminAuthPrivilege	Administrator Tools [Administrator Tools]
<Email>		
Administrator Email Address	delivery.mail: 01.adminMailAddress	Administrator's e-mail address
<Reception Settings>		
Reception Protocol	delivery.mail:01.receiveProtocol	POP3 [POP3] IMAP4 [IMAP4] SMTP [SMTP]
Email Reception Interval	delivery.mail: 01.receiveIntervalSetting	ON [On] OFF [Off]
minute(s) (2-1440)	delivery.mail: 01.receiveIntervalSetting	2 to 1440
Max. Reception Email Size	delivery.mail: 01.receiveMailSizeLimit	1 to 50
Email Storage in Server	delivery.mail:01.serverMailHold	ALL [On] NOT [Off]
SMTP Server Address	delivery.mail:01.smtpServerName	IP address or hostname
SMTP Port Number	delivery.mail:01.smtpPortNumber	1 to 65535
SMTP Authentication	delivery.mail:01.smtpAuth	TRUE [On] FALSE [Off]
SMTP Authentication Email Address	delivery.mail: 01.smtpAuthMailAddress	Email address
SMTP Authentication User Name	delivery.mail: 01.smtpAuthUserName	User name



Configuration item	Attribute	Value
SMTP Authentication Password	delivery.mail: 01.smtpAuthPassWord	Password
SMTP Authentication Encryption	delivery.mail: 01.smtpAuthEncryption	AUTO [Auto Select] TRUE [Enable] FALSE [Disable]
<POP before SMTP>		
POP before SMTP	delivery.mail:01.popBeforeSmtP	TRUE [On] FALSE [Off]
Timeout Setting after POP Auth.	delivery.mail:01.popAuthWaitTime	0 to 10000
<POP3/IMAP4>		
POP3/IMAP4 Server Name	delivery.mail: 01.pop3imap4serverName	POP3/IMAP4 server name
POP3/IMAP4 Encryption	delivery.mail: 01.pop3Imap4Encryption	AUTO [Auto Select] TRUE [Enable] FALSE [Disable]
POP3 Reception Port No.	delivery.mail: 01.pop3ReceivePortNumber	1 to 65535
IMAP4 Reception Port No.	delivery.mail: 01.imap4ReceivePortNumber	1 to 65535
<Email Address>		
Email Address	delivery.mail:01.faxMailAddress	Email address
Fax Email User Name	delivery.mail: 01.faxMailUserName	User name
Fax Email Password	delivery.mail:01.faxMailPassWord	Password
Email Notification Address	delivery.mail:01.mailInfoAddress	Email address
Email Notification User Name	delivery.mail: 01.mailInfoUserName	User name

Configuration item	Attribute	Value
Email Notification Password	delivery.mail:01.mailInfoPassWord	Password
<Authentication Type>		
User Authentication Settings	system.userauthCommon:01.userAuthentication	Off [Off] User Code [User Code Authentication] Local [Basic Authentication] Windows [Windows Authentication] LDAP [LDAP Authentication] RDH [Integration Server Authentication]
<Printer Job Authentication>		
Printer Job Authentication	system.userauthPrinter:01.printerJobAuthentication	ALL [Entire] Simple [Simple (All)] Part [Simple (Limitation)]
Limitation Range 1 to 5 (Starting address)	system.userauthPrinter:01.range<N>From (<N> represents a number between 1 and 5.)	Starting address of IP address range
Limitation Range 1 to 5 (Ending address)	system.userauthPrinter:01.range<N>To (<N> represents a number between 1 and 5.)	Ending address of IP address range
Parallel Interface (Simple)	system.userauthPrinter:01.centro	TRUE [Exclude Authentication] FALSE [Do not Exclude Authentication]
USB (Simple)	system.userauthPrinter:01.usb	TRUE [Exclude Authentication] FALSE [Do not Exclude Authentication]
<Windows Authentication>		

