# Device Manager NX Enterprise
# Important Information about Device Configuration

*Complete View of Your Fleet Status*

# Copyrights/Trademarks/Patents



# Revision History

| Date | Revision No. | Revision Details |
|---|---|---|
| Aug. 2013 | 1.0 | First release of document |
| May 2014 | 1.1 | Second release of document |
| Mar. 2016 | 1.2 | Third release of document |
| | | |

*Some illustrations or explanations in this document may differ from your product due to improvement or change in the product. Contents of this document are subject to change without notice.*

# Contents

# Introduction

With the Device Manager NX Enterprise (herein called "DMNX"), extended functions can be set remotely by using DMNX Management Extension. These extended functions, which are described in this document, are special functions that have not been released to users in the past. Caution must be taken when using these special functions as there are restrictions on the setting methods, the behavior of the device(s) which will be affected by these settings, etc.
This document includes important information such as the setting methods and restrictions. Be sure to read this document before configuring these functions.

## Important Notes

- Each function is executed using DMNX Management Extension (Java applet). Therefore, these functions can only be used on Ricoh devices released in autumn 2007 or later, which are equipped with Java virtual machines (devices equipped with Device SDK Type-J*). For details, please check your local Ricoh website for a list of supported devices or contact the Ricoh Group.
  * Architecture for running Java applications on the Java virtual machine installed in the device. "SDK" stands for "Software Development Kit".
- Currently, these functions cannot be used on devices with a 4-line or 2-line LCD panel.
- When these functions are used, the Java applet is sent from DMNX to each individual device and installation to the device starts automatically. If you wish to uninstall the Java applet from the device, you must create an uninstall template using DMNX and then execute the uninstall template. Refer to the *DMNX Administration Guide* for information on how to create an uninstall template.
- Settings required for DMNX Management Extension are indicated by a dagger mark (†). (Refer to the screenshots in this document.)

# 1. Preparations

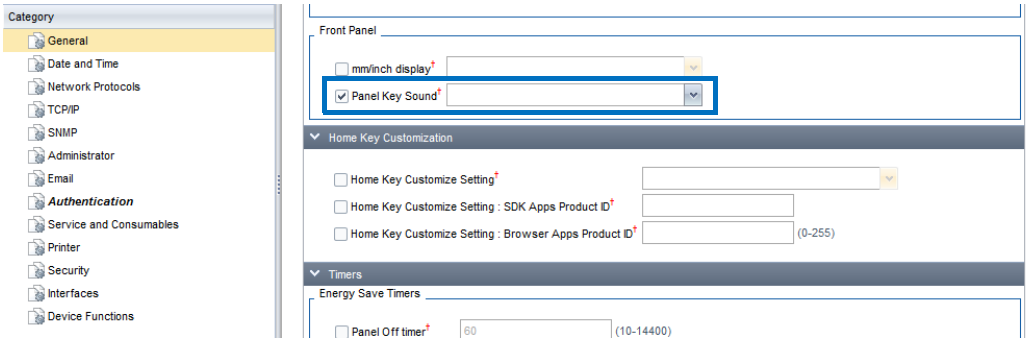
- At the time of DMNX installation, enable the **Enable DMNX Management Extension** checkbox. By enabling this checkbox, DMNX Management Extension will simultaneously be installed with DMNX and remote configuration of the extended functions will become possible.
  This setting can also be changed after DMNX installation. From the Navigation Tree for DMNX, select **System → Server Settings → System Information and Settings**, and enable the **Enable DMNX Management Extension for Configuration Templates** checkbox in **Server Settings**. Refer to the *DMNX Administration Guide* for details.
- A "Standard Device Preferences" template for configuring each function must be created using DMNX. Refer to the *DMNX Administration Guide* for information on how to create a "Standard Device Preferences" template.

# 2. General

This section includes information on the extended functions available for the **General** category.

## 2.1 Panel Key Sound

You can select whether to turn the key sound on or off for when the soft keys on the panel of the device are pressed.




### ■Configuring the Setting

1. Enable the **Panel Key Sound** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **On [simple]** | A sound is emitted when a soft key is pressed. The volume is set automatically. |
| **Off** | No sound is emitted when a soft key is pressed. |
| **Lowest** | When a soft key is pressed, a sound is emitted at the lowest volume level. |
| **Low** | When a soft key is pressed, a sound is emitted at low volume level. |
| **Medium** | When a soft key is pressed, a sound is emitted at medium volume level. |
| **High** | When a soft key is pressed, a sound is emitted at high volume level. |

### ■Related Functions

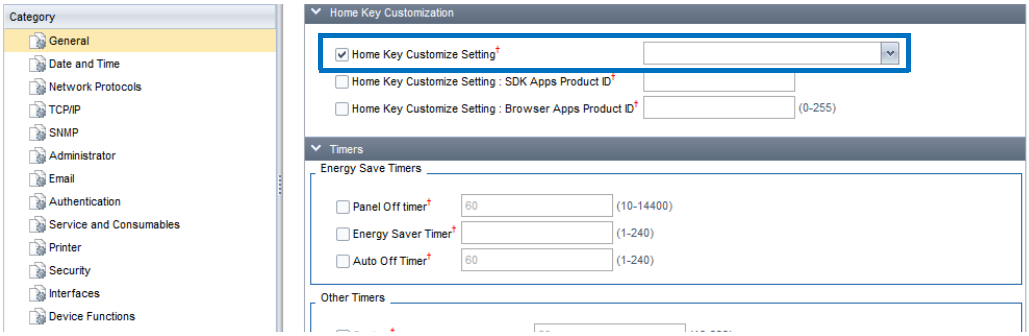
None

### ■Restrictions

- The settings available for this function differ depending on the device used. For details, contact the Ricoh Group.

## 2.2 Home Key Customize Setting

You can configure devices to launch an SDK application (Device SDK Type-J Application) or a browser application when the device's Home key is pressed.