Configuration item	Attribute	Value
Domain Name	system.userauthWindows: 01.domainName	Domain name
SSL	system.userauthWindows:01.ssl	TRUE [On] FALSE [Off]
Kerberos Authentication	system.userauthWindows: 01.kerberos	TRUE [On] FALSE [Off]
Authentication Realm	system.userauthWindows:01.realm	Realm1 [Realm 1] to Realm5 [Realm 5]
<LDAP Authentication>		
LDAP Authentication	system.userauthLdap: 01.LDAPAuthenticationServer	Server1 [LDAP Server 1] to Server5 [LDAP Server 5]  Multiple values can be specified by separating each value using a forward slash.
LDAP Login Attribute	system.userauthLdap: 01.LDAPLoginNameAttribute	LDAP login attribute
Global Identifier	system.userauthLdap: 01.LDAPGlobalUniquelIdentifier	LDAP global unique identifier
<Integration Server Authentication>		
Server Name	system.userauthRdh: 01.RDHServerName	Server name
Domain Name	system.userauthRdh: 01.RDHDomainName	Domain name
Authentication Type	system.userauthRdh: 01.RDHServerKind	Windows_native [Windows Authentication (Native)] Windows_NT [Windows Authentication (NT Compatible)] RdhOriginal [Basic Authentication] ([Integration Server]) Notes [Notes Authentication] Default [Default]

Configuration item	Attribute	Value
SSL	system.userauthRdh:01.ssl	TRUE [On] FALSE [Off]
<Access Control>		
Copier (Black & White)	usageControl.applRestrict: 01.copyBlack	OFF [Disable] ON [Enable]
Copier (Single Color)	usageControl.applRestrict: 01.copyMono	OFF [Disable] ON [Enable]
Copier (Two-color)	usageControl.applRestrict: 01.copyTwin	OFF [Disable] ON [Enable]
Copier (Full Color)	usageControl.applRestrict: 01.copyFull	OFF [Disable] ON [Enable]
Printer (Black & White)	usageControl.applRestrict: 01.printerBlack	OFF [Disable] ON [Enable]
Printer (Color)	usageControl.applRestrict: 01.printerFull	OFF [Disable] ON [Enable]
Fax	usageControl.applRestrict:01.fax	OFF [Off] ON [On]
Scanner	usageControl.applRestrict: 01.scannerBlack	OFF [Off] ON [On]
Document Server	usageControl.applRestrict: 01.documentServer	OFF [Off] ON [On]
Paper Tray		
Paper Tray 1 to 10	inputTray:<xx>.InputMediaTypeCu rrent (<xx> represents a number between 01 and 10.)	Paper type number For details about the value for each paper type, see Appendix.

Configuration item	Attribute	Value
Paper Tray 1 to 10	inputTray:<xx>.InputMediaTypeCurrent2 (<xx> represents a number between 01 and 10.)	Paper type number For details about the value for each paper type, see Appendix.
<Maintenance>		
Protect Printer Display Panel	printer.Maintenance:01.ProtectPrinterOperationPanel	Off [Off] Level 1 [Level 1] Level 2 [Level 2]
List/Test Print Lock	printer.Maintenance:01.List/TestPrintLock	On [On] Off [Off]
<Printer System>		
Misfeed Recovery	printer.System:01.MisfeedRecovery	On [On] Off [Off]
Print Error Report	printer.System:01.PrintErrorReport	On [On] Off [Off]
Auto Continue	printer.System:01.AutoContinue	Off [Off] Immediate [Immediate] 1 minute [1 min.] 5 minute [5 min.] 10 minute [10 min.] 15 minute [15 min.]
Memory Overflow	printer.System:01.MemoryOverflow	Do not print [Do not Print] Error information [Error Information]
Job Separation	printer.System:01.JobSeparation	On [On] Off [Off]
Auto Delete Temporary Print Jobs	printer.System:01.AutoDeleteTemporaryPrintJobs	On [On] Off [Off]