### ■Configuring the Setting

1. Enable the **Home Key Customize Setting** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Disable** | No application will launch. |
| **SDK** | The SDK application specified in **Home Key Customize Setting: SDK Apps Product ID** will launch. |

### ■Related Functions

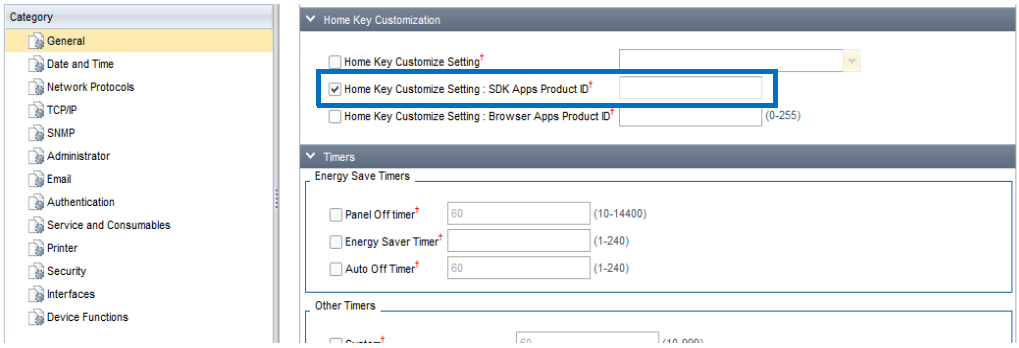
- 2.3 "Home Key Customize Setting: SDK Apps Product ID" (☞ page 9)

### ■Restrictions

- The **Disable** and **SDK** settings are only available for devices released in autumn 2011 or later. For details, please check your local Ricoh website for a list of supported devices or contact the Ricoh Group.

## 2.3 Home Key Customize Setting: SDK Apps Product ID

You can specify the SDK application (Device SDK Type-J Application) that is launched when the device's Home key is pressed.




### ■Configuring the Setting

1. Select **SDK** of **Home Key Customize Setting**.
2. Enable the **Home Key Customize Setting: SDK Apps Product ID** checkbox.
3. In the field, enter the product ID of the SDK application.

### ■Related Functions

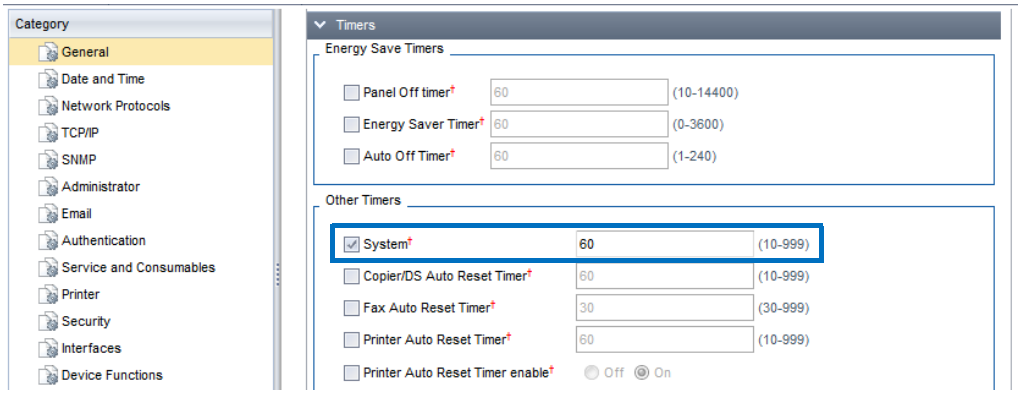
- 2.2 "Home Key Customize Setting" (☞ page 8)

### ■Restrictions

- This function is only available for devices released in autumn 2011 or later. For details, please check your local Ricoh website for a list of supported devices or contact the Ricoh Group.
- Device SDK Type-C Applications will not launch even if the product ID is entered.

## 2.4 Other Timers: System Auto Reset Timer Setting

You can specify how long the device waits before automatically changing to the screen of the specified application.




### ■Configuring the Setting

1. Enable the **System** checkbox.
2. Specify a value between 10 and 999 seconds to set for **System Auto Reset Timer**.

### ■Related Functions

None

### ■Restrictions

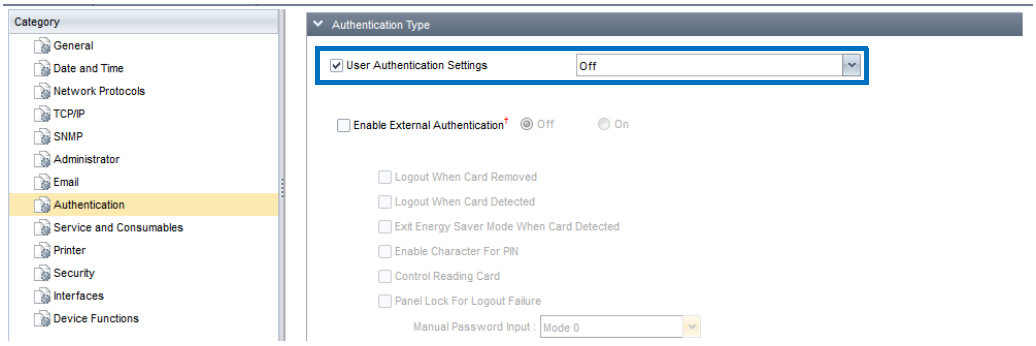
- This function cannot be used on Pro 8110/8120 and MP CW2200.

# 3. Authentication

This section includes information on the extended functions available for the **Authentication** category.

## 3.1 User Authentication Settings

You can select whether to perform user authentication as well as the authentication method to use.
The authentication setting made here is applied to each of the following applications: Copier, Document Server, Fax, Printer, and Scanner. By using functions such as **Disable authentication: Copy**, authentication can be enabled or disabled separately for each individual application.




### ■Configuring the Setting

1. Enable the **User Authentication Settings** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Off** | User authentication is not performed. |
| **User Code Authentication** | User code authentication is performed. |
| **Basic Authentication** | Basic authentication is performed. |
| **Windows Authentication** | Windows authentication is performed. |
| **LDAP Authentication** | LDAP authentication is performed. |
| **Integration Server Authentication** | Integration server authentication is performed. |

## ■Related Functions

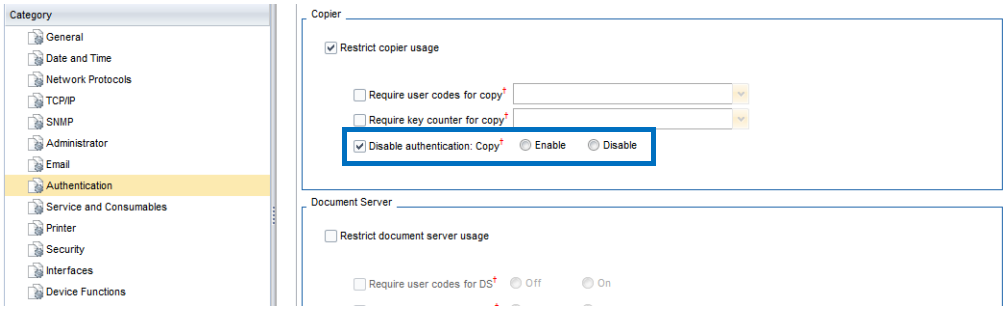
- 3.2 “Disable Authentication: Copy” (☞ page 14)
- 3.3 “Disable Authentication: DS” (☞ page 15)
- 3.4 “Disable Authentication: Fax”(☞ page 16)
- 3.5 “Disable Authentication: Printer” (☞ page 17)
- 3.6 “Disable Authentication: Scanner” (☞ page 18)

## ■Restrictions

None

## 3.2 Disable Authentication: Copy

You can select whether authentication is performed for the Copier application. This function is available when **User Authentication Settings** is not set to **Off**.