Configuration item	Attribute	Value
hour(s) (1-200)	printer.System: 01.WaittimeforAutoDeleteTemporaryPrintJobs	1 to 200
Auto Delete Stored Print Jobs	printer.System: 01.AutoDeleteStoredPrintJobs	On [On] Off [Off]
hour(s) (1-200)	printer.System: 01.WaittimeforAutoDeleteStoredPrintJobs	1 to 200
Initial Print Job List	printer.System:01.InitialPrintJobList	Complete List [Complete List] List Per User ID [List per User ID]
Rotate by 180 Degrees	printer.System: 01.Rotateby180Degrees	On (On) Off (Off)
Print Compressed Data	printer.System: 01.CompressedData	Allow Processing [On] Do not Allow [Off]
Memory Usage	printer.System:01.MemoryUsage	Font Priority [Font Priority] Frame Priority [Frame Priority]
Duplex Print	printer.System:01.Duplex	Off [Off] Long Edge Bind [Long Edge Bind] Short Edge Bind [Short Edge Bind]
Copies	printer.System:01.Copies	1 to 999
Blank Page Print	printer.System:01.BlankPagePrint	On [On] Off [Off]
B&W Page Detect	printer.System:01.B&WPageDetect	On [On] Off [Off] By Page [Per Page] By File [Per Job]
Edge Smoothing	printer.System:01.EdgeSmoothing	On [On] Off [Off]

Configuration item	Attribute	Value
Toner Saving	printer.System:01.TonerSaving	On [On] Off [Off]
Spool Image	printer.System:01.SpoolImage	On [On] Off [Off]
Reserved Job Waiting Time	printer.System: 01.ReservedJobWaitingTime	Long Wait [Long Wait] Medium Wait [Medium Wait] Short Wait [Short Wait] In Reserved Job Order [In Reserved Job Order]
Printer Language	printer.System:01.PrinterLanguage	Printer language
Sub Paper Size	printer.System:01.SubPaperSize	Auto [Auto] Off [Off]
Paper Size	printer.System:01.PageSize	Paper size Examples: A4, 8 1/2 x 11
Letterhead Setting	printer.System: 01.LetterheadSetting	Off [Off] Auto Detect [Auto Detect] On (Always) [On (Always)]
Bypass Tray Setting Priority	printer.System: 01.BypassTraySettingPriority	Driver/Command Settings [Driver/Command Settings] Machine Settings [Machine Settings]
Edge to Edge Print	printer.System:01.EdgeToEdgePrint	On [On] Off [Off]
Default Printer Language	printer.System: 01.DefaultPrinterLanguage	Printer language
Tray Switching	printer.System:01.TraySwitching	On [On] Off [Off]

Configuration item	Attribute	Value
Collate Type	printer.System:01.CollateType	Collate [Collate] Rotating Collate [Rotating Collate] Shift Collate [Shift Collate]
Staple Type	printer.System:01.StapleType	Off [Off] Top Left Slant [Top Left Slant] Top Right Slant [Top Right Slant] Left 2 [Left 2] Right 2 [Right 2] Top 2 [Top 2] Top Left [Top Left] Top Right [Top Right] Center [Center]
Punch Type	printer.System:01.PunchType	Off [Off] Left 2 [Left 2] Top 2 [Top 2] Right 2 [Right 2] Left 3 [Left 3] Top 3 [Top 3] Right 3 [Right 3] Left 4 [Left 4] Top 4 [Top 4] Right 4 [Right 4]
Extended Auto Tray Switching	printer.System: 01.ExtendedAutoTraySwitching	On [On] Off [Off]
Virtual Printer	printer.System:01.VirtualPrinter	On [On] Off [Off]
<Interface Settings>		



Configuration item	Attribute	Value
I/O Buffer	printer.HostInterface:01.I/OBuffer	16 KB [16 KB] 32 KB [32 KB] 64 KB [64 KB] 128 KB [128 KB] 256 KB [256 KB] 512 KB [512 KB] 1 MB [1 MB]
I/O Timeout	printer.HostInterface:01.I/OTimeout	10 seconds [10 sec.] 15 seconds [15 sec.] 20 seconds [20 sec.] 25 seconds [25 sec.] 60 seconds [60 sec.]
<PCL settings>		
Orientation	printer.PCLSettings:01.Orientation	Portrait [Portrait] Landscape [Landscape]
Form Lines	printer.PCLSettings:01.FormLines	5 to 128
Font Source	printer.PCLSettings:01.FontSource	Resident [Resident] RAM [RAM] HDD [HDD] Slot DIMM [Slot DIMM] SD [SD] SD Font Download [SD Font Download]
Font Number	printer.PCLSettings:01.FontNumber	0 to 65535
Point Size	printer.PCLSettings:01.PointSize	4 to 999.75 (0.25/unit)
Font Pitch	printer.PCLSettings:01.FontPitch	0.44 to 99.99 (0.01/unit)
Symbol Set	printer.PCLSettings:01.SymbolSet	Symbol set name
Courier Font	printer.PCLSettings:01.CourierFont	Regular [Regular] Dark [Dark]