### ■Configuring the Setting

1. Enable the **Restrict copier usage** checkbox.
2. Enable the **Disable authentication: Copy** checkbox.
3. Select a setting.

| Setting | Description |
|---|---|
| **Enable** | User authentication is performed. |
| **Disable** | User authentication is not performed. |

### ■Related Functions

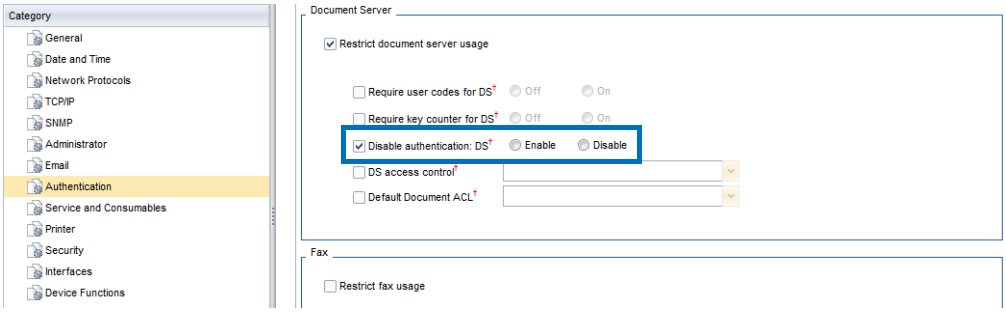
- 3.1 “User Authentication Settings” (☞ page 12)

### ■Restrictions

None

## 3.3 Disable Authentication: DS

You can select whether authentication is performed for the Document Server application.
This function is available when **User Authentication Settings** is not set to **Off**.




### ■Configuring the Setting

1. Enable the **Restrict document server usage** checkbox.
2. Enable the **Disable authentication: DS** checkbox.
3. Select a setting.

| Setting | Description |
|---|---|
| **Enable** | User authentication is performed. |
| **Disable** | User authentication is not performed. |

### ■Related Functions

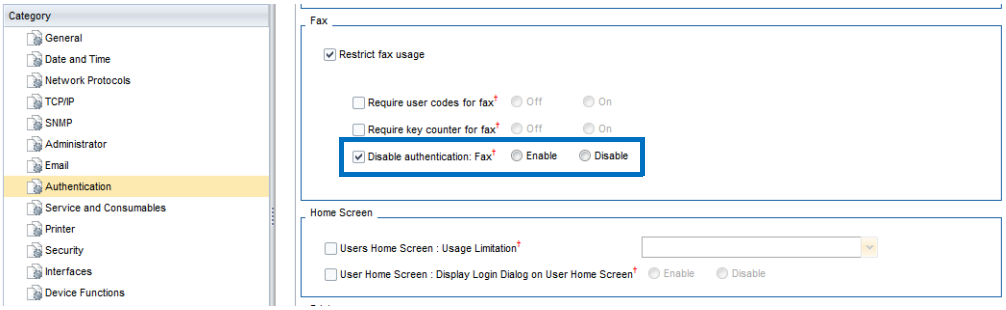
- 3.1 "User Authentication Settings" (☞ page 12)

### ■Restrictions

None

## 3.4 Disable Authentication: Fax

You can select whether authentication is performed for the Fax application.
This function is available when **User Authentication Settings** is not set to **Off**.




### ■Configuring the Setting

1. Enable the **Restrict fax usage** checkbox.
2. Enable the **Disable authentication: Fax** checkbox.
3. Select a setting.

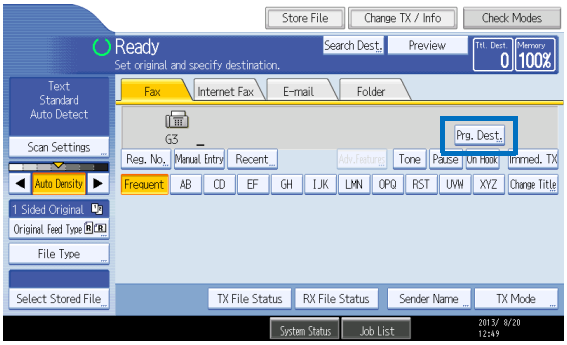
| Setting | Description |
|---|---|
| **Enable** | User authentication is performed. |
| **Disable** | User authentication is not performed. |

### ■Related Functions

- 3.1 “User Authentication Settings” (☞ page 12)

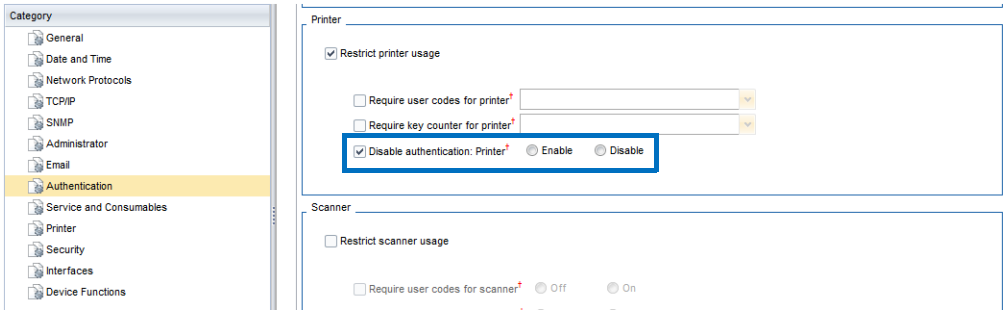
### ■Restrictions

- When **Disable** is set, the “**Prg. Dest.**” button shown on the LCD panel of the MFP will not function.



## 3.5 Disable Authentication: Printer

You can select whether authentication is performed for the Printer application. This function is available when **User Authentication Settings** is not set to **Off**.




### ■Configuring the Setting

1. Enable the **Restrict printer usage** checkbox.
2. Enable the **Disable authentication: Printer** checkbox.
3. Select a setting.

| Setting | Description |
|---|---|
| **Enable** | User authentication is performed. |
| **Disable** | User authentication is not performed. |

### ■Related Functions

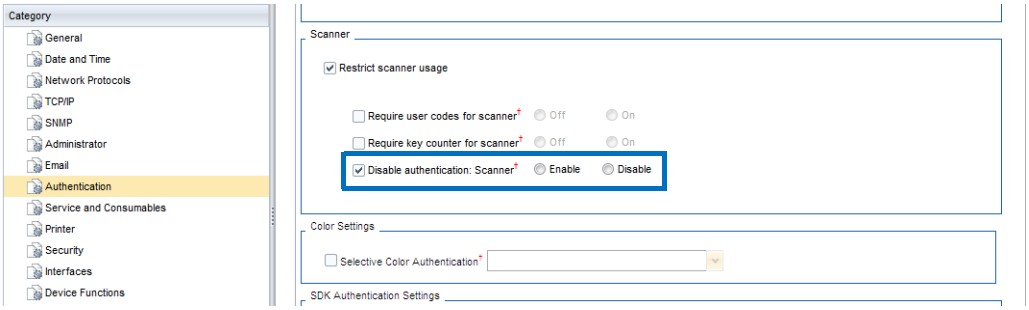
- 3.1 "User Authentication Settings" (☞ page 12)

### ■Restrictions

None

## 3.6 Disable Authentication: Scanner

You can select whether authentication is performed for the Scanner application. This function is available when **User Authentication Settings** is not set to **Off**.




### ■Configuring the Setting

1. Enable the **Restrict scanner usage** checkbox.
2. Enable the **Disable authentication: Scanner** checkbox.
3. Select a setting.

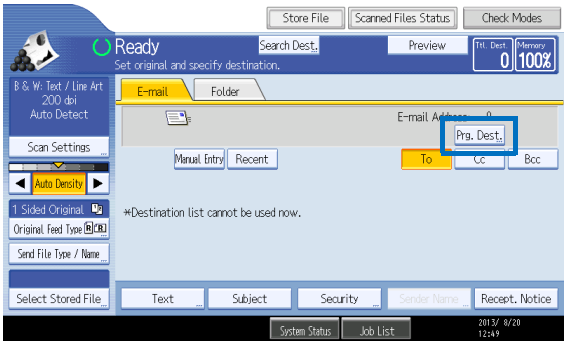
| Setting | Description |
|---|---|
| **Enable** | User authentication is performed. |
| **Disable** | User authentication is not performed. |

### ■Related Functions

- 3.1 "User Authentication Settings" (☞ page 12)

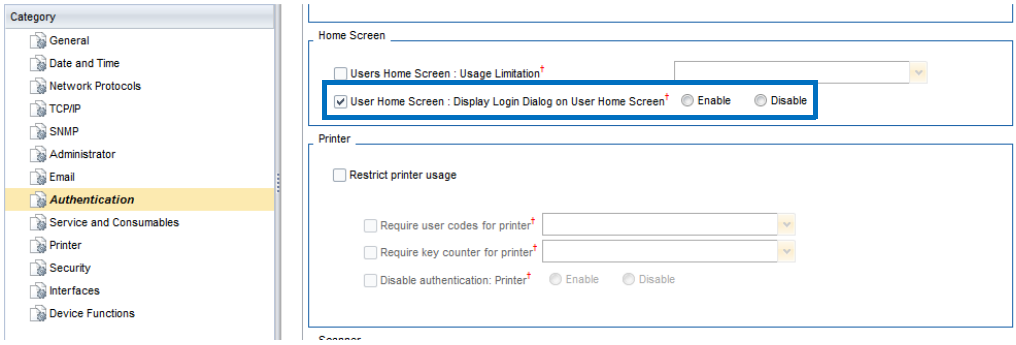
### ■Restrictions

- When **Disable** is set, the "**Prg. Dest.**" button shown on the LCD panel of the MFP will not function.



## 3.7 User Home Screen: Display Login Dialog on User Home Screen

You can select whether to display the Authentication screen on the device's Home screen.




### ■Configuring the Setting

1. Enable the **User Home Screen: Display Login Dialog on User Home Screen** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Enable** | The Authentication screen is displayed on the Home screen. |
| **Disable** | The Authentication screen is not displayed on the Home screen. |

Set this function to **Disable** if authentication is disabled for any one of the Copier, Document Server, Fax, Printer, or Scanner applications. If it is set to **Enable**, since the Authentication screen will be displayed when the Home screen is shown even if authentication is not performed for the application, you will not be able to view the application screen without performing authentication.

### ■Related Functions

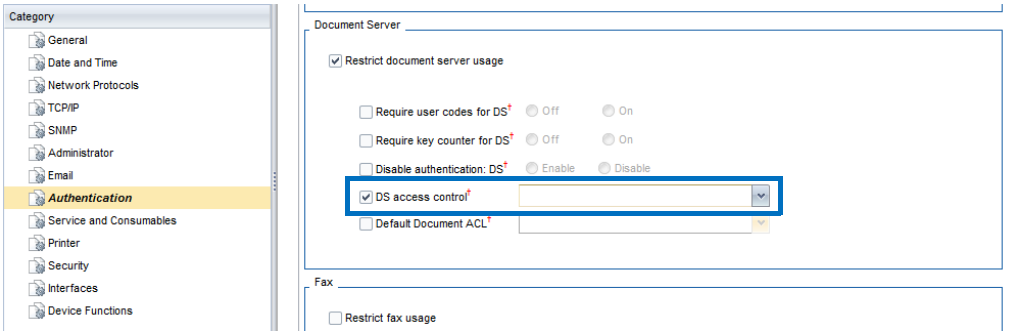
- 3.1 "User Authentication Settings" (☞ page 12)
- 3.2 "Disable Authentication: Copy" (☞ page 14)
- 3.3 "Disable Authentication: DS" (☞ page 15)
- 3.4 "Disable Authentication: Fax"(☞ page 16)
- 3.5 "Disable Authentication: Printer" (☞ page 17)
- 3.6 "Disable Authentication: Scanner" (☞ page 18)

## ■Restrictions

- This function is only available for devices released in autumn 2011 or later (devices with Home screen display). For details, please check your local Ricoh website for a list of supported devices or contact the Ricoh Group.

## 3.8 DS Access Control

You can control who can access the Document Server on the Web Image Monitor (WIM). The Document Server functions can also be controlled.