Configuration item	Attribute	Value
Extend A4 Width	printer.PCLSettings: 01.ExtendA4Width	On [On] Off [Off]
Append CR to LF	printer.PCLSettings: 01.AppendCRtoLF	On [On] Off [Off]
Resolution	printer.PCLSettings:01.Resolution	300 x 300 [300 dpi] 600 x 600 [600 dpi Fast] 600 x 600 x 2 [600 dpi Standard] 1200 x 1200 [1200 dpi]
Tray Parameters (Auto Select)	printer.PCLTrayParameters: 01.AutoSelect	0 to 99
Tray Parameters (Tray 1 to Tray 7)	printer.PCLTrayParameters: 01.Tray<N> (<N> represents a number between 1 and 7.)	0 to 99
Tray Parameters (Large Capacity Tray)	printer.PCLTrayParameters: 01.LargeCapacityTray	0 to 99
Tray Parameters (Bypass Tray)	printer.PCLTrayParameters: 01.BypassTray	0 to 99
<PS Settings>		
Job Timeout	printer.PSSettings:01.JobTimeout	0 to 999
Wait Timeout	printer.PSSettings:01.WaitTimeout	0 to 999
Data Format	printer.PSSettings:01.DataFormat	Binary Data [Binary Data] TBCP [TBCP]
Resolution	printer.PSSettings:01.Resolution	300 x 300 [300 dpi] 600 x 600 [600 dpi Fast] 600 x 600 x 2 [600 dpi Standard] 1200 x 1200 [1200 dpi]

Configuration item	Attribute	Value
Color Settings	printer.PSSettings:01.ColorSetting	None [None] Fine [Fine] Super Fine [Super Fine]
Color Profile	printer.PSSettings:01.ColorProfile	Auto [Auto] Presentation [Presentation] Solid Color [Solid Color] Photographic [Photographic] User Setting [User Setting]
Process Color Model	printer.PSSettings: 01.ProcessColorModel	Color [Color] Black & White [Black & White]
Orientation Auto Detect	printer.PSSettings: 01.OrientationAutoDetect	On [On] Off [Off]
Tray Parameters (Auto Select)	printer.PSTrayParameters: 01.AutoSelect	0 to 99
Tray Parameters (Tray 1 to Tray 7)	printer.PSTrayParameters: 01.Tray<N> (<N> represents a number between 1 and 7.)	0 to 99
Tray Parameters (Large Capacity Tray)	printer.PSTrayParameters: 01.LargeCapacityTray	0 to 99
Tray Parameters (Bypass Tray)	printer.PSTrayParameters: 01.BypassTray	0 to 99
<PDF Settings>		
Resolution	printer.PDFSettings:01.Resolution	300 x 300 [300 dpi] 600 x 600 [600 dpi Fast] 600 x 600 x 2 [600 dpi Standard] 1200 x 1200 [1200 dpi]
Color Settings	printer.PDFSettings:01.ColorSetting	None [None] Fine [Fine] Super Fine [Super Fine]

Configuration item	Attribute	Value
Color Profile	printer.PDFSettings:01.ColorProfile	Auto [Auto] Presentation [Presentation] Solid Color [Solid Color] Photographic [Photographic] User Setting [User Setting]
Process Color Model	printer.PDFSettings: 01.ProcessColorModel	Color [Color] Black & White [Black & White]
Orientation Auto Detect	printer.PDFSettings: 01.OrientationAutoDetect	On [On] Off [Off]
New PDF Fixed Password	printer.PDFSettings: 01.NewPDFFixedPassword	PDF password
New PDF Group Password	printer.PDFSettings: 01.NewPDFGroupPassword	PDF group password
<LDAP Server Settings>		
LDAP Server	ldapServer.ldapServer:01.option	TRUE [On] FALSE [Off]
<LDAP Server 1> to <LDAP Server 5>		
LDAP Server 1 to 5	ldapServer.ldapServerSetting:<xx> .ldapinfoRegistered (<xx> represents a number between 01 and 05.)	TRUE [Program] FALSE [Delete]
Identification Name	ldapServer.ldapServerSetting:<xx> .dispname (<xx> represents a number between 01 and 05.)	Name
Server Name	ldapServer.ldapServerSetting:<xx> .hostname (<xx> represents a number between 01 and 05.)	Server name