### ■Configuring the Setting

1. Enable the **Restrict document server usage** checkbox.
2. Enable the **DS access control** checkbox.
3. Enable the checkbox for the setting you want to apply.

| Setting | Description |
|---|---|
| **Deny all WIM access** | The administrator and all users are not permitted to access the Document Server on WIM. (The "Document Server" menu and the various logs for "Document Server" on the "Job" screen will not be displayed.) |
| **Deny user WIM access but allow admin access** | All users except the administrator are not permitted to access the Document Server on WIM. (The "Document Server" menu and the various logs for "Document Server" on the "Job" screen will not be displayed.) |
| **Hide print icon and print job history** | The "Print" button is not displayed in the Document Server document list screen for the administrator and all users. Also, "Print Job History" for "Document Server" is not displayed on the "Job" screen. |

| Setting | Description |
|---|---|
| **Hide fax remote send history** | "Fax Remote Send History" for "Document Server" on the "Job" screen is not displayed for the administrator and all users.<br>When the device's fax transmission function is disabled or the device is not equipped with a fax, the "Send" button will not appear in the Document Server document list. |
| **Hide scanner remote send history** | "Scanner Remote Send History" for "Document Server" on the "Job" screen is not displayed for the administrator and all users.<br>When the device's scan transmission function is disabled or the device is not equipped with a scanner, the "Send" button will not appear in the Document Server document list. |
| **Hide download in document list and in file details** | The "Download" button is not displayed in the Document Server document list screen or the File Details screen for the administrator and all users. |
| **Hide delete icon** | The "Delete" button is not displayed in the Document Server document list screen for the administrator and all users. |
| **Disallow guest access** | Unauthenticated users (GUEST) cannot access the Document Server on WIM. (The "Document Server" menu and the various logs for "Document Server" on the "Job" screen will not be displayed.) |

Whether the "Document Server" menu and "Print Job History", "Fax Remote Send History", and "Scanner Remote Send History" for "Document Server" on the "Job" screen are displayed, depends on the combination of the following conditions and the user's privileges:

- **Deny user WIM access but allow admin access** settings
- **Disallow guest access** settings
- Authentication function setting

✓: Content displayed

| | | Adminis-trator | Authenti-cated user | Unauthen-ticated user (GUEST) |
|---|---|---|---|---|
| Deny user WIM access but allow admin access: Disabled Disallow guest access: Disabled | Authentication function: Enabled | ✓ | ✓ | |
| | Authentication function: Disabled | ✓ | ✓ | ✓ |
| Deny user WIM access but allow admin access: Enabled Disallow guest access: Disabled | Authentication function: Enabled | ✓ | | |
| | Authentication function: Disabled | ✓ | | |
| Deny user WIM access but allow admin access: Disabled Disallow guest access: Enabled | Authentication function: Enabled | ✓ | ✓ | |
| | Authentication function: Disabled | ✓ | ✓ | |
| Deny user WIM access but allow admin access: Enabled Disallow guest access: Enabled | Authentication function: Enabled | ✓ | | |
| | Authentication function: Disabled | ✓ | | |

## ■Related Functions

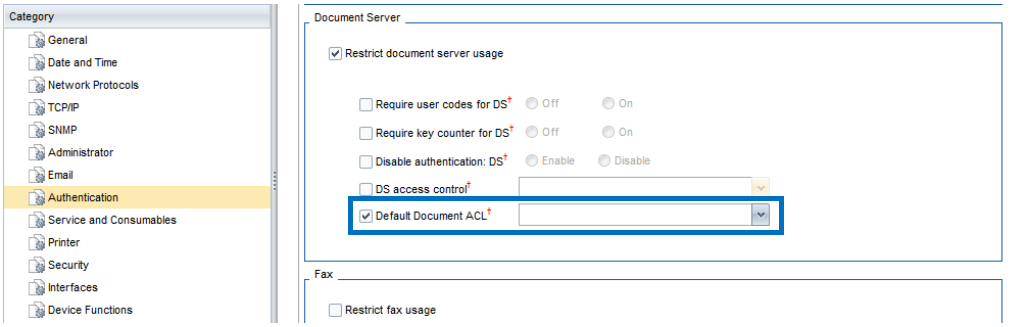
None

## ■Restrictions

- This function will become effective after the device reboots.

## 3.9 Default Document ACL

You can set default user access privileges for a document when it is newly stored to the device's Document Server. This function can be used when external authentication such as Windows authentication, LDAP authentication, and RDH authentication is performed.
However, the user who stored the document is given owner privileges and is not affected by this function.




### ■Configuring the Setting

1. Enable the **Restrict document server usage** checkbox.
2. Enable the **Default Document ACL** checkbox.
3. Select a setting.

| Setting | Description |
|---|---|
| **Read-only** | Users are only permitted to view the documents. |
| **Edit** | Users are permitted to edit the documents. However, they cannot delete documents. |
| **Edit/Delete** | Users are permitted to edit and delete documents. |
| **Full control** | Users are permitted to perform all operations permitted to the document owner. Users are able to perform all operations including changing the access privileges of the document. |

If Card Authentication Package V2 has been implemented, select **Full control**.

### ■Related Functions

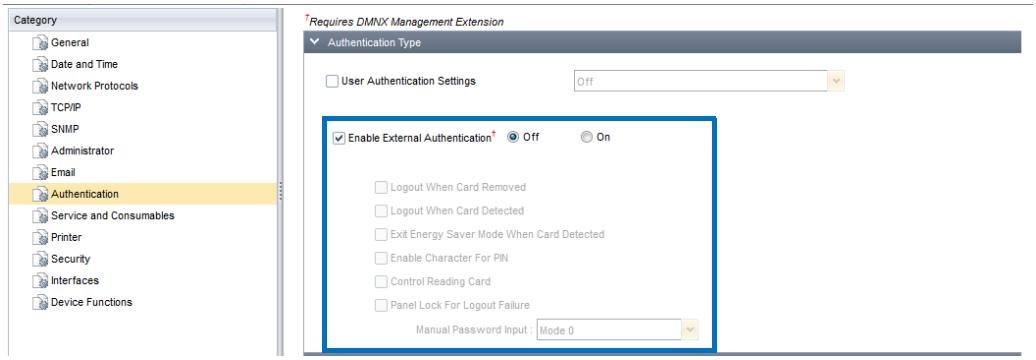
None

### ■Restrictions

- This function is not available for devices that are not equipped with a Document Server.

## 3.10 Enable External Authentication

You can configure extended authentication that uses an IC card.




### ■Configuring the Setting

1. Enable the **Enable External Authentication** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Off** | Extended authentication is not used. |
| **On** | Extended authentication is used. |

3. When **Enable External Authentication** is set to **On**, enable the checkbox for the setting you want to apply. For **Manual Password Input**, select a setting.

| Setting | Description |
|---|---|
| **Logout When Card Removed** | The user remains logged in while the IC card is in contact with the card reader. The user is logged out when the IC card is removed from the card reader.<br>**Logout When Card Detected** cannot be enabled at the same time. |
| **Logout When Card Detected** | The user is logged out when the IC card is held against the card reader while the user is logged in. This is a setting for contactless IC cards.<br>**Logout When Card Removed** cannot be enabled at the same time. |
| **Exit Energy Saver Mode When Card Detected** | You can select whether to set the device to recover from Energy Saver Mode when the IC card is held against the card reader. This is a setting for contactless IC cards. |
| **Enable Character For PIN** | Enables entering alphabetical characters in addition to numbers for the password. |

| Setting | Description | |
|---|---|---|
| **Control Reading Card** | The cache for the IC card's login ID and password is used for login. Use this setting when the authentication process takes time. | |
| **Panel Lock For Logout Failure** | This setting prevents other users from logging in before the logout process is completed. Use this setting when the logout process takes time. | |
| **Manual Password Input** | You can set whether to require the users to enter a password when they hold up their IC card against the card reader. | |
| | **Mode 0** | The Password Entry screen is not displayed. |
| | **Mode 1** | The Password Entry screen is displayed with the entry field blank. |
| | **Mode 2** | The Password Entry screen is displayed with the password retrieved from the IC card entered in the entry field (the password will appear as asterisks). The number of asterisks shown is the maximum number of characters possible for the password. |
| | **Mode 3** | The Password Entry screen is only displayed when the password cannot be retrieved from the IC card. The entry field will be blank. |

If Card Authentication Package V2 has been implemented, it is recommended that the following settings be used:

- **Logout When Card Removed**: Enable
- **Manual Password Input**: **Mode 0** or **Mode 2**

## ■Related Functions

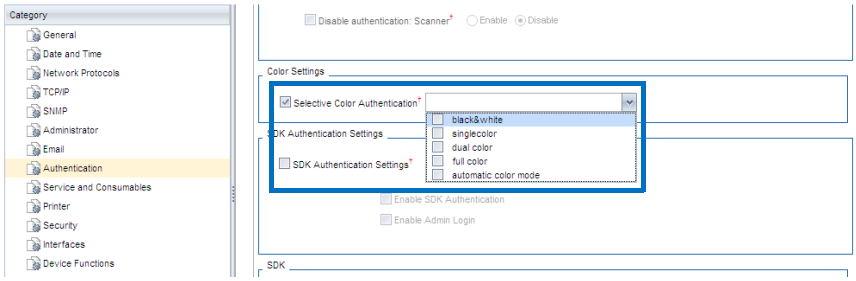
None

## ■Restrictions

- The **Manual Password Input**, **Enable Character For PIN**, and **Control Reading Card** settings are only available for devices released in spring 2009 or later. And the **Panel Lock For Logout Failure** setting is only available for devices released in autumn 2012 and later (with exceptions). For details, please check your local Ricoh website for a list of supported devices or contact the Ricoh Group.

## 3.11 Selective Color Authentication

You can select whether authentication is performed for each color mode in the Copier application.
This function is available when User Authentication settings for the Copier application is not set to off.




### ■Configuring the Setting

1. Enable the **Selective Color Authentication** checkbox.
2. Enable the checkbox of the color mode for which you want to perform authentication.

| Setting | Description |
|---|---|
| **black&white** | Authentication is performed when using the Black & White mode. |
| **single color** | Authentication is performed when using the Single Color mode. |
| **dual color** | Authentication is performed when using the Two-color mode. |
| **full color** | Authentication is performed when using the Full Color mode. |
| **automatic color mode** | Authentication is performed when using the Auto Color mode. |

### ■Related Functions

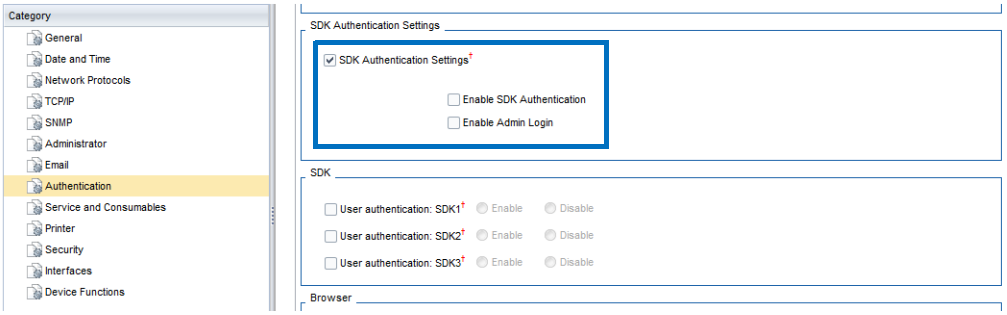
- 3.2 “Disable Authentication: Copy” (☞ page 14)

### ■Restrictions

None

## 3.12 SDK Authentication Settings

You can configure external authentication that uses an SDK application.




### ■Configuring the Setting

1. Enable the **SDK Authentication Settings** checkbox.
2. Enable the checkbox for the setting you want to apply.

| Setting | Description |
|---|---|
| **Enable SDK Authentication** | Enables the use of a server that performs external authentication using an SDK application.<br>In order to make the settings effective, select **LDAP Authentication** in **User Authentication Settings**.<br>To use an authentication method other than LDAP authentication, disable this setting. |
| **Enable Admin Login** | The server that performs external authentication using an SDK application is given the same administrative privileges as the Address Book in the device. Enabling this setting will allow operations that require administrative privileges to be performed from outside the device. |

### ■Related Functions

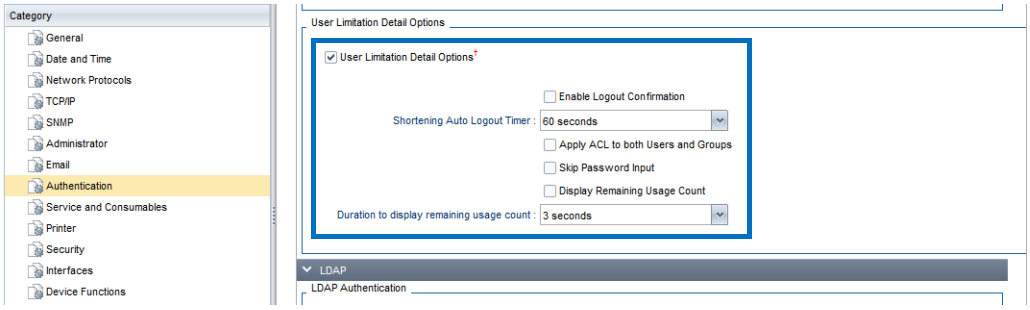
- 3.1 "User Authentication Settings" (☞ page 12)

### ■Restrictions

None

## 3.13 User Limitation Detail Options

You can make detailed settings for user restrictions.