Configuration item	Attribute	Value
Search Base	ldapServer.ldapServerSetting:<xx> .dn (<xx> represents a number between 01 and 05.)	Search start point
Port Number	ldapServer.ldapServerSetting:<xx> .port (<xx> represents a number between 01 and 05.)	Port number
SSL	ldapServer.ldapServerSetting:<xx> .ssl (<xx> represents a number between 01 and 05.)	TRUE [On] FALSE [Off]
Authentication	ldapServer.ldapServerSetting:<xx> .bind (<xx> represents a number between 01 and 05.)	NONE [Off] SIMPLE [On] SASL [High Security] KERBEROS [Kerberos Authentication]
Authentication Realm	ldapServer.ldapServerSetting:<xx> .realm (<xx> represents a number between 01 and 05.)	REALM1 [Realm 1] to REALM5 [Realm 5]
User Name	ldapServer.ldapServerSetting:<xx> .userId (<xx> represents a number between 01 and 05.)	User name
Password	ldapServer.ldapServerSetting:<xx> .password (<xx> represents a number between 01 and 05.)	Password
Identification Name	ldapServer.ldapServerSetting:<xx> .cnAttr (<xx> represents a number between 01 and 05.)	Identification name

Configuration item	Attribute	Value
Email Address	ldapServer.ldapServerSetting:<xx> .mailAttr (<xx> represents a number between 01 and 05.)	Email address
Fax Number	ldapServer.ldapServerSetting:<xx> .faxAttr (<xx> represents a number between 01 and 05.)	Fax number
Company Name	ldapServer.ldapServerSetting:<xx> .oAttr (<xx> represents a number between 01 and 05.)	Company name
Department Name	ldapServer.ldapServerSetting:<xx> .ouAttr (<xx> represents a number between 01 and 05.)	Department name
Attribute	ldapServer.ldapServerSetting:<xx> .sub1Attr (<xx> represents a number between 01 and 05.)	Attribute
Key Display	ldapServer.ldapServerSetting:<xx> .sub1Attrdisp (<xx> represents a number between 01 and 05.)	Key display
<Authentication Realm Settings 1> to <Authentication Realm Settings 5>		
Realm Name	system.userauthKerberosRealm:<xx> >.realmName (<xx> represents a number between 01 and 05.)	Realm name
KDC Server Name	system.userauthKerberosRealm:<xx> >.kdcServerName (<xx> represents a number between 01 and 05.)	KDC server name

Configuration item	Attribute	Value
Domain Name	system.userauthKerberosRealm:<xx>.domain (<xx> represents a number between 01 and 05.)	Domain name
<Firmware Update Settings>		
Permit Firmware Update	system.commonBase:01.firmUpdate	TRUE [On] FALSE [Off]
Permit Firmware Structure Change	system.commonBase:01.compChange	TRUE [On] FALSE [Off]
<User Lockout Policy>		
User Lockout Policy	system.secPasswordLock:01.lockEnable	TRUE [On] FALSE [Off]
Number of Attempts before Lockout	system.secPasswordLock:01.lockTimes	1 to 10
Lockout Release Timer	system.secPasswordLock:01.lockReleaseEnable	TRUE [On] FALSE [Off]
Lock Out User for	system.secPasswordLock:01.lockReleaseTime	1 to 9999
<Interface Settings>		
Ethernet Speed	network.ifEthernet:01.ifEtherSpeed	ETHER_SPEED_AUTO_SELECT [Auto Select] ETHER_SPEED_100M_FULL [100Mbps Full Duplex] ETHER_SPEED_100M_HALF [100Mbps Half Duplex] ETHER_SPEED_10M_FULL [10Mbps Full Duplex] ETHER_SPEED_10M_HALF [10Mbps Half Duplex]
<Device Functions>		

Configuration item	Attribute	Value
SDK/J Platform	sdk.sdkSetting:01.JavaVMOnOff	Off [Disable] On [Enable]
<Web Browser NX>		
Action	browserNx:Action_<xxx> (<xxx> represents a number between 001 and 099.)	Add/Edit [Add] or [edit] Delete [Delete]
Title	browserNx:Title_<xxx> (<xxx> represents a number between 001 and 099.)	"Icon name" Up to 254 characters can be entered. \$, ¥, ", and ' cannot be used.
URL	browserNx:Url0<n>_<xxx> (<n> represents a number between 1 and 7.) (<xxx> represents a number between 001 and 099.)	"The URL of the shortcut"

To specify the paper type for a paper tray in a CSV file, specify the values according to the following table:

#### Value and paper type of "inputTray:<xx>.InputMediaTypeCurrent"

Value	Paper Type	Value	Paper Type
1	Plain Paper	4096	Thick Paper
2	Recycled Paper	8192	Plain Paper: Back Side
4	Special Paper	16384	Thick Paper: Back Side
8	Color Paper	32768	Thin Paper
16	Letterhead	66536	Glossy Paper
32	Preprinted Paper	131072	Translucent Paper
64	Prepunched Paper	262144	Back Copied Paper
128	Label Paper	524288	Color Paper 1
256	Bond Paper	1048576	Color Paper 2



Value	Paper Type	Value	Paper Type
512	Cardstock	2097152	Postcard
1024	Tab Stock	4194304	Postcard: Back Side
2048	OHP (Transparency)		

**Value and paper type of "inputTray:<xx>.InputMediaTypeCurrent2"**

Value	Paper Type	Value	Paper Type
0000000001	White	0000000000000001	Plain Paper 2
0000000002	Yellow	0000000000000002	Coated Paper 2
0000000004	Green	0000000000000004	Coated Paper 3
0000000008	Blue	0000000000000008	Special Paper 5
0000000010	Purple	0000000000000010	Special Paper 6
0000000020	Ivory	0000000000000020	Thick Glossy Paper
0000000040	Orange	0000000000000040	Coated Paper: Gloss Print
0000000080	Pink	0000000000000080	Coated Paper (Glossy)
000000000001	Red	000000000000000001	Coated Paper (Glossy: Thick Paper)
000000000002	Gray	000000000000000002	Coated Paper (Matted)
000000000004	Thick Paper 2	000000000000000004	Coated Paper (Matted: Thick Paper)
000000000008	Film	000000000000000008	Waterproof Paper
000000000010	Envelope	000000000000000010	Thick Paper 4
000000000020	Inkjet Postcard	000000000000000020	Thick Paper 4: Back Side
000000000040	HG Plain Paper	000000000000000040	Plain Paper/Recycled Paper

Value	Paper Type	Value	Paper Type
0000000000080	Thick Paper 3	0000000000000000000080	Coated Paper (High Gloss)
000000000000001	Special Paper 2	000000000000000000000001	Color Paper 3
000000000000002	Special Paper 3	000000000000000000000002	Inkjet Plain
000000000000004	Middle Thick Paper	000000000000000000000004	Translucent Paper (Black & White)
000000000000008	Special Paper 4	000000000000000000000008	Translucent Paper (Color)
000000000000010	Coated Paper	000000000000000000000010	Film (Matted)
000000000000020	Thick Paper 2: Back Side	000000000000000000000020	Coated Paper (CAD)
000000000000040	Thick Paper 3: Back Side	000000000000000000000040	Glossy Photo Paper/ Semi-Glossy Paper
000000000000080	Plain Paper 1		

#### ↓ Note

- Do not change the information in lines through three, as this information is used for identification.
- For details about the configuration items, see page 157 "List of Device Preference Setting Items".