### ■Configuring the Setting

1. Enable the **User Limitation Detail Options** checkbox.
2. Enable the checkbox for the setting you want to apply. For **Shortening Auto Logout Timer** and **Duration to display remaining usage count**, select a setting.

| Setting | Description | |
|---|---|---|
| **Enable Logout Confirmation** | A logout confirmation screen is displayed when the Logout button is pressed. | |
| **Shortening Auto Logout Timer** | You can select the interval for retry attempts when auto logout fails. | |
| | **60 seconds** | When the specified number of seconds elapses, auto logout is attempted again. |
| | **10 seconds** | |
| | **20 seconds** | |
| | **30 seconds** | |
| **Apply ACL to both Users and Groups** | The user can log in only when authentication with the Address Book in the device and external authentication using the SDK application are completed.<br>When this setting is disabled, login is possible if either authentication with the Address Book in the device or external authentication using the SDK application is completed. | |
| **Skip Password Input** | The Password Entry screen is not displayed at the time of login. | |

<table>
<tr><th>Setting</th><th colspan="2">Description</th></tr>
<tr><td>Display Remaining Usage Count</td><td colspan="2">When a limit has been set for a function such as Copy, the number of times the function can be used is displayed.</td></tr>
<tr><td rowspan="5">Duration to display remaining usage count</td><td colspan="2">You can select how long the remaining number of times the function can be used is displayed.</td></tr>
<tr><td>3 seconds</td><td rowspan="4">The remaining number of times the function can be used is displayed for the specified number of seconds.</td></tr>
<tr><td>6 seconds</td></tr>
<tr><td>9 seconds</td></tr>
<tr><td>12 seconds</td></tr>
</table>

If Card Authentication Package V2 has been implemented, it is recommended that the following setting be used:

- **Enable Logout Confirmation**: Enable

## ■Related Functions

- 3.10 “Enable External Authentication” (☞ page 25)

## ■Restrictions

None

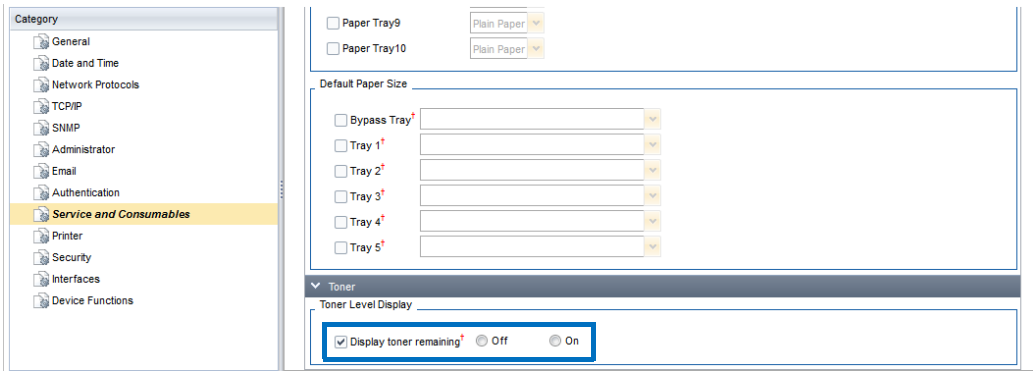
# 4. Service and Consumables

This section includes information on the extended functions available for the **Service and Consumables** category.

| Category | Subcategory | | Extended Function | Page |
|---|---|---|---|---|
| **Service and Consumables** | **Toner** | **Toner Level Display** | **Display toner remaining** | 32 |

## 4.1 Display Toner Remaining

You can select whether to display the "toner level icon" in the device's LCD panel.




### ■Configuring the Setting

1. Enable the **Display toner remaining** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Off** | The toner level icon is not displayed. |
| **On** | The toner level icon is displayed. |

### ■Related Functions

None

### ■Restrictions

- The toner level icon can only be displayed on LCD panels with a screen resolution of WVGA or SVGA.

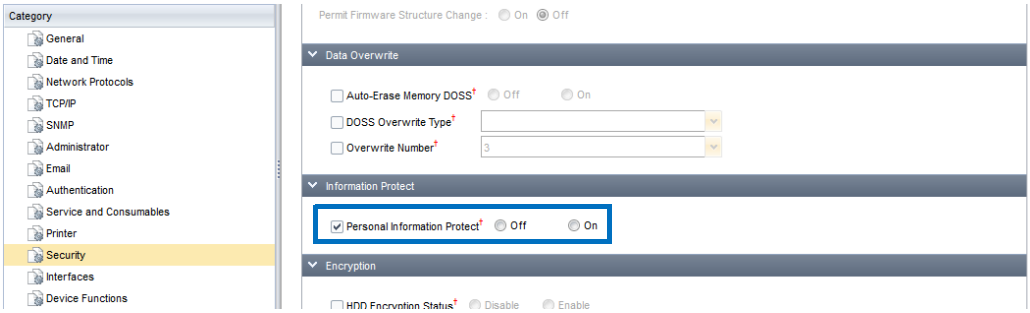
# 5. Security

This section includes information on the extended functions available for the **Security** category.

| Category | Subcategory | Extended Function | Page |
|---|---|---|---|
| **Security** | **Information Protect** | **Personal Information Protect** | 34 |

## 5.1 Personal Information Protect

You can select whether to allow only the administrator to view the device's job history.




### ■Configuring the Setting

1. Enable the **Personal Information Protect** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Off** | All users can view the job history. |
| **On** | Only the administrator can view the job history. |

### ■Related Functions

None

### ■Restrictions

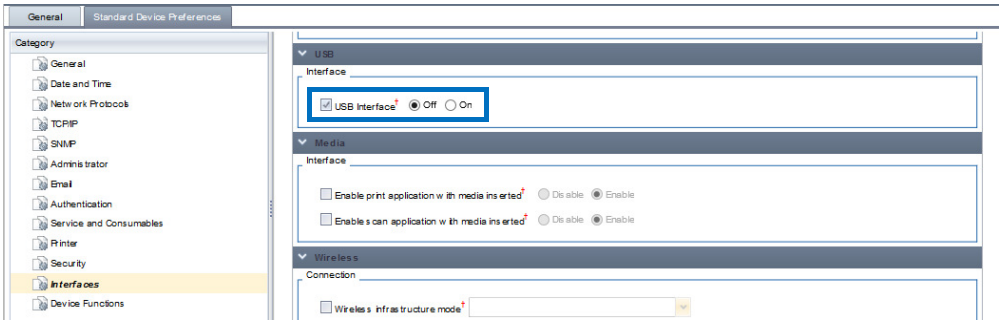
- This function will become effective after the device reboots.

# 6. Interfaces

This section includes information on the extended functions available for the **Interfaces** category.

## 6.1 USB Interface

You can select whether to enable the USB function when an optional board for USB connection is installed on a device.