## 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:

### general

Field name	Explanation
general#logVersion	log version number
general#logSourceId	device serial number
general#logSourceId_sld	device alias ID

Field name	Explanation
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
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

Field name	Explanation
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
general#sdkApplInfo	SDK 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 Device Manager 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)

Field name	Explanation
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)
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_scan#scanSettingPoster	poster

**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

Field name	Explanation
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
source_memory#srcMemCreateTime	create time
source_memory#srcMemTrackId	track ID
source_memory#srcMemPdIdDocumentName	print document name
source_memory#srcMemPcLoginName	login name
source_memory#srcMemPcLoginName_sld	alias ID of the login name
source_memory#srcMemPcName	computer name
source_memory#srcMemPcName_sld	alias ID of the computer name
source_memory#srcMemPcLoginComp_sld	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
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

Field name	Explanation
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)
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_sld	alias ID of the login name



Field name	Explanation
source_pdl#pdlPcName	computer name
source_pdl#pdlPcName_sld	alias ID of the computer name
source_pdl#pdlPcLoginComp_sld	alias ID of the login name and computer name
source_pdl#pdlPcPortName	port name
source_pdl#pdlPcPrinterName	printer icon name
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

Field name	Explanation
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)
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

Field name	Explanation
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)
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)

Field name	Explanation
destination_plot#plotStartTime_c	start time (corrected by service)
destination_plot#plotStartValidTimeFlag	reliability of corresponding start time information
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 info two-color large sizes
destination_plot#plotPrintCount2Cb	print count info two-color small sizes
destination_plot#plotPrintCountFCa	print count info full color large sizes
destination_plot#plotPrintCountFCb	print count info full color small sizes
destination_plot#plotPrint-CountYMC	print count info color (YMC) development

Field name	Explanation
destination_plot#plotPrintCountBK	print count infoblack development
destination_plot#plotBindbook	booklet
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
destination_plot#plotStapleMode	staple mode

# Command Line Tools

Where Device Manager NX is not launched as an application from the Start menu, its functions can still be accessed by using it as a Windows service. Operating Device Manager NX as a service allows you to run tasks such as creating reports and conducting polling without launching the application. This makes operation more convenient by preventing problems such as failing to run tasks.

The four command line tools shown below are provided so that Device Manager NX will operate as a Windows service.

## ★ Important

- To use the tools, log in with administrative privileges.
- This function can be used in Device Manager NX Accounting. It is not available in Device Manager NX Lite.
- Before running this function, stop Device Manager NX Accounting.
- If you use this function to switch to service operation, the procedure for launching Device Manager NX Accounting does not change.
- During service operation, "Device Manager NX Accounting (Service)" is displayed as the product name in the window title.
- The pop-up function for notification messages cannot be used during service operation. To use the pop-up function for notification messages, first launch Device Manager NX Accounting.
- During service operations, a network drive cannot be specified as the save destination of reports. If a network drive has already been specified as the destination, an error will occur, and the report will not be saved.

### Batch file for registration as a service

Registers Device Manager NX in the Windows services.

For details, see page 229 "Batch File for Registration as a Service".

### Batch file for canceling registration as a service

Removes Device Manager NX from the Windows services.

For details, see page 229 "Batch File for Canceling Registration as a Service".

### Batch file for starting the service

Starts Device Manager NX as a Windows service.

For details, see page 229 "Batch File for Starting the Service".

### Batch file for stopping the service

Stops Device Manager NX as a Windows service.

For details, see page 230 "Batch File for Stopping the Service".

---

## Batch File for Registration as a Service

---

Use the procedure below to register Device Manager NX to the Windows services using the command prompt.

**1. Open the command prompt and go to the "tools\service" folder in the installation path for Device Manager NX.**

The default path is "C: \Program Files\Ricoh\MDM\tools\service", but the actual path may differ depending on the installation method used.

**2. Execute the "install.bat" command.**

**Note**

- "RICOH MDM Central Manager Service" and "RICOH MDM Device Manager Service" are added to the Windows services.
- The "Startup Type" and "Log On" settings for the two added services are as follows:
  - Startup Type: Automatic
  - Log On: Local System account

---

## Batch File for Canceling Registration as a Service

---

Use the procedure below to remove Device Manager NX from the Windows services using the command prompt.