### ■Configuring the Setting

1. Enable the **USB Interface** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Off** | The USB function is disabled. |
| **On** | The USB function is enabled. |

### ■Related Functions

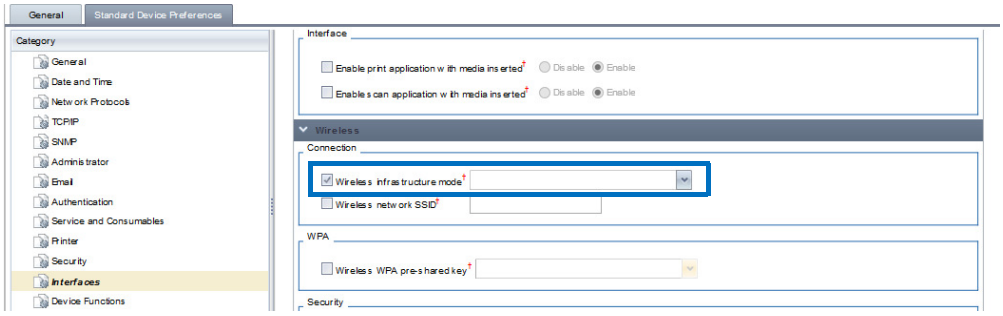
None

### ■Restrictions

- This function only supports USB type B connectors.

## 6.2 Wireless Infrastructure Mode

You can select the mode for wireless LAN communication when an optional board for a wireless LAN connection is installed on a device.




### ■Configuring the Setting

1. Enable the **Wireless infrastructure mode** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **802.11 Ad-hoc Mode** | Ad-hoc Mode is used for communication. |
| **Infrastructure Mode** | Infrastructure Mode is used for communication. |

### ■Related Functions

None

### ■Restrictions

None

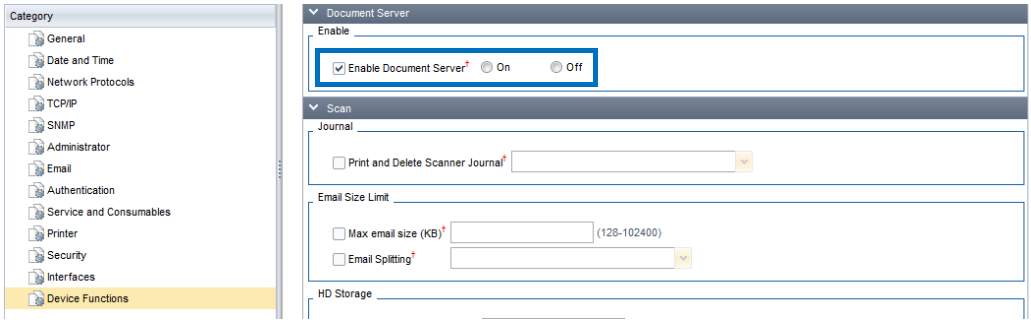
# 7. Device Functions

This section includes information on the extended functions available for the **Device Functions** category.

| Category | Subcategory | | Extended Function | Page |
|---|---|---|---|---|
| Device Functions | Document Server | Enable | Enable Document Server | 39 |
| | Scan | HD Storage | Store non-DS jobs to HD | 40 |
| | Function Priority | | Application switch method | 41 |

## 7.1 Enable Document Server

You can select whether to allow use of the Document Server.




### ■Configuring the Setting

1. Enable the **Enable Document Server** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **On** | The Document Server function is enabled. |
| **Off** | The Document Server function is disabled. |

### ■Related Functions

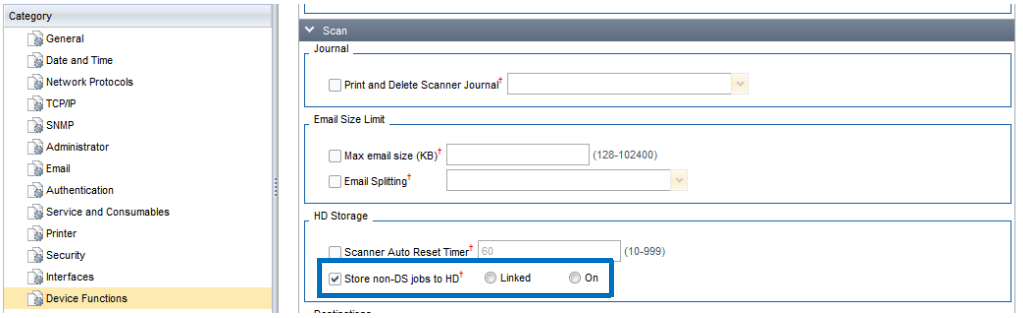
- 7.2 “Store Non-DS Jobs to HD” (☞ page 40)

### ■Restrictions

None

## 7.2 Store Non-DS Jobs to HD

You can select whether to enable the printing of temporary documents and saved documents and also whether to link the printing of temporary/saved documents with the Document Server function.




### ■Configuring the Setting

1. Enable the **Store non-DS jobs to HD** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **Linked** | Whether the printing of temporary/saved documents is available is linked to whether the Document Server function is enabled or disabled. |
| **On** | The printing of temporary/saved documents is available regardless of the Document Server function. |

Whether the printing of temporary/saved documents is available depends on the combination of **Enable Document Server** and **Store non-DS jobs to HD** settings, as shown below.

| | | Store non-DS jobs to HD | |
|---|---|---|---|
| | | **Linked** | **On** |
| **Enable Document Server** | **On** | Enabled | Enabled |
| | **Off** | Disabled | Enabled |

### ■Related Functions

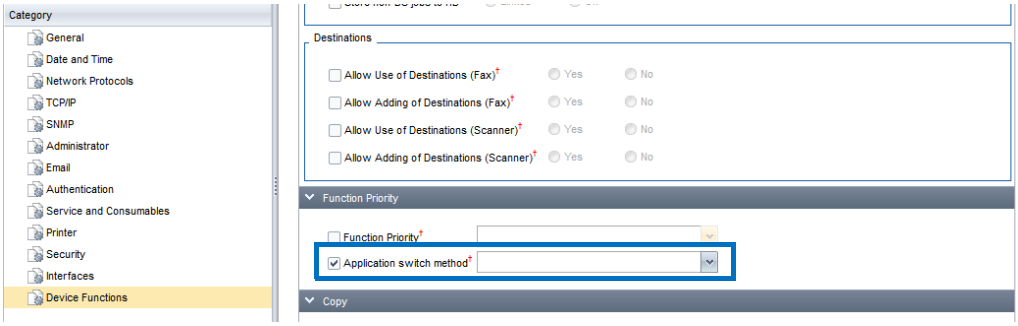
- 7.1 “Enable Document Server” (☞ page 39)

### ■Restrictions

- The setting for this function is disabled if the device detects an HDD malfunction.

## 7.3 Application Switch Method

You can select either to use the device's hard keys or the soft keys on the device's LCD panel to switch applications.




### ■Configuring the Setting

1. Enable the **Application switch method** checkbox.
2. Select a setting.

| Setting | Description |
|---|---|
| **SoftKey** | The soft keys on the device's LCD panel are used. |
| **HardKey** | The hard keys on the device are used. |

### ■Related Functions

None

### ■Restrictions

None


RICOH