**1. Open the command prompt and go to the "tools\service" folder in the installation path for Device Manager NX.**

The default path is "C: \Program Files\Ricoh\MDM\tools\service", but the actual path may differ depending on the installation method used.

**2. Execute the "uninstall.bat" command.**

**Note**

- "RICOH MDM Central Manager Service" and "RICOH MDM Device Manager Service" are removed from the Windows services.
- Device Manager NX cannot be updated or uninstalled while it is registered as a Windows service. To update or uninstall it, cancel the registration as a service.

---

## Batch File for Starting the Service

---

To start a Windows service that was stopped to run Device Manager NX for data backup or recovery, run the batch file for starting the service.

Use the procedure below to start Device Manager NX as a Windows service using the command prompt.

**1. Open the command prompt and go to the "tools\service" folder in the installation path for Device Manager NX.**

The default path is "C: \Program Files\Ricoh\MDM\tools\service", but the actual path may differ depending on the installation method used.

**2. Execute the "start.bat" command.**

**↓ Note**

- "RICOH MDM Central Manager Service" and "RICOH MDM Device Manager Service" start.

---

## Batch File for Stopping the Service

---

To run Device Manager NX for data backup or recovery while a Windows service is running, stop the service.

Use the procedure below to stop Device Manager NX as a Windows service using the command prompt.

**1. Open the command prompt and go to the "tools\service" folder in the installation path for Device Manager NX.**

The default path is "C: \Program Files\Ricoh\MDM\tools\service", but the actual path may differ depending on the installation method used.

**2. Execute the "stop.bat" command.**

**↓ Note**

- "RICOH MDM Central Manager Service" and "RICOH MDM Device Manager Service" stop.



# Troubleshooting

Problem	Causes and solutions
A device on the network is not detected.	<ul style="list-style-type: none"> <li>• 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.</li> <li>• Check the discovery range. For details, see page 22 "Searching for Devices".</li> </ul>
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.
Devices are not added to a group.	Devices are added automatically to a manual group. To add a device to a group, drag a device from the device list and drop it in the group (folder) to which the device is to be added.
Batch settings using a template cannot be performed.	<ul style="list-style-type: none"> <li>• Check that the access account has been correctly set.</li> <li>• Correctly set the access account, and overwrite the access account of the target device. For details, see page 19 "Configuring Access Accounts".</li> </ul>
Backup has failed.	<ul style="list-style-type: none"> <li>• Quit Device Manager NX before performing a backup.</li> <li>• Check the destination to save the backup file. Create a new folder as the destination for saving the backup file.</li> <li>• Device Manager NX cannot be backed up while it is used as a service. If it is being used as a service, stop the service before executing the backup.</li> </ul>
Restore has failed.	Device Manager NX cannot be restored while it is used as a service. If it is being used as a service, stop the service before restoring the system.

Problem	Causes and solutions
<p>The number of remaining licenses does not increase even if applications are deactivated/uninstalled.</p>	<p>Deactivation between the target device and the RICOH Software Server was not correctly processed.</p> <p>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.</p>
<p>An access account cannot be deleted.</p>	<p>An access account cannot be deleted if it's in any of the following conditions:</p> <ul style="list-style-type: none"> <li>• The account is assigned to a profile in [Administrator] or [SNMP] category in a [Basic Device Preferences] template.</li> <li>• The account is assigned to the access account of discovery task.</li> <li>• The account is assigned to the access account in any of the device that is displayed in the device list.</li> </ul> <p>In order to delete an access account, it must be released from those assignments.</p>

# Trademarks

Firefox® is a registered trademark of the Mozilla Foundation.

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

Safari is a trademark of Apple Inc., registered in the U.S. and other countries.

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

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 Enterprise
  - Microsoft® Windows® 10 Education
- The product names of Windows Server 2012 are as follows:
  - Microsoft® Windows Server® 2012 Essentials
  - Microsoft® Windows Server® 2012 Standard
- The product names of Windows Server 2012 R2 are as follows:
  - Microsoft® Windows Server® 2012 R2 Essentials

Microsoft® Windows Server® 2012 R2 Standard

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

Microsoft® Windows Server® 2016 Essentials

Microsoft® Windows Server® 2016 Standard

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

---

MEMO

---

MEMO



